ISE SAML-certificaat

Inhoud

Inleiding

Dit document beschrijft Security Association Markup Language (SAML) systeemcertificaten in Cisco Identity Services Engine (ISE). Het betreft het doel van de SAML-certificaten, de wijze waarop de vernieuwing moet worden uitgevoerd, en tenslotte het beantwoorden van veelvuldige veelgestelde vragen. Het programma bestrijkt ISE van versie 2.4 tot 3.0. Het programma dient echter gelijk te zijn aan of identiek te zijn aan andere ISE 2.x en 3.x softwarereleases, tenzij anders vermeld.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

1. Cisco ISE
2. De gebruikte terminologie om verschillende soorten ISE- en verificatie-, autorisatie- en accounting (AAA)-implementaties te beschrijven
3. RADIUS-protocol en AAA-basis
4. SAML-protocol
5. SSL/TLS en x509-certificaten
6. Basisinfrastructuur (PKI)

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Identity Services Engine (ISE), release 2.4 - 3.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de

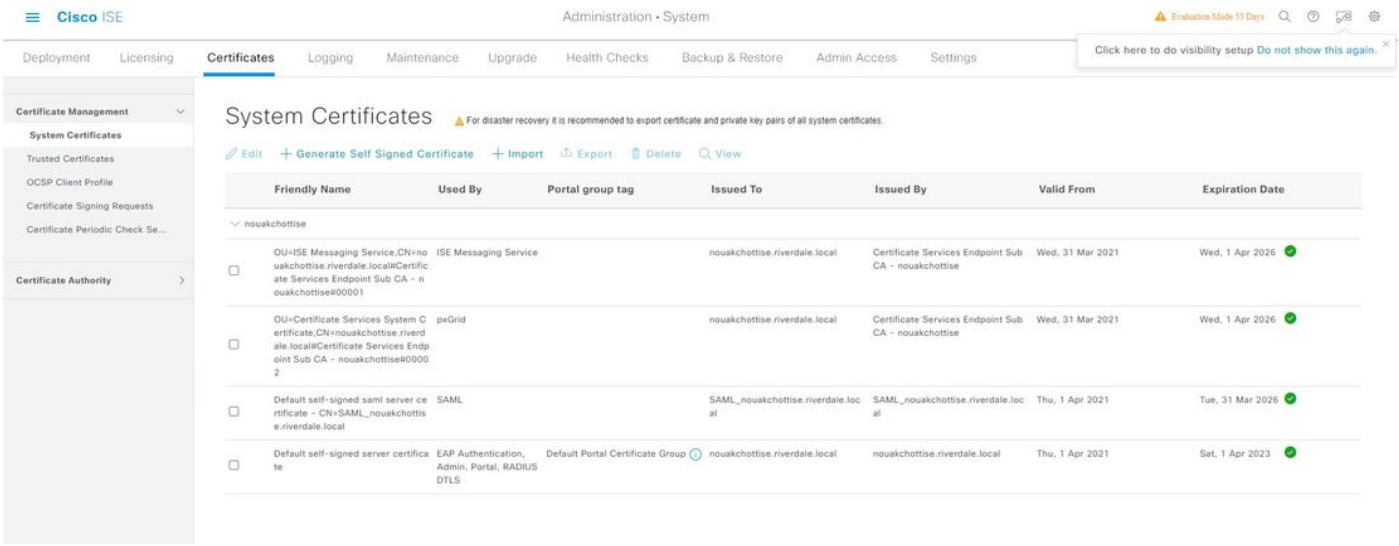
mogelijke impact van om het even welke opdracht of configuratie begrijpt.

SSL-certificaten in ISE

Een Secure Socket Layer (SSL) certificaat is een digitaal bestand dat een individu, een server of een andere digitale entiteit identificeert en die entiteit associeert met een openbare sleutel. Een zelfgetekend certificaat wordt ondertekend door de maker. Certificaten kunnen zelf worden ondertekend of digitaal worden ondertekend door een externe certificaatautoriteit (CA) - doorgaans een eigen CA-server van het bedrijf of een bekende CA-verkoper. Een door CA ondertekend digitaal certificaat wordt beschouwd als een industriestandaard en veiliger dan een door zichzelf ondertekend certificaat.

