Comprendre et dépanner les alarmes de réplication de certificat ISE

Table des matières

Introduction

Ce document décrit les alarmes de réplication et leur dépannage dans Cisco Identity Services Engine® (ISE).

Conditions préalables

Exigences

Cisco recommande que vous ayez des connaissances sur Cisco Identity Services Engine® (ISE).

Composants utilisés

Les informations contenues dans ce document sont basées sur ces versions matérielles et logicielles.

- Cisco Identity Services Engine® (ISE) 3.4 et versions ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Alarme de réplication

Les alarmes de réplication dans Cisco ISE offrent une visibilité sur l'état de santé et de synchronisation de l'infrastructure de réplication à travers le déploiement. Ces alarmes permettent d'identifier les conditions susceptibles d'affecter la cohérence des données, la communication entre les noeuds ou les processus de réplication, ce qui permet aux administrateurs de détecter et de résoudre les problèmes avant qu'ils n'affectent le fonctionnement du système. Il est essentiel de comprendre l'objectif et l'importance des alarmes de réplication pour maintenir un déploiement ISE sain et garantir que les données de configuration et d'exploitation restent synchronisées sur tous les noeuds.

Alarmes de réplication de certificats ISE

Échec de la réplication du certificat

L'alarme Échec de la réplication de certificat est générée lorsque Cisco ISE ne parvient pas à répliquer les données liées au certificat à partir du noeud d'administration principal (PAN) vers un ou plusieurs noeuds dans le déploiement. ISE réplique automatiquement les certificats et leur configuration associée chaque fois que des certificats sont importés, générés, renouvelés ou modifiés sur le PAN principal afin de maintenir la cohérence sur tous les noeuds. Cette alarme indique que le processus de réplication a échoué, ce qui a entraîné une configuration de certificat incohérente sur le ou les noeuds affectés.

Motif de l'alarme

L'alarme Échec de la réplication de certificat peut se produire lorsque Cisco ISE ne parvient pas à transférer, valider ou installer les données relatives au certificat sur un ou plusieurs noeuds. Causes courantes :

- Problèmes de communication réseau : La perte de paquets, la latence élevée du réseau, les restrictions de pare-feu bloquant le trafic de réplication, les problèmes de routage entre les noeuds ISE ou une non-concordance de MTU provoquant la fragmentation ou l'abandon des

paquets peuvent interrompre la réplication des certificats.
- Problèmes de service de réplication : La réplication de certificat peut échouer si RabbitMQ, JGroups ou d'autres services de réplication internes ne sont pas disponibles, redémarrent ou ne fonctionnent pas correctement.
- Échecs de validation de certificat : La réplication peut échouer si la chaîne de certificats est incomplète, si des certificats d'autorité de certification ou intermédiaires sont manquants, si le certificat a expiré ou est endommagé, ou s'il contient une utilisation de clé non prise en charge ou un format non valide.
- Problèmes de communication du noeud : Si le noeud de destination est hors connexion, redémarrage, désinscription, déconnexion du déploiement ou inaccessible, la réplication de certificat ne peut pas être terminée.
- Espace disque insuffisant : L'espace disque disponible sur le noeud de destination est insuffisant pour importer et installer le certificat répliqué.
- Problèmes de base de données interne : La réplication peut échouer si la base de données de configuration ISE ne parvient pas à stocker ou à mettre à jour les métadonnées de certificat.

Impact de l'alarme

L'impact de cette alarme dépend du type de certificat répliqué et des services qui en dépendent. Une réplication de certificat défaillante peut entraîner une configuration de certificat incohérente sur les noeuds ISE, des incohérences dans les certificats HTTPS, des échecs d'authentification EAP, des problèmes d'établissement d'approbation pxGrid, des échecs d'inscription ou d'approvisionnement de certificat SCEP, des incohérences dans le magasin de certificats approuvés et des échecs de validation TLS avec des intégrations externes.

Échec temporaire de la réplication de certificat

L'alarme Échec temporaire de la réplication de certificat est générée lorsque Cisco ISE est temporairement incapable de répliquer les données liées au certificat à partir du noeud d'administration principal (PAN) vers un ou plusieurs noeuds du déploiement. Contrairement à l'alarme Échec de la réplication de certificat, cette alarme indique que l'échec de la réplication est considéré comme temporaire et Cisco ISE relance automatiquement l'opération de réplication lorsque la condition sous-jacente est résolue.

