



NASLORD

LDAP CONFIGURATION GUIDE (SUPER-USERS)



Gallium Inc.

1250 Rene-Levesque W. Montreal (Quebec) H3B 4W8

NASLORD 3.0.0

LDAP Configuration Guide (Super-Users)

Version: 3.0.0

Date: 2026-07-14

Product: NASLord

Vendor: Gallium Inc.

Audience: Super-users (NASLord administrators)



TABLE OF CONTENTS

1. Configure DNS on the NASLord Instance.....	3
2. Create required groups and users on the Domain Controller	3
Create allowed-users security group in the DC Organizational Unit	
Create denied-users security group in the DC Organizational Unit	
Create super-users security group in the DC Organizational Unit	
Create a user used as service account	
3. Configure Certificate CA services on the Domain Controller	4
4. Validate Certificate and LDAP connection	16
5. Get the certificate using CMD (Command Prompt) - Method 1	20
6. Get the certificate using AD CS and Certificate Export - Method 2.....	21
7. NASLord LDAP configuration	27



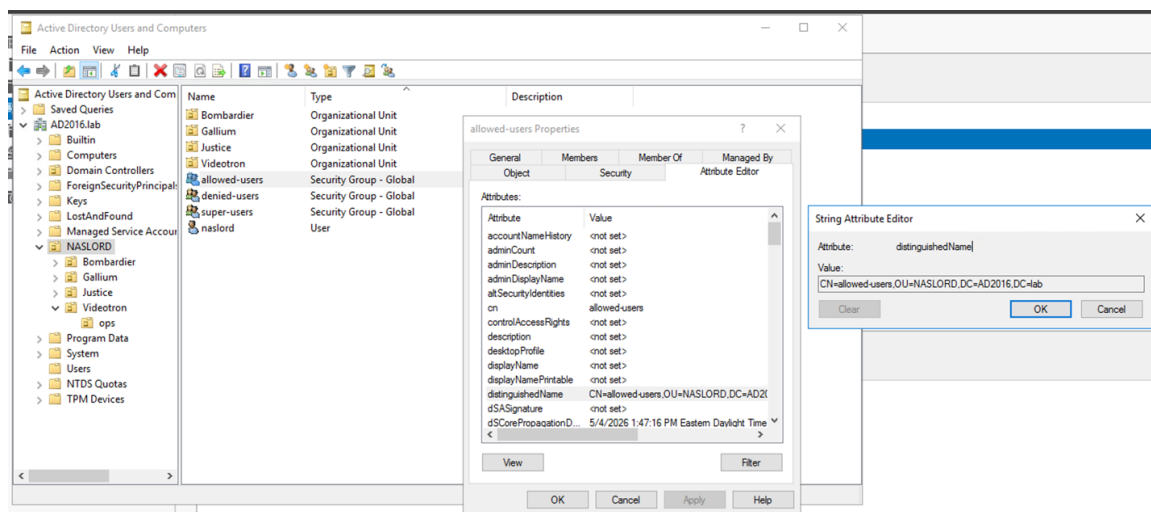
1. CONFIGURE DNS ON THE NASLORD INSTANCE (SKIP IF DNS IP ADDRESS IS ALREADY CONFIGURED):

- Open a web console on NASLord instance through your Hypervisor, login and enter *configure* to execute the configuration script.
- Type *Y* on the *change network configuration prompt* and hit *Enter*.
- Type *N* on *enable DHCP* and hit *enter*.
- Enter the FQDN, IPs and DNS IPs.
- Once the configure script is done, reboot the instance.

2. CREATE REQUIRED GROUPS AND USERS ON THE DOMAIN CONTROLLER:

- Create allowed-users security group in the DC Organizational Unit
- Create denied-users security group in the DC Organizational Unit
- Create super-users security group in the DC Organizational Unit
- Create a user used as service account to link the NASLord instance to the DC LDAPS server.
- Gather the previously created groups/user *distinguished names* and save for later for the NASLord instance LDAPS configuration.

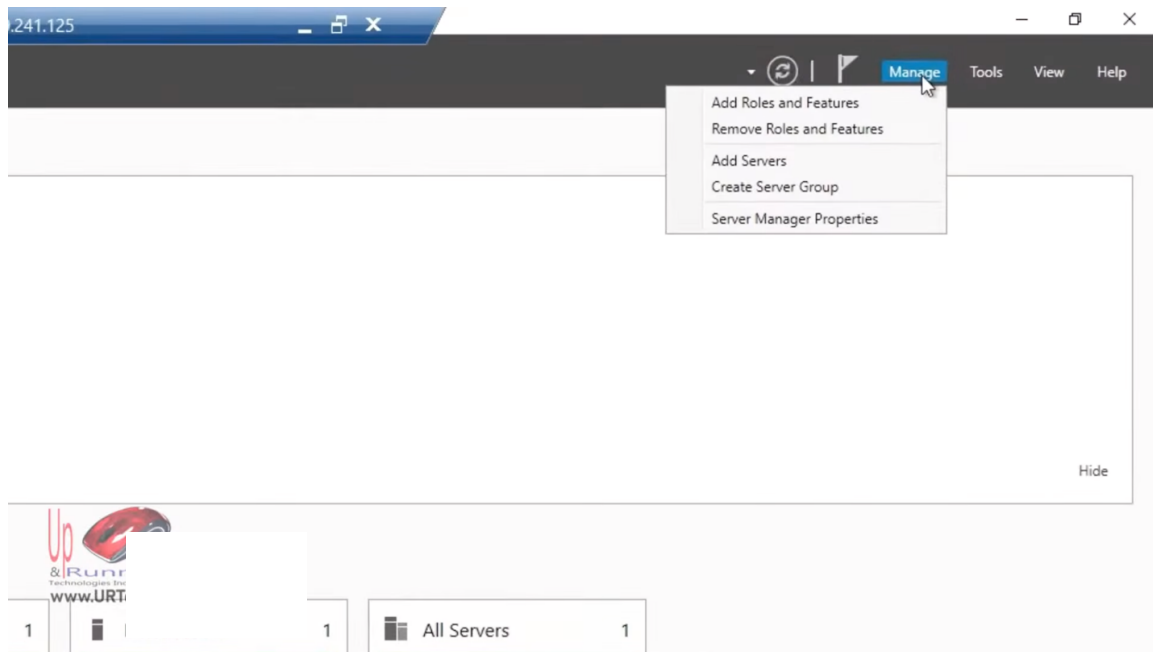
Ex.



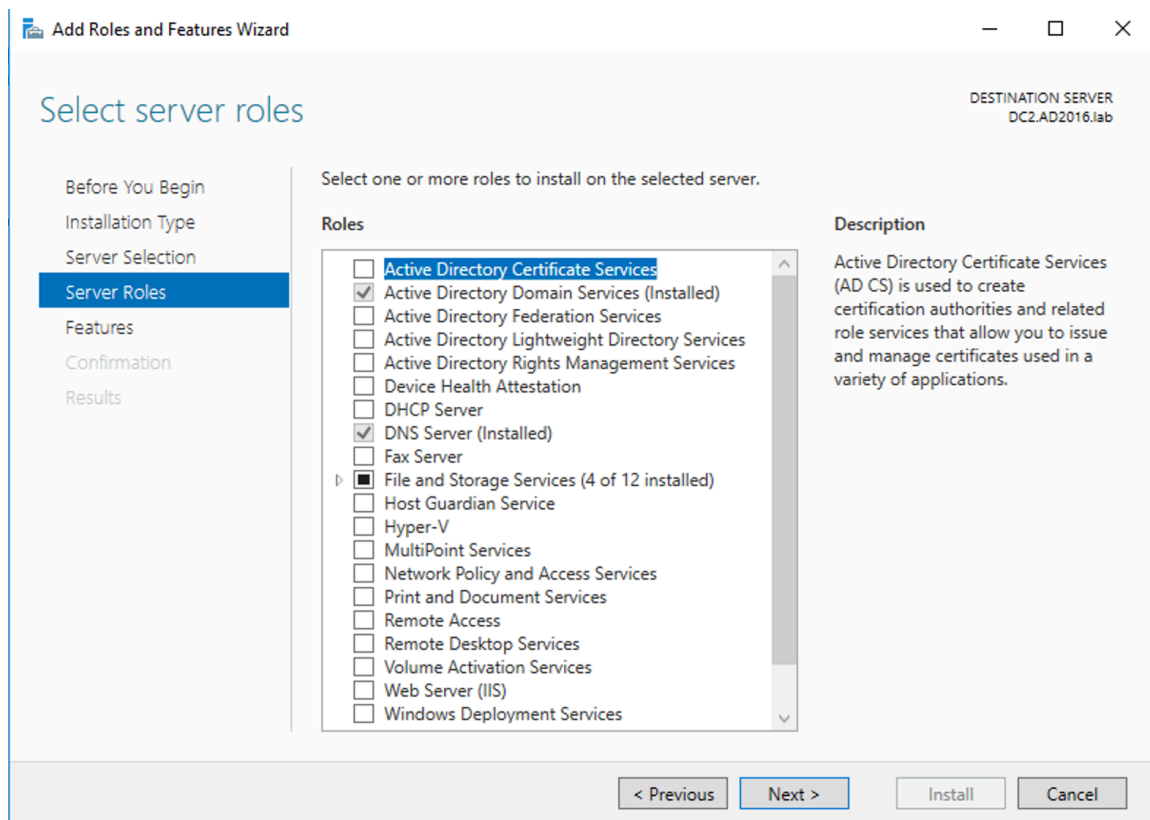
3. CONFIGURE CERTIFICATE CA SERVICES ON THE DOMAIN CONTROLLER:

