Comprendre et dépanner les réplications ISE

Table des matières

Introduction

Ce document décrit la réplication et son dépannage dans Cisco Identity Services Engine® (ISE).

Conditions préalables

Exigences

Cisco vous recommande de connaître 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 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.

Réplication dans Cisco ISE

La réplication dans ISE est le processus de synchronisation des données de configuration et d'exploitation sur plusieurs noeuds dans un déploiement afin de les maintenir cohérentes.

Le noeud d'administration principal est chargé de répliquer les modifications apportées au déploiement sur tous les autres noeuds (secondaires) du déploiement.

Cisco ISE utilise JGroups, une structure de communication de groupe fiable, dans le cadre de son architecture de réplication. JGroups permet aux noeuds d'un déploiement ISE de communiquer entre eux et d'échanger des données de réplication. Il fournit l'infrastructure de messagerie qui permet de fournir des mises à jour de configuration et de base de données entre les noeuds tout en maintenant la synchronisation sur l'ensemble du déploiement.

- JGroups est un cadre de communication utilisé par Cisco ISE pour la réplication ; elle ne stocke pas les données répliquées elle-même.
- Toutes les données de Cisco ISE ne sont pas répliquées via JGroups. Différents services utilisent des mécanismes de communication différents en fonction du type de données transférées.
- Si la réplication est temporairement interrompue, certains services Cisco ISE peuvent continuer à fonctionner en utilisant les données disponibles localement jusqu'à ce que la synchronisation soit restaurée.

Exemples de méthodes de transfert de données

Données	Méthode de communication
Messages de configuration et de réplication	JGroups

Collecte de bundles de support	API HTTPS (port TCP 443)
Déboguer la configuration	API HTTPS (port TCP 443)
Journaux et rapports en direct	RabbitMQ ou UDP, selon la configuration du déploiement

Conditions préalables et contrôles de validation pour la réplication Cisco ISE

- Résolution DNS : les recherches DNS directes et inversées doivent être résolues pour tous les noeuds Cisco ISE participant au déploiement. Une résolution DNS appropriée est requise pour les opérations de communication et de réplication des noeuds.
- Synchronisation NTP : tous les noeuds Cisco ISE doivent être synchronisés sur une source NTP fiable pour garantir une heure système cohérente tout au long du déploiement. La synchronisation temporelle est essentielle pour la réplication et la validation des certificats.
- Certificats : le certificat d'administration installé sur chaque noeud Cisco ISE doit être valide et approuvé. Les processus de réplication s'appuient sur le certificat Admin pour sécuriser les communications entre les noeuds.
- Exigences en matière de ports : la connectivité réseau doit permettre la communication sur les ports requis pour la réplication et les services entre noeuds :

Service	Protocole/port
HTTPS (SOAP)	TCP/443
Synchronisation et réplication des données (JGroups)	TCP/12001
Accès administratif	TCP/8443
Service de messagerie ISE (SSL)	TCP/8671
Synchronisation de la propriété des terminaux Profiler	TCP/6379

- Accessibilité du réseau : la connectivité réseau entre les noeuds Cisco ISE doit être stable et la latence ne doit pas dépasser 300 ms. La vérification de la latence et de la perte de paquets entre les noeuds garantit une réplication fiable.
- État de la liaison de la file d'attente : les certificats de messagerie Cisco ISE sont utilisés pour sécuriser la communication entre les noeuds sur le port TCP 8671. Des certificats de messagerie non valides ou endommagés peuvent entraîner des erreurs de liaison de file d'attente et des échecs de réplication. Dans de tels scénarios, le certificat de l'autorité de certification racine ISE ou les certificats de messagerie ISE doivent être régénérés selon les besoins.
- Service de tunnel ISE : le service de tunnel ISE de Cisco fonctionne dans des déploiements distribués et facilite la communication sécurisée entre les noeuds. Le service doit être exécuté sur tous les noeuds applicables pour prendre en charge la 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
- Correctif ISE et version : le noeud d'administration principal et le noeud de jonction (noeud autonome) doivent avoir la même version et le même niveau de correctif pour l'enregistrement et la synchronisation du noeud afin de fonctionner en toute transparence.

Phases de réplication dans Cisco ISE

La réplication dans Cisco ISE se compose de trois phases distinctes qui fonctionnent ensemble pour établir et maintenir la synchronisation entre tous les noeuds du déploiement. Chaque phase a une fonction spécifique, en commençant par l'intégration des noeuds, suivie de la synchronisation initiale de la base de données, et enfin de l'échange continu de mises à jour incrémentielles pour maintenir la synchronisation de tous les noeuds.

