Lab 3

DEPLOYING AND CONFIGURING DHCP AND DNS SERVICES

EXERCISE 1: PLANNING IP ADDRESSES FOR THE NETWORK

In this exercise, you are responsible for subnetting a network to suit a particular network organization plan. To complete this exercise, you must determine what IPv4 addresses you should use on the networks for which you are responsible.

With the assigned Ipv4 block, the student are requested to make a plan for its usage, in particular.

- IPv4 Network:
- Subnet Mask:
- Gateway:
- IP address for Servers: DC1, DC2, Web, VPN, DNS, DHCP, File, …
- IP address for special devices: Printer, scanner, switch, routers,..
- IP range for DHCP
- Reservation IP

EXERCISE 2: MANUALLY CONFIGURING TCP/IP

In this exercise, you configure the IP addresses and other TCP/IP configuration parameters for your computers

	DC1	DC2	Win 10 Workstation
IP Address			
Subnet Mask			
Preferred DNS Server			

After manually configuring the three servers' TCP/IP clients, you must test them by trying to connect to the other servers on the network.

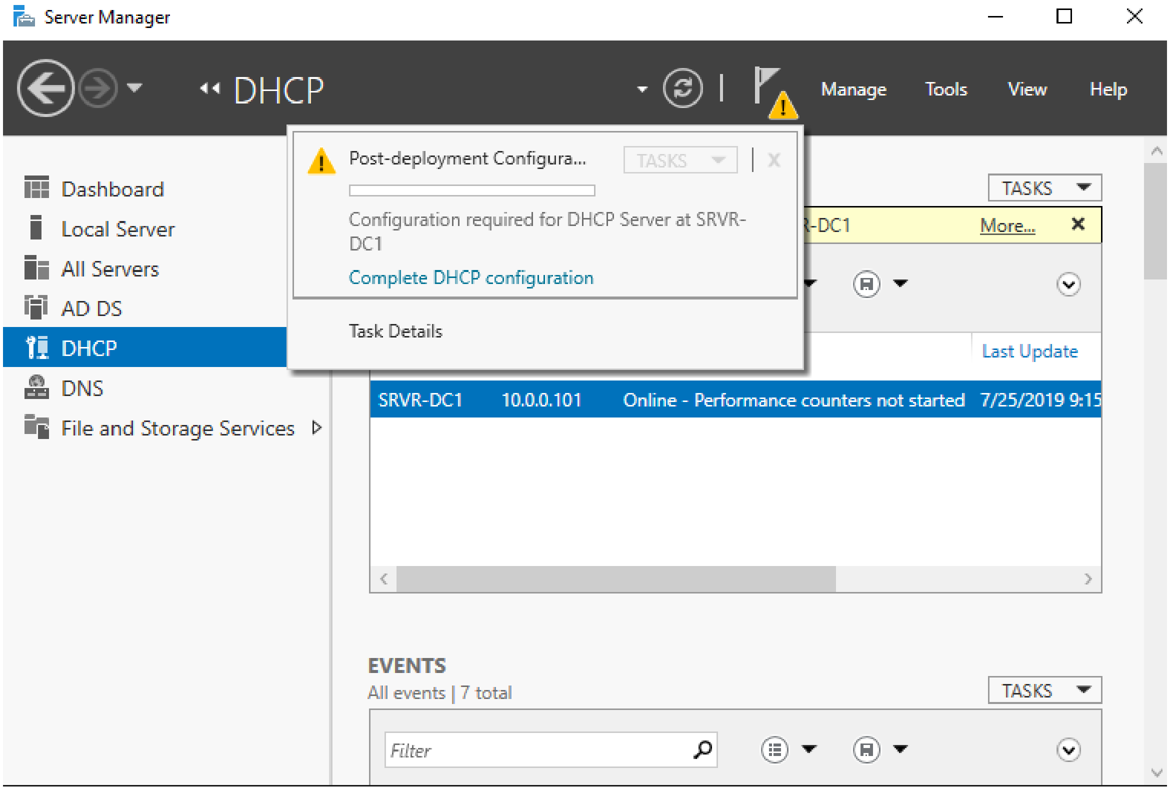
EXERCISE 3: INSTALLING DHCP SERVER ROLE

1. Log on to the DC1 computer
2. In **Server Manager**, click **Manage** and then click **Add Roles And Features**.
3. In the **Add Roles And Features** wizard, on the **Before You Begin** page, click **Next**.
4. On the **Select Installation Type** page and **Select Destination Server** page, click Next.
5. On the **Select Server Roles** page, in the Roles list, select the **DHCP Server** check box.
6. In the Add Features That Are Required For DHCP Server dialog box, click Add Features, and then click Next.
7. On the Select Features page, click Next.

8. On the DHCP Server page, click Next.
9. On the Confirm Installation Selections page, click Install. When the role is installed, click Close.

Complete installation and authorize a DHCP server

10. Click **Notifications**, and then click **Complete DHCP configuration**



Post-deployment Configura...

Configuration required for DHCP Server at SRVR-DC1

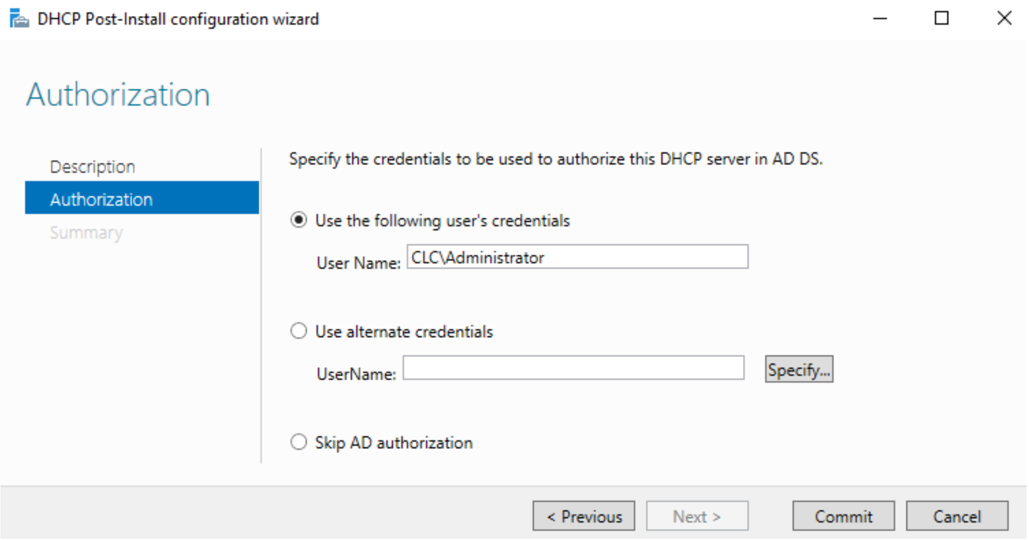
Complete DHCP configuration

Task Details

SRVR-DC1	10.0.0.101	Online - Performance counters not started	7/25/2019 9:15

11. In the **DHCP Post-Install Configuration** wizard, on the Description page, click Next.

12. On the Authorization page, specify the credentials required to authorize the server in AD DS. The account you use should be a member of the **Domain Admins** Global security group. Click **Commit** to complete authorization and create the required security groups.



