Problemen met ISE 3.4 VPN- en RADIUS-verificatiefouten oplossen

Inhoud

uitgeven

ISE 3.4 Patch 4-implementaties ondervinden verificatiefouten wanneer een SAN (Secondary Administration Node) uitvalt. Authenticatieverzoeken die zijn gericht aan de Primary Policy Administration Node (PPAN) mislukken ook, waardoor onderbrekingen ontstaan voor ASA VPN-verbindingen en RADIUS-verificaties. De SAN-node wordt weergegeven als losgekoppeld in het ISE-implementatiedashboard en logboeken geven EAP/TLS-gerelateerde fouten en problemen met het bijhouden van sessies aan.

milieu

- Cisco Identity Services Engine (ISE)
- Network Access Devices (NAD's): omvat Meraki-apparaten en/of ASA-firewall
- Topologie: ISE-implementatie met meerdere knooppunten met SAN en PPAN

resolutie

1.- Verwijder alle persona's van de SAN-node via de Cisco ISE-beheerinterface door naar Beheer > Systeem > Implementatie te navigeren. Hierdoor worden de verificatiepogingen voor de mislukte node gestopt en kunnen de niet-getroffen nodes de verwerking hervatten.

Opmerking: na persoonlijke verwijdering wordt de SAN-node weergegeven als losgekoppeld (Red X) in het implementatiedashboard.

2.- Forceer de ASA-firewall handmatig om de SAN-node als MISLUKT te beschouwen, zodat verdere verificatiepogingen niet naar het niet-beschikbare SAN kunnen worden gericht. Deze actie wordt uitgevoerd op de ASA-configuratie en zorgt voor failover naar operationele ISE-knooppunten.

3.- Controleer de ISE-implementatie voor een goede synchronisatie en controleer de gezondheidsstatistieken, inclusief CPU-, geheugen- en schijfgebruik.

4.- Controleer of de verificatiediensten operationeel zijn door te controleren of nieuwe Dot1x- en RADIUS-verzoeken worden verwerkt door de niet-getroffen ISE-knooppunten.

5.- Verzamel DEBUG-logs en pakketopnames tijdens verificatiefouten om de EAP/TLS-onderhandelingstiming en sessieresets te analyseren.

6.- Blijf de gezondheidsstatistieken en het verificatiegedrag van het ISE-systeem bewaken na SAN-failover-gebeurtenissen.

7.- Valideer het failover-gedrag van Meraki RADIUS, waarbij wordt opgemerkt dat ISE geen ondersteuning biedt voor RADIUS-pakketten voor de detectie van de beschikbaarheid van de server.

Voorbeeldlogberichten

```
Accounting start was received for non-existing session
```

```
Error getting peer certificate from SSL Connection
```

```
packet for this endpoint 58-6D-67-XX-XX-XX is being processed right now so drop the new EAP session
```

```
Long step latency ;2=57290
```

```
Endpoint 58-6D-67-XX-XX-XX abandoned EAP session xxxxxxxxx/552628443/4183334 and started EAP session
```

Oorzaak

De hoofdoorzaak is een storing van de SAN-node als gevolg van een storing in de ISP-koppeling, wat leidt tot inconsistenties in het bijhouden van sessies en EAP/TLS-onderhandelingsfouten tussen de aanvragende, NAD- en ISE-knooppunten. Bovendien vertrouwen Meraki-apparaten op "Status-Server" RADIUS-pakketten voor failover-detectie, die Cisco ISE niet ondersteunt, wat resulteert in voortdurende verificatiepogingen om de mislukte SAN-node te detecteren.

Verwante inhoud

- Hoe te integreren: Meraki-netwerken met ISE
- Remote Access VPN configureren met RADIUS-verificatie op ISE en toewijzen van groepsbeleid
- 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.