Comprendre la prise en charge de plusieurs domaines AD dans Umbrella

Table des matières

Introduction

Ce document décrit la prise en charge de plusieurs domaines AD dans Cisco Umbrella.

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.

Aperçu

La prise en charge de plusieurs domaines Active Directory dans votre organisation parapluie est désormais activée par défaut.

Si vous avez déjà intégré plusieurs domaines AD dans des organisations parapluie distinctes, ces organisations peuvent être consolidées en une seule organisation parapluie avec prise en charge de plusieurs domaines AD. Reportez-vous à cet article pour plus de détails.

Conditions préalables à la prise en charge de plusieurs domaines AD

- Un compte d'utilisateur avec le nom d'ouverture de session OpenDNS_Connector doit être créé dans chaque domaine et être conforme aux exigences spécifiées dans la documentation Umbrella. Il est recommandé de conserver le même mot de passe pour ce compte dans les domaines Active Directory.
- Pour le déploiement avec des appliances virtuelles, un connecteur AD est requis pour chaque domaine AD dans un site Umbrella, avec un second connecteur facultatif pour la redondance si nécessaire.
- Si votre déploiement inclut uniquement des clients itinérants ou AnyConnect, un seul connecteur AD multidomaine* peut synchroniser des utilisateurs/groupes AD à partir de plusieurs domaines. Cela nécessite la création du compte OpenDNS_Connector avec le même mot de passe dans chaque domaine. Cette fonctionnalité n'est pas activée par défaut et vous devez créer un ticket d'assistance pour l'activer.
- Le connecteur Active Directory doit exécuter la version 1.2.3 ou ultérieure.
- Tous les autres pré-requis spécifiés dans la documentation Umbrella sont également applicables pour les domaines multi-AD.

Limites de la prise en charge de plusieurs domaines AD (déploiements d'appareils virtuels)

- L'authentification interdomaine n'est actuellement pas reconnue par le connecteur AD. Si un utilisateur AD s'authentifie auprès d'un contrôleur de domaine local appartenant à un autre domaine AD, le connecteur AD ne peut pas récupérer le mappage utilisateur-IP AD pour cet utilisateur. L'appliance virtuelle ne peut pas associer une identité d'utilisateur à cette adresse IP et, par conséquent, aucune stratégie basée sur Active Directory ne peut être appliquée pour cet utilisateur. La solution de contournement consiste à inclure les contrôleurs de domaine des deux domaines AD dans le même site Umbrella tant que les critères des sites Umbrella (spécifiés dans la documentation Umbrella) ne sont pas affectés.
- Les stratégies globales ne s'appliquent pas aux groupes AD avec des membres interdomaines. Pour créer une stratégie qui s'applique aux utilisateurs de plusieurs domaines, vous devez ajouter les groupes/utilisateurs appropriés de chaque domaine à la stratégie.

Limitations de la prise en charge de plusieurs domaines AD (déploiements de clients itinérants)

- Les déploiements AnyConnect / Client d’itinérance ne sont pas affectés par les limitations d’authentification entre domaines.
- Lorsque la fonctionnalité Connecteur AD multidomaine est activée, Umbrella peut prendre en charge les groupes AD avec des membres de groupes interdomaines. Il faut le demander explicitement en levant un ticket d'assistance. La même fonctionnalité permet également à

un seul connecteur de synchroniser les identités AD de plusieurs domaines AD.

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.