Lab Assignment & Solution

Cybersecurity Professional Program

Microsoft Security

Domain Name System

MS-03-L1
Configuring DNS

Lab Objective

Understand how to work with a Windows DNS server.

Lab Mission

Configure DNS as a primary DNS server and add records.

Lab Duration

1–1.5 hours

Requirements

- Basic knowledge of domain environments and Windows Server 2016
- Basic knowledge of CMD and networking commands

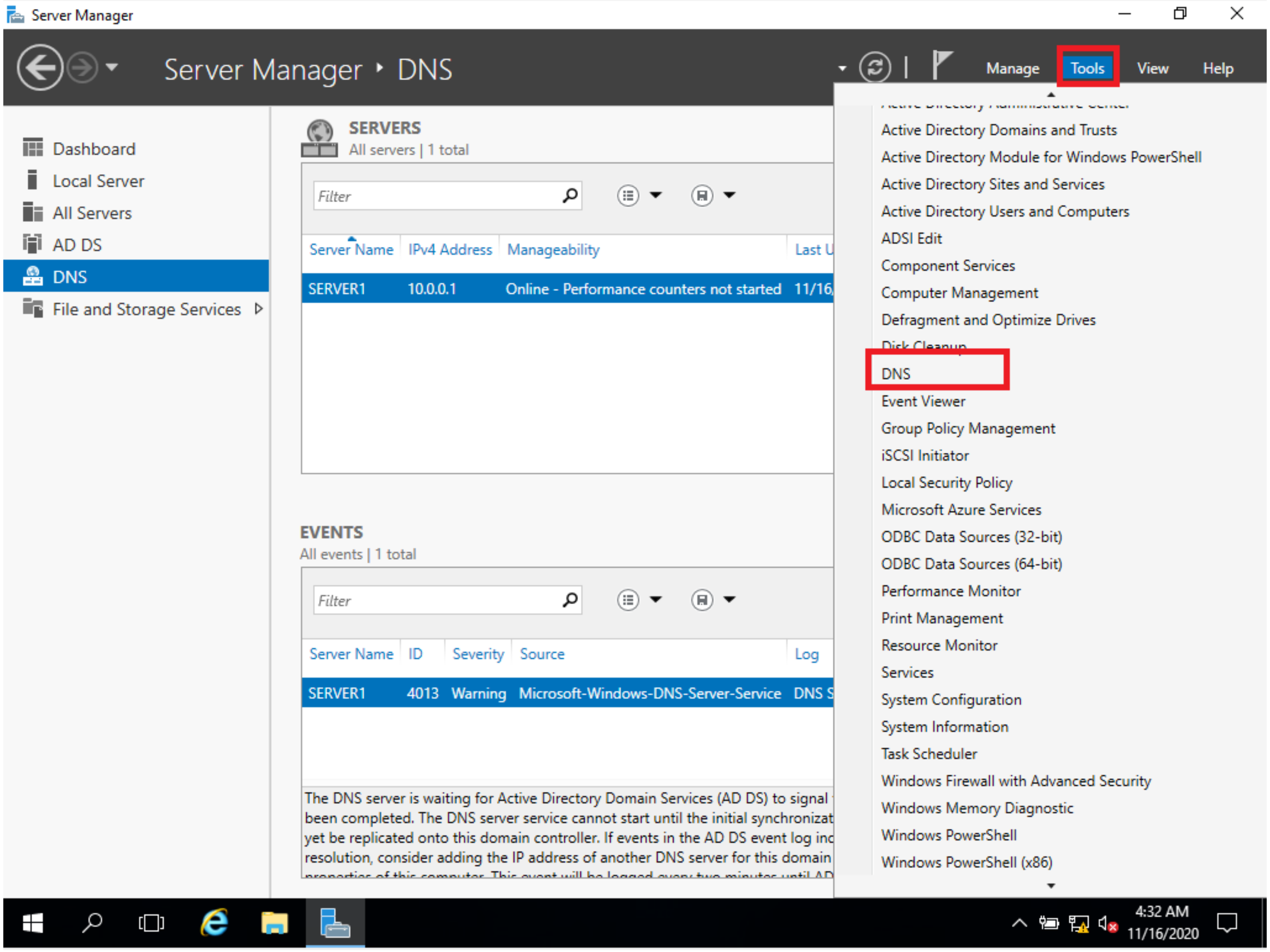
Resources

- Environment & Tools
    - VirtualBox
        - Windows Server 2016
        - Windows 10 Client

Lab Task 1: Configure DNS

Add and resolve A and CNAME records.

