Secure Shell (SSH) - FAQ

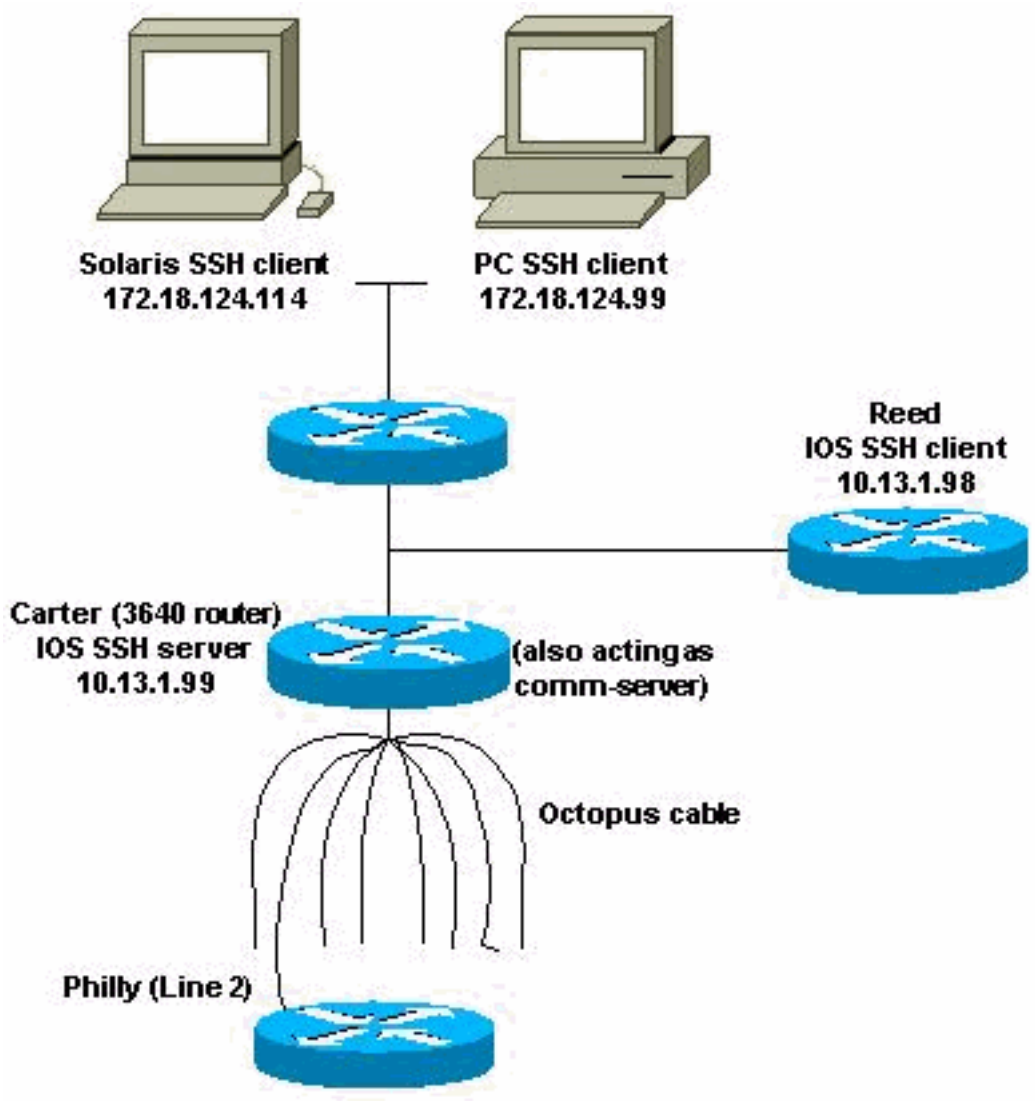
Contenu

Introduction

Ce document répond aux questions les plus fréquentes (Forum aux questions) liées à Secure Shell (SSH). Le code de SSH de Cisco IOS® est code d'original de Cisco.

Comment est-ce que je configure l'accès à la ligne de terminal de SSH (également connu sous le nom d'inverse-TELNET) ?

Ceci a été introduit la première fois dans des quelques Plateformes de la version du logiciel Cisco IOS 12.2.2.T.




```
Router(config)#line line-number [ending-line-number]
Router(config-line)#no exec
Router(config-line)#login {local | authentication listname
Router(config-line)#rotary group
Router(config-line)#transport input {all | ssh}
Router(config-line)#exit
Router(config)#ip ssh port portnum rotary group

!--- Line 1 SSH Port Number 2001 line 1 no exec login authentication default rotary 1 transport
input ssh !--- Line 2 SSH Port Number 2002 line 2 no exec login authentication default rotary 2
transport input ssh !--- Line 3 SSH Port Number 2003 line 3 no exec login authentication default
rotary 3 transport input ssh ip ssh port 2001 rotary 1 3
```

Référence des commandes

ip ssh port
ip ssh port *portnum* **rotary** *group*
no ip ssh port *portnum* **rotary** *group*

- portnum - Spécifie le port auquel le SSH doit se connecter, comme 2001.
- groupe tournant - Spécifie le ce rotary défini doit rechercher un nom valide.

