Entender e solucionar problemas de alarmes de replicação de certificado do ISE

Contents

Introdução

Este documento descreve os alarmes de replicação e sua solução de problemas no Cisco Identity Services Engine® (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça o Cisco Identity Services Engine® (ISE).

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software.

- Cisco Identity Services Engine® (ISE) 3.4 e versões posteriores.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Alarme de replicação

Os alarmes de replicação no Cisco ISE oferecem visibilidade do estado e do status de sincronização da estrutura de replicação durante a implantação. Esses alarmes ajudam a identificar condições que podem afetar a consistência de dados, a comunicação de nós ou os processos de replicação, permitindo que os administradores detectem e resolvam problemas antes que eles afetem as operações do sistema. Entender a finalidade e o significado dos alarmes de replicação é essencial para manter uma implantação saudável do ISE e garantir que a configuração e os dados operacionais permaneçam sincronizados em todos os nós.

Alarmes de replicação de certificado ISE

Falha na Replicação de Certificado

O alarme Certificate Replication Failed é gerado quando o Cisco ISE falha ao replicar dados relacionados ao certificado do Primary Administration Node (PAN) para um ou mais nós na implantação. O ISE replica automaticamente os certificados e suas configurações associadas sempre que eles são importados, gerados, renovados ou modificados no PAN principal para manter a consistência em todos os nós. Esse alarme indica que o processo de replicação não foi bem-sucedido, resultando em uma configuração de certificado inconsistente no(s) nó(s) afetado(s).

Motivo do alarme

O alarme Falha na replicação de certificado pode ocorrer quando o Cisco ISE não consegue transferir, validar ou instalar com êxito dados relacionados ao certificado em um ou mais nós. As causas comuns incluem

- Problemas de comunicação de rede: Perda de pacotes, alta latência de rede, restrições de firewall que bloqueiam o tráfego de replicação, problemas de roteamento entre nós ISE ou uma incompatibilidade de MTU que cause fragmentação ou quedas de pacotes podem

interromper a replicação de certificados.
- Problemas do serviço de replicação: A replicação de certificado poderá falhar se RabbitMQ, JGroups ou outros serviços de replicação internos estiverem indisponíveis, reiniciando ou não funcionando corretamente.
- Falhas na validação do certificado: A replicação poderá falhar se a cadeia de certificados estiver incompleta, se a CA ou os certificados intermediários estiverem ausentes, se o certificado tiver expirado ou estiver corrompido ou se contiver um uso de chave sem suporte ou um formato inválido.
- Problemas de comunicação de nó: Se o nó de destino estiver offline, a reinicialização, o cancelamento do registro, a desconexão da implantação ou a inacessibilidade, a replicação do certificado não poderá ser concluída.
- Espaço em disco insuficiente: O nó de destino não tem espaço em disco disponível suficiente para importar e instalar o certificado replicado.
- Problemas internos do banco de dados: A replicação poderá falhar se o banco de dados de configuração do ISE não puder armazenar ou atualizar os metadados do certificado.

Impacto do alarme

O impacto desse alarme depende do tipo de certificado que está sendo replicado e dos serviços que dependem dele. A falha na replicação do certificado pode resultar em configuração de certificado inconsistente nos nós do ISE, incompatibilidades de certificado HTTPS, falhas de autenticação EAP, problemas de estabelecimento de confiança do pxGrid, falhas de registro SCEP ou de provisionamento de certificado, inconsistências no repositório de certificados confiáveis e falhas de validação de TLS com integrações externas.

Falha temporária na replicação de certificado

O alarme Falha temporária na replicação de certificado é gerado quando o Cisco ISE não pode replicar temporariamente dados relacionados ao certificado do PAN (Nó de administração primário) para um ou mais nós na implantação. Diferentemente do alarme Falha na Replicação de Certificado, esse alarme indica que a falha na replicação é considerada transitória e o Cisco ISE repete automaticamente a operação de replicação quando a condição subjacente é resolvida.

