Cisco IOS XE en GuestShell CA Trust Mudhra Wantrouwgids

Inhoud

Doel

Dit document biedt richtlijnen voor Cisco IOS® XE voor het wantrouwen van eMudhra Root en Intermediate Certificate Authorities in noodgevallen.

Gebruik deze handleiding om CA-vertrouwen te controleren en te beheren voor services waarvan de configuratie de betreffende hiërarchieën mogelijk maakt. De toepasbaarheid van het product en de vereiste probleemoplossing worden gedefinieerd in de Cisco-informatie. Controleer de opdrachtondersteuning en de impact van de service voor uw Cisco IOS XE-release voordat u het vertrouwen wijzigt.

Cisco-informatie: cisco-sa-emudhra-info-ScS22A1r

Getroffen Mudhra CA-certificaten: origineel en kruisondertekend

Voorraad geverifieerd op 29 oktober 2026. Acht eMudhra-licentiesleutels worden beïnvloed: zes voor TLS en twee voor codeondertekening. Elke sleutel wordt weergegeven in een origineel door emSign uitgegeven CA-certificaat en een door Sectigo ondertekend CA-certificaat. De inventaris bevat dus 16 certificaten: 12 TLS en 4 code-signing certificaten.

Elk origineel/kruisondertekend paar heeft hetzelfde onderwerp en dezelfde publieke sleutel, maar een andere emittent, serienummer en SHA-256 certificaat vingerafdruk. De twee formulieren bieden alternatieve certificeringstrajecten en moeten beide in een audit worden opgenomen.

A. Emittenten en de desbetreffende inventaris van certificaten

Emittent A — Originele TLS-certificaten: CN=emSign Root TLS CA - G3, O=Mudhra Technologies Limited, C=IN.

Uitgever B — Oorspronkelijke codeondertekeningscertificaten: CN=emSign Root CS CA - G3, O=Mudhra Technologies Limited, C=IN.

Emittent C — Alle kruisondertekende certificaten: CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB (Sectigo).

G3B proefpersonen: O=Mudhra BV, C=NL. G3C-proefpersonen: O=Mudhra Inc, C=US. Elke variantcel vermeldt de referentie van de emittent, hexadecimale seriële en SHA-256-vingerafdruk (twee regels). Het leiden van zero padding verandert geen seriële waarde.

Betrokken CA (CN) van afgifte	Oorspronkelijk certificaat Emittent / serial (hex) / SHA-256	Sectigo kruisondertekend certificaat Emittent / serial (hex) / SHA-256
1. EM DV TLS CA - G3B TLS	Emittent A A4AEE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	Emittent C A024FDF4BA665C785CE4A02048385 45A883F349AEDFD5F3A649B5498FF 1712BA8B448F3F2A91DBC5A766FCD
2. EM OV TLS CA - G3B TLS	Emittent A 6CADA367FB1C100088120EA202D568 98B896625C0C230ADEEC3EB2CF6AAD50 01ECF9156A68644E82374CE5833BC25B	Emittent C E94223BDE92F914E5AB9ACABFDAC 5F1DED4DD590AF74631290CF073B1 2AAC6A1FA479778A0BD43579BD832
3. EM EV TLS CA - G3B TLS	Emittent A C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C7559D 0F8EB192A218D4741A3BA75184333838	Emittent C D8F8685E4F2BD9D82402A85A1C1EB 579480AEA166290BD3C643589E795F D0E54E86505D180F1DFF99EFD3199
4. EM DV TLS CA - G3C TLS	Emittent A 588B2E3C2BB8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	Emittent C 91F347F1A5B7D39962B95E0EE4E299 62B7F9868263F72F6911FC78CEAF72 979158B7368BF648683BB2AA39B02E
5. EM OV TLS CA - G3C	Emittent A	Emittent C