Motif de l'alarme

L'alarme est généralement générée en raison de conditions transitoires qui empêchent temporairement la réplication du certificat. Causes courantes :

- Problèmes de communication réseau temporaires : Brèves interruptions du réseau, perte de

paquets, latence élevée, retards de pare-feu ou problèmes de routage temporaire entre les noeuds ISE.
- Initialisation ou redémarrage du service de réplication : RabbitMQ, JGroups ou d'autres services de réplication internes redémarrent ou sont temporairement indisponibles.
- Indisponibilité temporaire du noeud : Le noeud de destination démarre, redémarre les services d'application, rejoint le déploiement ou est temporairement inaccessible.
- Contraintes de ressources système temporaires : Une utilisation CPU élevée, une pression de mémoire ou un conflit d'E/S sur disque retardent temporairement le traitement de réplication.
- Opérations administratives simultanées : La réplication des certificats peut être retardée pendant qu'une autre importation, sauvegarde, restauration, installation de correctifs ou synchronisation du déploiement de certificats est en cours.
- Délais de base de données temporaire ou de file de réplication : Les opérations de base de données internes ou les files d'attente de réplication traitent temporairement d'autres demandes de synchronisation.

Impact de l'alarme

Dans la plupart des cas, cette alarme a un impact minimal sur le fonctionnement, car Cisco ISE tente automatiquement à nouveau l'opération de réplication. Cependant, tant que la réplication n'est pas terminée, des incohérences temporaires peuvent exister entre les noeuds, notamment :

- Propagation retardée de certificats nouvellement importés ou renouvelés
- Non-concordance de configuration de certificat temporaire sur le déploiement
- Disponibilité retardée des services basés sur des certificats sur le noeud affecté
- Délais temporaires dans les services HTTPS, EAP, pxGrid ou SCEP s'ils dépendent du certificat répliqué

Si l'alarme persiste ou se produit à plusieurs reprises, elle entraîne l'alarme Échec de la réplication de certificat.

Dépannage des alarmes de réplication de certificats ISE

Il s'agit des facteurs courants à vérifier lors du dépannage ou de la vérification des alarmes de réplication de certificat dans ISE.

1. Vérification de l'état de déploiement du noeud

Pour que la réplication de certificat réussisse, le noeud secondaire doit être dans un état Connected dans le déploiement Cisco ISE. Accédez à Administration > System > Deployment et vérifiez l'état du noeud affecté. Passez le curseur sur l'icône Information (i) en regard de l'état du

noeud pour examiner les détails de la synchronisation et les messages de réplication en attente.

L'état de synchronisation affiché pour chaque noeud indique son état actuel de réplication et de connectivité :

- Vert : le noeud est synchronisé avec le déploiement et la réplication fonctionne normalement.
- Jaune : le noeud n'est pas synchronisé, l'enregistrement du noeud a échoué ou la connectivité du cluster a été perdue. Cet état indique que le noeud n'est pas accessible par le cluster depuis les cinq dernières minutes.
- Rouge - Le noeud est inaccessible et ne peut pas être contacté par le biais de vérifications de connectivité réseau, telles que la requête ping ICMP ou HTTPS.

Si le noeud affiche un état Jaune ou Rouge, il indique un problème de réplication ou de connectivité affectant ce noeud. Vérifiez également le nombre de messages de réplication affichés dans les informations du noeud. Le nombre de messages en attente doit être inférieur ou égal à 5 000. Une file d'attente contenant plus de 5 000 messages en attente indique que la file d'attente de réplication s'est accumulée, ce qui peut retarder ou empêcher la réplication.

2. Vérification de l'alarme de liaison de file d'attente dans le déploiement

La réussite de la réplication dans Cisco ISE dépend de la disponibilité et de la communication du service de messagerie RabbitMQ et de l'infrastructure de communication de cluster JGroups. Si l'un des composants rencontre des problèmes de communication, Cisco ISE génère des erreurs de liaison de file d'attente, qui peuvent interrompre la réplication entre les noeuds de déploiement.

Pour vérifier l'état de l'alarme, accédez à Operations > Dashboard > Alarms et vérifiez les erreurs de liaison de file d'attente sur les noeuds affectés.

