Comprendre et dépanner les alarmes de réplication de noeud ISE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Alarmes de réplication ISE
- Alarmes de réplication de noeud ISE
  - Échec de la réplication
    - Motif de l'alarme
    - Impact de l'alarme
  - Réplication arrêtée
    - Motif de l'alarme
    - Impact de l'alarme
    - Dépannage de la réplication en échec et alarme de réplication arrêtée
  - Alarme de réplication lente
    - Motif de l'alarme
    - Alarme de réplication lente - Informations
    - Alarme de réplication lente - Avertissement
    - Alarme de réplication lente - Erreur
- Dépannage des alarmes de réplication de noeud
- Collecte des journaux pour les alarmes de réplication
- Référence

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.

Alarmes de réplication ISE

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 noeud ISE

Échec de la réplication

L'alarme Échec de la réplication est générée lorsque les noeuds secondaires du déploiement ne peuvent pas consommer les messages répliqués par le noeud Administration principale dans le déploiement. Cette alarme indique que le processus de réplication a échoué et que le noeud affecté ne dispose plus de la dernière configuration ou des dernières données opérationnelles.

Contrairement aux alarmes de réplication spécifiques aux certificats, cette alarme représente une défaillance dans le cadre de réplication général et peut avoir un impact sur plusieurs objets et services de configuration à travers le déploiement.

Motif de l'alarme

L'alarme Échec de la réplication peut se produire lorsque Cisco ISE ne parvient pas à transférer ou à appliquer les données répliquées. Causes courantes :

- Problèmes de communication réseau : Perte de paquets, latence réseau élevée, restrictions de pare-feu, problèmes de routage ou non-concordance des MTU perturbant la communication entre les noeuds ISE.
- Problèmes de service de réplication : RabbitMQ, JGroups ou d'autres services de réplication internes ne sont pas disponibles, redémarrent ou ne fonctionnent pas correctement.
- Problèmes de communication du noeud : Le noeud de destination est hors ligne, redémarre, désinscrit, déconnecté du déploiement ou inaccessible.
- Problèmes de synchronisation de base de données : Le noeud de destination ne peut pas valider les données répliquées en raison d'erreurs de base de données ou d'échecs de synchronisation.
- Contraintes de ressources système : Utilisation CPU élevée, pression de mémoire, espace disque insuffisant ou E/S disque lourdes retardant le traitement de réplication.
- Problèmes de résolution DNS ou de nom d’hôte : Résolution DNS incorrecte, avant ou arrière, empêchant la communication entre les noeuds.
- Incohérences de version ou de déploiement : La réplication échoue si les noeuds ne fonctionnent pas sur des versions logicielles prises en charge ou si le déploiement est dans un état incohérent après une mise à niveau ou un enregistrement de noeud.
- Expiration du certificat d'administration : le certificat d'administration des noeuds ISE a expiré, est endommagé ou non valide, ce qui entraîne l'échec de la réplication.
- Queue Link Errors : le déploiement ou les noeuds affectés affichent les erreurs de liaison de file d'attente où le certificat de messagerie ISE / la chaîne d'autorité de certification racine ISE est endommagé ou non valide sur le port 8671.
- Le service Stunnel est désactivé / hors ligne : le service Stunnel s'exécute sur tous les noeuds du déploiement distribué. L'état Désactivé/Non en cours d'exécution du service Stunnel entraîne l'échec des alarmes de réplication.
- Les ports de réplication sont bloqués : les ports 12001, 8671, 443, 8443 et 6379 doivent être ouverts entre les noeuds du déploiement et le réseau pour que les procédures de réplication du déploiement soient transparentes.

Impact de l'alarme

L'impact dépend du type de données répliquées. Les pannes de réplication peuvent entraîner une configuration incohérente sur les noeuds ISE, une propagation retardée des modifications administratives, des politiques obsolètes, des périphériques réseau manquants ou des

informations d'identité, des pannes de synchronisation des certificats et des données de point d'extrémité incohérentes. Si la réplication reste infructueuse pendant une période prolongée, les opérations administratives et la cohérence des politiques sur l'ensemble du déploiement peuvent être affectées.

Réplication arrêtée

L'alarme « Réplication arrêtée » est générée lorsque le noeud d'administration principal n'est pas en mesure de répliquer les informations sur les noeuds secondaires du déploiement. Cette alarme indique que le processus de réplication a échoué et que le ou les noeuds affectés ne disposent plus de la dernière configuration ou des dernières données opérationnelles.

