



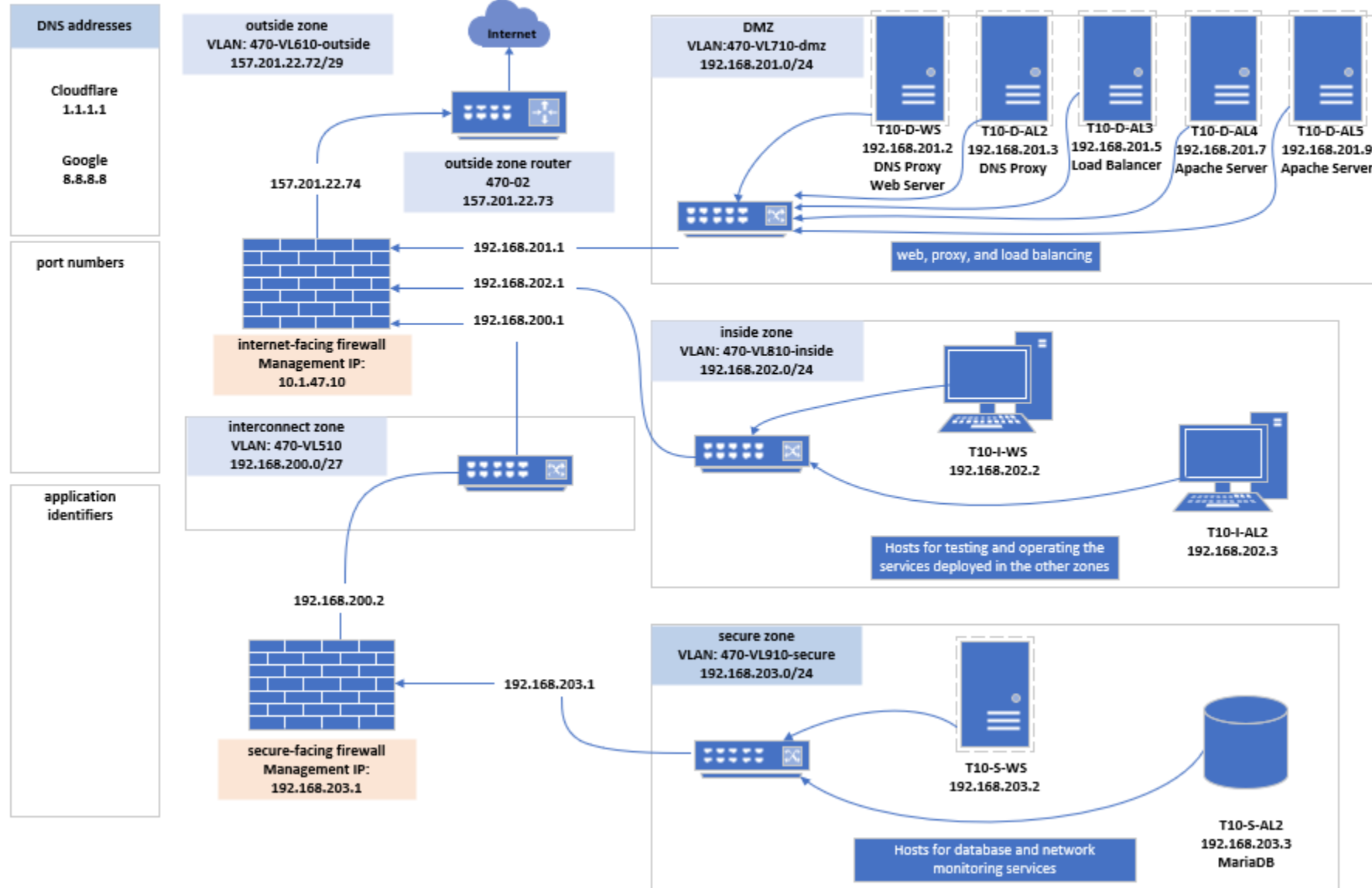
Task: Above-and-Beyond 3

cit470

Task: Diagram

team 10 Layer 3: outside zones' public IPv4 address assignments

public space (IPv4 subnet ID)	router	firewall (dynamic NAT)	static NAT	(broadcast)
157.201.22.72/29	157.201.22.73	157.201.22.74 470t10ra.cit.byui.edu	157.201.22.75- 157.201.22.78	157.201.22.79



Active Directory Installation



Select destination server

DESTINATION SERVER
T10-D-WS

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

- ☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter: <input type="text"/>			
Name	IP Address	Operating System	
T10-D-WS	192.168.201.2	Microsoft Windows Server 2022 Standard	

