OpenDNS_Connector KerberosまたはLDAPログインエラーイベントの解決

内容

はじめに

このドキュメントでは、ログインイベントがDN not foundを報告する場合に、OpenDNS_ConnectorユーザのKerberosまたはLDAPログインエラーを解決する方法について説明します。

問題

この記事は、KerberosおよびLDAPへの認証が失敗するが、ログインイベントが引き続き検出されるコネクタエラーに適用されます。ログインイベントは「DN not found」を示します。

解決方法

opendns_connectorユーザのUserPrincipalNameプロパティを確認し、更新する必要があります。

1. opendns_connectorアカウントのユーザープロパティを開きます。

2. 「UserPrincipalName」がアカウントのメールアドレスで定義されていることを確認します。

3. UserPrincipalName値を別のアカウントと比較して、形式と想定される定義を確認します。

4. 必要に応じて値を更新します。

UserPrincipalNameフィールドに値を入力すると、コネクタは適切な操作を再開できます。

原因

不明なユーザー名または無効なパスワードが原因で、ログオンに失敗しました。イベントがまだ見つかっても、システムが「DN not found」をレポートするため、ログに問題が表示されます。

例：

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!

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。