Comprender y solucionar problemas de réplicas de ISE

Contenido

Introducción

Este documento describe la replicación y su solución de problemas en Cisco Identity Services Engine® (ISE).

Prerequisites

Requirements

Cisco recomienda que conozca Cisco Identity Services Engine® (ISE).

Componentes Utilizados

La información de este documento se basa en estas versiones de hardware y software.

- Cisco Identity Services Engine 3.4 y versiones posteriores.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Replicación en Cisco ISE

La replicación en ISE es el proceso de sincronización de la configuración y los datos operativos entre varios nodos en una implementación para mantenerlos consistentes.

El nodo de administración principal es responsable de replicar los cambios realizados en la implementación en todos los demás nodos (secundarios) de la implementación.

Cisco ISE utiliza JGgroups, un marco de comunicación de grupo fiable, como parte de su arquitectura de replicación. JGgroups permite que los nodos de una implementación de ISE se comuniquen entre sí e intercambien datos de replicación. Proporciona el marco de mensajería que ayuda a ofrecer actualizaciones de la base de datos y la configuración entre nodos, a la vez que mantiene la sincronización a lo largo de la implementación.

- JGgroups es un marco de comunicación utilizado por Cisco ISE para la replicación; no almacena los datos replicados en sí.
- No todos los datos de Cisco ISE se replican a través de JGgroups. Los diferentes servicios utilizan diferentes mecanismos de comunicación en función del tipo de datos que se transfieren.
- Si se interrumpe temporalmente la replicación, algunos servicios de Cisco ISE pueden seguir funcionando con los datos disponibles localmente hasta que se restaure la sincronización.

Ejemplos de métodos de transferencia de datos

Datos	Método de comunicación

Mensajes de configuración y replicación	JGgroups
Admitir recopilación de paquetes	API HTTPS (puerto TCP 443)
Configuración de depuración	API HTTPS (puerto TCP 443)
Registros e informes en directo	RabbitMQ o UDP, dependiendo de la configuración de implementación

Requisitos previos clave y comprobaciones de validación para la replicación de Cisco ISE

- Resolución de DNS: las búsquedas de DNS directo e inverso deben resolverse correctamente para todos los nodos de Cisco ISE que participen en la implementación. Se requiere una resolución DNS adecuada para las operaciones de comunicación y replicación de nodos.
- Sincronización de NTP: todos los nodos de Cisco ISE deben sincronizarse con un origen de NTP fiable para mantener un tiempo del sistema uniforme a lo largo de la implementación. La sincronización horaria es esencial para la replicación y la validación de certificados.
- Certificados: el certificado de administrador instalado en cada nodo de Cisco ISE debe ser válido y de confianza. Los procesos de replicación se basan en el certificado de administrador para la comunicación segura entre nodos.
- Requisitos de puerto: la conectividad de red debe permitir la comunicación a través de los puertos necesarios para la replicación y los servicios entre nodos:

Servicio	Protocolo/puerto
HTTPS (SOAP)	TCP/443
Sincronización y replicación de datos (JGgroups)	TCP/12001
Acceso administrativo	TCP/8443

Servicio de mensajería ISE (SSL)	TCP/8671
Sincronización de propiedad de terminales del analizador	TCP/6379

- Alcance de la red: la conectividad de red entre los nodos Cisco ISE debe ser estable y la latencia no debe superar los 300 ms. La verificación de la latencia y la pérdida de paquetes entre nodos ayuda a garantizar una replicación fiable.
- Estado del enlace de cola: los certificados de mensajería Cisco ISE se utilizan para proteger la comunicación entre nodos a través del puerto TCP 8671. Los certificados de mensajería no válidos o dañados pueden dar lugar a errores de link de cola y errores de replicación. En estos casos, el certificado de CA raíz de ISE o los certificados de mensajería de ISE deben regenerarse según corresponda.
- Servicio de túnel ISE: el servicio de túnel ISE de Cisco funciona en implementaciones distribuidas y facilita la comunicación segura entre nodos. El servicio debe estar ejecutándose en todos los nodos aplicables para admitir la replicación. El estado del servicio se puede verificar desde la CLI de Cisco ISE mediante el comando:
  show tech-support | incluir stunnel
- Parche y versión de ISE: el nodo de administración principal y el nodo de unión (nodo independiente) deben tener la misma versión y el mismo nivel de parche para que el registro y la sincronización del nodo funcionen sin problemas.

