فهم خدمات المرجع المصدق الداخلي ل ISE

المحتويات

المقدمة

يصف هذا المستند خدمة CA وخدمة التسجيل عبر النقل الآمن (EST) الموجودة في محرك خدمات تعريف Cisco (ISE).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- محرك خدمات كشف الهوية (ISE)
- الشهادات والبنية الأساسية للمفاتيح العام (PKI)
- بروتوكول تسجيل الشهادة البسيط (SCEP)
- بروتوكول حالة الشهادة عبر الإنترنت (OCSP)

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى Identity Services Engine 3.0.

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.

خدمة المرجع المصدق (CA)

يمكن أن تكون الشهادات موقعة ذاتيا أو موقعة رقميا من قبل مرجع مصدق خارجي (CA). توفر هيئة الشهادة الداخلية ISE (ISE CA) من Cisco إصدار وإدارة الشهادات الرقمية لنقاط النهاية من وحدة تحكم مركزية للسماح للموظفين باستخدام أجهزتهم الشخصية على شبكة الشركة. تعتبر الشهادة الرقمية الموقعة على المرجع المصدق (CA) معياريا صناعيا وأكثر أمانا. عقدة إدارة السياسة الأساسية (PAN) هي المرجع المصدق الجذر. عقد خدمة السياسة (PSN) هي عقد CA التابعة ل PAN الأساسية.

وظيفة ISE CA

يوفر ISE CA هذه الوظيفة:

- إصدار الشهادة: للتحقق من صحة طلبات توقيع الشهادة (CSRs) وتوقيعها لنقاط النهاية المتصلة بالشبكة.
- إدارة المفاتيح: إنشاء المفاتيح والشهادات وتخزينها بأمان على كل من عقد PAN و PSN.
- تخزين الشهادات: يقوم بتخزين الشهادات التي يتم إصدارها للمستخدمين والأجهزة.
- دعم بروتوكول حالة الشهادة عبر الإنترنت (OCSP): يوفر مستجيب OCSP للتحقق من صحة الشهادات.

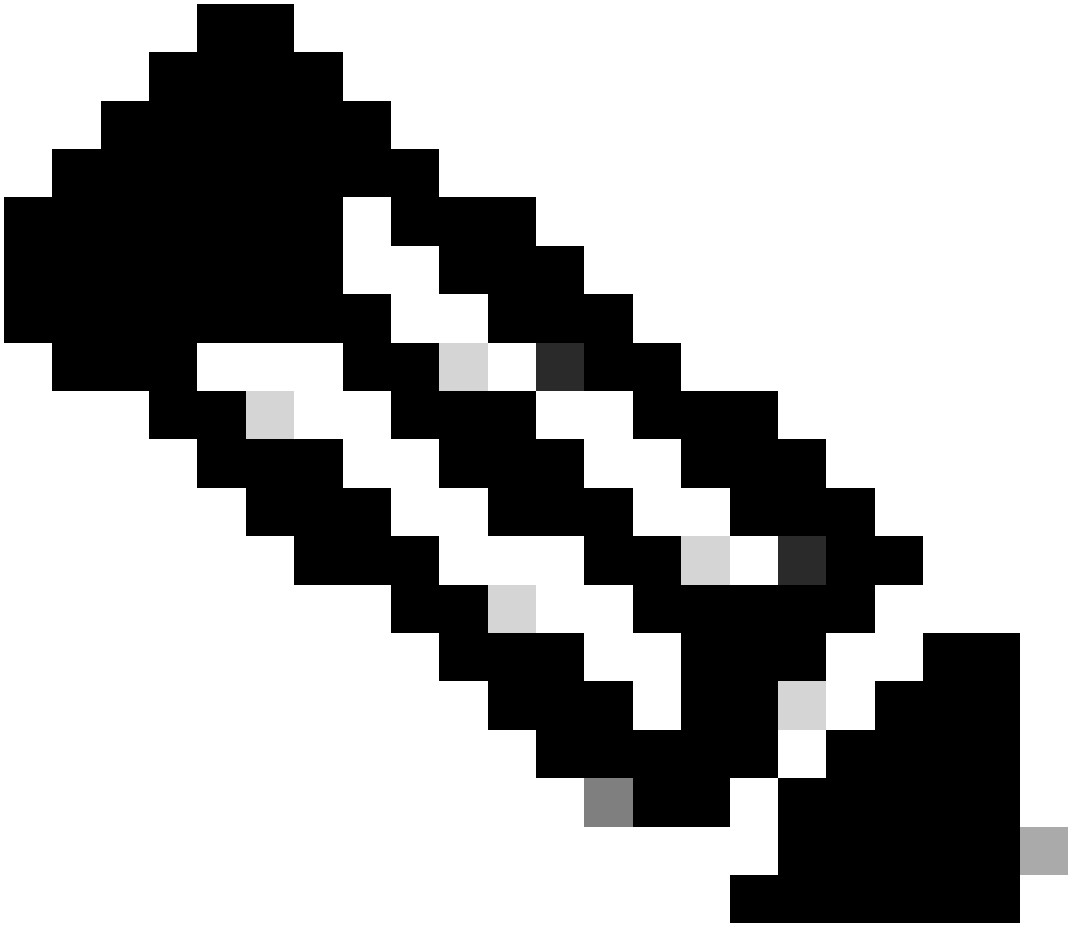
شهادات ISE CA الموزعة على عقد خدمة الإدارة والسياسة

