;

Candela TECHNOLOGIES Network Testing and Emulation Solutions

sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

LANforge Server Installation on Windows using a Domain Controller

Goal: Install the LANforge Server software on a Windows machine from a Domain Controller, then configure the Windows machine as a resource in a LANforge cluster.

The LANforge InterOp solution of Candela Technologies is used to support real clients for testing access points. InterOp provides the test engineer with automation for testing mobile devices. In this cookbook we will deploy the LANforge-Server solution from a Domain Controller. This cookbook requires LANforge-Server version 5.5.2 and above.

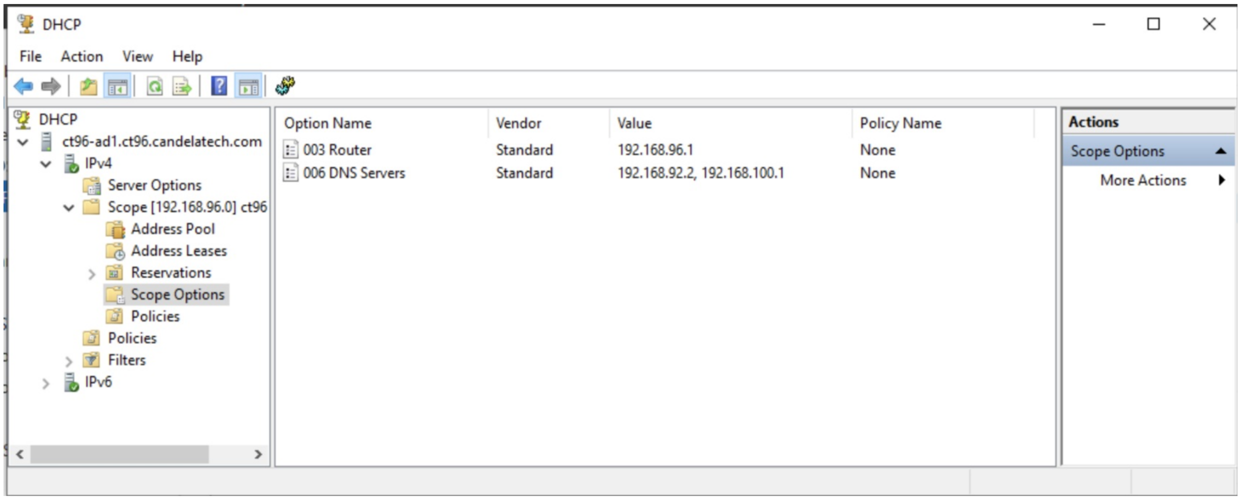
Table of Contents

Before getting started

- Starting with a basic Domain Controller, described in Appendix A.
- This requires LANforge version 5.5.2 or newer.
- LANforge-Server is incompatible with devices running Windows S. If your device is running in S mode, refer to this KB article on switching out of "S" mode.
- To keep terminology brief, some abbreviations:
  - Active Directory Users and Computers (ADUC)
  - Domain Controller (DC)
  - Fully Qualified Domain Name (FQDN)
  - Group Policy Management (GPM)
  - Group Policy Object (GPO)
  - Organizational Unit (OU)
  - Windows Management Instrumentation (WMI)

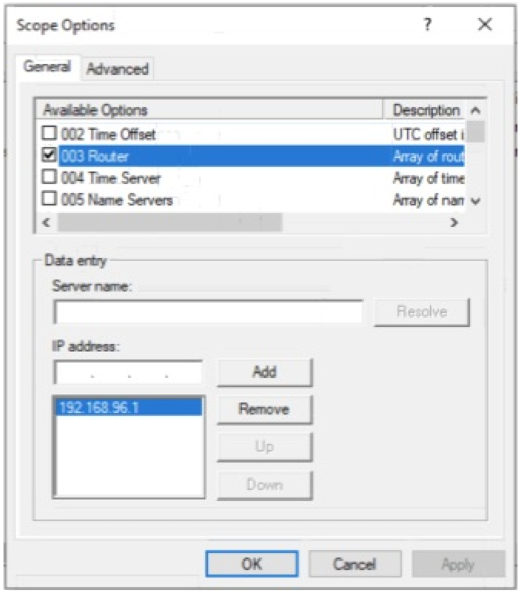
Preconfiguring networking for Domain Controller

1. In the Server Manager screen, go to: Tools → DHCP → expand your domain → IPv4 → Double click Scope → Double click Scope Options.



Option Name	Vendor	Value	Policy Name
003 Router	Standard	192.168.96.1	None
006 DNS Servers	Standard	192.168.92.2, 192.168.100.1	None

2. Right click and select Configure Options. Check 003 Router, and under IP Address, click Add to add the default gateway you want the Windows machines to resolve to. Click Apply and OK.

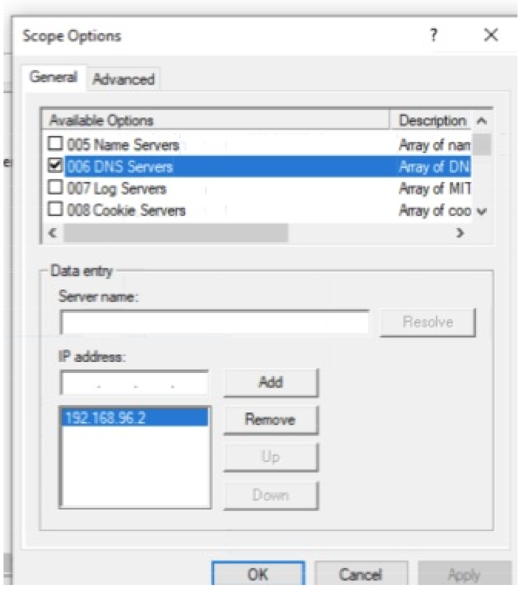


Available Options	Description
□ 002 Time Offset	UTC offset i
☑ 003 Router	Array of rout
□ 004 Time Server	Array of time
□ 005 Name Servers	Array of nan

Server name:

IP address: 192.168.96.1

3. Scroll down from 003 Router, to find 006 DNS Servers. Same as above, click Add to add the DNS servers the Windows machines will need. Click Apply and OK. Close out of this window, and the DHCP window.



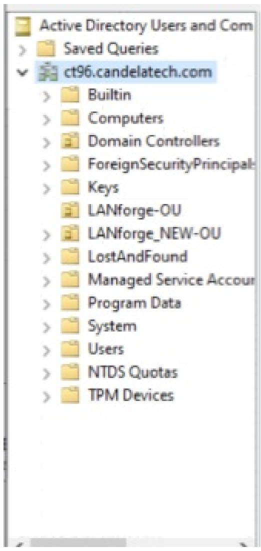
Available Options	Description
□ 005 Name Servers	Array of nan
☑ 006 DNS Servers	Array of DN
□ 007 Log Servers	Array of MIT
□ 008 Cookie Servers	Array of coo

Server name:

