Configurer SSH sur les routeurs et les commutateurs

Table des matières

Introduction

Le présent document décrit comment configurer et déboguer le protocole Secure Shell (SSH) sur les routeurs ou les commutateurs Cisco qui exécutent le logiciel Cisco IOS®.

Conditions préalables

Exigences

L'image Cisco IOS utilisée doit être une image k9 (crypto) afin de prendre en charge SSH. Par exemple, c3750e-universalk9-tar.122-35.SE5.tar est une image k9 (chiffrée).

Composants utilisés

Les informations contenues dans ce document sont basées sur le logiciel Cisco IOS 3600 (C3640-IK9S-M), Version 12.2(2)T1.

SSH a été introduit dans les plates-formes et images Cisco IOS suivantes :

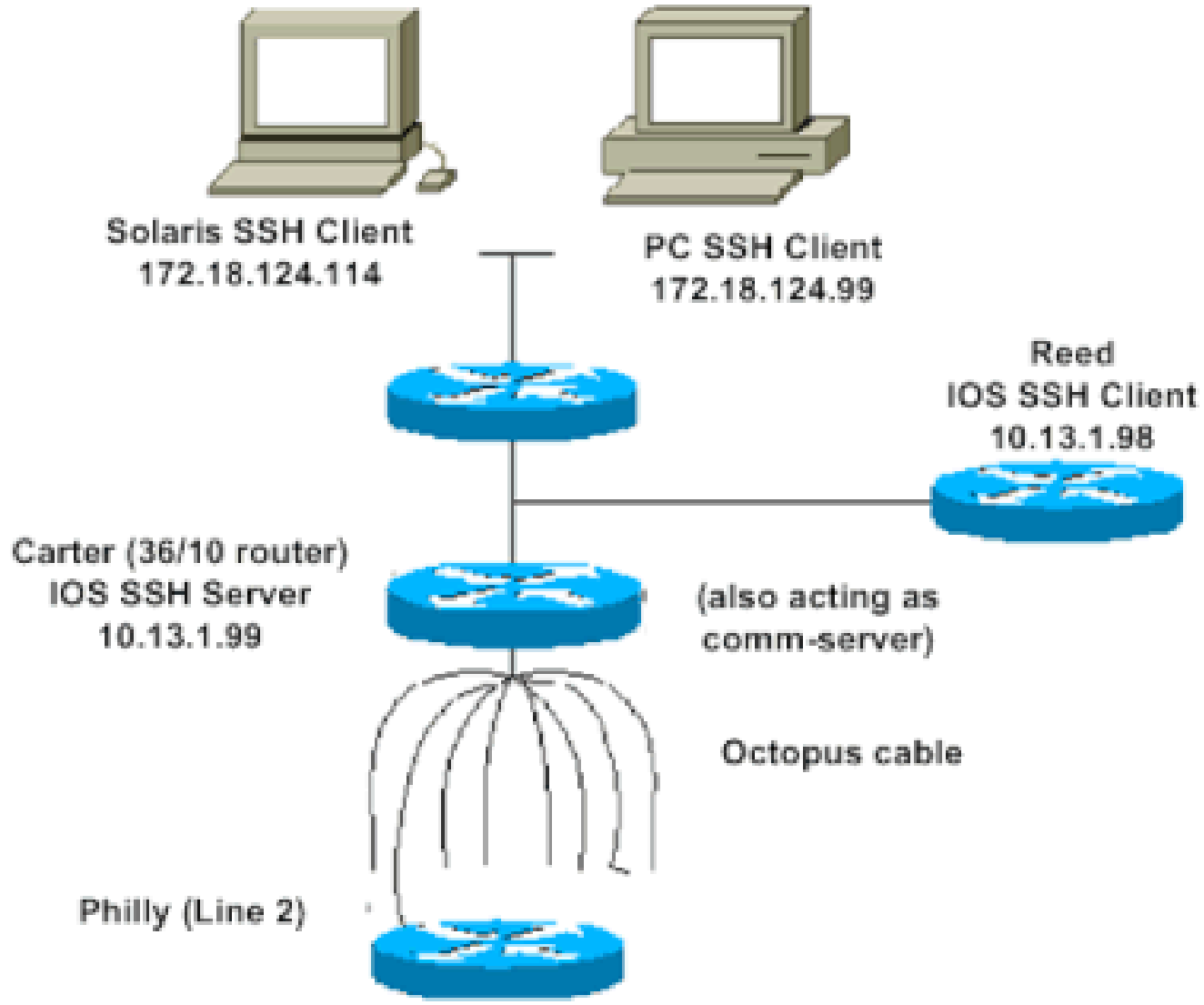
- L’accès à la ligne de terminal SSH (ou « reverse-Telnet ») a été introduit dans les plateformes Cisco IOS et les images à partir de Cisco IOS 12.2.2.T.
- La prise en charge de la version 2.0 du SSH (SSH v2) a été introduite dans les plateformes Cisco IOS et les images à partir de Cisco IOS 12.1(19)E.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Consultez les conventions des conseils techniques de Cisco pour en savoir plus.