بعد التثبيت، يتم توزيع عقدة Cisco ISE بشهادة CA الجذر وشهادة CA للعقدة لإدارة الشهادات لنقاط النهاية.

عند إعداد نشر، تصبح العقدة المعينة كعقدة الإدارة الأساسية (PAN) المرجع المصدق الجذر. تحتوي PAN على شهادة CA الجذر وشهادة CA للعقدة موقعة بواسطة CA الجذر.

عند تسجيل عقدة إدارة ثانوية (SAN) إلى PAN، يتم إنشاء شهادة مرجع مصدق للعقدة وتوقيعها من المرجع المصدق الجذر على عقدة الإدارة الأساسية.

يتم توفير أي عقدة خدمة نهج (PSN) مسجلة مع PAN لنقطة النهاية وشهادة OCSP الموقعة بواسطة المرجع المصدق للعقدة من PAN. عقد خدمة السياسة (PSN) هي عقد CA التابعة لـ PAN. عند إستخدام ISE CA، يصدر CA لنقطة النهاية على PSN الشهادات إلى نقاط النهاية التي تصل إلى الشبكة.



ملاحظة: من ISE 3.1 Patch 2 و ISE 3.2 FCS، تم تغيير التسلسل الهرمي لشهادات OCSP.

وفقا لمعيار RFC 6960:

"يجب أن يقوم مصدر الشهادة بأحد الأمور التالية:

- توقيع استجابات OCSP نفسها، أو

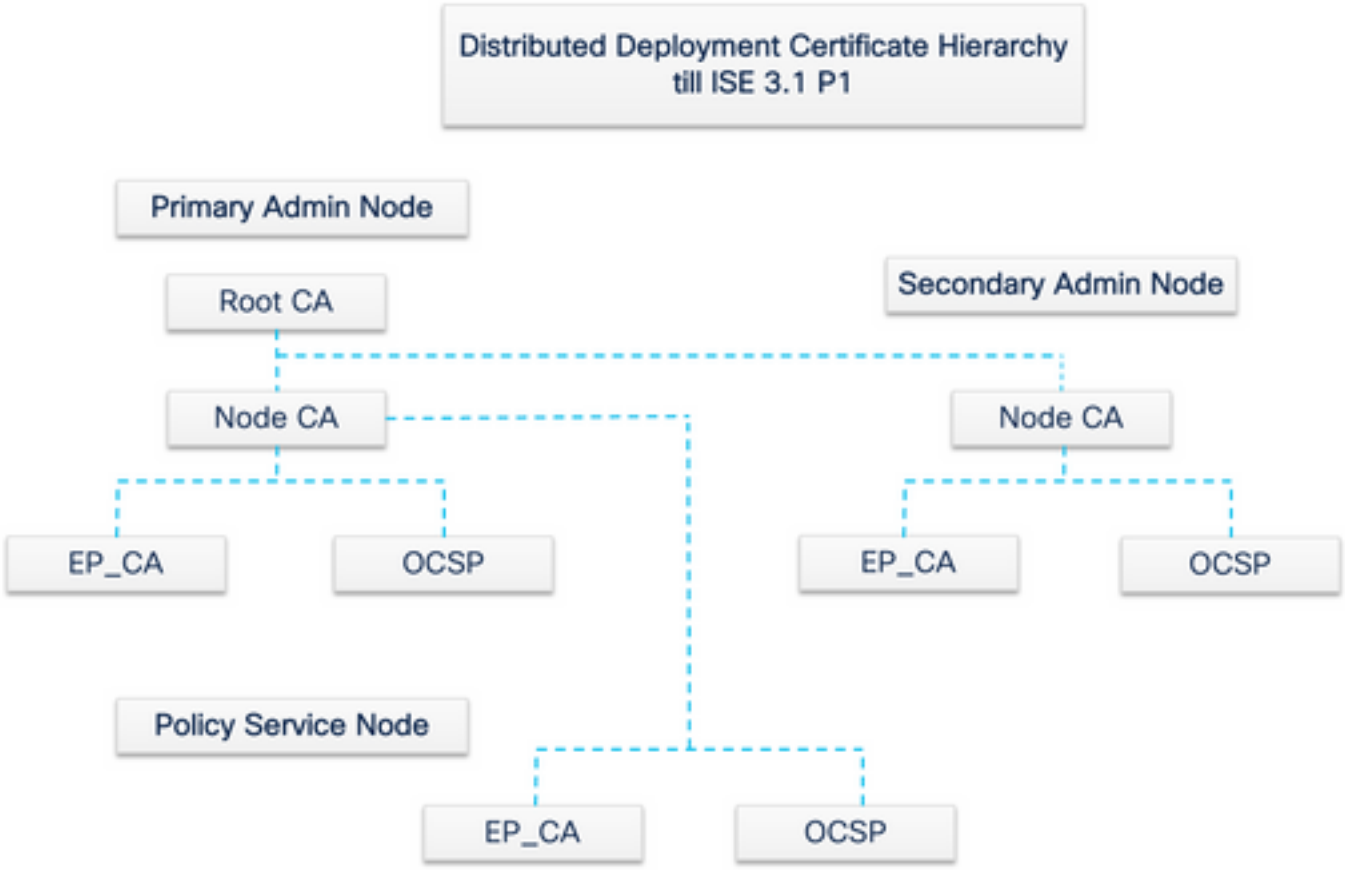
- تعيين هذه السلطة بشكل صريح لكيان آخر

"يجب أن تصدر شهادة الموقع على الاستجابة OCSP مباشرة من المرجع المصدق المحدد في الطلب. "

"يجب أن يعترف النظام (الذي يعتمد) على استجابات OCSP بشهادة تفويض صادرة عن CA ال تصدر الشهادة المعنية إلا إذا كانت شهادة التفويض والشهادة (التي تم تحديدها)

للإلغاء موقعين بنفس المفتاح."

لكي تكون متوافقة مع معيار RFC المذكور سابقا، يتم تغيير التدرج الهرمي لشهادة المستجيب OCSP في ISE. تم الآن إصدار شهادة المستجيب OCSP بواسطة المرجع المصدق الفرعي لنقطة النهاية لنفس العقدة بدلا من المرجع المصدق للعقدة في PAN.



التسجيل عبر خدمة النقل الآمن (EST)

ظل مفهوم البنية التحتية للمفتاح العام قائما لفترة طويلة. وتصادق هذه المذكرة هوية المستخدمين والأجهزة عن طريق أزواج المفاتيح العامة الموقعة في شكل شهادات رقمية. التسجيل عبر النقل الآمن (EST) هو بروتوكول لتوفير هذه الشهادات. تحدد خدمة EST كيفية تنفيذ تسجيل الشهادة للعملاء الذين يستخدمون إدارة الشهادة عبر صياغة الرسائل المشفرة (CMC) عبر نقل آمن. وفقا لمعيار IETF - يصف معيار EST بروتوكول لإدارة الشهادات يتسم بالبساطة والوظيفة في الوقت نفسه يستهدف عملاء البنية الأساسية للمفتاح العام (PKI) الذين يحتاجون إلى الحصول على شهادات العملاء وشهادات المرجع المصدق المرتبطة بها. كما يدعم أزواج المفاتيح العامة/الخاصة التي يصنعها العملاء، فضلا عن الأزواج الرئيسية التي يصنعها القانون الجنائي.

