Problemen met ISE-certificaatreplicatiealarmen begrijpen en oplossen

Inhoud

Inleiding

In dit document worden de replicatiealarmen en de probleemoplossing in Cisco Identity Services Engine® (ISE) beschreven.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco Identity Services Engine® (ISE).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende hardware- en softwareversies.

- Cisco Identity Services Engine® (ISE) 3.4 en hogere versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

replicatiealarm

Replicatiealarmen in Cisco ISE bieden inzicht in de status van de status en synchronisatie van het replicatieframework in de implementatie. Deze alarmen helpen bij het identificeren van omstandigheden die van invloed kunnen zijn op de consistentie van gegevens, knooppuntcommunicatie of replicatieprocessen, waardoor beheerders problemen kunnen detecteren en oplossen voordat ze van invloed zijn op systeemactiviteiten. Inzicht in het doel en de betekenis van replicatiealarmen is essentieel voor het handhaven van een gezonde ISE-implementatie en ervoor te zorgen dat configuratie- en operationele gegevens over alle knooppunten gesynchroniseerd blijven.

Replicatiealarmen ISE-certificaat

Certificaatreplicatie mislukt

Het alarm Certificaatreplicatie mislukt wordt gegenereerd wanneer Cisco ISE er niet in slaagt certificaatgerelateerde gegevens van de primaire beheernode (PAN) naar een of meer knooppunten in de implementatie te repliceren. ISE repliceert automatisch certificaten en de bijbehorende configuratie wanneer certificaten worden geïmporteerd, gegenereerd, vernieuwd of gewijzigd op het primaire PAN om de consistentie tussen alle knooppunten te behouden. Dit alarm geeft aan dat het replicatieproces niet succesvol was, wat resulteerde in een inconsistente certificaatconfiguratie op de getroffen node(s).

Reden voor alarm

Het alarm Certificaatreplicatie mislukt kan optreden wanneer Cisco ISE niet in staat is om certificaatgerelateerde gegevens over te dragen, te valideren of te installeren op een of meer nodes. Gemeenschappelijke oorzaken zijn onder meer

- Problemen met netwerkcommunicatie: pakketverlies, hoge netwerklatentie, firewallbeperkingen die replicatieverkeer blokkeren, routeringsproblemen tussen ISE-

knooppunten of een MTU-mismatch die pakketfragmentatie of -dalingen veroorzaakt, kunnen de replicatie van certificaten onderbreken.
- Problemen met replicatieservices: Certificaatreplicatie kan mislukken als RabbitMQ, JGroups of andere interne replicatieservices niet beschikbaar zijn, opnieuw worden gestart of niet correct functioneren.
- Fouten bij certificaatvalidatie: replicatie kan mislukken als de certificaatketen onvolledig is, CA- of tussenliggende certificaten ontbreken, het certificaat is verlopen of beschadigd, of het bevat niet-ondersteund sleutelgebruik of een ongeldig formaat.
- Problemen met knooppuntcommunicatie: als het doelknooppunt offline is, opnieuw wordt opgestart, niet wordt geregistreerd, de verbinding met de implementatie wordt verbroken of onbereikbaar is, kan de certificaatreplicatie niet worden voltooid.
- Onvoldoende schijfruimte: de doelnode heeft niet voldoende schijfruimte beschikbaar om het gerepliceerde certificaat te importeren en te installeren.
- Problemen met interne databases: Replicatie kan mislukken als de ISE-configuratiedatabase de certificaatmetagegevens niet kan opslaan of bijwerken.

Impact van het alarm

De impact van dit alarm hangt af van het type certificaat dat wordt gerepliceerd en de diensten die erop vertrouwen. Mislukte certificaatreplicatie kan leiden tot inconsistente certificaatconfiguratie in ISE-knooppunten, HTTPS-certificaatmismatches, EAP-verificatiefouten, problemen met het instellen van pxGrid-vertrouwen, SCEP-inschrijvings- of certificaatprovisioning, inconsistenties in het vertrouwde certificaatarchief en TLS-validatiefouten met externe integraties.

Certificaatreplicatie tijdelijk mislukt

Het alarm Certificaatreplicatie tijdelijk mislukt wordt gegenereerd wanneer Cisco ISE tijdelijk niet in staat is om certificaatgerelateerde gegevens van de primaire beheernode (PAN) naar een of meer knooppunten in de implementatie te repliceren. In tegenstelling tot het alarm Certificaatreplicatie mislukt, geeft dit alarm aan dat de replicatiefout als van voorbijgaande aard wordt beschouwd en dat Cisco ISE de replicatiebewerking automatisch opnieuw probeert wanneer de onderliggende toestand is opgelost.

