ACI-foutcode F3081 oplossen: SAML-certificaat verlopen

Inhoud

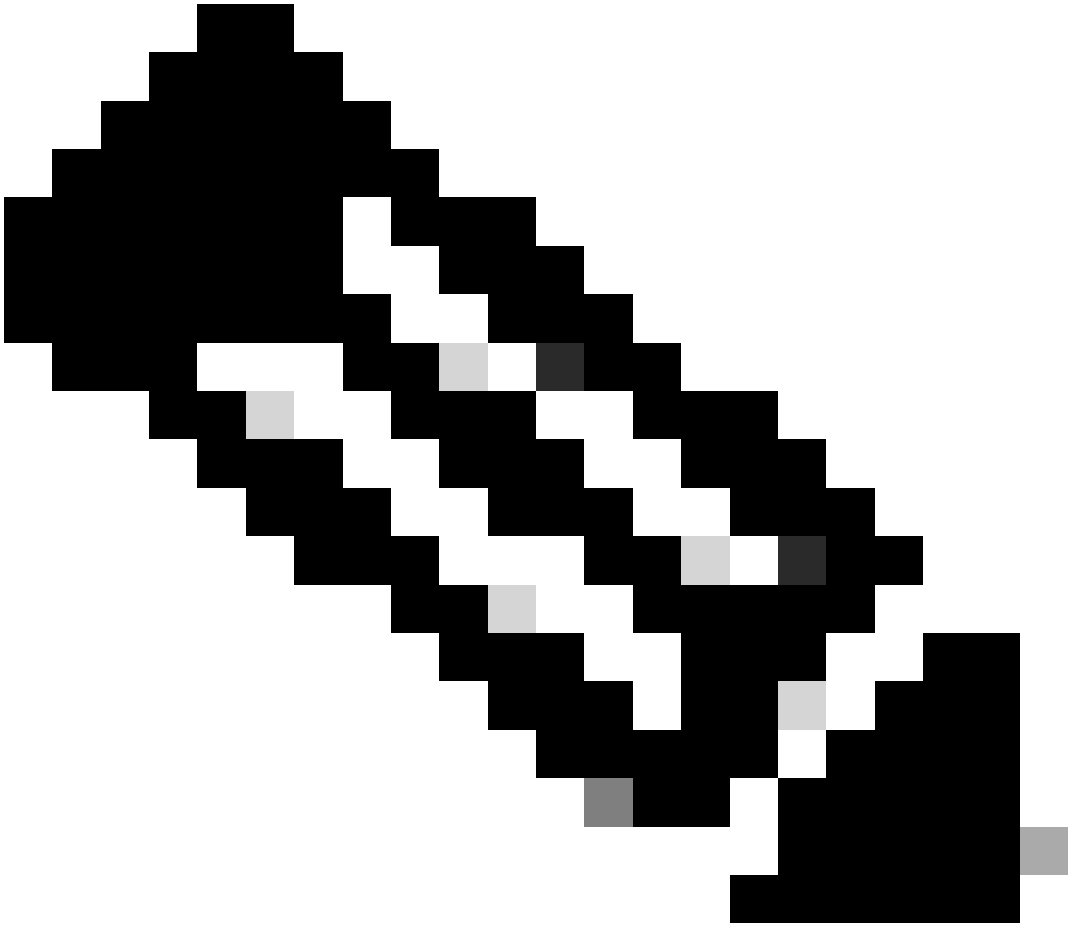
Inleiding

Dit document beschrijft ACI-fout F3081 en de bijbehorende herstelstappen.

Achtergrondinformatie

Deze fout treedt op wanneer een SAML X.509-certificaat over een maand verloopt op een APIC.

```
F3081: fltAaaSamlEncCertSamlEncCertExpiring
Severity: major
Explanation: This fault occurs when the SAML X.509 Certificate is going to expire in one month.
Recommended Action: If you see this fault, take the following actions:
Update SAML X.509 Certificate soon.
```



Opmerking: hetzelfde kan ook gebeuren zonder SAML-implementatie. Als SAML echter niet wordt gebruikt, heeft dit geen invloed op het systeem.

Intersight Connected ACI-stoffen

Deze fout wordt actief gemonitord als onderdeel van Proactieve ACI-opdrachten.

Als u een met Intersight verbonden ACI-stof hebt, wordt er namens u een serviceaanvraag gegenereerd om aan te geven dat er gevallen van deze fout zijn aangetroffen in uw met Intersight verbonden ACI-stof.

Snel starten om fout te adresseren

1. Valideer de status van het verlopen van het certificaat van SAML X.509, als het het Verlopen of Verlopen Fout toont, wordt F3081 verhoogd.

