تثبيت الشهادات الرقمية ل SSL وتجديدها واستكشاف أخطاء هذه الشهادات وإصلاحها على Cisco ISE

المحتويات

المقدمة

يصف هذا المستند تثبيت شهادة SSL وتجديدها وحلولها لمعظم المشاكل الشائعة التي

تمت مالحظتها على محرك خدمات الهوية.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن أنت تعرف Identity Service Engine GUI.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco Identity Service Engine 3.x.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يقدم هذا المستند الخطوات الموصى بها والقائمة المرجعية للمشاكل الشائعة التي يجب التحقق منها ومعالجتها قبل البدء في أستكشاف أخطاء Cisco وإصالحها واستدعاء دعم Cisco التقني.

الشهادة هي وثيقة إلكترونية تعرف شخص أو خادم أو شركة أو كيان آخر وترتبط ذلك الكيان بمفتاح عام.

يتم توقيع الشهادة الموقعة ذاتيا من قبل منشئها. يمكن أن تكون الشهادات موقعة ذاتيا أو موقعة رقميا من قبل مرجع مصدق خارجي (CA).

تعتبر الشهادة الرقمية الموقعة على المرجع المصدق (CA) معيارا صناعيا وأكثر أمانا.

تستخدم الشهادات في شبكة لتوفير وصول آمن.

يستخدم Cisco ISE شهادات الاتصال بين العقد، وللتوصيل مع الخوادم الخارجية مثل خادم Syslog وخادم موزج الويب وجميع بوابات المستخدم النهائي (بوابات الضيف والكفيل والأجهزة الشخصية).

تعرف الشهادات عقدة Cisco ISE إلى نقطة نهاية وتؤمن الاتصال بين نقطة النهاية تلك وعقدة Cisco ISE.

يتم إستخدام الشهادات لجميع إتصالات HTTPS واتصالات بروتوكول المصادقة المتوسع (EAP).

يقدم هذا المستند الخطوات الموصى بها والقائمة المرجعية للمشاكل الشائعة التي يجب التحقق منها ومعالجتها قبل البدء في أستكشاف أخطاء Cisco وإصالحها واستدعاء دعم Cisco التقني.

تأتي هذه الحلول مباشرة من طلبات الخدمة التي حلها الدعم الفني من Cisco. إذا كانت

شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل للخطوات التي تتخذها لمعالجة المشاكل.

التكوين

توضح الأدلة التالية كيفية إستيراد واستبدال الشهادات:

إستيراد شهادة نظام

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

إستبدال شهادة منتهية الصلاحية

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

المشكلات الشائعة

السيناريو 1: تعذر إستبدال شهادة مدخل تنتهي صلاحيتها على عقدة ISE

الخطأ

أثناء ربط شهادة المدخل الجديدة ب CSR، تفشل عملية ربط الشهادة مع الخطأ الموضح أدناه:

خطأ داخلي. اطلب من مسؤول ISE التحقق من السجلات للحصول على مزيد من التفاصيل

أكثر الأسباب شيوعا لهذا الخطأ هي:

- يكون للشهادة الجديدة نفس اسم الموضوع للشهادة الموجودة

- إستيراد شهادة مجددة تستخدم نفس المفتاح الخاص للشهادة الموجودة

الحل

1. تعيين إستخدام المدخل مؤقتا لشهادة أخرى على نفس العقدة
2. حذف شهادة المدخل المنتهية الصلاحية
3. تثبيت "شهادة المدخل" الجديدة ثم تعيين إستخدام المدخل

على سبيل المثال، إذا كنت ترغب في تعيين إستخدام المدخل مؤقتا لشهادة موجودة باستخدام مصادقة EAP، اتبع الخطوات التالية:

الخطوة 1. تحديد الشهادة وتحريرها باستخدام مصادقة EAP، وإضافة دور المدخل تحت الاستخدام والحفظ

الخطوة 2. حذف شهادة المدخل المنتهية الصلاحية

الخطوة 3. تحميل شهادة المدخل الجديدة دون تحديد أي دور (قيد الاستخدام) وإرسال

الخطوة 4. تحديد شهادة المدخل الجديدة وتحريرها وتعيين دور المدخل تحت الاستخدام والحفظ

السيناريو 2: لا يمكن إنشاء مقياسين CSR لنفس عقدة ISE مع إستخدام متعدد الاستخدام

أطخلا

يفشل إنشاء CSR جديد لنفس العقدة مع إستخدام متعدد الاستخدام مع الخطأ:
توجد بالفعل شهادة أخرى بنفس الاسم المألوف. يجب أن تكون الأسماء المألوفة فريدة.

الحل

يتم ترميز الأسماء المألوفة ل CSR ترميزا ثابتا لكل عقدة ISE حتى ال تسمح بإنشاء 2 CSRs لنفس العقدة مع الاستخدام المتعدد. توجد حالة الاستخدام في عقدة معينة، وهناك شهادة موقعة من CA يتم إستخدامها لاستخدام مصادقة EAP و Admin وشهادة أخرى موقعة من CA يتم إستخدامها لاستخدام SAML والمدخل والكل الشهادات قيد الانتاء.