Diagramme de réseau SSH v2



Test d'authentification

Test d'authentification sans SSH

Testez d'abord l'authentification sans SSH pour vous assurer que l'authentification fonctionne avec le routeur Carter avant d'ajouter SSH. L'authentification peut se faire à l'aide d'un nom d'utilisateur et d'un mot de passe locaux ou d'un serveur d'authentification, d'autorisation et de gestion de comptes (AAA) qui exécute TACACS+ ou RADIUS. (L'authentification par mot de passe de ligne est impossible avec SSH.) Cet exemple montre l'authentification locale, qui vous permet de créer une connexion Telnet dans le routeur avec le nom d'utilisateur Cisco et le mot de passe Cisco.

Remarque : Dans ce document, vty est utilisé pour indiquer le type de terminal virtuel.

```
!--- The aaa new-model command causes the local username and password on the router to be used in the al

aaa new-model
username cisco password 0 cisco
```

```
line vty 0 4
transport input telnet

!--- Instead of aaa new-model, you can use the login local command.
```

Test d'authentification avec SSH

Pour tester l’authentification avec SSH, vous devez ajouter les instructions précédentes, ce qui activera SSH sur Carter, et tester SSH à partir du PC et des stations UNIX.

```
ip domain-name rtp.cisco.com

!--- Generate an SSH key to be used with SSH.

crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
```

À ce stade, la commande show crypto key mypubkey rsa doit afficher la clé générée. Après avoir ajouté la configuration SSH, testez votre capacité à accéder au routeur à partir du PC et de la station UNIX.

Ensembles de configuration facultatifs

Empêcher les connexions non SSH

Si vous voulez empêcher les connexions non SSH, ajoutez la commande transport input ssh sous les lignes pour limiter le routeur aux connexions SSH seulement. Les Telnets directs (non SSH) sont refusés.

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

Effectuez un test pour vous assurer que les utilisateurs non SSH ne peuvent pas connecter par Telnet au routeur Carter.

Configurer un routeur ou un commutateur IOS comme client SSH

Il y a quatre étapes nécessaires pour activer la prise en charge de SSH sur un routeur Cisco IOS :

1. Configurez la commande hostname.

2. Configurez le domaine DNS.

3. Générez la clé SSH.

4. Activez la prise en charge du transport SSH pour le vty.

Si vous voulez avoir un périphérique qui joue le rôle de client SSH pour l'autre, vous pouvez ajouter SSH à un deuxième périphérique appelé Reed. Cela met ces appareils dans un mode « client-serveur », où Carter agit en tant que serveur et Reed en tant que client. La configuration du client Cisco IOS SSH sur Reed est la même que celle requise pour la configuration du serveur SSH sur Carter.

```
!--- Step 1: Configure the hostname if you have not previously done so.

hostname carter

!--- The aaa new-model command causes the local username and password on the router to be used in the al

aaa new-model
username cisco password 0 cisco

!--- Step 2: Configure the DNS domain of the router.

ip domain-name rtp.cisco.com

!--- Step 3: Generate an SSH key to be used with SSH.

crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2

!--- Step 4: By default the vty transport is Telnet. In this case, Telnet is disabled and only SSH is su

line vty 0 4
transport input ssh

!--- Instead of aaa new-model, you can use the login local command.
```