Betrokken CA (CN) van afgifte	Oorspronkelijk certificaat Emittent / serial (hex) / SHA-256	Sectigo kruisondertekend certificaat Emittent / serial (hex) / SHA-256
TLS	296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F993F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	8D5A4811939EF447D77111CDD9849A 7485B51C0ED192878FA1D2F948FB52 E1842CC5086C4B67F7BE5B2039DE94
6. EM EV TLS CA - G3C TLS	Emittent A 8009928A64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2CD41F669933FCB072D9A1148D0261F3	Emittent C 05F078752DECE7A1BB8595D3031671 FD9D5C2DBBD4995AB69B8D50C439D 7B00529199C2FD01B2174EB58F0702
7. EM OV CS CA - G3B Codeondertekening	Emittent B 7818933F8F85B4619A2B35FBA83D0A 9E39DE2881273ACC225A149C72BA3E0F 51424963669AB633EE1DC7DF5DB067B4	Emittent C 41E32B73AC185D6CE0D7480BACF84 A496E23AC0CAB8155FC9B117B97EA 8EFCBB9041AEC8804D5A308D2D01C
8. EM OV CS CA - G3C Codeondertekening	Emittent B 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCCA2CEB29 B3B093921DE45474DA7DF48874C630B1	Emittent C D6A5EF613B390F32EF9CDF349F7728 84112972B8E59D14560AE7E7119654 4AAD119990CF3722BFC1E3B91615E1

B. Certificeringstrajecten om te onderscheiden

Oorspronkelijk TLS-pad

```
emSign ECC Root CA - G3
  +-- emSign Root TLS CA - G3 (issued by emSign ECC Root CA - G3)
       +-- Original EM DV/OV/EV TLS CA - G3B or G3C
            +-- TLS identity certificate
```

Oorspronkelijk pad voor codeondertekening (root CS direct vertrouwd)

```
emSign Root CS CA - G3
  +-- Original EM OV CS CA - G3B or G3C
       +-- Code-signing identity certificate
```

Sectigo cross-signed path (TLS en code signeren)

```
AAA Certificate Services
  +-- One of the eight cross-signed CAs listed above
       +-- TLS or code-signing identity certificate
```

Een TLS-pad kan ook worden beëindigd bij emSign Root TLS CA - G3 wanneer die CA rechtstreeks wordt vertrouwd. De diagrammen tonen relevante emittentrelaties; het geaccepteerde pad is afhankelijk van de vertrouwensankers en het validatiebeleid van de verbruikende dienst.

De bovenliggende/onderliggende CA's die in het voorbeeld worden getoond, bieden ketencontext en worden niet gerekend tot de acht gecompromitteerde emissiesleutels. Een beslissing om een ouder/root te verwijderen of te wantrouwen staat los van het identificeren van een gecompromitteerde tussensleutel.

Gebruik voor de identificatie het certificaatnummer en het serienummer samen met de SHA-256-vingerafdruk. Een onderwerpnaam alleen is onvoldoende. Een certificaat vingerafdruk identificeert één certificaat variant; een SPKI SHA-256 hash identificeert de publieke sleutel gedeeld door de originele en cross-signed formulieren. Het verwijderen van alleen een in de cache opgeslagen tussenproduct voorkomt niet dat een peer het via een resterende vertrouwde pad presenteert.

Bronnen en controledatum

Certificaatidentificatoren werden op 29 oktober 2026 geverifieerd aan de hand van de bijlagen bij openbare incidenten. Elk origineel/kruisondertekend paar bevat dezelfde publieke sleutel. Gebruik de live Cisco-informatie voor producttoepasbaarheid en herstelstatus.

Cisco-informatie: cisco-sa-emudhra-info-ScS22A1r

Mozilla incident record: eMudhra intermediate key compromis (2083449)

Originele CA-certificaatbijlage (9664066)

AAA-kruisondertekende CA-certificaatbijlage (9664067)

Apple: originele en kruisondertekende TLS-certificaatpaden en vingerafdrukken

Met ingang van 31 oktober 2026 wordt emSign Root CA - G1 niet geïdentificeerd onder de gecompromitteerde CA's die in deze handleiding worden vermeld. Het voortdurende vertrouwen blijft onderhevig aan uw organisatiebeleid en daaropvolgende adviserende updates.

Hoe Cisco IOS XE Certificate Trust beheert

Geconfigureerde PKI-trustpoints zijn in het bezit van CA-/identiteitscertificaten en validatiebeleid. De PKI-trustpool bevat ingebouwde en gedownloade CA-certificaten voor services die deze gebruiken. Identificeer de vertrouwensbron en het beleid dat door elke relevante service wordt gebruikt; het wijzigen van de vertrouwensgroep vervangt niet afzonderlijk geconfigureerde vertrouwensrelaties.