في هذا السيناريو:

الخطوة 1. إنشاء CSR الأول باستخدام متعدد الاستخدام

الخطوة 2. ربط الشهادة الموقعة من قبل CA مع CSR الأول وتعيين دور مصادقة EAP و Admin

الخطوة 3. إنشاء CSR ثان باستخدام متعدد الاستخدام

الخطوة 4. ربط الشهادة الموقعة من CA مع CSR الثاني وتعيين SAML ودور المدخل

السيناريو 3: تعذر ربط الشهادة الموقعة من المرجع المصدق لاستخدام المدخل بسبب عدم القدرة على تعيين علامة المدخل للشهادة والحصول على خطأ

أطخلا

يؤدي ربط شهادة موقعة من CA لاستخدام المدخل إلى حدوث الخطأ:

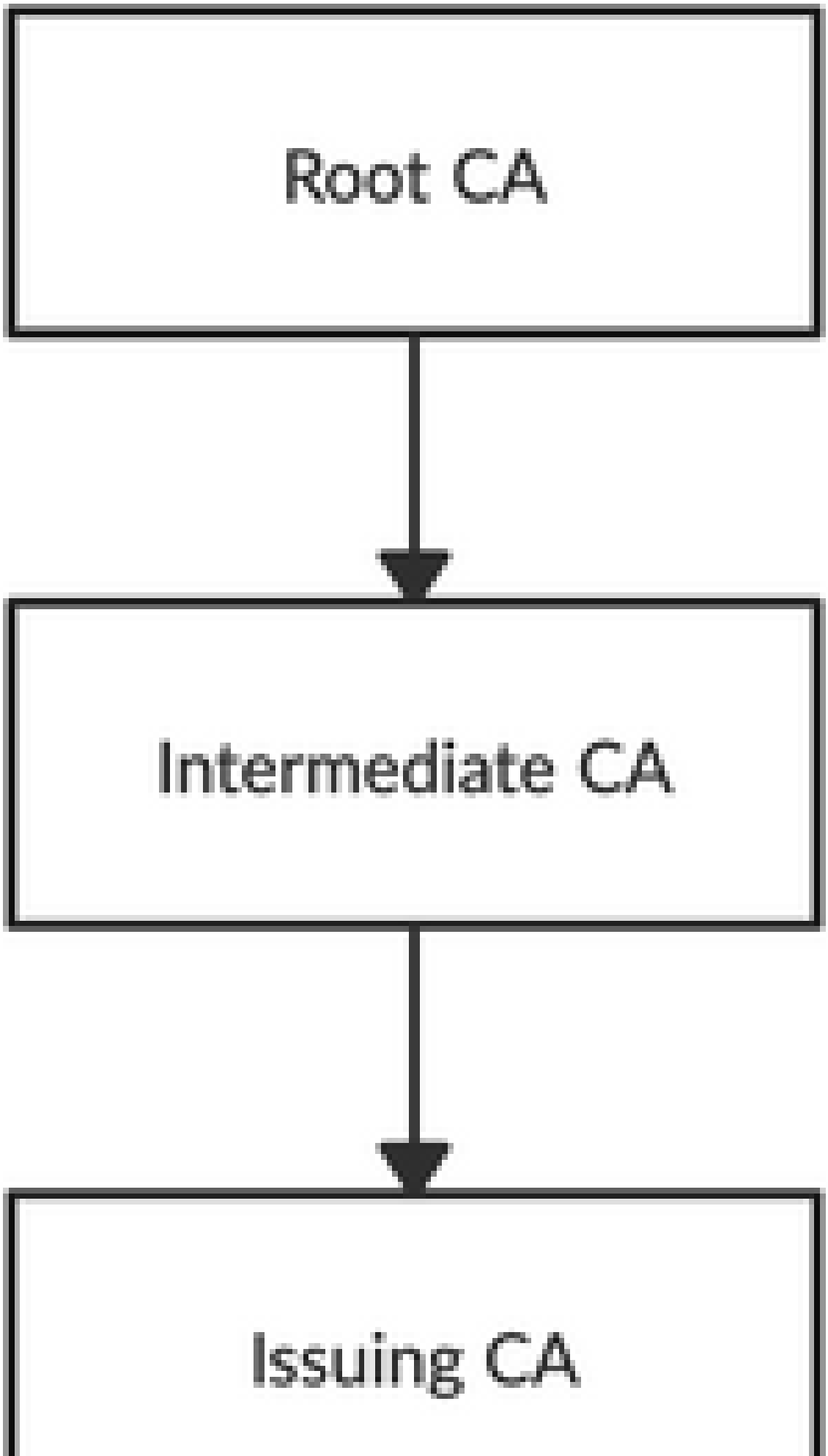
توجد شهادة (شهادات) موثوق بها واحدة أو أكثر تشكل جزءا من سلسلة شهادات نظام المدخل أو مدخل مع نفس الاسم الموضوع ولكن له رقم تسلسلي مختلف. تم إجهاض عملية الاستيراد/التحديث. للاستيراد/التحديث الناجح، تحتاج إما إلى تعطيل دور مصادقة المؤول المستند إلى سلة التوسق من شهادة موثوق بها مكررة أو تغيير دور المدخل من شهادة النظام التي تحتوي على الشهادة الموثوق بها المكررة في سلسلتها.