Cisco ISE is gebaseerd op PKI om veilige communicatie met zowel endpoints en beheerders, tussen ISE en andere servers/services en tussen Cisco ISE-knooppunten in een multinationale implementatie te bieden. PKI maakt gebruik van X.509 digitale certificaten voor de overdracht van openbare sleutels voor encryptie en decryptie van berichten en voor de verificatie van de authenticiteit van andere certificaten die gebruikers en apparaten vertegenwoordigen. Via het Cisco ISE-beheerportaal kunt u deze X.509-certificaten beheren.

In ISE zijn systeemcertificaten servercertificaten die een Cisco ISE-knooppunt voor andere toepassingen identificeren (zoals endpoints, andere servers, enz.). Elk Cisco ISE-knooppunt heeft zijn eigen systeemcertificaten die zijn opgeslagen op het knooppunt, samen met de bijbehorende privé-toetsen. Elk systeemcertificaat kan in kaart worden gebracht in 'Roles' die het doel van het certificaat aangeven zoals in de afbeelding.



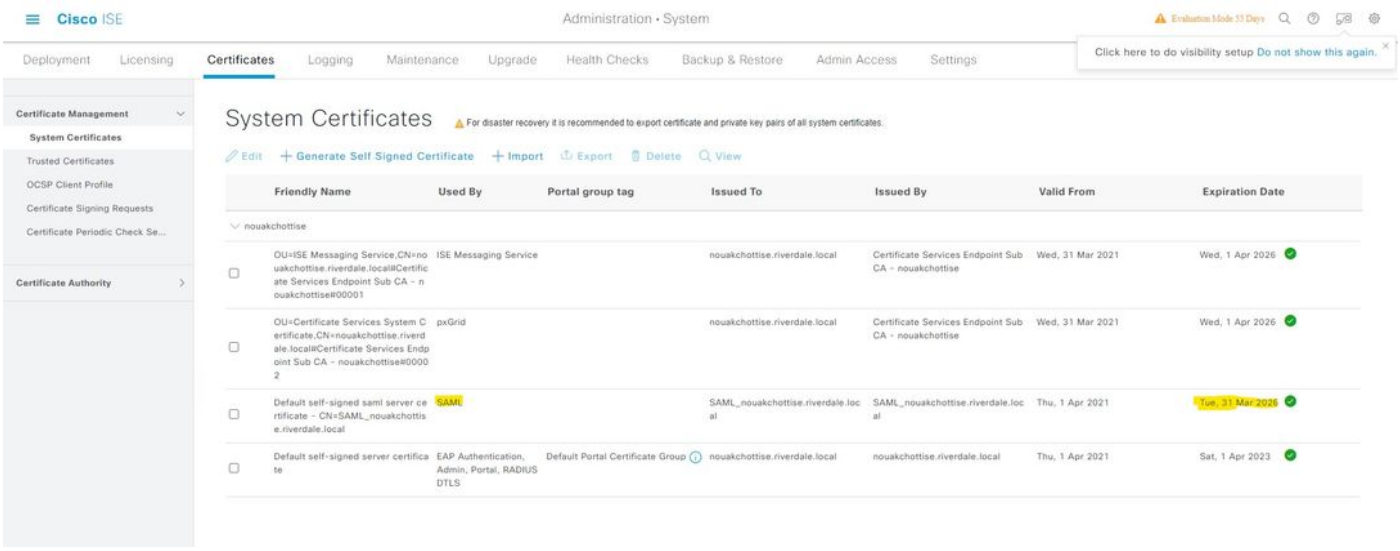
ISE 3.0 systeemcertificaten

Het toepassingsgebied van dit document is alleen van toepassing op het SAML-certificaat. Raadpleeg voor andere certificaten in ISE en meer over SSL-certificaten in ISE in het algemeen dit document: TLS/SSL-certificaten in ISE - Cisco

