Configure los Destinatarios de Notificación SNMP en un Switch a través de la CLI

Objetivo

El protocolo simple de administración de red (SNMP) es un protocolo de administración de red para redes IP que ayuda a registrar, almacenar y compartir información sobre los dispositivos de la red. Es un protocolo de capa de aplicación compuesto por un administrador SNMP, un agente SNMP y una base de información de administración (MIB) .

- Administrador SNMP: el administrador SNMP es en realidad un equipo administrativo que puede formar parte de un sistema de administración de red (NMS). Ejecuta las aplicaciones de monitoreo SNMP y recibe las notificaciones enviadas por el software Agente. El administrador SNMP utiliza la mayor cantidad de procesamiento y memoria necesaria para la administración de la red.
- Agente SNMP: los dispositivos del agente SNMP pueden ser un switch, un router u otro ordenador entre muchos otros. Aquí es donde reside la MIB. Los dispositivos del agente SNMP traducen la información a un formato que puede interpretar el administrador SNMP. Las notificaciones se envían al administrador SNMP y se denominan notificaciones de trampa o solicitudes de información. El dispositivo agente SNMP envía notificaciones de trampa cuando el dispositivo alcanza un parámetro específico. Los mensajes de trampa pueden ser autenticación de usuario incorrecta, uso de CPU, estado de link y otros eventos significativos. Esto ayuda al administrador a abordar los problemas de la red. Las trampas son simplemente notificaciones y no son reconocidas por el servidor de notificaciones. El servidor de notificaciones reconoce la solicitud de información. La información sólo está disponible en SNMPv2c y v3.
- MIB: Una MIB es un área de almacenamiento de información virtual para la información de administración de red. Se compone de una colección de objetos administrados.

SNMP tiene tres versiones significativas.

- SNMPv1: esta es la versión inicial de SNMP.
- SNMPv2c: esta versión utiliza una forma de seguridad basada en la comunidad, al igual que SNMPv1, reemplazando el Marco de seguridad y administración basado en el participante de SNMPv2.
- SNMPv3: es un protocolo basado en estándares interoperables definido en RFC2273, 2274 y 2275. Proporciona acceso seguro a los dispositivos mediante la autenticación y el cifrado de paquetes a través de la red. Debido a las vulnerabilidades de seguridad de otras versiones de SNMP, se recomienda utilizar SNMPv3.

Este documento tiene como objetivo mostrarle cómo configurar el host con la dirección IP 192.168.100.139 como el destinatario de notificación SNMP de las trampas SNMPv2c usando la Interfaz de línea de comandos (CLI) de un switch.

En este artículo se asume que ya ha instalado y configurado el administrador SNMP. También supone que ya ha agregado el switch al administrador SNMP para monitorear.

Dispositivos aplicables

- Serie Sx250
- Serie Sx300
- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

Versión del software

- 1.4.7.05 — Sx300, Sx500
- 2.2.8.04: Sx250, Sx350, SG350X, Sx550X

Configuración de la Cadena de Comunidad SNMP en un Switch

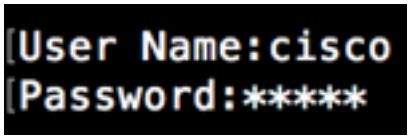
Las cadenas de comunidad SNMP actúan como contraseñas incrustadas que autentican el acceso a los objetos MIB. Sólo se define en SNMPv1 y SNMPv2 ya que SNMPv3 funciona con usuarios en lugar de con comunidades. Los usuarios pertenecen a grupos que tienen derechos de acceso asignados. Utilice la cadena de comunidad como contraseña o nombre de grupo al agregar el switch al administrador SNMP. Se debe configurar una cadena de comunidad al configurar SNMP para que el host SNMP y el administrador SNMP puedan conectarse.

Una cadena de comunidad puede tener una de estas propiedades:

- Sólo lectura (RO): esta opción permite el acceso de lectura a los dispositivos de administración autorizados a todos los objetos de la MIB, pero no permite el acceso de escritura.
- Read-write (RW): esta opción permite el acceso de lectura y escritura a los dispositivos de administración autorizados a todos los objetos de la MIB; sin embargo, no permite el acceso a las cadenas de comunidad.

Para configurar una cadena de comunidad SNMP, siga estos pasos:

Paso 1. Inicie sesión en el switch.



Paso 2. Cambie al modo de configuración global.

```
SG500#configure terminal
```

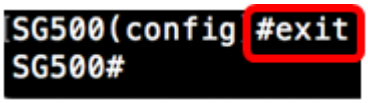
Paso 3. En el modo de configuración global, configure la cadena de comunidad ingresando el siguiente comando.

```
SG500(config)#snmp-server community [word][view ro|rw][access-list number]
```

- Word: esto actuará como una contraseña y permitirá el acceso al protocolo SNMP.
- view: (Opcional) Especifique el registro de vista al que puede acceder la comunidad.
- ro|rw — (Opcional) Especifique uno de los dos campos de sólo lectura (o) si desea que las estaciones de administración autorizadas recuperen objetos MIB. Especifique read-write (rw) si desea que las estaciones de administración autorizadas recuperen y modifiquen objetos MIB. El valor predeterminado es el acceso de sólo preparación a todos los objetos.
- access-list-number: (Opcional) Introduzca un número de lista de acceso IP estándar entre 1 y 99 y entre 1300 y 1999.