Saisissez cette commande au SSH, du client SSH Cisco IOS (Reed) au serveur SSH Cisco IOS (Carter), pour tester ce qui suit :

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99
```

Configurez un routeur IOS en tant que serveur SSH qui effectue l’authentification de l’utilisateur en fonction du RSA.

Suivez ces étapes pour configurer le serveur SSH afin d'effectuer l'authentification en fonction du RSA.

1. Précisez le nom d'hôte.

```
Router(config)#hostname <host name>
```

2. Définissez le nom de domaine par défaut.

```
Router(config)#ip domain-name <Domain Name>
```

3. Générez des paires de clés RSA.

```
Router(config)#crypto key generate rsa
```

4. Configurez les clés SSH-RSA pour l'authentification de l'utilisateur et du serveur.

```
Router(config)#ip ssh pubkey-chain
```

5. Configurez le nom d'utilisateur SSH.

```
Router(conf-ssh-pubkey)#username <user name>
```

6. Précisez la clé publique RSA de l'homologue distant.

```
Router(conf-ssh-pubkey-user)#key-string
```

7. Précisez le type et la version de clé SSH. (Cette étape est facultative.)

```
Router(conf-ssh-pubkey-data)#key-hash ssh-rsa <key ID>
```

8. Quittez le mode actuel pour retourner au mode d’exécution privilégié (privileged EXEC).

```
Router(conf-ssh-pubkey-data)#end
```

Ajouter un accès à la ligne de terminal SSH

Si vous avez besoin d'une authentification de ligne de terminal SSH sortante, vous pouvez configurer et tester SSH pour les Telnets inverses sortants via Carter, qui joue le rôle de serveur de communication vers Philly.

```
ip ssh port 2001 rotary 1
line 1 16
   no exec
   rotary 1
   transport input ssh
   exec-timeout 0 0
   modem InOut
   stopbits 1
```

Si Philly est relié au port 2 de Carter, vous pouvez configurer SSH à Philly par l’intermédiaire de Carter, et ce, à partir de Reed en utilisant la commande suivante :

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -p 2002 10.31.1.99
```

Vous pouvez utiliser la commande suivante de Solaris :

```
ssh -c 3des -p 2002 -x -v 10.13.1.99
```

Restreindre l'accès SSH à un sous-réseau

Vous devez limiter la connectivité SSH à un sous-réseau précis, où toutes les autres tentatives du protocole SSH des adresses IP externes au sous-réseau sont abandonnées.

Vous pouvez faire de même en suivant ces étapes :

1. Définissez une liste d'accès qui autorise le trafic à partir de ce sous-réseau spécifique.
2. Limitez l'accès à l'interface de ligne VTY avec une commande `access-class`.

Voici un exemple de configuration. Dans cet exemple, seul l’accès SSH au sous-

réseau 10.10.10.0 255.255.255.0 est autorisé; tous les autres se verront refuser l’accès.

```
Router(config)#access-list 23 permit 10.10.10.0 0.0.0.255
Router(config)#line vty 5 15
Router(config-line)#transport input ssh
Router(config-line)#access-class 23 in
Router(config-line)#exit
```

Remarque : La même procédure servant à verrouiller l’accès SSH est également utilisée pour les plateformes de commutateurs.

Configurez le SSH, version 2

```
carter(config)#ip ssh version 2
```

Variations sur la sortie de la commande banner

La sortie de la commande banner varie entre la connexion Telnet et les différentes versions de connexions SSH. Le tableau suivant montre comment les différentes options de la commande banner fonctionnent avec différents types de connexions.

