Konfigurieren der Authentifizierungseinstellungen des SSH-Servers auf einem Switch über die CLI

Einführung

Secure Shell (SSH) ist ein Protokoll, das eine sichere Remote-Verbindung mit bestimmten Netzwerkgeräten ermöglicht. Diese Verbindung stellt Funktionen bereit, die einer Telnet-Verbindung ähnlich sind, jedoch verschlüsselt sind. Mithilfe von SSH kann der Administrator den Switch über die Befehlszeilenschnittstelle (CLI) mit einem Drittanbieterprogramm konfigurieren.

Der Switch fungiert als SSH-Client, der den Benutzern im Netzwerk SSH-Funktionen bereitstellt. Der Switch verwendet einen SSH-Server, um SSH-Dienste bereitzustellen. Wenn die SSH-Serverauthentifizierung deaktiviert ist, übernimmt der Switch jeden SSH-Server als vertrauenswürdig, was die Sicherheit in Ihrem Netzwerk verringert. Wenn der SSH-Dienst auf dem Switch aktiviert ist, wird die Sicherheit erhöht.

Dieser Artikel enthält Anweisungen zum Konfigurieren der Serverauthentifizierung auf einem verwalteten Switch über die CLI.

Anwendbare Geräte

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

Softwareversion

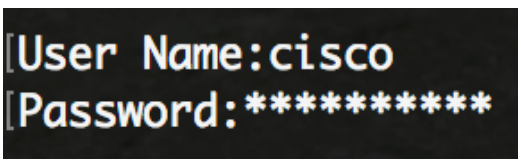
- 1.4.7.06 - Sx300, Sx500
- 2.2.8.04 - Sx350, SG350X, Sx550X

Konfigurieren der SSH-Servereinstellungen

Konfigurieren der Authentifizierungseinstellungen für den SSH-Server

Schritt 1: Melden Sie sich bei der Switch-Konsole an. Der Standard-Benutzername und das Kennwort lautet cisco/cisco. Wenn Sie einen neuen Benutzernamen oder ein neues Kennwort konfiguriert haben, geben Sie stattdessen die Anmeldeinformationen ein.

Hinweis: Um zu erfahren, wie Sie über SSH oder Telnet auf eine SMB-Switch-CLI zugreifen, klicken Sie hier.



Hinweis: Die Befehle können je nach dem genauen Switch-Modell variieren. In diesem Beispiel

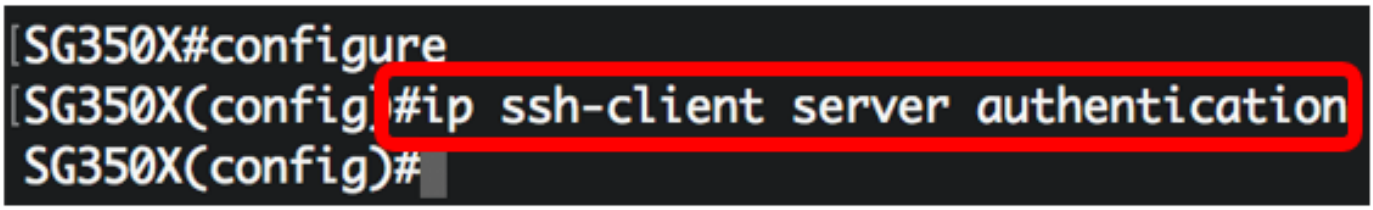
erfolgt der Zugriff auf den Switch SG350X über Telnet.

Schritt 2: Geben Sie im privilegierten EXEC-Modus des Switches Folgendes ein, um in den globalen Konfigurationsmodus zu wechseln:

```
Konfiguration von SG350X#
```

Schritt 3: Um die Remote-SSH-Serverauthentifizierung durch den SSH-Client zu aktivieren, geben Sie Folgendes ein:

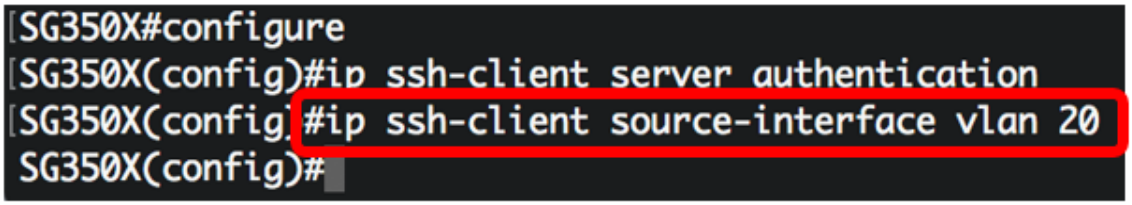
```
SG350X(config)#ip SSH-Client-Serverauthentifizierung
```