Skip to step 4 if you already have a Certificate CA on you Domain Controller.

- a. Add Roles and Features:



b. Select Active Directory Certificate Services:



c. Hit *Add Features* when prompted.

d. Follow the Wizard steps and hit *Install* to install the services on the Domain Controller.

- e. Under Roles and Features, select AD CS Configuration and use Wizard to configure CA:

The screenshot shows the 'AD CS Configuration' wizard window. The title bar reads 'AD CS Configuration'. The main window has a left-hand navigation pane with the following items: 'Credentials' (highlighted in blue), 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main content area is titled 'Credentials' and contains the following text: 'Specify credentials to configure role services'. Below this, there are two sections of role services that require specific group membership: 'To install the following role services you must belong to the local Administrators group:' followed by a list: 'Standalone certification authority', 'Certification Authority Web Enrollment', and 'Online Responder'; and 'To install the following role services you must belong to the Enterprise Admins group:' followed by a list: 'Enterprise certification authority', 'Certificate Enrollment Policy Web Service', 'Certificate Enrollment Web Service', and 'Network Device Enrollment Service'. At the bottom of the main content area, there is a 'Credentials:' label, a text box containing 'AD2016\administrator', and a 'Change...' button. Below the text box is a link that says 'More about AD CS Server Roles'. The bottom of the window features a navigation bar with four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

Credentials

DESTINATION SERVER
DC2.AD2016.lab

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: AD2016\administrator Change...

[More about AD CS Server Roles](#)

< Previous Next > Configure Cancel

f. Select *Certification Authority* Role services and hit Next:

The screenshot shows the 'AD CS Configuration' window with the 'Role Services' tab selected. The left-hand navigation pane lists the following steps: Credentials, Role Services (highlighted), Setup Type, CA Type, Private Key, Cryptography, CA Name, Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Select Role Services to configure' and lists five services with checkboxes: 'Certification Authority' (checked), 'Certification Authority Web Enrollment' (unchecked), 'Online Responder' (unchecked), 'Network Device Enrollment Service' (unchecked), and 'Certificate Enrollment Web Service' (unchecked). Below this list is a link for 'More about AD CS Server Roles'. The top right corner indicates the 'DESTINATION SERVER' as 'DC2.AD2016.lab'. At the bottom, there are four buttons: '< Previous', 'Next >' (highlighted), 'Configure', and 'Cancel'.

g. Select *Enterprise CA* and hit Next:

The screenshot shows the 'AD CS Configuration' window with the 'Setup Type' tab selected. The left sidebar lists the steps: Credentials, Role Services, Setup Type (highlighted), CA Type, Private Key, Cryptography, CA Name, Certificate Request, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the setup type of the CA'. It explains that Enterprise CAs use Active Directory Domain Services (AD DS) to simplify certificate management, while Standalone CAs do not. Two radio buttons are present: 'Enterprise CA' (selected) and 'Standalone CA'. Below the 'Enterprise CA' option, it states that Enterprise CAs must be domain members and are typically online to issue certificates or manage policies. Below the 'Standalone CA' option, it states that Standalone CAs can be members of a workgroup or domain, do not require AD DS, and can be used offline. A link 'More about Setup Type' is at the bottom of the main area. The top right corner shows 'DESTINATION SERVER' as 'DC2.AD2016.lab'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
DC2.AD2016.lab

Setup Type

- Credentials
- Role Services
- Setup Type**
- CA Type
- Private Key
 - Cryptography
 - CA Name
 - Certificate Request
- Certificate Database
- Confirmation
- Progress
- Results

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

☒ Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

☐ Standalone CA
Standalone CAs can be members of a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

[More about Setup Type](#)

< Previous Next > Configure Cancel

h. Select *Root CA* and hit next:

The screenshot shows the 'AD CS Configuration' window with the 'CA Type' step selected in the left-hand navigation pane. The main area is titled 'Specify the type of the CA' and contains explanatory text about PKI hierarchies. Two radio buttons are present: 'Root CA' (selected) and 'Subordinate CA'. The 'Root CA' option is accompanied by the text: 'Root CAs are the first and may be the only CAs configured in a PKI hierarchy.' The 'Subordinate CA' option is accompanied by the text: 'Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.' At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'Next >' button is highlighted with a blue border. The window title bar shows standard minimize, maximize, and close buttons. The top right corner of the window displays 'DESTINATION SERVER' and 'DC2.AD2016.lab'.

AD CS Configuration

DESTINATION SERVER
DC2.AD2016.lab

CA Type

- Credentials
- Role Services
- Setup Type
- CA Type**
- Private Key
 - Cryptography
 - CA Name
 - Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

☒ Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

☐ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

[More about CA Type](#)

< Previous Next > Configure Cancel

- i. Select *Create a new Private Key* and hit next:

The screenshot shows the 'AD CS Configuration' window with the 'Private Key' step selected in the left-hand navigation pane. The main area is titled 'Specify the type of the private key'. It contains a paragraph explaining that a CA must have a private key to generate and issue certificates. Below this, there are three radio button options: 'Create a new private key' (which is selected), 'Use existing private key', and 'Select a certificate and use its associated private key'. Each option has a brief description. At the bottom of the main area is a link 'More about Private Key'. The bottom of the window features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
DC2.AD2016.lab

Private Key

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key**
- Cryptography
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

- ☒ **Create a new private key**
Use this option if you do not have a private key or want to create a new private key.
- ☐ **Use existing private key**
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.
 - ☐ **Select a certificate and use its associated private key**
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.
 - ☐ **Select an existing private key on this computer**
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous Next > Configure Cancel

j. Select *SHA256* Algorithm and hit next:

AD CS Configuration

DESTINATION SERVER
DC2.AD2016.lab

Cryptography for CA

- Credentials
- Role Services
- Setup Type
- CA Type
- Private Key
- Cryptography**
- CA Name
- Validity Period
- Certificate Database
- Confirmation
- Progress
- Results

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about Cryptography](#)

< Previous Next > Configure Cancel

k. Type the name of your CA and hit next:

The screenshot shows the 'AD CS Configuration' window with the 'CA Name' step selected in the left-hand navigation pane. The main area is titled 'Specify the name of the CA' and includes a descriptive paragraph: 'Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' Below this, there are three input fields: 'Common name for this CA:' with the value 'AD2016-DC2-CA', 'Distinguished name suffix:' with the value 'DC=AD2016,DC=lab', and 'Preview of distinguished name:' with the value 'CN=AD2016-DC2-CA,DC=AD2016,DC=lab'. A link 'More about CA Name' is located below the preview field. In the top right corner, the 'DESTINATION SERVER' is listed as 'DC2.AD2016.lab'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
DC2.AD2016.lab

CA Name

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
AD2016-DC2-CA

Distinguished name suffix:
DC=AD2016,DC=lab

Preview of distinguished name:
CN=AD2016-DC2-CA,DC=AD2016,DC=lab

[More about CA Name](#)