SAML-certificaat in ISE

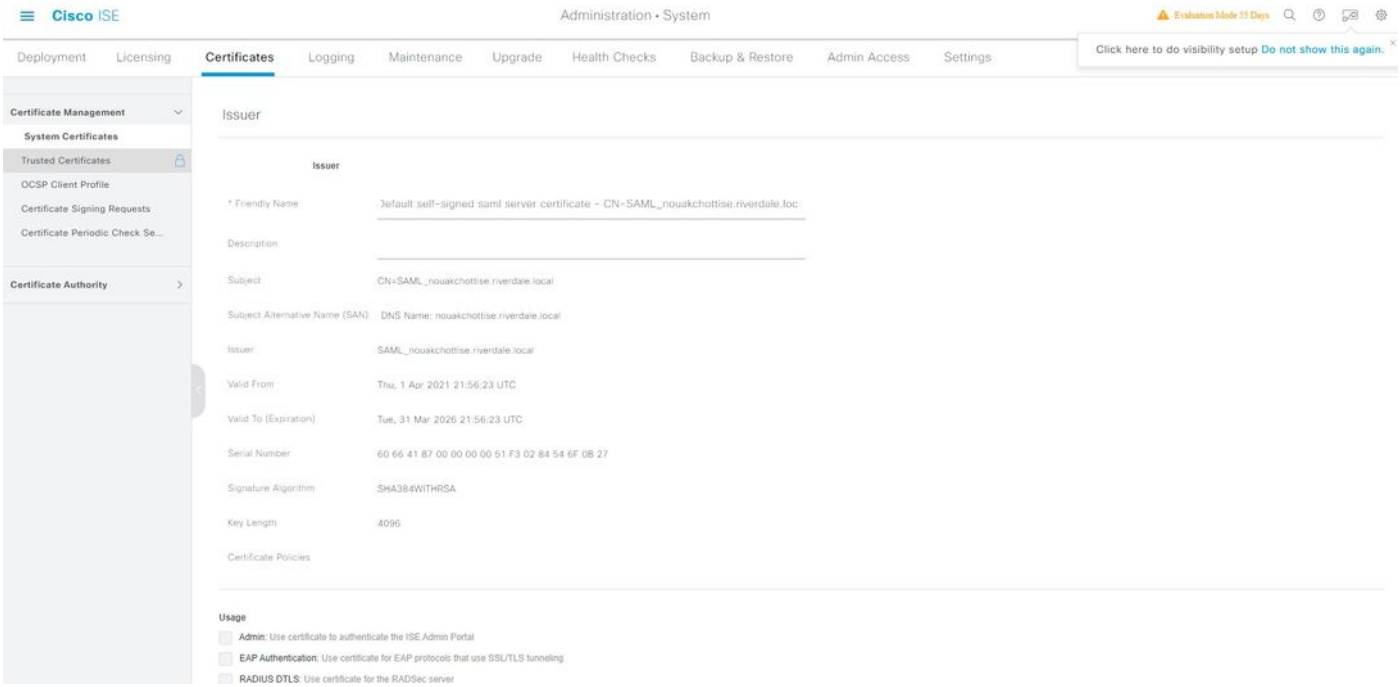
Het SAML-certificaat in ISE wordt bepaald door te zoeken naar systeemcertificaten met de SAML-vermelding in het veld Gebruiksrechtovereenkomst. Dit certificaat zal worden gebruikt om te communiceren met de identificatieaanbieders van SAML (IDP), zoals te controleren of de SAML-

antwoorden van de juiste IDP worden ontvangen en om communicatie met de IDP te waarborgen. Opmerking: voor SAML-gebruik bestemde certificaten kunnen niet worden gebruikt voor andere diensten zoals Admin, EAP-verificatie enzovoort.



Voor het eerst dat ISE-installaties worden geïnstalleerd, heeft ISE een eigen SAML server certificaat met deze eigenschappen:

Sleutelgrootte: 2048
Geldigheid: één jaar
Gebruik in hoofdzaak: Digitale handtekeningen (signalering)
Uitgebreid gebruik: TLS-webserververificatie (1.3.6.1.5.7.3.1)



Opmerking: Aanbevolen wordt om geen certificaat te gebruiken dat de waarde van 2.5.29.37.0 bevat voor de Any Purpose Object identifier in de eigenschap Extended Key Gebruik. Als u een certificaat gebruikt dat de waarde van 2.5.29.37.0 bevat voor de Any Purpose Object identifier in de eigenschap Extended Key Gebruik, wordt het certificaat ongeldig verklaard en wordt de volgende foutmelding weergegeven: "source=local ;

type=fatal ; bericht="unSUPPORT certificaat".

