解析OpenDNS_Connector Kerberos或LDAP登录错误事件

目录

简介

本文档介绍在找不到登录事件报告DN时，如何解决OpenDNS_Connector用户的Kerberos或LDAP登录错误。

问题

本文适用于连接器错误，其中对Kerberos和LDAP的身份验证失败，但仍然找到登录事件。登录事件表示“找不到DN”。

解决方案

必须验证并更新opendns_connector用户的UserPrincipalName属性：

1.打开opendns_connector帐户的用户属性。

2.确保使用帐户的电子邮件地址定义“UserPrincipalName”。

3.将UserPrincipalName值与另一个帐户进行比较，以确认格式和预期定义。

4.如有必要，请更新该值。

填充UserPrincipalName字段后，连接器可以恢复正常操作。

原因

由于用户名未知或密码错误，登录失败。日志在仍找到事件时显示问题，但系统会报告“DN not found”。

例如：

```
Logon failure: unknown user name or bad password.
```

7/22/2019 3:16:01 PM: Using NTLM for LDAP://10.0.0.31:389/DC=Nephrology,DC=com communication to fetch t

7/16/2019 4:33:18 PM: DN not found!

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）。