Fases de replicación en Cisco ISE

La replicación en Cisco ISE consta de tres fases distintas que se combinan para establecer y mantener la sincronización en todos los nodos de la implementación. Cada fase tiene un propósito específico, que comienza con la incorporación de nodos, seguido de la sincronización inicial de la base de datos y, por último, el intercambio continuo de actualizaciones incrementales para mantener todos los nodos sincronizados.

- Registro de nodos
- Sincronización completa arriba
- Sincronización incremental hacia arriba

Introducción al registro de nodos en Cisco ISE

El registro de nodos es el proceso a través del cual un nodo de Cisco ISE se une a una implementación existente y establece la comunicación con el nodo de administración principal

(PAN).

Durante el registro del nodo:

Paso 1: El nodo de unión (nodo independiente) inicia la comunicación con el nodo de administración principal.

Paso 2: La validación del certificado mutuo se realiza mediante el certificado de administración de Cisco ISE.

Paso 3: Como parte del proceso de comunicación, se validan la resolución DNS, la sincronización NTP, la accesibilidad de la red y la accesibilidad a los puertos necesarios.

Paso 4: El nodo de administración principal verifica que el nodo independiente o el nodo de unión esté ejecutando una versión de Cisco ISE y un nivel de parche compatibles.

Paso 5: Se intercambian información de implementación, funciones de nodo y relaciones de confianza.

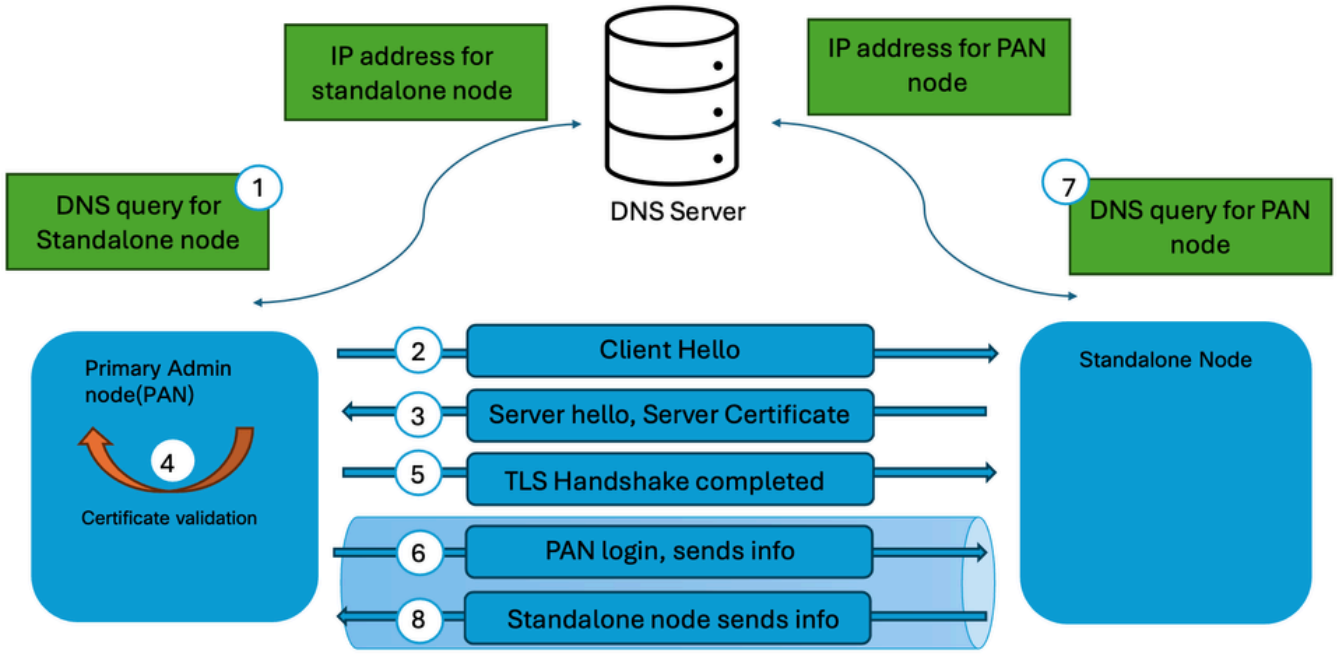
Paso 6: Los servicios de replicación de bases de datos se inicializan y preparan para la sincronización.

La finalización correcta del registro de nodos establece el nodo como miembro de confianza de la implementación y permite que comiencen los procesos de replicación.