Si des erreurs de liaison de file d'attente sont présentes, renouvelez le certificat CA racine Cisco ISE, car les échecs de communication liés au certificat entraînent généralement des erreurs de liaison de file d'attente. Une fois le problème de certificat résolu, la réplication reprend généralement automatiquement sans nécessiter d'intervention supplémentaire.

Remarque : Référez-vous à la documentation Erreurs de liaison de file d'attente ISE pour des informations détaillées sur les erreurs de liaison de file d'attente.

---

3. Vérification de la latence et de la connectivité du réseau

La réplication Cisco ISE repose sur une connectivité réseau stable entre les noeuds de déploiement. Une latence réseau élevée ou une connectivité intermittente peuvent retarder la réplication et entraîner des échecs de synchronisation, en particulier dans les déploiements géographiquement dispersés.

Vérifiez la latence du réseau entre les noeuds affectés à l'aide de tests de connectivité tels que ping. Pour une réplication fiable, la latence aller-retour entre les noeuds doit rester dans un délai d'environ 300 ms. Le dépassement constant de ce seuil peut nuire aux performances de réplication et à la synchronisation.Vérifiez également qu'il n'y a pas de pannes réseau intermittentes, de perte de paquets ou de restrictions de pare-feu affectant la communication entre les noeuds de déploiement.

4. Vérifiez que le certificat n'est pas déjà présent sur le noeud affecté

La réplication de certificat peut échouer si le certificat en cours de réplication existe déjà sur le noeud secondaire.

Accédez à Administration > System > Certificates, sélectionnez le noeud affecté et vérifiez si le certificat est déjà installé. Si le certificat est présent, vérifiez ses propriétés pour vous assurer qu'il correspond au certificat en cours de réplication et déterminez s'il existe des certificats en double ou en conflit.

5. Vérifier l'utilisation des ressources système

Une utilisation élevée des ressources système peut affecter les performances de Cisco ISE et retarder les tâches de réplication. Une utilisation excessive du processeur, de la mémoire ou du disque peut empêcher la réussite des processus de réplication.

Vérifiez que le noeud affecté dispose de suffisamment de ressources système disponibles et que l'utilisation des ressources reste dans les limites de fonctionnement recommandées. Si l'utilisation des ressources est constamment élevée, allouez des ressources supplémentaires ou réduisez la charge de travail sur le noeud pour restaurer les performances normales de réplication.

Remarque : Reportez-vous au Guide de performance et d'évolutivité pour les directives recommandées concernant le dimensionnement du matériel et l'allocation des ressources pour les déploiements Cisco ISE.

---

6. Vérification de la disponibilité des ports dans le déploiement et le réseau

La réplication Cisco ISE nécessite que des ports TCP spécifiques restent ouverts entre tous les noeuds du déploiement pour garantir une communication ininterrompue et une réplication réussie. Si l'un de ces ports est bloqué par un pare-feu, une stratégie de contrôle d'accès ou un périphérique réseau, des échecs de réplication ou des problèmes de synchronisation peuvent se produire.

Vérifiez que ces ports TCP sont ouverts et accessibles entre tous les noeuds Cisco ISE :

- TCP 443 - Communication HTTPS
- TCP 8443 - Communication administrative
- TCP 1201 - Communication et réplication de cluster JGroups
- TCP 6379 - Services de messagerie internes
- TCP 8671 - Messagerie Cisco ISE (RabbitMQ)

Connectez-vous à l'interface de ligne de commande Cisco ISE et exécutez la commande show ports pour vérifier les ports mentionnés autorisés dans le noeud.

Vérifiez que les ports requis sont activés sur le noeud Cisco ISE et assurez-vous qu'ils sont autorisés sur le chemin réseau. Vérifiez qu'aucun pare-feu intermédiaire, périphérique de sécurité ou stratégie réseau ne bloque la communication sur ces ports entre les noeuds de déploiement.

Collecte des journaux pour les alarmes de réplication

Il s'agit des composants communs qui doivent être définis en mode debug pour isoler et dépanner les alarmes de réplication dans Cisco ISE.

- Replication-Deployment (replication.log et ise-psc.log)
- Replication-JGroup (replication.log et ise-psc.log)
- Replication Tracker (tracking.log)
- hibernate (hibernate.log)
- JMS (replication.log)

Référence

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.5
- Dépannage et activation des débogages sur ISE
- Collecter l'offre groupée d'assistance sur Identity Services Engine

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.