- Enregistrement du noeud
- Synchronisation complète active
- Synchronisation incrémentielle active

Comprendre l'enregistrement des noeuds dans Cisco ISE

L'enregistrement d'un noeud est le processus par lequel un noeud Cisco ISE rejoint un déploiement existant et établit la communication avec le noeud d'administration principal (PAN).

Pendant l'enregistrement du noeud :

Étape 1: Le noeud de jonction (noeud autonome) initie la communication avec le noeud

d'administration principal.

Étape 2: La validation mutuelle des certificats est effectuée à l'aide du certificat d'administration Cisco ISE.

Étape 3: La résolution DNS, la synchronisation NTP, l'accessibilité du réseau et l'accessibilité requise des ports sont validées dans le cadre du processus de communication.

Étape 4: Le noeud d'administration principal vérifie que le noeud autonome/noeud de jonction exécute une version et un niveau de correctif Cisco ISE compatibles.

Étape 5: Les informations de déploiement, les rôles de noeud et les relations d'approbation sont échangés.

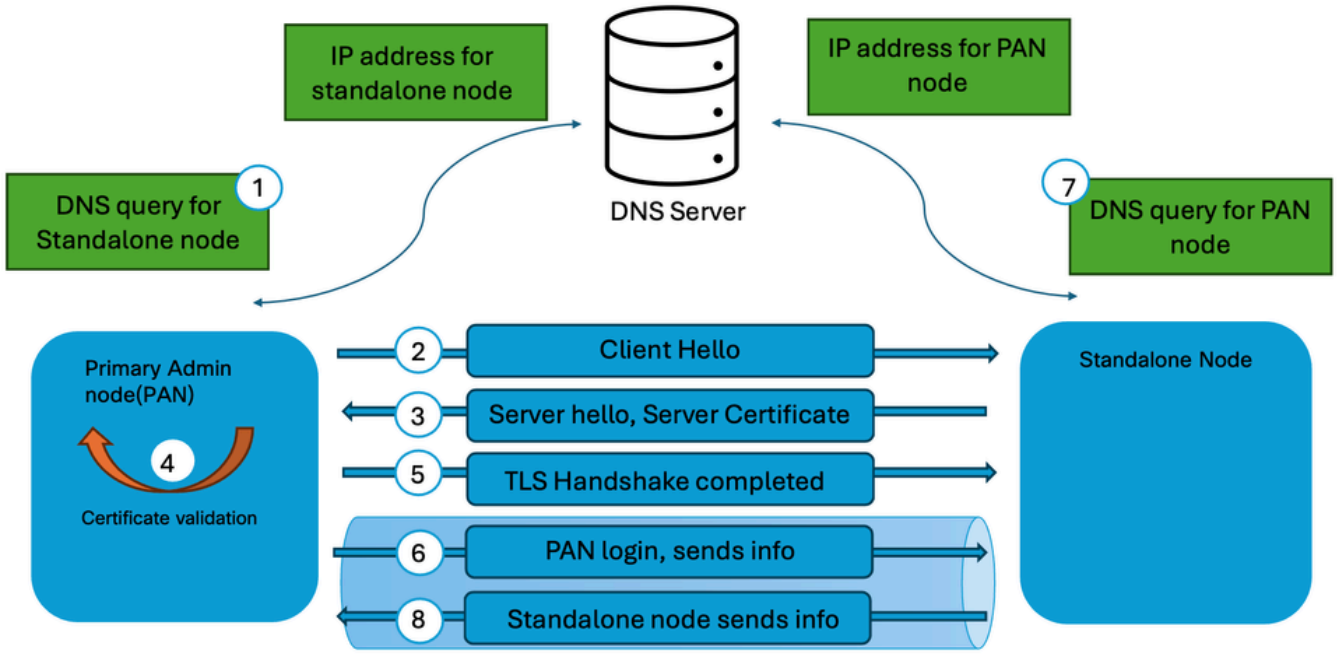
Étape 6: Les services de réplication de base de données sont initialisés et préparés pour la synchronisation.

La réussite de l'enregistrement du noeud établit le noeud en tant que membre approuvé du déploiement et permet aux processus de réplication de commencer.

