Comment configurer SSH sur les commutateurs Catalyst qui exécutent CatOS

Contenu

Introduction

Ce document donne des instructions pas à pas pour configurer la version 1 de Secure shell (SSH) sur des commutateurs Catalyst exécutant OS de Catalyst (CatOS). La version testée est cat6000-supk9.6-1-1c.bin ou une version ultérieure.

Conditions préalables

Conditions requises

Ce tableau montre le statut de support de SSH dans les commutateurs. Les utilisateurs enregistrés peuvent accéder à ces images logicielles en visitant le centre logiciel.

CatOS SSH

Périphérique	Prise en charge de la fonctionnalité SSH
Cat 4000/4500/2948G/2980G (CatOS)	Images K9 en date de 6.1
Cat 5000/5500 (CatOS)	Images K9 en date de 6.1
Cat 6000/6500 (CatOS)	Images K9 en date de 6.1
SSH IOS	
Périphérique	**Prise en charge de la fonctionnalité SSH**
Cat 2950*	12.1(12c)EA1 et plus récent
Cat 3550*	12.1(11)EA1 et plus récent
Cat 4000/4500 (Logiciel Cisco IOS intégré) *	12.1(13)EW et plus récent **
Cat 6000/5500 (Logiciel Cisco IOS intégré) *	12.1(11b)E et plus récent
Cat 8540/8510	12.1(12c)EY et plus récent, 12.1(14)E1 et plus récent
Non SSH	
Périphérique	**Prise en charge de la fonctionnalité SSH**
Cat 1900	non
Cat 2800	non
Cat 2948G-L3	non
Cat 2900XL	non
Cat 3500XL	non
Cat 4840G-L3	non
Cat 4908G-L3	non

* La configuration est couverte en configurant le Secure Shell sur les routeurs et commutateurs exécutant le Cisco IOS.

** Il n'y a aucune prise en charge de SSH dans le train 12.1E pour le Logiciel Cisco IOS intégré par exécution de Catalyst 4000.

Consultez le formulaire d'autorisation d'exportation de logiciel de cryptage afin de solliciter le 3DES.

Ce document suppose que l'authentification fonctionne avant l'implémentation de SSH (par le mot de passe telnet, TACACS+) ou de RADIUS. Le SSH avec le Kerberos n'est pas pris en charge avant l'implémentation de SSH.