1. Controle en voorbereiding

Controleer de softwarerelease, de tijd van het apparaat en de geïnstalleerde certificaten:

<#root>

```
show version show clock show crypto pki trustpoints show running-config | section crypto pki trustpoint
```

Vergelijk het volledige certificaat Emittent en het hexadecimale serienummer met de inventaris, waarbij het onderwerp als ondersteunende context wordt gebruikt. Wanneer Cisco IOS XE alleen MD5- en SHA1-vingerafdrukken weergeeft, kan de SHA-256-vingerafdruk van de inventaris niet rechtstreeks in die uitvoer worden vergeleken; deze wordt geleverd voor verificatie van certificaatbestanden buiten het apparaat. Toonaangevende 00 padding in serienummers kan verschillen. Zoekopdrachten met leveranciersnamen identificeren alleen kandidaten. Noteer de services die afhankelijk zijn van elk vertrouwenspunt en controleer zowel originele als ondertekende paden, inclusief direct vertrouwde tussenpersonen.

Voorbeelden: root CA en getroffen SubCA

Er worden verkorte voorbeelden van het uitgebreide certificaat weergegeven; andere velden worden weggelaten. Vergelijk het onderwerp, de uitgever en het serienummer.

Voorbeeld CA-hoofdmap: emSign ECC-hoofdmap CA - G3

```
CA Certificate
  Certificate Serial Number (hex): 3CF607A968700EDA8B84
  Issuer:
    cn=emSign ECC Root CA - G3
  Subject:
    cn=emSign ECC Root CA - G3
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Voorbeeld van getroffen subCA: origineel door emSign afgegeven certificaat

```
CA Certificate
  Certificate Serial Number (hex): 00A4AEE678F23362B4C0E460B772F214
  Issuer:
    cn=emSign Root TLS CA - G3
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Voorbeeld van getroffen subca: kruisondertekend certificaat van Sectigo

```
CA Certificate
  Certificate Serial Number (hex): 00A024FDF4BA665C785CE4A020483858B7
  Issuer:
    cn=AAA Certificate Services
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Beide SubCA-formulieren hebben hetzelfde onderwerp, maar verschillende emittenten en serials. Match de volledige emittent en seriële aan de inventaris; toonaangevende 00 padding kan verschillen. Noteer de bijbehorende Trustpoints om de eigenaar van het trustpoint of de pool te vinden. De getoonde wortel is kettingcontext; het is niet een van de acht gecompromitteerde uitgiftesleutels.

Houd een hersteltoegangsmethode en een goedgekeurde vervangingsbundel beschikbaar. Gebruik waar nodig de goedgekeurde back-upprocedure voor certificaten/sleutels. Maak een back-up van de configuratie; dit exemplaar alleen is geen back-up met privésleutel:

<#root>

```
copy running-config <BACKUP-CONFIG-URL>
```

Plaatsaanduidingen met haakse beugels vervangen door goedgekeurde apparaatspecifieke waarden. Gebruik een bestandssysteem dat wordt weergegeven door weergavebestandssystemen, zoals flash: of bootflash:.

2. Trustpaden controleren

Verwijder direct vertrouwde subbevoegde instanties

Verwijder direct vertrouwde subCA's van trustpoints en gedownloade trustpool-bundels. Vertrouw niet op herroepingsinstellingen om het directe vertrouwen in een gecompromitteerde CA te ondermijnen.

Optionele verwijdering van root-CA

Root CA verwijdering is een optionele aanbeveling voor extra bescherming. Een vereiste hoofdmap kan betrouwbaar blijven wanneer de werkelijke CRL/OCSP-controles van de service de huidige status verkrijgen, de getroffen submap evalueren onder een betrouwbare bovenliggende instantie, de getroffen originele, ondertekende en toepasselijke langere ketens weigeren en de validatie mislukken als geen van de geconfigureerde methoden de bruikbare status biedt. Onder deze geverifieerde voorwaarden beschermt de herroepingscontrole tegen de geïdentificeerde gecompromitteerde emittenten zonder de root te verwijderen.

Overweeg het verwijderen van onnodige root / trust ankers om de afhankelijkheid van herroepingsdiensten te verminderen. Beoordeel eerst de afhankelijkheden van de service: het verwijderen van AAA-certificaatservices kan niet-gerelateerde legitieme ketens onderbreken. Bedek zowel eMudhra- als AAA-paden. Het verwijderen van alleen een subCA in de cache blokkeert geen door gelijken geleverde kopie via een resterende vertrouwde ouder.

Een geselecteerd vertrouwenspunt verwijderen

Voor een door de beheerder geconfigureerd vertrouwenspunt dat is geselecteerd voor verwijdering:

<#root>