حالات إستخدام EST

يمكن إستخدام بروتوكول EST:

- لتسجيل أجهزة الشبكة عن طريق معرف الجهاز الفريد الآمن

- لحلول BYOD

لماذا؟

إمداد شهادة عنوان كل من بروتوكولي EST و SCEP. EST هو خليفة لبروتوكول تسجيل الشهادة البسيط (SCEP). نظرا لبساطته، كان SCEP البروتوكول الفعلي في تقديم الشهادات لسنوات عديدة. ومع ذلك، يوصى باستخدام EST عبر SCEP لهذه الأسباب:

- إستخدام قوائم التحكم في الوصول (TLS) للنقل الآمن للشهادات والرسائل - في EST، يمكن ربط طلب توقيع الشهادة (CSR) إلى طالب موثوق به ومصادق عليه بالفعل مع TLS. الا يستطيع العملاء الحصول على شهادة إلا أنفسهم. في SCEP، تتم مصادقة CSR بواسطة سر مشترك بين العميل و CA. وهذا يقدم شواغل أمنية لأن شخصا لديه حق الوصول إلى السر المشترك يمكنه أن يولد شهادات لكيانات أخرى غير نفسها.
- دعم تسجيل الشهادات الموقعة على ECC - توفر EST سرعة تشفير. إنه يدعم تشفير المنحنى البيضاوي (ECC). الا يدعم بروتوكول SCEP بروتوكول ECC ويعتمد على تشفير RSA. يوفر نظام تصحيح الأخطاء (ECC) مستوى أمان أكبر وأداء أفضل من خوارزميات التشفير الأخرى مثل RSA حتى أثناء إستخدامه لحجم مفتاح أصغر كثيرا.
- تم تصميم EST لدعم إعادة تسجيل الشهادة تلقائيا.

