Dépannage de l'intégration AD Umbrella Insights ne détectant pas le trafic utilisateur

Table des matières

Introduction

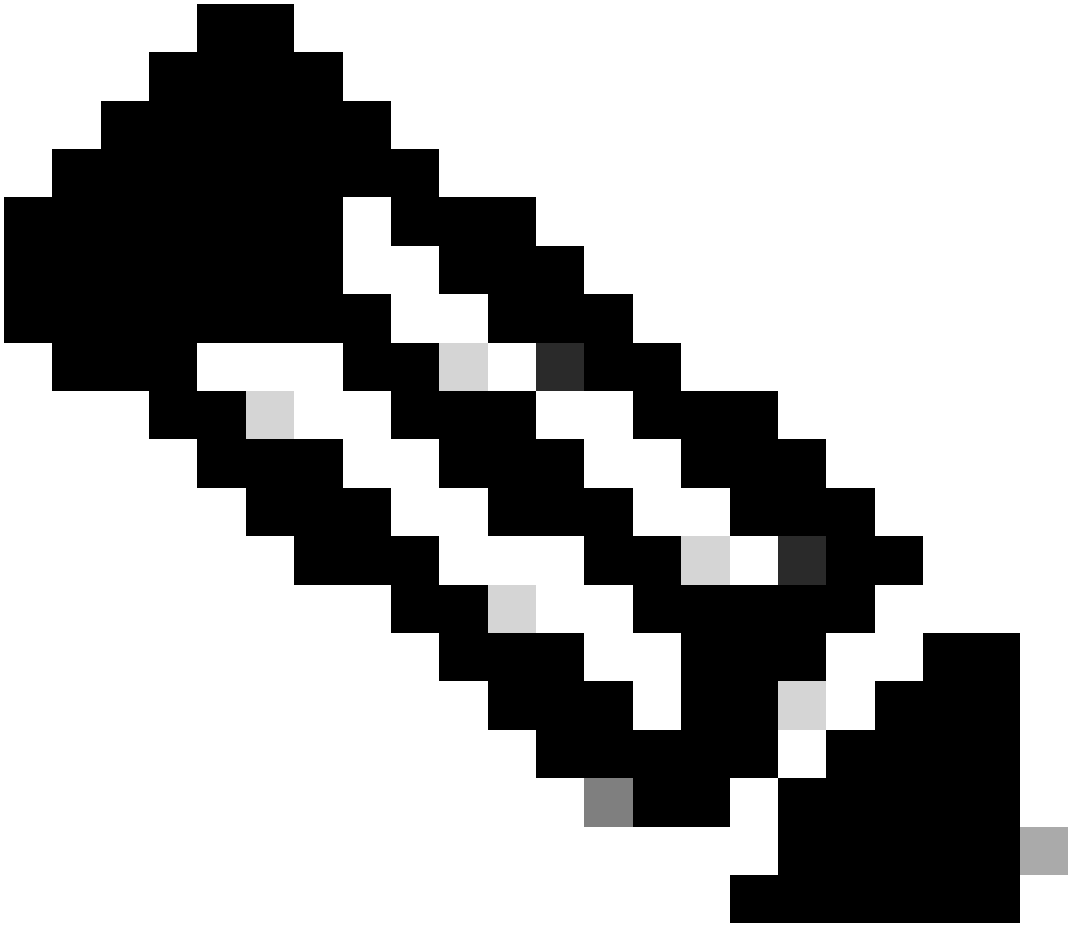
Ce document décrit comment dépanner l'intégration AD Umbrella Insights qui ne détecte pas le trafic utilisateur.

Aperçu

Vous avez installé Umbrella Insights, configuré un connecteur et des appareils virtuels et enregistré vos contrôleurs de domaine. Tous vos composants sont affichés en vert et fonctionnent dans le tableau de bord sous `déploiements -> Sites et Active Directory`. Cependant, vous avez une stratégie configurée pour utiliser des utilisateurs AD ou des objets de groupe, mais vous ne voyez toujours pas l'activité utilisateur signalée dans le tableau de bord ou la stratégie appliquée correctement.

Vous remarquerez peut-être également que cette entrée se répète dans le fichier OpenDNSAuditClient.log

`Dernier événement reçu à 1970-01-01 00:00:00`



Remarque : Le fichier journal se trouve dans C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\
VERSION = version installée du service Connector, telle que v1.1.22

Explication

La raison principale de ce problème est que les événements de connexion d'audit peuvent ne pas être configurés dans votre domaine Active Directory. Le message du journal indique que le connecteur n'a pas vu un seul événement utilisateur depuis son installation. Actuellement, ce n'est pas quelque chose qui génère une erreur dans le tableau de bord.