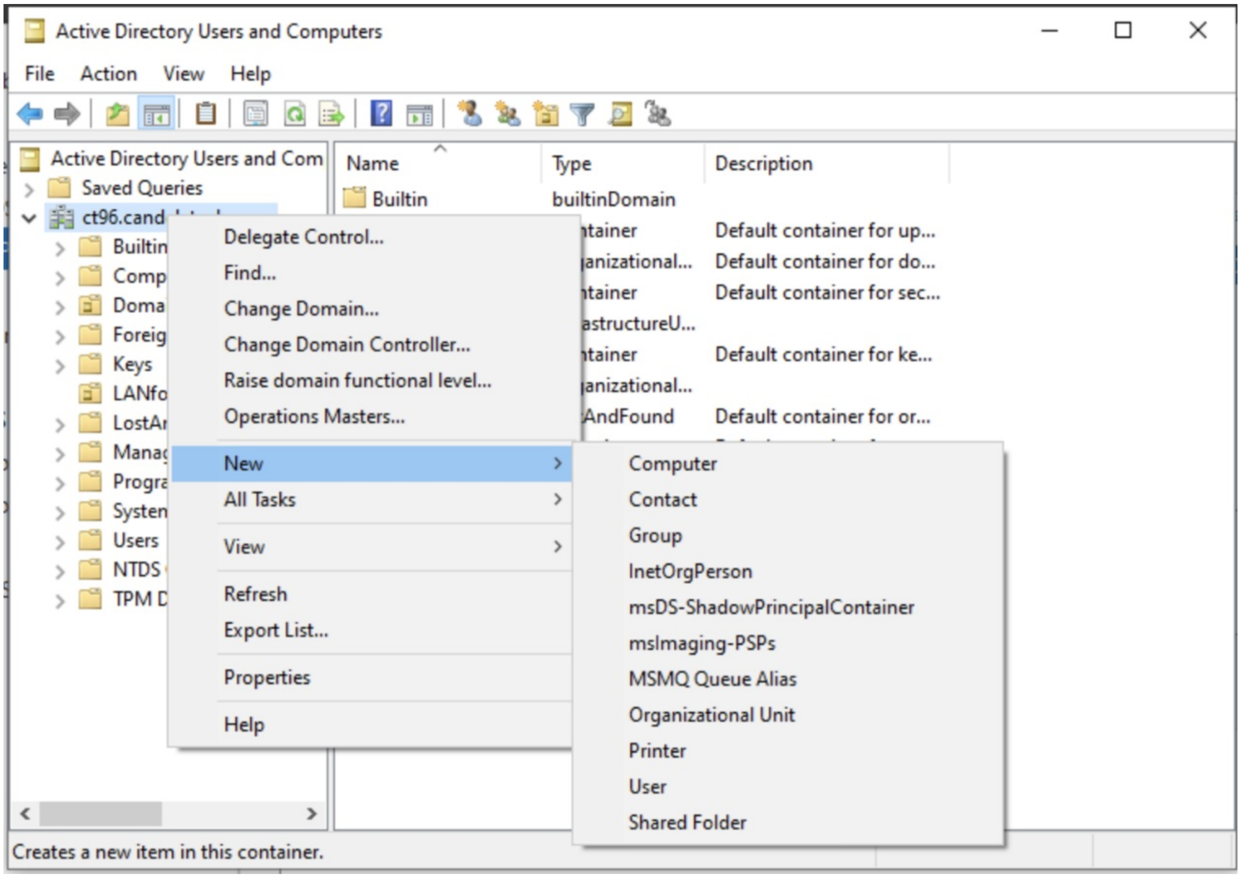
IP address: 192.168.96.2

Creating OU and User details

4. Navigate to the ADUC tool, from the Server Manager screen, Tools → Active Directory Users and Computers (ADUC). On the left hand side, there is an entry for the domain.



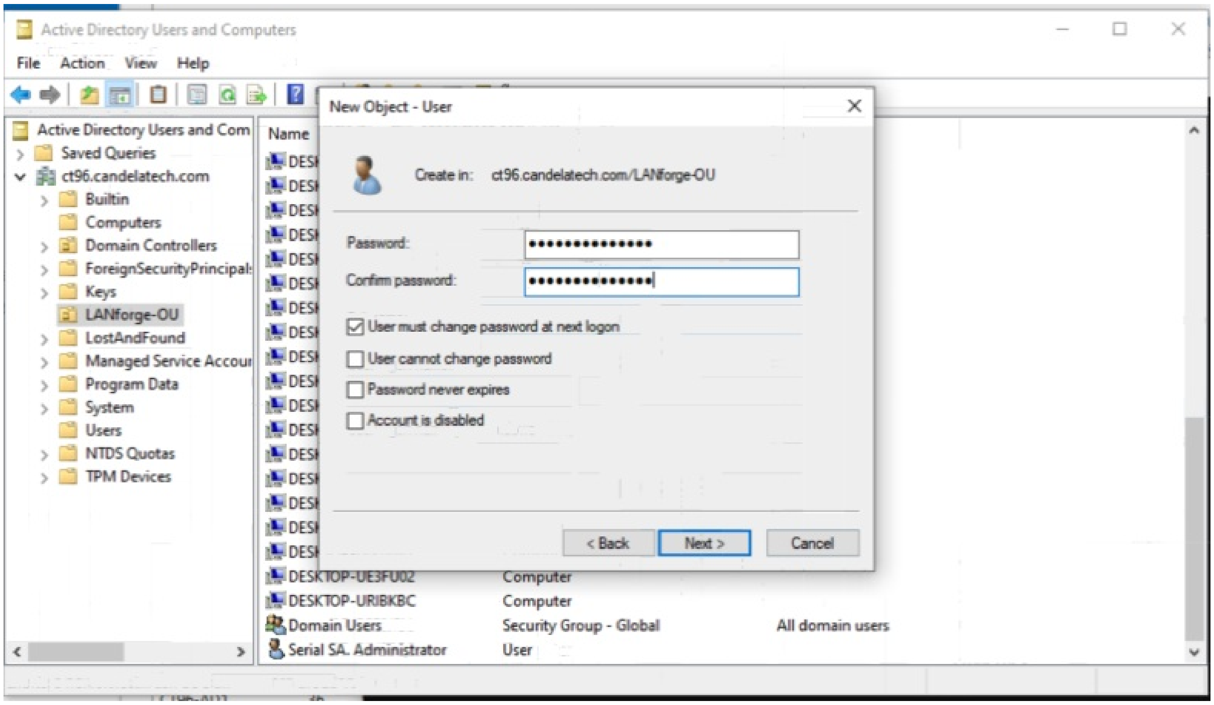
5. Right click on the domain and expand the New option, and click Organizational Unit. Name it, and make sure "Protect from accidental deletion" is checked. Once created you will see the name of the newly created OU in the domain panel on the left hand side.



6. Select the newly created OU, right click → New → User. Fill in the User's First name, Last name and Initials. This User will be used to log into each computer. User logon name should be First name. User logon name (pre-Windows 2000): should be First name. Click Next. Type in the password for the account.

Save this password for later; we will need it.

Uncheck User must change password at next logon. Click Next, then Finish, as shown in the pictures below.



New Object - User

Create in: ct96.candelatech.com/LANforge-OU

Password: ••••••••••••••

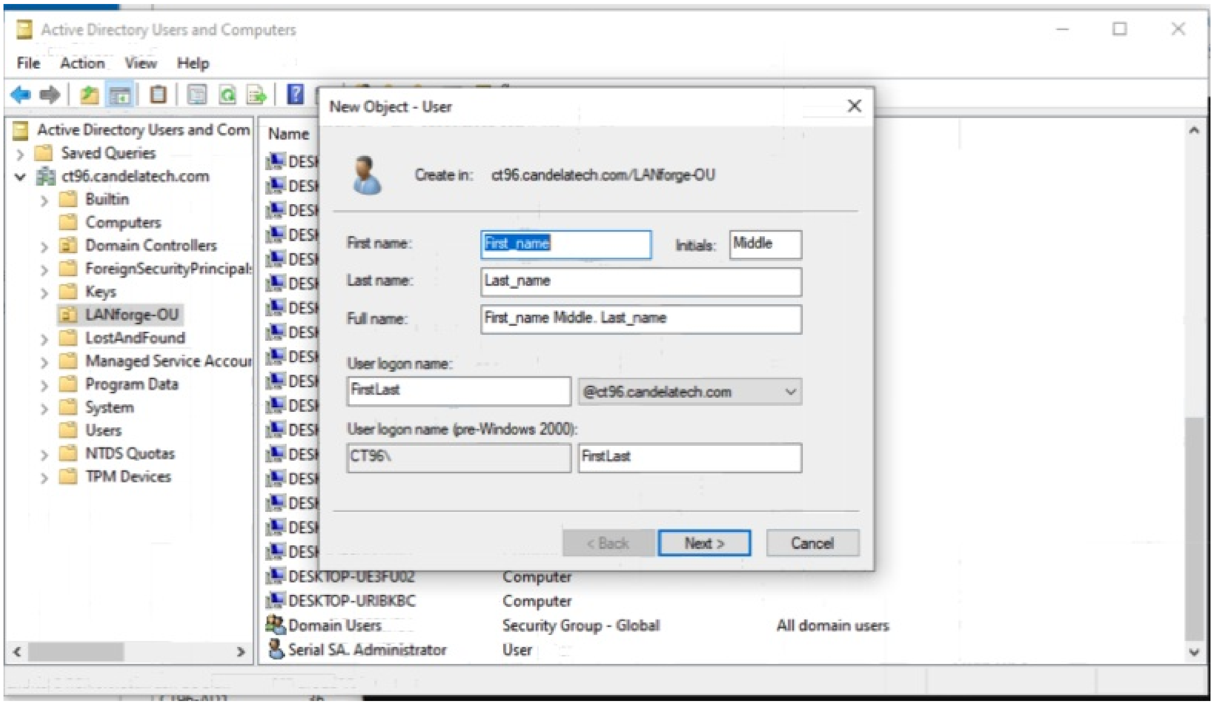
Confirm password: ••••••••••••••

☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled



New Object - User

Create in: ct96.candelatech.com/LANforge-OU

First name: First_name

Initials: Middle

Last name: Last_name

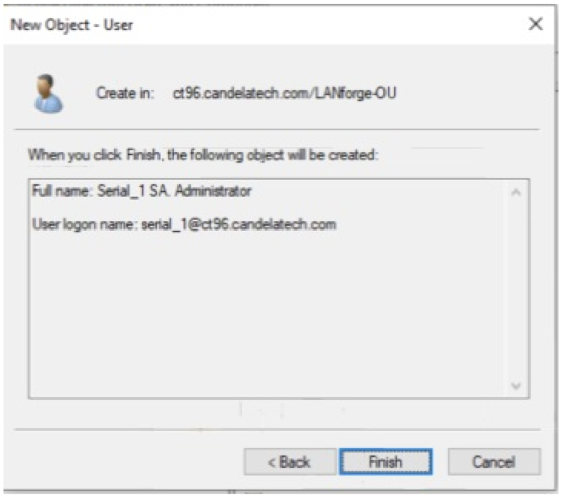
Full name: First_name Middle. Last_name

User logon name:

FirstLast @ct96.candelatech.com

User logon name (pre-Windows 2000):

