Configurazione dei destinatari delle notifiche SNMP su uno switch dalla CLI

Obiettivo

Simple Network Management Protocol (SNMP) è un protocollo di gestione di rete per reti IP che consente di registrare, archiviare e condividere informazioni sui dispositivi della rete. Si tratta di un protocollo a livello di applicazione composto da SNMP Manager, SNMP Agent e MIB (Management Information Base).

- SNMP Manager — SNMP Manager è in realtà un computer di amministrazione che può far parte di un Network Management System (NMS). Esegue le applicazioni di monitoraggio SNMP e riceve le notifiche inviate dal software dell'agente. Il programma di gestione SNMP utilizza la maggior parte dell'elaborazione e della memoria necessaria per la gestione della rete.
- Agente SNMP: i dispositivi dell'agente SNMP possono essere, tra gli altri, uno switch, un router o un altro computer. È qui che risiede il MIB. I dispositivi dell'agente SNMP convertono le informazioni in un formato che può essere interpretato da SNMP Manager. Le notifiche vengono inviate al programma di gestione SNMP e vengono chiamate notifiche trap o richieste Inform. Le notifiche di trap vengono inviate dal dispositivo agente SNMP quando il dispositivo raggiunge un parametro specifico. I messaggi trap possono essere costituiti da un'autenticazione utente non corretta, dall'utilizzo della CPU, dallo stato dei collegamenti e da altri eventi significativi. Ciò consente all'amministratore di risolvere i problemi di rete. I trap sono semplicemente notifiche e non vengono riconosciuti dal server di notifica. La richiesta di informazioni viene riconosciuta dal server di notifica. Inform è disponibile solo su SNMPv2c e v3.
- MIB: un MIB è un'area di storage virtuale per le informazioni di gestione della rete. È composto da un insieme di oggetti gestiti.

L'SNMP ha tre versioni significative.

- SNMPv1: è la versione iniziale di SNMP.
- SNMPv2c: questa versione utilizza una forma di sicurezza basata sulla community, proprio come SNMPv1, sostituendo la struttura amministrativa e di sicurezza basata su party di SNMPv2.
- SNMPv3: protocollo interoperabile basato su standard definito nelle RFC 2273, 2274 e 2275. Fornisce accesso sicuro ai dispositivi tramite l'autenticazione e la crittografia dei pacchetti sulla rete. A causa delle vulnerabilità di sicurezza di altre versioni di SNMP, si consiglia di utilizzare SNMPv3.

In questo documento viene spiegato come configurare l'host con l'indirizzo IP 192.168.100.139 come destinatario della notifica SNMP dei trap SNMPv2c tramite l'interfaccia della riga di comando (CLI) di uno switch.

In questo articolo si presume che SNMP Manager sia già stato installato e configurato. Inoltre, si presume che lo switch sia già stato aggiunto al programma di gestione SNMP per il monitoraggio.

Dispositivi interessati

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

Versione del software

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

Configurazione della stringa della community SNMP su uno switch

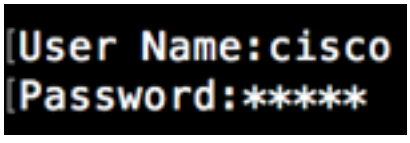
Le stringhe della community SNMP fungono da password incorporate che autenticano l'accesso agli oggetti MIB. È definito solo in SNMPv1 e SNMPv2 poiché SNMPv3 funziona con gli utenti anziché con le community. Gli utenti appartengono a gruppi a cui sono stati assegnati diritti di accesso. Utilizzare la stringa della community come password o nome di gruppo quando si aggiunge lo switch a SNMP Manager. Una stringa della community deve essere configurata durante la configurazione di SNMP in modo che l'host SNMP e il programma di gestione SNMP possano connettersi.

Una stringa della community può avere una delle seguenti proprietà:

- Read-only (RO) - Questa opzione consente l'accesso in lettura ai dispositivi di gestione autorizzati a tutti gli oggetti nel MIB, ma non l'accesso in scrittura.
- Read-write (RW) - Questa opzione consente l'accesso in lettura e scrittura ai dispositivi di gestione autorizzati per tutti gli oggetti nel MIB, ma non consente l'accesso alle stringhe della community.

Per configurare una stringa della community SNMP, eseguire la procedura seguente:

Passaggio 1. Accedere allo switch.



Passaggio 2. Passare alla modalità di configurazione globale.

```
SG500#configure terminal
```

Passaggio 3. In modalità di configurazione globale, configurare la stringa della community immettendo il comando seguente.

