Installatie, vernieuwing en probleemoplossing van SSL digitale certificaten op Cisco ISE

Inleiding

Dit document bevat de benodigde stappen voor SSL-certificeringsinstallatie, -vernieuwing en -oplossingen voor de meeste gebruikelijke certificeringsproblemen die worden waargenomen op een Identity Services Engine. Dit document bevat de aanbevolen stappen en de controlelijst van gebruikelijke problemen die moeten worden geverifieerd en aangepakt voordat u begint met het oplossen van problemen en Cisco Technical Support belt.

Deze oplossingen komen direct van serviceaanvragen die de technische ondersteuning van Cisco heeft opgelost. Als uw netwerk actief is, zorg er dan voor dat u de mogelijke impact begrijpt van de stappen die u neemt om de problemen aan te pakken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- GUI voor Identity Services Engine

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversie:

- Cisco Identity Services Engine 2.7

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 begrijpt.

Achtergrondinformatie

Een certificaat is een elektronisch document dat een individu, een server, een bedrijf of een andere entiteit identificeert en die entiteit met een openbare sleutel associeert. Een ondertekend certificaat wordt door zijn eigen schepper ondertekend. Certificaten kunnen zelf worden ondertekend of digitaal worden ondertekend door een externe certificaatinstantie (CA). Een door CA ondertekend digitaal certificaat wordt beschouwd als een industriestandaard en veiliger.

Certificaten worden in een netwerk gebruikt om veilige toegang te verschaffen. Cisco ISE gebruikt certificaten voor communicatie tussen knooppunten en voor het communiceren met externe servers zoals de systeemserver, voedingsserver en alle portals van de eindgebruiker (gast,

sponsor en persoonlijke apparaten portals). Certificaten identificeren een Cisco ISE-knooppunt voor een eindpunt en beveiligen de communicatie tussen dat eindpunt en het Cisco ISE-knooppunt. Er worden certificaten gebruikt voor alle HTTPS-communicatie en de MAP-communicatie (Extensible Verification Protocol).

Configureren

In de volgende gidsen wordt uitgelegd hoe u certificaten invoert en vervangt:

Invoercertificaat

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

Een verlopen certificaat vervangen

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

Veelvoorkomende problemen

Scenario 1: kan een verloopportal voor een ISE-knooppunt niet vervangen

Fout

Terwijl het nieuwe Portal certificaatcertificaat met de CSR is gebonden, verandert het certificaat niet in de onderstaande fout:

Interne fout. Vraag uw ISE-beheerder om de logbestanden te controleren voor meer informatie

De meest voorkomende redenen voor deze fout zijn:

- Het nieuwe certificaat heeft dezelfde naam als het bestaande certificaat

- Voer een nieuw certificaat in waarbij gebruik wordt gemaakt van dezelfde privésleutel van een bestaand certificaat

Oplossing

1. Wijs tijdelijk het poortgebruik aan een ander certificaat op hetzelfde knooppunt toe
2. Verwijdert het verloopportal-certificaat
3. Installeer het nieuwe Portalecertificaat en verdeel vervolgens de portal-gebruik

Als u bijvoorbeeld tijdelijk het poortgebruik aan een bestaand certificaat wilt toewijzen met behulp van EAP-verificatie, volgt u de volgende stappen:

Stap 1 . Selecteer en Bewerk het certificaat met EAP-verificatiegebruik, voeg een portal toe onder Gebruik en bewaar het certificaat

Stap 2. Verwijdert het verloopcertificaat

Stap 3. Upload het nieuwe Portal, zonder enige rol (onder Gebruik) te selecteren en in te dienen

Stap 4. Selecteer en Bewerk het nieuwe Portal certificaatformulier, wijzig Portal rol onder Gebruik en slaat deze op

Scenario 2: Kan geen twee CSR voor hetzelfde ISE-knooppunt genereren met gebruik op meerdere manieren

Fout

Nieuwe CSR-creatie voor hetzelfde knooppunt met gebruik voor meerdere gebruikers levert de fout niet op:
Er is al een ander certificaat met dezelfde vriendelijke naam. Vriendelijke namen moeten uniek zijn.

Oplossing

De namen van de Vriendelijk van CSR zijn hard-gecodeerd voor elk ISE-knooppunt, zodat er geen 2 CSR's kunnen worden gemaakt voor hetzelfde knooppunt met gebruik op meerdere apparaten. Het gebruiksgeval is op een specifiek knooppunt, er is één door CA ondertekend certificaat dat wordt gebruikt voor gebruik van Admin en EAP authenticatie en een ander door CA ondertekend certificaat dat wordt gebruikt voor SAML en Portal gebruik en beide certificaten zullen verlopen.

In dit scenario:

Stap 1. Maken van eerste CSR met meervoudig gebruik

Stap 2. Bind het door CA ondertekende certificaat met eerste CSR en verdeel de Admin- en EAP-verificatierol

Stap 3. Een tweede CSR genereren met gebruik op meerdere manieren

Stap 4. Bind het CA-ondertekend certificaat met tweede CSR en wijs SAML en Portal rol toe

Scenario 3: Kan het door CA ondertekende certificaat voor poortgebruik niet binden of de portal tag aan het certificaat toewijzen en een fout verkrijgen