DHCP Post-Install configuration wizard

Authorization

Specify the credentials to be used to authorize this DHCP server in AD DS.

● Use the following user's credentials

User Name: CLC\Administrator

○ Use alternate credentials

UserName:

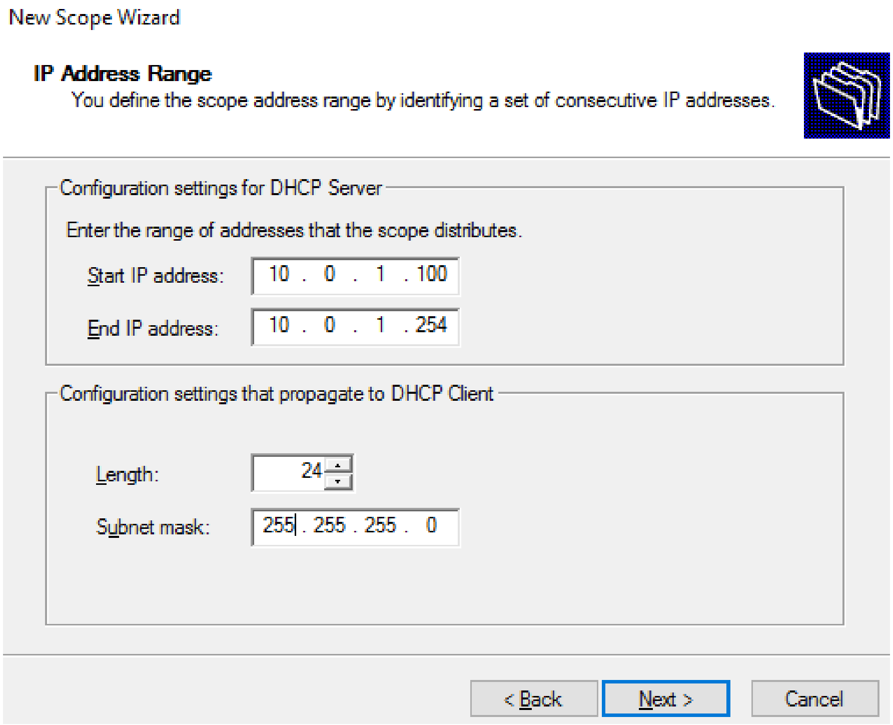
○ Skip AD authorization

EXERCISE 4: CREATING A DHCPV4 SCOPE

A scope is a range of IP addresses that a DHCP server uses to supply clients on a particular subnet with IP addresses. It also contain related information that is used to configure your network clients.

To create a DHCP IPv4 scope using the DHCP console, use the following procedure:

1. In the DHCP console, expand the DHCP server, right-click IPv4, and then click New Scope.
2. In the New Scope Wizard, on the Welcome to the New Scope Wizard page, click Next.
3. On the Scope Name page, provide a name and description for your scope. These should be meaningful. Click Next.
4. On the IP Address Range page, in the Start IP address box, type the first valid IPv4 address in your scope. In the End IP Address box, type the last valid IP address in your scope. In the Length list, click the number of bits in the subnet mask.


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: 10 . 0 . 1 . 100

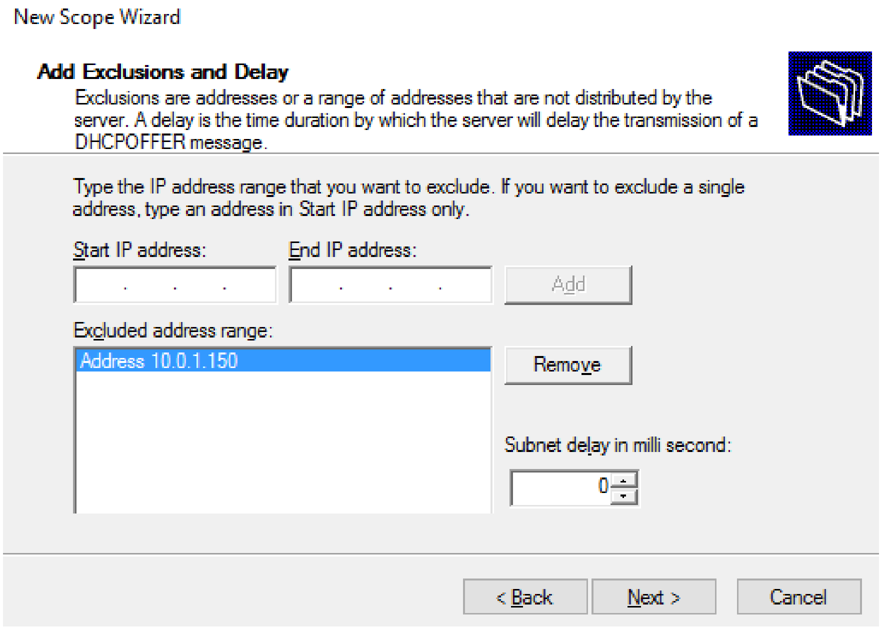
End IP address: 10 . 0 . 1 . 254

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

5. On the Add Exclusions and Delay page, in the Start IP Address and End IP address fields, type any ranges of IP addresses that you wish to exclude from the allocation pool and click Add. You can exclude individual IP addresses if you want.
6. In the Subnet Delay box, enter a value to delay allocation of DHCPOFFER messages to your client computers. Usually, this value is not used. Click Next.


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 DHCPOFFER 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: . . .

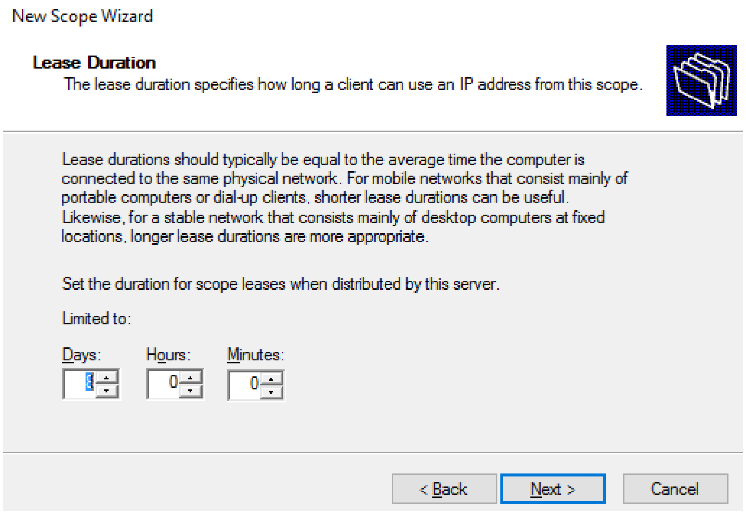
Excluded address range:

Address 10.0.1.150

Subnet delay in milli second: 0

7. On the Lease Duration page, enter the value of the lease period. This is the period that DHCP clients continue to use their allocated IP address before they must renew or release it. The default is eight days. Use a shorter interval for scopes that have limited

address capacity, or when clients frequently move between subnets and scopes. Click Next.