Caractéristiques clés

- Se produit lorsqu'un nouveau noeud est ajouté au déploiement.
- Établit des canaux de confiance et de communication.
- Ne transfère pas immédiatement la base de données de configuration complète.
- Prérequis pour les opérations de synchronisation ultérieures.

Référez-vous à Comprendre le processus d'enregistrement de noeud dans Cisco ISE pour une explication détaillée du processus d'enregistrement de noeud.



Processus d'enregistrement des noeuds

Remarque : Le noeud ajouté au déploiement doit être un noeud autonome. En outre, le rôle d'administration principale du noeud d'administration principal (PAN) doit être activé dans le déploiement pour permettre l'enregistrement du noeud dans Cisco ISE.

Comprendre la synchronisation complète dans Cisco ISE

La synchronisation complète est un processus de réplication de base de données complet dans lequel la base de données de configuration entière est transférée du PAN principal vers un autre noeud. La synchronisation complète ne transfère pas uniquement les enregistrements modifiés. Au lieu de cela, l'ensemble des données de configuration est reconstruit sur le noeud récepteur.

Une synchronisation complète peut se produire dans des scénarios tels que :

- Synchronisation initiale après enregistrement du noeud.
- Récupération après des échecs de réplication.
- Incohérences importantes dans la base de données.
- Rejoindre un noeud au déploiement.
- Synchronisation manuelle initiée par les procédures de dépannage du TAC Cisco.
- Mécanismes de réplication interne déterminant que la synchronisation incrémentielle ne peut plus restaurer la cohérence de la base de données.

Pendant la synchronisation complète :

Étape 1: Le noeud Administration principale prépare un instantané de base de données complet.

Étape 2: Les données de configuration sont empaquetées dans le fichier .dmp et transmises au noeud récepteur.

Étape 3: Les données répliquées existantes sur le noeud récepteur sont validées et mises à jour.

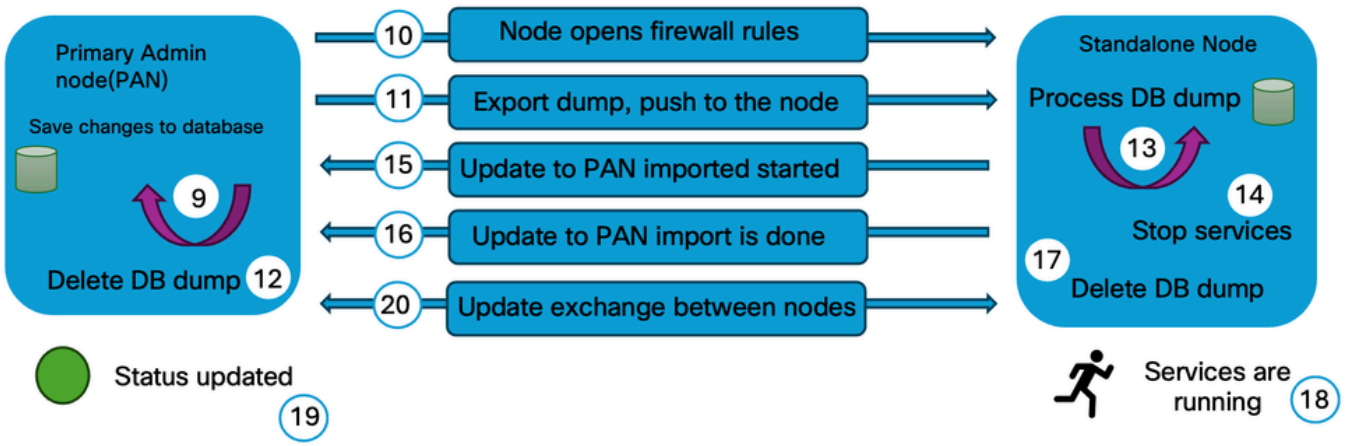
Étape 4: Toute la base de données de configuration est reconstruite pour correspondre au noeud Administrateur principal.

Étape 5: L'état de la réplication est vérifié une fois terminé.

Une synchronisation complète impliquant beaucoup plus de données qu'une synchronisation incrémentielle, elle nécessite un temps de traitement et des ressources réseau supplémentaires.

Caractéristiques de la synchronisation complète

- Transfère la base de données de configuration complète.
- Consomme plus de bande passante et de ressources système.
- Dure plus longtemps que la synchronisation incrémentielle.
- Restaure la cohérence de la base de données en cas de divergence.
- Généralement, cette opération est moins fréquente que la synchronisation incrémentielle.



