Descripción de Umbrella Encryption para AD Sync

Contenido

Introducción

Antecedentes

Cifrado para carga de datos de AD

Cifrado para recuperación de datos de AD

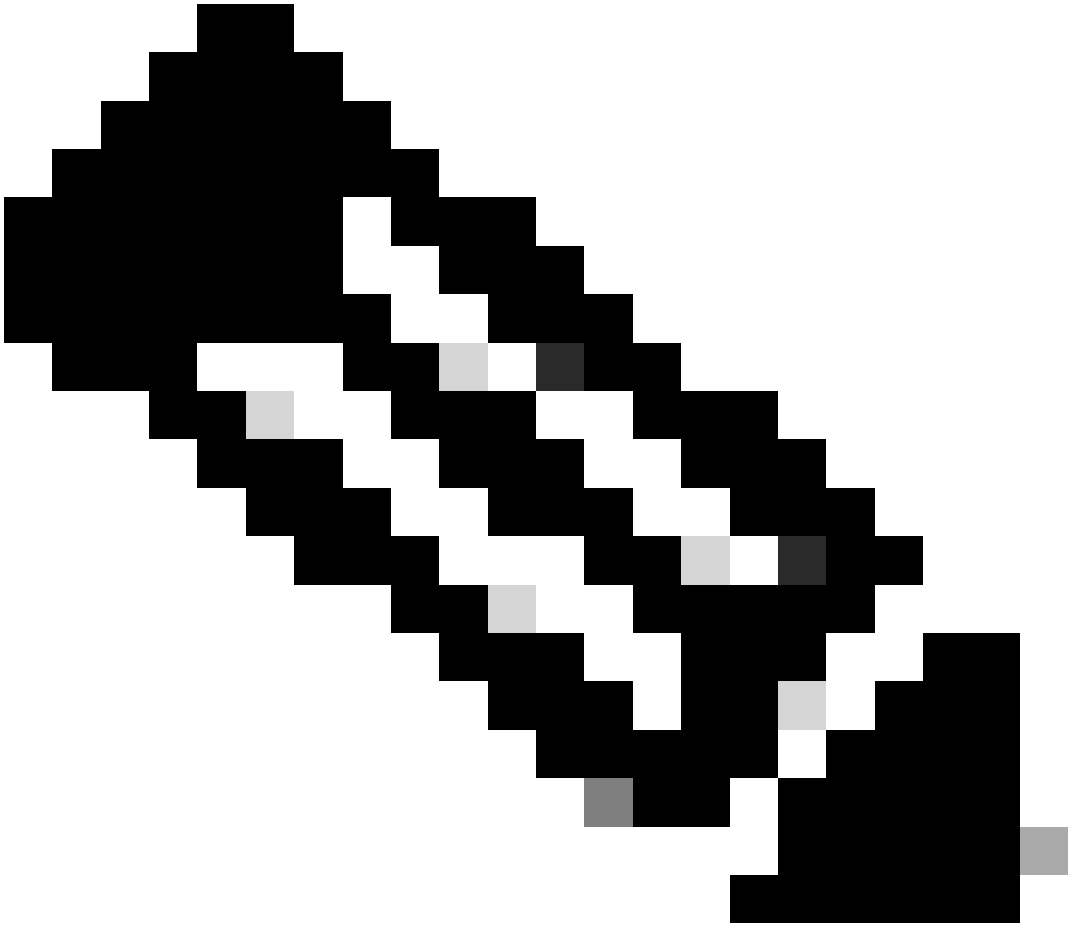
Introducción

Este documento describe el cifrado de Umbrella para la sincronización de AD, por ejemplo, cómo se cifra esta transferencia de datos.

Antecedentes

El software Umbrella AD Connector recupera los detalles de la información de usuario, equipo y grupo de su controlador de dominio AD mediante LDAP. Sólo se almacenan los atributos necesarios de cada objeto, incluidos sAMAccountName, dn, userPrincipalName, memberOf, objectGUID, primaryGroupId (para usuarios y equipos), y primaryGroupToken (para grupos).

Estos datos se cargan en Umbrella para su uso en Configuración de políticas e informes. Estos datos también son necesarios para el filtrado por usuario o por equipo.



Nota: objectGUID se envía en forma de hash.

Para averiguar exactamente qué se está sincronizando, puede ver los archivos .ldif que contiene:

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

En este artículo se describe cómo se cifra esta transferencia de datos.