Reden voor alarm

Het alarm wordt meestal gegenereerd als gevolg van voorbijgaande omstandigheden die de replicatie van certificaten tijdelijk voorkomen. Veel voorkomende oorzaken zijn:

- Tijdelijke problemen met netwerkcommunicatie: korte netwerkonderbrekingen, pakketverlies, hoge latentie, firewallvertragingen of tijdelijke routeringsproblemen tussen ISE-knooppunten.
- Initialisatie of herstart van de replicatieservice: RabbitMQ, JGroups of andere interne

replicatieservices worden opnieuw gestart of zijn tijdelijk niet beschikbaar.
- Tijdelijke onbeschikbaarheid van node: De doelnode start op, start de toepassingsservices opnieuw op, maakt opnieuw deel uit van de implementatie of is tijdelijk onbereikbaar.
- Tijdelijke beperkingen van de systeembronnen: hoge CPU-benutting, geheugendruk of I/O-conflicten op de schijf vertragen de replicatieverwerking tijdelijk.
- Gelijktijdige beheerbewerkingen: Certificaatreplicatie kan worden uitgesteld terwijl een ander certificaat wordt geïmporteerd, geback-upt, teruggezet, geïnstalleerd of gesynchroniseerd.
- Tijdelijke vertragingen in database- of replicatiewachtrijen: interne databasebewerkingen of replicatiewachtrijen zijn tijdelijk bezig met het verwerken van andere synchronisatieverzoeken.

Impact van het alarm

In de meeste gevallen heeft dit alarm een minimale operationele impact omdat Cisco ISE de replicatiebewerking automatisch opnieuw probeert. Totdat de replicatie met succes is voltooid, kunnen er echter tijdelijke inconsistenties tussen nodes bestaan, waaronder:

- Vertraagde vermeerdering van nieuw ingevoerde of vernieuwde certificaten
- Mismatch in de configuratie van tijdelijke certificaten in de implementatie
- Vertraagde beschikbaarheid van op certificaten gebaseerde services op de getroffen node
- Tijdelijke vertragingen in HTTPS-, EAP-, pxGrid- of SCEP-services als deze afhankelijk zijn van het gerepliceerde certificaat

Als het alarm aanhoudt of herhaaldelijk voorkomt, leidt dit tot alarm voor mislukte certificaatreplicatie.

Problemen met replicatiealarmen van ISE-certificaat oplossen

Dit zijn de gemeenschappelijke factoren die moeten worden geverifieerd bij het oplossen van problemen of het verifiëren van certificaatreplicatiealarmen in ISE.

1. De implementatiestatus voor de node controleren

Om de replicatie van certificaten te laten slagen, moet het secundaire knooppunt zich in een Connected-toestand bevinden binnen de Cisco ISE-implementatie. Navigeer naar Beheer > Systeem > Implementatie en controleer de status van de betreffende node. Beweeg de muis over het pictogram Informatie (i) naast de knooppuntstatus om de synchronisatiedetails en eventuele replicatieberichten in behandeling te bekijken.

De synchronisatiestatus die voor elk knooppunt wordt weergegeven, geeft de huidige replicatie-

en connectiviteitsstatus aan:

- Groen – De node wordt gesynchroniseerd met de implementatie en de replicatie werkt normaal.
- Geel – De node is niet meer gesynchroniseerd, de registratie van de node is mislukt of de clusterconnectiviteit is verloren gegaan. Deze status geeft aan dat het knooppunt de afgelopen vijf minuten niet bereikbaar is geweest voor het cluster.
- Rood – De node is onbereikbaar en kan niet worden gecontacteerd via netwerkconnectiviteitscontroles, zoals ICMP-ping of HTTPS.

Als de node een gele of rode status weergeeft, duidt dit op een probleem met replicatie of connectiviteit dat van invloed is op die node. Controleer bovendien het aantal replicatieberichten dat wordt weergegeven in de knooppuntinformatie. Het aantal in behandeling zijnde berichten moet 5.000 of minder bedragen. Een wachtrij met meer dan 5.000 openstaande berichten geeft aan dat de replicatiewachtrij zich heeft verzameld, wat succesvolle replicatie kan vertragen of voorkomen.

2. Controleer het koppelingsalarm in de wachtrij in de implementatie

Succesvolle replicatie in Cisco ISE is afhankelijk van de beschikbaarheid en communicatie van de RabbitMQ-berichtenservice en het JGroups-clustercommunicatiekader. Als een van beide componenten communicatieproblemen ondervindt, genereert Cisco ISE Queue Link-fouten, die de replicatie tussen implementatieknooppunten kunnen onderbreken.

Om de alarmstatus te controleren, navigeert u naar Bewerkingen > Dashboard > Alarmen en controleert u op Queue Link-fouten op de getroffen knooppunten.