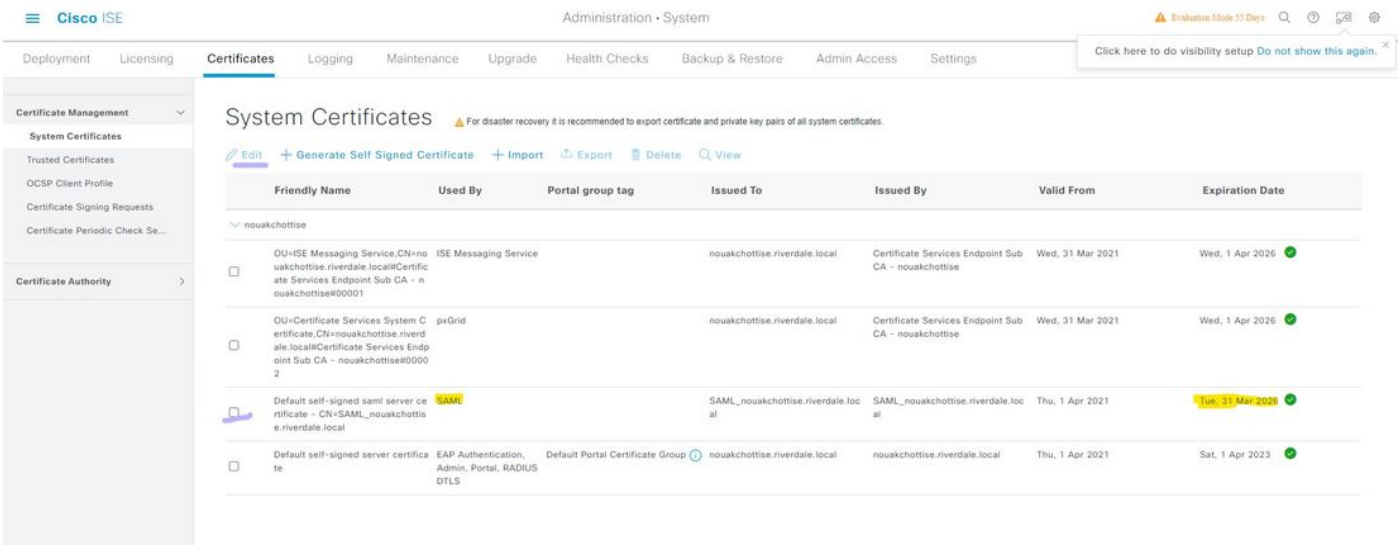
ISE-beheerders zullen dit zelf ondertekende SAML-certificaat moeten vernieuwen vóór het verstrijken, zelfs als de SAML-functie niet actief wordt gebruikt.

