

ISE e-mailalarmmeldingen werken niet na software-upgrade

Inhoud

uitgifte

E-mailalarmmeldingen van de Cisco Identity Services Engine (ISE) worden niet aan geconfigureerde ontvangers bezorgd. De SMTP-testfunctie binnen ISE slaagt, maar daadwerkelijke alarmgebeurtenissen leiden niet tot het verzenden van e-mailmeldingen. Dit probleem begon op te treden na het upgraden van ISE versie 3.2 naar 3.4 Patch 3, en bleef zelfs na het toepassen van 3.4 Patch 5. De alarmberichten werkten kort na het toepassen van Patch 5, maar werkten niet meer toen de e-mailmeldingen opnieuw werden ingeschakeld nadat ze tijdelijk waren uitgeschakeld vanwege een hoog volume.

milieu

- Cisco Identity Services Engine (ISE) versie 3.4 Patch 5
- ISE-implementatie met 6 PSN's (Policy Service Nodes), 2 MnT-nodes (Monitoring & Troubleshooting) en 2 PAN's (Policy Administration Nodes)
- Primaire MnT-knooppunt: COR089ISE-MnT02 (IP: 172.29.134.2)
- SMTP-server: smtp1.us.parker.corp
- Eerdere werkconfiguratie op ISE versie 3.2
- Probleem gestart na upgrade van versie 3.2 naar 3.4 Patch 3 in oktober

resolutie

Als u problemen met de ISE-alarmmeldingen wilt oplossen, volgt u de diagnostische en

oplossingsstappen die in de volgende secties worden beschreven.

Stap 1: Controleer de SMTP-configuratie en testfunctionaliteit

Bevestig dat de SMTP-test binnen ISE succesvol is en verifieer de configuratie van de e-mailserver:

1. Navigeer naar Beheer > Systeem > Instellingen > SMTP-server in de ISE GUI.
2. Controleer alle SMTP-instellingen, waaronder het serveradres, de poort, de TLS/STARTTLS-configuratie en de verificatie-instellingen.
 - Controleer of het IP-adres of FQDN van de SMTP-server (Mail Gateway) correct is.
 - Controleer de SMTP-poort: Standaardpoort 25. Als veilige verzending (TLS/STARTTLS) is ingeschakeld, moet deze expliciet overeenkomen met de geopende poort op de e-mailserver (zoals poort 587).
3. Test de SMTP-verbinding met behulp van de ingebouwde testfunctie.
4. Coördineer met de beheerders van de e-mailserver om te bevestigen of teste-mails op serverniveau worden ontvangen.

Stap 2: Debug-logging inschakelen op primaire MnT-node

Gebruik root-toegang om te isoleren of het probleem een interne trigger is of een externe verbindingfout met de server:

```
tail -F /opt/CSC0cpm/logs/ise-psc.log
2026-06-02 14:51:54,851 WARN [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
2026-06-02 14:51:54,851 INFO [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
2026-06-02 14:51:54,853 ERROR [MnT-AlarmWorkerMail-Threadpool-0][[]] cisco.mnt.common.alarms.AlarmWorke
```

Als verdere probleemoplossing vereist is of als u niet kunt controleren via root, schakelt u gedetailleerde logboekregistratie in om alarmgeneratie- en e-mailbezorgpogingen vast te leggen.

Schakel deze foutopsporingscomponenten in op de primaire MnT-node:

```
cisco-mnt  
cpm-mnt
```

Stap 3: Leg netwerkverkeer vast tijdens alarmgebeurtenissen

Voer pakketvastlegging uit om te controleren of ISE probeert SMTP-verbindingen te maken voor alarmgebeurtenissen:

1. Navigeer naar **Bewerkingen > Problemen oplossen > Diagnostische hulpprogramma's > TCP Dump** op de primaire MnT-node.
2. Selecteer de netwerkinterface die wordt gebruikt om met de SMTP-server te communiceren.
3. Start het vastleggen van het pakket.
4. Voer tijdens het vastleggen zowel:
 - Voer de SMTP-test uit vanaf ISE (om bekende goede SMTP-sessie vast te leggen).
 - Genereer of wacht tot er een echte alarmgebeurtenis plaatsvindt.
5. Stop het vastleggen en download het PCAP-bestand voor analyse.

Stap 4: Toepassingslogboeken bewaken tijdens het genereren van alarmen

Monitor ISE-toepassingslogboeken om pogingen tot het verzenden van e-mails te identificeren.

Voer deze opdracht uit op de primaire MnT-knooppunt CLI terwijl een alarm wordt gegenereerd:

```
show logging application ise-psc.log tail
```

Leg de uitvoer vast en noteer de tijdstempel van alle alarmgebeurtenissen die e-mailmeldingen moeten activeren.

Stap 5: Coördineren met e-mailserverbeheer

Werk samen met e-mailserverbeheerders om de verwerking aan de serverzijde te verifiëren.

Laat het e-mailteam tijdens het testen van het alarm de SMTP-serverlogboeken controleren op:

- SMTP-verbindingen vanaf het IP-adres van de primaire MnT-node
- Status van acceptatie, afwijzing of uitstel van bericht
- Eventuele foutcodes of afwijzingsredenen als berichten niet worden geaccepteerd

Stap 6: Gevangen gegevens analyseren en resolutie implementeren

Controleer de verzamelde pakketopnamen, logbestanden en servergegevens om te bepalen:

- Of ISE probeert om alarm e-mails te verzenden (zichtbaar in packet capture).
- Reactiecodes van de server en eventuele afwijzingsredenen.
- Verschillen tussen succesvolle SMTP-testsessies en alarm-getriggerde sessies.

Voer op basis van de analyse passende oplossingen uit, zoals:

- De configuratie of het beveiligingsbeleid van de SMTP-server aanpassen.
- Instellingen voor ISE-e-mailmeldingen wijzigen.
- Het adres van de afzender of de verificatieparameters bijwerken.

Stap 7: Debug-logboekregistratie uitschakelen

Schakel na het oplossen van problemen de componenten voor foutopsporingslogboekregistratie

uit om groei van logbestanden te voorkomen.

Schakel de foutopsporingscomponenten uit op de primaire MnT-node:

```
cisco-mnt (disable)  
cpm-mnt (disable)
```

Oorzaak

Het probleem kan voortkomen uit verschillen in de manier waarop de MnT-node (Primary Monitoring & Troubleshooting) SMTP-sessies voor alarmeringsgebeurtenissen afhandelt ten opzichte van SMTP-testfuncties. Terwijl de SMTP-test slaagt, kunnen de daadwerkelijke alarm-getriggerde e-mailpogingen mislukken als gevolg van configuratie-incompatibiliteit, server-side filtering of wijzigingen in het e-mailverzendproces dat in de nieuwere ISE-versie is geïntroduceerd.

Gerelateerde inhoud

- [Cisco ISE 3.4-beheergids - Problemen oplossen](#)
- [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.