

Oplossen van Secure Email Gateway AWS Cloud Migration LDAP Connection Timeout

Inhoud

uitgifte

Na de migratie van de Cisco Secure Email Gateway (SEG)-omgeving naar het Amazon Web Services (AWS) Cloud-gehoste SEG-platform, ervaren beheerders aanhoudende problemen met de aanmelding en prestaties.

Symptomen waren onder meer:

- Aanzienlijke vertragingen bij de toegang tot de SEG in zowel GUI- als CLI-interfaces
- Buitensporig veel tijd nodig voor verificatie na het invoeren van gebruikersnaam en wachtwoord
- Zeer traag laden van het hoofddashboard/de hoofdpagina
- De algemene reactiesnelheid van het platform was extreem traag
- Problemen waren het meest merkbaar tijdens LDAP-geverifieerde toegang

Uit de analyse van het vastleggen van pakketten blijkt dat SEG TCP-sessies naar LDAP-servers worden afgesloten door de Gateway Load Balancer (GWLB) na ongeveer 350 seconden inactieve tijd, waardoor vertragingen en time-outs bij de verificatie worden veroorzaakt.

milieu

- Cisco Secure Email Gateway (SEG) gemigreerd naar AWS Cloud-gehoste platform
- Versie asyncOS: 16.0.4-016
- LDAP-verificatie geconfigureerd met Active Directory

- AWS Gateway Load Balancer (GWLB) in het netwerkpad
- Cisco Secure Email en Web Manager hebben ook last van hetzelfde probleem
- SSL/TLS-codering ingeschakeld voor LDAP-verbindingen op poort 3269

resolutie

Pas de instellingen voor de levensduur van de LDAP-verbinding aan om te voorkomen dat de time-outs van de sessie niet actief zijn als gevolg van de AWS Gateway Load Balancer met de volgende stappen:

1. Maak verbinding met de SEG CLI en krijg toegang tot de LDAP-configuratie:

```
device# ldapconfig
```

2. Zoek het LDAP-serverprofiel en wijzig de instelling "Maximale levensduur per verbinding met de server (in seconden)". Wijzig deze waarde in 300 seconden om ervoor te zorgen dat de verbindingen worden vernieuwd voordat de uitschakeldrempel van 350 seconden voor de gateway-taakverdeling wordt overschreden.

Oorspronkelijke configuratie:

```
Max lifetime per connection: 1800
```

Bijgewerkte configuratie:

```
Max lifetime per connection: 300
```

3. Zet de configuratiewijzigingen vast en laat het systeem de nieuwe instellingen toepassen.

4. Breng de identieke LDAP-verbinding levenslange wijziging aan op de Cisco Secure Email and Web Manager met dezelfde configuratie van 300 seconden.

5. Test de GUI- en CLI-inlogfunctionaliteit. Na het implementeren van de wijzigingen moeten de inlogtijden worden teruggebracht tot ongeveer 5 seconden en mogen de verificatievertragingen niet langer optreden.

6. Controleer de omgeving op herhaling van het probleem en verzamel pakketopnames als er problemen blijven bestaan.

Oorzaak

Packet capture-analyse toonde aan dat de AWS Gateway Load Balancer (GWLB) na ongeveer 350 seconden inactieve TCP-sessies beëindigde. De standaardlevensduur van de LDAP-verbinding van de SEG is 1800 seconden, wat de inactieve time-outdrempel van 350 seconden van de GWLB overschrijdt. Wanneer LDAP-verbindingen meer dan 350 seconden inactief bleven, zou de GWLB de TCP-sessies afbreken, waardoor authenticatievertragingen en time-outs ontstaan wanneer gebruikers probeerden in te loggen. Door de levensduur van de LDAP-verbinding tot 300 seconden te beperken, vernieuwt de SEG proactief verbindingen voordat de GWLB-time-out optreedt en voorkomt het vertragingen bij de verificatie.

Gerelateerde inhoud

- [Gebruikershandleiding voor AsyncOS 16.5 voor Cisco Secure Email Cloud Gateway - GD \(General Deployment\)](#)
- [Gebruikershandleiding voor AsyncOS 16.5 voor Cisco Secure Email and Web Manager - GD \(General Deployment\)](#)

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.