Components Used

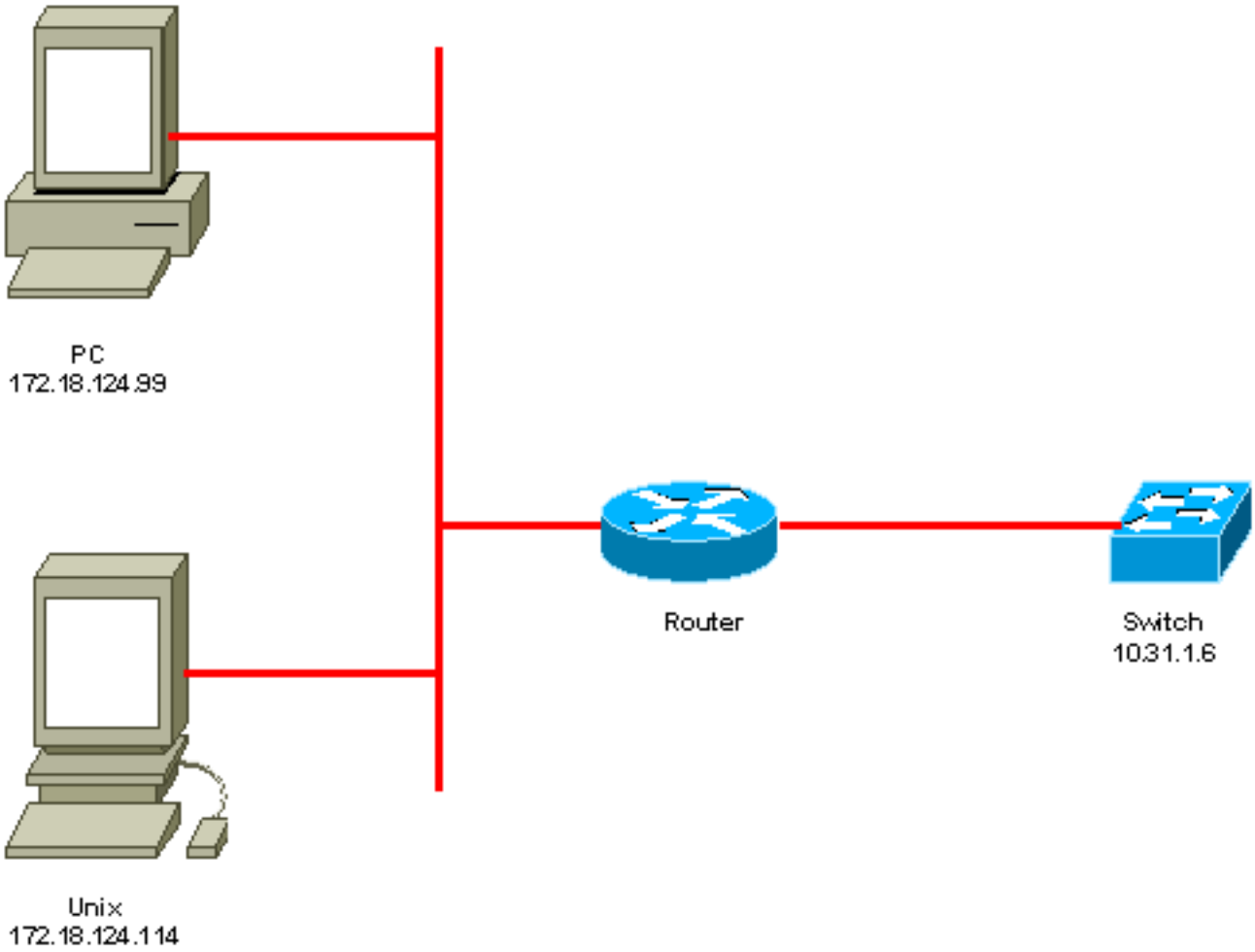
Ce document expose seulement les séries de Catalyst 2948G, Catalyst 2980G, Catalyst 4000/4500, Catalyst 5000/5500, et Catalyst 6000/6500 exécutant l'image de CatOS K9. Référez-vous à la section UDLD de ce document pour de plus amples détails.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Diagramme du réseau



Configuration du commutateur

```
!--- Generate and verify RSA key. sec-cat6000> (enable) set crypto key rsa 1024
Generating RSA keys..... [OK]
sec-cat6000> (enable) ssh_key_process: host/server key size: 1024/768
 !--- Display the RSA key. sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
57733285367170478570985060663476874686971696394035244062067857533870155088852 5
69969147833053784006695698761020781095949864817996533001801084478586347277306 7
```

```
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
!--- Restrict which host/subnets are allowed to use SSH to the switch. !--- Note: If you do not
do this, the switch will display the message !--- "WARNING!! IP permit list has no entries!"
sec-cat6000> set ip permit 172.18.124.0 255.255.255.0
172.18.124.0 with mask 255.255.255.0 added to IP permit list.
!--- Turn on SSH. sec-cat6000> (enable) set ip permit enable ssh
SSH permit list enabled.
!--- Verity SSH permit list. sec-cat6000> (enable) show ip permit
Telnet permit list disabled.
Ssh permit list enabled.
Snmp permit list disabled.
Permit List Mask Access-Type
---------------- ---------------- -------------
172.18.124.0 255.255.255.0 telnet ssh snmp

Denied IP Address Last Accessed Time Type
----------------- ------------------ ------
```

Désactiver le SSH

Dans certaines situations, il peut être nécessaire de désactiver le SSH sur le commutateur. Vous devez vérifier si le SSH est configuré sur le commutateur et si oui, le désactiver.

Pour vérifier si le SSH a été configuré sur le commutateur, émettez la commande de **show crypto key.** Si le résultat affiche la clé RSA, alors le SSH a été configuré et activé sur le commutateur. Un exemple est montré ici.