< Previous Next > Configure Cancel

1. Select the validity period of the CA and hit next:

The screenshot shows the 'AD CS Configuration' window with the 'Validity Period' step selected in the left-hand navigation pane. The main area is titled 'Specify the validity period' and contains the following text: 'Select the validity period for the certificate generated for this certification authority (CA):'. Below this, there is a text box containing the number '5' and a dropdown menu set to 'Years'. The text 'CA expiration Date: 5/27/2031 2:13:00 PM' is displayed below the input. A warning message states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' A link 'More about Validity Period' is located at the bottom of the main area. The bottom of the window features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

DESTINATION SERVER
DC2.AD2016.lab

Validity Period

Credentials
Role Services
Setup Type
CA Type
Private Key
 Cryptography
 CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 5/27/2031 2:13:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous Next > Configure Cancel

m. Specify the database locations (use default) and hit next:

The screenshot shows the 'AD CS Configuration' wizard window. The title bar reads 'AD CS Configuration'. The main window has a left-hand navigation pane with the following items: 'Credentials', 'Role Services', 'Setup Type', 'CA Type', 'Private Key' (with sub-items 'Cryptography', 'CA Name', and 'Validity Period'), 'Certificate Database' (which is highlighted with a blue background), 'Confirmation', 'Progress', and 'Results'. The main area is titled 'CA Database' and contains the heading 'Specify the database locations'. Below this heading are two text input fields. The first field is labeled 'Certificate database location:' and contains the text 'C:\Windows\system32\CertLog'. The second field is labeled 'Certificate database log location:' and also contains the text 'C:\Windows\system32\CertLog'. In the top right corner of the main area, it says 'DESTINATION SERVER' followed by 'DC2.AD2016.lab'. At the bottom of the main area, there is a link that says 'More about CA Database'. At the very bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

AD CS Configuration

CA Database

DESTINATION SERVER
DC2.AD2016.lab

Specify the database locations

Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

More about CA Database

< Previous Next > Configure Cancel

- n. Validate configurations and hit *Configure*:

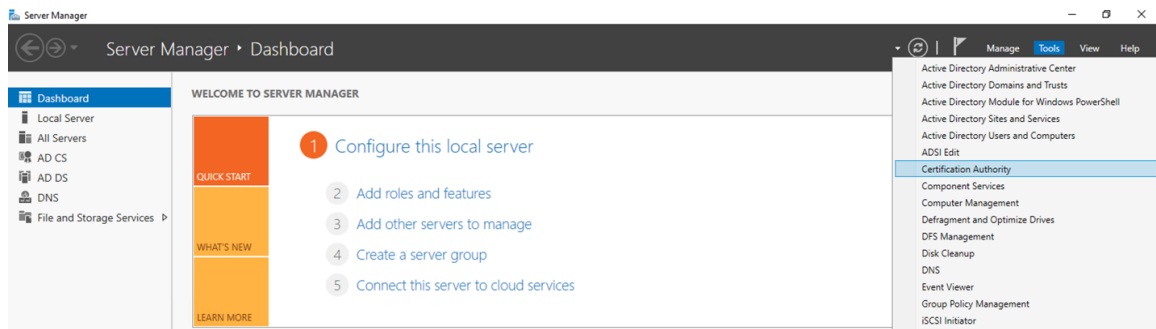
The screenshot shows the 'AD CS Configuration' window in Windows Server. The title bar reads 'AD CS Configuration'. The window is divided into a left sidebar and a main content area. The sidebar contains a list of steps: 'Credentials', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation' (highlighted in blue), 'Progress', and 'Results'. The main content area has a header 'Confirmation' and a sub-header 'DESTINATION SERVER DC2.AD2016.lab'. Below this, it says 'To configure the following roles, role services, or features, click Configure.' and a button with an upward arrow and the text 'Active Directory Certificate Services'. Underneath, a section titled 'Certification Authority' lists the following configuration details: CA Type: Enterprise Root; Cryptographic provider: RSA#Microsoft Software Key Storage Provider; Hash Algorithm: SHA256; Key Length: 2048; Allow Administrator Interaction: Disabled; Certificate Validity Period: 5/27/2031 2:13:00 PM; Distinguished Name: CN=AD2016-DC2-CA,DC=AD2016,DC=lab; Certificate Database Location: C:\Windows\system32\CertLog; Certificate Database Log Location: C:\Windows\system32\CertLog. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure' (highlighted in blue), and 'Cancel'.

Certification Authority	
CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	5/27/2031 2:13:00 PM
Distinguished Name:	CN=AD2016-DC2-CA,DC=AD2016,DC=lab
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

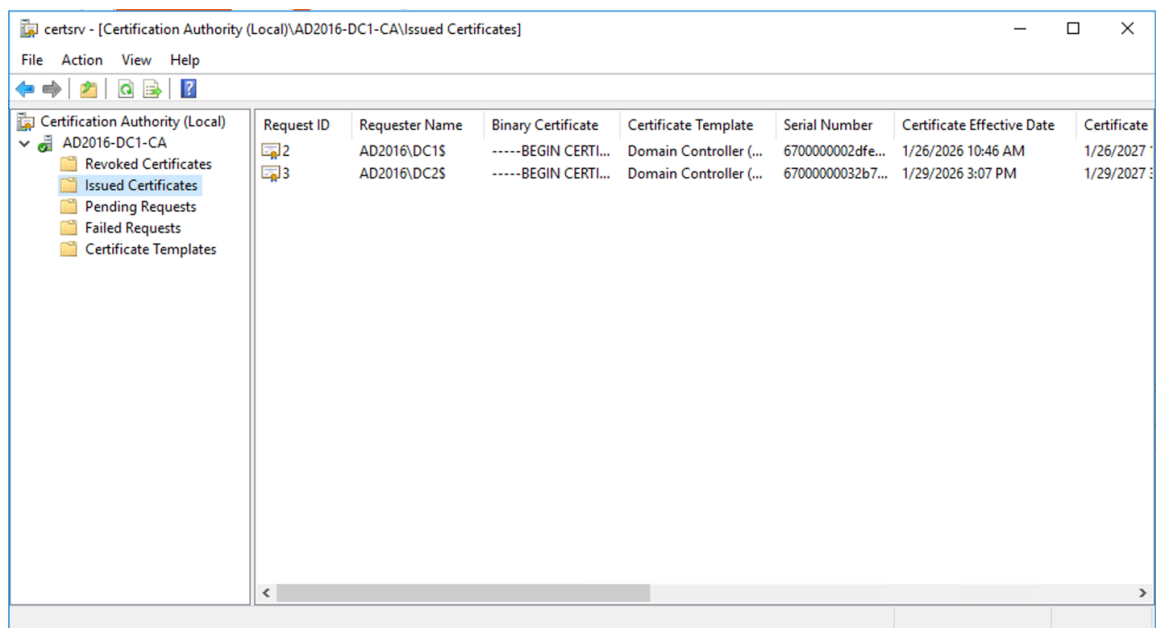
- o. **Reboot the Windows Server to generate a certificate.**

4. VALIDATE CERTIFICATE AND LDAP CONNECTION:

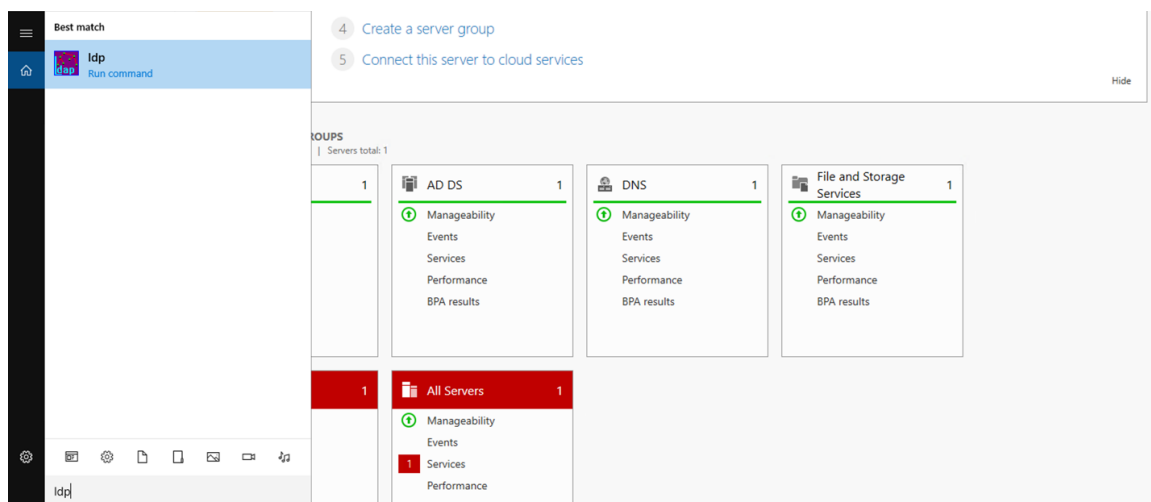
- a. Open the *Certification Authority* manager:



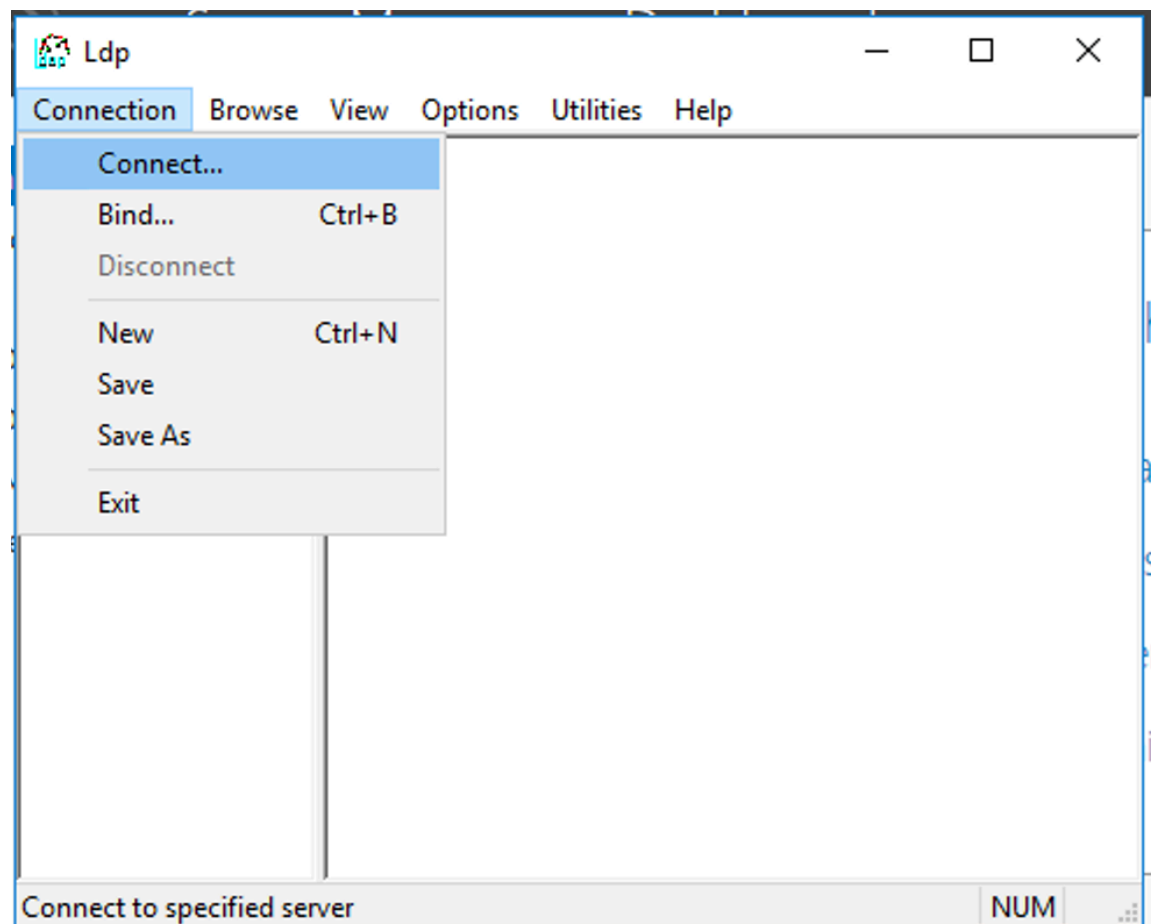
- b. Open the *Issued Certificates* folder. There should be one issued certificate to the Domain Controller:



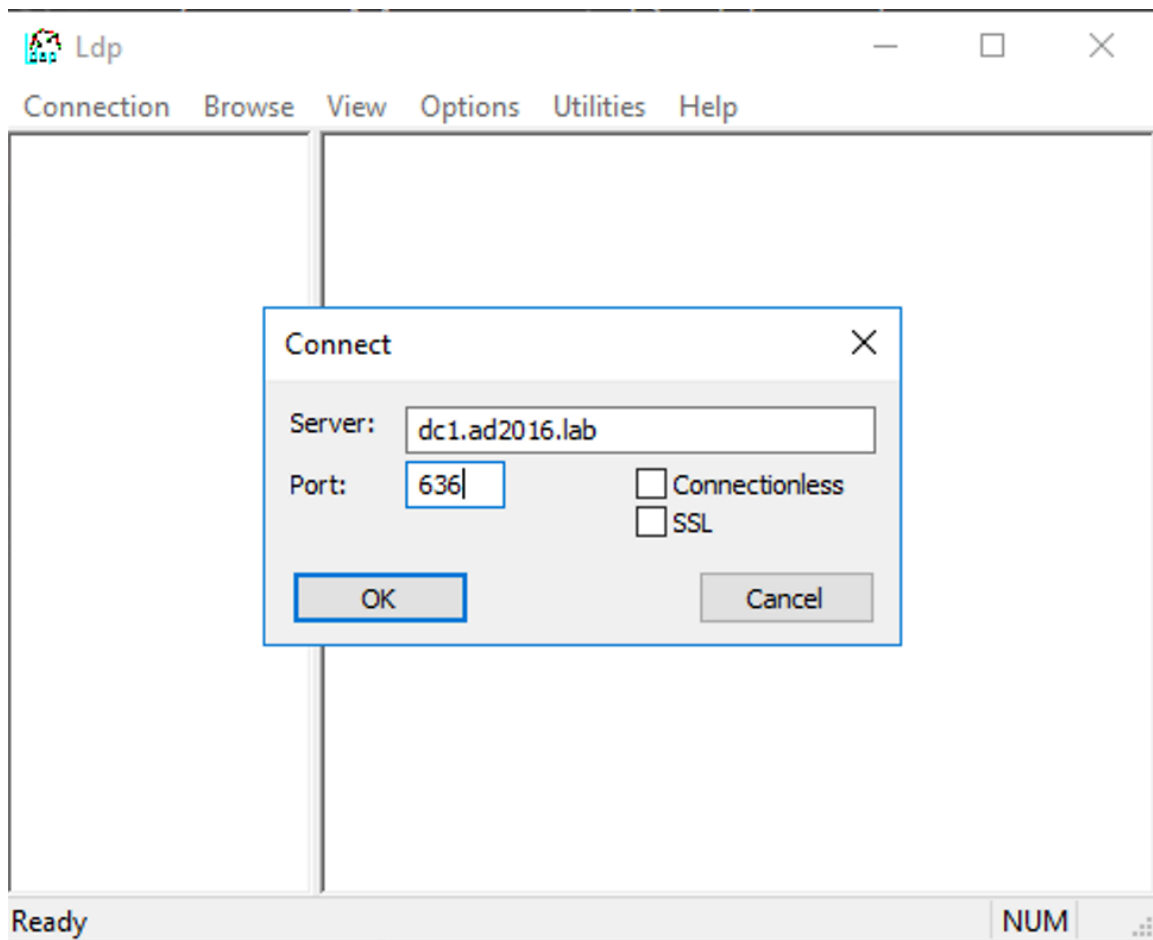
c. Open *ldp* console to test the LDAP connection:



