Comprendre le chiffrement Umbrella pour la synchronisation AD

Table des matières

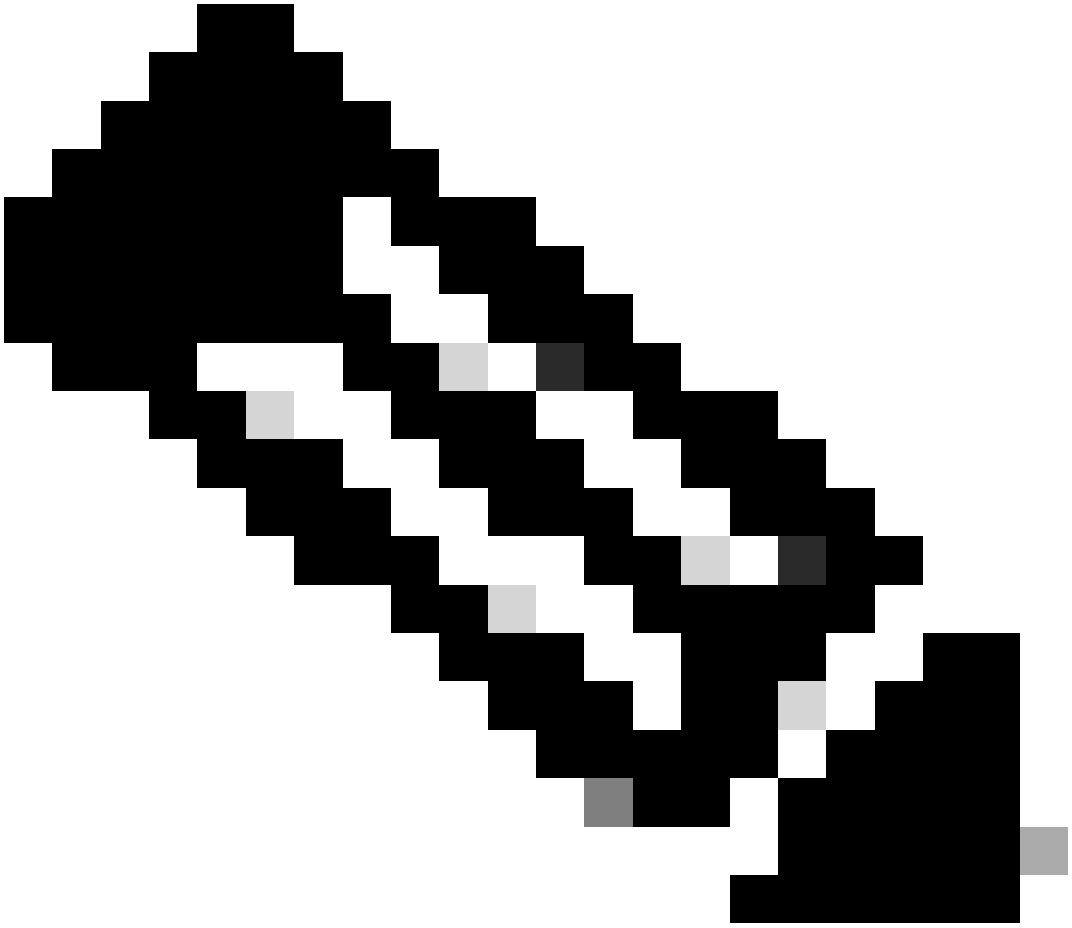
Introduction

Ce document décrit le chiffrement Umbrella pour la synchronisation AD, comme la façon dont ce transfert de données est chiffré.

Informations générales

Le logiciel Umbrella AD Connector récupère les détails des informations d'utilisateur, d'ordinateur et de groupe à partir de votre contrôleur de domaine AD à l'aide du protocole LDAP. Seuls les attributs nécessaires sont stockés à partir de chaque objet, notamment sAMAccountName, dn, userPrincipalName, memberOf, objectGUID, primaryGroupId (pour les utilisateurs et les ordinateurs) et primaryGroupToken (pour les groupes).

Ces données sont ensuite téléchargées dans Umbrella pour être utilisées dans la configuration des stratégies et la création de rapports. Ces données sont également requises pour le filtrage par utilisateur ou par ordinateur.



Remarque : objectGUID est envoyé sous forme hachée.

Pour savoir exactement ce qui est synchronisé, vous pouvez consulter les fichiers .ldif contenus dans :

```
C:\Program Files\OpenDNS\OpenDNS Connector\ADSync\*.ldif
```

Cet article décrit comment ce transfert de données est chiffré.