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

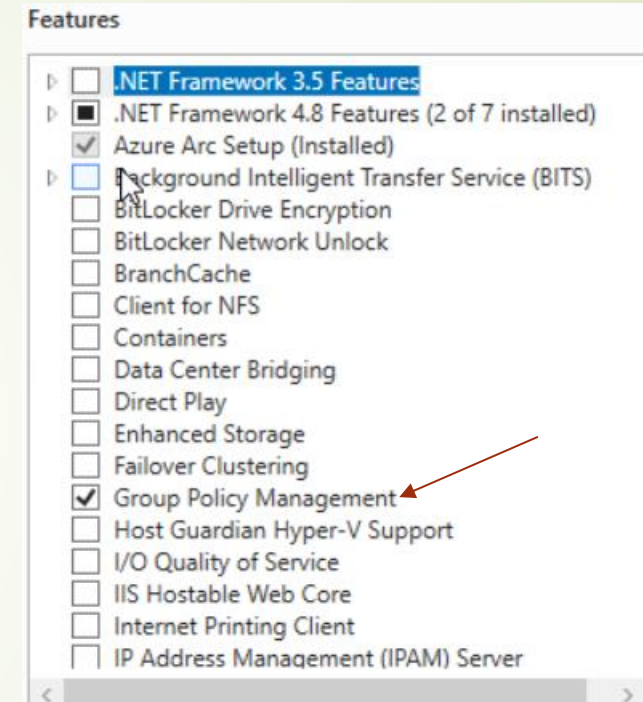
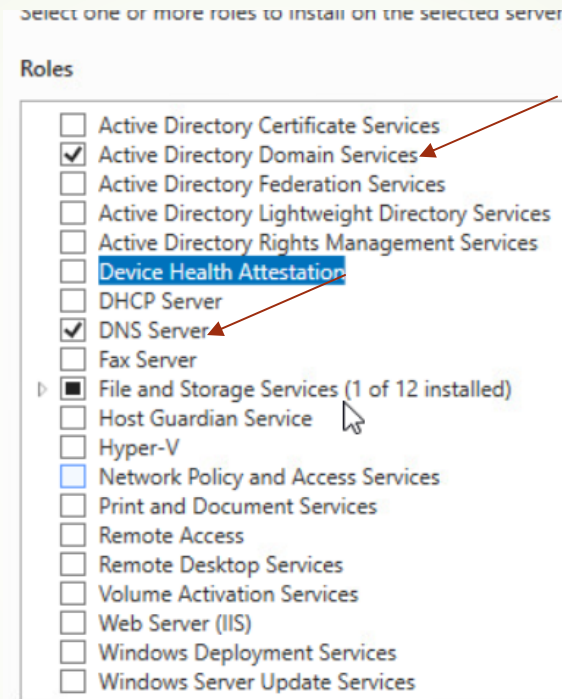
Cancel

Active Directory Installation

Under “Roles”
Select the “Active
Directory Domain
Services” and the
“DNS Server”
options.

Under “Features”
make sure that
“Group Policy
Manager” is
selected.

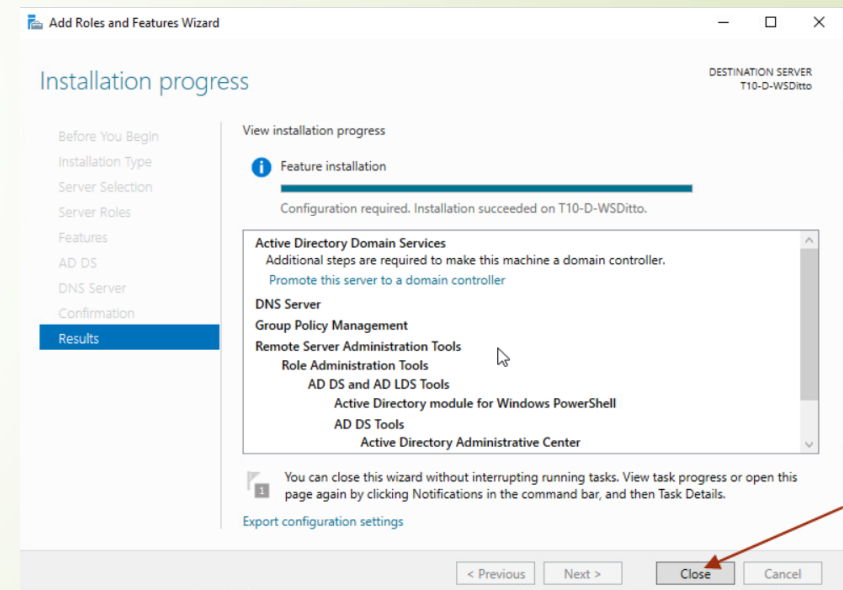
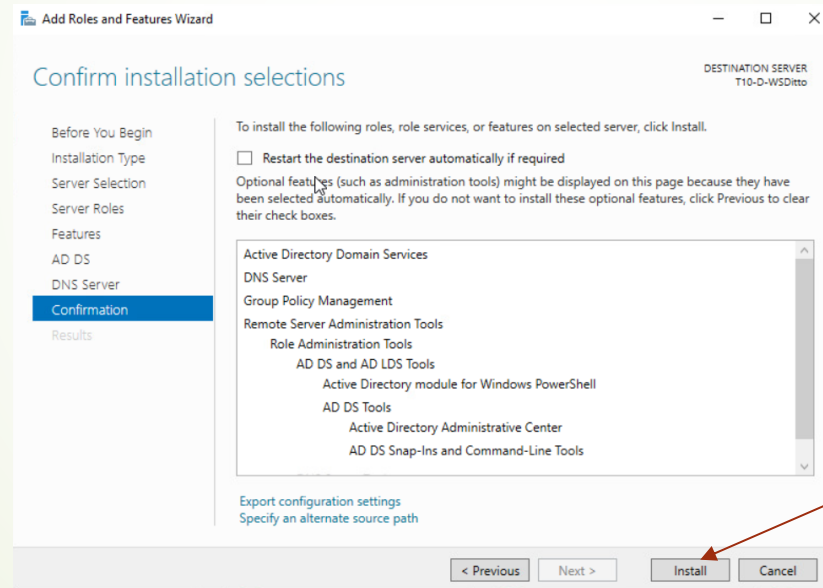
Click Next and then
click Next on the
following two
pages.



