NetApp Knowledge Base

# Users authenticated by an LDAP server randomly face "Access Denied" errors

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/Users_authe…

Updated: Wed, 31 Aug 2022 14:26:08 GMT

## Applies to

- ONTAP 9
- LDAP client with Centrify LDAP servers
- UNIX authentication with auth-sys-extended-groups
- Multiprotocol environment & Name-Mapping unix-win or win-unix

## Issue

Users experience random "Access Denied" errors when trying to access data they normally have access to. The error will remain for 24 hours until it is cleared.

## Cause

Two causes have been identified:

1. The LDAP server does not respond to the search query within the defined query timeout threshold.
2. The LDAP server randomly returns a noSuchObject error in the search response, although the UID in the search query exists

## Solution

Multiple steps can be taken to resolve and/or workaround this issue:

- From ONTAP:
  - The query timeout value can be increased up to 10 seconds in the LDAP client configuration
  - A user-dn and group-dn can be configured to limit the search scope for Users and Groups to specific paths as opposed to the entire catalog
  - Once the issue occured, clearing the name-service group-membership cache and nfs credential cache will force ONTAP to query one more time the LDAP server for the user information.

- In order to resolve this issue on the long term, contact NetApp Technical Support to collect data and packet traces, then open a support case with your LDAP server vendor for further assistance.

## Additional Information

additionalInformation_text