Secure Shell (SSH) - FAQ

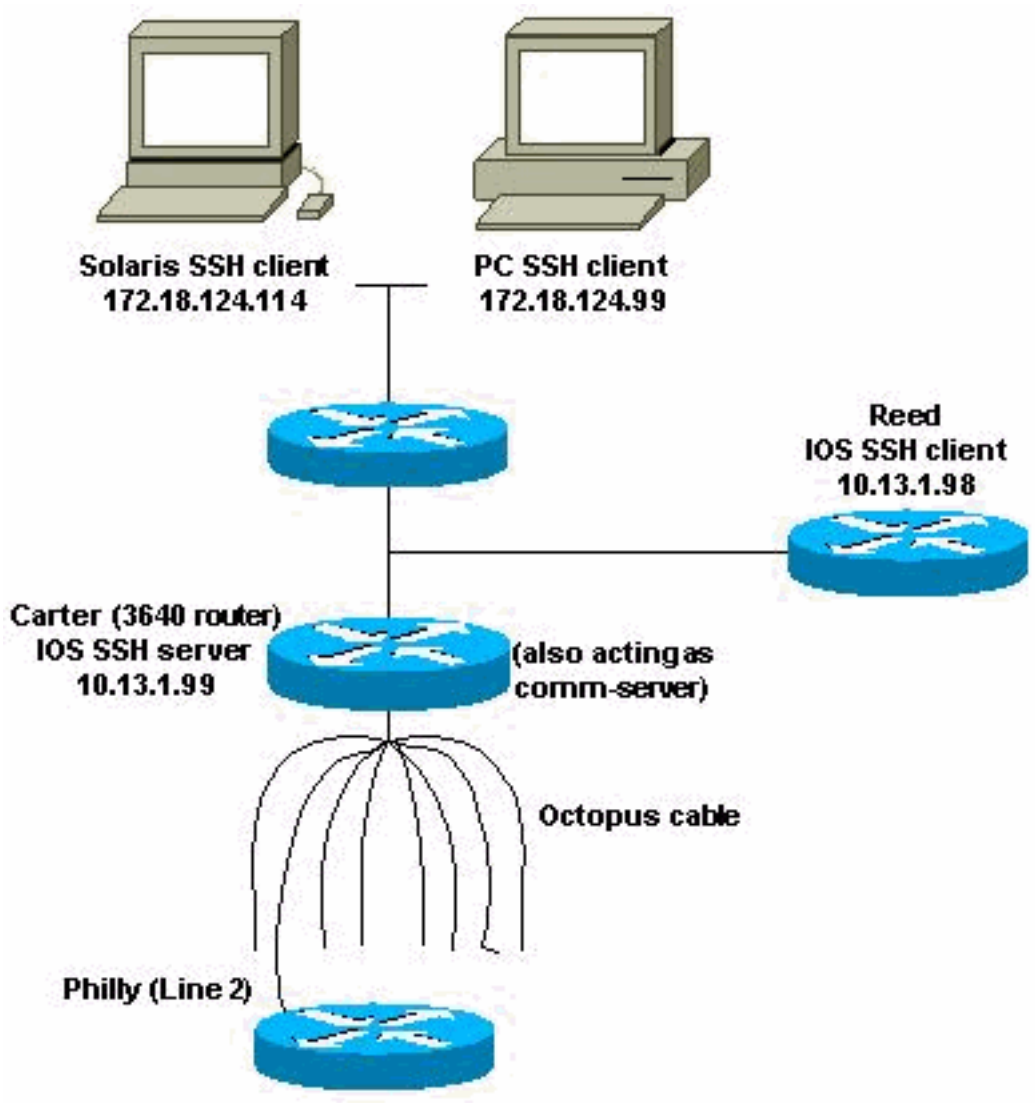
Contenu

Introduction

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

Comment configurer l’accès à la ligne de terminal SSH (également appelé invertelnet) ?