الحل

الخطوة 1. تحقق من سلسلة شهادات الشهادة الموقعة من CA (لاستخدام المدخل) وفي مخزن

الشهادات الموثوق بها، تحقق من وجود أي شهادات مكررة من سلسلة الشهادات.
الخطوة 2. قم بإزالة الشهادة المكررة أو قم بإلغاء تحديد خانة الاختيار Trust لمصادقة المسؤول المستند إلى شهادة من الشهادة المكررة.

على سبيل المثال، تحتوي شهادة المدخل الموقعة من قبل CA على سلسلة الشهادات التالية:


Root CA
Intermediate CA
Issuing CA

الـ 3 في سلسلة الشهادات (يمكن أن تكون شهادة منتهية الصلاحية) وقم بإزالة الشهادات المكررة من مخزن الشهادات الموثوق بها.

السيناريو 4: تعذر حذف الشهادة الافتراضية الموقعة ذاتيا والمنتهية الصلاحية من مخزن الشهادات الموثوق بها

الخطأ

يؤدي حذف الشهادة الافتراضية الموقعة ذاتيا والمنتهية الصلاحية من مخزن الشهادات الموثوق بها إلى حدوث الخطأ:
غير مسموح بتعطيل الشهادة أو حذفها أو الثقة بأنها تمت الإشارة إليها إما في شهادات النظام و/أو في syslog الآمن بضمان أهداف التسجيل عن بعد.

الحل

1. تحقق من عدم اقتران الشهادة الافتراضية الموقعة ذاتيا والمنتهية الصلاحية بأي هدف تسجيل عن بعد موجود. يمكن التحقق من هذا الإجراء تحت الإدارة > النظام > تسجيل الدخول > أهداف التسجيل عن بعد > تحديد SecureSyslogCollector(آت) وتحريرها
2. تحقق من أن الشهادة الافتراضية المنتهية الصلاحية الموقعة ذاتيا غير مقترنة بأي دور معين (إستخدام). يمكن التحقق من ذلك تحت الإدارة > النظام > الشهادات > شهادات النظام.

إذا إستمرت المشكلة، اتصل ب TAC.

السيناريو 5: تعذر ربط شهادة CA الموقعة ب pxGrid مع CSR على عقدة ISE

الخطأ

أثناء ربط شهادة pxGrid الجديدة ب CSR، تفشل عملية ربط الشهادة مع الخطأ:

يجب أن تحتوي شهادة PxGrid على مصادقة العميل والخادم في ملحق إستخدام المفتاح الموسع (EKU).

الحل

تأكد من أنه يجب أن تحتوي شهادة pxGrid الموقعة من CA على كل من مصادقة خادم ويب TLS (1.3.6.1.5.5.7.3.1) ومصادقة عميل ويب TLS (1.3.6.1.5.5.7.3.2) باستخدام مفتاح موسع لأنه يتم إستخدامه لكل من مصادقة العميل والخادم (لتأمين الاتصال بين عميل PxGrid والخادم)

الرابط المرجعي: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

السيناريو 6: تعذر حذف الشهادة الافتراضية الموقعة ذاتيا والمنتهية الصلاحية من مخزن الشهادات الموثوق به بسبب تكوين ملف تعريف LDAP أو

SCEP RA الموجود

الخطأ

يؤدي حذف الشهادة الافتراضية الموقعة ذاتيا والمنتهية الصلاحية من مخزن الشهادات الموثوق بها إلى حدوث الخطأ:

تعذر حذف "شهادة الثقة" لأنه تمت الإشارة إليها في مكان آخر، ربما من ملف تعريف SCEP RA أو مصدر هوية LDAP

* شهادة خادم التوقيع الذاتي الافتراضية

لحذف الشهادة (الشهادات)، احذف توصيف SCEP RA أو حرر مصدر تعريف LDAP لعدم إستخدام هذه الشهادة.

الحل

1. انتقل إلى إدارة > إدارة الهوية > مصادر الهوية الخارجية > LDAP > اسم الخادم > الاتصال
2. تأكد من أن LDAP Server Root CA الي يستخدم "شهادة الخادم الافتراضية الموقعة ذاتيا"
3. إذا لم يكن خادم LDAP يستخدم الشهادة المطلوبة لتوصيل آمن، انتقل إلى إدارة > نظام > شهادات > مرجع شهادات > إعدادات CA الخارجية > توصيفات SCEP RA
4. تأكد من أن أي من توصيفات SCEP RA ال تستخدم شهادة ذاتية التوقيع افتراضي

موارد إضافية

كيفية تثبيت شهادة حرف بدل
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

إدارة شهادات ISE
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

تثبيت شهادة مرجع مصدق من جهة خارجية على ISE
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html

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).