Motif de l'alarme

L'alarme « Réplication arrêtée » peut se produire lorsque le noeud d'administration principal ne parvient pas à transférer les données répliquées. Causes courantes :

- Problèmes de communication réseau : Perte de paquets, latence réseau élevée, restrictions de pare-feu, problèmes de routage ou non-concordance des MTU perturbant la communication entre les noeuds ISE.
- Problèmes de service de réplication : RabbitMQ, JGroups ou d'autres services de réplication internes ne sont pas disponibles, redémarrent ou ne fonctionnent pas correctement dans le noeud Administration principale.
- Contraintes de ressources système : Utilisation CPU élevée, pression de mémoire, espace disque insuffisant ou E/S disque lourdes retardant le traitement de réplication dans le noeud d'administration principal.
- Problèmes de résolution DNS ou de nom d’hôte : Résolution DNS incorrecte, avant ou arrière, empêchant la communication entre les noeuds.
- Incohérences de version ou de déploiement : La réplication échoue si les noeuds ne fonctionnent pas sur des versions logicielles prises en charge ou si le déploiement est dans un état incohérent après une mise à niveau ou un enregistrement de noeud.
- Expiration du certificat d'administration : le certificat d'administration des noeuds ISE a expiré, est endommagé ou non valide, ce qui entraîne l'échec de la réplication.
- Queue Link Errors : le déploiement ou les noeuds affectés affichent les erreurs de liaison de file d'attente où le certificat de messagerie ISE / la chaîne d'autorité de certification racine ISE est endommagé ou non valide sur le port 8671.
- Le service Stunnel est désactivé / hors ligne : le service Stunnel s'exécute sur tous les

noeuds du déploiement distribué. L'état Désactivé/Non en cours d'exécution du service Stunnel entraîne l'échec des alarmes de réplication.

- Les ports de réplication sont bloqués : les ports 12001, 8671, 443, 8443 et 6379 doivent être ouverts entre les noeuds du déploiement et le réseau pour que les procédures de réplication du déploiement soient transparentes.

Impact de l'alarme

Lorsque la réplication s'arrête, les noeuds du déploiement ne reçoivent plus de mises à jour de configuration du noeud d'administration principal. Il peut en résulter des politiques incohérentes, des définitions de périphériques réseau obsolètes, des informations manquantes sur les terminaux, des retards de synchronisation des certificats et des incohérences de configuration dans le déploiement. Si la réplication reste arrêtée pendant une période prolongée, les modifications administratives apportées au PAN principal ne peuvent pas prendre effet sur le noeud affecté tant que la synchronisation n'est pas restaurée.

Dépannage de la réplication en échec et alarme de réplication arrêtée

Alarme de réplication lente

Chaque fois qu'une modification de configuration est effectuée sur le PAN principal, Cisco ISE place la modification dans la file d'attente de réplication et la synchronise sur les noeuds secondaires. Dans des conditions normales, la réplication est terminée en peu de temps. Toutefois, si la file d'attente de réplication commence à s'accumuler ou si le noeud de destination prend plus de temps que prévu pour traiter les demandes de réplication, Cisco ISE génère une alarme de réplication lente.

Cisco ISE classe ces alarmes en trois niveaux de gravité :

- Informations de réplication lente
- Avertissement de réplication lente
- Erreur de réplication lente

Motif de l'alarme

L'alarme de « réplication lente » est généralement générée en raison de conditions temporaires qui retardent le traitement de la réplication. Causes courantes :

- Utilisation temporaire des ressources système : De courtes périodes d'utilisation CPU élevée, d'utilisation de la mémoire ou d'E/S disque accrues peuvent retarder le traitement de réplication.
- Latence réseau : De brèves augmentations de la latence du réseau ou une perte de paquets mineure entre les noeuds ISE peuvent ralentir le transfert de données.
- Modifications importantes de la configuration : Les importations de terminaux en masse, les mises à jour de stratégies, les importations de certificats ou d'autres modifications administratives importantes augmentent la quantité de données à répliquer.
- Opérations système en arrière-plan : Les activités de sauvegarde, de restauration, de purge, d'installation de correctifs ou de mise à niveau augmentent temporairement la charge du système.
- File d'attente de réplication : Plusieurs modifications de configuration effectuées sur une courte période peuvent augmenter temporairement la file d'attente de réplication.
- Délais de service temporaires : RabbitMQ, JGroups ou les services de base de données subissent de courts retards de traitement tout en continuant à fonctionner normalement.

