了解AD同步的Umbrella加密

目录

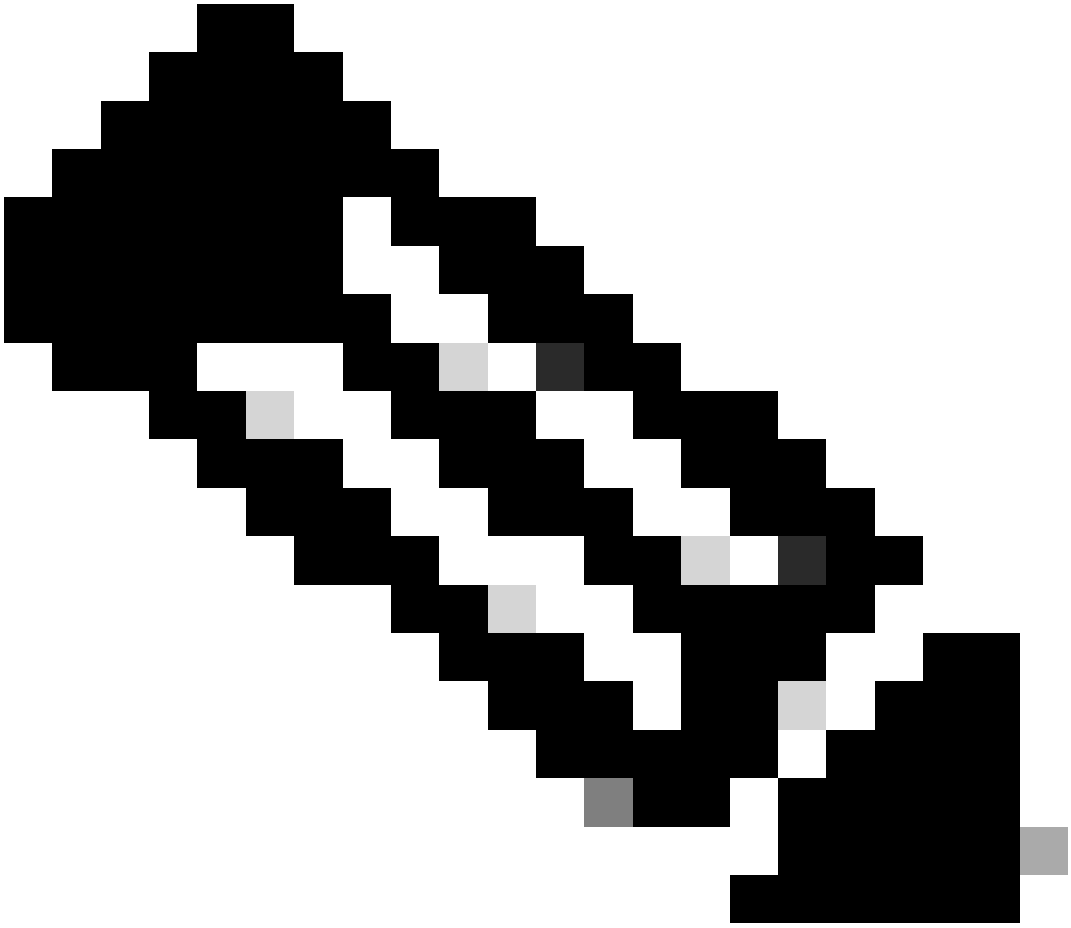
简介

本文档介绍用于AD同步的Umbrella加密，例如如何加密此数据传输。

背景信息

Umbrella AD连接器软件使用LDAP从AD域控制器检索用户、计算机和组信息的详细信息。仅存储每个对象中必要的属性，其中包括sAMAccountName、dn、userPrincipalName、memberOf、objectGUID、primaryGroupId（用于用户和计算机）和primaryGroupToken（用于组）。