Le SSH est-il pris en charge sur le Catalyst 2900 ?

Non, il n'est pas.

Comment est-ce que je peux déterminer quelles Plateformes et versions de code prennent en charge le SSH ?

Voyez le navigateur de caractéristique (clients enregistrés seulement) et spécifiez la caractéristique de **SSH**.

Quand j'essaye de retirer certain SSH commande de mon routeur, il continue à me demander de créer des clés RSA afin d'activer le SSH. Pourquoi cela ?

Un exemple de ce problème est affiché ici :

```
804#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
804(config)#no ip ssh time-out 120
Please create RSA keys to enable SSH.
804(config)#no ip ssh authen
Please create RSA keys to enable SSH.
804(config)
```

Vous avez rencontré l'ID de bogue Cisco CSCdv70159 (clients enregistrés seulement).

La version SSH 2 de Cisco IOS prend en charge-elle le Norme de signature numérique (DSS) ?

La version SSH 2 de Cisco IOS ne prend en charge pas le DSS.

Le serveur de SSH de Cisco IOS prend en charge-il l'expédition d'agent ?

Le SSH de Cisco IOS ne prend en charge pas l'expédition d'agent. Il interopère avec toutes les réalisations commerciales de SSH.

Quels mécanismes d'authentification client sont pris en charge sur le serveur de SSH de Cisco IOS ?

La version SSH 2 (SSHv2) de Cisco IOS prend en charge des méthodes d'authentification clavier-interactives et basées sur mot de passe. En plus de ces méthodes d'authentification, les améliorations SSHv2 pour la caractéristique de clés RSA (disponible dans le Logiciel Cisco IOS version 15.0(1)M et plus tard) prend en charge l'authentification basée sur RSA de clé publique pour le client et le serveur. Pour des informations supplémentaires sur les mécanismes d'authentification pris en charge par le serveur de SSH de Cisco IOS, référez-vous au support sécurisé de version 2 de shell.

Ce qui fait les **gens du pays d'**erreur **: Octets corrompus de contrôle sur le** moyen d'**entrée** ?

Les checkbytes corrompus signifie que le paquet de SSH reçu a manqué son contrôle d'intégrité. C'est habituellement en raison de déchiffrement incorrect. C'est également en raison d'une clé incorrecte utilisée. La clé incorrecte est provoqué par par la baisse d'un paquet chiffré de SSH. Vous avez l'un ou l'autre lâché un paquet chiffré qui devrait avoir été envoyé ou avez relâché un paquet chiffré reçu qui devrait avoir été déchiffré.

Le SSH de support de Cisco IOS avec le Blowfish chiffre-t-il ?

Le Cisco IOS ne prend en charge pas le SSH avec le chiffrement de Blowfish. Quand un client SSH envoie un tel chiffrement sans support, les messages de débogage d'affichages de routeur mentionnés dans le client SSH envoie le chiffrement sans support (de Blowfish).

Quand j'essaye de générer des clés RSA pour l'accès de SSH sur un routeur utilisant la commande de crypto key generate rsa dans le mode de config, je reçois cette erreur : `% d'entrée non valide détectée au repère de « ^ »`. Il ne permet pas le routeur de générer les clés RSA pour activer l'accès de SSH pour le routeur. Comment cette erreur est-elle résolue ?

Cette erreur apparaît quand l'image utilisée sur le routeur ne prend en charge pas la commande de **crypto key generate rsa**. Cette commande est prise en charge seulement dans des images de Sécurité. Afin de résoudre cette erreur utilisez l'image de Sécurité de la gamme appropriée du routeur Cisco IOS utilisé.

Les images chiffrées prennent en charge-elles le chiffrement fort pour utiliser le SSH avec des chiffrements tels que 3DES ou AES ?

Oui. Seulement chiffrement fort de support d'images chiffrées. Afin d'utiliser le SSH avec des chiffrements tels que 3DES ou AES vous devez avoir des images chiffrées sur votre périphérique de Cisco.

Ces messages sont vus dans les logs quand j'essaye de configurer le SSH sur un routeur : `SSH2 13 : RSA_sign : clé privée non trouvée` et `SSH2 13 : la création de signature a manqué, l'état -1`. Comment résoudre ce problème ?

Ces messages de log sont dus vu aux id de bogue Cisco CSCsa83601 (clients enregistrés seulement) et CSCtc41114 (clients enregistrés seulement). Référez-vous à ces pour en savoir plus de bogues.

Informations connexes

- Page d'assistance SSH
- Support et documentation techniques - Cisco Systems