Características clave

- Se produce cuando se agrega un nuevo nodo a la implementación.
- Establece canales de confianza y comunicación.
- No transfiere inmediatamente la base de datos de configuración completa.
- Sirve como requisito previo para las operaciones de sincronización posteriores.

Consulte Comprensión del proceso de registro de nodos en Cisco ISE para obtener una explicación detallada del proceso de registro de nodos.



Proceso de registro de nodos

Nota: El nodo que se va a agregar a la implementación debe ser un nodo independiente. Además, el nodo de administración principal (PAN) debe tener la función de administración principal habilitada en la implementación para permitir el registro de nodos en Cisco ISE.

Comprensión de Full Sync en Cisco ISE

La sincronización completa es un proceso de replicación de la base de datos completo en el que toda la base de datos de configuración se transfiere desde el PAN principal a otro nodo. La sincronización completa no transfiere sólo los registros modificados. En su lugar, todo el conjunto de datos de configuración se reconstruye en el nodo receptor.

Una sincronización completa puede ocurrir en escenarios tales como:

- Sincronización inicial después del registro del nodo.
- Recuperación de errores de replicación.
- Incoherencias significativas en la base de datos.
- Volver a unir un nodo a la implementación.
- Sincronización manual iniciada a través de los procedimientos de resolución de problemas de Cisco TAC.
- Mecanismos de replicación interna que determinan que la sincronización incremental ya no puede restaurar la coherencia de la base de datos.

Durante la sincronización completa:

Paso 1: El nodo de administración principal prepara una instantánea completa de la base de datos.

Paso 2: Los datos de configuración se empaquetan en el archivo .dmp y se transmiten al nodo receptor.

Paso 3: Los datos replicados existentes en el nodo de recepción se validan y actualizan.

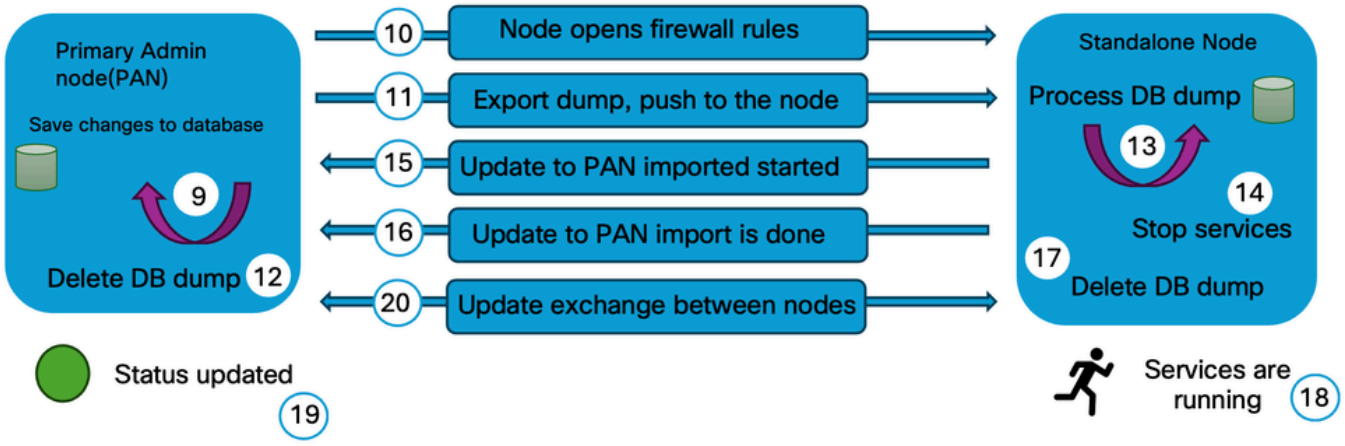
Paso 4: Toda la base de datos de configuración se reconstruye para que coincida con el nodo de administración principal.

Paso 5: El estado de la replicación se verifica al finalizar.

Dado que una sincronización completa implica muchos más datos que una sincronización incremental, requiere tiempo de procesamiento y recursos de red adicionales.

Características de la sincronización completa

- Transfiere la base de datos de configuración completa.
- Consume más ancho de banda y recursos del sistema.
- Lleva más tiempo que la sincronización incremental.
- Restaura la coherencia de la base de datos cuando se detectan discrepancias.
- Suele ocurrir con menos frecuencia que la sincronización incremental.



