Problemen oplossen ISE Admin SAML Login mislukt met toegang geweigerd vanwege ontbrekende domeinnaamconfiguratie

Inhoud

uitgifte

Identity Services Engine (ISE) admin Security Assertion Markup Language (SAML) login mislukt met een "Access Denied" fout na een succesvolle Azure Entra authenticatie. Hoewel Azure Entra een succesvolle SAML-verificatie toont, ontzegt ISE toegang tot het beheerportaal. Bovendien mislukt het genereren van Certificate Signing Request (CSR) met de volgende fout:

```
cpm.admin.caservice.utils.CAUtil -::admin::addLocalCert:- Error occurred managing certificates :::-CSRF
```

ISE-logboeken tonen DNS-resolutiefouten voor de FQDN- en SSL-handdruk-uitzonderingen van de node tijdens interne HTTPS-validatie:

```
SSLHandshakeException: No subject alternative names matching IP address 10.X.X.X found
```

Het systeem geeft ook herhaalde waarschuwingen weer over verlopen standaard zelfondertekende certificaten en RESTConf die terugvallen op HTTP vanwege het niet beschikbaar zijn van certificaten.

milieu

- Cisco Identity Services Engine (ISE) versie 3.4 Patch 3
- Azure Entra (voorheen Azure AD) geconfigureerd als SAML Identity Provider

- ISE-beheer toegankelijk via zowel IP-adres als FQDN
- Omgeving opgewaardeerd van ISE 3.3 naar 3.4

resolutie

1. Controleer de huidige ISE-knooppuntconfiguratie en DNS-resolutie door de volgende opdrachten uit te voeren:

```
show running-config | include domain
nslookup xxxxxxxxxx.internal
ping xxxxxxxxxx.internal
```

Opmerking: de verwachte resultaten tonen een succesvolle DNS-resolutie die het juiste IP-adres retourneert zonder DNS-fouten.

---

2. Voeg de domeinnaam opnieuw toe aan de ISE-knooppuntconfiguratie met behulp van de ISE CLI:

```
device# config t
device(config)# ip domain-name xxxxxxxxxx.internal
```

3. Navigeer naar Beheer > Systeem > Certificaten > Certificaten in de ISE GUI en genereer het standaard zelfondertekende certificaat. Zorg ervoor dat het nieuwe certificaat zowel het FQDN- als het IP-adres in het veld Alternatieve naam (SAN) voor het onderwerp bevat.

4. Bevestig dat het geregenereerde certificaat het IP-adres van de node in het SAN-veld bevat en dat het naar behoren is gekoppeld aan zowel de beheerservices als de portaalservices.

5. Test de ISE admin SAML login. De verificatie moet nu slagen zonder de fout "Toegang geweigerd".

Oorzaak

Dit probleem wordt veroorzaakt door Cisco Bug ID CSCwm59777, die betrekking heeft op IP-domeinnaamverwerking tijdens upgrades van ISE 3.3 naar ISE 3.4. Tijdens het upgradeproces wordt de topniveaudomeinnaamconfiguratie van de node verwijderd, waardoor ISE haar eigen FQDN niet goed kan oplossen. Dit veroorzaakt twee gerelateerde problemen:

1. DNS-resolutiefout: ISE kan de eigen hostnaam niet oplossen, waardoor interne HTTPS-oproepen de validatie van de hostnaam tijdens de SAML-verificatieverwerking mislukken.
2. Mismatch van certificaat SAN: het standaard beheerderscertificaat bevat niet het IP-adres van de node in het SAN-veld, waardoor SSL-handdruk uitvalt wanneer ISE interne HTTPS-validatie probeert met het IP-adres als een fallback.

De combinatie van deze problemen resulteert in succesvolle Azure Entra SAML-verificatie gevolgd door ISE-toegangsweigering vanwege mislukte interne certificaatvalidatie.

Gerelateerde inhoud

- Cisco Bug ID CSCwm59777
- ISE Admin Log in Flow configureren via SAML SSO met Azure AD
- Cisco Technical Support en downloads

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.