إجراء إستيراد شهادة CVP Smart License CSSM

المحتويات

مسألة

يواجه CVP Call Server أخطاء الترخيص الذكي "التحقق من التوقيع" في سجلات SmartAgent. يتطلب النظام إستيراد شهادة CSSM (مدير البرامج الذكية من Cisco) إلى مخزن مفاتيح CVP لحل حالات فشل التحقق من التوقيع أثناء عمليات تحديث حالة الترخيص العادية. بدون سلسلة شهادات CSSM المناسبة، لا يمكن CVP التحقق من حركات الترخيص مع مدير البرامج الذكية من Cisco، مما يؤدي إلى مشاكل في توافق الترخيص.

البيئة

- Cisco Customer Voice Portal (CVP) Call Server، الإصدار 12.6.2
- برنامج مركز الاتصال - Packaged Contact Center Enterprise (PCCE)
- خدمات CVP: Call Server، WSM (Web Service Manager)، VXML Server
- تنسيق مخزن مفاتيح Java JCEKS لإدارة الشهادات
- دمج الترخيص الذكي مع مدير البرامج الذكية (CSSM) من Cisco

قرار

اتبع هذه الخطوات التفصيلية لاستيراد شهادة CSSM إلى مخزن مفاتيح CVP Call Server.

الخطوة 1: التعرف على كلمة مرور مخزن المفاتيح

افتح نافذة أمر كمسؤول وانتقل إلى الدليل الرئيسي CVP لفك تشفير كلمة مرور مخزن المفاتيح:

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

قم بتسجيل كلمة المرور المعروضة من قبل هذه الأداة المساعدة كما هي مطلوبة لكل أوامر الأدوات المفتاحية التالية.

الخطوة 2: مخزن المفاتيح الحالي للنسخ الاحتياطي

إنشاء نسخة إحتياطية من مخزن المفاتيح الموجود من دليل الأمان:

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

الخطوة 3: تصدير محتويات مخزن المفاتيح الحالية

إنشاء قائمة بكافة الشهادات الحالية في مخزن المفاتيح كمرجع:

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

راجع الملف الذي تم إنشاؤه لفهم مخزون الشهادة الحالي.

الخطوة 4: تنزيل شهادات CSSM

الحصول على سلسلة شهادات CSSM المطلوبة من عنوان URL الخاص بالنقل الموجود على صفحة ترخيص CVP. تعتمد متطلبات الشهادة على نوع الشهادة:

للشهادات الموقعة من CA: تنزيل الشهادات "الجذر" و"الوسيط" بشكل فردي بتنسيق .cer

للشهادات الموقعة ذاتيا: تنزيل شهادة CSSM مباشرة

حفظ ملفات الشهادات في دليل أمان CVP:

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

الخطوة 5: إستيراد شهادة جذر CSSM (توقيع CA)

للشهادات الموقعة من CA، قم باستيراد الشهادة الجذر أولا:

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

الخطوة 6: إستيراد الشهادة الوسيطة CSSM (توقيع CA)

إذا كانت هناك شهادة وسيطة، قم باستيرادها باستخدام هذا الأمر:

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

الخطوة 7: إستيراد شهادة CSSM ذاتية التوقيع (بديل)

للشهادات الموقعة ذاتيا، قم باستيراد شهادة CSSM مباشرة:

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

الخطوة 8: التحقق من إستيراد الشهادة

تأكد من وجود الشهادات الجديدة في مخزن المفاتيح:

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

راجع قائمة الشهادات الجديدة للتحقق من إستيراد شهادات CSSM بنجاح.

الخطوة 9: إعادة التشغيل والتحقق من الخدمة

عد إعادة التشغيل، تأكد من بدء تشغيل خادم CVP وسجل وقت إعادة التشغيل. بعد إعادة التشغيل، تحقق من حالة جميع خدمات CVP:

- خادم المكالمات
- WSM (مدير خدمة الويب)
- خادم VXML

انتظر حوالي 20 دقيقة بعد بدء تشغيل الخدمة قبل متابعة التحقق من الصحة.

الخطوة 10: التحقق من دقة الحل

قم بإجراء خطوات التحقق من الصحة التالية:

تحقق من سجلات SmartAgent:

انتقل إلى C:\Cisco\CVP\logs\WSM وقم بالفرز حسب تاريخ التعديل. قم بفحص أحدث سجلات SmartAgent. يجب أن يظهر إستئناف توقيع تقارير الحالة لمدة 15 دقيقة في السجلات بعد وقت إعادة التشغيل.

التحقق من حالة الترخيص:

قم بالوصول إلى صفحة ترخيص CVP وتأكيد النظام الذي يظهر حالة "مسجل" و"في حالة التوافق" دون أخطاء.

إجراء التراجع (في حالة حدوث مشاكل)

في حالة مواجهة مشاكل أثناء عملية إستيراد الشهادة، اتبع خطوات التراجع التالية:

الخطوة 1: إيقاف جميع خدمات CVP (خادم المكالمات، WSM، VXML)

الخطوة 2: انتقل إلى دليل الأمان:

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

الخطوة 3: حذف مخزن المفاتيح المعدل:

```
del .keystore
```

الخطوة 4: إستعادة مخزن مفاتيح النسخ الاحتياطي:

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

الخطوة 5: إعادة تشغيل جميع خدمات CVP

السبب

نظرا لأن مخزن مفاتيح CVP Call Server على سلسلة شهادات CSSM المطلوبة للتحقق من الشهادات الذاتية من Cisco. أثناء عمليات الترخيص الذكية، يحاول مدير البرامج الذكية من Cisco التحقق من صحة التوقيع المستند إلى شهادة. بدون شهادات CSSM المناسبة في مخزن مفاتيح Java JCEKS، تفشل محاولات التحقق من التوقيع هذه، مما يؤدي إلى أخطاء معالمات الترخيص ومشاكل التوافق المحتملة.

المحتوى ذي الصلة

- [الدعم الفني والتنزيلات من Cisco]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).