Active Directory Installation

Click
"Install"

Click
"Close"

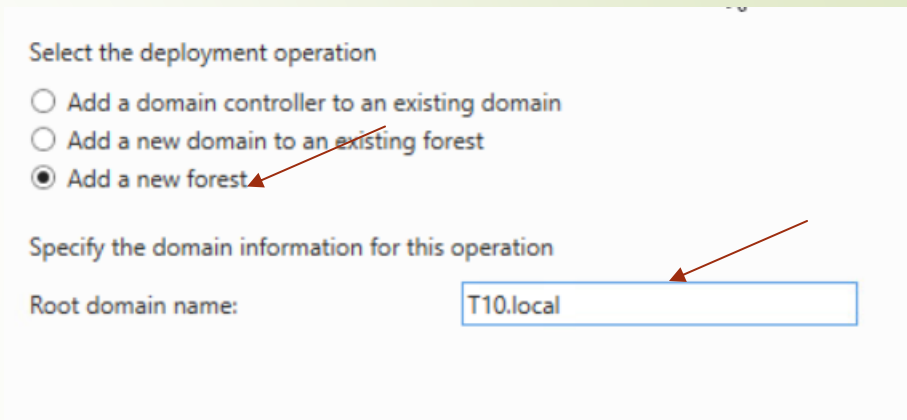
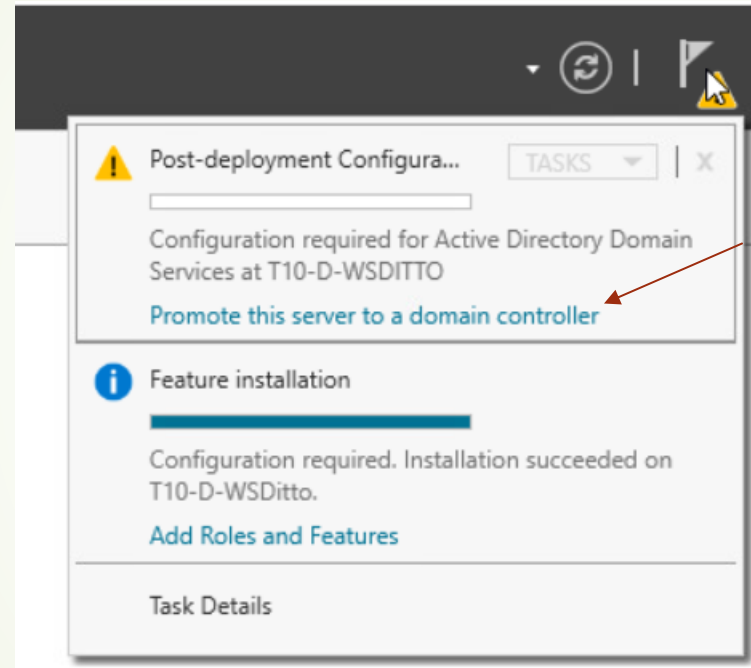


Active Directory Installation

Click on the exclamation flag and then select "Promote this server to domain controller".

When the Active Directory Domain Services Configuration Wizard opens, Select "Add a new forest".

Enter your Domain name and click "Next".



Active Directory Installation

Enter a
DSRM
Password

Click "Next"

On the DNS
Options
page click
"Next"

The screenshot displays the 'DNS Options' page of the Active Directory Installation Wizard. The left pane shows the 'Forest functional level' and 'Domain functional level' both set to 'Windows Server 2016'. Under 'Specify domain controller capabilities', the 'Domain Name System (DNS) server' and 'Global Catalog (GC)' are checked, while 'Read only domain controller (RODC)' is unchecked. The 'Type the Directory Services Restore Mode (DSRM) password' section has two password fields, both masked with dots. The right pane shows the 'DNS Options' tab selected in the left navigation pane. A warning message at the top states: 'A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...'. Below this, the 'Specify DNS delegation options' section has a 'Create DNS delegation' checkbox which is unchecked. At the bottom right, the 'Next >' button is highlighted with a red arrow.

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

- ☒ Domain Name System (DNS) server
- ☒ Global Catalog (GC)
- ☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

DNS Options

TARGET SERVER
T10-D-WSditto

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... Show more X

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify DNS delegation options

☐ Create DNS delegation

More about DNS delegation

< Previous Next > Install Cancel

Active Directory Installation



Active Directory Installation

On the other Options Page and the Paths page leave the default settings and click "Next".

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

T10

Specify the location of the AD DS database, log files, and SYSVOL

Database folder:

C:\Windows\NTDS

Log files folder:

C:\Windows\NTDS

SYSVOL folder:

C:\Windows\SYSVOL

Active Directory Installation

Review options then click “Next”.

Once Prerequisite Check is completed click “Install”.

The Server will automatically restart.

Review your selections:

Configure this server as the first Active Directory domain controller in a new forest.

The new domain name is "T10.local". This is also the name of the new forest.

The NetBIOS name of the domain: T10

Forest Functional Level: Windows Server 2016

Domain Functional Level: Windows Server 2016

Additional Options:

Global catalog: Yes

DNS Server: Yes

Create DNS Delegation: No

These settings can be exported to a Windows PowerShell script to automate additional installations

[View script](#)

[More about installation options](#)

Prerequisites Check

TARGET SERVER
T10-D-WSDitto

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation. [Show more](#)

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

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

[Rerun prerequisites check](#)

View results

⚠ 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 "T10.local". Otherwise, no action is required.

