

Erreur de vérification de signature d'AnyConnect Hostscan sur le Linux

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Problème](#)

[Solution](#)

Introduction

Ce document décrit comment résoudre une erreur de connexion de Client à mobilité sécurisé Cisco AnyConnect si vous déployez Hostscan sur le Linux.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco AnyConnect
- Cisco Secure Desktop (CSD)
- Linux

[Composants utilisés](#)

Les informations dans ce document affectent les utilisateurs de Linux qui exécutent CSD Hostscan.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

Quand un utilisateur de Linux dirige Cisco Anyconnect en même temps que CSD Hostscan, un message d'erreur apparaît qui indique que **l'estimation de posture a manqué** avec un **Hostscan initialisent l'erreur** :

Dans le fichier de **libcsd.log**, un message d'erreur indique que le certificat utilisé afin de signer la binaire CSD Hostscan a expiré :

```
[Thu Feb 07 18:52:15.774 2013][libcsd][all][csd_init]
hello
[Thu Feb 07 18:52:15.774 2013][libcsd][all][csd_init]
libcsd.so version 3.1.02040
[Thu Feb 07 18:52:15.774 2013][libcsd][debug]
[hs_transport_init] initialization
[Thu Feb 07 18:52:15.774 2013][libcsd][debug]
[hs_file_verify_with_killdate] verifying file
signature: file = [/opt/cisco/anyconnect/lib/libaccurl.so.4.2.0],
signer = [Cisco Systems, Inc.], type = [2] [Thu Feb 07 18:52:15.963
2013][libcsd][error][verify_cb]
Error 10, certificate has expired [Thu Feb 07 18:52:15.963 2013][libcsd][error][verify_cert]
Certificate is not trusted
[Thu Feb 07 18:52:15.964 2013][libcsd][error]
[hs_file_verify_with_killdate] unable to verify
the certificate trust.
[Thu Feb 07 18:52:15.964 2013][libcsd][error][hs_dl_load_global]
file signature invalid, not
loading library (/opt/cisco/anyconnect/lib/libaccurl.so.4.2.0).
```

Remarque: Des utilisateurs de Mac et Windows ne sont pas affectés par cette question. C'est parce que code client de Mac et Windows vérifie que le certificat utilisé pour signer est **valide au moment du code signant**, tandis que les contrôles de programmation de client Linux si le certificat utilisé pour signer est **actuellement valide**.

Solution

Puisque le problème est provoqué par d'ici la date à l'où le certificat a été signé, vous pouvez changer l'horloge système afin de permettre à l'utilisateur pour se connecter ; cependant, ce n'est pas une difficulté.

L'ID de bogue Cisco [CSCue49663](#) (clients [enregistrés](#) seulement) a été classé afin de résoudre ce problème. Afin d'obtenir la difficulté, améliorez à la version 3.1.02043 d'AnyConnect, ou à la mise à jour seulement le module d'engine de Hostscan à la version 3.0.11046, comme affiché ici :

```
webvpn
enable outside
csd hostscan image disk0:/hostscan 3.1.02043-k9.pkg
csd enable
anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1 regex "Windows NT"
anyconnect image disk0:/anyconnect-macosx-i386-3.1.02040-k9.pkg 2 regex "Mac OS"
anyconnect image disk0:/anyconnect-linux-3.1.02043-k9.pkg* 3 regex "Linux"
```

Remarque: Ces encres se connectent aux bonnes versions des téléchargements logiciels (clients [enregistrés](#) seulement).