```
configure terminal no crypto pki trustpoint <TRUSTPOINT-NAME> end
```

Controleer de bevestiging voordat u deze accepteert. Trustpoint-verwijdering vernietigt de bijbehorende certificaten. Als de identiteit van een apparaat moet worden vervangen, verkrijgt u een vervangend certificaat dat overeenkomt met de apparaatsleutel en werkt u de servicebinding bij met behulp van de inschrijvingsprocedure voor de service. Het installeren van een nieuw CA-certificaat alleen vervangt de apparaatidentiteit niet.

Gebruik voor gedownloade trustpool-vermeldingen de procedure voor het vervangen van bundels. Ingebouwde of door functies beheerde ankers vereisen de ondersteunde productupdate of Cisco TAC-richtlijnen.

3. Werk de gedownloade Trustpool bij, indien nodig

Gebruik deze stappen wanneer een gedownloade bundel moet worden vervangen. Een vereiste ouder/root kan vertrouwd blijven onder de geverifieerde herroepingsvoorwaarden in stap 2.

3.1 Controleer of een gedownloade bundel is geïnstalleerd en gebruikt

<#root>

```
show running-config | section crypto pki certificate pool show crypto pki trustpool verbose show crypto
```

Zoek naar bundel vermeldingen onder crypto pki certificaat pool en CA records gemarkeerd Trustpool: Gedownload. Bundelbestandsnamen kunnen verschillen van ios.p7b of ios_core.p7b. Een opgeslagen bestand of een geconfigureerde URL voor het vernieuwen alleen bewijst niet dat de certificaten worden geïnstalleerd of gebruikt door een service. Bevestig dat de service gebruikmaakt van de vertrouwensgroep en vergelijk de CA-records met de betreffende inventaris. Als er geen gedownloade CA's zijn geïnstalleerd, slaat u het opruimen en vervangen over; beoordeelt u nog steeds andere vertrouwensbronnen.

3.2 Reinig de gedownloade vertrouwenspool

Houd hersteltoegang en een goedgekeurde herstelbundel beschikbaar voordat u deze opruimt. Downloaden achteraf kan mislukken als de overdracht afhankelijk is van het vertrouwen dat wordt verwijderd. Plan voor onderbreking van afhankelijke diensten.

<#root>

```
configure terminal crypto pki trustpool clean end
```

```
show crypto pki trustpool verbose
```

Bevestig dat gedownloade CA-records zijn verdwenen. Cleanup verwijdert alle gedownloade trustpool-certificaten en hun beheerde bundelbestanden; ingebouwde CA's en afzonderlijke trustpoints blijven bestaan. Sla niet op totdat de vervanging en servicecontroles succesvol zijn.

3.3 De goedgekeurde vervangingsbundel verkrijgen en installeren

Zorg voor een goedgekeurde Cisco-ondertekende bundel. Selecteer ios.p7b of ios_core.p7b voor de vereiste services en bevestig dat de betrokken certificaten en ongewenste vertrouwensankers die hierboven zijn geïdentificeerd, zijn uitgesloten. De oudere bundels die op 31 oktober 2026 zijn gecontroleerd, bevatten emSign Root CA - G1 in ios.p7b, maar noch eMudhra- noch AAA Certificate Services CA's in ios_core.p7b. Core heeft een kleinere vertrouwensset: controleer de afhankelijkheid van de service voordat u overschakelt en controleer de inhoud van de bundel die u installeert. Stage it buiten beheerde trustpool-opslag met behulp van goedgekeurde HTTPS- of SCP-overdracht.

Cisco volledige CA-bundel: ios.p7b

Cisco Core CA-bundel: ios_core.p7b

<#root>

```
show file systems copy <APPROVED-BUNDLE-SOURCE-URL> <STAGED-BUNDLE-URL> configure terminal crypto pki tr
```

De gefaseerde URL kan bijvoorbeeld flash zijn: approved-ios.p7b. Als het importeren mislukt, zet u een goedgekeurde bundel terug voordat u deze opslaat. Controleer de beoogde CA's en de vereiste verbindingen. Opschonen is geen certificaatontkenner: controleer de resterende vertrouwensrelaties, ingebouwde CA's en alternatieve paden die de getroffen ketens afwijzen door middel van gedwongen intrekking of verwijdering van vertrouwenspaden.

4. Validatie- en vernieuwingsbeleid configureren

Voordat u wijzigingen aanbrengt, noteert u het bestaande trustpool-beleid, het getroffen trustpoint-

beleid, bindingen voor certificaten en vernieuwde URL's, zodat deze indien nodig kunnen worden hersteld.

Voor relevante geconfigureerde vertrouwenspunten:

<#root>

