Contenu

Introduction

Ce document décrit une erreur qui est produite quand une ressource (CIS) en serveur d'informations de Cisco est configurée pour la négociation de Secure Sockets Layer (SSL) (prise de contact), et elle décrit également les étapes qui sont utilisées afin de résoudre l'erreur.

Problème

Cette erreur apparaît dans **cs_server.log** :

```
Unable to load strong truststore file
```

Cette erreur indique qu'il y a un problème avec des tentatives d'accéder à ou lire le fichier qui est spécifié par la valeur **forte d'emplacement de fichier de Truststore**.

> Remarque: Par défaut, la valeur il est placé à **cis_server_keystore_strong.jks.**

Quand il n'y a pas un problème, le log contient ce message :

```
Successfully loaded strong keystore from file
```

Solution

Procédez comme suit pour résoudre ce problème :

1. Vérifiez que le fichier fort de truststore est présent.

   Pour des systèmes Linux, naviguez vers le **LS - l > app > Composite_Software > CIS_6.2.0 > conf > serveur > Sécurité cis_server_truststore_strong.jks.**

   Pour des systèmes de Microsoft Windows, naviguez vers le **C de dir : > app > cis620 > conf > serveur > Sécurité > cis_server_truststore_strong.jks.**
2. Vérifiez que le **cis_server_truststore_strong.jks** a lu des autorisations. Le fichier doit être accessible en lecture.

3. Entrez dans le **keytool - répertoriez la** commande pour le fichier afin de vérifier si le keytool imprime un résultat. Si vous ne voyez aucune sortie, le fichier de truststore pourrait être corrompu.

Remarque: Le mot de passe par défaut qui est utilisé par keytool est **changeit**.Voici un exemple :

```
C:\apps\cis620\jre\bin\keytool -list -keystore cis_server_truststore_strong.jks

Enter keystore password: changeit
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 79 entries
digicertassuredidrootca, Jan 7, 2008,...
```