Dépannage des problèmes de synchronisation du connecteur AD d'accès sécurisé

Table des matières

Problème

Le connecteur AD installé sur un contrôleur de domaine ne se synchronise pas correctement avec Cisco Secure Access. Le connecteur rencontre plusieurs échecs de synchronisation, notamment :

- Échecs de synchronisation Delta avec erreurs « Accès refusé » (COMException 0x80070005).
- Échec de lecture du journal des événements du contrôleur de domaine avec UnauthorizedAccessException : Tentative d'exécution d'une opération non autorisée.
- Problèmes d'inscription au cloud indiquant un « format URI non valide » lors du téléchargement du manifeste.
- HTTP 404 "object_not_found" erreurs pour AssetID spécifique pendant les tentatives de synchronisation.

Le connecteur semble être connecté au service cloud Cisco Secure Access, mais échoue tant du côté des autorisations Active Directory que de la configuration de l'enregistrement dans le cloud.

Environnement

- Accès sécurisé Cisco avec connecteur AD
- Connecteur AD version 1.15.2
- Connecteur AD installé sur le contrôleur de domaine
- Compte de service personnalisé (svcCiscoUmbrella) au lieu du compte Cisco_Connector par défaut
- Configuration de l'environnement test/pilote

Résolution

La résolution impliquait de résoudre les problèmes d'autorisations Active Directory et d'enregistrement dans le cloud par le biais d'un processus de réinstallation complet :

Étape 1: Vérification et nettoyage des entrées de connecteur AD existantes

Dans le tableau de bord Accès sécurisé, vérifiez l'entrée Connecteur Active Directory pour l'hôte et supprimez toutes les entrées obsolètes ou en double pour le même serveur, le cas échéant.

Étape 2: Assurez la désinstallation complète

Désinstallez complètement le service Connecteur Active Directory existant pour vous assurer qu'aucune configuration résiduelle ne reste susceptible de provoquer des problèmes d'enregistrement.

Étape 3: Exécuter les scripts du contrôleur de domaine

Avant de réinstaller le connecteur, exécutez les scripts de configuration du contrôleur de domaine appropriés pour vous assurer que les autorisations appropriées sont définies. Le script doit être exécuté sur chaque contrôleur de domaine applicable, bien que le connecteur lui-même puisse résider en dehors du contrôleur de domaine sur un autre ordinateur joint au domaine.

Étape 4: Configurer les autorisations de compte de service

Accordez les autorisations Active Directory requises au compte de service :

- Autorisations de synchronisation AD (domaine/étendue racine, le cas échéant) :
    - Lire

    - Réplication des modifications de répertoire
    - Réplication de toutes les modifications de répertoire (si nécessaire dans l'environnement)
    - Réplication des modifications de répertoire dans le jeu filtré (si nécessaire dans l'environnement)
- Accès au journal des événements sur le contrôleur de domaine :
    - Ajoutez le compte de service au groupe Lecteurs du journal des événements.
    - Assurez-vous d'une autorisation équivalente basée sur des stratégies pour lire le journal de sécurité.

Étape 5: Réinstaller le connecteur AD

Réinstallez le service Connecteur AD pour générer un nouveau manifeste et un AssetID valide, garantissant ainsi un enregistrement correct dans le cloud.

Étape 6: Redémarrer et valider

Après l'installation et la configuration des autorisations :

1. Redémarrez le service Connecteur Active Directory.
2. Surveillez les journaux du connecteur pour confirmer que l'accès est refusé et que les erreurs non autorisées s'arrêtent.
3. Vérifiez que les entrées de synchronisation réussies apparaissent dans les journaux (par exemple, « ADSync LDIF RESPONSE: 200 Succès »).

Motif

Les problèmes de synchronisation sont dus à deux facteurs principaux :

1. Autorisations Active Directory insuffisantes : Le compte de service personnalisé

(svcCiscoUmbrella) ne disposait pas des autorisations AD requises pour la synchronisation delta et l'accès au journal des événements DC, ce qui a généré des erreurs « Access is deny » et « UnauthorizedAccessException ».
2. Problèmes d'enregistrement cloud : L'instance du connecteur a été mal enregistrée ou pointait vers un AssetID non valide/ancien, ce qui a provoqué des erreurs de format d'URI non valide lors du téléchargement du manifeste et des erreurs HTTP 404 « object_not_found » lors des tentatives de synchronisation.

Ces problèmes ont été aggravés par des procédures d'installation incomplètes dans lesquelles les scripts de configuration du contrôleur de domaine n'ont pas été correctement exécutés avant l'installation du connecteur.

Autres informations utiles

- Configuration du connecteur Cisco Secure Access AD
- Autorisations de connecteur AD requises
- Guide d'installation du connecteur AD
- Dépannage du connecteur AD
- Configuration du compte de service du connecteur AD
- Assistance technique de Cisco et téléchargements

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.