Entender e solucionar problemas de replicações do ISE

Contents

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento do Cisco Identity Services Engine® (ISE).

Componentes Utilizados

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

- Cisco Identity Services Engine 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.

Replicação no Cisco ISE

A replicação no ISE é o processo de sincronização de dados operacionais e de configuração em vários nós em uma implantação para mantê-los consistentes.

O Nó de Administração Principal é responsável por replicar as alterações feitas na implantação para todos os outros nós (secundários) na implantação.

O Cisco ISE usa JGroups, uma estrutura de comunicação de grupo confiável, como parte de sua arquitetura de replicação. O JGroups permite que os nós em uma implantação do ISE se comuniquem entre si e troquem dados de replicação. Ele fornece a estrutura de mensagens que ajuda a fornecer atualizações de configuração e banco de dados entre nós, mantendo a sincronização em toda a implantação.

- O JGroups é uma estrutura de comunicação usada pelo Cisco ISE para replicação; ele não armazena os dados replicados.
- Nem todos os dados no Cisco ISE são replicados por meio de JGroups. Diferentes serviços usam diferentes mecanismos de comunicação com base no tipo de dados que está sendo transferido.
- Se a replicação for temporariamente interrompida, alguns serviços do Cisco ISE podem continuar a operar usando dados disponíveis localmente até que a sincronização seja restaurada.

Exemplos de Métodos de Transferência de Dados

Dados	Método de comunicação

Mensagens de configuração e replicação	JGroups
Suporte à coleta de pacotes	API HTTPS (porta TCP 443)
Configuração de depuração	API HTTPS (porta TCP 443)
Logs ao vivo e relatórios	RabbitMQ ou UDP, dependendo da configuração de implantação

Principais pré-requisitos e verificações de validação para replicação do Cisco ISE

- Resolução DNS: pesquisas de DNS diretas e reversas devem ser resolvidas com êxito para todos os nós do Cisco ISE que participam da implantação. A resolução DNS adequada é necessária para a comunicação de nós e operações de replicação.
- Sincronização de NTP: todos os nós do Cisco ISE devem ser sincronizados com uma origem de NTP confiável para manter o tempo do sistema consistente durante a implantação. A sincronização de horário é essencial para a replicação e validação de certificado.
- Certificados: o certificado Admin instalado em cada nó do Cisco ISE deve ser válido e confiável. Os processos de replicação dependem do certificado Admin para comunicação segura entre nós.
- Requisitos de porta: a conectividade de rede deve permitir a comunicação pelas portas necessárias para serviços de replicação e entre nós:

Serviço	Protocolo/Porta
HTTPS (SOAP)	TCP/443
Sincronização e Replicação de Dados (JGroups)	TCP/12001
Acesso administrativo	TCP/8443

Serviço de mensagens do ISE (SSL)	TCP/8671
Sincronização de propriedade do ponto final do Profiler	TCP/6379

- Acessibilidade de rede: a conectividade de rede entre os nós do Cisco ISE deve ser estável e a latência não deve exceder 300 ms. A verificação da latência e da perda de pacotes entre os nós ajuda a garantir uma replicação confiável.
- Status do enlace da fila: os certificados de mensagens do Cisco ISE são usados para proteger a comunicação entre nós pela porta TCP 8671. Certificados de mensagens inválidos ou corrompidos podem resultar em erros de link de fila e falhas de replicação. Nesses cenários, o certificado da CA raiz do ISE ou os certificados de mensagens do ISE devem ser regenerados conforme apropriado.
- ISE Stunnel Service:O serviço Cisco ISE Stunnel opera em implantações distribuídas e facilita a comunicação segura entre os nós. O serviço deve estar em execução em todos os nós aplicáveis para dar suporte à replicação. O status do serviço pode ser verificado no Cisco ISE CLI usando o comando:
  show tech-support | inclui o atordoamento
- Patch e versão do ISE:o nó primário de administração e o nó de união (nó autônomo) devem ter a mesma versão e o mesmo nível de patch para que o registro do nó e a sincronização funcionem perfeitamente.

Fases de replicação no Cisco ISE

A replicação no Cisco ISE consiste em três fases distintas que funcionam juntas para estabelecer e manter a sincronização em todos os nós na implantação. Cada fase tem uma finalidade específica, começando com a integração do nó, seguida pela sincronização inicial do banco de dados e, finalmente, pela troca contínua de atualizações incrementais para manter todos os nós sincronizados.