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

[More about prerequisites](#)

< Previous Next >

Install Cancel

Install Cockpit

```
[cditto@T10-D-AL3 ~]$ sudo dnf install cockpit-podman cockpit-machines cockpit-networkmanager cockpit-packagekit
```

```
[cditto@T10-D-AL3 ~]$ sudo systemctl enable --now cockpit.socket
```

```
[cditto@T10-D-AL3 ~]$ sudo systemctl start cockpit cockpit.socket
```

```
[cditto@T10-D-AL3 ~]$ sudo systemctl status cockpit
```

```
● cockpit.service - Cockpit Web Service
   Loaded: loaded (/usr/lib/systemd/system/cockpit.service; static; vendor preset: enabled)
   Active: active (running) since Fri 2024-02-16 19:39:06 CST; 8s ago
     Docs: man:cockpit-ws(8)
   Process: 532788 ExecStartPre=/usr/libexec/cockpit-certificate-ensure --for-cockpit (code=0)
  Main PID: 532795 (cockpit-tls)
    Tasks: 1 (limit: 23500)
   Memory: 700.0K
    CGroup: /system.slice/cockpit.service
            └─532795 /usr/libexec/cockpit-tls
```

```
Feb 16 19:39:06 T10-D-AL3.localdomain systemd[1]: Starting Cockpit Web Service.
```

```
Feb 16 19:39:06 T10-D-AL3.localdomain systemd[1]: Started Cockpit Web Service.
```

```
[cditto@T10-D-AL3 ~]$ sudo firewall-cmd --permanent --add-service=cockpit
```

```
[cditto@T10-D-AL3 ~]$ sudo firewall-cmd --reload
```

Install Cockpit



Install Cockpit

Cancel **New Profile** Add

Identity **IPv4** IPv6 Security

IPv4 Method

☐ Automatic (DHCP) ☐ Link-Local Only

☒ Manual ☐ Disable

Addresses

Address	Netmask	Gateway	
192.168.201.5	255.255.255.0	192.168.201.1	✕
			✕

DNS Automatic ☐ OFF

192.168.201.4

Separate IP addresses with commas



Routes Automatic ☒ ON

Address	Netmask	Gateway	Metric	
				✕



Forever-Fi x **m** Firefox Privacy Not

Q https://192.168.201.5:9090

🌐 https://192.168.201.5:9090/ —

This time, search with:  

Install Cockpit



https://192.168.201.5:9090

tation [Blog](#) [Bug tracker](#) [GitHub organization](#)

AlmaLinux

User name

Password

[Other options](#)

[Log in](#)

Server: T10-D-AL3.localdomain
Log in with your server user account.

Web console is running in limited access mode. [Turn on administrative access](#)

T10-D-AL3.localdomain running AlmaLinux 8.9 (Midnight Oncilla)

Configuration

Hostname	T10-D-AL3.localdomain edit
System time	Feb 16, 2024, 7:23 PM
Domain	Join domain
Performance profile	virtual-guest
Cryptographic policy	Default
Secure shell keys	Show fingerprints

Install Cockpit

Join a domain

Domain address	<input type="text" value="T10.local"/>
Domain administrator name	<input type="text" value="Administrator"/>
Domain administrator password	<input type="password" value="••••••••••"/>

Configuration

Hostname	T10-D-AL3.localdomain
System time	Feb 16, 2024, 7:26 PM
Domain	T10.local
Performance profile	virtual-guest
Cryptographic policy	Default
Secure shell keys	Show fingerprints

Install Cockpit



Active Directory Installation






**Deploy an authoritative DNS
server that resolves
“localdomain” hostnames**



Previous to this assignment the an installation of the Unbound proxy server was installed. To view the details of that installation please see M02 Task: Proxy services.