Proceso de sincronización completa

Comprensión de la sincronización incremental en Cisco ISE

La sincronización incremental es el mecanismo de replicación en curso que utiliza Cisco ISE para distribuir los cambios de configuración después de que los nodos se hayan unido correctamente a la implementación. Cuando un administrador realiza un cambio de configuración en PAN, Cisco ISE no transfiere toda la base de datos. En su lugar, sólo los registros modificados se replican en los nodos del suscriptor.

Entre los ejemplos de cambios replicados a través de la sincronización incremental se incluyen:

- Modificaciones de políticas
- Actualizaciones o adiciones de dispositivos de red
- Cambios del grupo de terminales
- Actualizaciones del perfil de autorización
- Cambios de configuración relacionados con certificados
- Actualizaciones de configuración de origen de identidad

El proceso de sincronización incremental funciona de forma continua y está diseñado para mantener la uniformidad en todos los nodos a la vez que se minimiza la utilización del ancho de banda y la sobrecarga de replicación.

Ventajas de la sincronización incremental

- Reduce el tráfico de replicación.
- Minimiza el tiempo de sincronización
- Permite la propagación rápida de los cambios de configuración.
- Mantiene una uniformidad casi en tiempo real en toda la implementación.

Flujo de trabajo de replicación

Paso 1: El cambio de configuración se produce en el nodo de administración principal.

Paso 2: El cambio se escribe en la base de datos del nodo de administración principal.

Paso 3: Los servicios de replicación identifican los registros modificados.

Paso 4: El nodo de administración principal escribe los nuevos eventos o cambios en una tabla de

transacciones.

Paso 5: Los subprocesos independientes de PAN publican la información o los cambios en los nodos secundarios de la implementación.

Paso 6: Los nodos secundarios de la implementación reciben los cambios del nodo de administración principal.

Paso 7: Los nodos secundarios de la implementación aplican los cambios recibidos del nodo de administración principal.

Paso 8: El estado de replicación se actualiza cuando se completa correctamente.

En condiciones de funcionamiento normales, la mayor parte de la actividad de replicación en Cisco ISE se produce a través de la sincronización incremental.

Nota: Si un nodo secundario identifica mensajes de replicación que faltan, inicia una solicitud al nodo de administración principal (PAN) para recuperar los mensajes que faltan y mantener la sincronización

---

Descripción General de Secuencia de Replicación y Estado de Sincronización

El flujo de trabajo de replicación general en una implementación de Cisco ISE se puede resumir de la siguiente manera:

1. Registro de nodos: Establece la confianza y agrega el nodo a la implementación.

2. Sincronización completa inicial: Transfiere la base de datos de configuración completa al nodo recién registrado.

3. Sincronización incremental: Propaga continuamente los cambios de configuración durante el funcionamiento normal.

4. Sincronización completa (cuando sea necesario): Vuelve a generar coherencia en la base de datos si se detectan problemas de replicación o discrepancias en la base de datos.

Este enfoque por fases permite a Cisco ISE mantener una base de datos de configuración uniforme en todos los nodos a la vez que se optimiza el uso de la red y el rendimiento de la replicación.

Estado de sincronización

El estado de sincronización mostrado para cada nodo indica su estado actual de replicación y conectividad:

- Verde: El nodo está sincronizado con la implementación y la replicación funciona con normalidad.
- Amarillo: el nodo no está sincronizado, el registro del nodo ha fallado o se ha perdido la conectividad del clúster (el clúster no ha podido alcanzar el nodo en los últimos cinco minutos).
- Rojo: el nodo es físicamente inalcanzable y no se puede contactar a través de las comprobaciones de conectividad de red (por ejemplo, ping ICMP y HTTPS).

Nota: Si la replicación no se produce correctamente, puede realizar la sincronización manual con los nodos secundarios con el nodo de administración principal iniciando sesión en el nodo de administración principal, navegue hasta Administración > Sistema > Implementación > seleccione el nodo y haga clic en Sincronizar.

Replicación de terminales

Replicación de terminales es el proceso mediante el cual ISE sincroniza la información de la base de datos de terminales entre todos los nodos de servicios de políticas (PSN) y el nodo de administración principal (PAN) para mantener una vista coherente de la identidad del terminal durante toda la implementación.