- Registro de nó
- Sincronização Completa Ativa
- Sincronização Incremental Ativa

Entender o registro de nós no Cisco ISE

O registro de nó é o processo pelo qual um nó do Cisco ISE ingressa em uma implantação existente e estabelece a comunicação com o PAN (Primary Administration Node, nó primário de

administração).

Durante o registro do nó:

Passo 1: O nó de junção (nó autônomo) inicia a comunicação com o nó de administração principal.

Passo 2: A validação do certificado mútuo é realizada usando o certificado de administração do Cisco ISE.

Passo 3: A resolução DNS, a sincronização NTP, o alcance da rede e a acessibilidade de porta necessária são validados como parte do processo de comunicação.

Passo 4: O Nó principal do administrador verifica se o nó autônomo/nó de união está executando uma versão e um nível de patch compatíveis do Cisco ISE.

Passo 5: Informações de implantação, funções de nó e relações de confiança são trocadas.

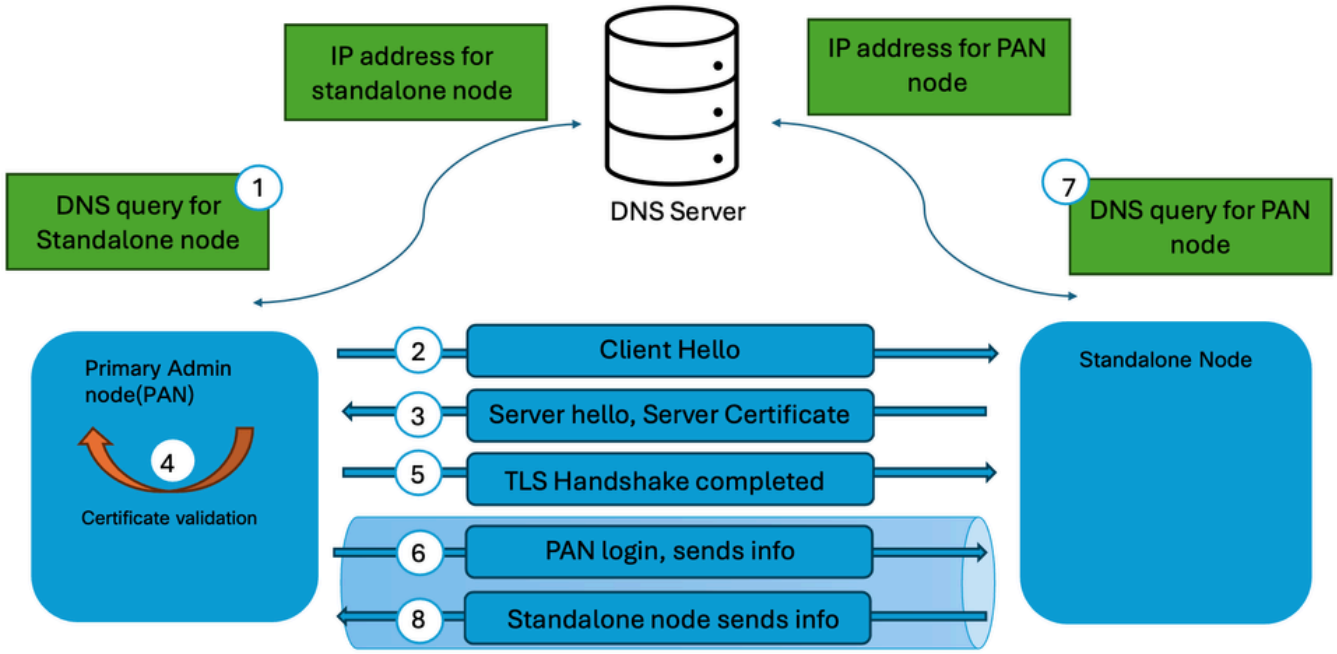
Passo 6: Os serviços de replicação de banco de dados são inicializados e preparados para sincronização.

A conclusão bem-sucedida do registro de nó estabelece o nó como um membro confiável da implantação e permite que os processos de replicação comecem.

