Configurar destinatários de notificação SNMP em um switch por meio da CLI

Objetivo

O SNMP (Simple Network Management Protocol) é um protocolo de gerenciamento de rede para redes IP que ajuda a gravar, armazenar e compartilhar informações sobre os dispositivos na rede. É um protocolo da camada de aplicação composto por um Gerenciador SNMP, um Agente SNMP e uma Base de Informações de Gerenciamento (MIB - Management Information Base) .

- Gerenciador SNMP — O Gerenciador SNMP é, na verdade, um computador administrativo que pode fazer parte de um Sistema de Gerenciamento de Rede (NMS). Ele executa os aplicativos de monitoramento SNMP e recebe as notificações enviadas pelo software Agent. O gerenciador SNMP usa o processamento e a memória mais necessários para o gerenciamento da rede.
- Agente SNMP — Os dispositivos do agente SNMP podem ser um switch, um roteador ou outro computador, entre muitos outros. É aqui que reside a MIB. Os dispositivos SNMP Agent traduzem informações em um formato que pode ser interpretado pelo gerenciador SNMP. As notificações são feitas para o gerenciador SNMP e são chamadas de notificações Trap ou de solicitações Inform. As notificações de interceptação são enviadas pelo dispositivo de agente SNMP quando um parâmetro específico é alcançado pelo dispositivo. As mensagens de interceptação podem ser autenticação de usuário incorreta, uso da CPU, status do link e outros eventos significativos. Isso ajuda o administrador a resolver problemas de rede. Armadilhas são apenas notificações, e não confirmadas pelo servidor de notificação. A solicitação de informações é confirmada pelo servidor de notificação. As informações estão disponíveis somente no SNMPv2c e v3.
- MIB — Uma MIB é uma área de armazenamento de informações virtual para informações de gerenciamento de rede. Ele é composto por uma coleção de objetos gerenciados.

O SNMP tem três versões significativas.

- SNMPv1 — Esta é a versão inicial do SNMP.
- SNMPv2c — Esta versão usa uma forma de segurança baseada em comunidade, assim como o SNMPv1, substituindo a Estrutura de Segurança e Administração baseada em Parte do SNMPv2.
- SNMPv3 — Este é um protocolo baseado em padrões interoperáveis definido em RFC2273, 2274 e 2275. Fornece acesso seguro a dispositivos autenticando e criptografando pacotes pela rede. Devido às vulnerabilidades de segurança de outras versões do SNMP, é recomendável usar SNMPv3.

Este documento tem como objetivo mostrar como configurar o host com o endereço IP 192.168.100.139 como o destinatário da notificação SNMP de interceptações SNMPv2c usando a Interface de Linha de Comando (CLI) de um switch.

Este artigo pressupõe que você já instalou e configurou o gerenciador SNMP. Também pressupõe que você já adicionou o switch ao gerenciador SNMP para monitoramento.

Dispositivos aplicáveis

- Sx250 Series
- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

Versão de software

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

Configurar a sequência de caracteres da comunidade SNMP em um switch

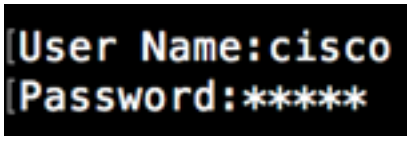
As strings de comunidade SNMP atuam como senhas incorporadas autenticando o acesso a objetos MIB. Ele é definido somente em SNMPv1 e SNMPv2, pois o SNMPv3 funciona com usuários em vez de comunidades. Os usuários pertencem a grupos com direitos de acesso atribuídos a eles. Use a string de comunidade como senha ou nome de grupo ao adicionar o switch ao Gerenciador SNMP. Uma string de comunidade deve ser configurada ao configurar o SNMP para que o host SNMP e o gerenciador SNMP possam se conectar.

Uma string de comunidade pode ter uma destas propriedades:

- Somente leitura (RO) — Essa opção permite acesso de leitura a dispositivos de gerenciamento autorizados para todos os objetos na MIB, mas não permite acesso de gravação.
- Read-write (RW) — Essa opção permite acesso de leitura e gravação a dispositivos de gerenciamento autorizados para todos os objetos na MIB, no entanto, ela não permite acesso às strings de comunidade.

Para configurar uma string de comunidade SNMP, siga estas etapas:

Etapa 1. Faça login no switch.