Processus de synchronisation complète

Comprendre la synchronisation incrémentielle dans Cisco ISE

La synchronisation incrémentielle est le mécanisme de réplication continue utilisé par Cisco ISE pour distribuer les modifications de configuration une fois que les noeuds ont rejoint le déploiement avec succès. Lorsqu'un administrateur modifie la configuration du PAN, Cisco ISE ne transfère pas la base de données entière. Seuls les enregistrements modifiés sont répliqués sur les noeuds d'abonné.

Exemples de modifications répliquées par synchronisation incrémentielle :

- Modifications de stratégie
- Ajouts ou mises à jour de périphériques réseau
- Modifications du groupe de terminaux
- Mises à jour des profils d'autorisation
- Modifications de configuration liées aux certificats
- Mises à jour de configuration source identité

Le processus de synchronisation incrémentielle fonctionne en continu et est conçu pour maintenir la cohérence sur tous les noeuds tout en minimisant l'utilisation de la bande passante et la surcharge de réplication.

Avantages de la synchronisation incrémentale

- Réduction du trafic de réplication.
- Réduit le temps de synchronisation.
- Permet une propagation rapide des modifications de configuration.
- Assure une cohérence quasiment en temps réel sur l'ensemble du déploiement.

Workflow de réplication

Étape 1: La configuration est modifiée sur le noeud d'administration principal.

Étape 2: La modification est enregistrée dans la base de données du noeud d'administration principal.

Étape 3: Les services de réplication identifient les enregistrements modifiés.

Étape 4: Le noeud d'administration principal écrit les nouveaux événements/modifications dans une table de transactions.

Étape 5: Des threads distincts du PAN publient les informations/modifications sur les noeuds secondaires du déploiement.

Étape 6: Les noeuds secondaires du déploiement reçoivent les modifications du noeud d'administration principal.

Étape 7: Les noeuds secondaires du déploiement appliquent les modifications reçues du noeud d'administration principal.

Étape 8: L'état de la réplication est mis à jour une fois terminé.

Dans des conditions de fonctionnement normales, la plupart des activités de réplication dans Cisco ISE se produisent par synchronisation incrémentielle.

Remarque : Si un noeud secondaire identifie des messages de réplication manquants, il lance une requête au noeud d'administration principal (PAN) pour récupérer les messages manquants et maintenir la synchronisation

---

Présentation de la séquence de réplication et état de synchronisation

Le workflow global de réplication dans un déploiement Cisco ISE peut être résumé comme suit :

1. Enregistrement du noeud : Établit la confiance et ajoute le noeud au déploiement.

2. Synchronisation complète initiale : Transfère la base de données de configuration complète vers le noeud nouvellement enregistré.

3. Synchronisation progressive : Propage en continu les modifications de configuration pendant le fonctionnement normal.

4. Synchronisation complète (si nécessaire) : Reconstruit la cohérence de la base de données si des problèmes de réplication ou des discordances sont détectés.

Cette approche progressive permet à Cisco ISE de maintenir une base de données de configuration cohérente sur tous les noeuds tout en optimisant l'utilisation du réseau et les performances de réplication.

État de synchronisation

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 (le noeud n'a pas été accessible par le cluster au cours des cinq dernières minutes).
- Rouge - Le noeud est physiquement inaccessible et ne peut pas être contacté par le biais de vérifications de connectivité réseau (par exemple, ping ICMP et HTTPS).

Remarque : Si la réplication ne se produit pas correctement, vous pouvez effectuer une synchronisation manuelle vers les noeuds secondaires avec le noeud Administration principale en vous connectant au noeud Administration principale, accédez à Administration > Système > Déploiement > sélectionnez le noeud, puis cliquez sur Synchroniser vers le haut.

Réplication des terminaux

La réplication des points de terminaison est le processus par lequel ISE synchronise les informations de base de données des points de terminaison sur tous les noeuds de service de stratégie (PSN) et le noeud d'administration principal (PAN) afin de maintenir une vue cohérente de l'identité des points de terminaison tout au long du déploiement.

- Cisco ISE gère une base de données de terminaux centralisée qui stocke les informations relatives aux périphériques se connectant au réseau. Ces informations incluent à la fois les terminaux configurés de manière statique et les terminaux acquis de manière dynamique via l'authentification, le profilage, l'évaluation de la position ou l'intégration avec des sources d'identité externes.