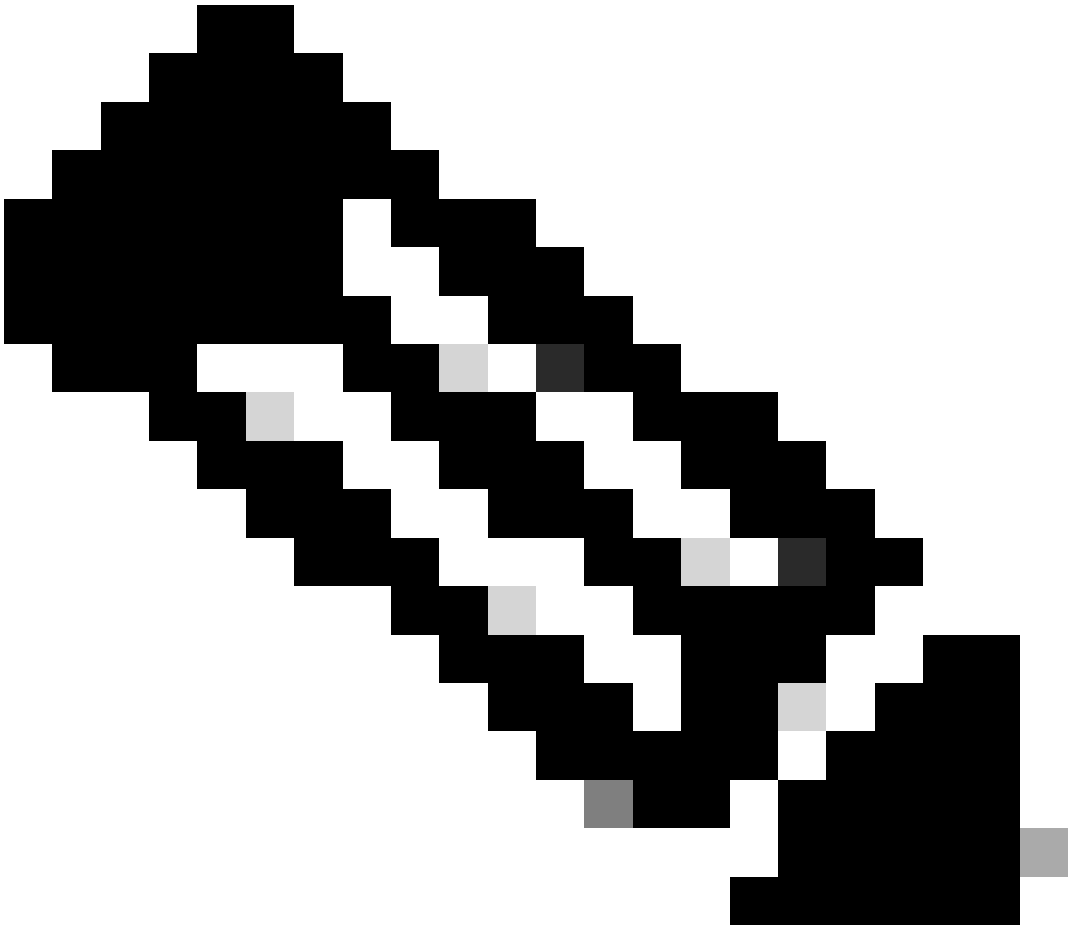
Cifrado para carga de datos de AD

El conector de Umbrella AD carga la información de AD en Umbrella mediante una conexión HTTPS segura. La carga entre la nube Connector <> Umbrella siempre está cifrada.

Cifrado para recuperación de datos de AD

A partir de la versión 1.1.22, el conector intenta ahora recuperar los detalles del usuario con cifrado entre el conector del controlador de dominio <>. Se intentan dos métodos:

- LDAPS. Los datos se transmiten a través de un túnel seguro.
- LDAP con autenticación Kerberos. Proporciona cifrado de nivel de paquete.



> Nota: LDAPS no se utiliza cuando el software del conector se ejecuta en el mismo servidor que el controlador de dominio utilizado para ADsync.

Si este intento falla por alguna razón, vuelve a este mecanismo:

- LDAP con autenticación NTLM. Esto proporciona autenticación segura pero la transferencia de datos entre el DC > Connector sucede sin encripción.

Para garantizar que el cifrado es posible, recomendamos:

- Habilite LDAPS en sus controladores de dominio. Esto va más allá de la compatibilidad con Umbrella, pero se puede habilitar con la documentación de Microsoft.
- Asegúrese de que el nombre de host de sus controladores de dominio esté configurado correctamente en 'Implementaciones > Sitios y AD'. Se requiere el nombre de host correcto para ambos métodos de cifrado. Si el nombre de host es incorrecto por alguna razón, recomendamos volver a registrar el controlador de dominio mediante nuestro script de configuración o ponerse en contacto con el servicio de soporte técnico de Umbrella.

Para confirmar que se está realizando el cifrado. Puede consultar el archivo de registro aquí:

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

Durante la sincronización de AD, verá entradas de registro como:

Conexión LDAPS correcta:
Uso de SSL para la comunicación <SERVER> para obtener el DN.

Autenticación Kerberos satisfactoria:
Uso de Kerberos para la comunicación <SERVER> para obtener el DN.

Mecanismo de conmutación por recuperación NTLM en uso:
Error de Kerberos para el host DC <SERVER>. El nombre de host puede no ser válido. Volver a la consulta NTLM.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).