然后，此数据上传到Umbrella，用于策略配置和报告。每用户或每计算机过滤也需要此数据。



注意：objectGUID以散列形式发送。

要确切了解正在同步的内容，您可以查看以下内容中包含的.ldif文件：

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

本文描述如何加密此数据传输。

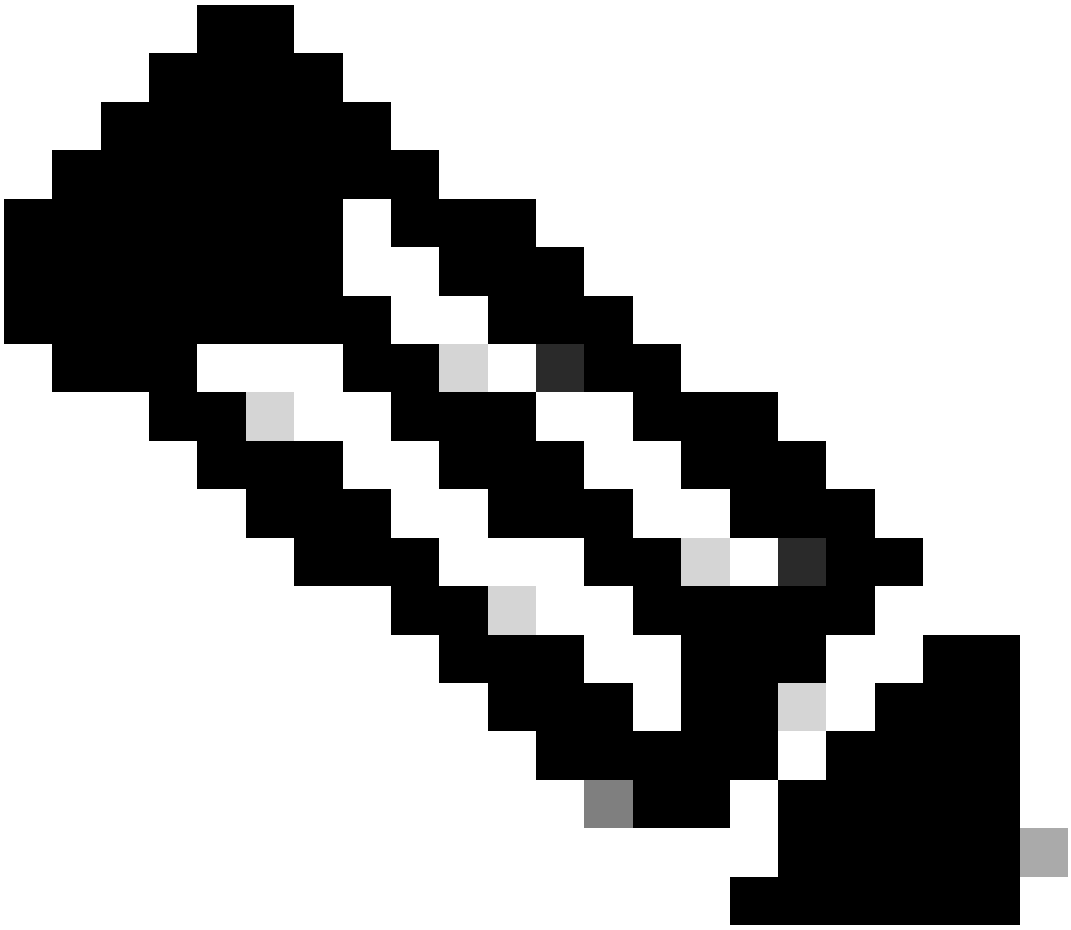
AD数据上传加密

Umbrella AD连接器使用安全的HTTPS连接将AD信息上传到Umbrella。Connector <> Umbrella云之间的上传始终是加密的。

AD数据检索加密

从v1.1.22开始，连接器现在尝试在域控制器<>连接器之间使用加密来检索用户详细信息。尝试两种方法：

- LDAPS。数据通过安全隧道传输。
- 采用Kerberos身份验证的LDAP。提供数据包级加密。



注意：当连接器软件与用于ADsync的域控制器在同一服务器上运行时，不使用LDAPS。

如果此尝试因任何原因而失败，它将恢复此机制：

- 使用NTLM身份验证的LDAP。这提供了安全的身份验证，但DC > Connector之间的数据传输没有加密。

为确保可以加密，我们建议：

- 在域控制器上启用LDAPS。 这不属于Umbrella支持的范围，但可以使用Microsoft的文档启用。
- 确保在“Deployments > Sites and AD”中正确配置了域控制器的主机名。两种加密方法都需要正确的主机名。如果主机名因任何原因不正确，我们建议使用我们的配置脚本重新注册域控制器，或者联系Umbrella支持。

确认加密正在进行。您可以在此处检查日志文件：

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

在AD同步期间，您会看到以下日志条目：

LDAP连接成功：
使用SSL进行<SERVER>通信以获取DN。

Kerberos身份验证成功：
使用Kerberos进行<SERVER>通信以获取DN。

正在使用的NTLM故障回复机制：
DC主机<SERVER>的Kerberos失败。主机名可能无效。回退到NTLM查询。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。