Etapa 2. Mude para o modo de configuração global.

```
SG500#configure terminal
```

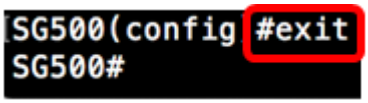
Etapa 3. No modo de configuração global, configure a string de comunidade inserindo o seguinte comando.

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

- word — Isso atuará como uma senha e permitirá o acesso ao protocolo SNMP.
- view — (Opcional) Especifique o registro de exibição acessível à comunidade.
- ro|rw — (Opcional) Especifique somente leitura (ro) se quiser que estações de gerenciamento autorizadas recuperem objetos MIB. Especifique a leitura/gravação (rw) se desejar que estações de gerenciamento autorizadas recuperem e modifiquem objetos MIB. O valor padrão é o acesso somente pronto a todos os objetos.
- access-list-number — (Opcional) Insira um número padrão da lista de acesso IP de 1 a 99 e 1300 a 1999.

Note: Neste exemplo, SNMPCmunity atuará como a senha. Isso será usado ao adicionar o switch ao gerenciador SNMP.

Etapa 4. Mude para o modo EXEC Privilegiado inserindo o comando **exit**.



Etapa 5. Verifique a configuração executando o 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#_
```

Etapa 6. (Opcional) Salve as configurações no arquivo de configuração.

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

```
SG50 #copy running-config startup-config
Overw  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#
```

Passo 7. Pressione **Y** para continuar.

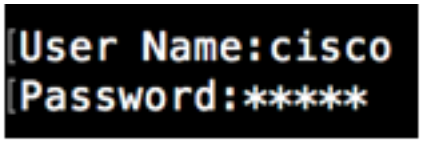
```
SG500#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
13-Jul-2017 19:36:07 %COPY-I-FILECPY: Files Copy - source URL running-config destination
 URL flash://startup-config
13-Jul-2017 19:36:14 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded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

Configurar destinatários de notificação SNMP em um switch por meio da CLI

O SNMP permite que o switch envie notificações aos gerenciadores SNMP quando ocorrem eventos. As notificações de SNMP podem ser interceptações ou solicitações de informação. Uma interceptação (Trap) é uma mensagem SNMP destinada a notificar o gerenciador SNMP sobre o evento que ocorreu. As interceptações não são confiáveis porque o receptor não envia uma confirmação quando uma interceptação é recebida. Uma informação SNMP opera com o mesmo princípio de uma interceptação (Trap). A principal diferença entre uma interceptação (Trap) e uma informação (Inform) é que o aplicativo remoto confirma o recebimento da informação. Além disso, uma interceptação (Trap) é descartada assim que é enviada, enquanto uma solicitação de informação é mantida na memória até que uma solicitação seja recebida, caso contrário ela expira. A informação SNMP não é suportada por SNMPv1.

Esta seção, embora opcional, o guiará na configuração de Destinatários de Notificação SNMP através da CLI do Switch.

Etapa 1. Faça login no switch.

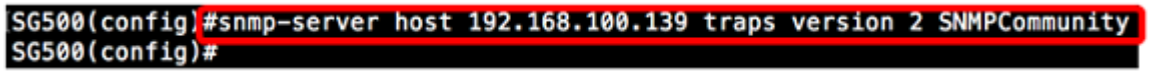


Etapa 2. Mude para o modo de configuração global.

```
SG500#configure terminal
```

Etapa 3. No modo de configuração global, especifique o destinatário da notificação executando o seguinte comando:

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



- snmp-server — Este comando permite que o dispositivo seja gerenciado por SNMP
- host — Este comando permite especificar o endereço IP do destinatário da notificação.

Note: Neste exemplo, o endereço IP é 192.168.100.139.

- tipo de notificação — Esse é o tipo de notificação que o gerente de rede receberá.
- **Note:** Neste exemplo, a notificação é definida como armadilhas em vez de informações.
- Versão — Usaria a versão SNMP especificada das notificações.

Note: Neste exemplo, a versão 2 é usada.

- Comunidade SNMP — Este é o nome da comunidade SNMP.

  Note: Neste exemplo, SNMPCmunity é inserido.

  Etapa 4. Mude para o modo EXEC Privilegiado inserindo o comando exit.

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

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

  Etapa 5. (Opcional) Salve as configurações no arquivo de configuração.

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

  Etapa 6. Pressione **Y** para confirmar a ação.

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

  Agora você deve ter adicionado um destinatário de notificação SNMP.