Configurer les paramètres d'authentification du serveur SSH sur un commutateur via l'interface de ligne de commande

Introduction

Secure Shell (SSH) est un protocole qui fournit une connexion à distance sécurisée à des périphériques réseau spécifiques. Cette connexion fournit une fonctionnalité similaire à une connexion Telnet, sauf qu'elle est chiffrée. SSH permet à l'administrateur de configurer le commutateur via l'interface de ligne de commande (CLI) avec un programme tiers.

Le commutateur agit en tant que client SSH qui fournit des fonctionnalités SSH aux utilisateurs du réseau. Le commutateur utilise un serveur SSH pour fournir des services SSH. Lorsque l'authentification du serveur SSH est désactivée, le commutateur prend n'importe quel serveur SSH comme approuvé, ce qui diminue la sécurité sur votre réseau. Si le service SSH est activé sur le commutateur, la sécurité est améliorée.

Cet article explique comment configurer l'authentification du serveur sur un commutateur géré via l'interface de ligne de commande.

Périphériques pertinents

- Série Sx300
- Gamme Sx350
- Gamme SG350X
- Série Sx500
- Gamme Sx550X

Version du logiciel

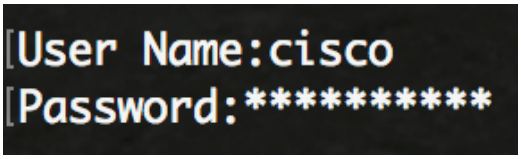
- 1.4.7.06 - Sx300, Sx500
- 2.2.8.04 - Sx350, SG350X, Sx550X

Configuration des paramètres du serveur SSH

Configuration des paramètres d'authentification du serveur SSH

Étape 1. Connectez-vous à la console du commutateur. Le nom d'utilisateur et le mot de passe par défaut sont cisco/cisco. Si vous avez configuré un nouveau nom d'utilisateur ou mot de passe, saisissez plutôt les informations d'identification.

Note: Pour savoir comment accéder à l'interface de ligne de commande d'un commutateur PME via SSH ou Telnet, cliquez ici.



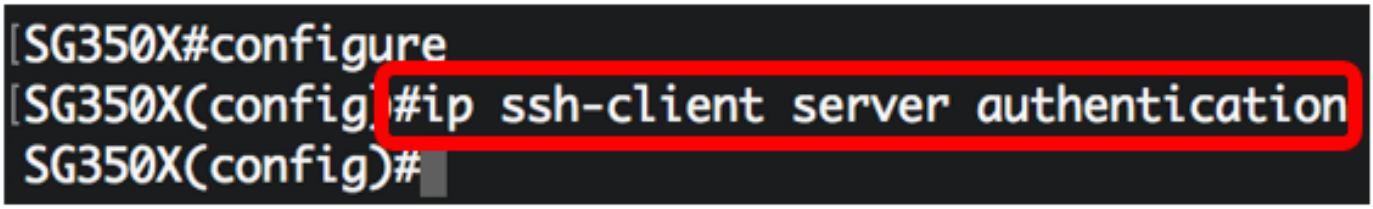
Note: Les commandes peuvent varier en fonction du modèle exact de votre commutateur. Dans cet exemple, le commutateur SG350X est accessible via Telnet.

Étape 2. À partir du mode d'exécution privilégié du commutateur, passez en mode de configuration globale en entrant ce qui suit :

```
SG350X#configure
```

Étape 3. Pour activer l'authentification du serveur SSH distant par le client SSH, saisissez ce qui suit :

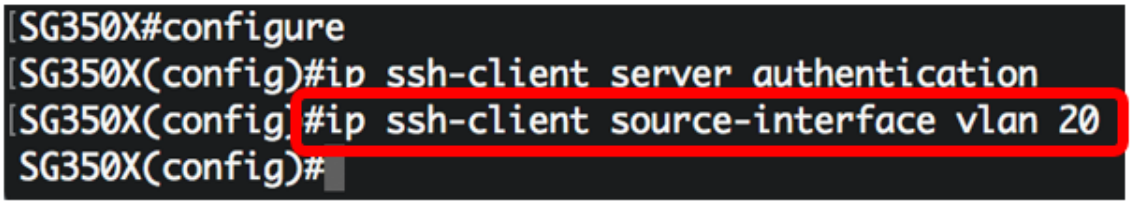
```
SG350X(config)#ip ssh-client server authentication
```