CT96\ FirstLast



New Object - User

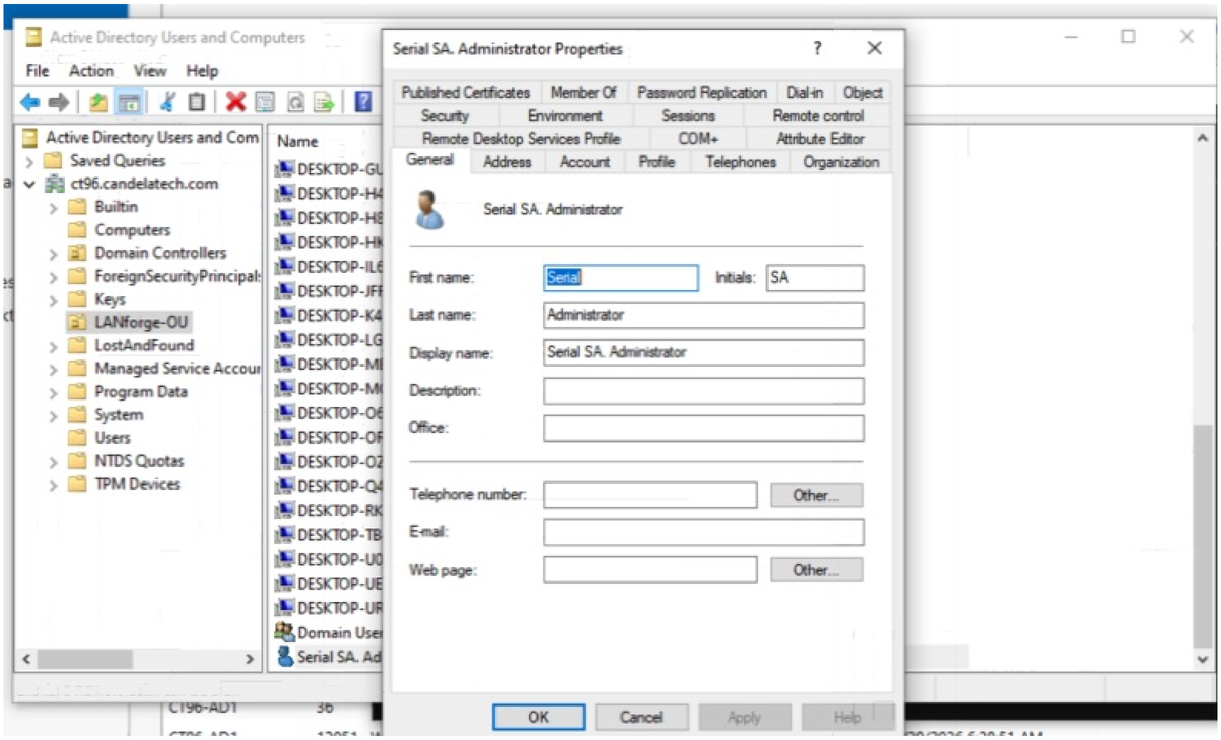
Create in: ct96.candelatech.com/LANforge-OU

When you click Finish, the following object will be created:

Full name: Serial_1 SA. Administrator

User logon name: serial_1@ct96.candelatech.com

7. Once this is done, double click on the newly created User in the new OU. The image below should be the same, sans First and Last name fields.



Serial SA. Administrator Properties

First name: Serial

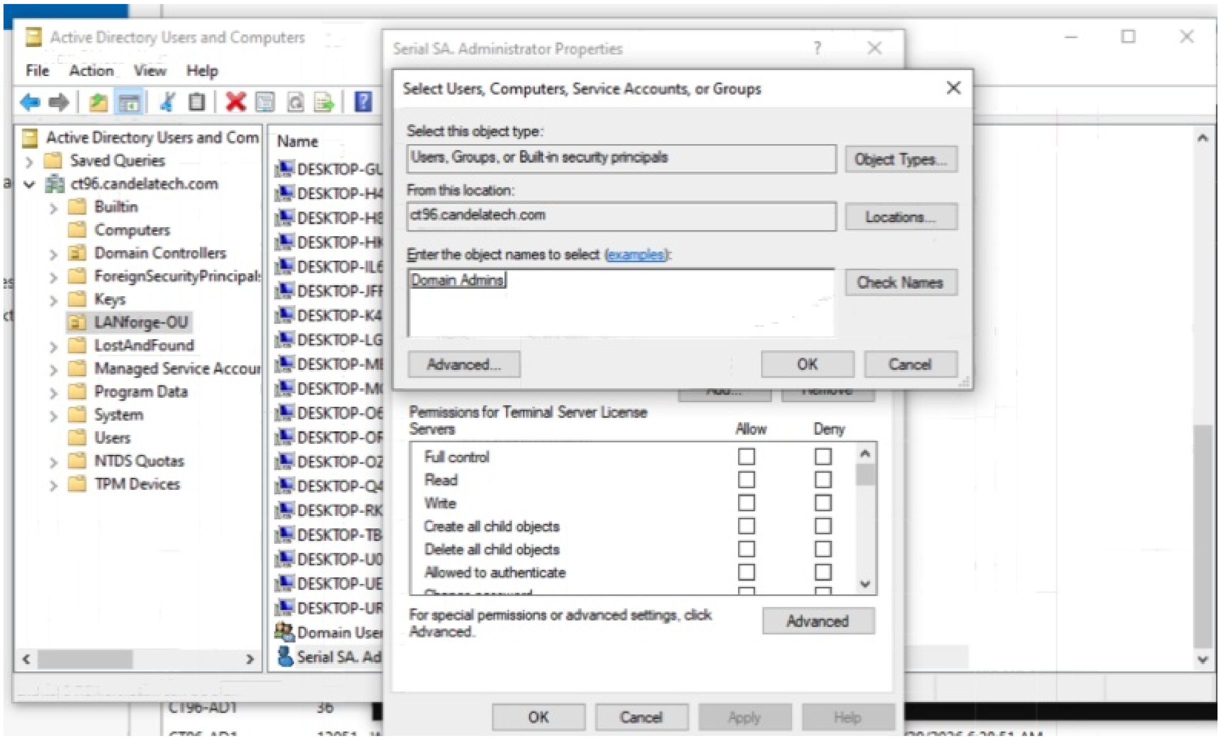
Initials: SA

Last name: Administrator

Display name: Serial SA. Administrator

8. Go to the security tab of this new User, and check to ensure the following is listed:
   - Everyone
   - SELF
   - Authenticated Users
   - SYSTEM
   - Domain Admins
   - Cert Publishers
   - Enterprise Admins
   - Administrators
   - Pre-Windows 2000 Compatible Access
   - Windows Authorization Access Group
   - Terminal Server License Servers

If not, below the listed security roles. Click Add..., and in the description box shown below, search for any missing items from the list above. Click Check Names, if it exists it will be underlined. Click OK.



Select this object type:
Users, Groups, or Built-in security principals

From this location:
ct96.candelatech.com

Enter the object names to select (examples):
Domain Admins

Permissions for Terminal Server License Servers

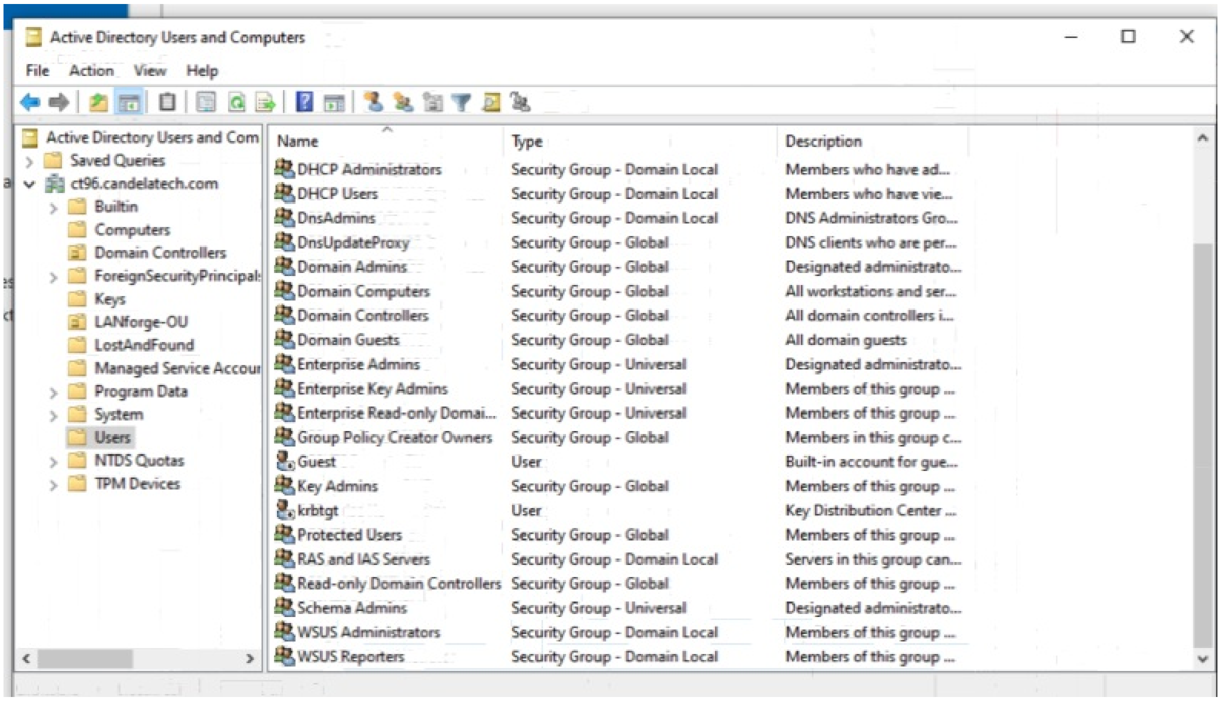
	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	□	□

For special permissions or advanced settings, click Advanced.