Fout

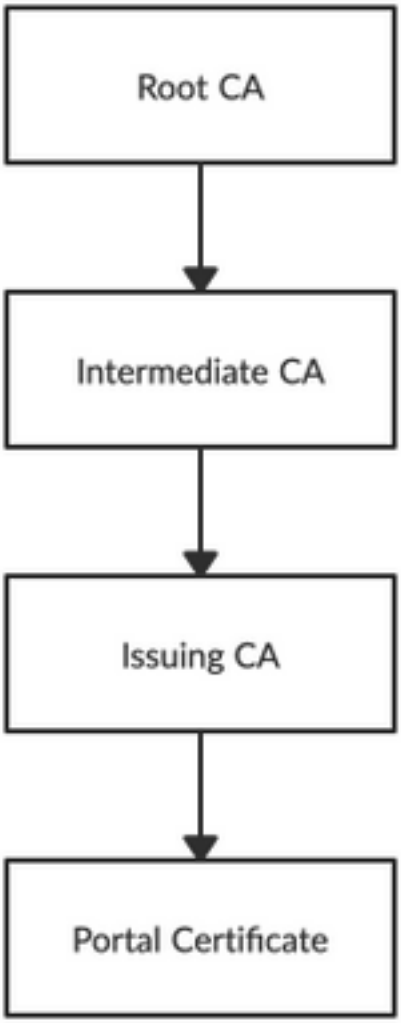
Een bindend CA-ondertekend certificaat voor poortgebruik maakt de fout:

Er is een of meer vertrouwde certificaten die deel uitmaken van de poortsysteemcertificeringsketen of zijn geselecteerd met bepaalde, op admin auth gebaseerde rol met dezelfde onderwerpnaam maar een ander serienummer hebben. Import/update werd afgebroken. Voor een geslaagde invoer/update moet u de op kar gebaseerde Admin auth rol van een duplicaat vertrouwd certificaat uitschakelen of de portal rol wijzigen van het systeemcertificaat dat het dubbele vertrouwde certificaat in de keten bevat.

Oplossing

Stap 1. Controleer de certificeringsketen van het door CA ondertekende certificaat (voor poortgebruik) en in de winkel Trusted Certificates, of u dubbele certificaten uit de certificeringsketen hebt.
Stap 2. Verwijder het duplicaat certificaat of uncheck het selectieteken **Vertrouwen voor op certificaat gebaseerde verificatie van de beheerder** uit het duplicaat certificaat.

Het door CA ondertekende poortcertificaat heeft bijvoorbeeld de volgende certificeringsketen:



Controleer of u een duplicaat certificaat hebt voor een van de 3 CA-certificaten in de certificeringsketen (dit kan een verlopen certificaat zijn) en verwijder het dubbele certificaat in de winkel Trusted Certificates.

Scenario 4: Kan het verlopen standaard zelfgetekende certificaat niet verwijderen uit de Trusted certificaatwinkel

Fout

Het verlopen standaard zelfgetekende certificaat verwijderen uit de Trusted certificaatwinkel leidt tot de fout:
Schakel uit of Verwijderen of Vertrouwingscertificaat is niet toegestaan omdat hiermee verwezen

wordt door ofwel het systeemcertificaat en/of het beveiligde Syslog-doel in het kader van de afstandsbediening.

Oplossing

1. Controleer dat het verlopen standaard zelf-getekende certificaat niet is gekoppeld aan een bestaand extern vastlegging doel. Dit kan worden geverifieerd onder ***Beheer > Systeem > Vastlegging > Afstandsdoelstellingen > Selecteren en bewerken SecureStarCollector(s)***
2. Controleer dat het verlopen zelfgetekende certificaat niet is geassocieerd met een specifieke rol (gebruik). Dit kan worden geverifieerd onder ***Administratie > Systeem > Certificaten > Systeemcertificaten***.

Neem contact op met TAC als het probleem zich blijft voordoen.

Scenario 5: Kan CA-ondertekend PxGrid-certificaat niet met CSR op een ISE-knooppunt verbinden

Fout

Terwijl het nieuwe PxGrid-certificaat met de CSR wordt gebonden, mislukt het certificaat-bindingsproces met fout:

Het certificaat voor pxGrid moet zowel client- als serververificatie bevatten in de uitgebreide Key Use (EKU)-uitbreiding.

Oplossing

Zorg ervoor dat het door CA ondertekende PxGrid-certificaat zowel voor TLS Web Server Verificatie (1.3.6.1.5.7.3.1) als voor TLS Web Client Verificatie (1.3.6.1.5.5.7.3.2) uitgebreid gebruik moet hebben omdat dit voor zowel client- als serververificatie wordt gebruikt (om communicatie tussen de PxGrid-client en server te beveiligen)

Referentielink: 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

Scenario 6: Kan het verlopen standaard zelfgetekende certificaat niet verwijderen uit de Trusted certificaatwinkel vanwege bestaande configuratie van LDAP of SCEP RA Profile

Fout

Het verlopen standaard zelfgetekende certificaat verwijderen uit de Trusted certificaatwinkel leidt tot de fout:

Trustcertificaat kan niet worden verwijderd omdat het elders wordt genoemd, mogelijk vanuit een SCEP RA-profiel of een LDAP-identiteitsbron

* Standaardservercertificaat met eigen naam

Verwijder het SCEP RA-profiel of bewerk de LDAP-identiteitsbron om dit certificaat niet te gebruiken.

Oplossing

1. Navigeren in naar ***Administratie > identiteitsbeheer > Externe identiteitsbronnen > LDAP > servernaam > Verbinding***
2. Zorg ervoor dat de LBP Server Root CA niet het "Standaard zichzelf getekende servercertificaat" gebruikt
3. Als LDAP-server niet het vereiste certificaat voor een beveiligde verbinding gebruikt, navigeer dan naar ***Administratie > Systeem > Certificaten > Certificaat Autoriteit > Externe CA-instellingen > SCEP RA-profielen***
4. Controleer of een van de SCEP RA-profielen geen standaard, zelf-ondertekend certificaat gebruikt

Aanvullende bronnen

Een jokerteken installeren
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

ISE-certificaten beheren
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

Installeer een CA-certificaat van derden op 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