Étape 4. Pour spécifier l'interface source dont l'adresse IPv4 sera utilisée comme adresse IPv4 source pour la communication avec les serveurs SSH IPv4, saisissez ce qui suit :

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

- interface-id - Spécifie l'interface source.



Note: Dans cet exemple, l'interface source est VLAN 20.

Étape 5. (Facultatif) Pour spécifier l'interface source dont l'adresse IPv6 sera utilisée comme adresse IPv6 source pour la communication avec les serveurs SSH IPv6, saisissez ce qui suit :

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

- interface-id : spécifie l'interface source.

Note: Dans cet exemple, l'adresse IPv6 source n'est pas configurée.

Étape 6. Pour ajouter un serveur approuvé à la table Trusted Remote SSH Server, saisissez ce qui suit :

```
SG350X(config)#ip ssh-client, empreinte digitale du serveur [hôte | adresse IP] [empreinte]
```

Les paramètres sont les suivants :

- host : nom DNS (Domain Name Server) d'un serveur SSH.
- ip-address : spécifie l'adresse d'un serveur SSH. L'adresse IP peut être une adresse IPv4, IPv6 ou IPv6z.

- empreinte digitale : empreinte digitale de la clé publique du serveur SSH (32 caractères hexadécimaux).

```
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)#
```

Note: Dans cet exemple, l'adresse IP du serveur est 192.168.100.1 et l'empreinte utilisée est 76:0d:a0:12:7f:30:09:d3:18:04:df:77:c8:8e:51:a8.

Étape 7. Entrez la commande **exit** pour revenir au mode d'exécution privilégié :

`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#
```

Étape 8. Pour afficher les paramètres d'authentification du serveur SSH sur le commutateur, saisissez ce qui suit :

`SG350X#`**`show ip ssh-client server [hôte | adresse IP]`**

Les paramètres sont les suivants :

- host : nom DNS (Domain Name Server) d'un serveur SSH.
- ip-address : spécifie l'adresse d'un serveur SSH. L'adresse IP peut être une adresse IPv4, IPv6 ou 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#
```

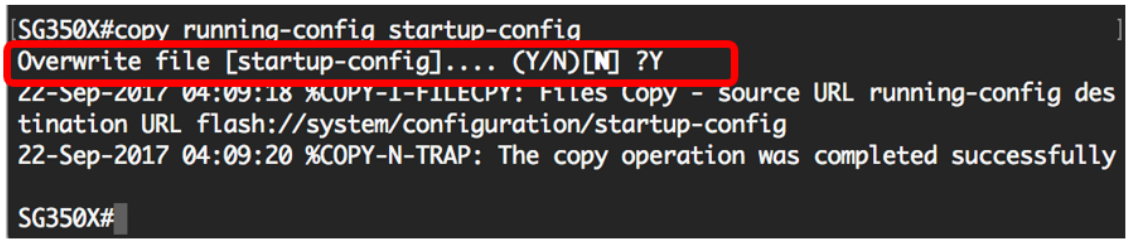
Note: Dans cet exemple, l'adresse IP du serveur 192.168.100.1 est entrée.

Étape 9. (Facultatif) Dans le mode d'exécution privilégié du commutateur, enregistrez les paramètres configurés dans le fichier de configuration initiale en saisissant ce qui suit :

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

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

Étape 10. (Facultatif) Appuyez sur **Y** pour Oui ou **N** pour Non sur votre clavier une fois le fichier Overwrite [startup-config].... apparaît.



Vous avez maintenant appris les étapes de configuration de l'authentification du serveur sur un commutateur géré via l'interface de ligne de commande.