# Entender a criptografia Umbrella para AD Sync

## Contents



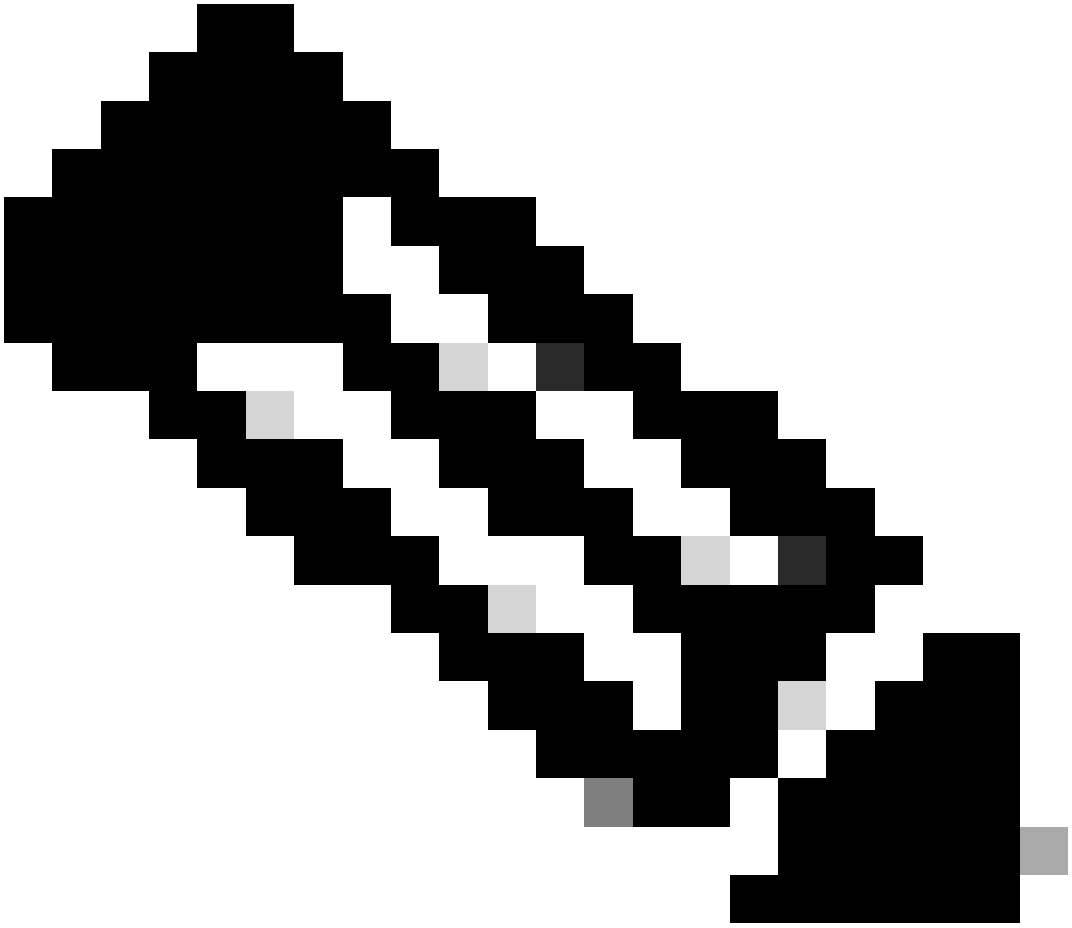
## Introdução

Este documento descreve a criptografia Umbrella para sincronização do AD, por exemplo, como essa transferência de dados é criptografada.

## Informações de Apoio

O software Umbrella AD Connector recupera detalhes das informações de Usuário, Computador e Grupo do Controlador de Domínio do AD usando LDAP. Somente os atributos necessários são armazenados de cada objeto, incluindo sAMAccountName, dn, userPrincipalName, memberOf, objectGUID, primaryGroupId (para usuários e computadores), e primaryGroupToken (para grupos).

Em seguida, esses dados são carregados no Umbrella para uso na Configuração e Relatórios de Políticas. Esses dados também são necessários para filtragem por usuário ou por computador.



Note: objectGUID é enviado no formato com hash.

Para descobrir exatamente o que está sendo sincronizado, você pode examinar os arquivos .ldif contidos em:

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

Este artigo descreve como essa transferência de dados é criptografada.