Características principais

- Ocorre quando um novo nó é adicionado à implantação.
- Estabelece confiança e canais de comunicação.
- Não transfere imediatamente o banco de dados de configuração completo.
- Serve como pré-requisito para operações de sincronização subsequentes.

Consulte Compreender o processo de registro de nó no Cisco ISE para obter uma explicação detalhada do processo de registro de nó.



Processo de registro do nó

Note: O nó sendo adicionado à implantação deve ser um nó autônomo. Além disso, o PAN (Primary Administration Node, nó primário de administração) deve ter a função de administração principal habilitada na implantação para permitir o registro de nós no Cisco ISE.

Entender a sincronização completa no Cisco ISE

A sincronização completa é um processo completo de replicação de banco de dados no qual todo o banco de dados de configuração é transferido do PAN primário para outro nó. A sincronização completa não transfere apenas registros modificados. Em vez disso, todo o conjunto de dados de configuração é reconstruído no nó receptor.

Uma sincronização completa pode ocorrer em cenários como:

- Sincronização inicial após o registro do nó.
- Recuperação de falhas de replicação.
- Inconsistências significativas no banco de dados.
- Reingressando um nó na implantação.
- Sincronização manual iniciada através dos procedimentos de solução de problemas do Cisco TAC.
- Mecanismos de replicação interna determinando que a sincronização incremental não pode mais restaurar a consistência do banco de dados.

Durante a sincronização completa:

Passo 1: O Nó de Administração Principal prepara um snapshot de banco de dados completo.

Passo 2: Os dados de configuração são empacotados no arquivo .dmp e transmitidos para o nó receptor.

Passo 3: Os dados replicados existentes no nó receptor são validados e atualizados.

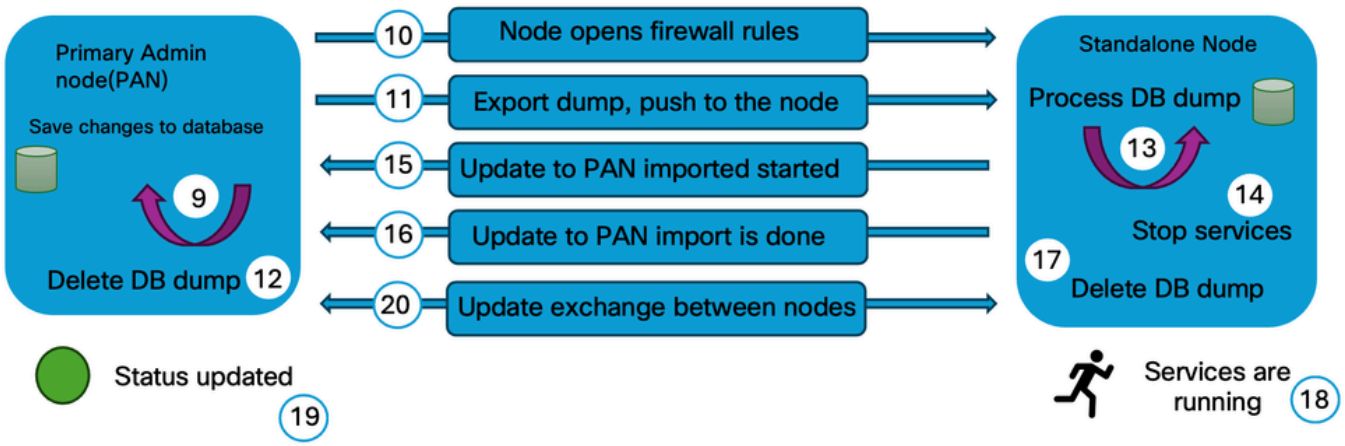
Passo 4: O banco de dados de configuração inteiro é recriado para corresponder ao nó Admin primário.

Passo 5: O status da replicação é verificado após a conclusão.

Como uma sincronização completa envolve significativamente mais dados do que uma sincronização incremental, ela requer tempo de processamento adicional e recursos de rede.

Características da sincronização completa

- Transfere o banco de dados de configuração completo.
- Consome mais largura de banda e recursos do sistema.
- Demora mais do que a sincronização incremental.
- Restaura a consistência do banco de dados quando são detectadas discrepâncias.
- Geralmente ocorre com menos frequência do que a sincronização incremental.