Als er fouten in de wachtrijkoppeling aanwezig zijn, verlengt u het Cisco ISE Root CA-certificaat, omdat communicatiefouten met betrekking tot certificaten vaak leiden tot fouten in de wachtrijkoppeling. Zodra het probleem met het certificaat is opgelost, wordt de replicatie doorgaans automatisch hervat zonder dat extra interventie nodig is.

Opmerking: Raadpleeg de documentatie ISE Queue Link Fouten voor gedetailleerde informatie over Queue Link Fouten.

---

3. Netwerklatentie en -connectiviteit controleren

Cisco ISE-replicatie is gebaseerd op stabiele netwerkconnectiviteit tussen implementatiemodes. Hoge netwerklatentie of intermitterende connectiviteit kan replicatie vertragen en kan leiden tot synchronisatiefouten, met name in geografisch gedistribueerde implementaties.

Controleer de netwerklatentie tussen de getroffen knooppunten met behulp van connectiviteitstests zoals ping. Voor betrouwbare replicatie moet de heen en weer geschakelde latentie tussen nodes binnen ongeveer 300 ms blijven. Latentie die deze drempel consequent overschrijdt, kan een negatieve invloed hebben op de replicatieprestaties en synchronisatie. Controleer ook of er geen intermitterende netwerkuitval, pakketverlies of firewallbeperkingen zijn die de communicatie tussen de implementatieknooppunten beïnvloeden.

4. Controleer of het certificaat niet al aanwezig is op het getroffen knooppunt

Certificaatreplicatie kan mislukken als het certificaat dat wordt gerepliceerd al bestaat op de secundaire node.

Navigeer naar Beheer > Systeem > Certificaten, selecteer de betreffende node en controleer of het certificaat al is geïnstalleerd. Als het certificaat aanwezig is, controleert u de eigenschappen ervan om te controleren of het overeenkomt met het certificaat dat wordt gerepliceerd en bepaalt u of er dubbele of tegenstrijdige certificaten bestaan.

5. Het gebruik van systeembronnen controleren

Een hoog gebruik van systeembronnen kan de Cisco ISE-prestaties beïnvloeden en replicatietaken vertragen. Overmatig CPU-, geheugen- of schijfgebruik kan voorkomen dat replicatieprocessen met succes worden voltooid.

Controleer of het getroffen knooppunt over voldoende systeembronnen beschikt en of het gebruik van bronnen binnen de aanbevolen operationele limieten blijft. Als het bronnengebruik constant hoog is, wijst u extra bronnen toe of verlaagt u de werklast op de node om de normale replicatieprestaties te herstellen.

Opmerking: raadpleeg de handleiding voor prestaties en schaalbaarheid voor de aanbevolen richtlijnen voor de grootte van hardware en de toewijzing van bronnen voor Cisco ISE-implementaties.

---

6. Controleren van de beschikbaarheid van poorten in de implementatie en het netwerk

Cisco ISE-replicatie vereist dat specifieke TCP-poorten open blijven tussen alle knooppunten in de implementatie om ononderbroken communicatie en succesvolle replicatie te garanderen. Als een van deze poorten wordt geblokkeerd door een firewall, toegangscontrolebeleid of netwerkapparaat, kunnen zich replicatiefouten of synchronisatieproblemen voordoen.

Controleer of deze TCP-poorten open en bereikbaar zijn tussen alle Cisco ISE-knooppunten:

- TCP 443 – HTTPS-communicatie
- TCP 8443 – Administratieve communicatie
- TCP 12001 – Groepen voor clustercommunicatie en -replicatie
- TCP 6379 – Interne berichtenservices
- TCP 8671 – Cisco ISE Messaging (RabbitMQ)

Meld u aan bij de Cisco ISE CLI en voer de opdracht Show Ports uit om te controleren of de genoemde poorten in de node zijn toegestaan.

Bevestig dat de vereiste poorten zijn ingeschakeld op de Cisco ISE-node en zorg ervoor dat ze zijn toegestaan op het netwerkpad. Controleer of er geen tussenliggende firewalls, beveiligingsapparaten of netwerkbeleidsregels zijn die de communicatie op deze poorten tussen de knooppunten van de implementatie blokkeren.

Logboekverzameling voor replicatiealarmen

Dit zijn de gemeenschappelijke componenten die moeten worden ingesteld in de debug-modus om replicatiealarmen in Cisco ISE te isoleren en problemen op te lossen.

- Replication-Deployment (replication.log en ise-psc.log)
- Replication-JGroup (replication.log en ise-psc.log)
- Replication Tracker (tracking.log)
- Sluimerstand (Hibernate.log)
- JMS (replication.log)

referentie

- Beheerdershandleiding voor de Cisco Identity Services-engine, release 3.5
- Troubleshooten en foutsporing inschakelen op ISE
- Verzamel ondersteuningspakket op de Identity Services-engine

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.