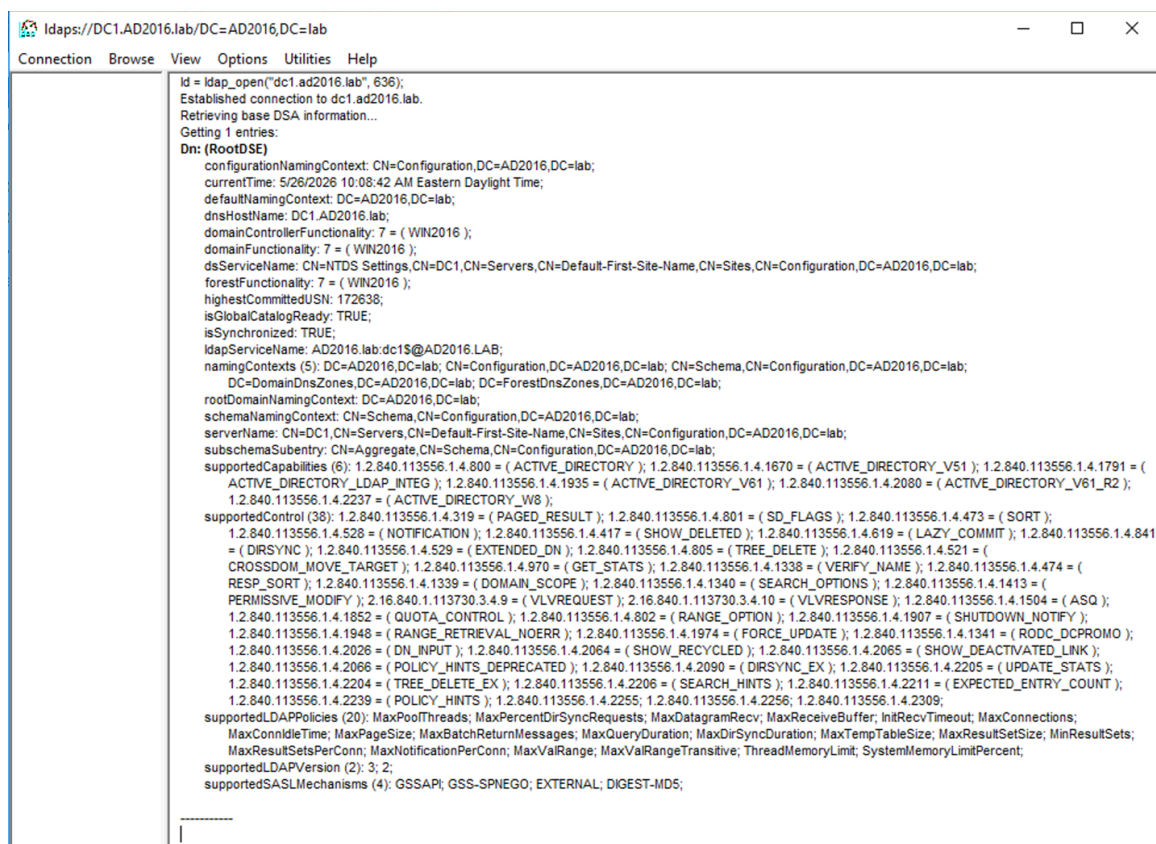
d. Hit *Connection* and *connect*:



e. Type the server FQDN and type port 636 and hit OK:



f. Confirm the connection is established:



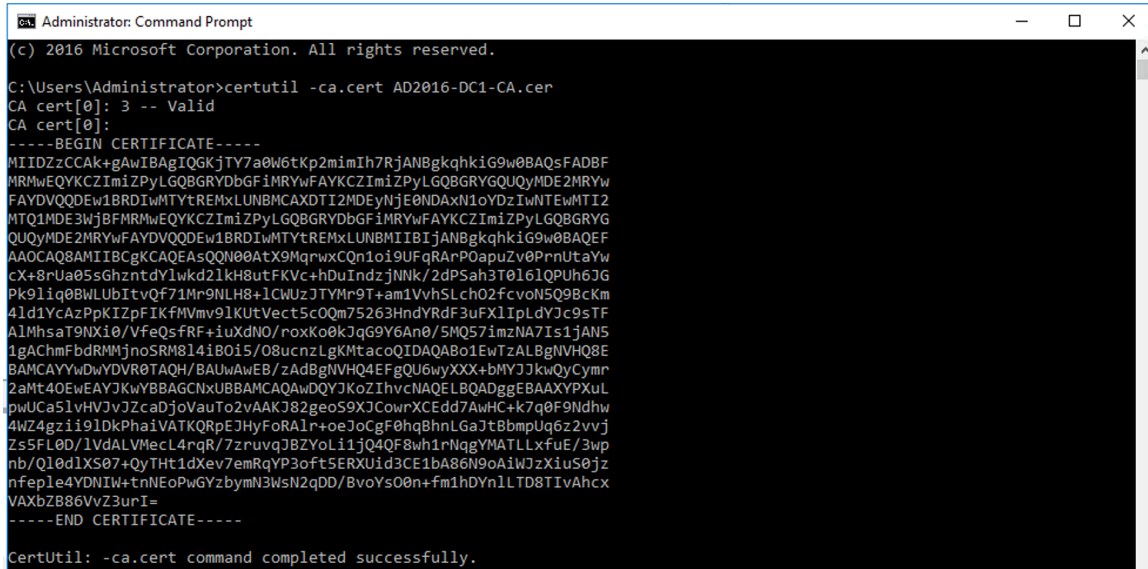
The screenshot shows a window titled "Idaps://DC1.AD2016.lab/DC=AD2016,DC=lab". The window has a menu bar with "Connection", "Browse", "View", "Options", "Utilities", and "Help". The main content area displays the following text:

```
Id = ldap_open("dc1.ad2016.lab", 636);
Established connection to dc1.ad2016.lab.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
configurationNamingContext: CN=Configuration,DC=AD2016,DC=lab;
currentTime: 5/26/2026 10:08:42 AM Eastern Daylight Time;
defaultNamingContext: DC=AD2016,DC=lab;
dnsHostName: DC1.AD2016.lab;
domainControllerFunctionality: 7 = ( WIN2016 );
domainFunctionality: 7 = ( WIN2016 );
dsServiceName: CN=NTDS Settings,CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=AD2016,DC=lab;
forestFunctionality: 7 = ( WIN2016 );
highestCommittedUSN: 172638;
isGlobalCatalogReady: TRUE;
isSynchronized: TRUE;
ldapServiceName: AD2016.lab:dc1$@AD2016.LAB;
namingContexts (5): DC=AD2016,DC=lab; CN=Configuration,DC=AD2016,DC=lab; CN=Schema,CN=Configuration,DC=AD2016,DC=lab;
DC=DomainDnsZones,DC=AD2016,DC=lab; DC=ForestDnsZones,DC=AD2016,DC=lab;
rootDomainNamingContext: DC=AD2016,DC=lab;
schemaNamingContext: CN=Schema,CN=Configuration,DC=AD2016,DC=lab;
serverName: CN=DC1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=AD2016,DC=lab;
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=AD2016,DC=lab;
supportedCapabilities (6): 1.2.840.113556.1.4.800 = ( ACTIVE_DIRECTORY ); 1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 ); 1.2.840.113556.1.4.1791 = (
ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIRECTORY_V61 ); 1.2.840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 );
1.2.840.113556.1.4.2237 = ( ACTIVE_DIRECTORY_W8 );
supportedControl (38): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556.1.4.801 = ( SD_FLAGS ); 1.2.840.113556.1.4.473 = ( SORT );
1.2.840.113556.1.4.528 = ( NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1.4.619 = ( LAZY_COMMIT ); 1.2.840.113556.1.4.841
= ( DIRSYNC ); 1.2.840.113556.1.4.529 = ( EXTENDED_DN ); 1.2.840.113556.1.4.805 = ( TREE_DELETE ); 1.2.840.113556.1.4.521 = (
CROSSDOM_MOVE_TARGET ); 1.2.840.113556.1.4.970 = ( GET_STATS ); 1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = (
RESP_SORT ); 1.2.840.113556.1.4.1339 = ( DOMAIN_SCOPE ); 1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = (
PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = ( VLVREQUEST ); 2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ );
1.2.840.113556.1.4.1852 = ( QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = ( RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY );
1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = ( RODC_DCPROMO );
1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED ); 1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK );
1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX ); 1.2.840.113556.1.4.2205 = ( UPDATE_STATS );
1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = ( EXPECTED_ENTRY_COUNT );
1.2.840.113556.1.4.2239 = ( POLICY_HINTS ); 1.2.840.113556.1.4.2255; 1.2.840.113556.1.4.2256; 1.2.840.113556.1.4.2309;
supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRecv; MaxReceiveBuffer; IntRecvTimeout; MaxConnections;
MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets;
MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent;
supportedLDAPVersion (2): 3; 2;
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;
```