9. The following will be separated into Allow or Deny checkboxes. Listed below is everything that should be **ALLOWED**.
    - Everyone: Allow change password.
    - SELF: Allow change password, read private information, write private information.
    - Authenticated Users: Allow Read phone and mail options, read private information, read public information, read remote information, read web information.
    - SYSTEM: Allow everything.
    - Domain Admins: Allow everything **except** full control.
    - Enterprise Admins: Allow everything **except** full control.
    - Administrators: Allow everything **except** full control.
    - Cert Publishers, Pre-Windows 2000 Compatible Access, Windows Authorization Access Group, Terminal Server License Servers should have various allowed abilities, which should come as default.

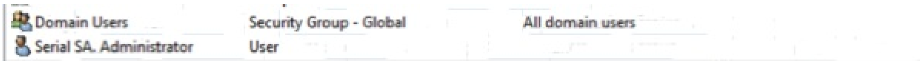
Once the security permissions match everything in steps 8 and 9, click OK and Apply, then close out of this window.

10. Back to the ADUC tool, on the left side, selecting your domain dropdown, find the Users folder and click it. Find the User "Domain Users". Click and drag "Domain Users" to your newly created OU. Example of the User folder is shown below.



Name	Type	Description
DHCP Administrators	Security Group - Domain Local	Members who have ad...
DHCP Users	Security Group - Domain Local	Members who have vie...
DnsAdmins	Security Group - Domain Local	DNS Administrators Gro...
DnsUpdateProxy	Security Group - Global	DNS clients who are per...
Domain Admins	Security Group - Global	Designated administrato...
Domain Computers	Security Group - Global	All workstations and ser...
Domain Controllers	Security Group - Global	All domain controllers i...
Domain Guests	Security Group - Global	All domain guests
Enterprise Admins	Security Group - Universal	Designated administrato...
Enterprise Key Admins	Security Group - Universal	Members of this group ...
Enterprise Read-only Domai...	Security Group - Universal	Members of this group ...
Group Policy Creator Owners	Security Group - Global	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group - Global	Members of this group ...
krbtgt	User	Key Distribution Center ...
Protected Users	Security Group - Global	Members of this group ...
RAS and IAS Servers	Security Group - Domain Local	Servers in this group can...
Read-only Domain Controllers	Security Group - Global	Members of this group ...
Schema Admins	Security Group - Universal	Designated administrato...
WSUS Administrators	Security Group - Domain Local	Members of this group ...
WSUS Reporters	Security Group - Domain Local	Members of this group ...

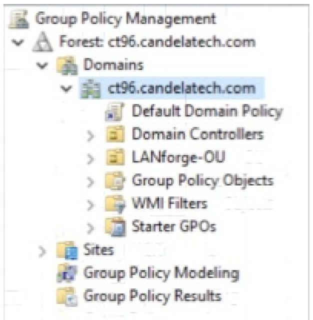
11. Your newly created OU should look something like this, with a normal user (first name last name) along with domain user. Close out of the ADUC window when finished with this step.



Domain Users	Security Group - Global	All domain users
Serial SA. Administrator	User	

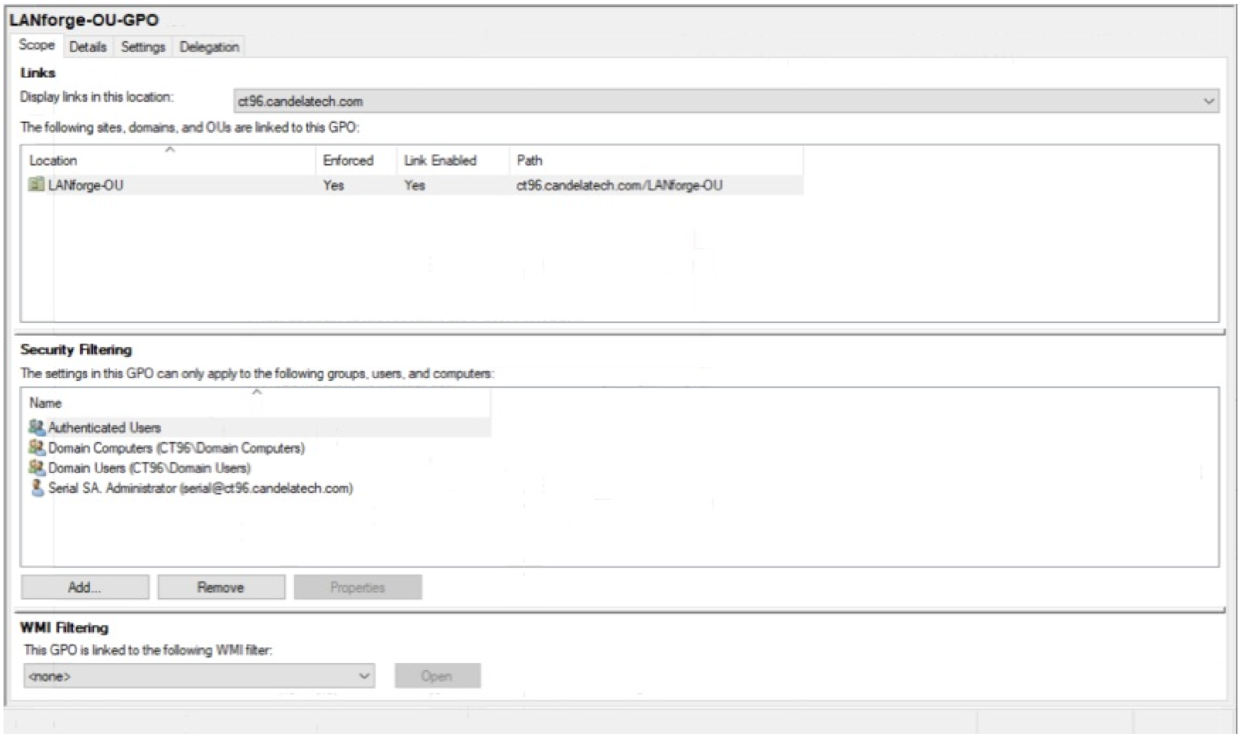
GPM, and creating your GPO

12. Back to the Server Manager, go to Tools → Group Policy Management (GPM). On the left hand side will be your domain. Click on it to open subfolder details. Right click your domain and you should see your OU you created in the ADUC tool.



13. In this new folder, right click and select Create a GPO in this domain, and Link it here.... Name it.

14. Click on the newly created GPO and the right side of the GPM tool will populate.



LANforge-OU-GPO

Links

Display links in this location: ct96.candelatech.com

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
LANforge-OU	Yes	Yes	ct96.candelatech.com/LANforge-OU

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

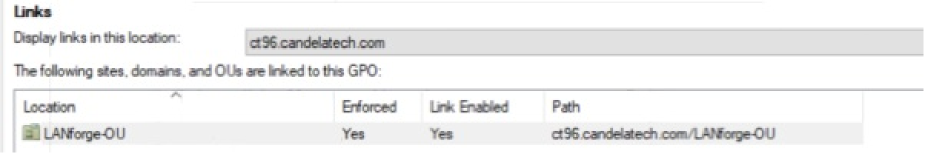
Name
Authenticated Users
Domain Computers (CT96\Domain Computers)
Domain Users (CT96\Domain Users)
Serial SA. Administrator (serial@ct96.candelatech.com)

WMI Filtering

This GPO is linked to the following WMI filter:

<none>

15. The right panel will contain information about linked GPOs to the currently selected OU as well as details on security filtering and WMI filtering.
16. Under the Links table, it should look like this:



Links

Display links in this location: ct96.candelatech.com

The following sites, domains, and OUs are linked to this GPO:

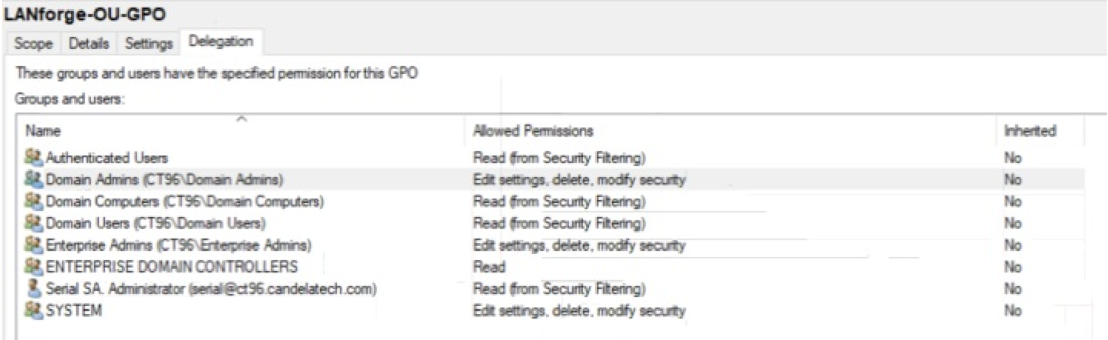
Location	Enforced	Link Enabled	Path
LANforge-OU	Yes	Yes	ct96.candelatech.com/LANforge-OU

17. The Security Filtering table will need the following:
    - Authenticated Users
    - Domain Computers
    - Domain Users
    - User (the one we created in ADUC)

To add new items to the Security Filter, click Add... and type in the description box exactly what is suggested above, i.e., Domain Users. Click Check Names and it should underline if it exists, then click OK.