```
configure terminal crypto pki trustpoint <VALIDATION-TRUSTPOINT> revocation-check crl ocsp exit end
```

Voor services die gebruikmaken van het trustpool-beleid:

<#root>

```
configure terminal crypto pki trustpool policy chain-validation revocation-check crl ocsp exit end show
```

Controleer of het weergegeven vertrouwensgroepbeleid de validatie naar de hoofdmap en lijsten met clocsp voortzet. Het apparaat probeert eerst CRL en probeert OCSP wanneer CRL-ophalen niet beschikbaar is. Een ingetrokken resultaat mislukt bij validatie wanneer het betreffende certificaat wordt geëvalueerd. Voeg er geen toe wanneer een succesvolle herroepingscontrole vereist is.

Controleer de juiste tijd, bereikbare CA-gepubliceerde status-eindpunten, geaccepteerde responsformaten en het ontbreken van toepasselijke uitzonderingen voor het overslaan van herroeping. De status van de getroffen subbevoegde autoriteiten moet worden beoordeeld onder een betrouwbare ouder. Direct vertrouwen in die SubCA kan de validatie stoppen voordat de bovenliggende optie wordt gecontroleerd. Controleer of de werkelijke service bruikbare, actuele status krijgt en de getroffen ketens afwijst. Als de toegang tot de statusserver en het afwijzingsgedrag niet kunnen worden geverifieerd, moet u de configuratie niet alleen als bevestigde beveiliging behandelen; verwijder de relevante vertrouwensroutes waar dit door uw mitigatieplan wordt vereist. Voeg er geen toe om de niet-beschikbare status te omzeilen.

CRL's in de cache vernieuwen voordat de bescherming wordt gecontroleerd

Een bruikbaar CRL dat al in de lokale cache/database is opgeslagen, kan worden hergebruikt, zelfs nadat de CA een nieuwer CRL heeft gepubliceerd. Controleer de bereikbaarheid van de statusserver en wis de oude CRL's voordat u de beveiliging valideert:

<#root>

```
show crypto pki crls clear crypto pki crl show crypto pki crls
```

De duidelijke opdracht verwijdert lokale CRL's voor alle trustpoints; het downloadt zelf geen vervangingen. Bevestig dat de oude items zijn verdwenen en start vervolgens een nieuwe verbinding of certificaatvalidatie in de betreffende service. Voer de show crypto pki crls opnieuw uit en controleer elke relevante uitgever, LastUpdate, NextUpdate en distributiepunt tegen de huidige publicatie van de CA's. Neem de moederemittenten CRL op die de getroffen SubCA dekt, niet alleen de ID-certificaten die CRL uitgeven. Bevestig dat de getroffen ketens zijn afgewezen. Het wissen kan tijdelijk van invloed zijn op nieuwe verbindingen terwijl statusgegevens worden opgehaald; de failclosed-validatie behouden.

De bron voor het vernieuwen van de bundel bekijken

Configureer voor aangesloten apparaten optioneel de goedgekeurde verlengingsbron van de bundel die is gebaseerd op de vervaldatum:

<#root>

```
configure terminal crypto pki trustpool policy cabundle url <APPROVED-REFRESH-BUNDLE-URL> exit end show
```

Bekijk alle geconfigureerde bundelbronnen. Vervaldatum-gestuurde verversing vervangt geen onmiddellijke beveiligingsupdate en mag geen ongewenst vertrouwenspad herstellen.

Optioneel filter voor certificaat-kaart: dekking en beperking

Een Cisco IOS XE-certificaatkaart (cert-map) komt overeen met certificaatkenmerken, zoals de naam van de uitgever. Als extra maatregel kan het filter helpen bij het weigeren van ID-certificaten (bladcertificaten) die rechtstreeks door de acht genoemde bevoegde autoriteiten zijn afgegeven. Controleer het bestaande vertrouwensreferentiecertificaatbeleid voordat u het toepast.

Gedrag werd op 29 oktober 2026 getest met behulp van laboratoriumindentiteiten onder EM DV TLS CA - G3B op experimentele laboratoriumapparaten. In PKI peer-certificaatvalidatie wees het filter een rechtstreeks uitgegeven identiteit af, maar blokkeerde het geen identiteit die was uitgegeven via een extra subca voor kinderen; een niet-beursgenoteerde legitieme emittent is geslaagd. Gedragsdekking gebruikt één getroffen emittent, met intrekking uitgeschakeld alleen op tijdelijke lab trustpoints om het filter te isoleren. Handdrukken van toepassingen en andere

releases zijn niet gevalideerd met dit filter; test de werkelijke service voordat u erop vertrouwt.

<#root>

configure terminal crypto pki certificate map EMSIGN-ISSUER-FILTER 10 issuer-name nc cn=EM DV TLS CA - G

NC betekent hier "bevat niet". Houd alle acht negatieve voorwaarden voor de naam van de uitgevende instelling in dezelfde vermelding, reeks 10: alle moeten overeenkomen om het certificaat te laten passeren dit filter. Een directe emittent die overeenkomt met een beursgenoteerde naam faalt in het filter.

Cisco IOS XE kan genormaliseerde items weergeven, bijvoorbeeld de naam van de emittent nc cn = em dv tls ca - g3b. Deze kleine letters en spatieformaat waren aanwezig in de gedragstest. Bevestig de kaart en de binding ervan aan het validatievertrouwenspunt dat daadwerkelijk door de service wordt gebruikt:

<#root>

show running-config | section crypto pki certificate map show running-config | section crypto pki trustp

Het filter biedt geen kettingbrede CA-denylist. Voorbeeld:

```
Trusted root CA
  +-- Affected SubCA
       +-- New child SubCA
            +-- ID (leaf) certificate
```

De uitgever van ID-certificaten is de nieuwe onderliggende SubCA, dus het filter van de naam van de uitgever identificeert de betrokken CA niet hoger in de keten. Andere controles, waaronder CA-beperkingen en intrekking, zijn nog steeds van toepassing. Gebruik dit filter alleen als extra bescherming naast de herroepingsvalidatie en de optionele procedures voor het verwijderen van de wortels in deze handleiding. Test rechtstreeks afgegeven, kind-SubCA en legitieme certificaten met de werkelijke service.

Rollback van stap 4

Herstel de vastgelegde herroepingsmethoden, kettingvalidatie-instellingen en bindingen voor de certificaatmap. Verwijder de URL's die met deze procedure zijn toegevoegd en herstel alle eerdere

URL's die zijn gewijzigd. In dit voorbeeld worden alleen de toegevoegde URL voor verversen en filterbinding verwijderd. De andere beleidsinstellingen worden niet hersteld:

<#root>

```
configure terminal crypto pki trustpool policy no cabundle url <ADDED-REFRESH-BUNDLE-URL> exit
```

```
crypto pki trustpoint <VALIDATION-TRUSTPOINT> no match certificate EMSIGN-ISSUER-FILTER exit end
```

Voer deze verwijderingen alleen uit waar de URL en binding zijn toegevoegd door deze procedure. Als een eerdere binding tussen certificaten en kaarten is vervangen, moet u deze herstellen. Verwijder een nieuw gemaakte kaart pas nadat u hebt bevestigd dat er geen andere configuratie naar verwijst.

Gebruik geen crypto pki trustpool beleid alleen wanneer het herstellen van de standaard is de beoogde, goedgekeurde uitkomst. Met deze uitgebreide reset worden de geconfigureerde URL's voor het vernieuwen gewist en wordt de herroepingscontrole op geen enkele ingesteld. Het vorige aangepaste beleid wordt niet teruggezet. Beleidsterugdraaiing herstelt geen verwijderde certificaten, keert de geïnstalleerde bundel terug of herstelt geen verwijderde CRL's. Controleer de vereiste services en de afwijzing van de getroffen keten opnieuw voordat u deze opslaat.

5. Controleer de bescherming en sla op

- Bevestig dat de getroffen originele en kruisondertekende ketens worden afgewezen, inclusief een tussenproduct dat door gelijken is geleverd. Indien langere ketens relevant zijn, controleer de afwijzing wanneer de betrokken CA hoger in de keten is.
- Bevestig dat de vereiste legitieme verbindingen nog steeds werken en dat elke vervangende identiteit gebonden is aan de beoogde service.
- Gedrag controleren wanneer herroepingsgegevens niet beschikbaar zijn. Bestaande TLS-/IPsec-sessies worden niet automatisch opnieuw gevalideerd door een beleidswijziging; gebruik indien nodig de door de service ondersteunde herverbindingsprocedure.

Nadat de controles zijn geslaagd:

<#root>