New Scope Wizard

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

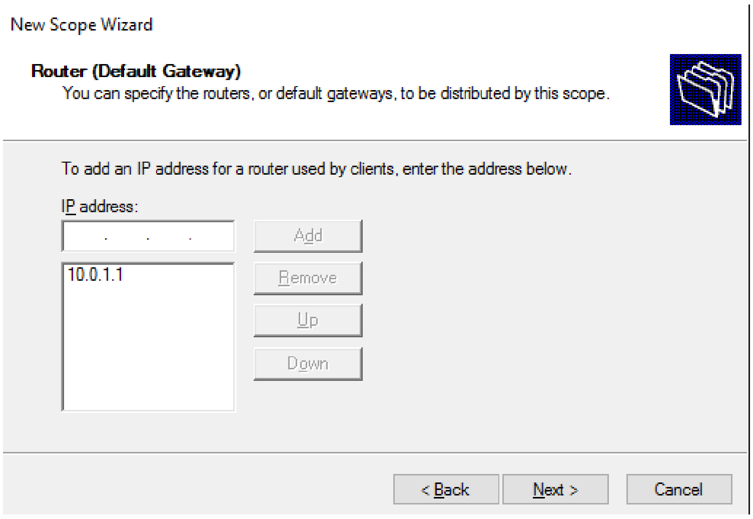
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop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

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

Limited to:

Days: 8 Hours: 0 Minutes: 0

8. On the Configure DHCP Options, click Yes, I Want To Configure These Options Now, and then click Next. You can reconfigure these options later in the DHCP console.
9. On the Router (Default Gateway) page, in the IP address box, type the IP address of the default gateway that will service clients in this scope and click Add. You can configure multiple gateways and order them in the list. Click Next.



New Scope Wizard

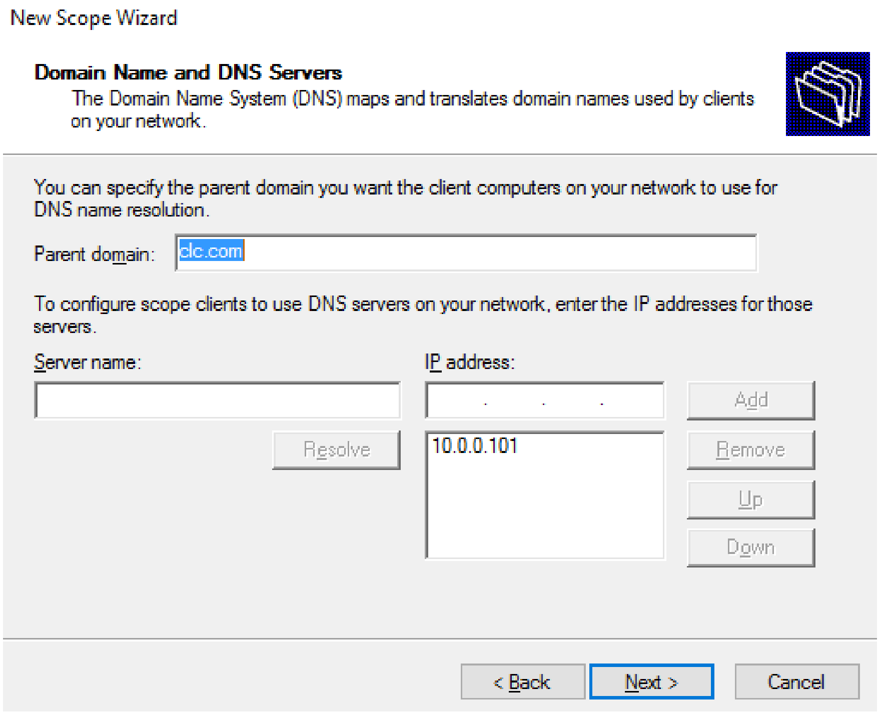
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

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

IP address:

10.0.1.1

10. On the Domain Name and DNS Servers page, in the Server Name box, type the fully qualified domain name (FQDN) or IP address of the primary DNS server for clients in this scope, click Add, and then click Next.



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: clc.com

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

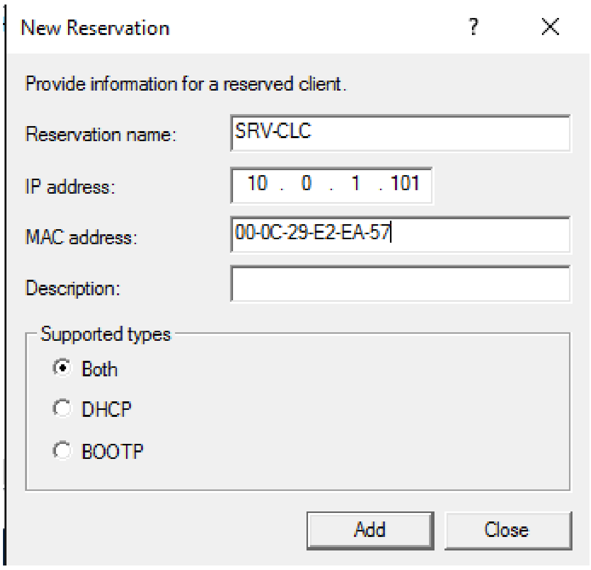
Server name:

IP address: 10.0.0.101

11. On the WINS Server page, if you use NetBIOS-based apps and do not use a GlobalNames zone for single-label name resolution, enter the IP address of one or more WINS servers and then click Next.
12. Finally, on the Activate Scope page, if you are ready to allow clients to obtain IP configurations from the scope, click Yes, I Want To Activate This Scope Now, and click Next. You can activate the scope later from the DHCP console. Click Finish.

Configure a DHCP reservation

13. To add a reservation, from the DHCP console, select the appropriate scope, right-click the Reservations node and then click New Reservation.



New Reservation

Provide information for a reserved client.

Reservation name: SRV-CLC

IP address: 10 . 0 . 1 . 101

MAC address: 00-0C-29-E2-EA-57

Description:

Supported types

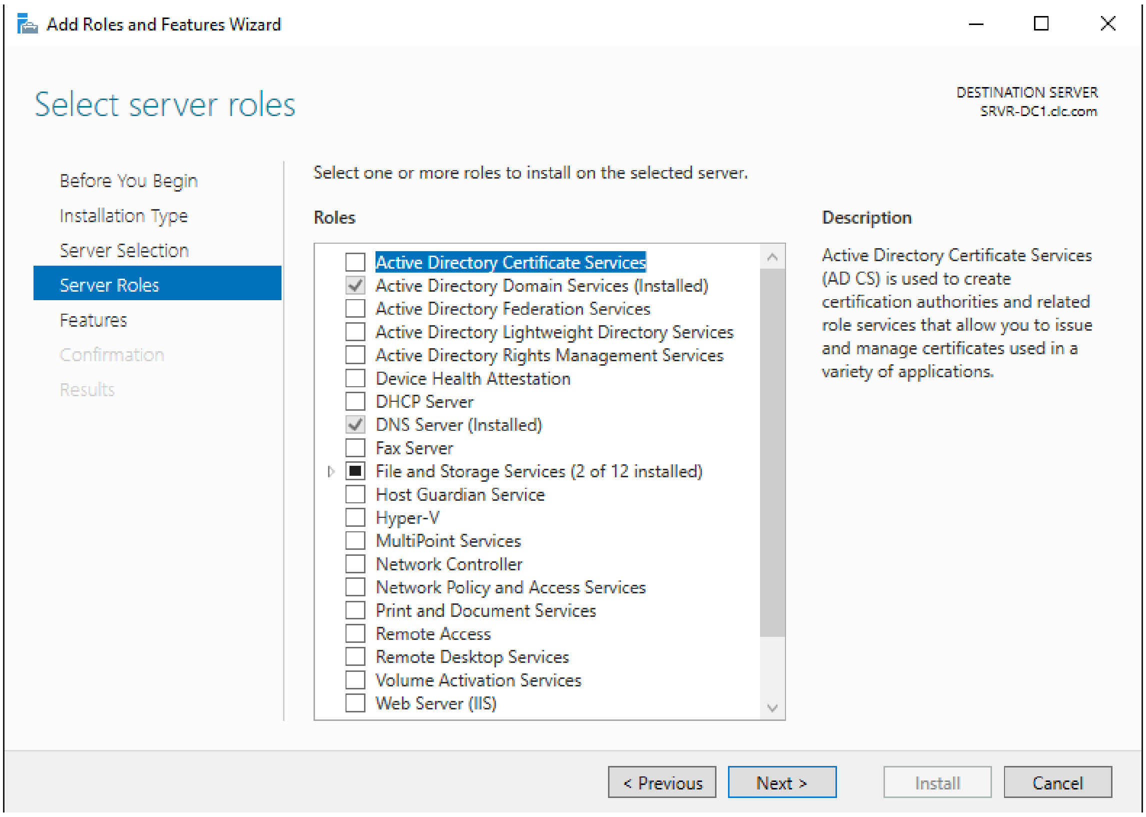
● Both
○ DHCP
○ BOOTP

Challenge:

- Confirming that DHCP work: demonstrate that a computer can automatically obtain IP from DHCP.
  Hint: Installing Windows 10 and configuring it to use DHCP for obtaining IP address
- Creating a DHCPv6 Scope
- What is DHCP superscope? Installing and configuring a superscope
- What is DHCP Relay agent?

EXERCISE 5: INSTALL AND CONFIGURE DNS SERVERS

1. Sign in to the DC1 server as a local administrator.
2. In Server Manager, click Manage and then click Add Roles And Features.
3. In the Add Roles And Features Wizard’s Before You Begin page, click Next.
4. On the Select Installation Type page, click Role-Based or Feature-Based Installation, and click Next.
5. On the Select Destination Server page, select the server from the Server Pool list, and click Next.
6. In the Roles list on the Select Server Roles page, select the DNS Server



Select server roles

DESTINATION SERVER
SRVR-DC1.clc.com

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

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

7. In the Add Roles And Features Wizard pop-up dialog box, click Add Features, and then click Next.
8. On the Select features page, click Next.
9. On the DNS Server page, click Next.

10. On the Confirm Installation Selections page, click Install. When the installation is complete, click Close.

EXERCISE 6: CONFIGURE FORWARDERS, ROOT HINTS, AND RECURSION

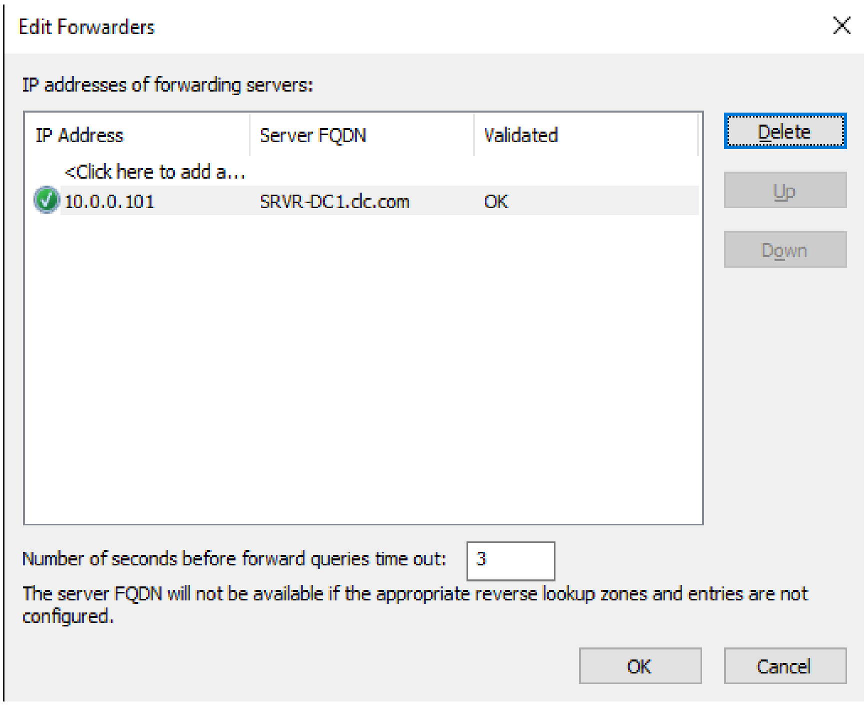
I. **Configure forwarders**: DNS forwarding enables you to define what happens to a DNS query when the petitioned DNS server is unable to resolve that DNS query.

With DNS forwarding, you can:

- Configure a DNS server only to respond to those queries that it can satisfy by reference to locally stored zone information. For all other requests, the petitioned DNS server must forward the request to another DNS server.
- Define the forwarding behavior for specific DNS domains by configuring DNS conditional forwarding. In this scenario, if the DNS query contains a specific domain name, for example Contoso.com, then it is forwarded to a specific DNS server.

To configure forwarding, use the following procedure:

1. In **Server Manager**, click **Tools**, and then click **DNS**.
2. In **DNS Manager**, right-click the **DNS server** in the navigation pane and click **Properties**.
3. In the Server Properties dialog box, on the **Forwarders** tab, click Edit.
4. In the IP Address list located in the Edit Forwarders dialog box, enter the IP address of the server to which you want to forward all DNS queries, and then click OK. You can configure several DNS servers here; those servers are petitioned in preference order. You can also set a timeout value, in seconds, after which the query is timed out



IP addresses of forwarding servers:

IP Address	Server FQDN	Validated
<Click here to add a...		
✓ 10.0.0.101	SRVR-DC1.dc.com	OK

