

Содержание

[Введение](#)

[Проблема](#)

[Решение](#)

Введение

Этот документ описывает ошибку, с которой встречаются, когда ресурс Сервера информации о Cisco (CIS) настроен для согласования Уровня защищенных сокетов (SSL) (квитирование), и это также описывает шаги, которые используются для решения ошибки.

Проблема

Эта ошибка появляется в `cs_server.log`:

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

Эта ошибка указывает, что существует проблема с попытками обратиться или считать файл, который задан **Сильным** значением **Расположения файла Базы доверенных сертификатов**.

Примечание: По умолчанию значение это установлено в `cis_server_keystore_strong.jks`.

Когда нет проблемы, журнал содержит это сообщение:

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

Решение

Для устранения указанной неполадки выполните следующие действия:

1. Проверьте, что присутствует сильный файл базы доверенных сертификатов.

Для Систем Linux перейдите к `ls-l> приложение> Composite_Software> CIS_6.2.0> conf> безопасность server> cis_server_truststore_strong.jks`.

Для систем Microsoft Windows перейдите `dir K:> приложения> cis620> conf> безопасность server>> cis_server_truststore_strong.jks`.

2. Проверьте, что `cis_server_truststore_strong.jks` считал разрешения. Файл должен быть читаемым.
3. Введите `keytool` - команда **списка** для файла, чтобы проверить, распечатывает ли `keytool` выходные данные. Если вы не видите выходных данных, файл базы

доверенных сертификатов мог бы быть поврежден.

Примечание: Пароль по умолчанию, который используется keytool, является **changeit**. Например:

```
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,...
```