## Criptografia para carregamento de dados do AD

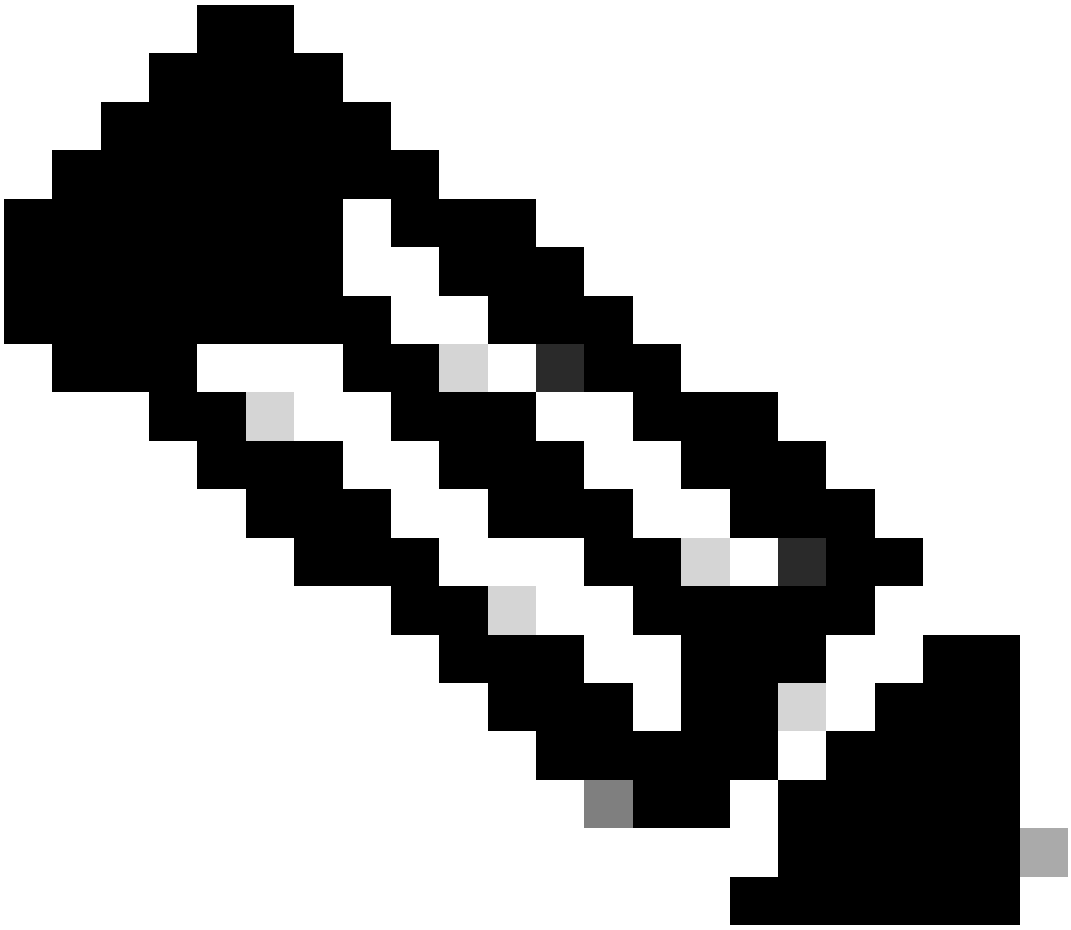
O Umbrella AD Connector carrega as informações do AD no Umbrella usando uma conexão HTTPS segura. O carregamento entre a nuvem do Connector <> Umbrella é sempre criptografado.

# Criptografia para recuperação de dados do AD

A partir da versão 1.1.22, o Conector agora tenta recuperar os detalhes do usuário com criptografia entre o Conector do Controlador de Domínio <>. Dois métodos são tentados:

- LDAPS. Os dados são transmitidos por um túnel seguro.
- LDAP com autenticação Kerberos. Fornece criptografia em nível de pacote.

---



> Note: LDAPS não é usado quando o software do Conector está sendo executado no mesmo servidor que o Controlador de Domínio usado para ADsync.

---

Se essa tentativa falhar por algum motivo, ela reverte para esse mecanismo:

- LDAP com autenticação NTLM. Isso fornece autenticação segura, mas a transferência de dados entre o conector DC > acontece sem criptografia.

Para garantir que a criptografia seja possível, recomendamos:

- Habilite LDAPS no(s) Controlador(es) de Domínio. Isso está além do escopo do suporte Umbrella, mas pode ser habilitado com a documentação da Microsoft.
- Certifique-se de que o nome de host do(s) seu(s) Controlador(es) de Domínio esteja(m) corretamente configurado em 'Implantações > Locais e AD'. O nome de host correto é necessário para ambos os métodos de criptografia. Se o nome do host estiver incorreto por qualquer motivo, recomendamos registrar novamente o Controlador de Domínio usando nosso script de configuração ou contatar o suporte do Umbrella.

Para confirmar se a criptografia está ocorrendo. Você pode verificar o arquivo de log aqui:

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

Durante a sincronização do AD, você vê entradas de log como:

Conexão LDAPS bem-sucedida:
Usando SSL para comunicação <SERVER> para buscar o DN.

Autenticação Kerberos bem-sucedida:
Usando Kerberos para comunicação <SERVER> para buscar o DN.

Mecanismo de failback NTLM em uso:
Falha de Kerberos para o Host DC <SERVER>. O nome de host pode ser inválido. Retornando à consulta NTLM.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.