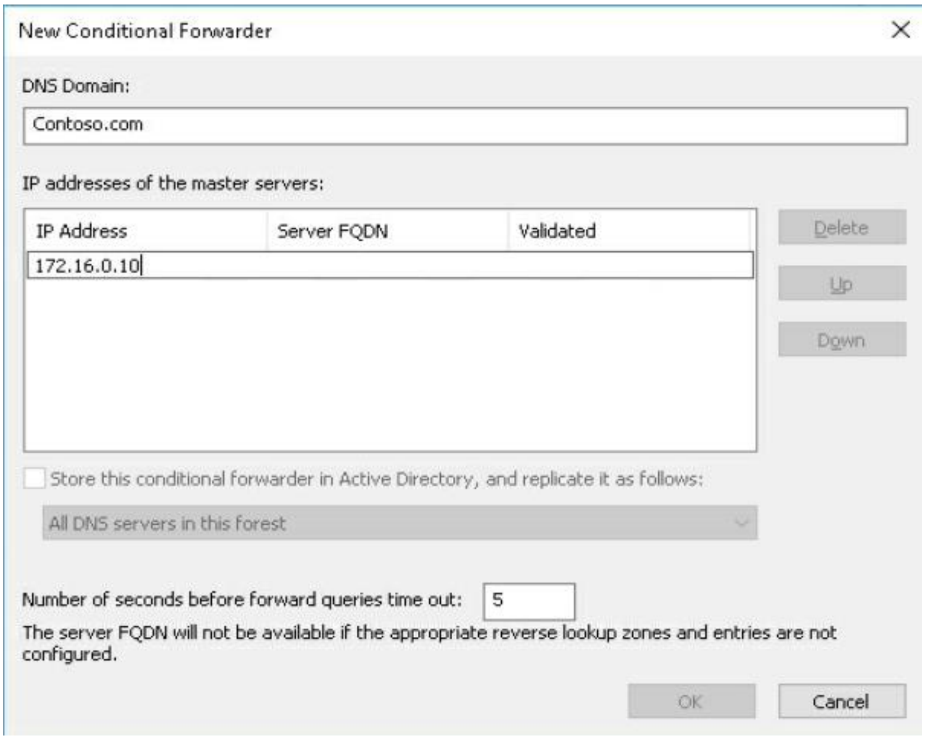
Number of seconds before forward queries time out: 3

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

5. In the Server Properties dialog box on the Forwarders tab you can view and edit the list of DNS forwarders. You can also determine what happens when no DNS forwarders can be contacted. By default, when forwarders cannot be contacted, root hints are used. Root hints are discussed in the next section. Click OK to complete configuration.

To enable and configure conditional forwarding, use the following procedure:

1. In DNS Manager, right-click the Conditional Forwarders node in the navigation pane, and then click New Conditional Forwarder.
2. On the New Conditional Forwarder dialog box, in the DNS Domain box, type the domain name for which you want to create a conditional forward. Next, in the IP address of the master servers list, enter the IP address of the server to use as a forwarder for this domain; press Enter.



New Conditional Forwarder

DNS Domain: Contoso.com

IP addresses of the master servers:

IP Address	Server FQDN	Validated
172.16.0.10		

□ Store this conditional forwarder in Active Directory, and replicate it as follows:

All DNS servers in this forest

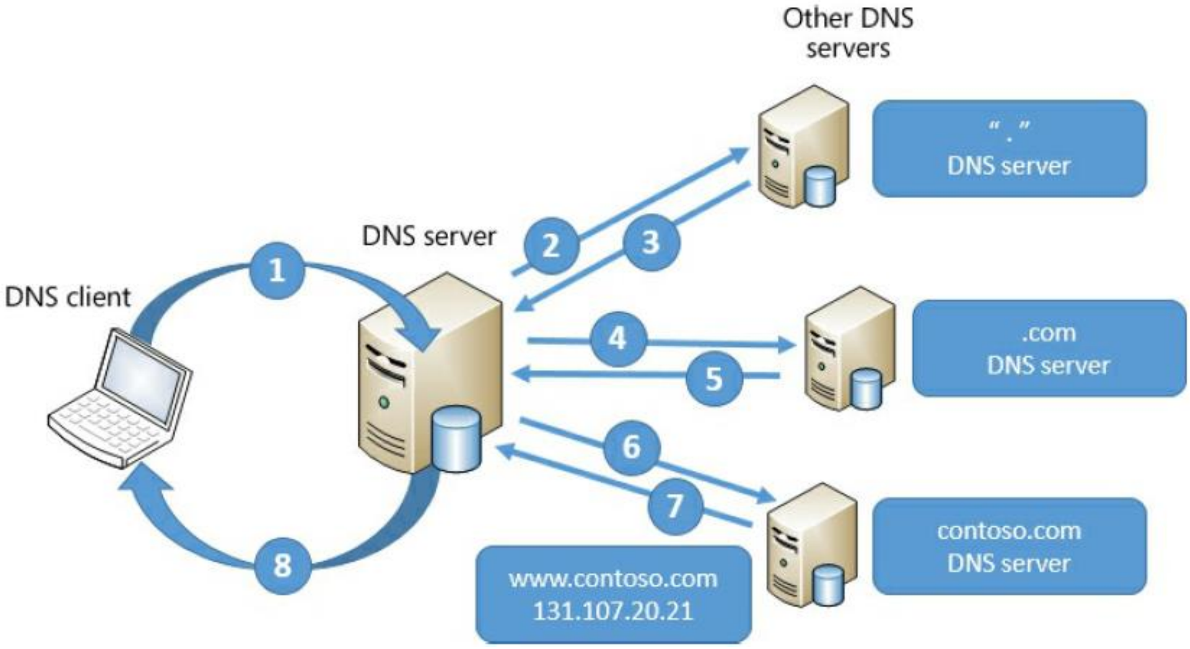
Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

3. Optionally, specify the Number of Seconds Before Forward Queries Time Out value. The default value is 5 seconds.
4. Click OK

II. Configure root hints

If you do not specify DNS forwarding, then when a petitioned DNS server is unable to satisfy a DNS query, it uses root hints to determine how to resolve it.



How Internet DNS queries work

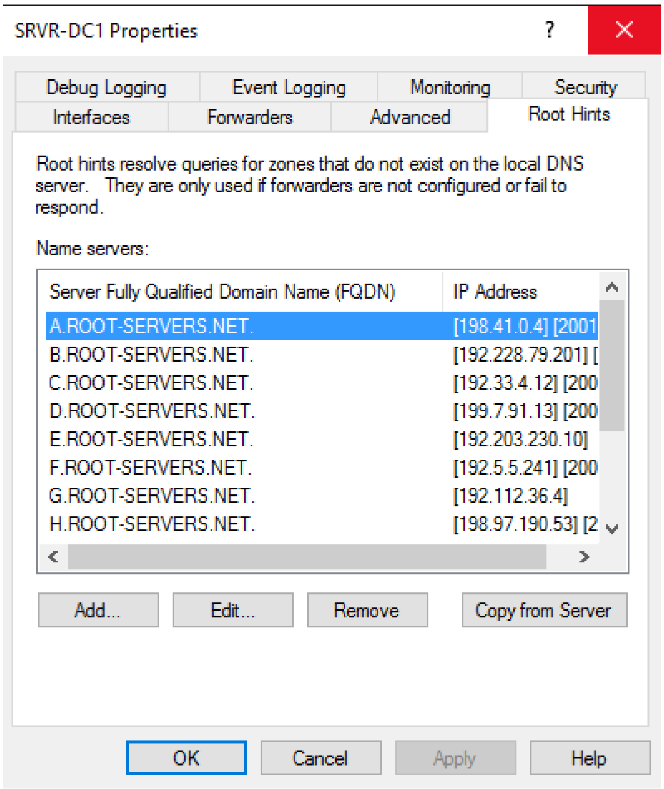
If a DNS server is not authoritative and holds no cache for that DNS domain, it petitions a root server to start the process of determining which server is authoritative for the petitioned record. However, without the IP address of the root name servers, this process cannot begin.