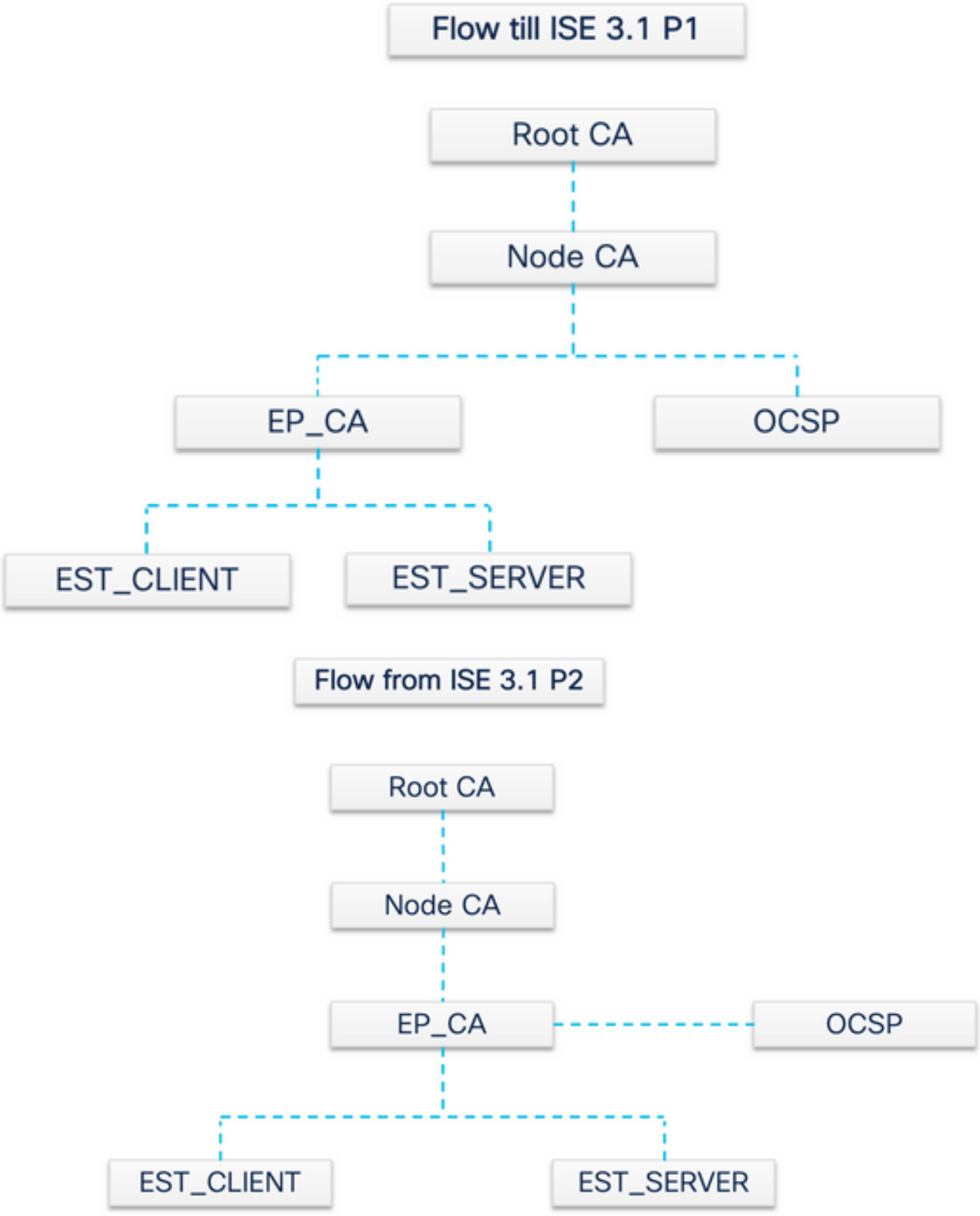
يساعد الأمان المؤكد من خلال TLS والتحسين المستمر على ضمان أمان معاملات EST من حيث الحماية المشفرة. يعمل الدمج الوثيق عبر بروتوكول SCEP مع محول وحدة التخزين عن بعد لحماية البيانات على التعرف على المخاوف الأمنية مع تقدم التقنية (RSA).

EST في ISE

لتنفيذ هذا البروتوكول، يلزم وجود عميل ووحدة خادم:

- EST Client - مضمنة في برنامج ISE Tomcat العادي.
- خادم EST - يتم نشره على خادم ويب مفتوح المصدر يسمى NGINX. يتم تشغيل هذه كعملية منفصلة، ويتم استماعه على المنفذ 8084.

يتم دعم مصادقة العميل والخادم المستندة إلى الشهادة بواسطة EST. يصدر المرجع المصدق لنقطة النهاية شهادة عميل EST وخادم EST. يتم تخزين شهادات عميل وخادم EST والمفاتيح الخاصة بها في قاعدة بيانات ISE CA NSS.



أنواع الطلبات في ISE EST

كلما ظهر خادم EST، يحصل على أحدث نسخة من كل شهادات CA من خادم CA ويخزنها. بعد ذلك، يمكن لعميل EST تقديم طلب شهادة CA للحصول على السلسلة بأكملها من خادم EST هذا. قبل أن يقوم بطلب تسجيل بسيط، يجب على عميل EST إصدار طلب شهادة CA أولا.

طلب شهادات CA (استنادا إلى RFC 7030)

1. يطلب عميل EST نسخة من شهادات CA الحالية.
2. HTTPS الحصول على رسالة بقيمة مسار العملية الخاصة ب /cacerts.

- يتم إجراء هذه العملية قبل أي طلبات EST أخرى.
- يتم إجراء طلب كل 5 دقائق للحصول على نسخة من أحدث شهادات CA.
- يجب أال يتطلب خادم EST مصادقة العميل.