```
show crypto pki certificates verbose show crypto pki trustpool policy write memory
```

Controleer de persistentie na de volgende geplande herlading en, indien van toepassing, op het standby-apparaat. Als de resultaten afwijken van het verwachte vertrouwensbeleid, behoudt u de logboeken en neemt u contact op met Cisco TAC voordat u de geverifieerde vertrouwenswijzigingen overweegt.

verdere lezing

Cisco IOS XE PKI Trustpool-beheer

Cisco: CA-ondertekende certificaten configureren met Cisco IOS XE PKI

Cisco: CRL-caching en herroepingscontrole

Cisco IOS XE GuestShell CA Trust Guide

Stap 1: Status van implementatie van GuestShell-apparaat controleren

Remediation is alleen vereist op Cisco IOS XE-systemen waar GuestShell is geïnstalleerd en in de ACTIEVE of GEÏMPLEMENTEERDE staat. Als GuestShell in de staat DEPLOYED staat, moet het eerst worden ingeschakeld met de opdracht 'guestShell enable' voordat herstelopdrachten worden uitgevoerd. Als de hostinglijst voor apps weergeven 'Geen app gevonden' aangeeft (GuestShell is niet geïmplementeerd of ingeschakeld), is er geen actie vereist op GuestShell.

A. GuestShell in GEÏMPLEMENTEERDE toestand (actie vereist: moet eerst inschakelen)

Wanneer de app-hostinglijst weergeven GuestShell in de GEÏMPLEMENTEERDE staat meldt, bestaat GuestShell-containeropslag, maar wordt de container gestopt. U moet 'guestshell enable' uitvoeren voordat u bash invoert (en optioneel 'guestshell disable' na het voltooien van de sanering als u terugkeert naar een stilstaande toestand):

<#root>

```
Router#

show app-hosting list
```

```
App id                                   State
---------------------------------------------------------
guestshell                               DEPLOYED
```

B. GuestShell in RUNNING State (Actie vereist: Ga direct verder)

Wanneer de app-hostinglijst toont dat GuestShell in de ACTIEVE staat is, wordt GuestShell actief uitgevoerd en kunt u rechtstreeks naar bash gaan:

<#root>

```
Router#

show app-hosting list

App id                                   State
---------------------------------------------------------
guestshell                               RUNNING
```

B. GuestShell niet ingeschakeld / niet geïmplementeerd (geen actie vereist)

Als de hostinglijst voor apps weergeven aangeeft dat er geen app is gevonden, is GuestShell niet geïnstalleerd of ingeschakeld op het systeem en zijn er geen verdere acties vereist:

<#root>

```
Router#

show app-hosting list

No App found
```

Stap 2: Toegang krijgen tot GuestShell en CA-wantrouwen toepassen

Voer deze opdrachten uit via de Cisco IOS XE privileged EXEC ('enable') prompt. Als GuestShell is INGEZET, schakelt u deze eerst in. Voer vervolgens de bash-shell in, escaleer naar root en configureer de CA-blokkeerlijst met behulp van de dynamische mapselectie om compatibiliteit te garanderen voor alle Cisco IOS XE-releases:

<#root>

```
! 1. If GuestShell is in DEPLOYED state, enable it first:
Router#
```

```
guestshell enable
```

```
! 2. Enter GuestShell bash shell:
Router#
```

```
guestshell run bash
```

```
! 3. Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$
```

```
sudo -s
```

```
! 4. Prepare the ca-trust blocklist directory (compatible with 17.15.x and 17.18.x):
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
mkdir -p "$d"
```

Wantrouwen gecompromitteerde eMudhra certificaten

Voer de opdrachten voor het uitpakken van vertrouwen uit om elk gecompromitteerd eMudhra-certificaat rechtstreeks in de map ca-trust-blokkeerlijst te extraheren, gevolgd door het opnieuw opbouwen van de systeemvertrouwenswinkel:

```
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_G3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  "$d/Comodo_AAA_Services_root.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20C3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_C3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;type=cert' \
  "$d/emSign_Root_CA_-_C1.pem"

update-ca-trust extract
```

Stap 3: Vertrouwde certificaten verifiëren in GuestShell

Controleer of de vier geëxtraheerde certificaten worden weergegeven in het beleid voor systeemwantrouwen/blokkering en worden uitgesloten van actieve vertrouwensankers met behulp

van de onderstaande verificatieopdracht. Het commando bevestigt dat de certificaten zijn geregistreerd in het beleid van de blocklist.

