NetApp® Knowledge Base

Access issues seen due to intermittent LDAP server down issue

Applies to

- Ontap 9.x
- LDAP
- CIFS
- NFS

Issue

- Access issues seen due to LDAP server intermittently going down
- Below error message seen in EMS logs

```
Sat Apr 12 12:48:48 +0200 [nodeA: secd: secd.nfsAuth.noUnixCreds:error]:
```

```
Vserver "vs1" cannot determine UNIX identity. Error: Acquire UNIX extended
credentials procedure failed **[  5002] FAILURE: Timed out waiting for a
LDAP (NIS & Name Mapping) connection after 5 seconds   [  5002] Unable to
make a connection (LDAP (NIS & Name Mapping):), Result:
RESULT_ERROR_SECD_CONNECTION_WAIT_TIMEOUT   [  5002] Failed to get user
info for id '391909'   [  5002] Source: LDAP unavailable. Ignoring and
trying next available source for user-id:
```

- Multiple LDAP servers are configured, Ontap is trying to connect to first LDAP server in list and it is timing out.

```
clus01::> ldap client show -vserver vs1 -instance
                             Vserver: vs1
           Client Configuration Name: ldap
                     LDAP Server List: ldap1.server.local,
                                       ldap2.server.local,
                                       ldap3.server.local,
                                       ldap4.server.local
```

- Pings to all LDAP servers are successful.
- LDAP check for timing out server is showing as below

```
clus01::> ldap check -vserver vs1
                 Vserver: vs1
Client Configuration Name: ldap
           LDAP Status: down
      LDAP Status Details: Error: Validate the Ldap configuration
procedure failed
**[  5000] FAILURE: Timed out waiting for a LDAP (NIS & Name
**          Mapping) connection after 5 seconds
   [  5000] Unable to make a connection (LDAP (NIS & Name Mapping):),
           Result: RESULT_ERROR_SECD_CONNECTION_WAIT_TIMEOUT
     LDAP DN Status Details: No LDAP DN configured
```

- LDAP check for working vserver is as below.

```
ldap check -vserver vs6
                 Vserver: vs6
Client Configuration Name: ldap
           LDAP Status: up
      LDAP Status Details: Successfully connected to LDAP server
```

```
        "10.2x.xxx.xx".
            LDAP DN Status Details: All the configured DNs are available.
```

- High number of LDAP queued requests are seen
- Issue resolves after rebooting the impacted LDAP server and resurfaces after sometime or few days
- Below logs can be collected to troubleshoot and isolate the issue.
    - When issue occurs start collecting packet traces, secd logging, sktrace logging, invoke ASUP.
    - Perform ldap check : `ldap check -vserver <>`
    - Ping all the LDAP servers : `network ping -vserver <> -lif <> - destination <>`
    - Invoke asup : `autosupport invoke -node * - type all -message "before traces"`
    - Start packet trace : `network trace start -node * -port <> -file-size 1024 -buffer-size 512 - rolling-traces 5`
    - Start sktrace : `systemshell -node * -command sudo sysctl sysvar.sktrace.CIFS_AUTH_enable=-1`
    - Start secd traces : `diag secd trace set -node * -vserverids <> -trace-all yes`
    - Invoke asup : `autosupport invoke -node * - type all -message "after traces"`
    - Once the issue is resolved by rebooting the ldap server, stop the logging so that the logs will not roll out.
    - Packet trace : `network trace stop -node * -port <>`
    - Sktrace : `systemshell -node * -command sudo sysctl sysvar.sktrace.CIFS_AUTH_enable=-0`
    - Secd : `diag secd trace set -node * -vserverids <> -trace-all no`
    - Perform ldap check : `ldap check -vserver <>`