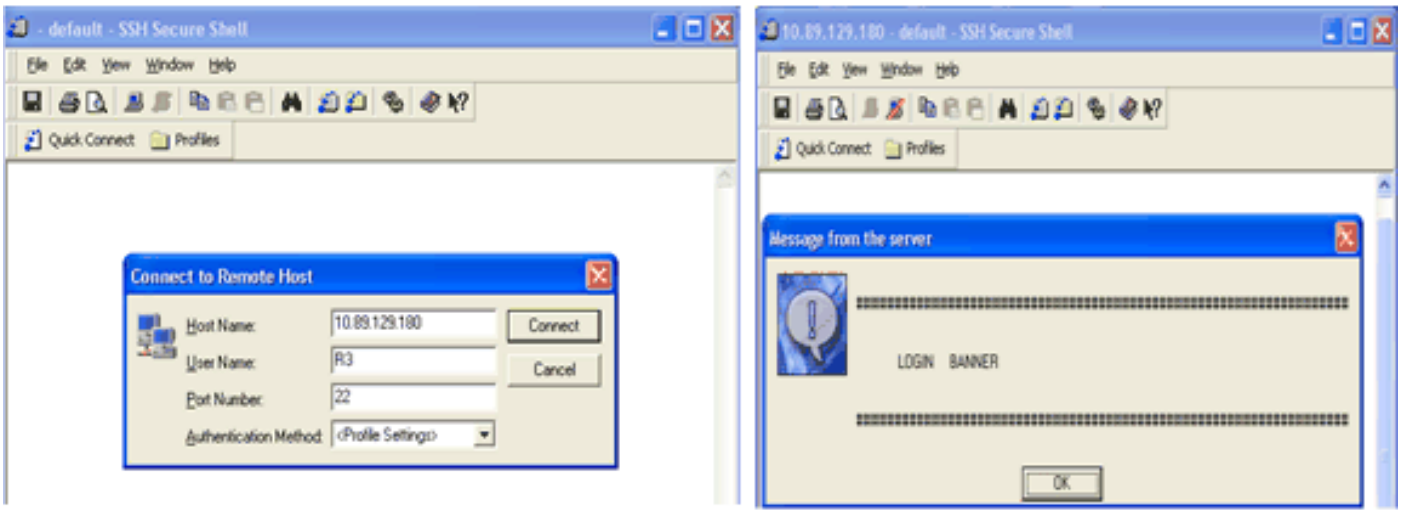
Options de commande de la bannière	Telnet	SSH v2
Journal des bannières	S’affiche avant la connexion à l’appareil.	S’affiche avant la connexion à l’appareil.
banner motd	S’affiche avant la connexion à l’appareil.	S’affiche après la connexion à l’appareil.
banner exec	S’affiche après la connexion à l’appareil.	S’affiche après la connexion à l’appareil.

Remarque : La version 1 du protocole SSH n’est plus recommandée.