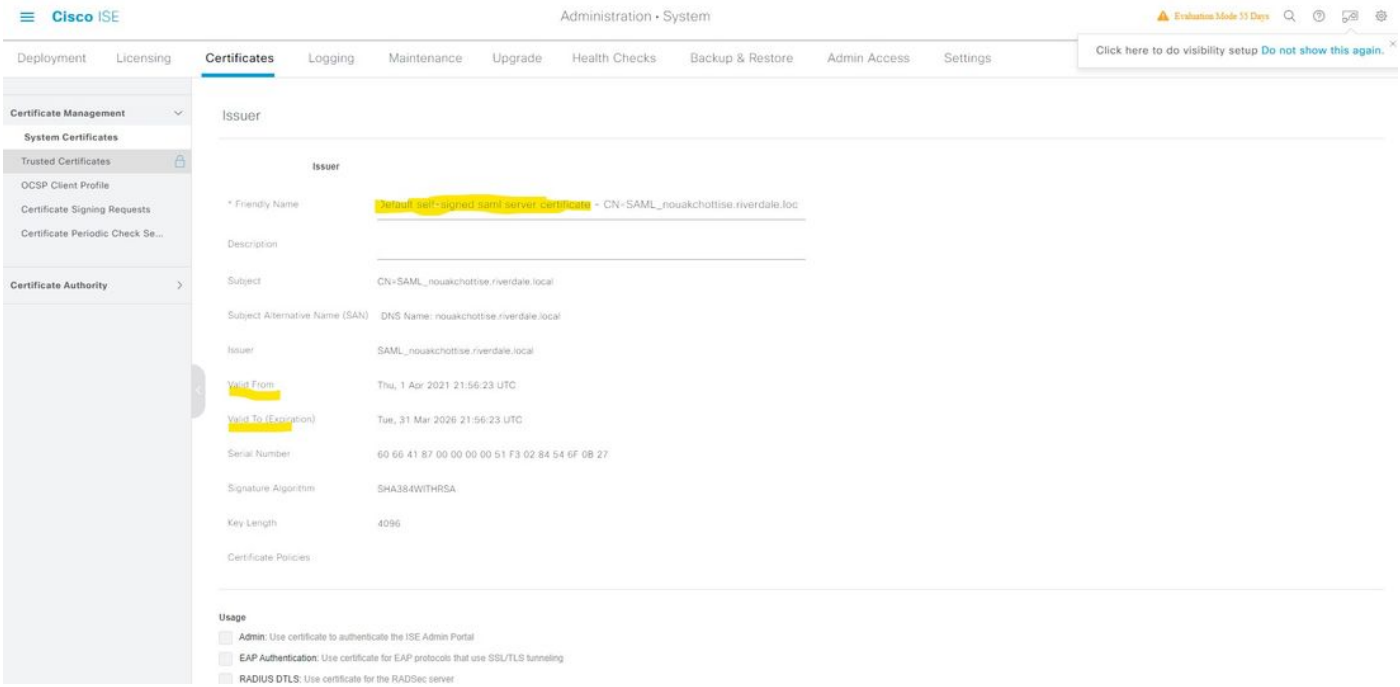
Verleng een zelf-ondertekend SAML-certificaat in ISE