2. Controleer of de certificaatverlener Cisco of een derde is.

3. Als de uitgever Cisco is, ga dan verder met het regenereren van het SAML Encryption Key Pair.

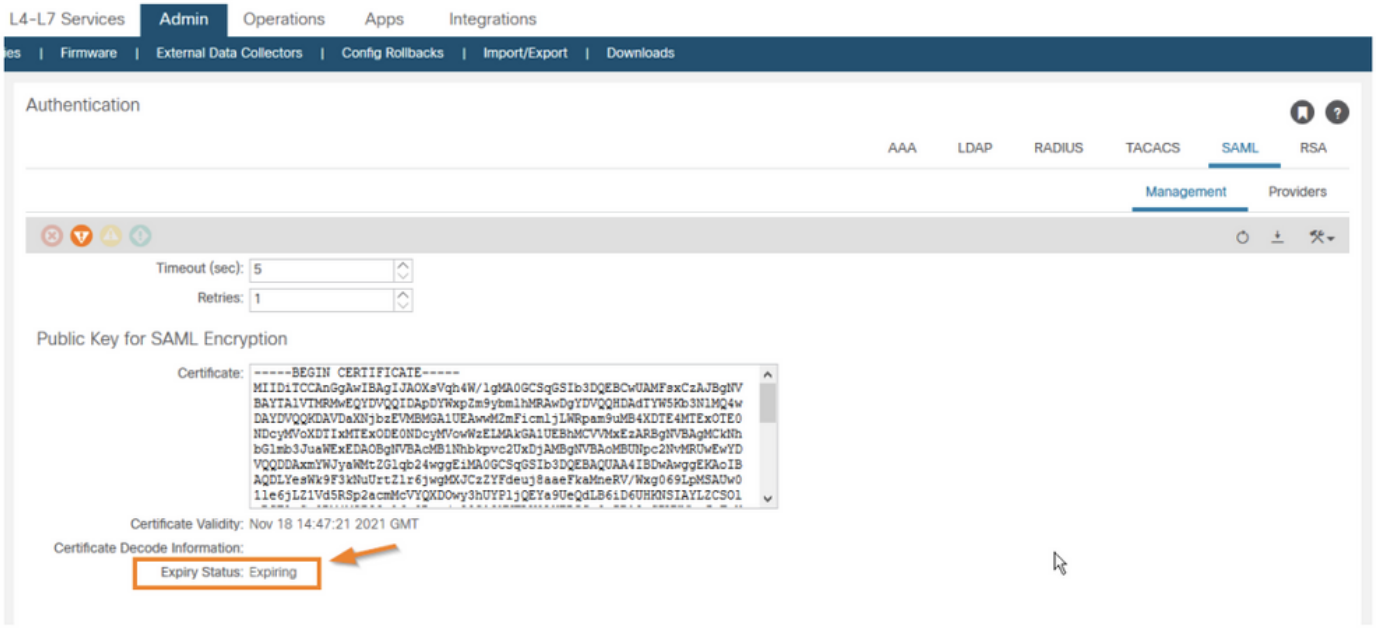
Gedetailleerde stappen om fouten aan te pakken