Schritt 4: Geben Sie Folgendes ein, um die Quellschnittstelle festzulegen, deren IPv4-Adresse als Quell-IPv4-Adresse für die Kommunikation mit IPv4-SSH-Servern verwendet wird:

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

- interface-id - Gibt die Quellschnittstelle an.



Hinweis: In diesem Beispiel ist die Quellschnittstelle VLAN 20.

Schritt 5: (Optional) Geben Sie Folgendes ein, um die Quellschnittstelle anzugeben, deren IPv6-Adresse als IPv6-Quelladresse für die Kommunikation mit IPv6 SSH-Servern verwendet wird:

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

- interface-id - Gibt die Quellschnittstelle an.

Hinweis: In diesem Beispiel ist die IPv6-Quelladresse nicht konfiguriert.

Schritt 6: Geben Sie Folgendes ein, um der Tabelle für vertrauenswürdige Remote-SSH-Server einen vertrauenswürdigen Server hinzuzufügen:

```
SG350X(config)#ip ssh-Client-Server-Fingerabdruck [Host | ip-address] [Fingerabdruck]
```

Die Parameter sind:

- host - Domain Name Server (DNS)-Name eines SSH-Servers.
- ip-address - Gibt die Adresse eines SSH-Servers an. Bei der IP-Adresse kann es sich um eine IPv4-, IPv6- oder IPv6z-Adresse handeln.
- fingerprint - Fingerprint des öffentlichen Schlüssels des SSH-Servers (32 Hexadezimalzeichen).

```
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)#
```

Hinweis: In diesem Beispiel lautet die IP-Adresse des Servers 192.168.100.1 und der verwendete Fingerabdruck 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8.

Schritt 7: Geben Sie den Befehl **exit** ein, um zum privilegierten EXEC-Modus zurückzukehren:

`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#
```

Schritt 8: Um die Authentifizierungseinstellungen des SSH-Servers auf dem Switch anzuzeigen, geben Sie Folgendes ein:

`SG350X#show ip ssh-client-Server [Host | ip-address]`

Die Parameter sind:

- host - Domain Name Server (DNS)-Name eines SSH-Servers.
- ip-address - Gibt die Adresse eines SSH-Servers an. Bei der IP-Adresse kann es sich um eine IPv4-, IPv6- oder IPv6z-Adresse handeln.

```
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#
```

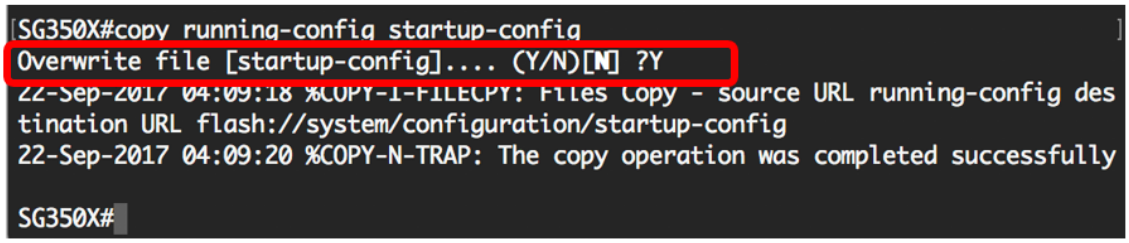
Hinweis: In diesem Beispiel wird die Server-IP-Adresse 192.168.100.1 eingegeben.

Schritt 9: (Optional) Speichern Sie im privilegierten EXEC-Modus des Switches die konfigurierten Einstellungen in der Startkonfigurationsdatei, indem Sie Folgendes eingeben:

`SG350X#copy running-config startup-config`

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

Schritt 10: (Optional) Drücken Sie **Y** für Yes (Ja) oder **N** für No (Nein) auf Ihrer Tastatur, sobald die Überschreibdatei [startup-config].... wird angezeigt.



Nun haben Sie gelernt, wie Sie die Serverauthentifizierung auf einem verwalteten Switch über die CLI konfigurieren.