```
###Verify with below command
[guestshell@guestshell ~]$ trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign
    label: AAA Certificate Services
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - G3
    trust: distrusted
    category: authority

--
    label: emSign Root CA - C1
    trust: distrusted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

Output will vary based on CentOS Stream version
###Verify CentOS Stream Version
[guestshell@guestshell ~]$ cat /etc/redhat-release
CentOS Stream release 8

OS                          CentOS Stream 8       CentOS Stream 9
Directory                   blacklist only        blocklist
Result shown                 trust: blacklisted    trust: distrusted
```

Stap 4: Persistentie en levenscyclus van de container

Opmerking over de persistentie van containers: deze wijzigingen in het certificaat blijven bestaan bij 'guestshell enable'- en 'guestshell disable'-bewerkingen en het opnieuw opstarten van het apparaat, omdat /etc/pki/ca-trust zich op een persistente containeropslag bevindt.

Terugkeren naar GEÏMPLEMENTEERDE staat (indien van toepassing): Als GuestShell oorspronkelijk in de GEÏMPLEMENTEERDE staat was en alleen in staat was om deze wantrouwprocedure uit te voeren, retourneert u GuestShell naar de vorige gestopt staat door bash te verlaten en 'guestshell disable' uit te voeren vanaf de exec-prompt met IOS-privileged:

<#root>

```
[root@guestshell ~]#

exit

[guestshell@guestshell ~]$

exit

Router#

guestshell disable
```

Belangrijke levenscyclusoverweging: als GuestShell volledig wordt vernietigd met 'guestshell destroy', wordt het containerbestandssysteem verwijderd. Als GuestShell vervolgens opnieuw wordt ingeschakeld, wordt de container opnieuw gemaakt vanaf het basissysteemimage en moeten deze stappen voor het oplossen van wantrouwen opnieuw worden toegepast.

Stap 5: Terugdraaiprocedure (CA Trust herstellen)

Als u de vertrouwensconfiguratie wilt omkeren en de standaard CA-trust wilt herstellen voor elke Cisco IOS XE-release, selecteert u dynamisch de map met actieve blokklijsten ($d), verwijdert u specifiek de vier certificaatbestanden die door deze procedure zijn toegevoegd (inclusief de hoofdmap Comodo AAA Services) en bouwt u de vertrouwenswinkel opnieuw op:

<#root>

```
! Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s


d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

! Remove only the four certificate files added during remediation:
rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \
      "$d/emSign_ECC_Root_CA_-_C3.pem" "$d/emSign_Root_CA_-_C1.pem"

! Rebuild the system CA trust store:
update-ca-trust extract
```

Controleer of de map met de blokklijst niet langer de verwijderde bestanden bevat:

<#root>

```
[root@guestshell ~]#

ls -l "$d"/

total 0
```

Bevestig CA Trust Restoration: Controleer of alle vijf certificaten zijn teruggekeerd naar actieve vertrouwensankers door de verificatieopdracht voor stap 3 opnieuw uit te voeren (alle vermeldingen melden vertrouwen: anker):

<#root>

```
[root@guestshell ~]#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
```

Voorbeeld van end-to-end transcriptie-uitvoering

Het transcript illustreert een volledige, succesvolle GuestShell-audit-, herstel- en verificatiesessie op een Cisco IOS XE-apparaat:

<#root>

```
Router#

guestshell run bash

[guestshell@guestshell ~]$ sudo -s
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

mkdir -p "$d"
```

```
bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=Comodo%20AAA%20Services%20ro

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;

bash-4.4#

update-ca-trust extract

bash-4.4#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    label: emSign ECC Root CA - G3
    trust: blacklisted
    category: authority

--
    label: AAA Certificate Services
    trust: blacklisted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - C1
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

bash-4.4#

cat /etc/redhat-release

CentOS Stream release 8
bash-4.4#
```

```
d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \ >       "$d/emSign_ECC_Root_C

bash-4.4#
bash-4.4#

update-ca-trust extract

bash-4.4#

ls -l "$d"/

total 0
```

Overzichtsmatrix van opdracht

operationele taak	
Gaststaat controleren	`show app-hosting list`
GuestShell inschakelen (indien GEÏMPLEMENTEERD)	`guestshell enable`
Voer GuestShell Bash in	`guestshell run bash`
Switch naar hoofdgebruiker	`sudo -s`

Blocklist-directory voorbereiden	`d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] || d=/etc/pki/ca-trust/source`
CA's extraheren naar de Blocklist	`trust extract --overwrite --format=pem-bundle ... (x4 CAs)`
CA Trust Store opnieuw samenstellen	`update-ca-trust extract`
Beleid voor wantrouwen controleren	`trust list --filter=trust-policy --purpose=server-auth`
De GEÏMPLEMENTEERDE status herstellen (optioneel)	`guestshell disable`
Vertrouwen terugdraaien/herstellen	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/em`

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.