Comprendre l'intégration de Cisco Umbrella AD et les appliances virtuelles

Table des matières

Introduction

Ce document décrit le fonctionnement de l'intégration d'Umbrella Active Directory (AD) lors de l'utilisation d'appliances virtuelles.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

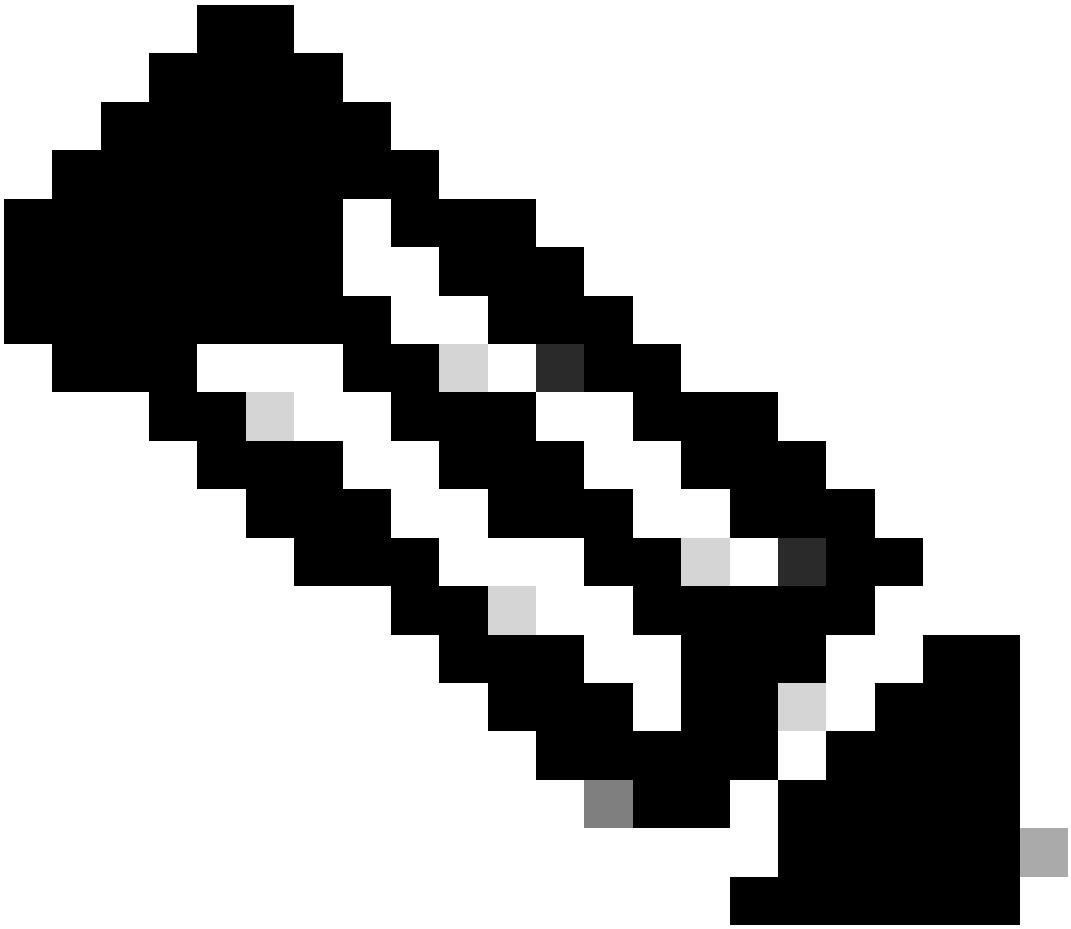
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Présentation de la fonctionnalité d'intégration d'Umbrella Active Directory aux appliances virtuelles

1. Le service Umbrella Connector extrait les événements de connexion avec les ID 4624, 528, 540, 538, 4647, 4634, 4768 et 4769 de l'Observateur d'événements Windows sur tous les contrôleurs de domaine du même site Umbrella que le serveur Connector. Ces événements de connexion incluent le nom d'utilisateur/ordinateur AD et l'adresse IP de la station de travail.

2. Le connecteur transmet un résumé des nouvelles entrées FOUND EVENT à tous les appareils

virtuels du même site Umbrella.



Remarque : Le connecteur met en cache les informations d'événement d'ouverture de session pour optimiser les performances, de sorte que les résumés ne sont pas toujours envoyés. En outre, les résumés ne sont pas envoyés pour les utilisateurs AD, les groupes AD ou les adresses IP qui ont été ajoutés à la liste des exceptions de compte de service Umbrella.

---

3. Chaque VA utilise le résumé pour créer un fichier de mappage entre l'adresse IP et l'utilisateur/ordinateur Active Directory.

4. Lorsqu'une requête DNS est envoyée à un serveur virtuel à partir d'une adresse IP particulière, le fichier de mappage est utilisé pour rechercher l'utilisateur/ordinateur AD associé.

5. L'utilisateur/l'ordinateur détermine la stratégie pour la demande et identifie la demande dans les rapports.

Fonctionnalité prévue

1. Un utilisateur se connecte au domaine Active Directory à l'aide d'un contrôleur de domaine qui a été enregistré auprès d'Umbrella.

2. Un connecteur de parapluie situé sur le même site de parapluie que ce contrôleur de domaine transmet un résumé à tous les VA situés sur ce même site de parapluie.

3. Le protocole DHCP ou une autre méthode garantit que les serveurs DNS de l'utilisateur sont des serveurs virtuels dans le même site parapluie que ce contrôleur de domaine.

4. Les requêtes DNS de l’utilisateur sont correctement identifiées par Umbrella.

Scénario pour le DC non enregistré dans Umbrella

Inversement, supposons qu'un utilisateur se connecte au domaine Active Directory à l'aide d'un contrôleur de domaine qui n'a pas été enregistré auprès d'Umbrella :

1. Le connecteur Umbrella ne voit jamais l'événement d'ouverture de session et n'a pas d'utilisateur/ordinateur AD + adresse IP à transférer aux VA.

2. Les VA ne peuvent pas ajouter/modifier une entrée de mappage.

3. Les requêtes DNS de l'utilisateur ne peuvent pas être associées à l'utilisateur (sauf si quelque chose a été mis en cache).

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.