Appliquer les stratégies aux comptes locaux dans Umbrella Active Directory

Table des matières

Introduction

Identification de l'appliance virtuelle et du compte local

- Recommandations pour l'appliance virtuelle Umbrella

Stratégie de compte local et de client d'itinérance Umbrella

- Recommandations pour Umbrella Roaming Client

Introduction

Ce document décrit le comportement de stratégie attendu lors de la synchronisation des produits Umbrella sur site avec Active Directory et les comptes d'utilisateurs locaux.

Identification de l'appliance virtuelle et du compte local

L'appliance virtuelle Umbrella reçoit des informations de connexion Active Directory des contrôleurs de domaine Windows. Il met en cache et identifie les utilisateurs Active Directory en fonction de leur adresse IP source.

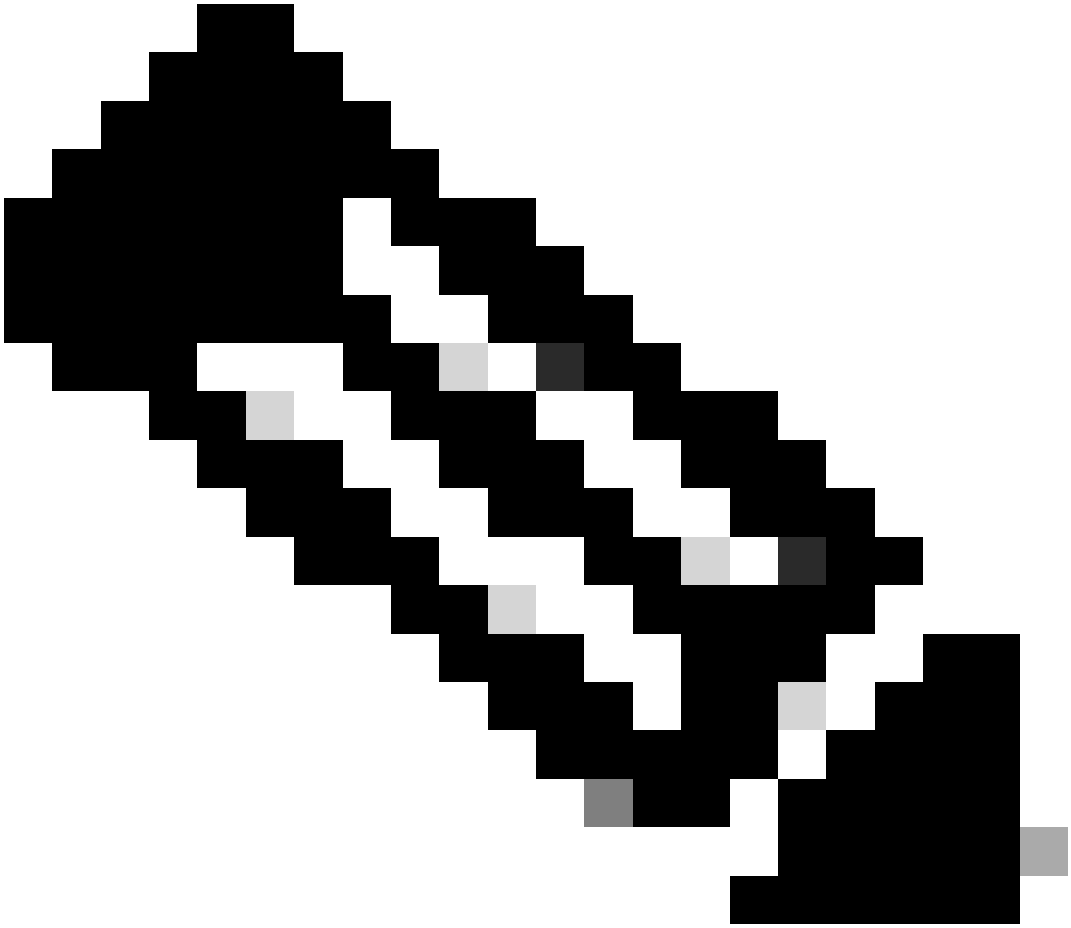
- Le contrôleur de domaine ne suit pas les ouvertures de session des utilisateurs locaux, de sorte que ces utilisateurs ne peuvent pas être directement identifiés par l'appliance virtuelle.
- Si un utilisateur Active Directory s'est récemment connecté à partir d'une adresse IP, l'identité mise en cache peut toujours être utilisée en fonction de notre cache. L'appliance virtuelle n'a aucun moyen de savoir que l'utilisateur Active Directory a été remplacé par un compte local.
- Si aucun utilisateur mis en cache n'est présent, l'appliance virtuelle utilise une identité par défaut (non Active Directory). L'identité déclenchée peut être :
  - Nom du site générique (par exemple, Site par défaut)
  - Réseau interne (adresse IP interne)
  - Réseau (adresse IP externe)

Recommandations pour l'appliance virtuelle Umbrella

- Restreignez l'accès aux comptes et mots de passe locaux.
- Créez une stratégie distincte pour le nom du site Umbrella (par exemple, Site par défaut). Attribuez à cette stratégie une priorité inférieure à votre stratégie utilisateur Active Directory standard. Cette stratégie plus restrictive s'applique lorsqu'aucun utilisateur Active Directory n'est détecté.

- Si vous avez besoin de stratégies différentes pour les comptes d'utilisateurs locaux, envisagez de déployer le client d'itinérance Umbrella.

Stratégie de compte local et de client d'itinérance Umbrella



> Remarque : Pour utiliser l'intégration d'Active Directory avec le client itinérant, accédez à Identités > Ordinateurs itinérants et activez le paramètre Activer l'application de la stratégie de groupe et d'utilisateur Active Directory.

Le client d'itinérance détecte les utilisateurs connectés à partir du Registre Windows, ce qui permet l'identification des utilisateurs Active Directory par leur GUID AD unique.

- Le client d'itinérance ne peut pas identifier les noms d'utilisateur locaux à des fins de stratégie.
- Lorsqu'un utilisateur AD est détecté, l'identité de l'utilisateur AD s'applique à l'application de

la stratégie, y compris les utilisateurs AD connectés avec des informations d'identification mises en cache hors réseau.
- Si aucun utilisateur AD n'est détecté (par exemple, lorsqu'un utilisateur local est connecté), l'identité de l'ordinateur itinérant est utilisée pour l'application de la stratégie.

Recommandations pour Umbrella Roaming Client

- Restreignez l'accès aux comptes et mots de passe locaux.
- Créez une stratégie distincte pour les ordinateurs itinérants avec une priorité inférieure à votre stratégie utilisateur AD standard. Cette stratégie s'applique aux ordinateurs itinérants qui ne sont pas associés au domaine ou qui ne sont pas utilisés par des utilisateurs locaux.

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.