5. GET THE CERTIFICATE USING CMD (COMMAND PROMPT) – METHOD 1:

- a. Open CMD and enter the `certutil -ca.cert [certificate name].cer`



```
Administrator: Command Prompt
(c) 2016 Microsoft Corporation. All rights reserved.

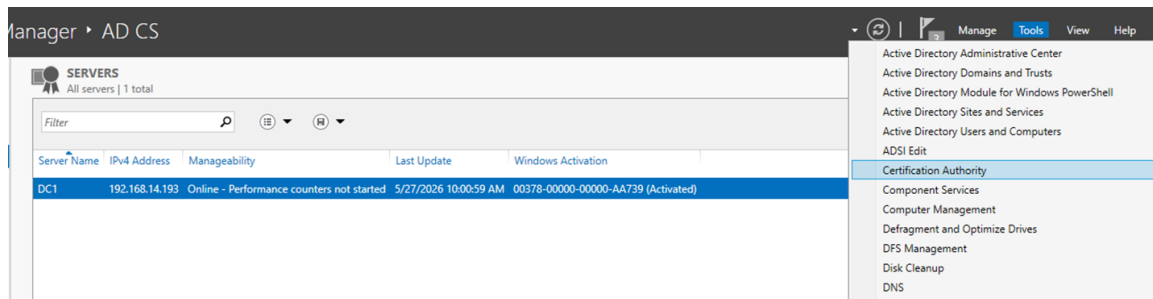
C:\Users\Administrator>certutil -ca.cert AD2016-DC1-CA.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDZzCCAk+gAwIBAgIQGKjTY7a0W6tKp2mimIh7RjANBgkqhkiG9w0BAQsFADBF
MRMwEQYKCZImiZPyLQBGRYDbGFIMRYwFAYKCIImiZPyLQBGRYQQUYmDE2MRyw
FAYDVQDEw1BRDIwMTYtREMxLUNBMCAxDTI2MDEyNjE0NDExNjE0YDZlWNTwMTI2
MTQ1MDE3WjBFMRMwEQYKCZImiZPyLQBGRYDbGFIMRYwFAYKCIImiZPyLQBGRYQ
QUYmDE2MRywFAYDVQDEw1BRDIwMTYtREMxLUNBMCAxDTI2MDEyNjE0NDExNjE0
AAOCAQ8AMIIBCgKCAQEASQQN00AtX9MqrwxQn1oi9UFqRarPOapuZv0PrnUtaYw
cX+8rUa0S5GhzntdYlwkD2lKH8utFKVc+hDuIndzjNNk/2dPSah3T0161QPUh6JG
Pk91iq0BWLUBItvQF71Mr9NLH8+1CWUzJTYMr9T+am1VvhSLch02fcvoN5Q9BCKm
4ld1YcAzPpKIzPFIKfMVmv9lKUtVect5cOQm75263HndYRdF3uFXlIpLdYJc9sTF
AlMhsaT9NXi0/VFeQsFRF+iuXdNO/roXKo0k3qG9Y6An0/5MQ57imzNA7Is1jAN5
1gAChmFbdRMMjnoSRM814iBOi5/08ucnzLgKtacoQIDAQABo1EwTzALBGNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU6wyXXX+bMYJJkwQyCymr
2aMt40EwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQELBQADggEBAAXYPxUL
pwUCa5lvHVjvJZcaDjoVauTo2vAAKJ82geoS9XJCowrXCedd7AwHC+k7q0F9Ndhw
4WZ4gzi91DkPhaiVATKORpEJHyFoRA1r+oeJoCgF0hqBhnLGAJtBbmqUq6z2vvj
Zs5FL0D/lVdALVMecL4nqR/7zruvqJBZYolijQ0F8wh1rNagYMATLLxfuE/3wp
nb/Q10dlXS07+QyTHT1dXev7emRqYP3oft5ERXUId3CE1bA86N9oAiWJzXius0jz
nfep1e4YDNIW+tnNEoPwGYzbymN3WsN2qDD/BvoYs00n+fmlhDYn1LT08TivAhcx
VAXbZB86VvZ3urI=
-----END CERTIFICATE-----

CertUtil: -ca.cert command completed successfully.
```

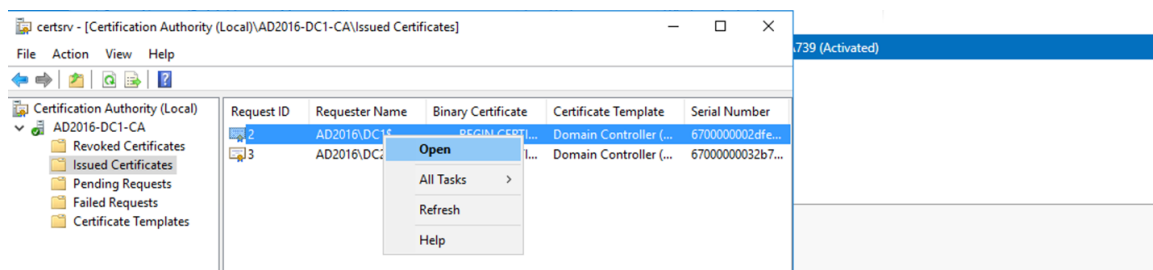
- b. Copy and save the certificate plain text for later for the NASlord LDAP authentication services configuration.

6. GET THE CERTIFICATE USING AD CS AND CERTIFICATE EXPORT – METHOD 2:

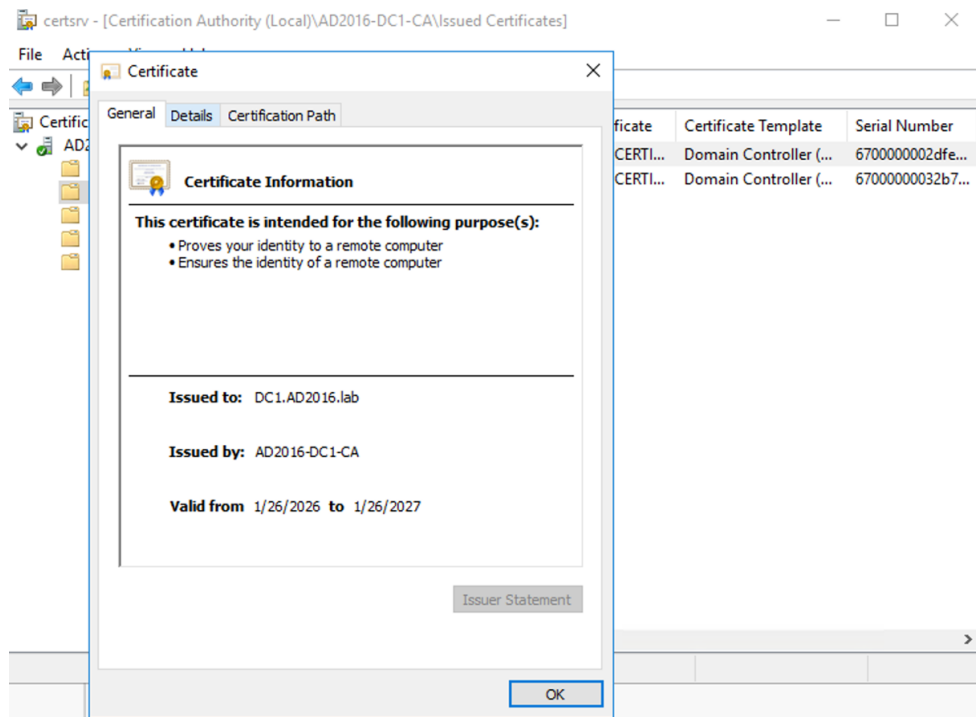
- a. Go to *Certification Authority*:



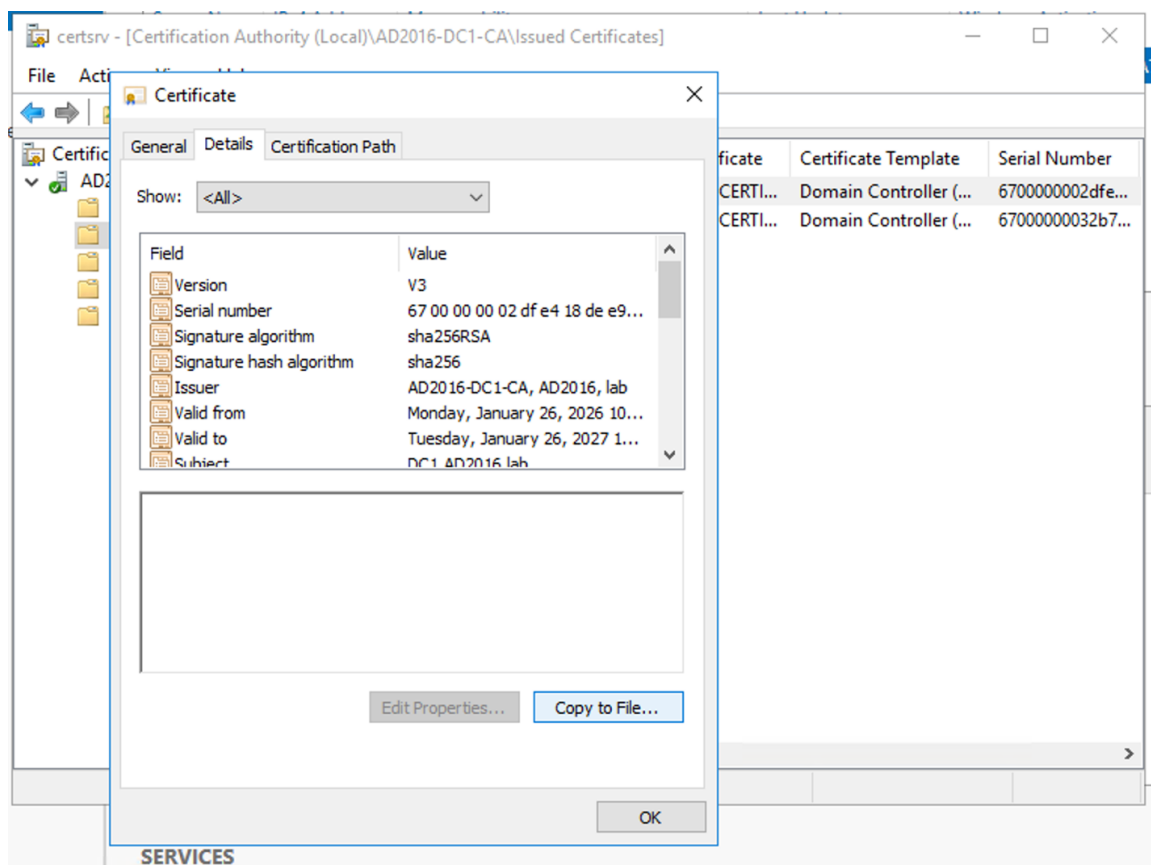
- b. Pull down the CA instance, hit *Issued Certificates*, right-click on the first issued Certificate and hit Open:



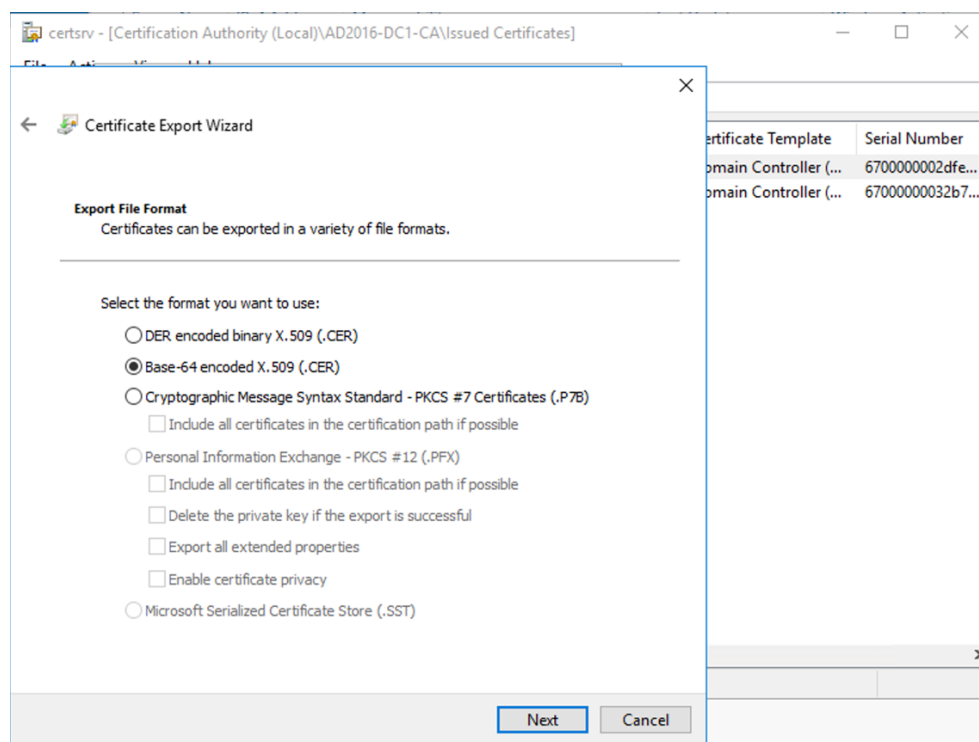
a. Hit *details*:



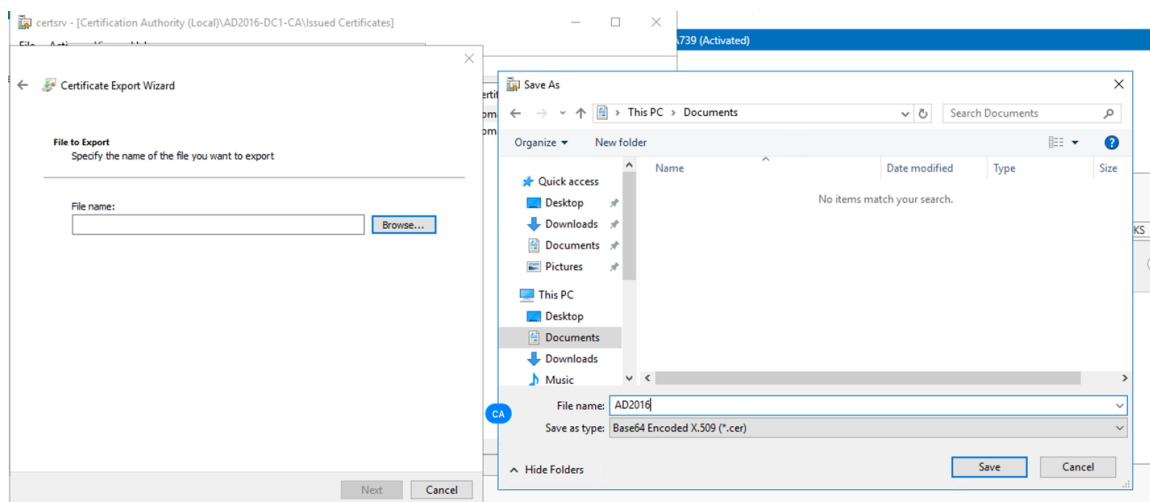
c. Hit *Copy to File...*:



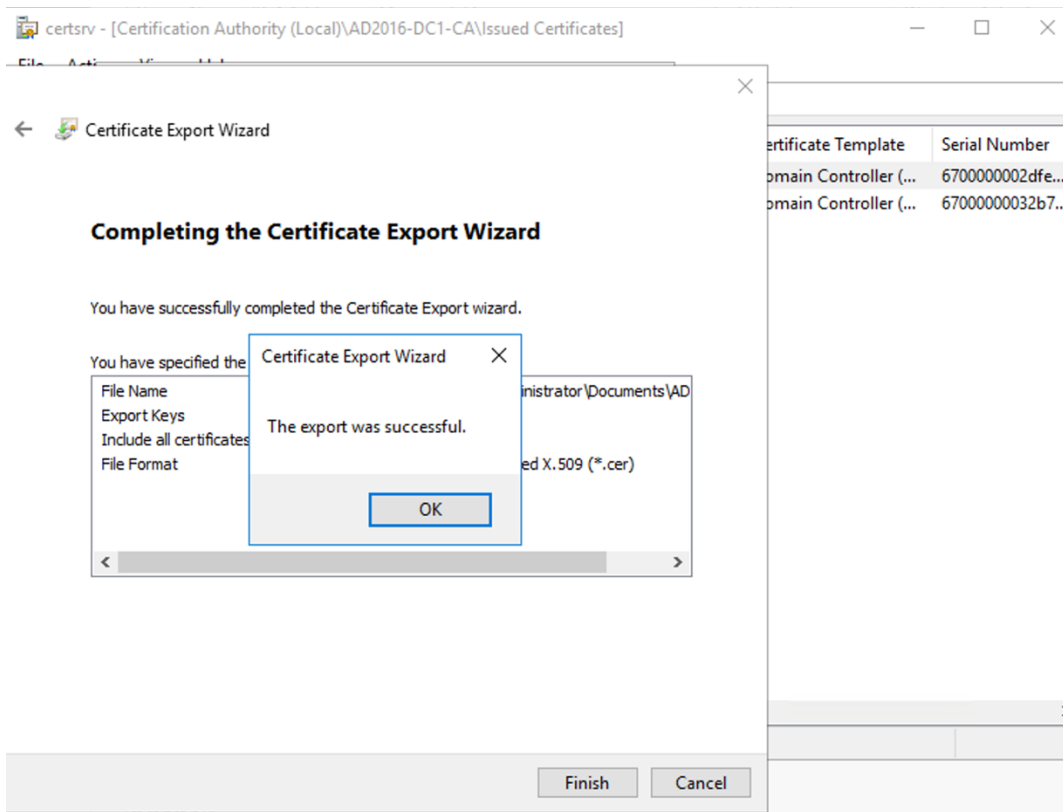
d. Choose *Base-64 encoded X.509* certificate:



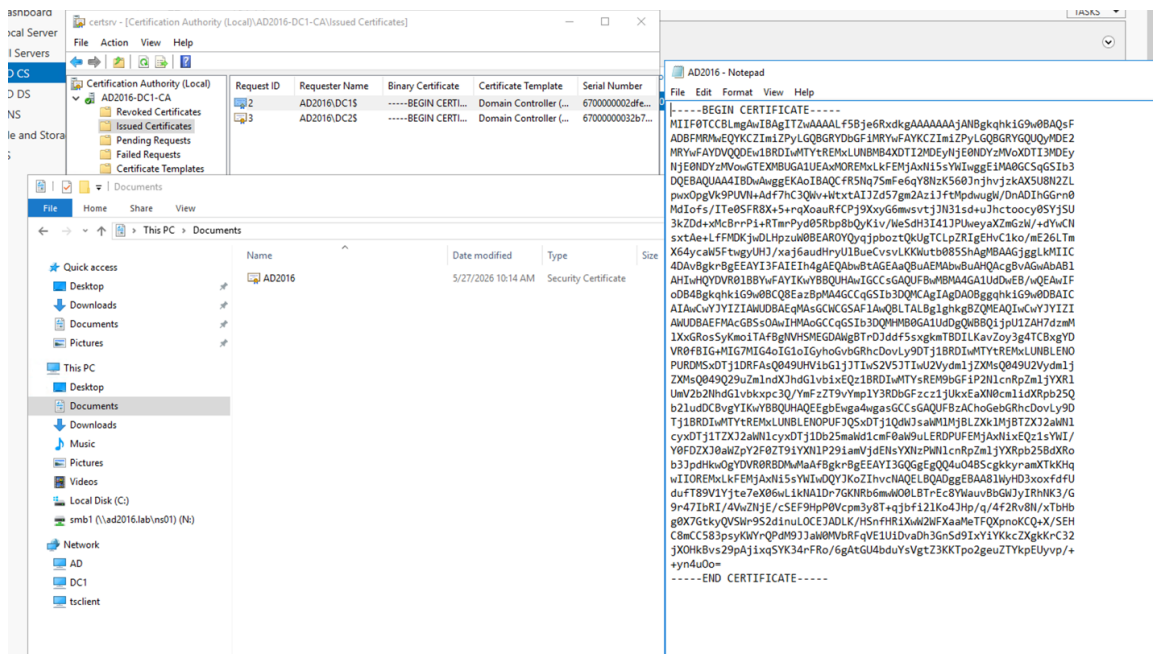
e. Hit *Browse*, name and save the certificate:



f. Hit *next* until the end of the Wizard and hit *Finish*:



- g. Go to the certificate location, right click on the previously saved certificate and choose *open with* > *Notepad*:



- h. Copy and save the certificate plain text for later for the NASlord LDAP authentication services configuration.

7. NASLORD LDAP CONFIGURATION:

- a. Go to *Admin Page*:

NASLORD [LICENSE: DEMO] English

LOGGED IN AS ADMIN (ADMIN) | ADMIN PAGE | CHANGE PASSWORD | LOGOUT | ABOUT

Welcome to NASLORD

Please select the type of Storage System that you would like to manage:

PowerScale Clusters

Tenant Manager

PowerProtect DD Appliances

Retention Lock Manager

ObjectScale Virtual Data Centers

Chargeback Manager

/NASLORD/showAdmin/ © 2021-2026 Gallium inc. | All rights reserved.

- b. Hit *LDAP Provider Management*:

NASLORD [LICENSE: DEMO] English

LOGGED IN AS ADMIN (ADMIN) | ADMIN PAGE | CHANGE PASSWORD | LOGOUT | ABOUT

Administrative Operations

← BACK

General Configuration

SYSTEM SETTINGS

LICENSE MANAGEMENT

LOCAL USER MANAGEMENT

TENANT MANAGEMENT

REPORT DELIVERY

LDAP PROVIDER MANAGEMENT

DATABASE MANAGEMENT

UPGRADE NASLORD

REBOOT THE NASLORD VM

SHUTDOWN THE NASLORD VM

LDAP Provider Management

- c. Hit *Edit*:

LDAP Provider Management

← BACK

LDAP Authentication **DISABLED**

No LDAP server URI is configured.

⚙ EDIT

- d. Enter the LDAP information using distinguished name form (Under AD user/group attributes) saved previously:

CONFIGURE LDAP PROVIDER

LDAP Authentication:

On

Connection

Bind DN (DN or user@example.com):

CN=naslord,OU=NASLORD,DC=AD2016,I

Bind Password:

.....

LDAP Server URI (space-separated list):

ldaps://DC1.AD2016.LAB

Require TLS Certificate

ALLOW

User Search

✎ SAVE

🗑 CLEAR

✕ CANCEL

CONFIGURE LDAP PROVIDER

User Search

User Search - Base:

DC=AD2016,DC=lab

User Search - Scope

SUBTREE

Group Search

Group Search - Base:

DC=AD2016,DC=lab

Group Search - Scope

SUBTREE

Group Type

Nested Active Directory Groups

Groups

Denied Users - Group DN:

CN=denied-users,OU=NASLORD,DC=AD2016,DC=lab

 SAVE

 CLEAR

 CANCEL



Gallium Inc.

1250 Rene-Levesque W. Montreal (Quebec) H3B 4W8

- e. Check the *Show advanced options* box. Leave *Start TLS* to *False* and scroll further down:

CONFIGURE LDAP PROVIDER

Denied Users - Group DN:

CN=denied-users,OU=NASLORD,DC=AD2016,DC=lab

Allowed Users - Group DN:

CN=allowed-users,OU=NASLORD,DC=AD2016,DC=lab

Super Users - Group DN:

CN=super-users,OU=NASLORD,DC=AD2016,DC=lab

☒ **Show advanced options**

Connection Options

Start TLS:

False

Network Timeout:

10

Do not enable Start TLS when connecting to your servers via LDAPS

SAVE

CLEAR

CANCEL

- f. Copy the CA Certificate plain text previously saved from the AD:

CONFIGURE LDAP PROVIDER

Start TLS:

False

Network Timeout:

10

Do not enable Start TLS when connecting to your servers via LDAPS

CA Certificate

Paste the CA Certificate here.

User and Group Search

User Search - Filter:

(sAMAccountName=%(user)s)

Group Search - Filter:

(objectClass=group)

SAVE

CLEAR

CANCEL

- g. We recommend to leave these options to default unless you need to customize them. Hit *Save* once the configuration is completed:

CONFIGURE LDAP PROVIDER

User and Group Search

User Search - Filter:
(sAMAccountName=%(user)s)

Group Search - Filter:
(objectClass=group)

Automatic User Attribute Mapping

First Name - Attribute:
givenName

Last Name - Attribute:
sn

Username - Attribute:
sAMAccountName

Email - Attribute:
mail

 **SAVE**

 **CLEAR**

 **CANCEL**

h. Confirm the connection and bind are successful:

 **NASLORD**

[LICENSE: VALID] English ▾

LOGGED IN AS **ADMIN (ADMIN)** | ADMIN PAGE | CHANGE PASSWORD | LOGOUT | ABOUT

LDAP Provider Management

← BACK

LDAP Authentication ENABLED

ldaps://DC1.AD2016.LAB

Connection and bind successful.

CONNECTED

⚙ EDIT