18. Next, at the top above the Links table, click on the Details tab and it should look similar to this:

19. Go to the Delegation tab, near the Details tab from the previous step, and check the various permissions against this example:



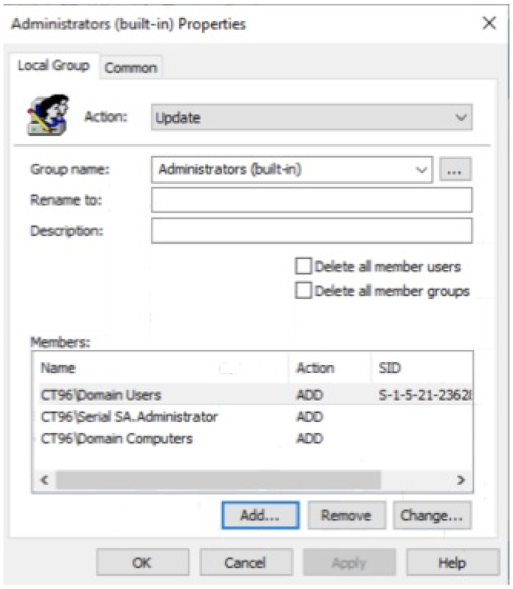
LANforge-OU-GPO

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (CT96\Domain Admins)	Edit settings, delete, modify security	No
Domain Computers (CT96\Domain Computers)	Read (from Security Filtering)	No
Domain Users (CT96\Domain Users)	Read (from Security Filtering)	No
Enterprise Admins (CT96\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
Serial SA. Administrator (serial@ct96.candelatech.com)	Read (from Security Filtering)	No
SYSTEM	Edit settings, delete, modify security	No

20. Now, on the panel to the left where the folders are displayed and the OU and GPO can be viewed, right click on the GPO, ensure that "Enforced" and "Link Enabled" are checked, then click Edit....
21. Follow this path: Computer Configuration → Preferences → Control Panel Settings → Local Users and Groups.
22. Right click → New → Local User. Action, drop down and select Update. For Group name copy and paste this "Administrators (built-in)" exactly.
23. Under the Members box at the bottom, ensure that Domain Users, User (from ADUC) and Domain Computers are in the box. Should look similar to this:



Administrators (built-in) Properties

Local Group | Common

Action: Update

Group name: Administrators (built-in)

Rename to:

Description:

□ Delete all member users

□ Delete all member groups

Members:

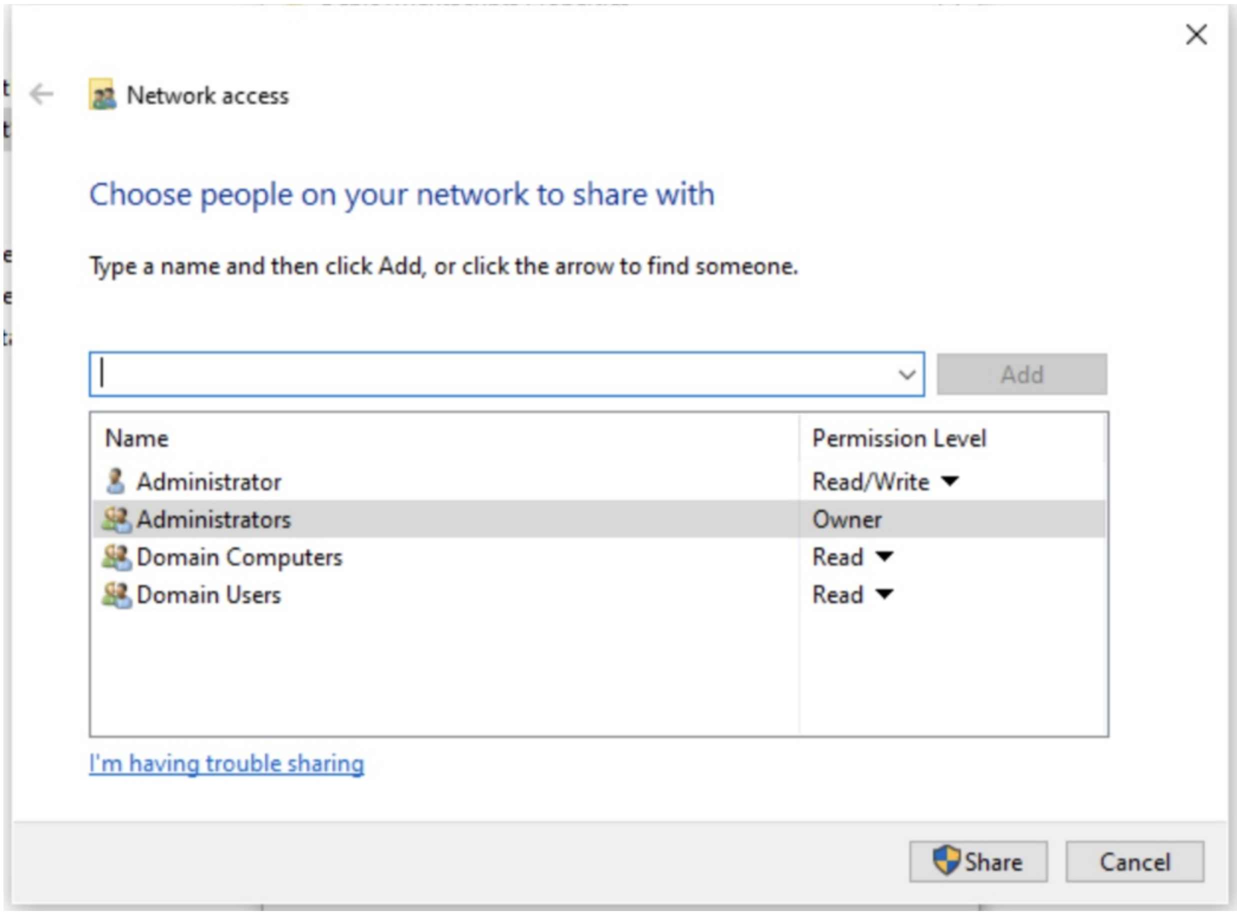
Name	Action	SID
CT96\Domain Users	ADD	S-1-5-21-2362
CT96\Serial SA.Administrator	ADD	
CT96\Domain Computers	ADD	

Details of your GPO

24. Left side of the GPM editor again, from Local Users and Groups, move to Scheduled Tasks.
25. Right click → New task (At least Windows 7). Name: Software Deployment Script. Description can be whatever you would like. Security options, When running the task, use the following user account: NT AUTHORITY\System. Select "Run whether the user is logged on or not". Check run with highest privileges.
26. Next tab, at the top, Triggers. Click New... at the bottom, and from the dropdown at the top of the new pop-up window, select "At startup". Click OK.
27. Next tab, at the top, Actions. Click New..., action will be Start a program. Program/script: `powershell.exe`. Add arguments: `-ExecutionPolicy Bypass -NoProfile -File "C:\LANforge-Install\windows_lf_setup.ps1"`. Please include quotes for the -File parameter.
28. Next tab, Settings. The only box that should be selected should be "Run task as soon as possible after scheduled start is missed".
29. Next tab, Common. One box here should be checked, "apply once and do not reapply".
30. Click OK to finish the "Software Deployment Script" properties window.
31. Follow this path: Computer Configuration → Preferences → Windows Settings → Registry. This is where we will be giving the arguments to the installation script.
32. Right click → New → Registry Item (this will apply for the next 8 settings). Follow these steps for each bullet point below. For each Registry Item, the Action, Hive and Key Path will be the same. Value name, Value type and Value data will differ.
    - Action → Update
    - Hive → HKEY_LOCAL_MACHINE
    - Key Path → SOFTWARE\CandelaTechnologies\LANforge-Server
    - **Value name → mode**
        - Value type → REG_SZ
        - Value data → Resource

- **Value name → clusterid**
    - Value type → REG_SZ
    - Value data → (IP address of LANforge manager, 523c, 521b, etc)
- **Value name → realm**
    - Value type → REG_DWORD
    - Value data → (realm of LANforge manager)
    - Base → Decimal
- **Value name → lfver**
    - Value type → REG_SZ
    - Value data → 5.5.2
- **Value name → password**
    - Value type → REG_SZ
    - Value data → (password set for the User from step 6 in the ADUC)
- **Value name → username**
    - Value type → REG_SZ
    - Value data → (whatever First name is set for the User created in the ADUC)
- **Value name → FQDN**
    - Value type → REG_SZ
    - Value data → (i.e. ct96.candelatech.com)
- **Value name → Installed**
    - Value type → REG_DWORD
    - Value data → 0
    - Base → Decimal

33. Once all 8 registry items have been made, go to Computer Configuration → Preferences → Windows Settings → Files.
34. Right click → New → File. Action: Replace. Source File: `\\SERVER-HOSTNAME\DeploymentScripts\windows_lf_setup.ps1`. Destination: `C:\LANforge-Install\windows_lf_setup.ps1`. Attributes: Archive. Click OK. Close out of the GPM editor.
35. Go to File Explorer, usually at the bottom of task bar. On the left hand side, go to `Local Disk (C:\)`. Right click → New → Folder. Name it `DeploymentScripts`. Click Share.... Next to the Add button, there will be a drop down arrow, click this arrow and choose find people....
36. Search for `DOMAIN\Administrator` (i.e. `CT96\Administrator`), as well as `BUILTIN\Administrator`. Add both of these, if they were not already added. Search for `Domain Computers` and `Domain Users`, add both. An example is shown below of who this folder should be shared with.



Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner
Domain Computers	Read ▾
Domain Users	Read ▾

37. Click share, ensure that `DeploymentScripts` is the name of the folder shared, as well as the file path, which should be `DOMAIN\DeploymentScripts`. Close out of these windows, and close File Explorer.
38. In the search bar, open PowerShell, and navigate to `C:\DeploymentScripts`, via `cd ..\..\DeploymentScripts\`.
39. Run this command to get the installation script: `wget http://www.candelatech.com/windows_lf_setup.ps1 -o windows_lf_setup.ps1`. Close out of PowerShell.

Windows client install

40. On a Windows client, if booting the computer for the first time, create a User named exactly the same as the User defined previously in this guide on step 6. Perform all nessecary Windows updates and installs through Windows update.
41. While the computer is updating, open a PowerShell terminal and type: `ipconfig`. Ensure that the default gateway for this client's IP address is the IP address of the Domain Controller.
42. In the Windows settings, search for "Access work or school". This requires Windows 10 or Windows 11 pro, and click Connect. Under Alternate Actions, click Join this device to a local Active Directory Domain. Type in the FQDN of the domain, i.e. ct96.candelatech.com.
43. If successful, a dialog box will pop up asking for username and password. This is the User as outlined in step 6. Enter username and password then click Next.
44. The next window will ask if an account should be added. It will be prepopulated with the username from step 43, and "Standard User", these defaults are fine. Click Next.
45. On the domain controller, go to Tools → ADUC, and on the left side click computers, drag newly listed computer to OU we created in step 5, on left side.
46. On client, click restart now.
47. After client reboots, logs from the install will be stored in `C:\LANforge-Install\Logs\`.

To list the files in descending order:

1. Go to the logs directory by typing this command into PowerShell: `cd C:\LANforge-Install\Logs\`.
2. Type this command: `ls | sort LastWriteTime -Descending`.
3. Files are written in the format as follows: `deployment-log-YYYYMMDD-HHMMSS.txt`.

To follow the logs, use the commands below:

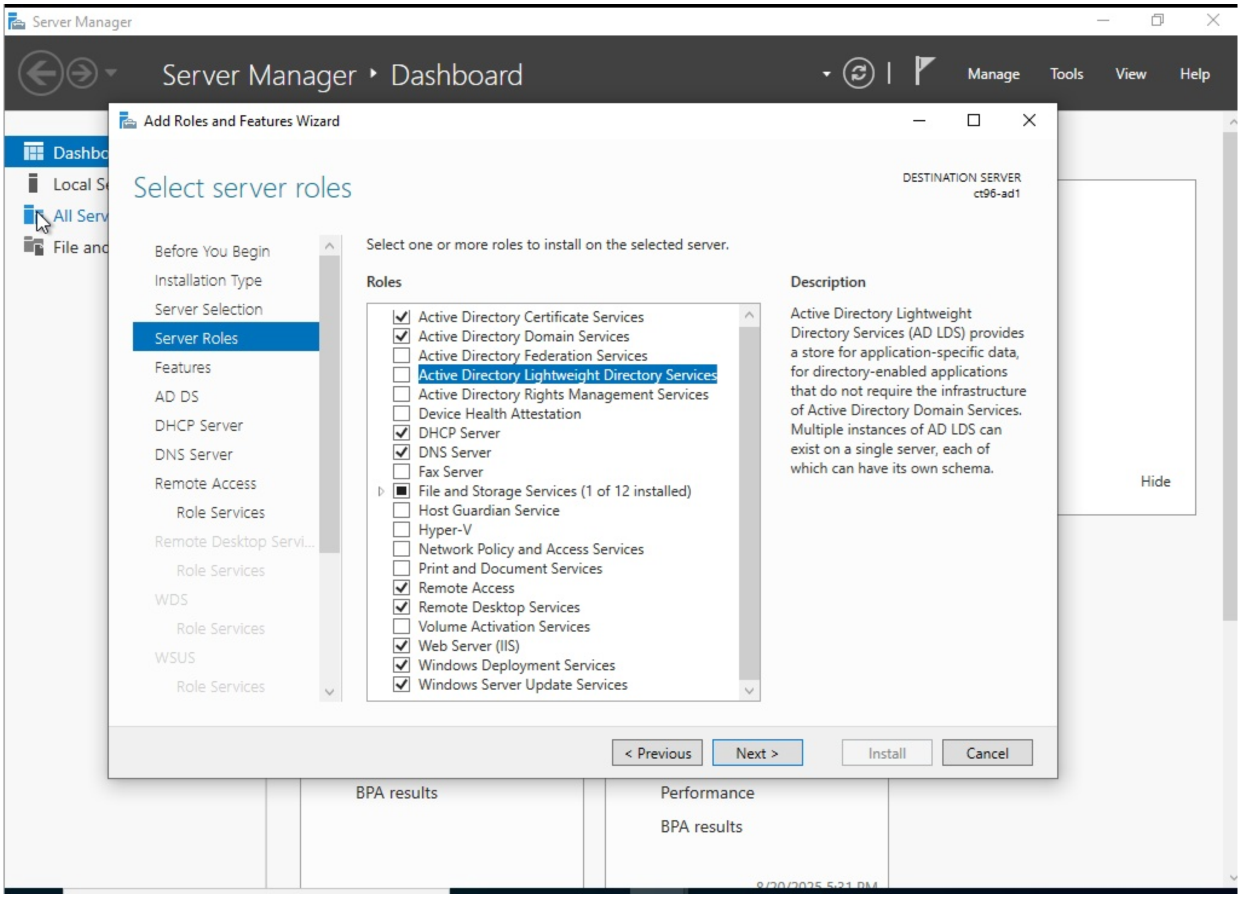
1. Go to the logs directory by typing this command into PowerShell: `cd C:\LANforge-Install\Logs\`.
2. Watch the top file with `Get-Content deployment-log-YYYYMMDD-HHMMSS.txt -Wait`.
3. Example file format: `deployment-log-20260116-133645.txt`, i.e., January 16th 2026 at 13:36:45.

To add additional Windows clients, repeat steps 40 - 46.

Appendix A

Setting up a basic domain controller requires Windows Server 2022 or greater.

1. Install Windows Server 2022 on your server of choice.
2. Hostname can be anything, however in our experience setting hostname in relation to the domain name (e.g. ct96.candelatech.com), hostname being ct96-ad1 (active directory #1) was descriptive enough.
3. Workgroup, similar to hostname i.e. ct96.
4. Set a static IP for the domain controller. This static IP will be the DNS server for the windows clients. Ensure that the static IP is on the same subnet as the default gateway in step 2.
    - Restart the server to make sure the static IP sticks.
5. Starting at the Server Manager dashboard, in the upper right hand corner next to Tools, click Manage. Click Add Roles and Features.
6. Installation Type should be Role-based.
7. Server Selection should show the server. If no server is being shown, use the Add Servers command from the Manage menu in the upper right of the Server Manager Dashboard. Then click Next.
8. Server roles will include (image shown below as example):
    - Activei Directory Domain Services
    - DHCP Server
    - DNS Server
    - File and Storage Services
        - File and iSCSI Services
    - Network Policy and Access Services
    - Remote Access
    - Remote Desktop Services
    - Web Server (IIS)
        - Web Server
        - Management Tools
    - Windows Deployment Services
    - Windows Server Update Services



Select server roles

DESTINATION SERVER
ct96-ad1

Select one or more roles to install on the selected server.