- Cisco ISE mantiene una base de datos centralizada de terminales que almacena información sobre los dispositivos que se conectan a la red. Esta información incluye tanto terminales configurados estáticamente como terminales aprendidos dinámicamente a través de la autenticación, la creación de perfiles, la evaluación de estado o la integración con fuentes de identidad externas.
- Cuando se crea o modifica la información del terminal, Cisco ISE replica los cambios en otros nodos de la implementación. Esta sincronización permite que cada nodo de servicio de políticas evalúe las solicitudes de autenticación y autorización utilizando la misma información de terminal, independientemente de qué PSN procese la solicitud.
- Cisco ISE se encarga automáticamente de la replicación de terminales, que forma parte del mecanismo de replicación de bases de datos general. Los administradores no están

obligados a iniciar manualmente la sincronización de terminales durante las operaciones normales.

Cómo Funciona Endpoint Replication

- Actualización de terminales: Un terminal se crea o actualiza mediante autenticación, definición de perfiles, estado o configuración manual.
- Detección de cambios: Cisco ISE detecta el cambio en el terminal y lo prepara para la replicación.
- Replicación: La información de terminales actualizada se replica en los otros nodos de la implementación mediante el marco de replicación de ISE.
- Sincronización de base de datos: Los nodos secundarios actualizan su base de datos de extremos local con la información replicada.
- Aplicación uniforme de políticas: Una vez completada la sincronización, todos los nodos de servicio de políticas utilizan la misma información de terminal para las decisiones de autenticación y autorización.

A partir de Cisco ISE versión 3.3, los terminales detectados dinámicamente no se replican automáticamente en todos los nodos. Esta función se puede habilitar o deshabilitar desde la ventana Replicación de terminales. Vaya a Administration > System > Settings > Endpoint Replication, active o desactive según los requisitos.

Nota: Es importante distinguir la replicación de terminales de la replicación de sesiones. La replicación de terminales sincroniza los registros persistentes de la base de datos de terminales (como las direcciones MAC, los grupos de terminales y la información de perfiles), mientras que la replicación de sesiones sincroniza la información de sesiones en tiempo de ejecución para permitir la aplicación de políticas y la continuidad operativa. Estos mecanismos funcionan de forma independiente y cumplen diferentes funciones dentro de la arquitectura de Cisco ISE.

Problemas Comunes de Replicación de Nodo

Escenario 1: Error en el registro del nodo debido a un error de resolución DNS

Error al registrar el nodo debido al motivo del error "no se puede resolver el nombre de host. Compruebe la configuración de DNS".

Pasos para verificar

- Asegúrese de que el servidor DNS válido esté configurado en el nodo de administración principal y en el nodo independiente. Verifique la configuración del servidor DNS mediante el comando show running-config | include name-server
- Valide la resolución de DNS directo e inverso en el nodo de administración principal y el nodo independiente mediante el comando nslookup FQDN del nodo para la búsqueda de DNS directo y la dirección ip nslookup del nodo para la búsqueda de DNS inversa.
- Valide la disponibilidad del servidor DNS desde el nodo de administración principal y el nodo independiente mediante el comando ping DNS server IP desde la CLI de los nodos ISE.

Escenario 2: Error al registrar el nodo debido al vencimiento del certificado de administrador

Error al registrar el nodo con el motivo del error "Error al cargar certificados. No se puede alcanzar el nodo en este momento. Inténtelo de nuevo más tarde".

Pasos para verificar

- Valide los certificados de administrador del nodo de administración principal y del nodo independiente para garantizar la validez y el estado del certificado. Vaya a Administration > System > Certificates, seleccione el nodo y verifique la validez y el estado del certificado de administración.
- Si el certificado de administrador ha caducado, reemplace o renueve el certificado y asegúrese de que se ha asignado el uso de administrador.

Escenario 3: Error de registro de nodo debido a discordancia de versión

Error al registrar el nodo; el motivo del error es "discrepancia de los detalles de la versión/parche".

Pasos para verificar

- Valide la versión del software junto con el parche del nodo de administración principal y el nodo independiente mediante el comando show version para asegurarse de que los detalles de la versión coinciden.

Componentes para registros de depuración

Estos son los componentes comunes que se configurarán en el modo debug para aislar y resolver problemas de replicación en Cisco ISE.

- Replicación-Implementación (replication.log e ise-psc.log)
- Replication-JGroup (replication.log y ise-psc.log)
- Rastreador de replicación (tracking.log)
- hibernar (hibernate.log)
- JMS (replication.log)
- ca-service (caservice.log)
- admin-ca (ise-psc.log)

Referencia

- Solucionar problemas y habilitar depuraciones en ISE
- ISE: error de enlace de cola
- Guía del administrador de Cisco Identity Services Engine, versión 3.4
- Guía del administrador de Cisco Identity Services Engine, versión 3.5

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).