Intégrer Active Directory hors connexion après le déploiement d'appliances virtuelles d'accès sécurisé

Table des matières

Problème

Après le déploiement de deux appliances virtuelles d'accès sécurisé (VA), l'intégration Active Directory (AD) a cessé de fonctionner dans le tableau de bord d'accès sécurisé. Auparavant, l'intégration AD était opérationnelle, mais après le déploiement VA, le connecteur AD s'affiche désormais comme hors connexion dans le tableau de bord d'accès sécurisé. Une assistance est requise pour restaurer la connectivité AD.

Environnement

- Technologie : Assistance pour les solutions (SSPT - contrat requis)
- Sous-technologie : Accès sécurisé
- Version du logiciel: TOUS
- Accès sécurisé (DNS-Advantage/Umbrella)
- Déploiement de deux appliances virtuelles d'accès sécurisé au siège
- Événement de modification : Installation des VA immédiatement avant la défaillance du connecteur AD
- Le connecteur AD était précédemment opérationnel et s'affiche désormais comme hors connexion dans le portail d'accès sécurisé

Résolution

Pour résoudre le problème de l'affichage hors connexion de l'intégration Active Directory dans le portail Secure Access après le déploiement de l'appliance virtuelle, effectuez les étapes de dépannage suivantes :

Capturer le trafic réseau pendant le redémarrage du connecteur

Exécutez une capture Wireshark sur toutes les interfaces du connecteur AD/contrôleur de domaine lors du redémarrage des services du connecteur. Cela permet d'identifier les échecs de communication réseau ou les tentatives d'accès non autorisées pendant l'initialisation du connecteur.

Étape 1 : Démarrez la capture Wireshark sur toutes les interfaces concernées

Démarrez Wireshark et commencez la capture sur toutes les interfaces du connecteur AD/contrôleur de domaine.

Étape 2 : Redémarrez Connector Services via le Gestionnaire de services Windows

Ouvrez services.msc, recherchez le service Connecteur OpenDNS, puis cliquez sur Redémarrer.

Étape 3 : Enregistrez le fichier de capture pour une analyse plus approfondie

Arrêtez la capture et exportez le fichier .pcap.

Collecter les journaux des connecteurs

Collecter les journaux à partir du connecteur AD pour une meilleure compréhension des erreurs ou des problèmes d'authentification :

1. Accédez au répertoire du journal.

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\vX.X.X
```

1. Collectez les fichiers journaux appropriés et préparez-les pour révision. Copiez tous les fichiers journaux du répertoire mentionné ci-dessus vers un emplacement sécurisé.

Vérifier les autorisations de compte du connecteur AD

Après l'introduction d'appliances virtuelles, le compte Connecteur AD nécessite des autorisations spécifiques pour fonctionner correctement. Si le compte ne dispose pas du rôle Lecteur du journal des événements, il peut rencontrer des exceptions d'accès non autorisées.

1. Affectez l'autorisation Lecteur du journal des événements au compte Connecteur Active Directory. Utilisez Utilisateurs et ordinateurs Active Directory (ADUC) ou Stratégie de groupe pour ajouter le compte Connecteur Active Directory au groupe Lecteurs du journal des événements.
2. Vérifiez que le compte dispose de la nouvelle autorisation. Vérifiez l'appartenance au groupe pour le compte Connecteur Active Directory afin de vérifier l'inclusion des lecteurs du journal des événements.

Exception courante trouvée

Lors du dépannage, cette exception peut être observée dans les journaux ou dans les informations d'état du connecteur :

```
* Exception type: system.unauthorizedaccessexception
message: Attempted to perform an unauthorized operation.
```

Cela indique que le compte Connecteur AD ne dispose pas d'autorisations suffisantes, en particulier le rôle Lecteur du journal des événements, qui est obligatoire après l'introduction des VA.

Aucune commande CLI n'a été trouvée pour indiquer le passage de l'état du connecteur AD hors ligne à en ligne.

Motif

La cause sous-jacente est des autorisations insuffisantes pour le compte Connecteur AD après le déploiement des appliances virtuelles d'accès sécurisé. Le compte n'a pas l'autorisation Lecteur de journal d'événements, qui est requise pour la fonctionnalité de connecteur AD appropriée. Cela entraîne une erreur « system.unauthorized accessexception » et empêche le connecteur de fonctionner en ligne dans le portail d'accès sécurisé.

Autres informations utiles

- 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.