Ceci a été introduit pour la première fois dans certaines plates-formes du logiciel Cisco IOS Version 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 SSH doit se connecter, par exemple 2001.
- Groupe rotatif - Spécifie le rotatif défini qui doit rechercher un nom valide.

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

Non, ce n'est pas le cas.

Comment puis-je déterminer quelles plates-formes et versions de code prennent en charge SSH ?

Reportez-vous au Navigateur de fonctionnalités (clients enregistrés uniquement) et spécifiez la fonction **SSH**.

Lorsque j'essaie de supprimer certaines commandes SSH de mon routeur, il me demande toujours de créer des clés RSA afin d'activer SSH. Pourquoi cela ?

Voici un exemple de ce problème :

```
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 uniquement).

Cisco IOS SSH version 2 prend-il en charge la norme DSS (Digital Signature Standard) ?

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

Le serveur SSH Cisco IOS prend-il en charge le transfert d'agent ?

Cisco IOS SSH ne prend pas en charge le transfert d'agent. Il interagit avec toutes les implémentations SSH commerciales.

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

Cisco IOS SSH version 2 (SSHv2) prend en charge les méthodes d'authentification interactives au clavier et basées sur un mot de passe. En plus de ces méthodes d'authentification, la fonctionnalité d'amélioration de SSHv2 pour les clés RSA (disponible dans le logiciel Cisco IOS Version 15.0(1)M et ultérieure) prend en charge l'authentification de clé publique basée sur RSA pour le client et le serveur. Pour plus d'informations sur les mécanismes d'authentification pris en charge par le serveur SSH Cisco IOS, référez-vous à Prise en charge de Secure Shell version 2.

Que fait l'erreur `Local : Octets de vérification endommagés sur la` moyenne `d'entrée` ?

Les octets de contrôle endommagés signifient que le paquet SSH a échoué à sa vérification d'intégrité. Ceci est généralement dû à un déchiffrement incorrect. Ceci est également dû à une clé incorrecte utilisée. La clé incorrecte est causée par la suppression d'un paquet SSH chiffré. Vous avez abandonné un paquet chiffré qui aurait dû être envoyé ou abandonné un paquet chiffré reçu qui aurait dû être déchiffré.

Cisco IOS prend-il en charge SSH avec Blowfish cipher ?

Cisco IOS ne prend pas en charge SSH avec Blowfish cipher. Lorsqu'un client SSH envoie un tel chiffrement non pris en charge, le routeur affiche les messages de débogage mentionnés dans SSH Client Sends Unsupport (Blowfish) Cipher.

Lorsque j'essaie de générer des clés RSA pour l'accès SSH sur un routeur à l'aide de la commande crypto key generate rsa en mode de configuration, je reçois cette erreur : `% Entrée non valide détectée au marqueur '^'.` Il ne permet pas au routeur de générer les clés RSA pour activer l'accès SSH pour le routeur. Comment cette erreur est-elle résolue ?

Cette erreur apparaît lorsque l'image utilisée sur le routeur ne prend pas en charge la commande **crypto key generate rsa**. Cette commande est prise en charge uniquement dans les images de sécurité. Afin de résoudre cette erreur, utilisez l'image de sécurité de la série appropriée du routeur Cisco IOS utilisé.

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

Oui. Seules les images Crypto prennent en charge le chiffrement fort. Pour utiliser SSH avec des chiffrement tels que 3DES ou AES, vous devez disposer d'images Crypto sur votre périphérique Cisco.

Ces messages apparaissent dans les journaux lorsque j'essaie de configurer SSH sur un routeur : `SSH2 13 : RSA_sign : clé privée introuvable` et `SSH2 13 : échec de la création de signature, état -1.` Comment résoudre ce problème ?

Ces messages de journal sont vus en raison des ID de bogue Cisco CSCsa83601 (clients enregistrés uniquement) et CSCtc41114 (clients enregistrés uniquement). Consultez ces bogues pour obtenir plus de renseignements.

Informations connexes

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