أما الطلب الثاني فهو طلب تسجيل بسيط ويحتاج إلى مصادقة بين عميل EST وخادم EST. يحدث ذلك في كل مرة تتصل فيها نقطة نهاية ب ISE وتضع طلبا للشهادة.

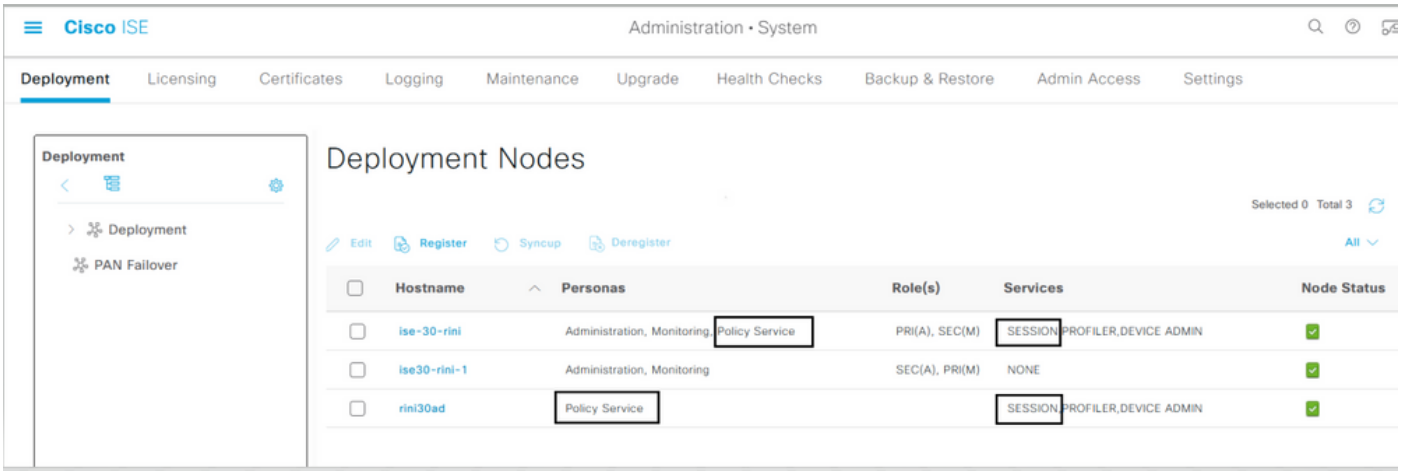
طلب تسجيل بسيط (استنادا إلى RFC 7030)

1. طلب عميل EST شهادة من خادم EST.
2. رسالة HTTPS POST بقيمة مسار العملية ل /simpleenroll.

- يقوم عميل EST بدمج طلب PKCS#10 ضمن هذه المكالمة التي يتم إرسالها إلى ISE.
- يجب أن يقوم خادم EST بمصادقة العميل.

