Umbrella Encryption für AD Sync verstehen

Inhalt

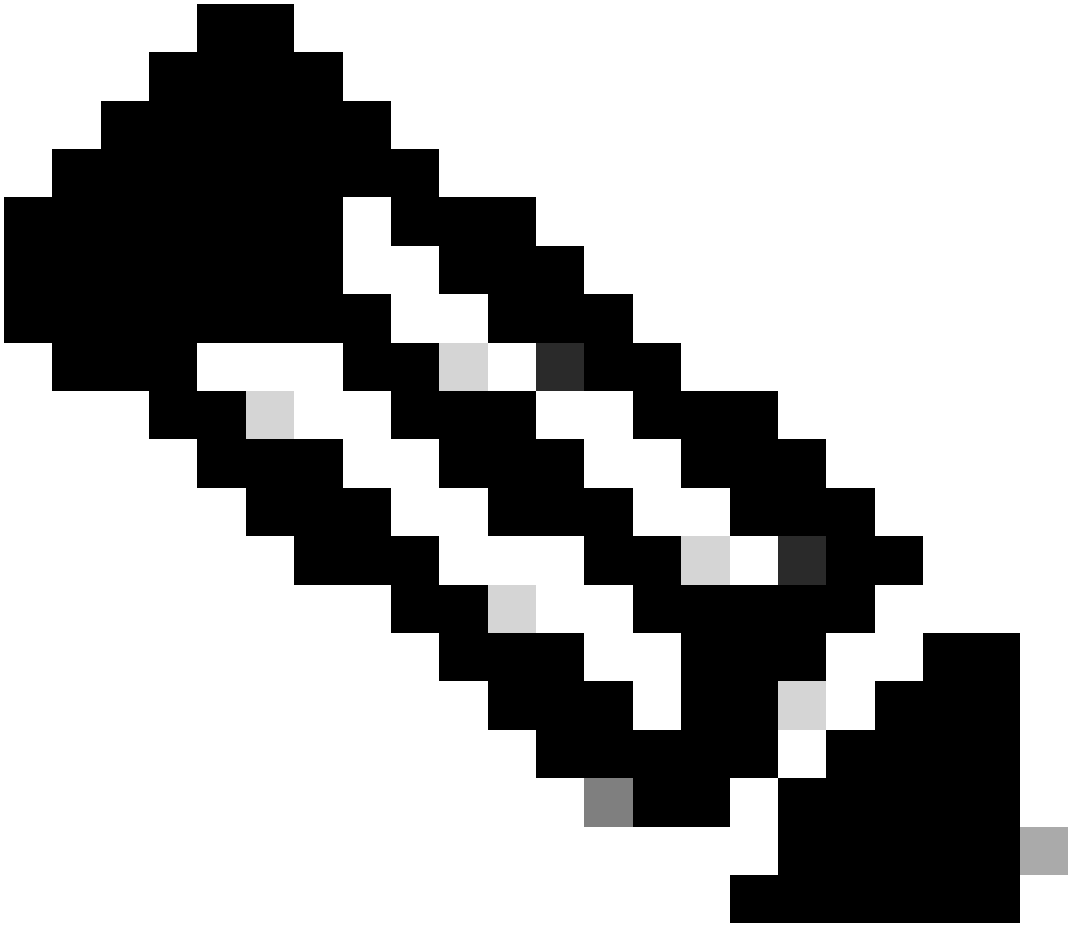
Einleitung

In diesem Dokument wird die Umbrella-Verschlüsselung für die AD-Synchronisierung beschrieben, z. B. wie diese Datenübertragung verschlüsselt wird.

Hintergrundinformationen

Die Umbrella AD Connector-Software ruft Details zu Benutzer-, Computer- und Gruppeninformationen mithilfe von LDAP von Ihrem AD Domain Controller ab. Von jedem Objekt werden nur die erforderlichen Attribute gespeichert. Dazu gehören sAMAccountName, dn, userPrincipalName, memberOf, objectGUID, primaryGroupId (für Benutzer und Computer) und primaryGroupToken (für Gruppen).

Diese Daten werden dann zur Verwendung in der Richtlinienkonfiguration und für das Reporting an Umbrella hochgeladen. Diese Daten sind auch für die Filterung nach Benutzer oder Computer erforderlich.



Anmerkung: objectGUID wird in Hashform gesendet.

Um herauszufinden, was genau synchronisiert wird, sehen Sie sich die .ldif-Dateien an, die in folgenden Dateien enthalten sind:

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

In diesem Artikel wird beschrieben, wie diese Datenübertragung verschlüsselt wird.