Root hints are used by DNS servers to enable them to navigate the DNS hierarchy on the Internet, starting at the root. Microsoft DNS servers are preconfigured with the relevant root hint records. However, you can modify the list of root hint servers by using the DNS Manager console or by using Windows PowerShell.

Editing Root Hints

To modify the root hints information using DNS Manager, use the following procedure:

1. In Server Manager, click Tools, and then click DNS.
2. In the DNS Manager console, locate the appropriate DNS server. Right-click the server and click Properties.
3. In the server Properties dialog box, click the Root Hints tab



Root hints resolve queries for zones that do not exist on the local DNS server. They are only used if forwarders are not configured or fail to respond.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
A.ROOT-SERVERS.NET.	[198.41.0.4] [2001
B.ROOT-SERVERS.NET.	[192.228.79.201] [
C.ROOT-SERVERS.NET.	[192.33.4.12] [200
D.ROOT-SERVERS.NET.	[199.7.91.13] [200
E.ROOT-SERVERS.NET.	[192.203.230.10]
F.ROOT-SERVERS.NET.	[192.5.5.241] [200
G.ROOT-SERVERS.NET.	[192.112.36.4]
H.ROOT-SERVERS.NET.	[198.97.190.53] [2

4. You can then add new records, or edit or remove any existing records. You can also click Copy From Server to import the root hints from another online DNS server. Click OK when you have finished editing root hints.

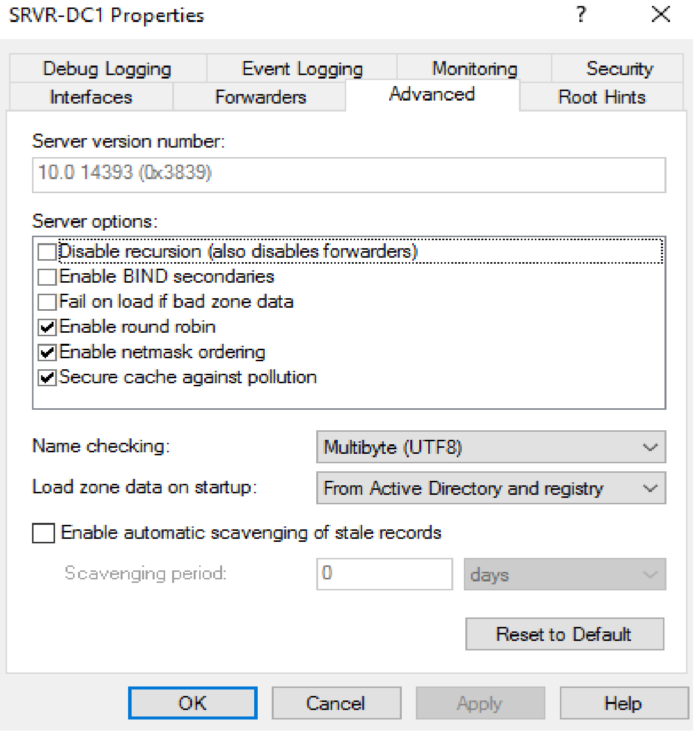
III. Configure recursion

Recursion is the name resolution process when a petitioned DNS server queries other DNS servers to resolve a DNS query on behalf of a requesting client. The petitioned server then returns the answer to the DNS client. By default, all DNS servers perform recursive queries on behalf of their DNS clients and other DNS servers that have forwarded DNS client queries to them.

However, since malicious people can use recursion as a means to attempt a denial of service attack on your DNS servers, you should consider disabling recursion on any DNS server in your network that is not intended to receive recursive queries.

To disable recursion, use the following procedure:

1. From Server Manager, click Tools, and then click DNS.
2. In the DNS Manager console, right-click the appropriate server, and then click Properties.
3. Click the Advanced tab, and then in the Server options list, select the Disable Recursion (Also Disables Forwarders) check box, and then click OK



Server version number: 10.0 14393 (0x3839)

Server options:

☐ Disable recursion (also disables forwarders)
☐ Enable BIND secondaries
☐ Fail on load if bad zone data
☑ Enable round robin
☑ Enable netmask ordering
☑ Secure cache against pollution

Name checking: Multibyte (UTF8)

Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records

Scavenging period: 0 days

EXERCISE 7: CREATE AND CONFIGURE DNS ZONES AND RECORDS

You can consider a DNS zone to be one or more domains and subdomains from your DNS infrastructure. You can store the zone in files on the DNS server or in the Active Directory Domain Services (AD DS) database. It is important that you know how and when to create primary and secondary zones, delegated zones, AD DS–integrated zones, and stub zones.

Overview of DNS zones

Zones are used by DNS servers to resolve client DNS queries. Usually, clients perform forward lookup queries in which a hostname must be resolved into the corresponding Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6) address. Forward lookup queries are resolved by reference to forward lookup zones.

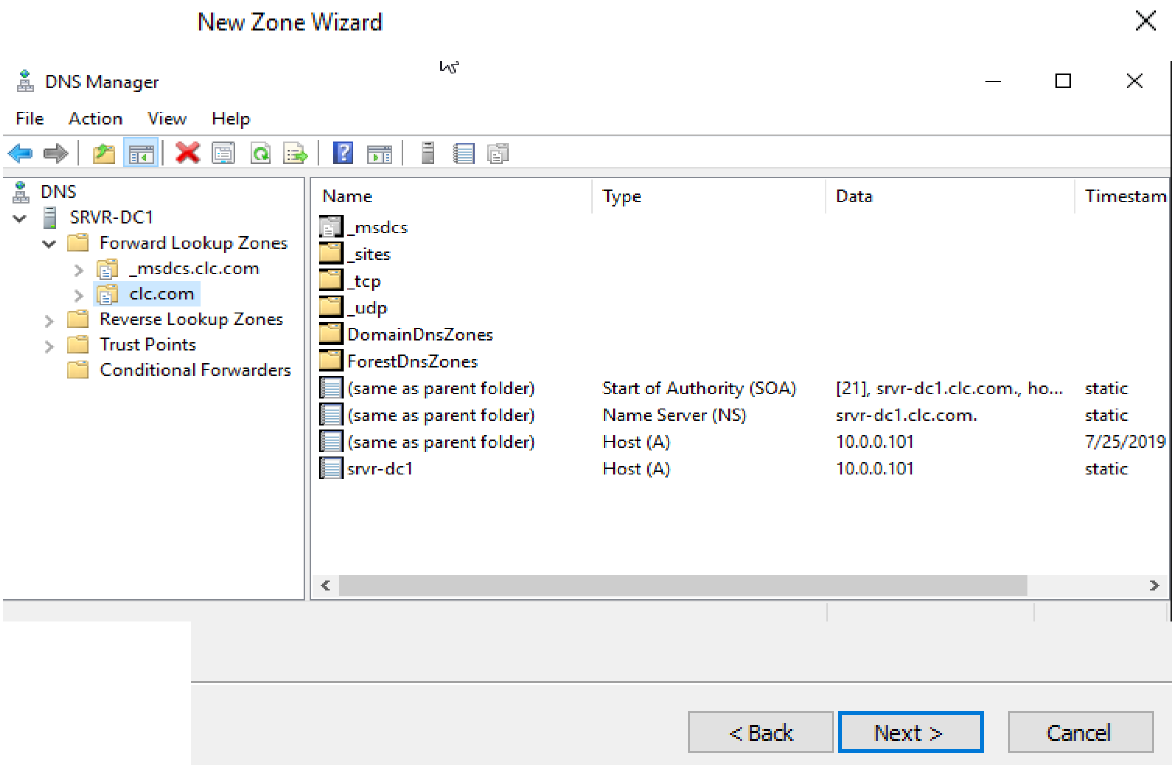
Less often, a DNS client queries a DNS server for the name of a host when it has the IPv4 or IPv6 address of the host. This is called a reverse lookup, and is satisfied by reference to a reverse lookup zone. Reverse lookup zones contain pointer (PTR) records.