Alarme de réplication lente - Informations

Une réplication lente ou bloquée est détectée lorsque le nombre de messages en attente dépasse 10000 ou lorsque le temps de réplication des messages est supérieur à une heure.

Vérification : vérifiez le nombre de messages de synchronisation en attente. Accédez à Administration > System > Deployment, sélectionnez le noeud affecté et cliquez sur l'icône Information (i) pour vérifier le nombre de messages de réplication en attente.

Alarme de réplication lente - Avertissement

Une réplication lente ou bloquée est détectée lorsque le nombre de messages en attente est supérieur à 20000 ou lorsque le temps de réplication des messages dépasse trois heures.

Vérification : vérifiez le nombre de messages de synchronisation en attente. Accédez à Administration > System > Deployment, sélectionnez le noeud affecté et cliquez sur l'icône Information (i) pour vérifier le nombre de messages de réplication en attente.

Alarme de réplication lente - Erreur

Une réplication lente ou bloquée est détectée lorsque le nombre de messages en attente est supérieur à 40000 ou lorsque le temps nécessaire à la réplication des messages dépasse cinq heures.

Vérification : vérifiez le nombre de messages de synchronisation en attente. Accédez à Administration > System > Deployment, sélectionnez le noeud affecté et cliquez sur l'icône Information (i) pour vérifier le nombre de messages de réplication en attente.

Dépannage des alarmes de réplication de noeud

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. 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.

---

5. 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.

6. Vérification de la résolution DNS

La réplication Cisco ISE repose sur une communication réussie entre tous les noeuds du déploiement. Pour que la communication entre les noeuds fonctionne correctement, les noeuds doivent être accessibles et la résolution DNS directe et inverse doit être configurée et fonctionner correctement. Les problèmes de résolution DNS peuvent empêcher les noeuds de communiquer, ce qui entraîne des échecs de réplication.

Pour vérifier la résolution DNS dans les noeuds ISE, connectez-vous à l'interface de ligne de commande Cisco ISE et utilisez la commande nslookup pour vérifier la résolution DNS directe et inverse pour chaque noeud du déploiement.

Exemple :

- Forward DNS lookup : la commande nslookup www.example.com doit renvoyer l'adresse IP du noeud Cisco ISE correspondant.
- Reverse DNS lookup : la commande nslookup 10.x.x.1 doit renvoyer le nom de domaine complet (FQDN) du noeud Cisco ISE correspondant.

7. Vérification du certificat de messagerie administrateur et ISE

Cisco ISE utilise le certificat Admin et le certificat de messagerie ISE pour établir une communication inter-noeuds sécurisée requise pour la réplication. Si l'un des certificats est non valide, expiré, endommagé, ou non approuvé, la réplication entre les noeuds de déploiement peut échouer.

Pour vérifier l'état du certificat, accédez à Administration > System > Certificates, sélectionnez le noeud affecté et consultez les certificats Admin et ISE Messaging. Vérifiez que les certificats sont valides, qu'ils n'ont pas expiré, qu'ils sont approuvés et qu'ils sont en bon état.

Si le certificat Admin ou le certificat de messagerie ISE est non valide, corrompu ou a expiré, remplacez ou renouvelez le certificat. Une fois le problème de certificat résolu, la réplication reprend après le rétablissement d'une communication sécurisée entre les noeuds.

Remarque : Référez-vous Erreurs de liaison de file d'attente ISE et Installer des certificats dans ISE pour plus d'informations sur le renouvellement des certificats.

---

8. Vérifiez l'état du service Stunnel ISE

Le service Stunnel de Cisco ISE est un service interne qui fournit une tunnellisation SSL/TLS sécurisée pour la communication entre les composants ISE et les services externes. Plutôt que d'implémenter le cryptage TLS indépendamment dans chaque application, ISE utilise Stunnel comme wrapper qui ajoute le cryptage SSL/TLS aux services qui communiquent via le protocole TCP simple. Cela améliore la sécurité tout en simplifiant la mise en oeuvre de communications sécurisées.

Le service Stunnel doit être à l'état Running sur tous les noeuds dans le déploiement Cisco ISE pour que la réplication fonctionne correctement. Le service dépend de certificats ISE Admin et ISE Messaging valides pour établir une communication TLS sécurisée entre les noeuds pendant le processus de réplication. L'état du service peut être vérifié à partir de l'interface de ligne de commande Cisco ISE à l'aide de la commande show tech-support | inclure l'étourneau

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.