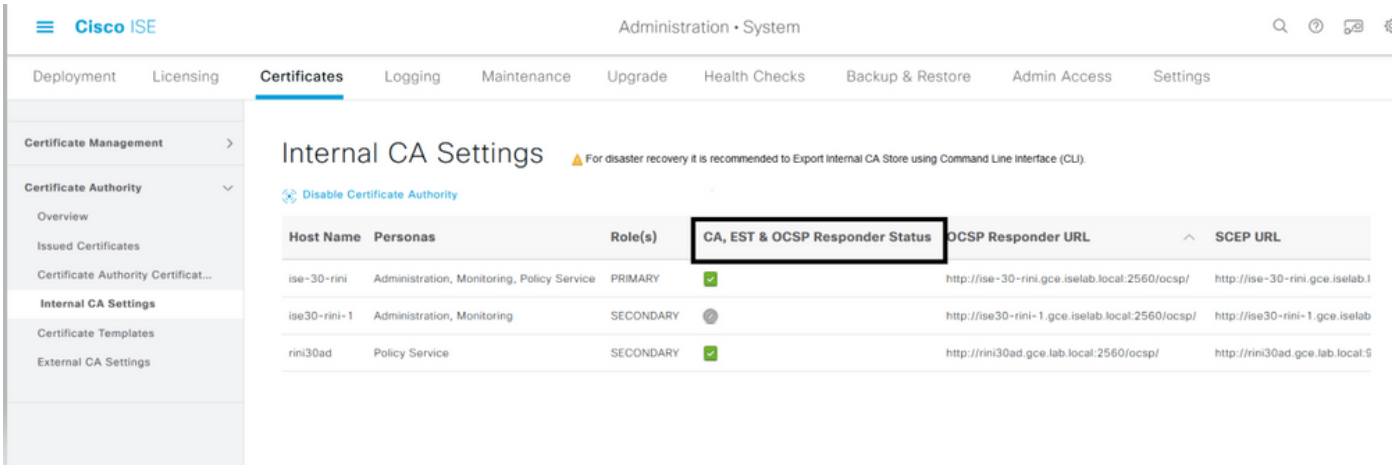
حالة خدمة EST و CA

يمكن تشغيل خدمات CA و EST فقط على عقدة خدمة النهج التي تم تمكين خدمات جلسة العمل عليها. لتمكين خدمات جلسة العمل على عقدة، انتقل إلى Administration > System > Deployment . حدد اسم المضيف للخادم الذي تحتاج خدمات جلسة العمل إلى تمكينها وانقر فوق Edit . حدد خانة **Enable Session Services** الاختيار ضمن "شخص خدمة النهج".



الحالة الموضحة في واجهة المستخدم الرسومية (GUI)

ترتبط حالة خدمة EST بحالة خدمة ISE CA على ISE. إذا كانت خدمة CA قيد التشغيل، تكون خدمة EST في وضع التشغيل، وإذا كانت خدمة CA معطلة، تكون خدمة EST معطلة أيضا.



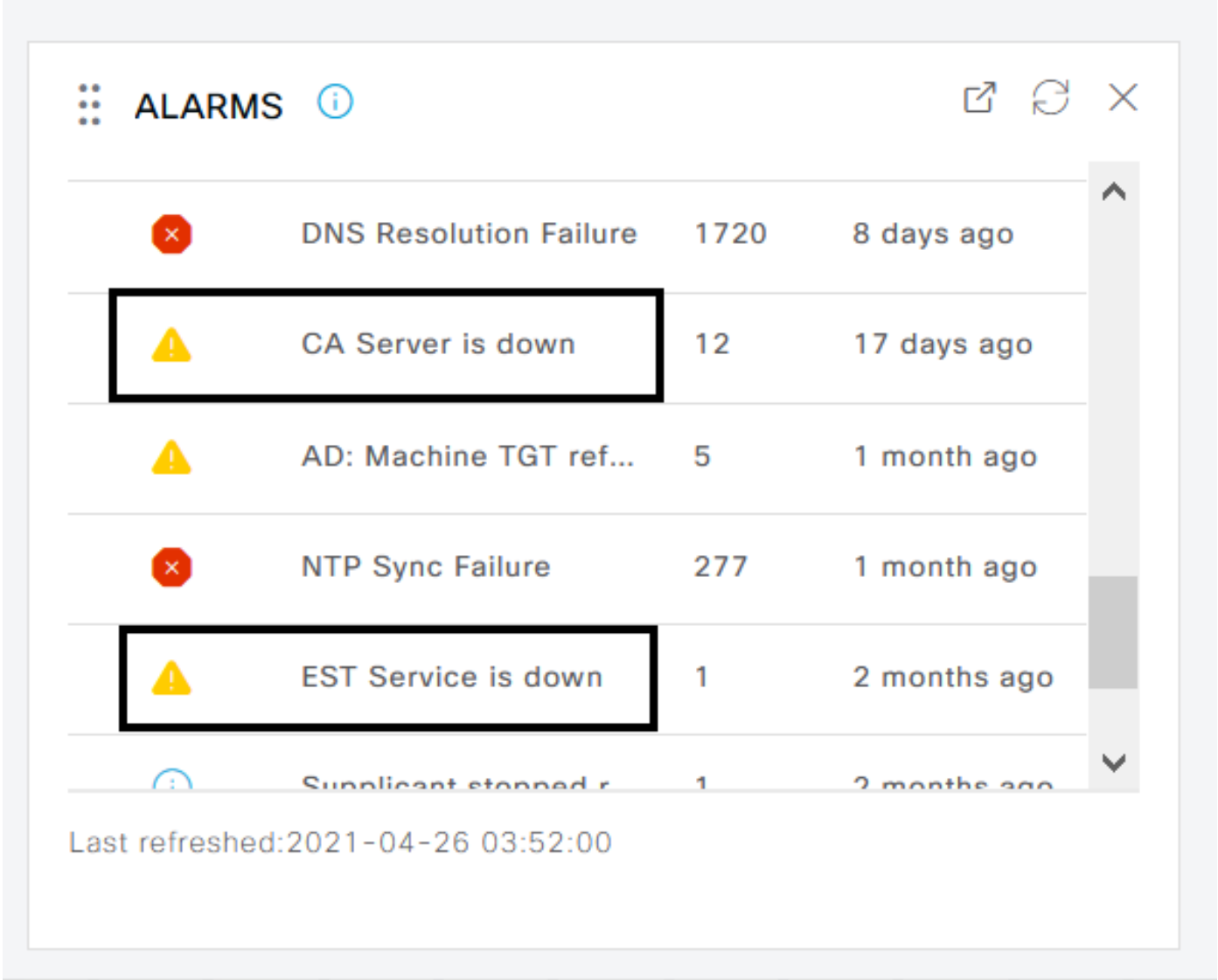
الحالة المعروضة على CLI (واجهة سطر الأوامر)

```
ise-30-rini/admin# sh app status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          61993
Database Server                        running          159 PROCESSES
Application Server                     running          72240
Profiler Database                      running          68224
ISE Indexing Engine                    running          74972
AD Connector                           running          78912
M&T Session Database                   running          68007
M&T Log Processor                      running          70533
Certificate Authority Service          running          63090
EST Service                            running          64492
SXP Engine Service                     disabled
Docker Daemon                          running          64427
TC-NAC Service                         disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
```