Check info on T10-D-AL2 Unbound proxy service

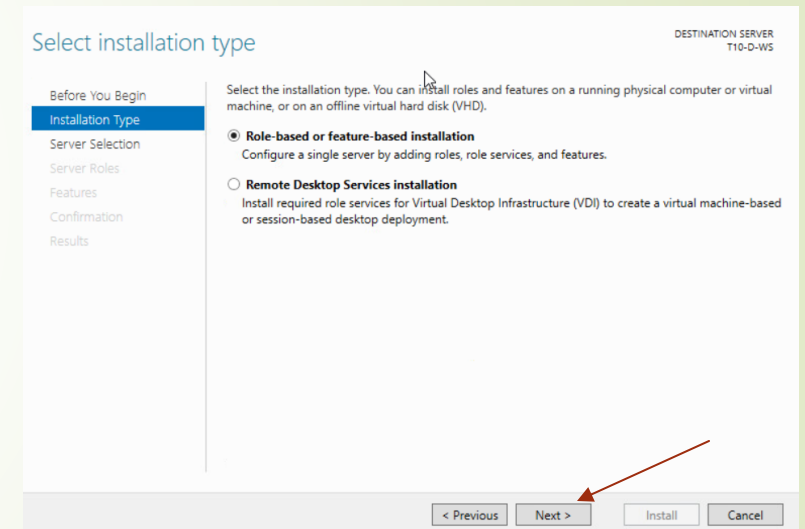
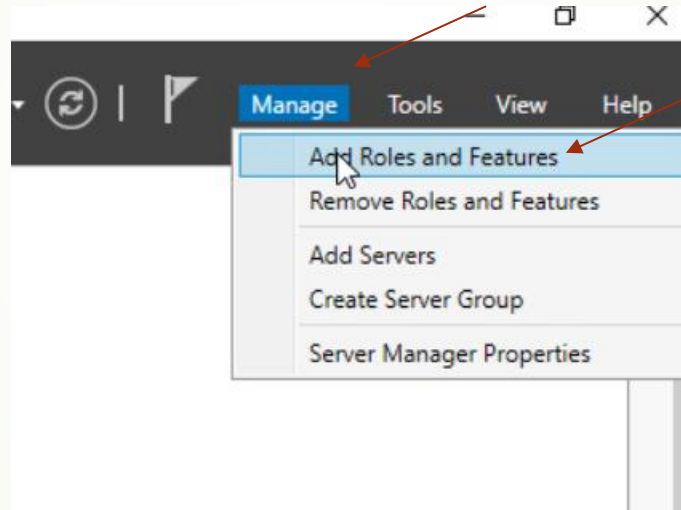
```
[cuditto@T10-D-AL2 ~]$ sudo dnf info unbound
Last metadata expiration check: 0:05:05 ago on Mon 12 Feb 2024 12:43:34 PM CST.
Installed Packages
Name           : unbound
Version        : 1.16.2
Release        : 5.el8
Architecture   : x86_64
Size           : 5.9 M
Source         : unbound-1.16.2-5.el8.src.rpm
Repository     : @System
From repo      : appstream
Summary        : Validating, recursive, and caching DNS(SEC) resolver
URL            : https://www.unbound.net/
License        : BSD
Description    : Unbound is a validating, recursive, and caching DNS(SEC)
                  : resolver.
                  :
                  : The C implementation of Unbound is developed and maintained by
                  : NLnet Labs. It is based on ideas and algorithms taken from a java
                  : prototype developed by Verisign labs, Nominet, Kirei and ep.net.
                  :
                  : Unbound is designed as a set of modular components, so that also
                  : DNSSEC (secure DNS) validation and stub-resolvers (that do not
                  : run as a server, but are linked into an application) are easily
                  : possible.
```


Check Unbound Status

```
[cditto@T10-D-AL2 ~]$ sudo systemctl status unbound
[sudo] password for cditto: 
● unbound.service - Unbound recursive Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/unbound.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-02-06 18:12:48 CST; 5 days ago
     Process: 1111 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_UNBOUND_ANCHOR" == "yes" ]; then /usr/sbin/unbound-anchor -a /var/lib/unbound/root.key -c /etc
     Process: 1086 ExecStartPre=/usr/sbin/unbound-checkconf (Code=exited, status=0/SUCCESS)
    Main PID: 1115 (unbound)
      Tasks: 4 (limit: 23499)
     Memory: 12.8M
    CGroup: /system.slice/unbound.service
            └─1115 /usr/sbin/unbound -d

Feb 06 18:12:49 T10-D-AL2.localdomain unbound[1115]: [1115:0] notice: init module 1: validator
Feb 06 18:12:49 T10-D-AL2.localdomain unbound[1115]: [1115:0] notice: init module 2: iterator
Feb 06 18:12:49 T10-D-AL2.localdomain unbound[1115]: [1115:0] info: start of service (unbound 1.16.2).
Feb 06 19:27:00 T10-D-AL2.localdomain unbound[1115]: [1115:1] info: generate keytag query _ta-4f66. NULL IN
Feb 07 07:05:41 T10-D-AL2.localdomain unbound[1115]: [1115:1] info: generate keytag query _ta-4f66. NULL IN
Feb 08 06:26:14 T10-D-AL2.localdomain unbound[1115]: [1115:0] info: generate keytag query _ta-4f66. NULL IN
Feb 09 06:11:46 T10-D-AL2.localdomain unbound[1115]: [1115:0] info: generate keytag query _ta-4f66. NULL IN
Feb 10 06:00:51 T10-D-AL2.localdomain unbound[1115]: [1115:0] info: generate keytag query _ta-4f66. NULL IN
Feb 11 04:07:16 T10-D-AL2.localdomain unbound[1115]: [1115:0] info: generate keytag query _ta-4f66. NULL IN
Feb 12 03:09:50 T10-D-AL2.localdomain unbound[1115]: [1115:0] info: generate keytag query _ta-4f66. NULL IN
lines 1-21/21 (END)
```

Install & Configure DHCP



Install & Configure DHCP

DESTINATION SERVER
T10-D-WS

Select destination server

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
T10-D-WS	192.168.201.2	Microsoft Windows Server 2022 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous **Next >** Install Cancel

Install & Configure DHCP

Select server roles

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

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

Description

Dynamic Host Configuration Protocol (DHCP) Server enables you to centrally configure, manage, and provide temporary IP addresses and related information for client computers.

DESTINATION SERVER
T10-D-WS

Add Roles and Features Wizard

Add features that are required for DHCP Server?