Processo de sincronização completa

Entender a sincronização incremental no Cisco ISE

A sincronização incremental é o mecanismo de replicação contínua usado pelo Cisco ISE para distribuir alterações de configuração depois que os nós tiverem ingressado com êxito na implantação. Quando um administrador faz uma alteração de configuração no PAN, o Cisco ISE não transfere todo o banco de dados. Em vez disso, somente os registros modificados são replicados para os nós do assinante.

Exemplos de alterações replicadas por meio de sincronização incremental incluem:

- Modificações de política
- Adições ou atualizações de dispositivos de rede
- Alterações no grupo de endpoints
- Atualizações de perfil de autorização
- Alterações de configuração relacionadas ao certificado
- Identificar atualizações de configuração de origem

O processo de sincronização incremental opera continuamente e é projetado para manter a consistência em todos os nós, minimizando a utilização da largura de banda e a sobrecarga de replicação.

Benefícios da Sincronização Incremental

- Reduz o tráfego de replicação.
- Minimiza o tempo de sincronização.
- Permite a propagação rápida de alterações de configuração.
- Mantém consistência quase em tempo real em toda a implantação.

Fluxo de Trabalho de Replicação

Passo 1: A alteração de configuração ocorre no nó de administração principal.

Passo 2: A alteração é gravada no banco de dados do Nó de administração primário.

Passo 3: Os serviços de replicação identificam os registros modificados.

Passo 4: O Nó de Administração Principal grava os novos eventos/alterações em uma tabela de

transações.

Passo 5: Segmentos separados do PAN publicam as informações/alterações nos nós secundários na implantação.

Passo 6: Os nós secundários na implantação recebem as alterações do Nó de administração primário.

Passo 7: Os nós secundários na implantação aplicam as alterações recebidas do Nó de administração primário.

Passo 8: O status da replicação é atualizado após a conclusão bem-sucedida.

Em condições normais de operação, a maior parte da atividade de replicação no Cisco ISE ocorre por meio de sincronização incremental.

Note: Se um nó secundário identificar mensagens de replicação ausentes, ele iniciará uma solicitação ao PAN (Primary Administration Node, Nó de Administração Primário) para recuperar as mensagens ausentes e manter a sincronização

---

Visão Geral da Sequência de Replicação e Status de Sincronização

O fluxo de trabalho geral de replicação em uma implantação do Cisco ISE pode ser resumido da seguinte forma:

1. Registro do Nó: Estabelece confiança e adiciona o nó à implantação.

2. Sincronização Completa Inicial: Transfere o banco de dados de configuração completo para o nó recém-registrado.

3. Sincronização Incremental: Propaga continuamente as alterações de configuração em toda a operação normal.

4. Sincronização Completa (Quando necessário): Recria a consistência do banco de dados se forem detectados problemas de replicação ou incompatibilidades de banco de dados.

Essa abordagem em fases permite que o Cisco ISE mantenha um banco de dados de configuração consistente em todos os nós, ao mesmo tempo em que otimiza a utilização da rede e o desempenho da replicação.

Status da Sincronização

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

- Verde - o nó está sincronizado com a implantação e a replicação está funcionando normalmente.
- Amarelo - O nó está fora de sincronização, o registro do nó falhou ou a conectividade do cluster foi perdida (o nó não pôde ser acessado pelo cluster nos últimos cinco minutos).
- Vermelho - o nó está fisicamente inacessível e não pode ser contatado por meio de verificações de conectividade de rede (por exemplo, ping ICMP e HTTPS).

Note: Se a replicação não ocorrer corretamente, você poderá executar a sincronização manual para os nós secundários com o nó de Administração primária efetuando login no Nó de Administração Primário, navegue para Administração > Sistema > Implantação > selecione o nó e clique em Sincronizar.

Replicação de endpoint

A Replicação de endpoint é o processo pelo qual o ISE sincroniza as informações do banco de dados de endpoint em todos os Policy Service Nodes (PSNs) e o Primary Administration Node (PAN) para manter uma exibição consistente da identidade do endpoint em toda a implantação.

- O Cisco ISE mantém um banco de dados de endpoint centralizado que armazena informações sobre dispositivos que se conectam à rede. Essas informações incluem endpoints configurados estaticamente e endpoints aprendidos dinamicamente por meio de autenticação, criação de perfil, avaliação de postura ou integração com fontes de identidade externas.