Before you create your zone, you must first determine whether the zone is a forward or reverse lookup zone. Then you must determine whether the zone is primary, secondary, or AD DS–integrated

Create primary zones

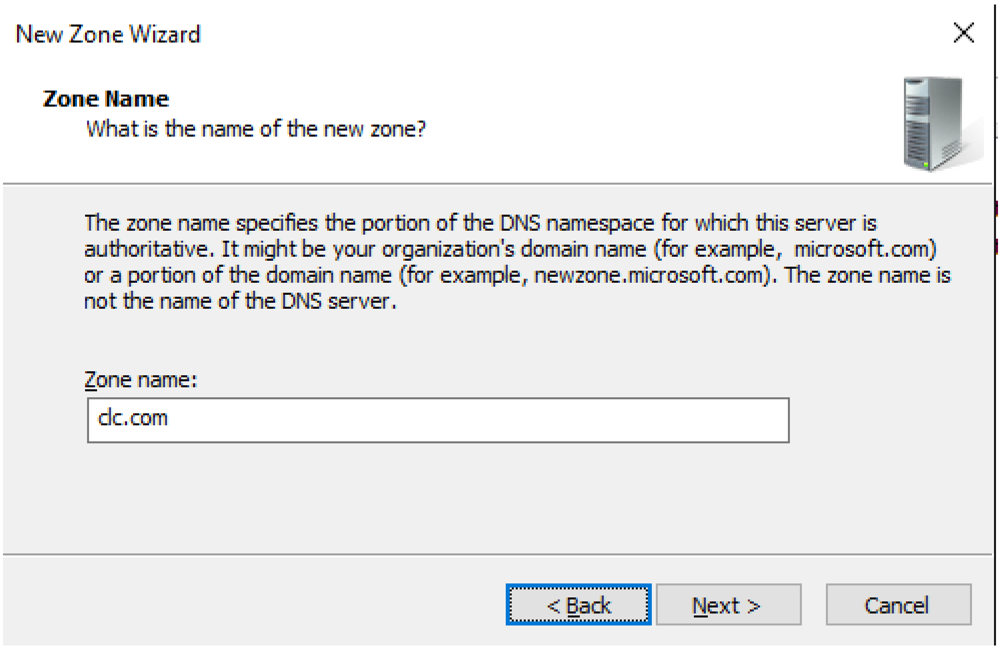
A primary zone is a writable copy of a DNS zone that exists on a DNS server. To create a primary zone, in the DNS Manager console, use the following procedure:

1. Right-click the Forward Lookup Zones node, and then click New Zone.
2. In the New Zone Wizard, on the Welcome To The New Zone Wizard page, click Next.
3. On the Zone Type page, select Primary Zone, and then click Next



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[21], srvr-dc1.clc.com., ho...	static
(same as parent folder)	Name Server (NS)	srvr-dc1.clc.com.	static
(same as parent folder)	Host (A)	10.0.0.101	7/25/2019
srvr-dc1	Host (A)	10.0.0.101	static

4. On the Zone Name page, in the Zone name box, type the zone name. For example, type clc.com. Click Next.



Zone Name

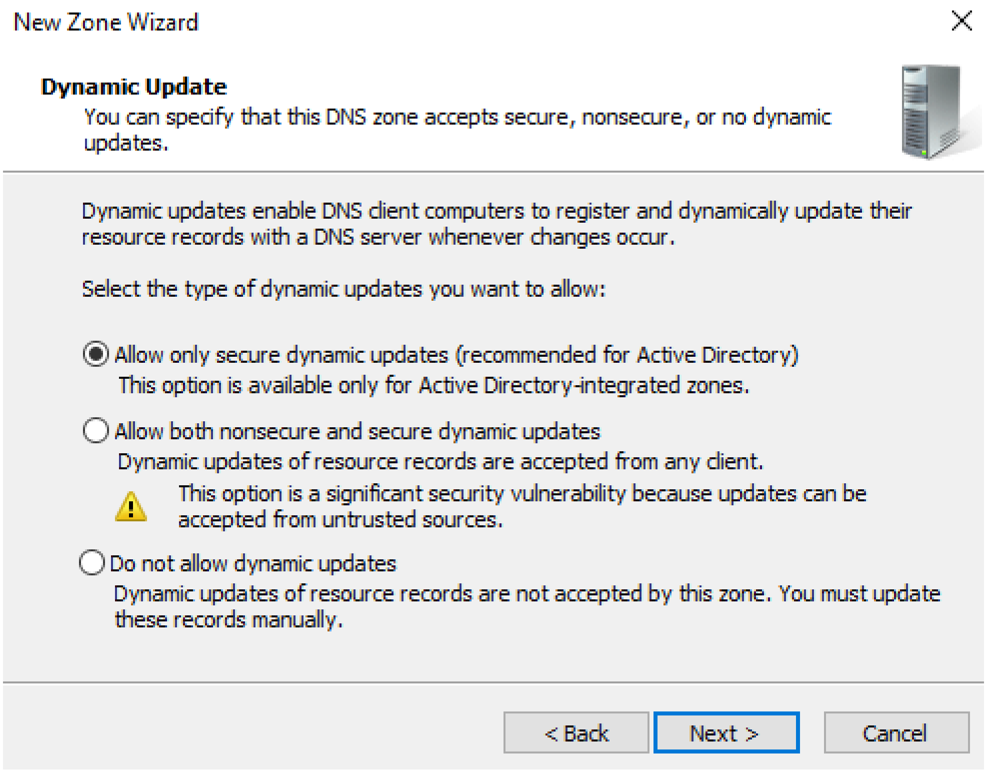
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: clc.com

5. On the Dynamic Update page, choose one of the options, and then click Next
6. On the Completing The New Zone Wizard page, click Finish.