Motivo do alarme

O alarme geralmente é gerado devido a condições transitórias que impedem temporariamente a replicação de certificado. As causas comuns incluem:

- Problemas temporários de comunicação de rede: Breves interrupções de rede, perda de pacotes, alta latência, atrasos de firewall ou problemas temporários de roteamento entre nós do ISE.

- Inicialização ou reinicialização do serviço de replicação: RabbitMQ, JGroups ou outros serviços de replicação interna estão sendo reiniciados ou temporariamente indisponíveis.
- Indisponibilidade temporária do nó: O nó de destino está sendo inicializado, reiniciando serviços de aplicativos, reingressando na implantação ou está temporariamente inacessível.
- Restrições temporárias de recursos do sistema: A alta utilização da CPU, a pressão da memória ou a contenção de I/O do disco atrasa temporariamente o processamento da replicação.
- Operações administrativas simultâneas: A replicação de certificado pode ser atrasada enquanto outra importação de certificado, backup, restauração, instalação de patch ou sincronização de implantação está em andamento.
- Atrasos do banco de dados temporário ou da fila de replicação: As operações internas do banco de dados ou as filas de replicação estão temporariamente ocupadas processando outras solicitações de sincronização.

Impacto do alarme

Na maioria dos casos, esse alarme tem um impacto operacional mínimo, pois o Cisco ISE repete automaticamente a operação de replicação. No entanto, até que a replicação seja concluída com êxito, podem existir inconsistências temporárias entre os nós, incluindo:

- Propagação atrasada de certificados recém-importados ou renovados
- Incompatibilidade de configuração de certificado temporário na implantação
- Disponibilidade atrasada de serviços baseados em certificado no nó afetado
- Atrasos temporários nos serviços HTTPS, EAP, pxGrid ou SCEP se eles dependerem do certificado replicado

Se o alarme persistir ou ocorrer repetidamente, ele levará ao alarme Falha na Replicação de Certificado.

Solucionar problemas de alarmes de replicação de certificado ISE

Esses são os fatores comuns que devem ser verificados durante a solução de problemas ou a verificação de alarmes de replicação de certificado no ISE.

1. Verificar Status de Implantação para o Nó

Para que a replicação do certificado tenha êxito, o nó secundário deve estar em um estado Conectado na implantação do Cisco ISE. Navegue até Administração > Sistema > Implantação e verifique o status do nó afetado. Passe o mouse sobre o ícone Information (i) ao lado do status do

nó para revisar os detalhes da sincronização e quaisquer mensagens de replicação pendentes.

O status de sincronização exibido para cada nó indica seu estado atual de replicação e conectividade:

- Verde - o nó é sincronizado com a implantação e a replicação está operando normalmente.
- Amarelo - O nó está fora de sincronização, o registro do nó falhou ou a conectividade do cluster foi perdida. Esse status indica que o nó não pode ser acessado pelo cluster nos últimos cinco minutos.
- Vermelho - O nó está inacessível e não pode ser contatado por meio de verificações de conectividade de rede, como ping ICMP ou HTTPS.

Se o nó exibir um status Amarelo ou Vermelho, ele indicará um problema de replicação ou conectividade que afeta esse nó. Além disso, verifique a contagem de mensagens de replicação exibida nas informações do nó. A contagem de mensagens pendentes deve ser 5.000 ou menos. Uma fila contendo mais de 5.000 mensagens pendentes indica que a fila de replicação foi acumulada, o que pode atrasar ou impedir a replicação bem-sucedida.

2. Verificar o Alarme de Enlace de Fila na Implantação

A replicação bem-sucedida no Cisco ISE depende da disponibilidade e da comunicação do serviço de mensagens RabbitMQ e da estrutura de comunicação de cluster JGroups. Se qualquer componente encontrar problemas de comunicação, o Cisco ISE gera Erros de enlace de fila, que podem interromper a replicação entre os nós de implantação.

Para verificar o status do alarme, navegue até Operations > Dashboard > Alarms e verifique Queue Link Errors nos nós afetados.