Nota: En este ejemplo, SNMPComcommunity actuará como contraseña. Esto se utilizará al agregar el switch al administrador SNMP.

Paso 4. Cambie al modo EXEC privilegiado ingresando el comando **exit**.



Paso 5. Verifique la configuración ejecutando el comando:

```
SG500#show snmp
```

```
SG500#show snmp

SNMP is enabled.


SNMP traps Source IPv4 interface:
SNMP informs Source IPv4 interface:
SNMP traps Source IPv6 interface:
SNMP informs Source IPv6 interface:

  Community-String    Community-Access    View name     IP address      Mask
------------------- ------------------ -------------- ------------ ------------
   SNMPCommunity         read only         Default     192.168.100.
                                                       139
      private            read write        Default         All
       public            read only         Default         All

 Community-String   Group name     IP address          Mask       Version  Type
----------------- ------------ --------------- --------------- ------- ------

Traps are enabled.
Authentication-failure trap is enabled.

Version 1,2 notifications
 Target Address    Type    Community   Version   Udp   Filter   To    Retries
                                                Port  name     Sec
--------------- ------- ---------- --------- ----- ------- ----- ---------
192.168.100.119    Trap   SNMPCommuni     2      162           0       0
                          ty


Version 3 notifications
 Target Address    Type    Username   Security Udp   Filter   To    Retries
                           Level    Port  name     Sec
--------------- ------- ---------- -------- ----- ------- ----- ---------

System Contact:
System Location:

SG500#_

SG500#_
```

Paso 6. (Opcional) Guarde los parámetros en el archivo de configuración.

```
SG500#copy running-config startup-config
```

```
SG500#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
13-Jul-2017 19:36:07 %COPY-I-FILECPY: Files Copy - source URL running-config destination
 URL flash://startup-config
13-Jul-2017 19:36:14 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
SG500#
```

Paso 7. Pulse **Y** para continuar.

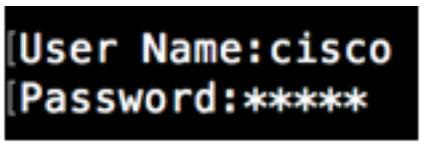
```
SG500#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
13-Jul-2017 19:36:07 %COPY-I-FILECPY: Files Copy - source URL running-config destination
 URL flash://startup-config
13-Jul-2017 19:36:14 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded
SG500#
```

Configure los Destinatarios de Notificación SNMP en un Switch a través de la CLI

SNMP permite que el switch envíe notificaciones a los administradores SNMP cuando se producen eventos. Las notificaciones SNMP pueden ser trampas o solicitudes de información. Una trampa es un mensaje SNMP destinado a notificar al administrador SNMP acerca del evento que ocurrió. Las trampas no son confiables porque el receptor no envía un reconocimiento cuando se recibe una trampa. Una Información SNMP funciona con el mismo principio que una Trampa. La diferencia principal entre una Trampa y una Información es que la aplicación remota reconoce la recepción de la Información. Además, se descarta una trampa tan pronto como se envía, mientras que una solicitud de información se guarda en la memoria hasta que se recibe una solicitud, de lo contrario se agota el tiempo de espera. SNMPv1 no admite la información SNMP.

Esta sección, aunque es opcional, le guiará en la configuración de los destinatarios de notificación SNMP a través de la CLI del switch.

Paso 1. Inicie sesión en el switch.

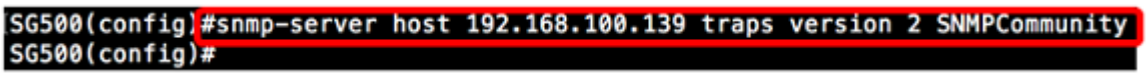


Paso 2. Cambie al modo de configuración global.

```
SG500#configure terminal
```

Paso 3. En el modo de configuración global, especifique el destinatario de la notificación ejecutando el siguiente comando:

```
SG500(config)#snmp-server host [IPaddress] traps
[version] SNMP Community
```



- snmp-server — Este comando permite que el dispositivo sea administrado por SNMP
- host: este comando le permite especificar la dirección IP del destinatario de la notificación.

  Nota: En este ejemplo, la dirección IP es 192.168.100.139.
- tipo de notificación: es el tipo de notificación que recibiría el administrador de red.
- **Nota:** En este ejemplo, la notificación se establece en trampas en lugar de informes.
- versión: utilizaría la versión SNMP especificada de las notificaciones.

  Nota: En este ejemplo, se utiliza la versión 2.

- Comunidad SNMP: es el nombre de la comunidad SNMP.

  Nota: En este ejemplo, se ingresa SNMPComcommunity.

  Paso 4. Cambie al modo EXEC privilegiado ingresando el comando exit.

```
SG500(config)#exit
```

```
SG500(config)#exit
SG500#_
```

  Paso 5. (Opcional) Guarde los parámetros en el archivo de configuración.

```
SG500#copy running-config startup config
```

  Paso 6. Pulse **Y** para confirmar la acción.

```
SG500#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?
```

  Ahora debería haber agregado un destinatario de notificación SNMP.