تنبيهات على لوحة المعلومات

يتم عرض التنبيه على لوحة معلومات ISE إذا كانت خدمات EST و CA معطلة.



التأثير إذا لم تكن خدمات CA و EST قيد التشغيل

- قد يحدث فشل في إستدعاء EST Client/cacerts عند تعطل خادم EST. كما /cacerts يمكن أن يحدث فشل الاستدعاء إذا لم تكتمل سلسلة شهادة CA لسلسلة EST.

- فشلت طلبات تسجيل شهادة نقطة النهاية المستندة إلى ECC.

- فواصل تدفق BYOD في حالة حدوث أي من الإخفاقين السابقين.
- يمكن إنشاء تنبيهات خطأ إرتباط قائمة الانتظار.

استكشاف الأخطاء وإصلاحها

إذا لم يعمل تدفق BYOD مع بروتوكول EST بشكل صحيح، فتحقق من هذه الشروط:

- تم إكمال سلسلة شهادات CA لنقطة نهاية خدمات الشهادات الفرعية. للتحقق مما إذا كانت سلسلة الشهادات مكتملة:

  1. انتقل إلى Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates .

  - حدد خانة الاختيار المجاورة للشهادة وانقر فوق عرض للتحقق من شهادة معينة.

- تأكد من تشغيل خدمات CA و EST. إذا لم تكن الخدمات قيد التشغيل، انتقل إلى Administration > System > Certificates > Certificate Authority > Internal CA Settings لتمكين خدمة CA.

- إذا تم إجراء ترقية، فاستبدل سلسلة شهادات ISE Root CA بعد الترقية. للقيام بذلك:

  1. اختَر Administration > System > Certificates > Certificate Management > Certificate Signing Requests.

- انقر.Generate Certificate Signing Requests (CSR)

- حدد ISE Root CA في Certificate(s) will be used for القائمة المنسدلة

- انقر.Replace ISE Root CA Certificate Chain

- تصحيح الأخطاء المفيد الذي يمكن تمكينه لفحص السجلات يتضمن est ، provisioning ، ca-service ، و ca-service-cert . راجع ise-psc.log وcatalina.out و caservice.log , و error.logالملفات.

معلومات ذات صلة

- 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).