Se houver erros de enlace de fila, renove o certificado CA raiz do Cisco ISE, pois falhas de comunicação relacionadas ao certificado geralmente resultam em erros de enlace de fila. Quando o problema do certificado é resolvido, a replicação normalmente é retomada automaticamente sem exigir intervenção adicional.

Note: Consulte a documentação Erros de link de fila do ISE para obter informações detalhadas sobre erros de link de fila.

---

3. Verificar a Latência e a Conectividade da Rede

A replicação do Cisco ISE depende de uma conectividade de rede estável entre os nós de

implantação. A alta latência de rede ou a conectividade intermitente pode atrasar a replicação e pode resultar em falhas de sincronização, particularmente em implantações distribuídas geograficamente.

Verifique a latência de rede entre os nós afetados usando testes de conectividade como ping. Para replicação confiável, a latência de ida e volta entre os nós deve permanecer dentro de aproximadamente 300 ms. A latência que excede consistentemente esse limite pode afetar negativamente o desempenho e a sincronização da replicação. Verifique também se não há interrupções intermitentes da rede, perda de pacotes ou restrições de firewall que afetem a comunicação entre os nós de implantação.

4. Verifique se o certificado ainda não está presente no nó afetado

A replicação de certificado poderá falhar se o certificado que está sendo replicado já existir no nó secundário.

Navegue para Administração > Sistema > Certificados, selecione o nó afetado e verifique se o certificado já está instalado. Se o certificado estiver presente, revise suas propriedades para garantir que ele corresponda ao certificado que está sendo replicado e determine se existem certificados duplicados ou conflitantes.

5. Verificar a Utilização de Recursos do Sistema

A alta utilização de recursos do sistema pode afetar o desempenho do Cisco ISE e atrasar as tarefas de replicação. Uma utilização excessiva de CPU, memória ou disco pode impedir que os processos de replicação sejam concluídos com êxito.

Verifique se o nó afetado tem recursos de sistema suficientes disponíveis e se a utilização de recursos permanece dentro dos limites operacionais recomendados. Se a utilização de recursos for consistentemente alta, aloque recursos adicionais ou reduza a carga de trabalho no nó para restaurar o desempenho de replicação normal.

Note: Consulte o Guia de desempenho e escalabilidade para obter as diretrizes recomendadas de alocação de recursos e dimensionamento de hardware para implantações do Cisco ISE.

---

6. Verificar a Disponibilidade da Porta na Implantação e na Rede

A replicação do Cisco ISE requer que portas TCP específicas permaneçam abertas entre todos

os nós na implantação para garantir comunicação ininterrupta e replicação bem-sucedida. Se qualquer uma dessas portas for bloqueada por um firewall, uma política de controle de acesso ou um dispositivo de rede, poderão ocorrer falhas de replicação ou problemas de sincronização.

Verifique se essas portas TCP estão abertas e acessíveis entre todos os nós do Cisco ISE:

- TCP 443 - comunicação HTTPS
- TCP 8443 - Comunicação administrativa
- TCP 12001 - Comunicação e replicação de cluster JGroups
- TCP 6379 - Serviços de mensagens internas
- TCP 8671 - Mensagens do Cisco ISE (RabbitMQ)

Faça login na CLI do Cisco ISE e execute o comando show ports para verificar as portas mencionadas permitidas no nó.

Confirme se as portas necessárias estão ativadas no nó do Cisco ISE e assegure-se de que sejam permitidas no caminho da rede. Verifique se nenhum firewall intermediário, dispositivo de segurança ou política de rede está bloqueando a comunicação nessas portas entre os nós de implantação.

Coleta de logs para alarmes de replicação

Esses são os componentes comuns que devem ser definidos no modo debug para isolar e solucionar problemas de alarmes de replicação no Cisco ISE.

- Implantação de replicação (replication.log e ise-psc.log)
- Replication-JGroup (replication.log e ise-psc.log)
- Replication Tracker (tracking.log)
- hibernar (hibernate.log)
- JMS (replication.log)

Referência

- Guia do Administrador do Cisco Identity Services Engine, Versão 3.5
- Solucionar problemas e ativar depurações no ISE
- Coletar pacote de suporte no Identity Services Engine

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.