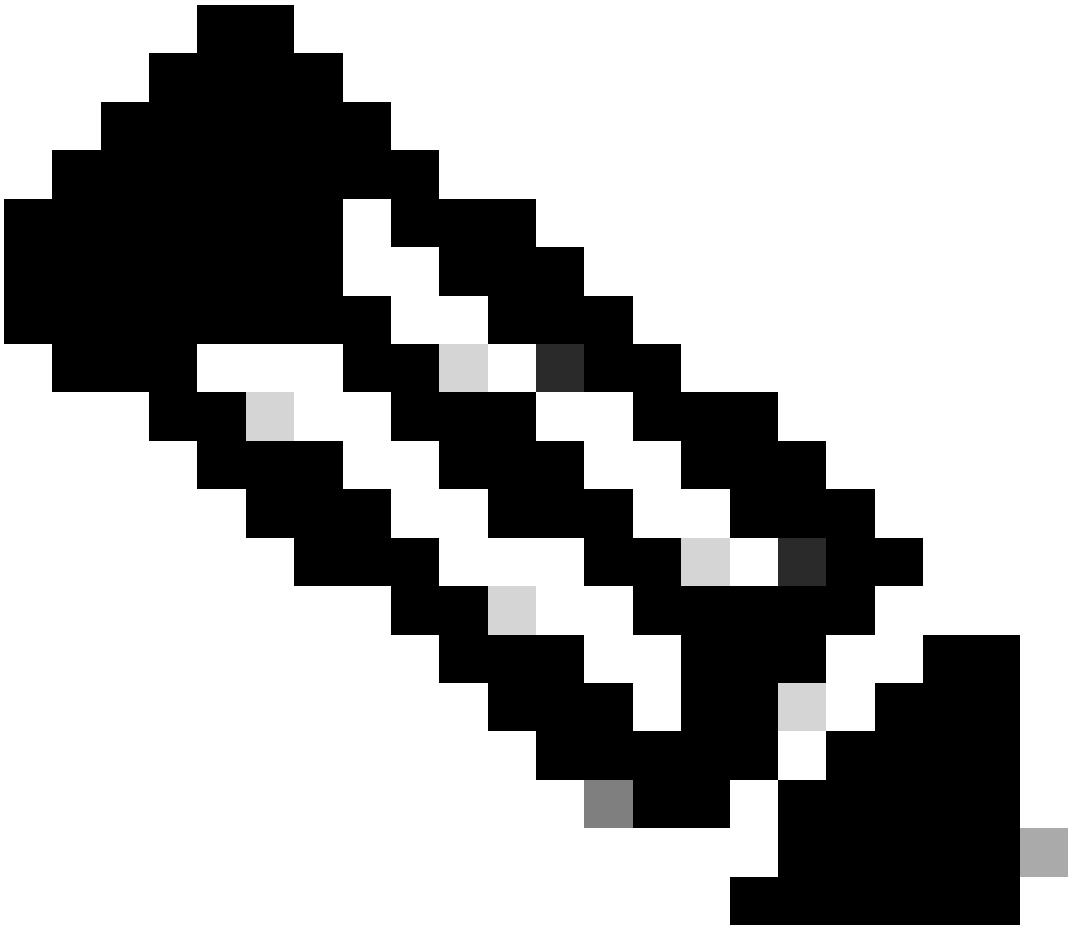
Chiffrement pour le téléchargement des données AD

Le connecteur AD Umbrella télécharge les informations AD vers Umbrella à l'aide d'une connexion HTTPS sécurisée. Le transfert entre le cloud Connector <> Umbrella est toujours chiffré.

Cryptage pour récupération des données AD

À partir de la version 1.1.2, le connecteur tente désormais de récupérer les détails utilisateur avec le chiffrement entre le connecteur du contrôleur de domaine <>. Deux méthodes sont tentées :

- LDAPS. Les données sont transmises via un tunnel sécurisé.
- LDAP avec authentification Kerberos. Assure le chiffrement au niveau des paquets.



> Remarque : LDAPS n'est pas utilisé lorsque le logiciel Connector est exécuté sur le même serveur que le contrôleur de domaine utilisé pour ADsync.

Si cette tentative échoue pour une raison quelconque, elle revient à ce mécanisme :

- LDAP avec authentification NTLM. Cela permet une authentification sécurisée, mais le transfert de données entre le DC > Connector se fait sans cryptage.

Pour vous assurer que le cryptage est possible, nous vous recommandons de :

- Activez LDAPS sur votre ou vos contrôleurs de domaine. Cela dépasse le cadre de la prise en charge d'Umbrella, mais peut être activé avec la documentation de Microsoft.
- Assurez-vous que le nom d'hôte de votre ou vos contrôleurs de domaine est correctement configuré dans « Déploiements > Sites et Active Directory ». Le nom d'hôte correct est requis pour les deux méthodes de cryptage. Si le nom d'hôte est incorrect pour une raison quelconque, nous vous recommandons de réenregistrer le contrôleur de domaine à l'aide de notre script de configuration, ou de contacter le support Umbrella.

Pour confirmer le cryptage. Vous pouvez consulter le fichier journal ici :

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\OpenDNSAuditClient.log
```

Pendant la synchronisation Active Directory, vous voyez des entrées de journal telles que :

Connexion LDAPS réussie :
Utilisation de SSL pour la communication <SERVER> pour récupérer le DN.

Authentification Kerberos réussie :
Utilisation de Kerberos pour la communication <SERVER> pour récupérer le DN.

Mécanisme de re-basculement NTLM utilisé :
Échec de Kerberos pour l'hôte DC <SERVER>. Le nom d'hôte peut être incorrect. Retour à la requête NTLM.

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.