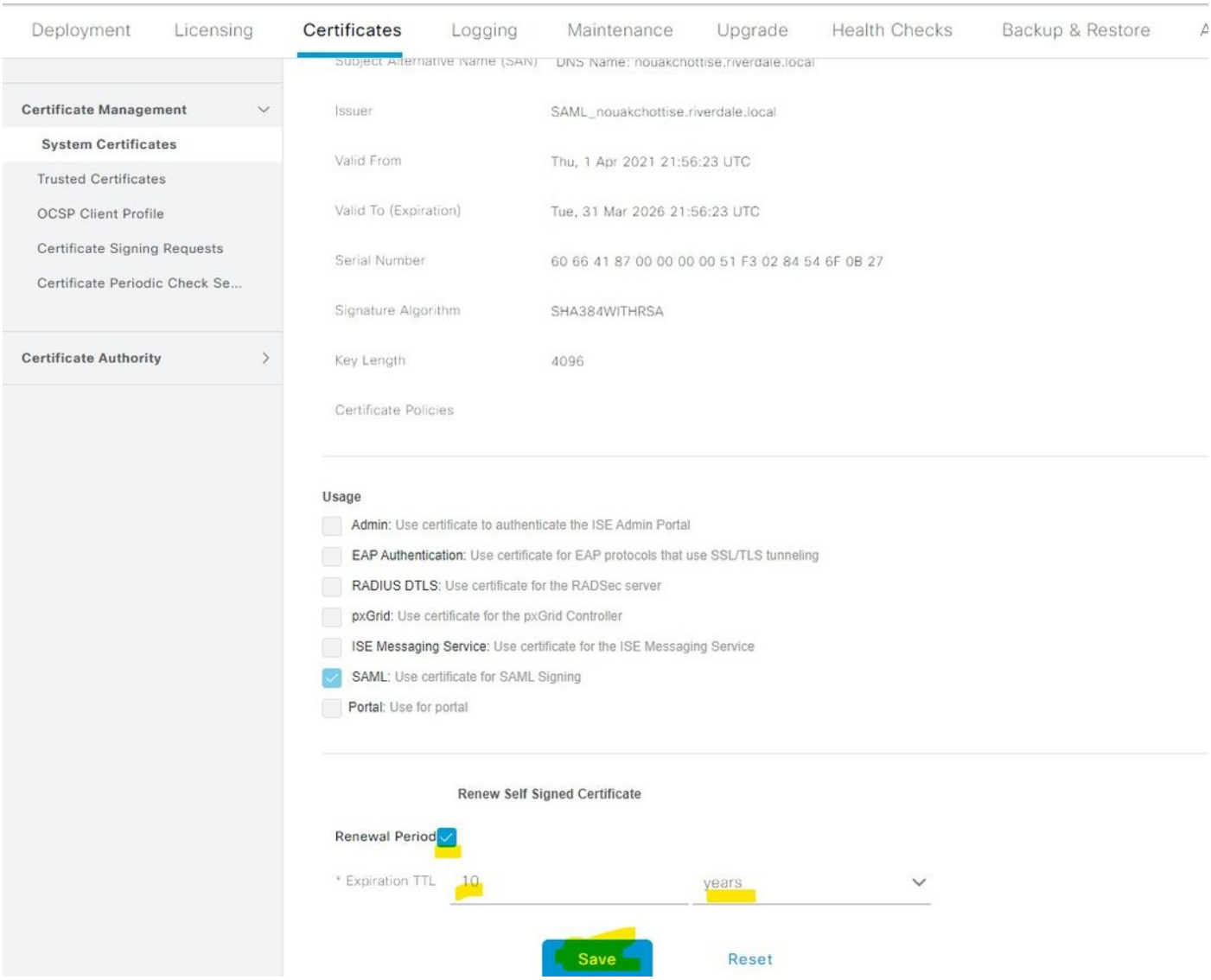
Een veelvoorkomend probleem waarmee gebruikers te maken hebben, is dat hun SAML certificaten uiteindelijk verlopen zijn en ISE waarschuwt hen met dit bericht:

```
Alarm Name :
Certificate Expiration

Details :
Trust certificate 'Default self-signed server certificate' will expire in 60 days :
Server=Kolkata-ISE-001

Description :
This certificate will expire soon. When it expires, ISE may fail when attempting to establish
secure communications with clients. Inter-node communication may also be affected

Severity :
Warning

Suggested Actions :
Replace the certificate. For a trust certificate, contact the issuing Certificate Authority
(CA). For a CA-signed local certificate, generate a CSR and have the CA create a new
certificate. For a self-signed local certificate, use ISE to extend the expiration date. You can
just delete the certificate if it is no longer used.
```

Voor zichzelf ondertekende servercertificaten is het mogelijk het certificaat te vernieuwen enkel om de verloopperiode van het vak te controleren en 5-10 jaar in te stellen zoals in de afbeelding wordt getoond.







In feite kan elk zelfondertekend certificaat dat niet actief wordt gebruikt door uw ISE-implementatieknooppunten, eenvoudig voor een periode van 10 jaar worden verlengd; Dit waarborgt dat u geen verloopberichten voor certificaten voor de services ontvangt die u niet

gebruikt. 10 jaar is de maximale toegestane levensduur voor ISE-certificaten, en zou meestal voldoende moeten zijn. Het actualiseren van systeemcertificaten op ISE leidt niet tot het opnieuw opstarten van diensten zolang deze niet zijn aangewezen voor "Admin"-gebruik.

Conclusie

Voor elk verlopen ISE-systeemcertificaat (zelf-ondertekend en CA-ondertekend) dat niet in gebruik is, is het ok om het te vervangen, te verwijderen of te vernieuwen, en het wordt aanbevolen om geen verlopen certificaten (Systeem of Vertrouwd) te hebben verlaten op ISE voordat u een ISE-upgrade uitvoert.

Gerelateerde informatie

- ISE 3.0 Certificaten beheren: Administrator Guide van Cisco Identity Services Engine, release 3.0 - basis voor setup [Cisco Identity Services Engine] - Cisco
- SSL-certificaten in ISE: TLS/SSL-certificaten in ISE - Cisco
- Technische ondersteuning en documentatie – Cisco Systems