Intégrer Active Directory à l'aide de VA ou CSC

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Aperçu

Implémentation sécurisée du client

- Exigences
- Comment ça fonctionne
- Où cela fonctionne
- Limites

Implémentation d'appliance virtuelle

- Exigences
- Où cela fonctionne
- Limites

Introduction

Ce document décrit deux méthodes d'intégration d'Active Directory (AD) avec Umbrella : Appliance virtuelle (VA) ou Cisco Secure Client (CSC).

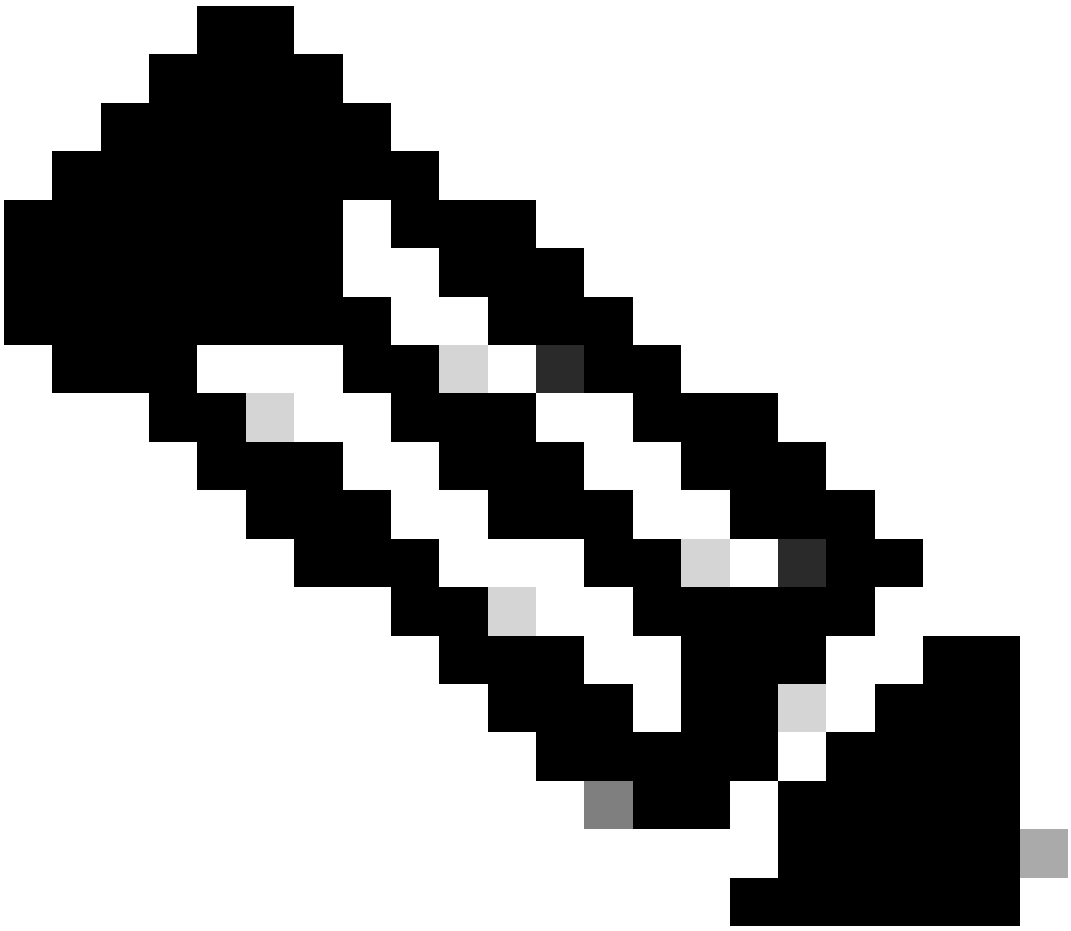
Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connecteur AD : Synchronise l'arborescence Active Directory d'un seul domaine Active Directory avec le tableau de bord. Pour l'implémentation VA, il synchronise également activement les événements de connexion des contrôleurs de domaine du même site Umbrella aux contrôleurs de domaine. L'arborescence AD de l'organisation est synchronisée au cloud Umbrella par le connecteur AD, qui extrait ces données du contrôleur de domaine enregistré. Les mises à jour de l'arborescence sont détectées et le nuage Umbrella est mis à jour dans les heures qui suivent.
- Contrôleur de domaine (serveur AD) : Les contrôleurs de domaine sont enregistrés dans le tableau de bord via le script .wsf de configuration d'enregistrement téléchargé à partir du tableau de bord. Le nom, le domaine et l'adresse IP interne sont ajoutés au tableau de bord pour indiquer au connecteur les adresses IP avec lesquelles effectuer la synchronisation. Si vous ne pouvez pas exécuter le script, l'enregistrement manuel est également possible. Contactez le service d'assistance Umbrella pour plus d'informations et d'assistance.

- Appliance virtuelle : Le redirecteur DNS Umbrella sur site. Applique (facultatif) l'identité AD sur le réseau ainsi que les adresses IP internes sur les rapports. Cela déclenche tous les clients itinérants derrière elle pour désactiver la protection DNS et passer en mode "Derrière la protection VA".
- Client sécurisé Cisco : Le service logiciel Umbrella sur site qui fournit le cryptage DNS ainsi que l'identification des utilisateurs à Windows et macOS. Également disponible sous forme de module AnyConnect.



> Remarque : Les conditions préalables diffèrent considérablement entre les deux implémentations. Reportez-vous à la mise en oeuvre spécifique pour connaître toutes les conditions requises.

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.