Valideren SAML X.509 Certificaat Vervalstatus

Via de APIC GUI

1. Navigeer naar Admin > AAA > Authentication > SAML > Management.

2. Valideren SAML X.509 Certificaat Vervalstatus. Expiring betekent dat het certificaat binnen een maand vervalt.



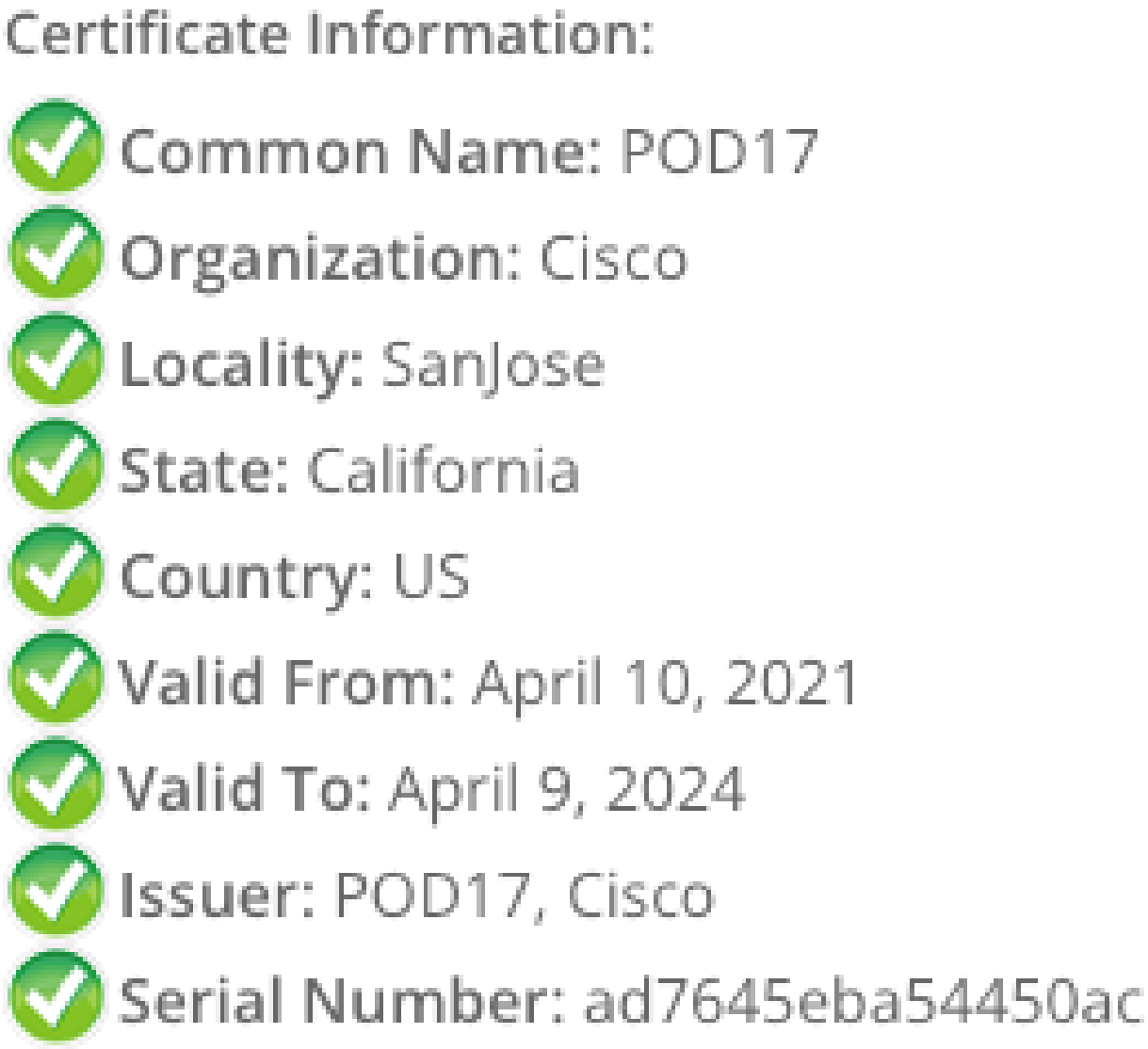
Certificaat van SAML X.509 regenereren en verlengen

Om deze fout op te lossen, kunt u deze verwijderen door het certificaat te regenereren en te vernieuwen en de verloopdatum te verlengen.

Het opnieuw genereren van het SAML X.509 certificaat heeft geen impact.

Voordat u verdergaat, dient u te controleren of de certificaatinstantie (CA) die het certificaat afgeeft, Cisco of een derde is.

Om de certificaatinhoud van APIC te verkrijgen, decodeer het certificaat in een X.509-decoder om de certificaatparameters te verkrijgen:

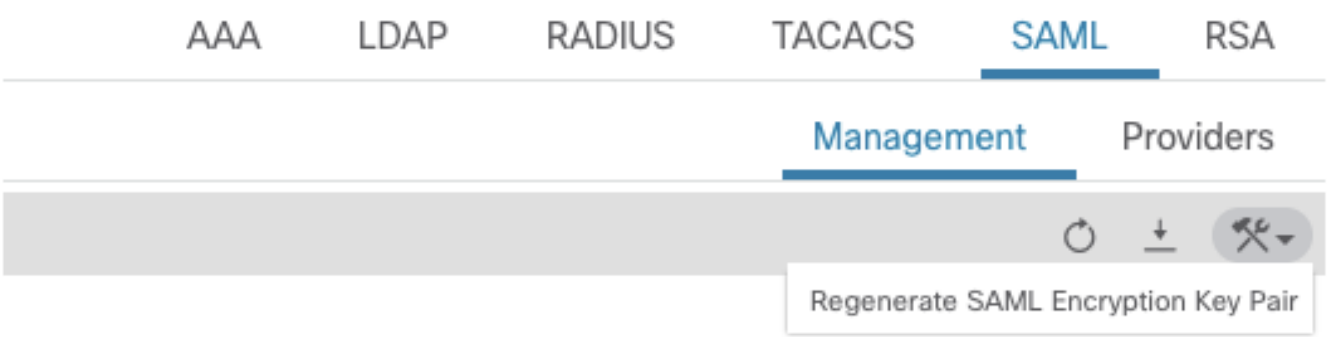


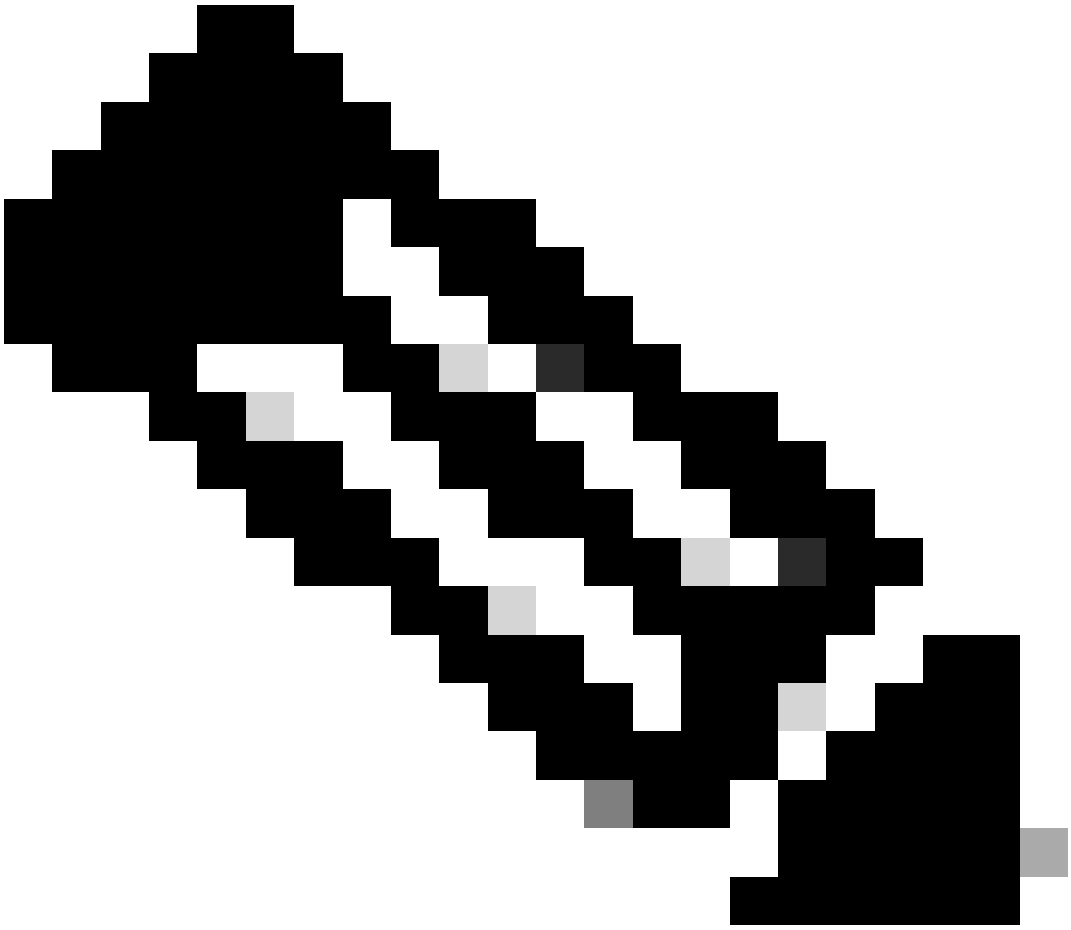
Als het certificaat is afgegeven door een derde CA, neemt u contact op met de CA om uw SAML X.509-certificaat te verlengen.

Als de certificaatverlener echter Cisco is, kunt u deze stappen uitvoeren.