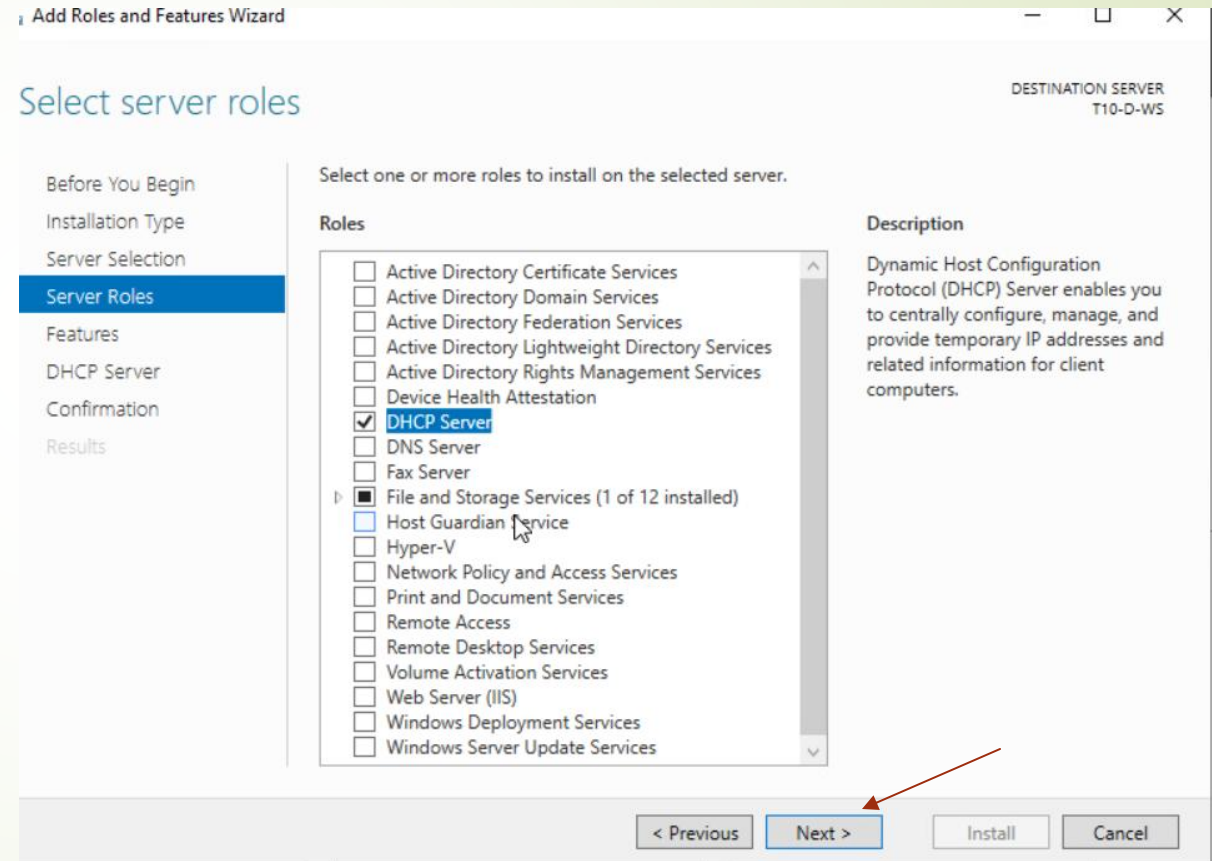
The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
 - Role Administration Tools
 - [Tools] DHCP Server Tools

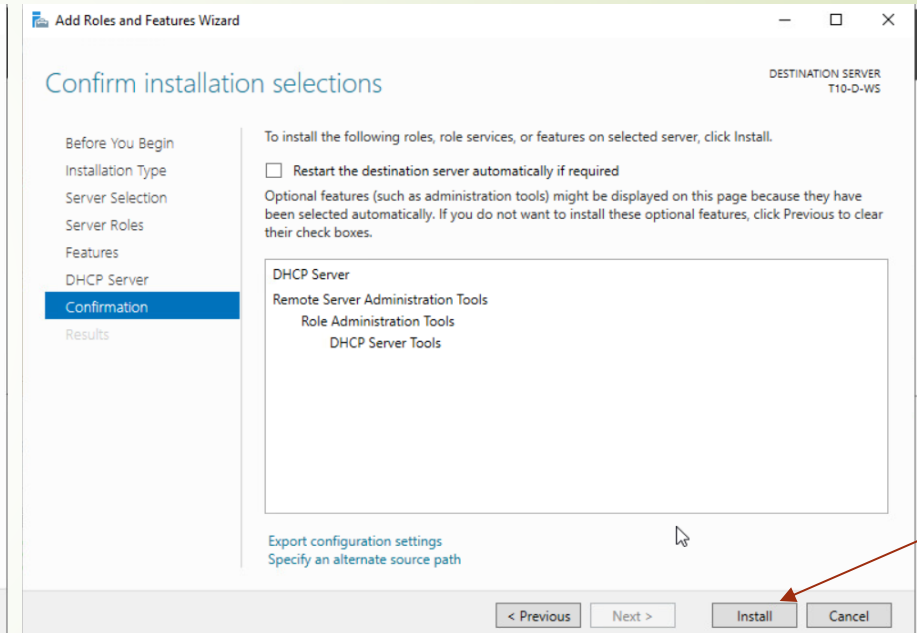
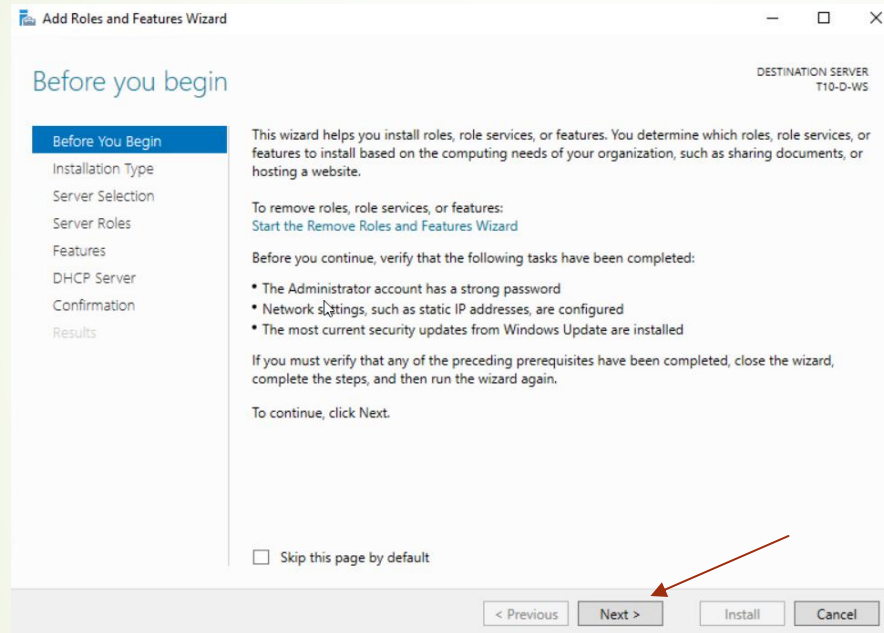
☒ Include management tools (if applicable)

