

Configurazione delle impostazioni di autenticazione del server SSH su uno switch dalla CLI

Introduzione

Secure Shell (SSH) è un protocollo che permette di connettersi in modo sicuro a dispositivi di rete remoti. Questa connessione offre una funzionalità simile a una connessione Telnet, con la differenza che è crittografata. SSH consente all'amministratore di configurare lo switch dalla riga di comando (CLI) con un programma di terze parti.

Lo switch agisce come client SSH che fornisce funzionalità SSH agli utenti della rete. Lo switch usa un server SSH per fornire i servizi SSH. Quando l'autenticazione del server SSH è disabilitata, lo switch considera attendibile qualsiasi server SSH, riducendo la sicurezza della rete. Se il servizio SSH è abilitato sullo switch, la sicurezza è migliorata.

Questo articolo fornisce istruzioni su come configurare l'autenticazione del server su uno switch gestito tramite la CLI.

Dispositivi interessati

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

Versione del software

- 1.4.7.06 - Sx300, Sx500
- 2.2.8.04 - Sx350, SG350X, Sx550X

Configurazione delle impostazioni del server SSH

Configurazione delle impostazioni di autenticazione del server SSH

Passaggio 1. Accedere alla console dello switch. Il nome utente e la password predefiniti sono cisco/cisco. Se sono stati configurati un nuovo nome utente o password, immettere queste credenziali.

Nota: per informazioni su come accedere alla CLI di uno switch per PMI tramite SSH o Telnet, fare clic [qui](#).

```
[User Name:cisco  
[Password:*****
```

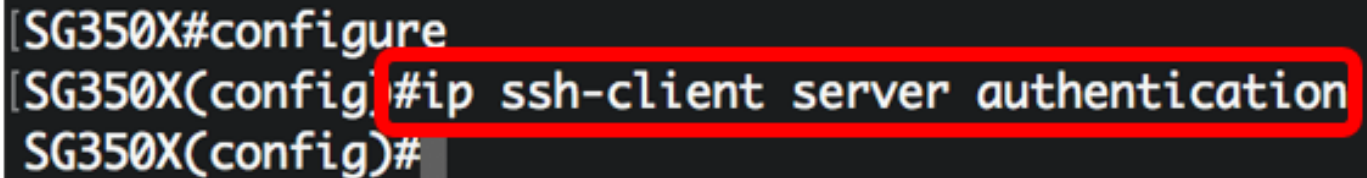
Nota: i comandi possono variare a seconda del modello di switch in uso. Nell'esempio, è possibile accedere allo switch SG350X in modalità Telnet.

Passaggio 2. In modalità di esecuzione privilegiata dello switch, accedere alla modalità di configurazione globale immettendo quanto segue:

```
SG350X#configure
```

Passaggio 3. Per abilitare l'autenticazione remota del server SSH da parte del client SSH, immettere quanto segue:

```
SG350X(config)#ip ssh-client server authentication
```

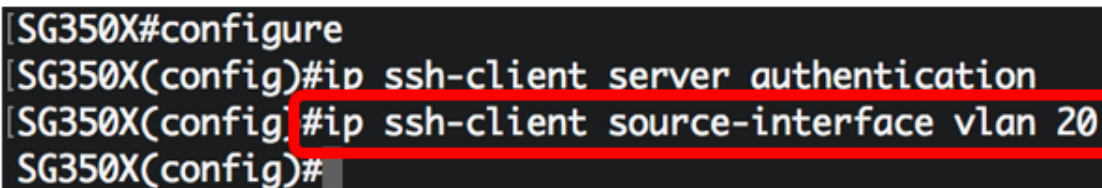


```
[SG350X#configure
[SG350X(config)#ip ssh-client server authentication
SG350X(config)#
```

Passaggio 4. Per specificare l'interfaccia di origine dell'indirizzo IPv4 da utilizzare come indirizzo IPv4 di origine per la comunicazione con i server SSH IPv4, immettere quanto segue:

```
SG350X(config)#ip ssh-client source-interface [id-interfaccia]
```

- interface-id - Specifica l'interfaccia di origine.



```
[SG350X#configure
[SG350X(config)#ip ssh-client server authentication
[SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#
```

Nota: Nell'esempio, l'interfaccia di origine è la VLAN 20.

Passaggio 5. (Facoltativo) Per specificare l'interfaccia di origine il cui indirizzo IPv6 verrà utilizzato come indirizzo IPv6 di origine per la comunicazione con i server SSH IPv6, immettere quanto segue:

```
SG350X(config)#ipv6 ssh-client source-interface [id-interfaccia]
```

- interface-id: per specificare l'interfaccia di origine.

Nota: In questo esempio l'indirizzo IPv6 di origine non è configurato.

Passaggio 6. Per aggiungere un server trusted alla tabella Server SSH remoto trusted, immettere quanto segue:

```
SG350X(config)#ip ssh-client server impronta digitale [host] | [indirizzo-ip] [impronta digitale]
```

I parametri sono:

- host: nome DNS (Domain Name Server) di un server SSH.
- ip-address: per specificare l'indirizzo di un server SSH. L'indirizzo IP può essere un indirizzo IPv4, IPv6 o IPv6z.
- impronta digitale - Impronta digitale della chiave pubblica del server SSH (32 caratteri esadecimali).

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#
```

Nota: Nell'esempio, l'indirizzo IP del server è 192.168.100.1 e l'impronta digitale utilizzata è 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8.

Passaggio 7. Per tornare in modalità di esecuzione privilegiata, immettere il comando **exit**:

```
SG350X(config)#exit
```

```
SG350X#configure
SG350X(config)#ip ssh-client server authentication
SG350X(config)#ip ssh-client source-interface vlan 20
SG350X(config)#$00.1 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8
SG350X(config)#exit
SG350X#
```

Passaggio 8. Per visualizzare le impostazioni di autenticazione del server SSH sullo switch, immettere quanto segue:

```
SG350X#show ip ssh-client server [host] | ip-address]
```

I parametri sono:

- host: nome DNS (Domain Name Server) di un server SSH.
- ip-address: per specificare l'indirizzo di un server SSH. L'indirizzo IP può essere un indirizzo IPv4, IPv6 o IPv6z.

```
SG350X(config)#exit
SG350X#show ip ssh-client server 192.168.100.1
SSH Server Authentication IS Enabled

Server address          : 192.168.100.1
Server Key Fingerprint : 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8

SG350X#
```

Nota: Nell'esempio, viene immesso l'indirizzo IP 192.168.100.1 del server.

Passaggio 9. (Facoltativo) In modalità di esecuzione privilegiata dello switch, salvare le impostazioni configurate nel file della configurazione di avvio immettendo quanto segue:

```
SG350X#copy running-config startup-config
```

```
[SG350X#copy running-config startup-config
Overwrite file [startup-config]... (Y/N)[N] ?
```

Passaggio 10. (Facoltativo) Premere **Y** per Yes (Sì) o **N** per No sulla tastiera quando si attiva Overwrite file [startup-config]...viene visualizzato il prompt ..

```
SG350X#copy running-config startup-config  
Overwrite file [startup-config]... (Y/N)[N] ?Y  
22-Sep-2017 04:09:18 %COPY-I-FILECOPY: Files Copy - source URL running-config des  
tination URL flash://system/configuration/startup-config  
22-Sep-2017 04:09:20 %COPY-N-TRAP: The copy operation was completed successfully  
SG350X#
```

A questo punto, è possibile imparare a configurare l'autenticazione del server su uno switch gestito dalla CLI.