Aperçu

Cet article clarifie et explore les deux méthodes différentes d'intégration d'Active Directory avec le tableau de bord Umbrella. Actuellement, les utilisateurs AD peuvent être appliqués à la stratégie et aux rapports via les appliances virtuelles Umbrella ou le client sécurisé Cisco.

Implémentation sécurisée du client

Exigences

- Un connecteur AD
- Un DC sur le tableau de bord
- L'utilisateur OpenDNS_Connector doit disposer d'une autorisation de contrôleur de domaine en lecture seule.
- Versions minimales du client sécurisé pour le client autonome (module AnyConnect) :
    - Fenêtres: 2.1.0 (4.5.01044)
    - OSX : 2.0.39 (4.5.02033).

Comment ça fonctionne

- L'utilisateur AD actuellement connecté est déterminé directement sur l'ordinateur local par le client itinérant qui lit le Registre local.
- Prend en charge au maximum un utilisateur connecté simultanément sur la station de travail.
- Deux utilisateurs simultanés peuvent empêcher l'application d'un utilisateur AD.
- Le GUID d'utilisateur AD et l'adresse IP interne sont reliés via EDNS0 dans le proxy DNS du client d'itinérance à la requête DNS envoyée aux résolveurs Umbrella, identifiant de manière unique l'utilisateur AD.
- Toutes les stratégies sont appliquées du côté du résolveur.
- Aucun connecteur actif n'est requis. Cependant, l'application de stratégie de groupe et d'utilisateur AD peut refléter la dernière synchronisation réussie de l'arborescence AD.

Où cela fonctionne

- Tout réseau au niveau mondial.
- Ne fonctionne pas derrière un appareil virtuel Umbrella, car la couche DNS est désactivée pour être transférée aux VA locaux.

Limites

- Nécessite que l'agent de terminal soit actif et activé sur la station de travail.
- Ne prend pas en charge les systèmes d'exploitation serveur.
- Impossible d'appliquer la stratégie basée sur l'IP réseau interne.

- Impossible d'appliquer la stratégie ou les rapports pour l'ordinateur AD (utilisez plutôt le nom d'hôte itinérant).

Le connecteur peut toujours tenter d'extraire les événements de connexion AD du DC enregistré. Cela peut entraîner une erreur de tableau de bord qui n'est pas pertinente pour l'intégration d'AD basée sur le client itinérant. Pour supprimer les erreurs avec les autorisations liées à l'extraction d'événements de connexion sans l'extraction d'événements, désactivez l'audit des événements de connexion (s'il n'est pas utilisé autrement) via l'inverse des instructions d'audit à partir d'ici.

Implémentation d'appliance virtuelle

Exigences

- Deux VA par site Umbrella
- Un connecteur AD (redondant et un second en option) par site Umbrella
- Chaque DC (qui n'est pas un DC en lecture seule) doit être enregistré dans le tableau de bord.
- L'utilisateur OpenDNS_Connector doit disposer de l'ensemble complet des autorisations requises.
- Les événements de connexion doivent être activés pour consigner les journaux d'événements de sécurité 4624 sur tous les contrôleurs de domaine. Voir les conseils de dépannage complets.

Comment ça fonctionne

- Les VA reçoivent les mappages d'utilisateur AD en fonction des journaux d'événements de connexion de sécurité des DC Windows.
- Chaque connexion de station de travail est consignée dans le journal des événements de sécurité du contrôleur de domaine du serveur de connexion en tant qu'événement de connexion unique, avec le nom d'utilisateur AD ou le nom d'ordinateur AD et l'adresse IP interne de la station de travail.
- Le connecteur analyse ces événements en temps réel via un abonnement WMI et synchronise ces événements à chaque VA sur le site Umbrella via TCP 443.
- L'appliance virtuelle crée un mappage d'utilisateur actif entre l'adresse IP interne d'un utilisateur/ordinateur Active Directory et le nom d'utilisateur de l'utilisateur/ordinateur Active Directory.
- L'appliance virtuelle n'a de visibilité que sur l'adresse IP source interne d'une requête DNS et utilise le fichier de mappage mentionné précédemment créé par les événements synchronisés par le connecteur. L'appliance virtuelle n'a aucune visibilité directe sur les personnes actuellement connectées à une machine. Ceci attache le GUID d'utilisateur AD et l'IP interne via EDNS0 à la requête DNS envoyée aux résolveurs Umbrella par l'AV, identifiant de manière unique l'utilisateur AD.
- Le hachage de l'ordinateur Active Directory est appliqué de la même manière.
- Toutes les stratégies sont appliquées du côté du résolveur.
- Un connecteur doit être fonctionnel et actif dans l'organisation pour recevoir un utilisateur AD, et les événements de connexion doivent être à jour.

- L'utilisateur doit être le dernier utilisateur AD à s'authentifier sur cet ordinateur, comme indiqué dans les journaux des événements.

Où cela fonctionne

Sur le réseau d'entreprise local, où tous les DNS sont dirigés vers un appareil virtuel Umbrella appartenant au même site Umbrella que le contrôleur de domaine auquel l'utilisateur s'est authentifié.

Limites

- L'ordinateur ne peut pas pointer vers une appliance virtuelle appartenant à un domaine AD ou à un site parapluie différent (les déploiements importants sur plusieurs domaines ne peuvent pas voir l'application AD de leur réseau de base).
- Les grands déploiements peuvent nécessiter une subdivision en sites parapluies avec des baies virtuelles distinctes.
- Des exceptions d'utilisateurs AD peuvent être nécessaires pour les utilisateurs AD de service.
- Il existe un débit maximal d'événements de connexion par seconde pour le connecteur mentionné précédemment, ce qui peut retarder l'application utilisateur. Il s'agit d'un facteur de latence du réseau et de nombre de VA.

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.