Add Features Cancel

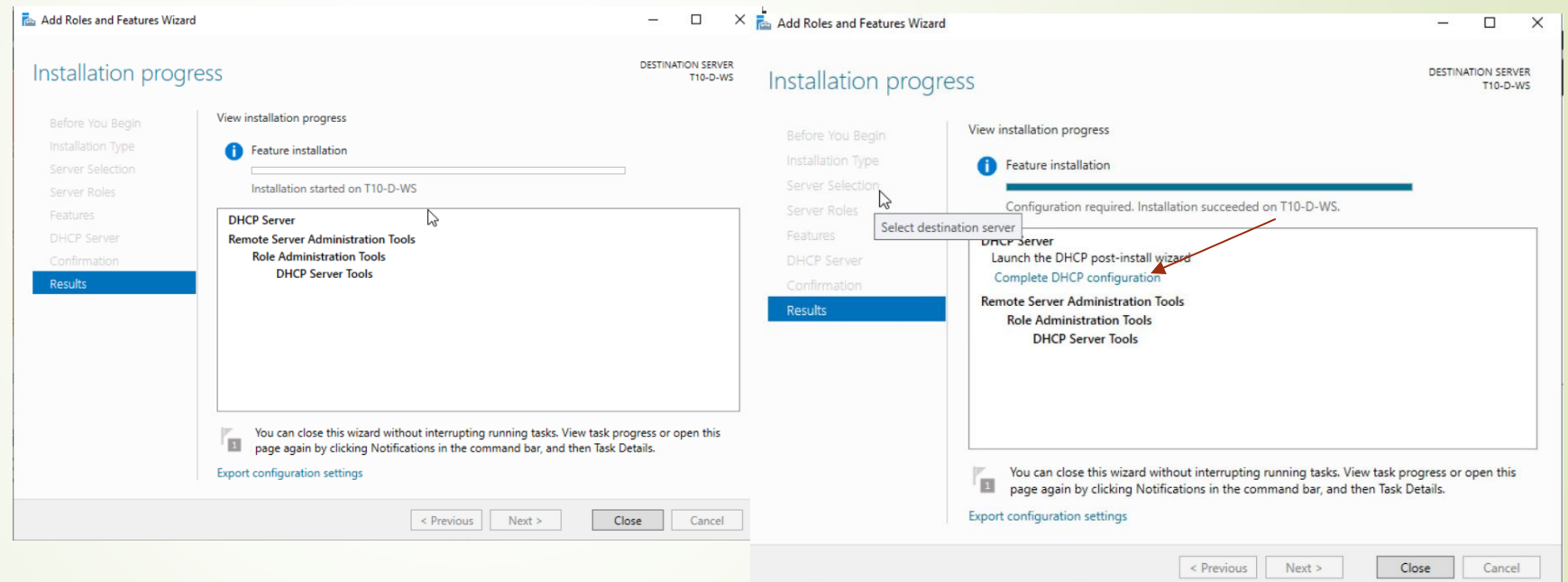
Install & Configure DHCP



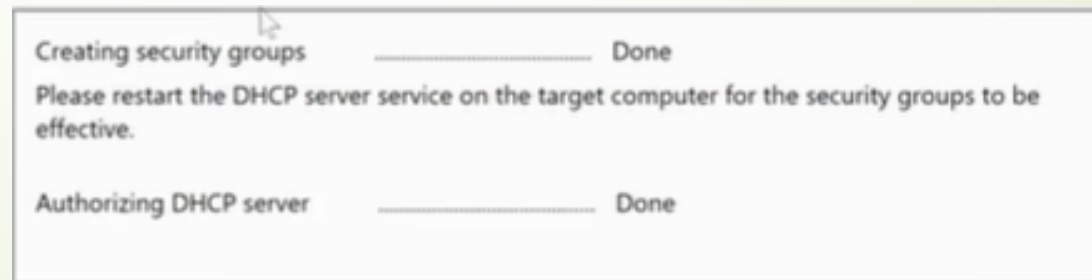
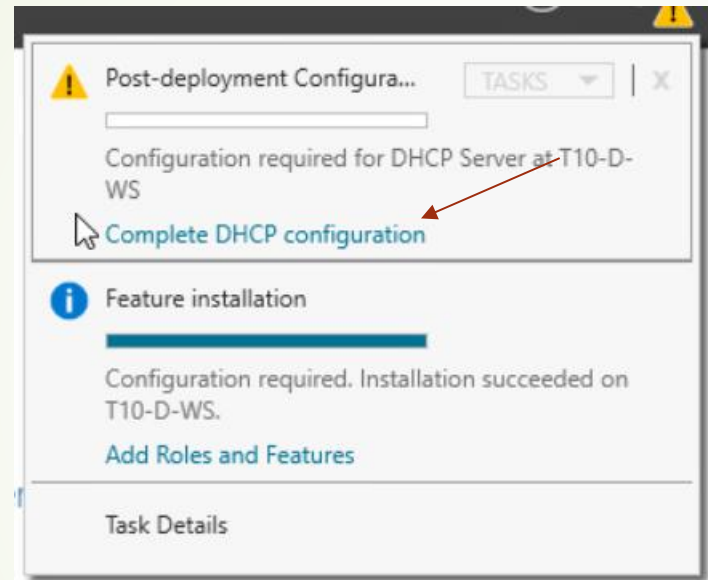
Install & Configure DHCP