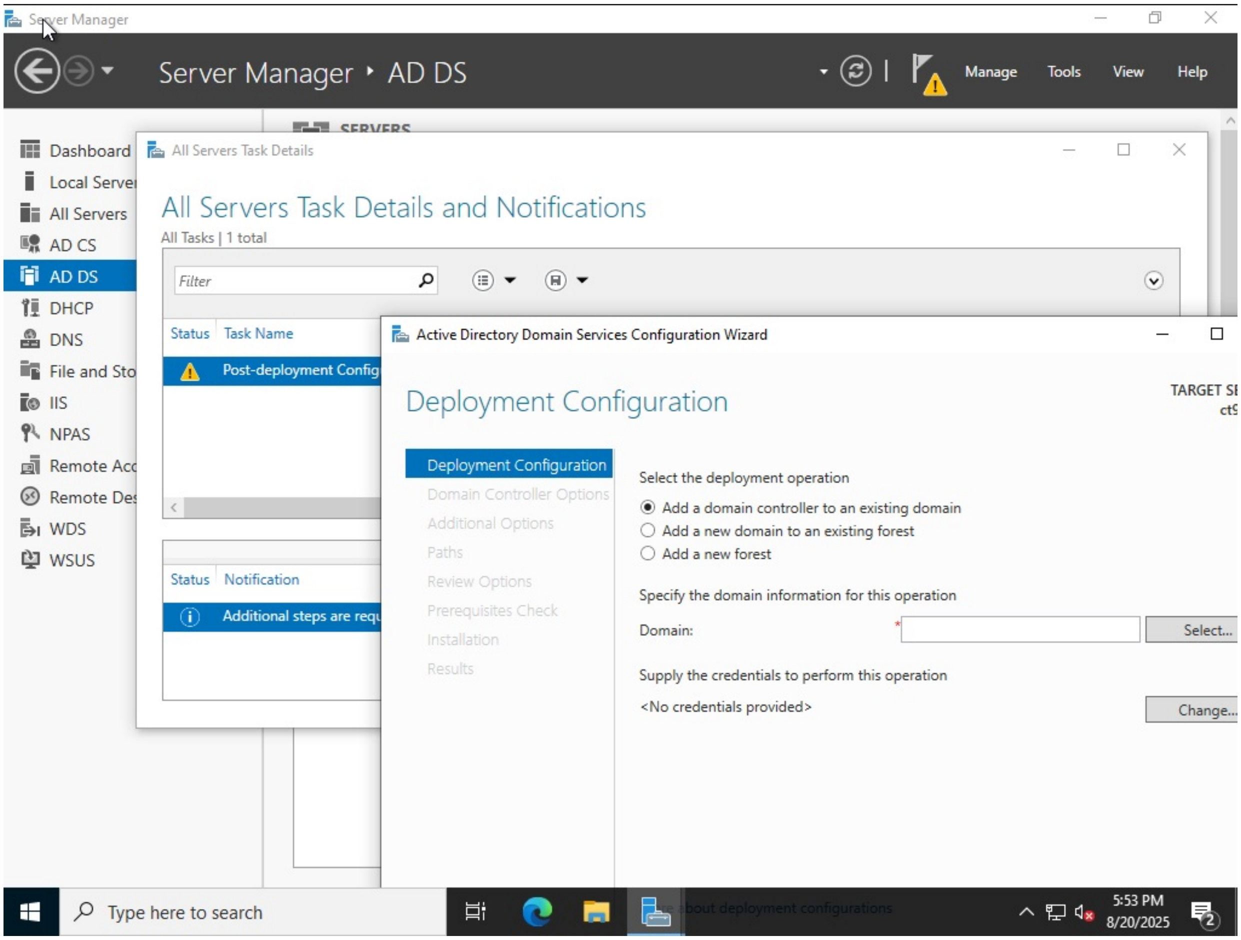
Roles

- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☑ DHCP Server
- ☑ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☑ Remote Access
- ☑ Remote Desktop Services
- ☐ Volume Activation Services
- ☑ Web Server (IIS)
- ☑ Windows Deployment Services
- ☑ Windows Server Update Services

Description

Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.

9. Features will include:
    - .NET Framework 4.8 Features
        - WCF Services
    - Azure Arc Setup
    - Group Policy Management
    - Microsoft Defender Antivirus
    - RAS Connection Manager Administration Kit
    - Remote Server Administration Tools
        - Feature Administration Tools
        - Role Administration Tools
    - RPC Over HTTP Proxy
    - System Data Archiver
    - System Insights
    - Telnet Client
    - Windows Internal Database
    - Windows PowerShell
    - Windows Process Activiation Service
    - WoW64 Support
    - XPS Viewer
10. Reboot for settings in step 8 and 9 to apply.
11. Upper right hand corner next to Manage and Tools there will be a notification flag, prompting the post deployment configuration. This will pull up the Active Directory Domain Services Configuration Wizard. Example image shown below.



All Servers Task Details and Notifications

All Tasks | 1 total

Status	Task Name
⚠	Post-deployment Config

Status	Notification
ⓘ	Additional steps are requ

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SE
ct9

Select the deployment operation

● Add a domain controller to an existing domain

○ Add a new domain to an existing forest

○ Add a new forest

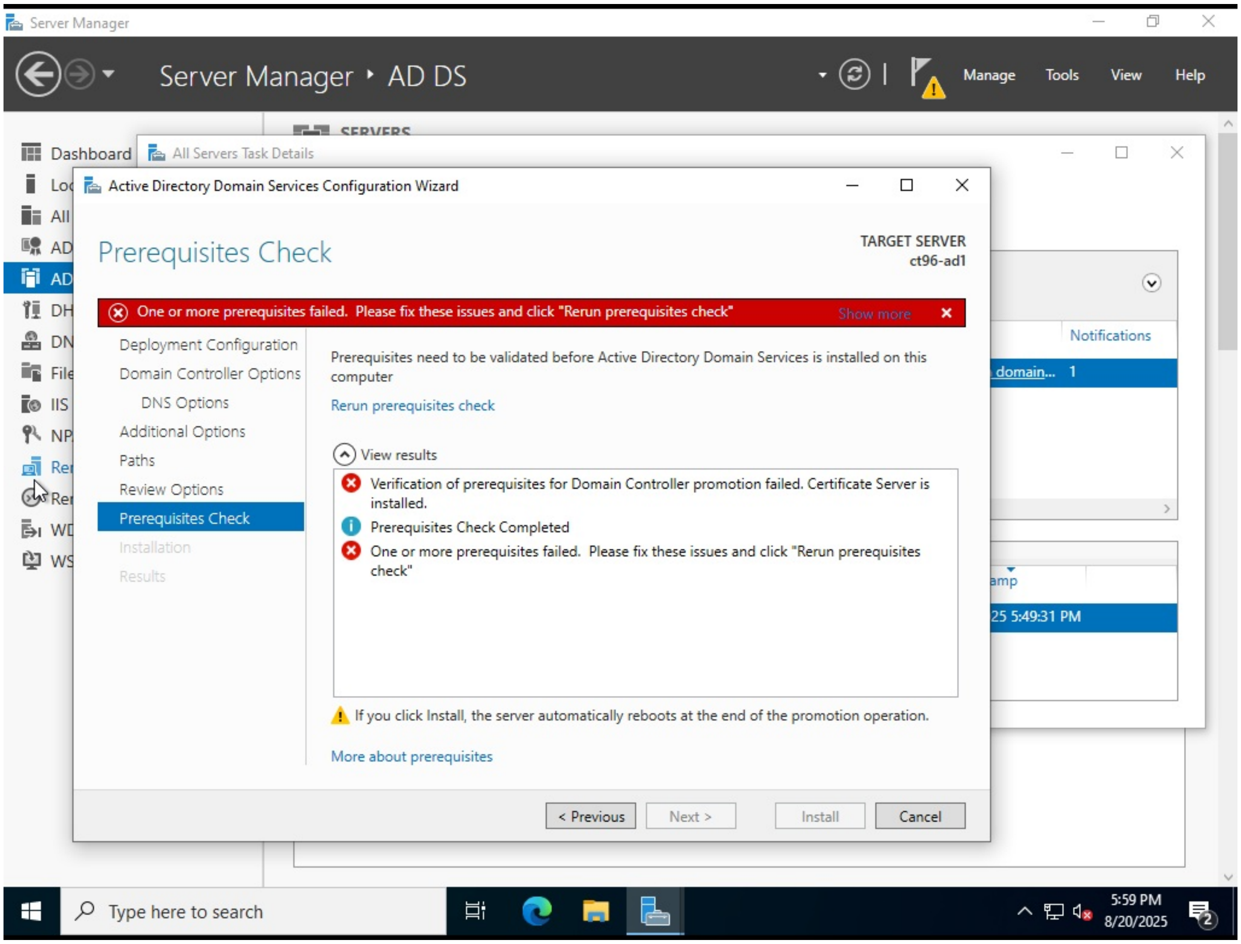
Specify the domain information for this operation

Domain: * Select...

Supply the credentials to perform this operation

<No credentials provided> Change...

12. Add a new forest, customize your domain name here. Functional level: Server 2012.
13. Directory Services Restore Mode (DSRM) password: customize here.
14. In case the Prerequisites Check fails, example image shown below, go to Remove Roles and Features in the upper right hand corner, where Add Roles and Features lives. Remove the roles and services shown in the second image shown below.



