Comprensión y solución de problemas de alarmas de replicación de certificados ISE

Contenido

Introducción

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

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre 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® (ISE) 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.

Alarma de replicación

Las alarmas de replicación de Cisco ISE proporcionan visibilidad del estado y el estado de sincronización del marco de replicación en toda la implementación. Estas alarmas ayudan a identificar las condiciones que pueden afectar a la coherencia de los datos, la comunicación de los nodos o los procesos de replicación, lo que permite a los administradores detectar y resolver problemas antes de que afecten a las operaciones del sistema. Comprender el propósito y la importancia de las alarmas de replicación es esencial para mantener una implementación de ISE saludable y garantizar que la configuración y los datos operativos permanezcan sincronizados en todos los nodos.

Alarmas de replicación de certificados ISE

Error de replicación de certificados

La alarma Certificate Replication Failed se genera cuando Cisco ISE no puede replicar los datos relacionados con el certificado del nodo de administración principal (PAN) en uno o más nodos de la implementación. ISE replica automáticamente los certificados y su configuración asociada siempre que se importen, generen, renueven o modifiquen certificados en el PAN principal para mantener la coherencia en todos los nodos. Esta alarma indica que el proceso de replicación no se realizó correctamente, lo que produjo una configuración de certificado incoherente en los nodos afectados.

Motivo de la alarma

La alarma Certificate Replication Failed puede producirse cuando Cisco ISE no puede transferir, validar o instalar correctamente los datos relacionados con el certificado en uno o más nodos. Las causas comunes incluyen

- Problemas de comunicación de red: La pérdida de paquetes, la alta latencia de red, las restricciones del firewall que bloquean el tráfico de replicación, los problemas de routing

entre nodos ISE o una discordancia de MTU que provoca la fragmentación o el descarte de paquetes pueden interrumpir la replicación de certificados.
- Problemas con el servicio de replicación: La replicación de certificados puede fallar si RabbitMQ, JGgroups u otros servicios de replicación interna no están disponibles, se están reiniciando o no funcionan correctamente.
- Fallos de validación de certificados: La replicación puede fallar si la cadena de certificados está incompleta, faltan certificados de CA o intermedios, el certificado ha caducado o está dañado, o contiene un uso de clave no admitido o un formato no válido.
- Problemas de comunicación del nodo: Si el nodo de destino está desconectado, reiniciando, anulando el registro, desconectado de la implementación o inaccesible, no se puede completar la replicación de certificados.
- Espacio en disco insuficiente: El nodo de destino no tiene suficiente espacio en disco disponible para importar e instalar el certificado replicado.
- Problemas internos de la base de datos: La replicación puede fallar si la base de datos de configuración de ISE no puede almacenar o actualizar los metadatos del certificado.

Impacto de la alarma

El impacto de esta alarma depende del tipo de certificado que se replica y de los servicios que dependen de él. La replicación de certificados fallida puede dar lugar a una configuración de certificados incoherente en los nodos ISE, discrepancias de certificados HTTPS, errores de autenticación EAP, problemas de establecimiento de confianza pxGrid, errores de inscripción SCEP o de aprovisionamiento de certificados, incoherencias en el almacén de certificados de confianza y errores de validación TLS con integraciones externas.

Error temporal de replicación de certificados

La alarma de error temporal de replicación de certificados se genera cuando Cisco ISE no puede replicar temporalmente los datos relacionados con certificados desde el nodo de administración principal (PAN) a uno o más nodos de la implementación. A diferencia de la alarma Certificate Replication Failed, esta alarma indica que la falla de replicación se considera transitoria, y Cisco ISE reintenta automáticamente la operación de replicación cuando se resuelve la condición subyacente.

Motivo de la alarma

La alarma suele generarse debido a condiciones transitorias que impiden temporalmente la replicación de certificados. Las causas comunes incluyen:

- Problemas de comunicación de red temporal: Breves interrupciones de red, pérdida de paquetes, alta latencia, retrasos del firewall o problemas de routing temporales entre nodos

ISE.
- Inicialización o reinicio del servicio de replicación: RabbitMQ, JGgroups u otros servicios de replicación interna se están reiniciando o no están disponibles temporalmente.
- No disponibilidad del nodo temporal: El nodo de destino se está iniciando, reiniciando los servicios de aplicación, volviendo a unirse a la implementación o está temporalmente inaccesible.
- Restricciones temporales de recursos del sistema: La alta utilización de la CPU, la presión de la memoria o la contención de E/S del disco retrasan temporalmente el procesamiento de replicación.
- Operaciones administrativas simultáneas: La replicación de certificados se puede retrasar mientras la importación, copia de seguridad, restauración, instalación de parches o sincronización de la implementación de otro certificado está en curso.
- Retrasos de la cola de replicación o base de datos temporal: Las operaciones de base de datos internas o las colas de replicación están temporalmente ocupadas procesando otras solicitudes de sincronización.

Impacto de la alarma

En la mayoría de los casos, esta alarma tiene un impacto operativo mínimo porque Cisco ISE reintenta automáticamente la operación de replicación. Sin embargo, hasta que la replicación se complete correctamente, pueden existir incoherencias temporales entre los nodos, entre las que se incluyen:

- Propagación retrasada de certificados recién importados o renovados
- Discordancia de configuración de certificado temporal en la implementación
- Disponibilidad retrasada de los servicios basados en certificados en el nodo afectado
- Retrasos temporales en los servicios HTTPS, EAP, pxGrid o SCEP si dependen del certificado replicado

Si la alarma persiste o se produce repetidamente, conduce a la alarma Certificate Replication Failed .

Solucionar problemas de alarmas de replicación de certificados ISE

Estos son los factores comunes que se deben verificar al resolver problemas o verificar las alarmas de replicación de certificados en ISE.

