Procedura di importazione del certificato CSM CVP Smart License

Sommario

Problema

CVP Call Server: si stanno verificando errori di verifica della firma nei registri SmartAgent relativi alle licenze smart. Il sistema richiede l'importazione del certificato CSM (Cisco Smart Software Manager) nel keystore CVP per risolvere gli errori di verifica della firma durante i normali processi di aggiornamento dello stato delle licenze. Senza la catena di certificati CSM appropriata, CVP non può convalidare le transazioni di licenza con Cisco Smart Software Manager, causando problemi di conformità delle licenze.

Ambiente

- Cisco Customer Voice Portal (CVP) Call Server versione 12.6.2
- Software Contact Center - Packaged Contact Center Enterprise (PCCE)
- Servizi CVP: Server di chiamata, WSM (Web Service Manager), server VXML
- Formato keystore Java JCEKS per la gestione dei certificati
- Integrazione di Smart Licensing con Cisco Smart Software Manager (CSSM)

Risoluzione

Attenersi alla procedura dettagliata seguente per importare il certificato CSM nel keystore di CVP Call Server.

Passaggio 1: Identifica la password del keystore

Aprire una finestra di comando come amministratore e passare alla directory principale CVP per decrittografare la password del keystore:

```
cd %CVP_HOME%\bin
DecryptKeystoreUtil.bat
```

Registrare la password visualizzata dall'utilità in quanto è necessaria per tutti i comandi keytool successivi.

Passaggio 2: Archivio chiavi corrente di backup

Creare una copia di backup del keystore esistente dalla directory di sicurezza:

```
cd %CVP_HOME%\conf\security
copy .keystore backup.keystore
```

Passaggio 3: Esporta contenuto keystore corrente

Genera un elenco di tutti i certificati correnti nel keystore per riferimento:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp.tx
```

Esaminare il file generato per comprendere l'inventario dei certificati corrente.

Passaggio 4: Scarica certificati CSM

Ottenere la catena di certificati CSM richiesta dall'URL di trasporto nella pagina CVP Licensing. I requisiti del certificato dipendono dal tipo di certificato:

Per i certificati firmati dall'autorità di certificazione: Scaricare i certificati radice e intermedio singolarmente in formato cer

Per i certificati autofirmati: Scarica il certificato CSM direttamente

Salvare i file del certificato nella directory di protezione CVP:

```
%CVP_HOME%\conf\security
```

Passaggio 5: Importa certificato radice CSM (firmato da CA)

Per i certificati firmati dall'autorità di certificazione, importare prima il certificato radice:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Passaggio 6: Importa certificato intermedio CSM (firmato da CA)

Se esiste un certificato intermedio, importarlo utilizzando questo comando:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Passaggio 7: Importa certificato CSM autofirmato (alternativa)

Per i certificati autofirmati, importare direttamente il certificato CSSM:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Passaggio 8: Verifica importazione certificati

Verificare che i nuovi certificati siano presenti nel keystore:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp_ne
```

Esaminare il nuovo elenco di certificati per verificare che i certificati CSM siano stati importati correttamente.

Passaggio 9: Riavvio e verifica del servizio

Riavviare il server CVP e registrare l'ora di riavvio. Dopo il riavvio, verificare che tutti i servizi CVP siano stati avviati:

- Server di chiamata
- WSM (Web Service Manager)
- Server VXML

Attendere circa 20 minuti dall'avvio del servizio prima di procedere alla convalida.

Passaggio 10: Convalida risoluzione

Eseguire i seguenti passaggi di convalida:

Controllare i registri SmartAgent:

Passare a C:\Cisco\CVP\logs\WSM e ordinare per data di modifica. Esaminare i report di stato di 15 minuti più recenti nei log di SmartAgent. L'eccezione di verifica della firma non deve più essere visualizzata dopo il riavvio.

Verifica stato licenze:

Accedere alla pagina delle licenze CVP e verificare che il sistema mostri lo stato "registrato" e "conforme" senza errori.

Procedura di rollback (in caso di problemi)

Se si verificano problemi durante il processo di importazione dei certificati, eseguire la procedura di rollback seguente:

Passaggio 1: Arresta tutti i servizi CVP (Call Server, WSM, VXML)

Passaggio 2: Passare alla directory di protezione:

```
cd %CVP_HOME%\conf\security
```

Passaggio 3: Eliminare il keystore modificato:

```
del .keystore
```

Passaggio 4: Ripristinare il keystore di backup:

```
rename backup.keystore .keystore
```

Passaggio 5: Riavvia tutti i servizi CVP

Causa

Il keystore di CVP Call Server non contiene la catena di certificati CSM necessaria per convalidare le firme digitali da Cisco Smart Software Manager. Durante le operazioni di gestione intelligente delle licenze, CVP tenta di verificare l'autenticità delle comunicazioni relative alle licenze

utilizzando la convalida della firma basata sui certificati. Senza i certificati CSSM appropriati nel keystore Java JCEKS, questi tentativi di verifica della firma hanno esito negativo, causando errori nelle transazioni di licenza e potenziali problemi di conformità.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).