Impossible d'afficher la bannière de connexion

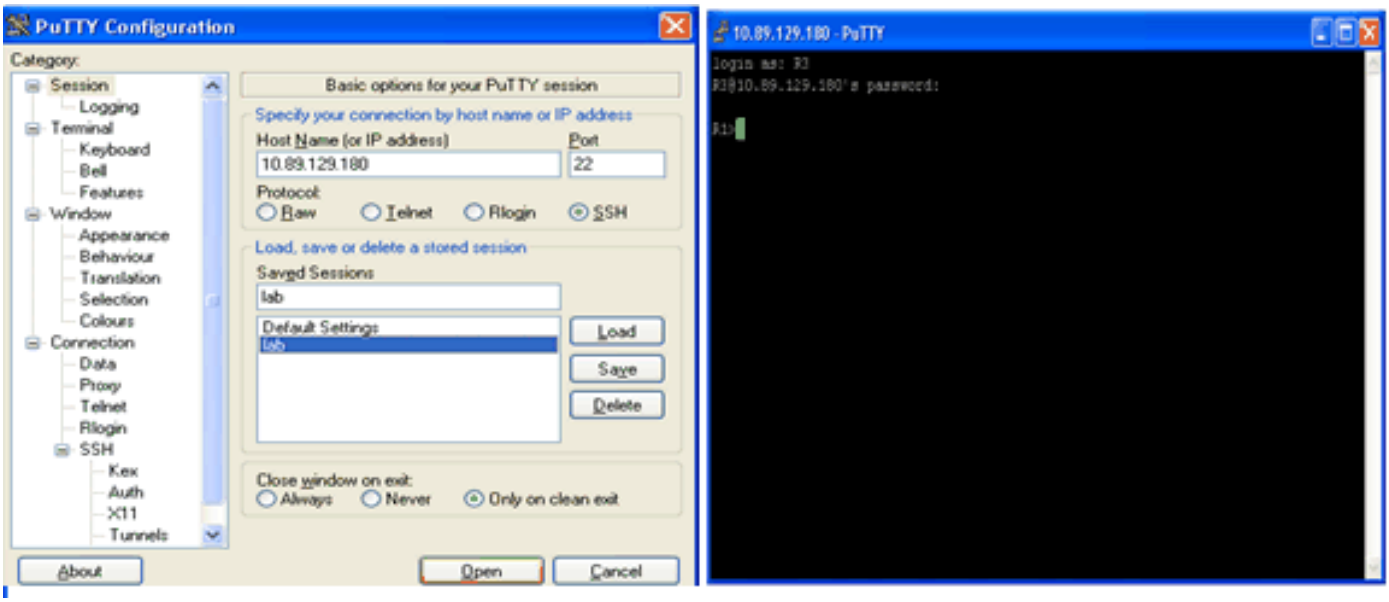
La version 2 du protocole SSH prend en charge la bannière de connexion. Lorsqu'elle lance la session SSH avec le routeur Cisco, la bannière de connexion s'affiche si le client SSH envoie le nom d'utilisateur. Par exemple, lorsque le client ssh Secure Shell est utilisé, la bannière de connexion s'affiche. Lorsque le client ssh PuTTY est utilisé, la bannière de connexion ne s'affiche pas. En effet, SSH envoie le nom d'utilisateur par défaut, tandis que PuTTY n'envoie pas le nom d'utilisateur par défaut.

Le client SSH a besoin du nom d'utilisateur pour lancer la connexion au périphérique compatible avec le protocole SSH. Le bouton Connect n'est pas activé si vous n'entrez pas le nom d'hôte et le nom d'utilisateur. L'image à l'écran montre que la bannière de connexion s'affiche lorsque SSH se connecte au routeur. La bannière invite ensuite l'utilisateur à saisir un mot de passe.



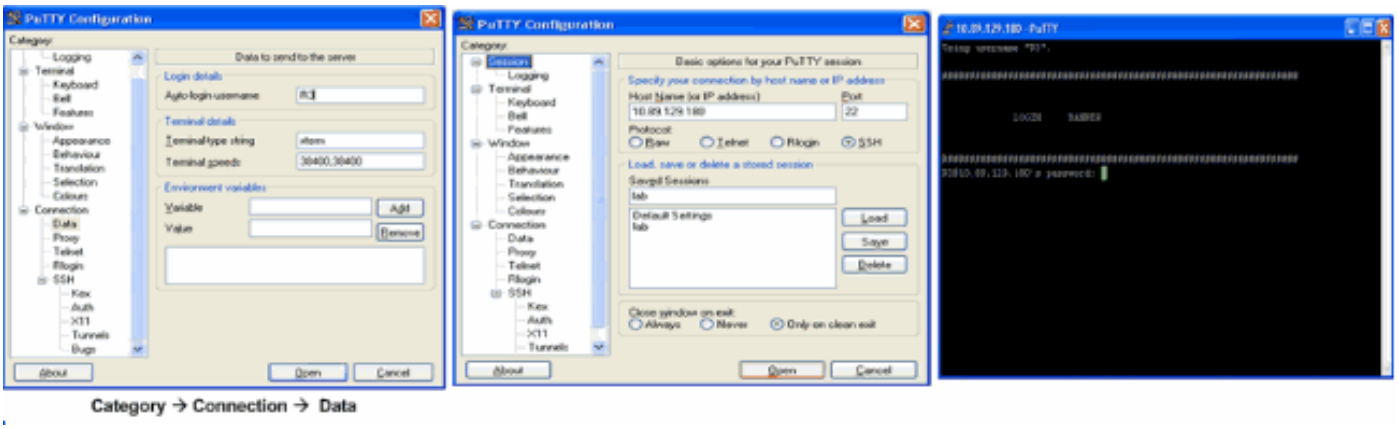
Message de la bannière invitant l'utilisateur à saisir un mot de passe