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

- parola — funziona come una password e consente l'accesso al protocollo SNMP.
- view - (Facoltativo) Specifica il record della vista accessibile alla comunità.
- ro|rw — (Facoltativo) Specificare la modalità di sola lettura (ro) se si desidera che le stazioni di gestione autorizzate recuperino gli oggetti MIB. Specificare read-write (rw) se si desidera che le stazioni di gestione autorizzate recuperino e modifichino gli oggetti MIB. Il valore predefinito è l'accesso in sola lettura a tutti gli oggetti.
- access-list-number: (facoltativo) immettere un numero di elenco degli accessi IP standard compreso tra 1 e 99 e tra 1300 e 1999.

Nota: Nell'esempio, SNMPCcommunity fungerà da password. Questo verrà utilizzato quando si aggiunge lo switch a SNMP Manager.

```
SG500(config)#snmp-server community SNMPCommunity view ro
SG500(config)#_
```

Passaggio 4. Passare alla modalità di esecuzione privilegiata immettendo il comando **exit**.

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

Passaggio 5. Verificare la configurazione eseguendo il 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#_
```

Passaggio 6. (Facoltativo) Salvare le impostazioni nel file di configurazione.

```
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#
```

Passaggio 7. Premere **Y** per continuare.

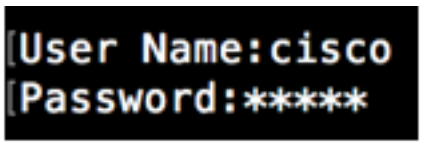
```
SG500#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?Y
13-Jul-2017 19:36:07 %COPY-I-FILECPY: Files Copy - source URL running-config destination
 URL flash://startup-config
13-Jul-2017 19:36:14 %COPY-N-TRAP: The copy operation was completed successfully
Copy succeeded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

Configurazione dei destinatari delle notifiche SNMP su uno switch dalla CLI

Il protocollo SNMP consente allo switch di inviare notifiche ai manager SNMP quando si verificano eventi. Le notifiche SNMP possono essere trap o richieste informative. Un trap è un messaggio SNMP che consente di notificare al programma di gestione SNMP l'evento che si è verificato. I trap non sono affidabili perché il destinatario non invia una conferma quando riceve un trap. Un SNMP Inform opera sullo stesso principio di un Trap. La differenza principale tra una trap e un Inform consiste nel fatto che l'applicazione remota conferma la ricezione dell'Inform. Inoltre, una trap viene scartata non appena viene inviata, mentre una richiesta Inform rimane in memoria fino a quando non viene ricevuta, altrimenti si verifica il timeout. SNMP Inform non è supportato da SNMPv1.

Questa sezione, sebbene facoltativa, consente di configurare i destinatari delle notifiche SNMP dalla CLI dello switch.

Passaggio 1. Accedere allo switch.

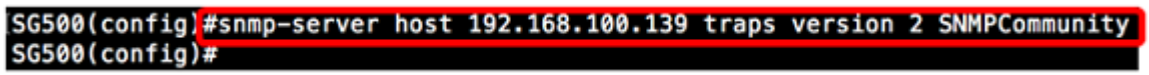


Passaggio 2. Passare alla modalità di configurazione globale.

```
SG500#configure terminal
```

Passaggio 3. In modalità di configurazione globale, specificare il destinatario della notifica eseguendo il comando seguente:

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



- snmp-server — questo comando consente al dispositivo di essere gestito da SNMP
- host: questo comando consente di specificare l'indirizzo IP del destinatario della notifica.

  Nota: Nell'esempio, l'indirizzo IP è 192.168.100.139.
- tipo di notifica: il tipo di notifica che il gestore della rete riceverebbe.
- **Nota:** In questo esempio, la notifica è impostata su trap anziché su informs.
- version - utilizza la versione SNMP specificata delle notifiche.

  Nota: nell'esempio viene utilizzata la versione 2.
- Community SNMP — è il nome della community SNMP.

Nota: Nell'esempio, viene immesso SNMPCcommunity.

Passaggio 4. Passare alla modalità di esecuzione privilegiata immettendo il comando exit.

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

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

Passaggio 5. (Facoltativo) Salvare le impostazioni nel file di configurazione.

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

Passaggio 6. Premere **Y** per confermare l'azione.

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

A questo punto è necessario aggiungere un destinatario della notifica SNMP.