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
```

Pour supprimer la clé crypto, émettez la commande de **clear crypto key rsa afin de désactiver le SSH sur le commutateur.** Un exemple est montré ici.

```
sec-cat6000> (enable) clear crypto key rsa
Do you really want to clear RSA keys (y/n) [n]? y
RSA keys has been cleared.
sec-cat6000> (enable)
```

débogage dans Catalyst

Pour activer des débogages, émettez la commande du **ssh 4 de set trace.**

Pour activer des débogages, émettez la commande du **ssh 0 de set trace.**

exemples de commande de débogage d'une bonne connexion

Solaris au Catalyst, Triple Data Encryption Standard (3DES), mot de passe telnet

Solaris

```
rtp-evergreen# ssh -c 3des -v 10.31.1.6
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host '10.31.1.6' added to the list of known hosts.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
root@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyseur

```
sec-cat6000> (enable) debug: _proc->tty = 0x8298a494, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: root
debug: Trying Local Login
Password authentication for root accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

PC au Catalyst, 3DES, mot de passe telnet

Catalyseur

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: des
```

```
debug: Received session key; encryption turned on.
debug: ssh login by user:
debug: Trying Local Login
Password authentication for accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 37
Unknown packet type received after authentication: 37
debug: ssh received packet type: 12
debug: ssh89: starting exec shell
debug: Entering interactive session.
```

Solaris au Catalyst, 3DES, authentification d'AAA (authentification, autorisation et traçabilité) (AAA)

Solaris

```
Solaris with aaa on:
rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
rtp-evergreen: Host '10.31.1.6' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
abcde123@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyseur

```
sec-cat6000> (enable) debug: _proc->tty = 0x82a07714, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: abcde123
debug: Trying TACACS+ Login
Password authentication for abcde123 accepted.
```

```
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

exemples de commande de débogage de ce qui peut aller mal

Débogage de Catalyst avec le client essayant Blowfish Cipher [non pris en charge]

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: blowfish
cipher_set_key: unknown cipher: 6
debug: Calling cleanup
```

Débogage de Catalyst avec le mauvais mot de passe telnet

```
debug: _proc->tty = 0x82897414, socket_index = 4
debug: version: SSH-1.5-1.2.26
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user:
debug: Trying Local Login
debug: Password authentication for failed.
```

Débogage de Catalyst avec la mauvaise authentification AAA

```
cat6000> (enable) debug: _proc->tty = 0x829abd94, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: junkuser
debug: Trying TACACS+ Login
debug: Password authentication for junkuser failed.
SSH connection closed by remote host.
debug: Calling cleanup
```

Dépannage

Cette section Routage traite différents scénarios de dépannage liés à la configuration de SSH sur des commutateurs Cisco.

Connexion impossible pour commuter par le SSH

Problème :

Ne peut pas se connecter au commutateur utilisant le SSH.

Les commandes d'**ip ssh de débogage donnent ce résultat :**

```
Jun 15 20:29:26.207: SSH2 1: RSA_sign: private key not found
Jun 15 20:29:26.207: SSH2 1: signature creation failed, status -1
```

Solution :

Ce problème de se produit en raison d'une des raisons suivantes :

- Les nouvelles connexions SSH échouent après avoir modifié le nom de hôte.
- SSH configuré avec des codes non marqués (ayant le FQDN du routeur).

Les solutions de contournement pour ce problème sont :

- Si le nom de hôte a été modifié, et le SSH ne fonctionne plus, alors mettez à zéro le nouveau code créez-en un autre avec l'étiquette appropriée.
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- N'utilisez pas des clés RSA anonymes (nommées après le FQDN du commutateur). Utilisez les codes étiquetés à la place.
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

Afin de résoudre ce problème pour toujours, mettez à niveau le logiciel IOS aux versions et plus récentes l'unes des dans lesquelles ce problème est réparé.

Un bogue a été classé au sujet de ceci. Pour plus d'informations, référez-vous au bogue Cisco portant l'ID **CSCsm68097 (clients enregistrés uniquement).**

Informations connexes

- Page d'assistance SSH
- Configuration de Secure Shell sur les routeurs et les commutateurs exécutant Cisco IOS
- Toolkit de débogage
- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.