Le client PuTTY ne nécessite pas le nom d'utilisateur pour lancer la connexion SSH au routeur. L'image à l'écran montre que le client PuTTY se connecte au routeur, puis demande le nom d'utilisateur et le mot de passe. La bannière de connexion ne s'affiche pas.



Connexion SSH au routeur

Cette capture d’écran montre que la bannière de connexion s’affiche lorsque PuTTY est configuré pour envoyer le nom d’utilisateur au routeur.



Envoyez le nom d’utilisateur au routeur

Commandes debug et show

Avant d’exécuter les commandes debug décrites ici, consultez les renseignements importants sur les commandes de débogages. Certaines commandes show sont prises en charge par l’outil Output Interpreter Tool (enregistré pour les clients seulement), qui vous permet d’afficher une analyse de la sortie de la commande show.

- debug ip ssh Affiche les messages de débogage pour SSH.
- show ssh Affiche l’état des connexions au serveur SSH.

```
carter#show ssh
  Connection     Version Encryption    State               Username
   0             2.0     DES           Session started     cisco
```

- show ip ssh Affiche les données de version et de configuration pour SSH.

```
carter#show ip ssh
  SSH Enabled - version 2.0
  Authentication timeout: 120 secs; Authentication retries: 3
```

Exemple de sortie de débogage

Débogage du routeur

```
00:23:20: SSH0: starting SSH control process
```

```
00:23:20: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-2.0-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH0: sending encryption confirmation
00:23:21: SSH0: keys exchanged and encryption on
00:23:21: SSH0: SSH_CMSG_USER message received
00:23:21: SSH0: authentication request for userid cisco
00:23:21: SSH0: SSH_SMSG_FAILURE message sent
00:23:23: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:23:23: SSH0: authentication successful for cisco
00:23:23: SSH0: requesting TTY
00:23:23: SSH0: setting TTY - requested: length 24, width 80; set:
   length 24, width 80
00:23:23: SSH0: invalid request - 0x22
00:23:23: SSH0: SSH_CMSG_EXEC_SHELL message received
00:23:23: SSH0: starting shell for vty
```

Débogage du serveur

Remarque : Il s'agit de la sortie d'une machine Solaris.

```
rtp-evergreen.rtp.cisco.com#ssh -c 3des -l cisco -v 10.31.1.99
rtp-evergreen#/opt/CISssh/bin/ssh -c 3des -l cisco -v 10.13.1.99
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 10.13.1.99 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 2.0,
   remote software version Cisco-1.25
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits)
   and host key (512 bits).
rtp-evergreen: Host '10.13.1.99' 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.
cisco@10.13.1.99'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.
```

Configurations incorrectes

Les sections suivantes présentent un exemple de sortie de débogage provenant de plusieurs configurations incorrectes.

SSH à partir d'un client SSH non compilé avec Data Encryption Standard (DES)

Mot de passe incorrect

Débogage du routeur

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-2.0-1.2.26
00:26:52: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

Envoi, par un client SSH, d'un chiffrement (Blowfish) non pris en charge

Débogage du routeur

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-2.0-W1.0
00:39:26: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

Obtenez l’erreur « %SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for » (%SSH-3-PRIVATEKEY : Impossible de récupérer la clé privée du RSA pour.