What resource records appear in the new zone you created by default?


New Zone Wizard

Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

● Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

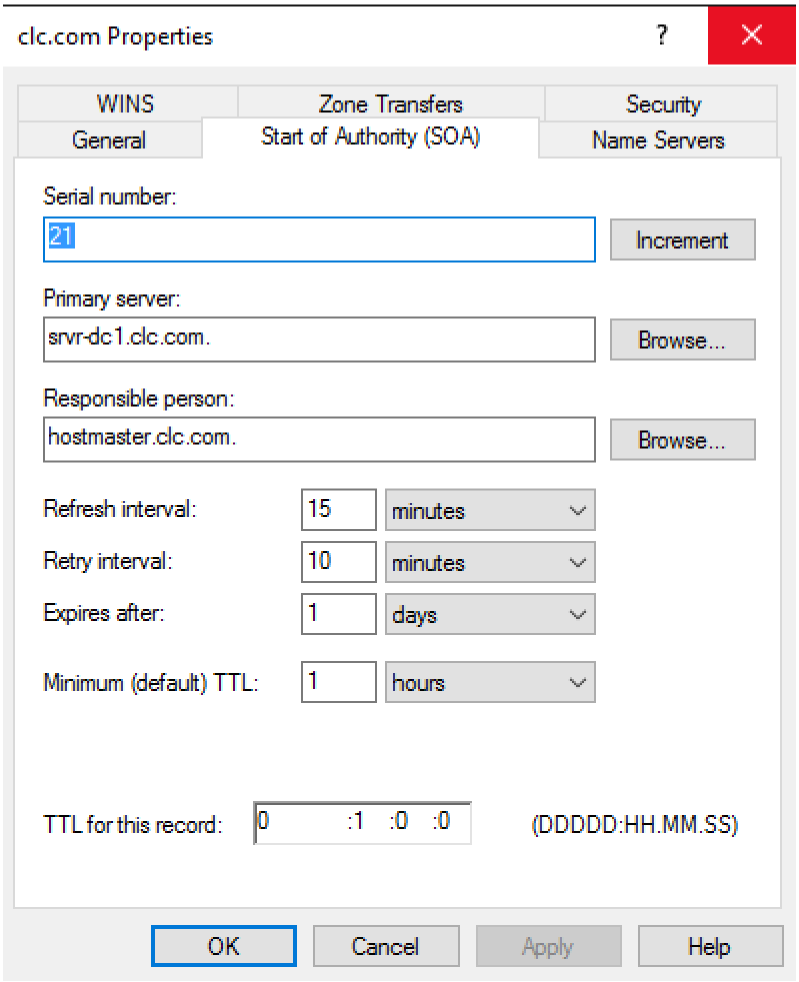
○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

○ Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

After you have created the primary zone, you can reconfigure it from the DNS Manager console by right-clicking the zone in the navigation pane and clicking Properties. You can then configure the following properties on each of the following tabs:

General: You can change the zone type, zone file name, the dynamic updates setting, and configure aging and scavenging.

Start of Authority (SOA): You can reconfigure the SOA record. This includes the Primary server’s Fully Qualified Domain Name (FQDN), the responsible person’s contact details, and the Refresh, Retry, and Expire intervals. These intervals determine:



Serial number: 21

Primary server: srvr-dc1.clc.com.

Responsible person: hostmaster.clc.com.

Refresh interval: 15 minutes

Retry interval: 10 minutes

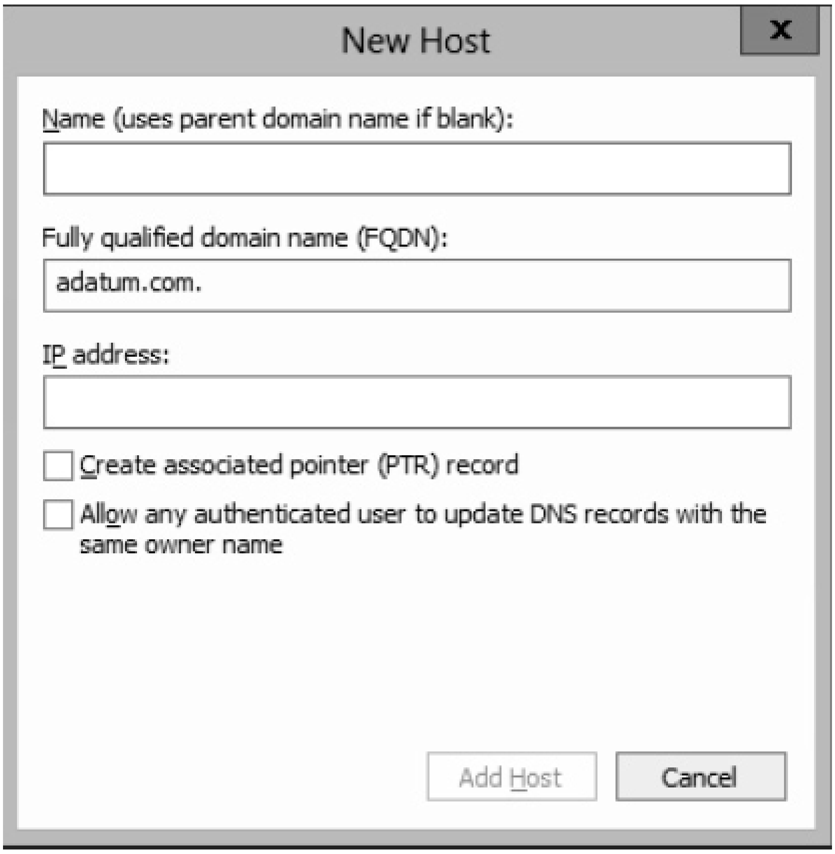
Expires after: 1 days

Minimum (default) TTL: 1 hours

TTL for this record: 0 :1 :0 :0 (DDDDD:HH.MM.SS)

EXERCISE 8. CREATING DNS RESOURCE RECORDS

1. In the DNS Manager console, expand and right-click your root domain zone (clc.com) and, from the context menu, select New Host (A or AAAA).
2. In the Name text box, type the host name of the Iweb server, e.g., Intranet.
3. In the IP Address text box, type IP of Web server, e.g., 10.0.0.102
4. Click Add Host. A DNS message box appears, stating that the resource record was created.
5. Click OK. A new, blank Add Host dialog box appears.
6. Repeat steps 2 to 4 to create Host records for other servers in your namespace design.
7. Click Done to close the Add Host dialog box



Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):
adatum.com.

IP address:

□ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

Challenges:

- Configure the DNS server to perform reverse name resolutions for all of the resource records you created in previous exercise. List the basic tasks you performed to complete the challenge and then take a screen shot of the DNS Manager console.

EXERCISE 9: MULTIHOMED SERVER AND ROUTING (optional)

- Adding a new interface for DC2 and configure it.
- Installing window 10 and configuring it to connect to the same network with that of external interface of DC2.
- Configuring Routing table to make windows 10 client to communicate with other computers