Prerequisites Check

TARGET SERVER
ct96-ad1

One or more prerequisites failed. Please fix these issues and click "Rerun prerequisites check"

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

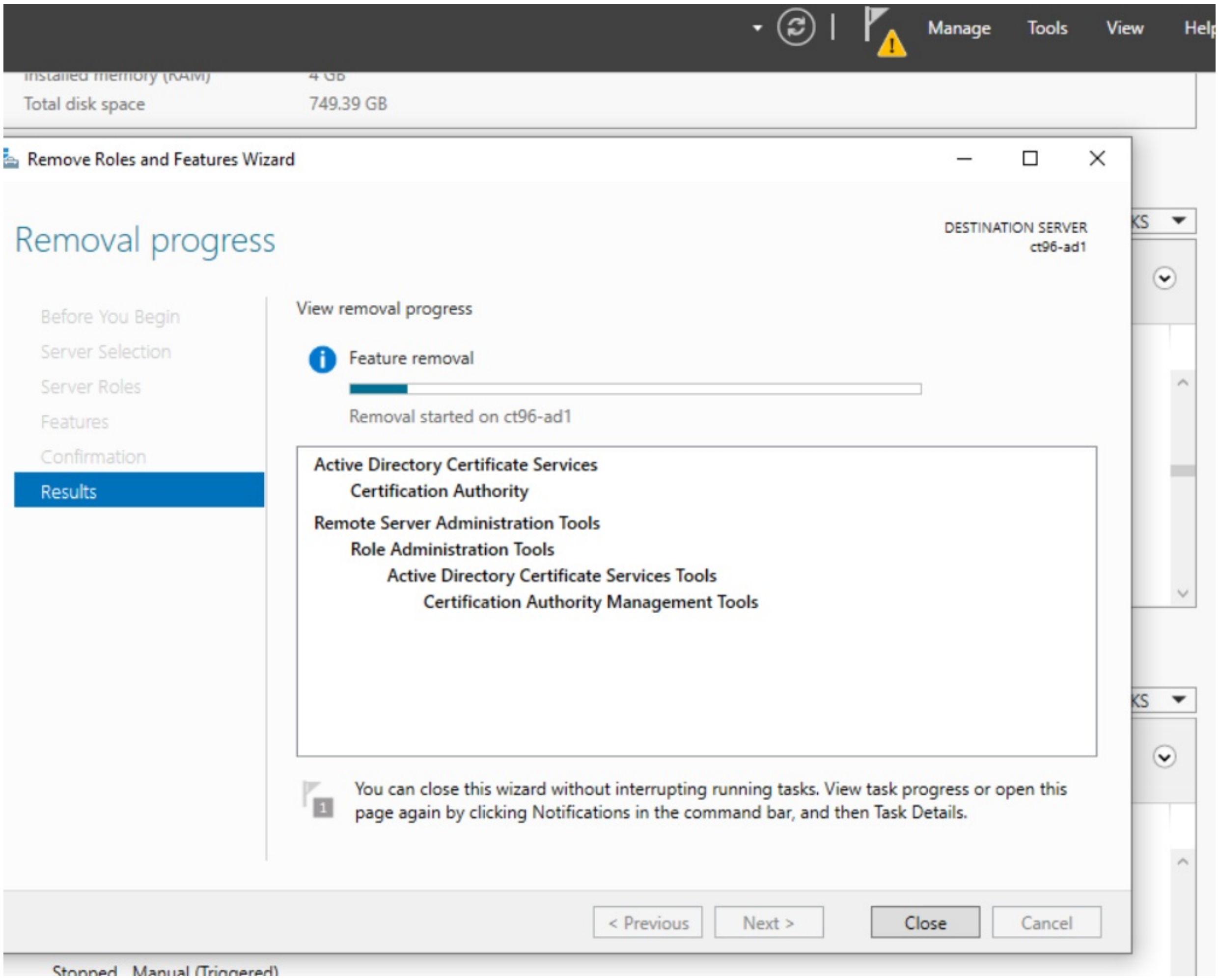
Rerun prerequisites check

View results

- Verification of prerequisites for Domain Controller promotion failed. Certificate Server is installed.
- Prerequisites Check Completed
- One or more prerequisites failed. Please fix these issues and click "Rerun prerequisites check"

If you click Install, the server automatically reboots at the end of the promotion operation.

More about prerequisites



Total disk space 749.39 GB

Removal progress

DESTINATION SERVER
ct96-ad1

View removal progress

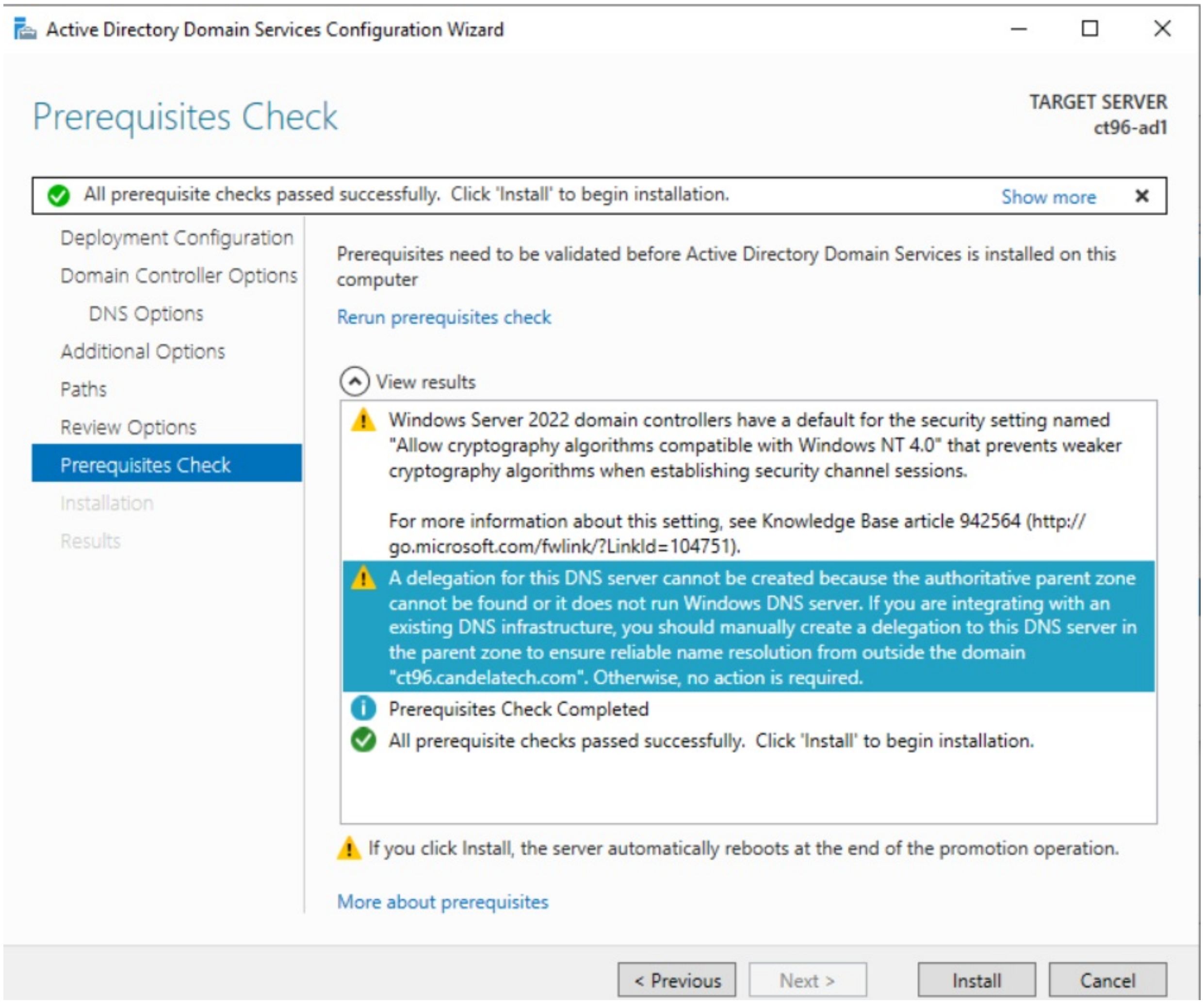
Feature removal

Removal started on ct96-ad1

Active Directory Certificate Services
    Certification Authority
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

15. If the Prerequisites Check succeeds, it will look similar to this:



Active Directory Domain Services Configuration Wizard

Prerequisites Check

TARGET SERVER
ct96-ad1

All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "ct96.candelatech.com". Otherwise, no action is required.

Prerequisites Check Completed

All prerequisite checks passed successfully. Click 'Install' to begin installation.

If you click Install, the server automatically reboots at the end of the promotion operation.

16. Next, go to Server Manager → Tools → Active Directory Users and Computers. Add User username/password. This is the **exact** same User as step 6 from the guide above. Set the password to never expire. Add this User to the group Administrators.
17. Open a PowerShell terminal as an Administrator and type: `Install-WindowsFeature DHCP -IncludeManagementTools`. Hit Enter.
18. Type: `Add-DhcpServerInDC -DnsName HOSTNAME.DOMAIN_NAME -IPAddress STATIC IP OF HOSTNAME`. Where hostname is the name of the Domain Controller Server, and domain name is the name of the domain chosen in step 12 of Appendix A. Hit Enter
19. Type: `Add-DhcpServer4Scope -Name “NETWORK_NAME” -StartRange IP_START -EndRange IP_END -SubnetMask 255.255.255.0`, where network name is the name of the network you want to create. IP start and IP end are the ranges of DHCP yo uwant to serve, with the corresponding proper subnet mask.

For more information, please visit this Microsoft Learn article on the subject.