Résolution

La principale chose à faire est de vérifier la stratégie de groupe AD pour la configuration de stratégie d'audit correcte :

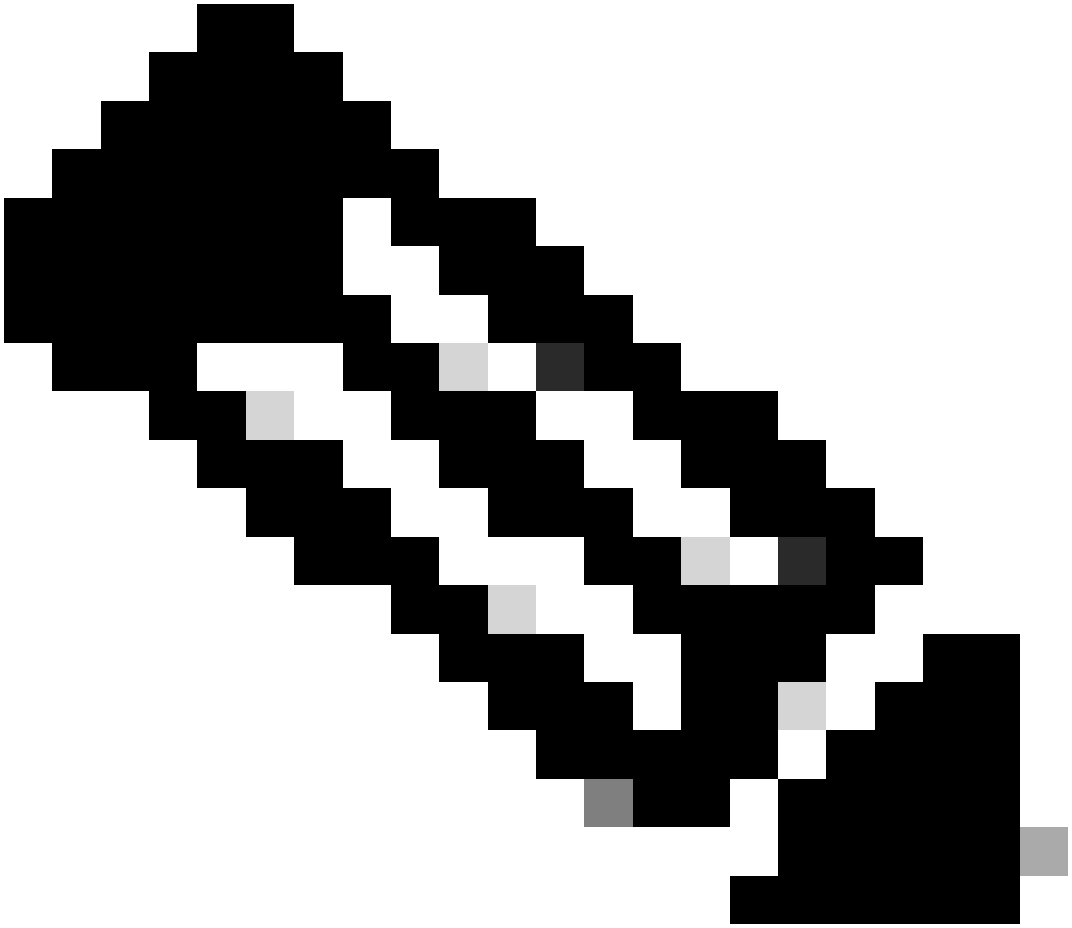
1. Sur le contrôleur de domaine, ouvrez le `panneau Gestion des stratégies de groupe situé dans Outils d'administration` et sélectionnez une stratégie qui s'applique aux contrôleurs de domaine (la stratégie de contrôleur de domaine par défaut serait la candidate probable).

2. Cliquez avec le bouton droit sur cette stratégie et sélectionnez Modifier pour afficher l'`Éditeur de gestion des stratégies de groupe`.

3. Accédez au dossier `"Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Stratégie d'audit"` et sélectionnez Auditer les événements d'ouverture de session pour afficher ses propriétés.

4. Cette stratégie doit être utilisée pour auditer les tentatives de réussite.

5. Exécutez la commande gpupdate pour appliquer la stratégie.



Remarque : Dans certains cas, il peut être nécessaire de configurer ce paramètre pour les « contrôleurs de domaine par défaut » et la stratégie de domaine par défaut.

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.