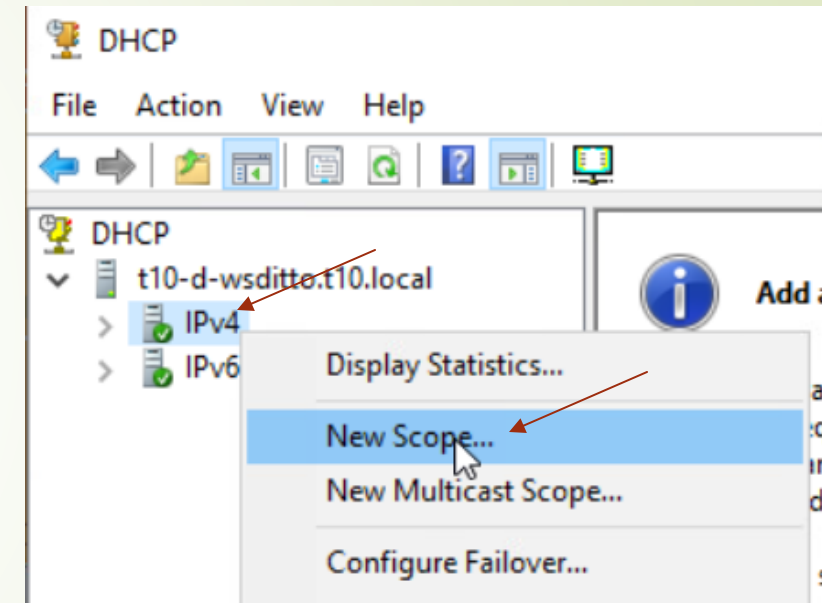
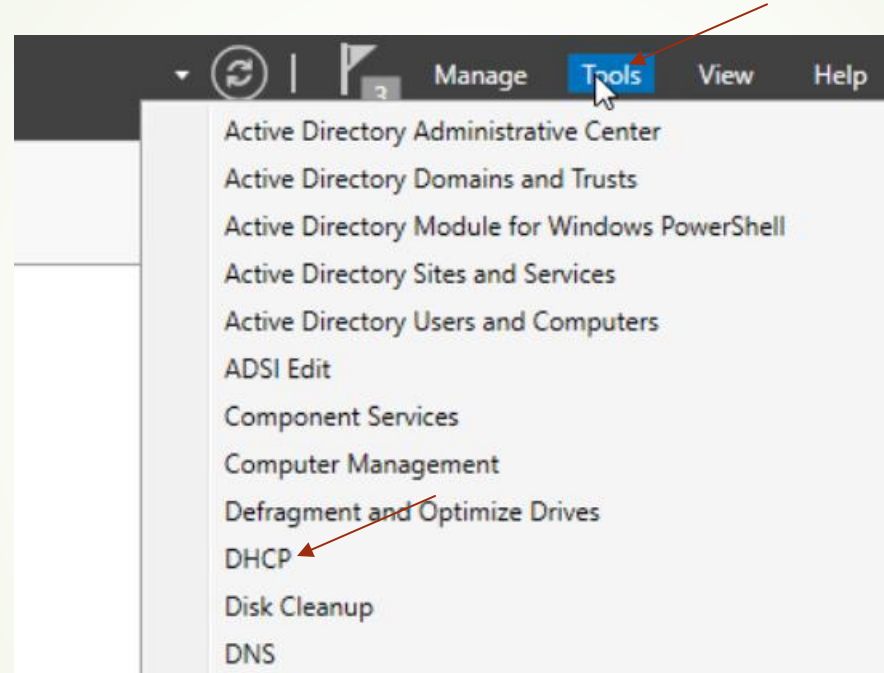
Install & Configure DHCP



Install & Configure DHCP




Install & Configure DHCP



Install & Configure DHCP

New Scope Wizard



Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

< Back **Next >** Cancel

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back **Next >** Cancel

Install & Configure DHCP

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 201 . 100

End IP address: 192 . 168 . 201 . 200

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

New Scope Wizard

Add Exclusions and Delay
Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . . End IP address: . . . Add

Excluded address range: Remove

Subnet delay in milli second: 0

< Back Next > Cancel

Install & Configure DHCP

New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back **Next >** Cancel

New Scope Wizard

Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.


Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now

☐ No, I will configure these options later

< Back **Next >** Cancel

Install & Configure DHCP



New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name: IP address:

Install & Configure DHCP

New Scope Wizard

WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name: IP address:

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

New Scope Wizard

Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

☒ Yes, I want to activate this scope now
☐ No, I will activate this scope later

Install & Configure DHCP



Install & Configure DHCP



Install & Configure DHCP



Install & Configure DHCP