1. Compruebe el estado de implementación del nodo

Para que la replicación de certificados se realice correctamente, el nodo secundario debe estar en el estado Conectado dentro de la implementación de Cisco ISE. Vaya a Administration > System > Deployment y verifique el estado del nodo afectado. Pase el cursor sobre el icono Information (i) situado junto al estado del nodo para revisar los detalles de sincronización y cualquier mensaje de replicación pendiente.

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. Este estado indica que el clúster no ha podido alcanzar el nodo en los últimos cinco minutos.
- Rojo: el nodo es inalcanzable y no se puede establecer contacto con él mediante comprobaciones de conectividad de red, como ping ICMP o HTTPS.

Si el nodo muestra un estado Amarillo o Rojo, indica un problema de replicación o conectividad que afecta a ese nodo. Además, compruebe el recuento de mensajes de replicación que se muestra en la información del nodo. El recuento de mensajes pendientes debe ser 5000 o menos. Una cola que contiene más de 5.000 mensajes pendientes indica que la cola de replicación se ha acumulado, lo que puede retrasar o impedir la replicación correcta.

2. Verifique la alarma de link de cola en la implementación

La replicación correcta en Cisco ISE depende de la disponibilidad y la comunicación del servicio de mensajería RabbitMQ y del marco de comunicación del clúster JGgroups. Si alguno de los componentes encuentra problemas de comunicación, Cisco ISE genera Errores de enlace de cola, que pueden interrumpir la replicación entre los nodos de implementación.

Para verificar el estado de alarma, navegue hasta Operaciones > Panel > Alarmas y verifique si hay Errores de Link de Cola en los nodos afectados.

Si hay errores de enlace de cola, renueve el certificado de CA raíz de Cisco ISE, ya que los errores de comunicación relacionados con el certificado suelen dar lugar a errores de enlace de cola. Una vez resuelto el problema del certificado, la replicación suele reanudarse automáticamente sin necesidad de intervención adicional.

Nota: Consulte la documentación de Errores de Link de Cola ISE para obtener información detallada sobre los Errores de Link de Cola.

---

3. Verificar la latencia y conectividad de la red

La replicación de Cisco ISE se basa en una conectividad de red estable entre nodos de implementación. La alta latencia de red o la conectividad intermitente pueden retrasar la replicación y provocar fallos de sincronización, especialmente en implementaciones distribuidas geográficamente.

Verifique la latencia de red entre los nodos afectados mediante pruebas de conectividad como ping. Para una replicación confiable, la latencia de ida y vuelta entre los nodos debe permanecer dentro de aproximadamente 300 ms. La latencia que supere constantemente este umbral puede afectar negativamente al rendimiento y la sincronización de la replicación.Compruebe también que no haya interrupciones intermitentes en la red, pérdida de paquetes o restricciones de firewall que afecten a la comunicación entre los nodos de implementación.

4. Compruebe que el certificado no está ya presente en el nodo afectado

La replicación de certificados puede fallar si el certificado que se está replicando ya existe en el nodo secundario.

Vaya a Administration > System > Certificates, seleccione el nodo afectado y verifique si el certificado ya está instalado. Si el certificado está presente, revise sus propiedades para asegurarse de que coincide con el certificado que se está replicando y determinar si existen certificados duplicados o en conflicto.

5. Verificar la utilización de los recursos del sistema

La alta utilización de recursos del sistema puede afectar al rendimiento de Cisco ISE y retrasar las tareas de replicación. Un uso excesivo de la CPU, la memoria o el disco puede impedir que los procesos de replicación se completen correctamente.

Verifique que el nodo afectado tenga suficientes recursos del sistema disponibles y que la utilización de los recursos se mantenga dentro de los límites operativos recomendados. Si la utilización de recursos es siempre alta, asigne recursos adicionales o reduzca la carga de trabajo en el nodo para restaurar el rendimiento normal de replicación.

Nota: Consulte la Guía de rendimiento y escalabilidad para ver las directrices recomendadas de asignación de recursos y tamaño de hardware para las implementaciones de Cisco ISE.

---

6. Verificar la disponibilidad de los puertos en la implementación y la red

La replicación de Cisco ISE requiere que determinados puertos TCP permanezcan abiertos entre todos los nodos de la implementación para garantizar una comunicación ininterrumpida y una replicación correcta. Si alguno de estos puertos está bloqueado por un firewall, una directiva de control de acceso o un dispositivo de red, pueden producirse errores de replicación o problemas de sincronización.

Verifique que estos puertos TCP estén abiertos y sean accesibles entre todos los nodos de Cisco ISE:

- TCP 443: comunicación HTTPS
- TCP 8443: comunicación administrativa
- TCP 12001: comunicación y replicación del clúster de JGgroups
- TCP 6379: servicios de mensajería interna
- TCP 8671: mensajería Cisco ISE (RabbitMQ)

Inicie sesión en la CLI de Cisco ISE y ejecute el comando show ports para verificar los puertos mencionados permitidos en el nodo.

Confirme que los puertos requeridos están habilitados en el nodo Cisco ISE y asegúrese de que estén permitidos a través de la trayectoria de red. Verifique que ningún firewall intermedio, dispositivo de seguridad o política de red esté bloqueando la comunicación en estos puertos entre los nodos de implementación.

Recopilación de registros para alarmas de replicación

Estos son los componentes comunes que se deben configurar en el modo debug para aislar y resolver problemas de alarmas 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)

Referencia

- Guía del administrador de Cisco Identity Services Engine, versión 3.5
- Solucionar problemas y habilitar depuraciones en ISE
- Recopile el paquete de asistencia en Identity Services Engine

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).