Dépannage du blocage d'un compte de service Active Directory par Umbrella Connector

Table des matières

[Introduction](#)

[Aperçu](#)

[Liste des comptes bloqués](#)

[Informations complémentaires](#)

Introduction

Ce document décrit comment dépanner le blocage d'un compte de service Active Directory par le connecteur Umbrella.

Aperçu

Le service Umbrella Connector établit des connexions WMI aux journaux d'événements de tout contrôleur de domaine enregistré qui fait partie du même [site Umbrella](#), afin de lire les informations d'événement de connexion. Ces événements de connexion sont ensuite analysés et téléchargés vers tous les appareils virtuels (VA) du même site Umbrella. L'appliance virtuelle crée ensuite un mappage utilisateur-IP temporaire pour ce nom d'utilisateur/cette adresse IP source. Quelques points méritent d'être soulignés :

- Umbrella Insights ne peut prendre en charge qu'un seul utilisateur connecté par IP à la fois
- L'événement de connexion le plus récemment traité à partir d'une adresse IP source « gagne »

Comme tous les événements d'ouverture de session sont égaux, le connecteur a une liste codée en dur de comptes de service AD communs dont les événements sont ignorés. Vous pouvez voir les événements de connexion de ces comptes pris dans le fichier journal du connecteur. Exemple :

Événement de l'utilisateur sur liste noire ignoré : `Connecteur_OpenDNS`

Cela permet d'empêcher les comptes de service (qui, tout comme les utilisateurs standard, génèrent des événements d'ouverture de session dans les journaux d'événements de sécurité du contrôleur de domaine) de remplacer le mappage utilisateur-IP de l'utilisateur réellement connecté.

Dans les environnements de grande taille, en fonction du processus/de l'application pour lequel un compte de service est utilisé, ils peuvent également générer des milliers d'événements de connexion chaque minute. Il s'agit également d'une charge supplémentaire pour le connecteur, qui peut se manifester sous la forme d'un délai entre l'ouverture de session de l'utilisateur et la

stratégie correcte appliquée, ou d'une stratégie correcte appliquée qui est ensuite perdue.

Liste des comptes bloqués

- _vmware_user_
- administrateur
- ANONYME
- Ouverture de session anonyme
- ASPNET
- Service local
- McAfeeMVSUser
- MHControl
- Service réseau
- netwrix
- Connecteur_OpenDNS
- peersyncsvc
- s-pcadmine
- SophosUpdateMgr
- SophosUpdMgr
- svc-altiris
- svc.iCreate

Informations complémentaires

Vous pouvez également exclure tout autre événement d'ouverture de session de compte AD du traitement par le connecteur. Consultez cet article pour obtenir des instructions :

<https://support.umbrella.com/hc/en-us/articles/231266088>

En outre, certains groupes Active Directory peuvent être exclus de la synchronisation Active Directory du connecteur, qui est effectuée pour remplir la zone de stratégie Tableau de bord avec une liste d'utilisateurs, d'ordinateurs et de groupes Active Directory. Vous pouvez le trouver ici :

<https://support.umbrella.com/hc/en-us/articles/115005206526>

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.