- Quando as informações de endpoint são criadas ou modificadas, o Cisco ISE replica as alterações em outros nós na implantação. Essa sincronização permite que cada Nó de serviço de política avalie solicitações de autenticação e autorização usando as mesmas informações de ponto final, independentemente de qual PSN processa a solicitação.

- A replicação de endpoint é tratada automaticamente pelo Cisco ISE e faz parte do mecanismo geral de replicação de banco de dados. Os administradores não precisam iniciar manualmente a sincronização de ponto de extremidade durante operações normais.

Como funciona a replicação de endpoint

- Atualização de endpoint: Um endpoint é criado ou atualizado por meio de autenticação, criação de perfil, postura ou configuração manual.
- Detecção de alterações: O Cisco ISE detecta a alteração no endpoint e a prepara para replicação.
- Replicação: As informações atualizadas de endpoint são replicadas para os outros nós na implantação usando a estrutura de replicação do ISE.
- Sincronização de Banco de Dados: Os nós secundários atualizam seu banco de dados de endpoint local com as informações replicadas.
- Aplicação consistente de políticas: Uma vez concluída a sincronização, todos os nós de serviço de política usam as mesmas informações de ponto final para decisões de autenticação e autorização.

A partir do Cisco ISE versão 3.3, os endpoints descobertos dinamicamente não são automaticamente replicados para todos os nós. Este recurso pode ser habilitado ou desabilitado na janela Replicação de Ponto de Extremidade. Navegue para Administração > Sistema > Configurações > Replicação de endpoint, habilite ou desabilite conforme o requisito.

Note: É importante distinguir a replicação de endpoint da replicação de sessão. A replicação de endpoint sincroniza registros persistentes de banco de dados de endpoint (como endereços MAC, grupos de endpoint e informações de criação de perfil), enquanto a replicação de sessão sincroniza as informações de sessão de tempo de execução para dar suporte à aplicação de políticas e à continuidade operacional. Esses mecanismos operam de forma independente e atendem a diferentes funções na arquitetura do Cisco ISE.

Problemas comuns de replicação de nó

Cenário 1: Falha no registro do nó devido a uma falha de resolução de DNS

Falha no registro do nó com o motivo do erro como "o nome do host não pode ser resolvido. Verifique sua configuração DNS".

Etapas para verificar

- Verifique se o servidor DNS válido está configurado no nó de administração primário e no nó autônomo. Verifique a configuração do servidor DNS usando o comando show running-config | incluir servidor de nome
- Valide a resolução de DNS de encaminhamento e reverso no Nó de Administração Primário e no Nó Autônomo usando o comando nslookup FQDN do nó para pesquisa de DNS de encaminhamento e nslookup ip address do nó para pesquisa de DNS reverso.
- Valide a acessibilidade do servidor DNS a partir do nó de administração primário e do nó autônomo usando o comando ping DNS server IP da CLI dos nós do ISE.

Cenário 2: Falha no registro do nó devido à expiração do certificado do administrador

Falha no registro do nó com a razão do erro como "Erro ao carregar certificados. Nó não alcançável no momento. Tente novamente mais tarde".

Etapas para verificar

- Valide os certificados admin do Nó de Administração Primário e do nó Autônomo para garantir a validade e o status do certificado. Navegue até Administration > System > Certificates, selecione o nó e verifique a validade e o status do certificado Admin.
- Se o certificado Admin tiver expirado, substitua ou renove o certificado e verifique se o uso Admin está atribuído.

Cenário 3: Falha no registro do nó devido à incompatibilidade de versão

Falha no registro do nó com o motivo do erro como "incompatibilidade de detalhes de versão/patch".

Etapas para verificar

- Valide a versão do software junto com o patch do nó Admin primário e do nó autônomo usando o comando show version para garantir que os detalhes da versão correspondam.

Componentes para Logs de Depuração

Esses são os componentes comuns que devem ser definidos no modo debug para isolar e solucionar problemas 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)
- ca-service (caservice.log)
- admin-ca (ise-psc.log)

Referência

- Solucionar problemas e ativar depurações no ISE
- ISE - Erro de enlace na fila
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.4
- Guia do Administrador do Cisco Identity Services Engine, Versão 3.5

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.