Une modification du nom de domaine ou du nom d’hôte peut déclencher ce message d’erreur. Utilisez les solutions de contournement suivantes :

- Mettez à zéro les clés RSA et générez de nouveau les clés.

```
crypto key zeroize rsa label key_name
crypto key generate rsa label key_name modulus key_size
```

- Si la solution de contournement précédente ne fonctionne pas, essayez ces étapes :

    1. Mettez à zéro toutes les clés RSA.
    2. Rechargez l’appareil.
    3. Créez de nouvelles clés étiquetées pour SSH.

Conseils

- Si vos commandes de configuration SSH sont rejetées comme étant des commandes illégales, vous n'avez pas correctement généré une paire de clés RSA pour votre routeur. Assurez-vous d’avoir indiqué un nom d’hôte et un domaine. Utilisez ensuite la commande crypto key generate rsa pour générer des paires de clés RSA et pour activer le serveur SSH.
- Lorsque vous configurez des paires de clés RSA, les messages d’erreur suivants peuvent s’afficher :

    1. `Aucun nom d’hôte indiqué.`

        Vous devez utiliser la commande de configuration globale hostname pour configurer un nom d’hôte pour le routeur.

    2. `Aucun domaine indiqué.`

        Vous devez utiliser la commande de configuration globale ip domain-name pour configurer un domaine d’hôte pour le routeur.

- Le nombre de connexions SSH autorisées est limité au nombre maximal de connexions vty configurées pour le routeur. Chaque connexion SSH utilise une vty ressource.

    •

    SSH utilise la sécurité locale ou le protocole de sécurité configuré par AAA sur votre routeur pour l’authentification de l’utilisateur. Lorsque vous configurez AAA, vous devez vous assurer que la console n’est pas exécutée sous AAA. Appliquez un mot-clé dans le mode de configuration globale pour désactiver AAA sur la console.

-

No SSH server connections running:

```
carter#show ssh %No SSHv2 server connections running.
```

Cette sortie suggère que le serveur SSH est désactivé ou pas correctement activé. Si vous avez déjà configuré SSH, il est recommandé de reconfigurer le serveur SSH sur le périphérique. Suivez ces étapes pour reconfigurer le serveur SSH sur l'appareil.

- Supprimez les paires de clés RSA. Après la suppression des paires de clés RSA, le serveur SSH est automatiquement désactivé.

```
carter(config)#crypto key zeroize rsa
```

Remarque : Il est important de générer des paires de clés avec une taille en bits d'au moins 768 lorsque vous activez la version 2 du protocole SSH.

Attention : Cette commande ne peut pas être annulée après avoir enregistré votre configuration. En outre, une fois les clés RSA supprimées, vous ne pouvez pas utiliser les certificats ou le CA ni participer à des échanges de certificats avec d'autres homologues IPSec, à moins de régénérer les clés RSA pour reconfigurer l'interopérabilité du CA, obtenir le certificat du CA et demander de nouveau votre certificat.

2. Reconfigurez le nom d'hôte et le nom de domaine de l'appareil.

```
carter(config)#hostname hostname

carter(config)#ip domain-name domainname
```

3. Générez des paires de clés RSA pour votre routeur. Cela active automatiquement le protocole SSH.

```
carter(config)#crypto key generate rsa
```

Remarque : Consultez le document crypto key generate rsa – Cisco IOS Security Command Reference, Release 12.3 (La clé de chiffrement génère le RSA – Référence de la commande de sécurité Cisco IOS) pour en savoir plus sur l'utilisation de cette commande

Remarque : Vous pouvez recevoir le message d'erreur `SSH2 0 : Unexpected mesg type received` (SSH2 0 : Type de message inattendu reçu) en raison d'un paquet que reçoit le routeur, mais qu'il ne comprend pas. Augmentez la longueur de clé tandis que vous générez des clés RSA pour SSH afin de résoudre ce problème.

4. Configurez le serveur SSH.

5. Afin d'activer et de configurer un routeur ou un commutateur Cisco pour le serveur SSH, vous devez configurer les paramètres SSH. Si vous ne configurez pas de paramètres SSH, les valeurs par défaut sont utilisées.

ip ssh {[timeout seconds] | [authentication-retries integer]}

```
carter(config)# ip ssh
```

Informations connexes

- **Pages d'assistance sur les produits SSH**

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.