Examiner le flux d'intégration d'Umbrella Active Directory

Table des matières

Introduction

Ce document décrit le flux de communication entre les composants opérationnels dans une intégration Cisco Umbrella Active Directory (AD).

Informations générales

La compréhension du flux de communication Active Directory peut aider à dépanner et à garantir un environnement correctement configuré avant le déploiement.

Flux de communication avec implémentation Active Directory Umbrella

Lorsque le script de connecteur AD s'exécute sur un contrôleur de domaine (DC)

Le script Windows établit une connexion unique du contrôleur de domaine au cloud sur le port TCP/443 à l'aide de HTTPS pour enregistrer le contrôleur de domaine sur le tableau de bord. Cet enregistrement permet au connecteur de reconnaître le contrôleur de domaine. Un appel est passé à avec **https://api.opendns.com** des paramètres spécifiques. Une fois que le script a correctement enregistré le contrôleur de domaine, il s'affiche sur le tableau de bord.

Les problèmes peuvent parfois être liés aux mises à jour du certificat racine sous Windows. Pour le savoir rapidement, accédez à Internet Explorer et pointez le navigateur vers : https://api.opendns.com/v2/OnPrem.Asset. Cette action imprime un message du type **1005 Missing API key**. « Si des erreurs ou des avertissements de certificat apparaissent sur cette page, vérifiez que la dernière

mise à jour des certificats racine de Microsoft est installée.

Mode de communication du connecteur AD

Le connecteur Active Directory communique avec le service de cloud Umbrella ou avec une appliance virtuelle de la manière suivante :

- Connecteur vers le cloud

  Le connecteur télécharge toutes les données Active Directory (AD) toutes les cinq minutes en cas de modification, à l'aide d'une connexion HTTPS sur le port 443 TCP. Seules les informations sur les groupes, les utilisateurs et les ordinateurs sont téléchargées. Aucun mot de passe n'est téléchargé et toutes les informations utilisateur sont hachées localement, ce qui rend les données uniques.

- Connecteur vers appareils virtuels

  Le connecteur envoie en permanence des événements AD aux appliances virtuelles via le port TCP 443 (non chiffré). Il s'agit d'une communication unidirectionnelle ; les appareils ne communiquent pas en retour avec les connecteurs. Une condition préalable obligatoire est que le connecteur et l'appliance virtuelle (VA) communiquent sur un réseau approuvé.

- Connecteur vers contrôleurs de domaine

  Le connecteur communique avec tous les contrôleurs de domaine situés sur le même site à l'aide des ports 389 TCP et 3268 TCP/UDP pour la synchronisation LDAP. Le connecteur communique également avec les contrôleurs de domaine à l'aide de WMI/RPC. Port 135 TCP est le port standard pour RPC et WMI. WMI utilise également un port attribué aléatoirement entre TCP 1024 et TCP 65535 pour Windows 2003 et versions antérieures, ou entre TCP 49152 et TCP 65535 pour Windows 2008 et versions ultérieures. Depuis la version 1.1.24, le connecteur communique également avec le contrôleur de domaine à l'aide de LDAP (LDAP over SSL) sur les ports 636 TCP et 3269 TCP.

Si des problèmes de communication sont observés, recherchez les proxys d'application de couche 7 susceptibles de bloquer ou d'abandonner des données. Un cas courant est la fonction d'inspection sur les périphériques Cisco qui agissent sur des protocoles tels que DNS, HTTP ou HTTPS. Pour plus d'informations, référez-vous à notre documentation sur Application de l'inspection de protocole de couche application.

Appliances virtuelles (VA) vers le cloud

Les appliances virtuelles communiquent fréquemment sur le port 443 TCP vers **api.opendns.com**, ainsi que sur le port 53 TCP/UDP pour les requêtes ou les sondes DNS, et sur le port 22, 25, 53, 80, 443 ou 476 TCP pour établir le tunnel de prise en charge. Les appliances virtuelles communiquent avec le cloud à l'aide des ports 53 UDP/TCP, 443 TCP, 123 TCP et 80 TCP. Ils reçoivent des

données des connecteurs sur le port 443 TCP (pas une connexion HTTPS), mais ne nécessitent aucune communication de retour.

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.