Resolve OpenDNS_Connector Kerberos or LDAP Log in Error Events

Contents

Introduction

This document describes how to resolve Kerberos or LDAP login errors for the OpenDNS_Connector user when login events report DN not found.

Problem

This article applies to Connector errors where authentication to Kerberos and LDAP fails, but login events are still found. Login events indicate "DN not found."

Solution

You must verify and update the UserPrincipalName property for the opendns_connector user:

1. Open the user properties for the opendns_connector account.

2. Ensure the "UserPrincipalName" is defined with the email address of the account.

3. Compare the UserPrincipalName value to another account to confirm format and expected definition.

4. Update the value if necessary.

Once you populate the UserPrincipalName field, the connector can resume proper operation.

Cause

A logon failure occurs due to an unknown user name or bad password. The logs display the issue as events are still found, but the system reports "DN not found."

For example:

```
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!