- Lorsque des informations sur les terminaux sont créées ou modifiées, Cisco ISE réplique les modifications sur d'autres noeuds du déploiement. Cette synchronisation permet à chaque noeud de service de stratégie d'évaluer les demandes d'authentification et d'autorisation à l'aide des mêmes informations de point d'extrémité, quel que soit le PSN qui traite la demande.

- La réplication des terminaux est gérée automatiquement par Cisco ISE et fait partie du mécanisme global de réplication des bases de données. Les administrateurs n'ont pas à lancer manuellement la synchronisation des points de terminaison pendant les opérations normales.

Fonctionnement de la réplication des terminaux

- Mise à jour des terminaux : Un point de terminaison est créé ou mis à jour via l'authentification, le profilage, la position ou la configuration manuelle.
- Détection des modifications : Cisco ISE détecte la modification du terminal et la prépare à la réplication.
- Réplication : Les informations de point d'extrémité mises à jour sont répliquées sur les autres noeuds du déploiement à l'aide de l'infrastructure de réplication ISE.
- Synchronisation de base de données : Les noeuds secondaires mettent à jour leur base de données de terminaux locale avec les informations répliquées.
- Application cohérente des politiques : Une fois la synchronisation terminée, tous les noeuds de service de stratégie utilisent les mêmes informations de point de terminaison pour les décisions d'authentification et d'autorisation.

À partir de la version 3.3 de Cisco ISE, les terminaux détectés dynamiquement ne sont pas automatiquement répliqués sur tous les noeuds. Cette fonctionnalité peut être activée ou désactivée à partir de la fenêtre Réplication des points de terminaison. Accédez à Administration > System > Settings > Endpoint Replication, enable ou disable selon le besoin.

Remarque : Il est important de distinguer la réplication des points de terminaison de la réplication de session. La réplication des points d'extrémité synchronise les enregistrements de base de données des points d'extrémité persistants (adresses MAC, groupes de points d'extrémité et informations de profilage), tandis que la réplication de session synchronise les informations de session d'exécution pour prendre en charge l'application des stratégies et la continuité opérationnelle. Ces mécanismes fonctionnent indépendamment et remplissent différentes fonctions dans l'architecture Cisco ISE.

Problèmes courants de réplication des noeuds

Scénario 1 : Échec de l'enregistrement du noeud en raison d'une résolution DNS

Échec de l'enregistrement du noeud avec le motif d'erreur « le nom d'hôte ne peut pas être résolu. Vérifiez votre configuration DNS ».

Étapes de vérification

- Assurez-vous que le serveur DNS valide est configuré dans le noeud Administration principale et le noeud Autonome. Vérifiez la configuration du serveur DNS à l'aide de la commande show running-config | include name-server
- Validez la résolution DNS directe et inverse dans le noeud d'administration principal et le noeud autonome à l'aide de la commande nslookup FQDN du noeud pour la recherche DNS directe et nslookup ip address du noeud pour la recherche DNS inverse.
- Validez l'accessibilité du serveur DNS à partir du noeud d'administration principal et du noeud autonome à l'aide de la commande ping DNS server IP à partir de l'interface de ligne de commande des noeuds ISE.

Scénario 2 : Échec de l'inscription du noeud en raison de l'expiration du certificat admin

Échec de l'inscription du noeud avec le motif d'erreur « Erreur lors du chargement des certificats ». Noeud inaccessible pour le moment. Réessayez plus tard".

Étapes de vérification

- Validez les certificats d'administration du noeud d'administration principal et du noeud autonome pour garantir la validité et l'état du certificat. Accédez à Administration > System > Certificates, sélectionnez le noeud et vérifiez la validité et l'état du certificat Admin.
- Si le certificat Admin a expiré, remplacez ou renouvelez le certificat et assurez-vous que l'utilisation Admin est attribuée.

Scénario 3 : Échec de l'enregistrement du noeud en raison d'une incompatibilité de version

Échec de l'inscription du noeud avec le motif d'erreur « version/patch details mismatch ».

Étapes de vérification

- Validez la version du logiciel avec le correctif du noeud d'administration principal et du noeud autonome à l'aide de la commande show version pour vous assurer que les détails de la version correspondent.

Composants des journaux de débogage

Il s'agit des composants communs qui doivent être définis en mode debug pour isoler et dépanner la 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)
- ca-service (caservice.log)
- admin-ca (ise-psc.log)

Référence

- Dépannage et activation des débogages sur ISE
- Erreur de liaison de file d'attente ISE
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.4
- Guide de l'administrateur de Cisco Identity Services Engine, version 3.5

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.