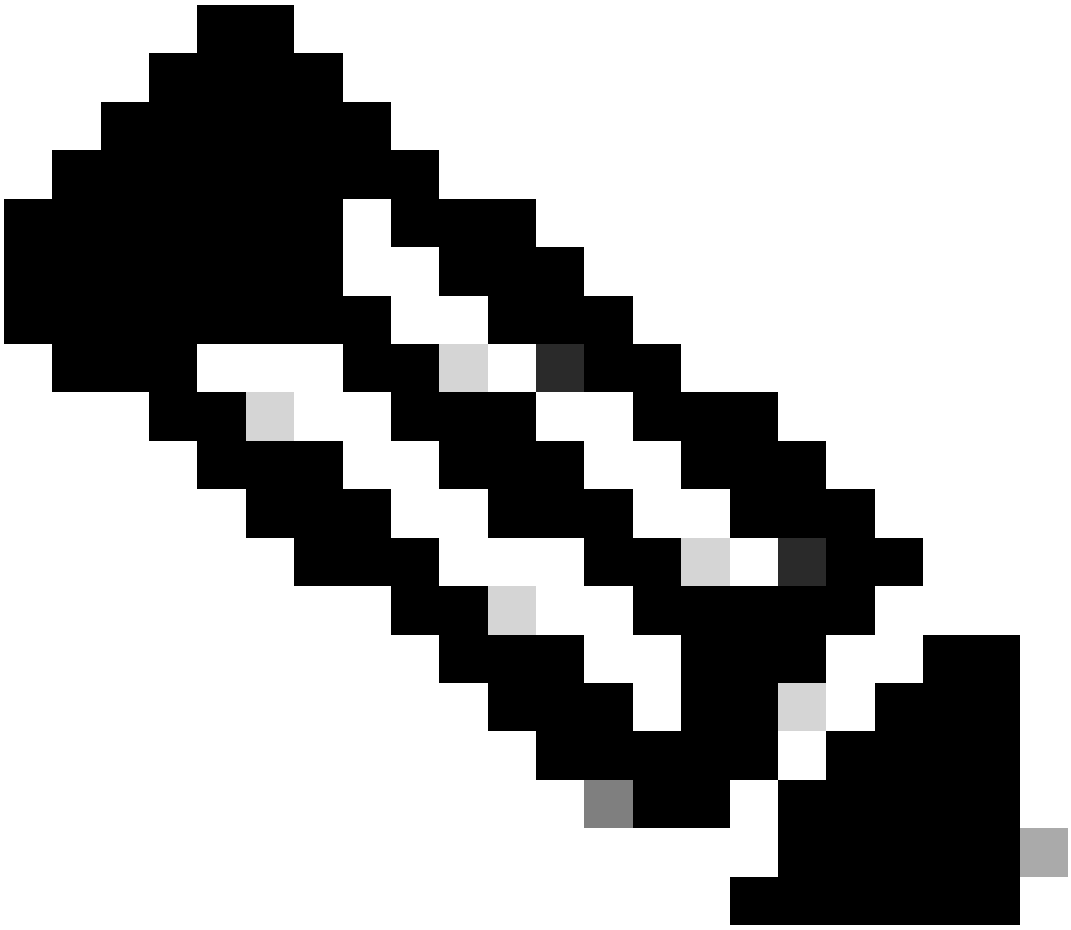
Verschlüsselung für AD-Daten-Upload

Der Umbrella AD Connector lädt die AD-Informationen über eine sichere HTTPS-Verbindung nach Umbrella hoch. Der Upload zwischen der Connector **<>** Umbrella Cloud ist immer verschlüsselt.

Verschlüsselung für den AD-Datenabruf

Ab Version 1.1.22 versucht der Connector jetzt, Benutzerdetails mit Verschlüsselung zwischen dem Connector des Domänencontrollers **<>** abzurufen. Es werden zwei Methoden versucht:

- LDAPS. Die Daten werden über einen sicheren Tunnel übertragen.
- LDAP mit Kerberos-Authentifizierung. Bietet Verschlüsselung auf Paketebene.



> Anmerkung: LDAPS wird nicht verwendet, wenn die Connector-Software auf demselben Server wie der für ADsync verwendete Domänencontroller ausgeführt wird.

Wenn dieser Versuch aus irgendeinem Grund fehlschlägt, wird auf diesen Mechanismus zurückgegriffen:

- LDAP mit NTLM-Authentifizierung. Dies ermöglicht eine sichere Authentifizierung, aber die Datenübertragung zwischen DC **>** Connector erfolgt ohne Verschlüsselung.

Um sicherzustellen, dass die Verschlüsselung möglich ist, empfehlen wir Folgendes:

- Aktivieren Sie LDAPS auf Ihren Domänencontrollern. Dieser Umbrella-Support ist nicht abgedeckt, kann jedoch mit der Dokumentation von Microsoft aktiviert werden.
- Stellen Sie sicher, dass der Hostname Ihres Domänencontrollers bzw. Ihrer Domänencontroller unter "Bereitstellungen > Standorte und AD" korrekt konfiguriert ist. Für beide Verschlüsselungsmethoden ist der richtige Hostname erforderlich. Wenn der Hostname aus irgendeinem Grund falsch ist, empfehlen wir, den Domain Controller mithilfe unseres Konfigurationsskripts neu zu registrieren, oder wenden Sie sich an den Umbrella-Support.

Bestätigung der Verschlüsselung. Sie können die Protokolldatei hier überprüfen:

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

Während der AD-Synchronisierung werden folgende Protokolleinträge angezeigt:

LDAPS-Verbindung erfolgreich:
Verwenden von SSL für die <SERVER>-Kommunikation zum Abrufen der DN.

Kerberos-Authentifizierung erfolgreich:
Verwenden von Kerberos für die <SERVER>-Kommunikation zum Abrufen des DN.

Verwendeter NTLM-Failback-Mechanismus:
Fehler bei Kerberos für DC-Host <SERVER>. Der Hostname kann ungültig sein. Zurückgreifen auf die NTLM-Abfrage.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.