Via APIC GUI

1. Navigeer naar Admin > AAA > Authentication > SAML > Management > Regenerate SAML Encryption Key Pair.



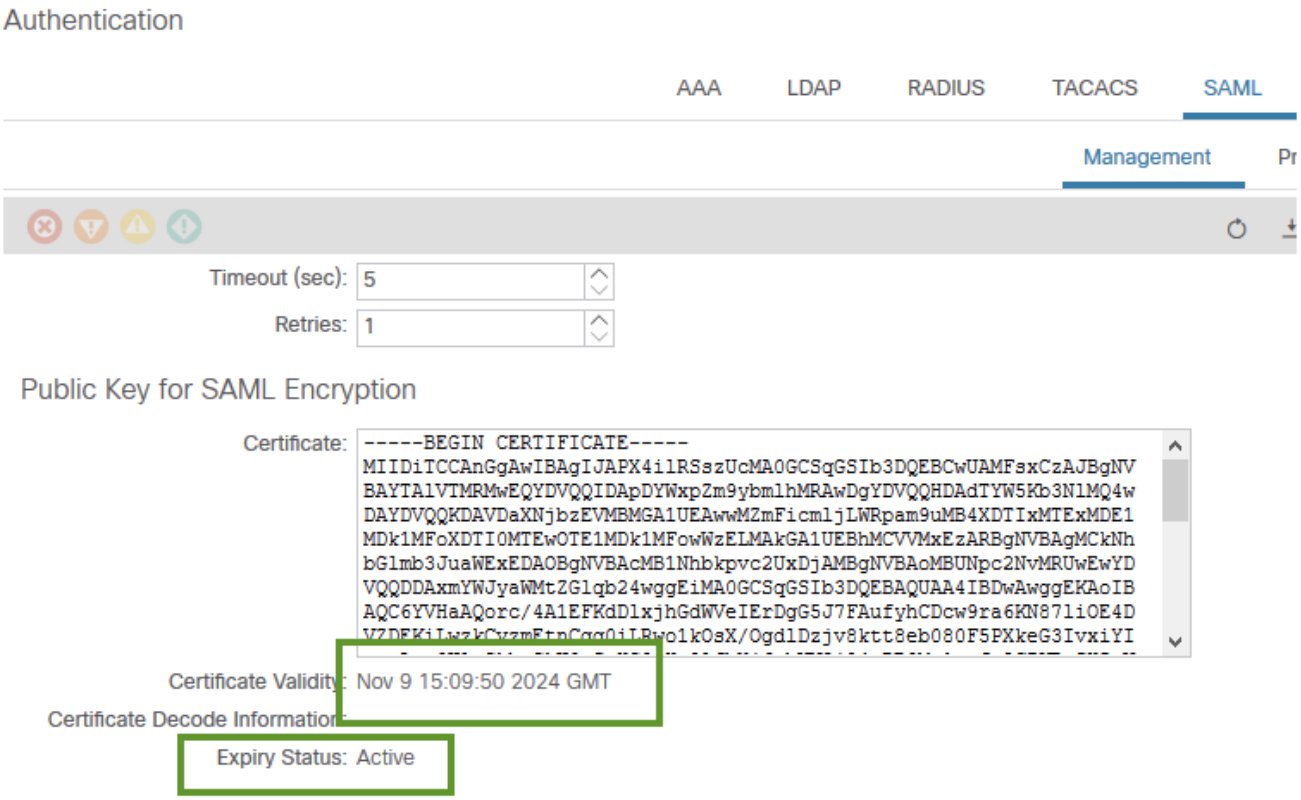


Opmerking: Door het certificaat te verlengen, wordt de in de geldigheid van het certificaat weergegeven verloopdatum verlengd tot een datum die drie jaar na de verversingsdatum valt.

Valideren als verloopstatus gewijzigd is in actief

Via de APIC GUI

1. Navigeer naar Admin > AAA > Authentication > SAML > Management.



Aanvullende informatie

SAML is een op XML gebaseerde open standaard dataformaat waarmee beheerders naadloos toegang kunnen krijgen tot een gedefinieerde reeks Cisco collaboration-toepassingen nadat ze zich in een van deze toepassingen hebben aangemeld. SAML beschrijft de uitwisseling van veiligheidsgerelateerde informatie tussen vertrouwde bedrijfspartners. Het is een verificatieprotocol dat door serviceproviders wordt gebruikt om een gebruiker te authenticeren. SAML maakt de uitwisseling van informatie over veiligheidsverificatie tussen een Identity Provider (IdP) en een serviceprovider mogelijk.

SAML SSO gebruikt het SAML 2.0 protocol om SSO voor meerdere domeinen en producten voor Cisco collaboration-oplossingen aan te bieden. SAML 2.0 schakelt SSO over Cisco-toepassingen in en maakt federatie tussen Cisco-toepassingen en een IDp mogelijk. Met SAML 2.0 hebben Cisco-beheergebruikers ook toegang tot beveiligde webdomeinen om gebruikersverificatie en -autorisatiegegevens te kunnen uitwisselen, tussen een IDp en een serviceprovider, zonder dat dit ten koste gaat van de beveiliging. De functie biedt beveiligde mechanismen voor het gebruik van gemeenschappelijke referenties en relevante informatie in verschillende toepassingen.

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.