1 On ***SERVER1***, in **Server Manager**, click **Tools** and select ***DNS***.

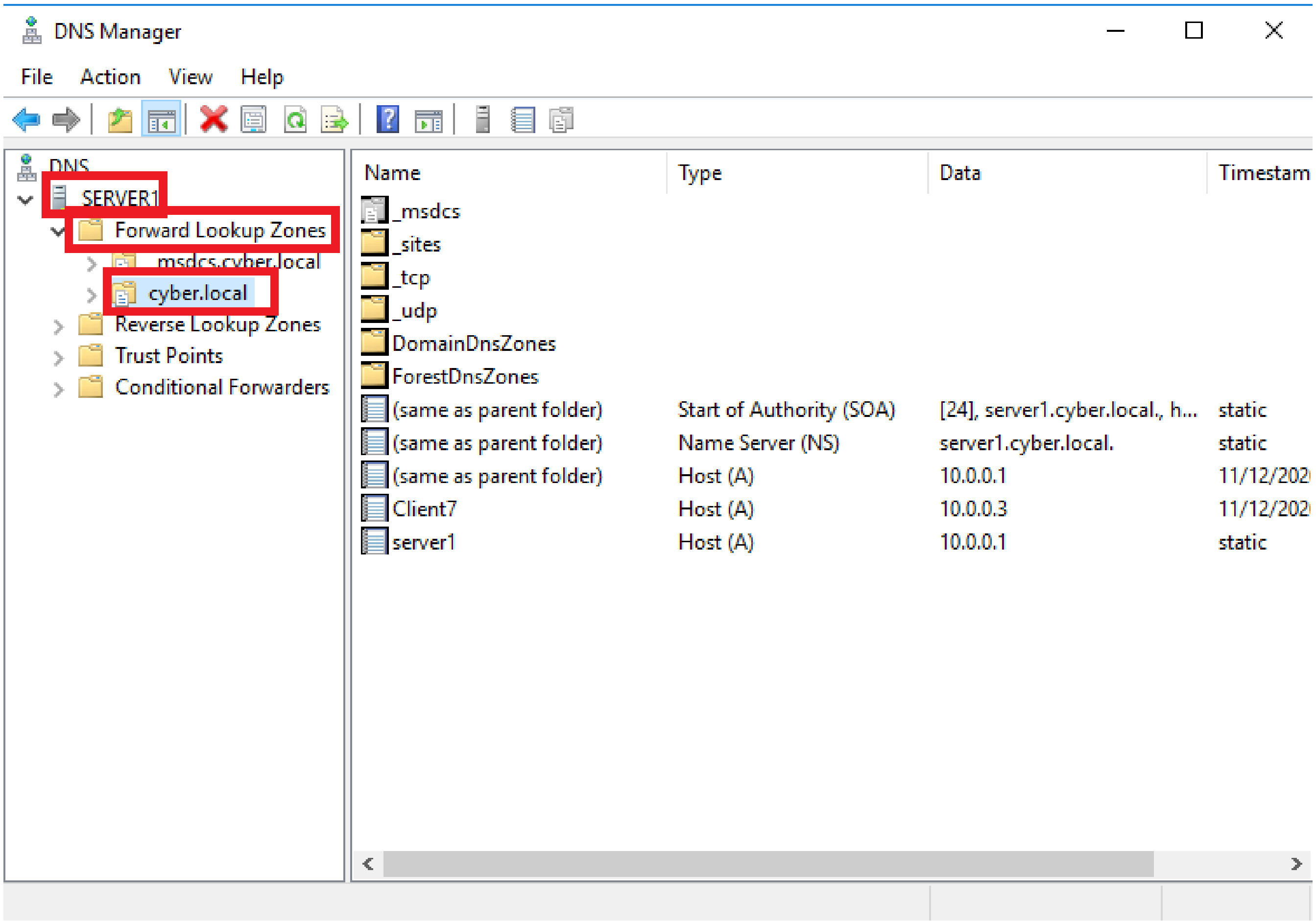


Server Name	IPv4 Address	Manageability	Last U
SERVER1	10.0.0.1	Online - Performance counters not started	11/16,

Server Name	ID	Severity	Source	Log
SERVER1	4013	Warning	Microsoft-Windows-DNS-Server-Service	DNS S

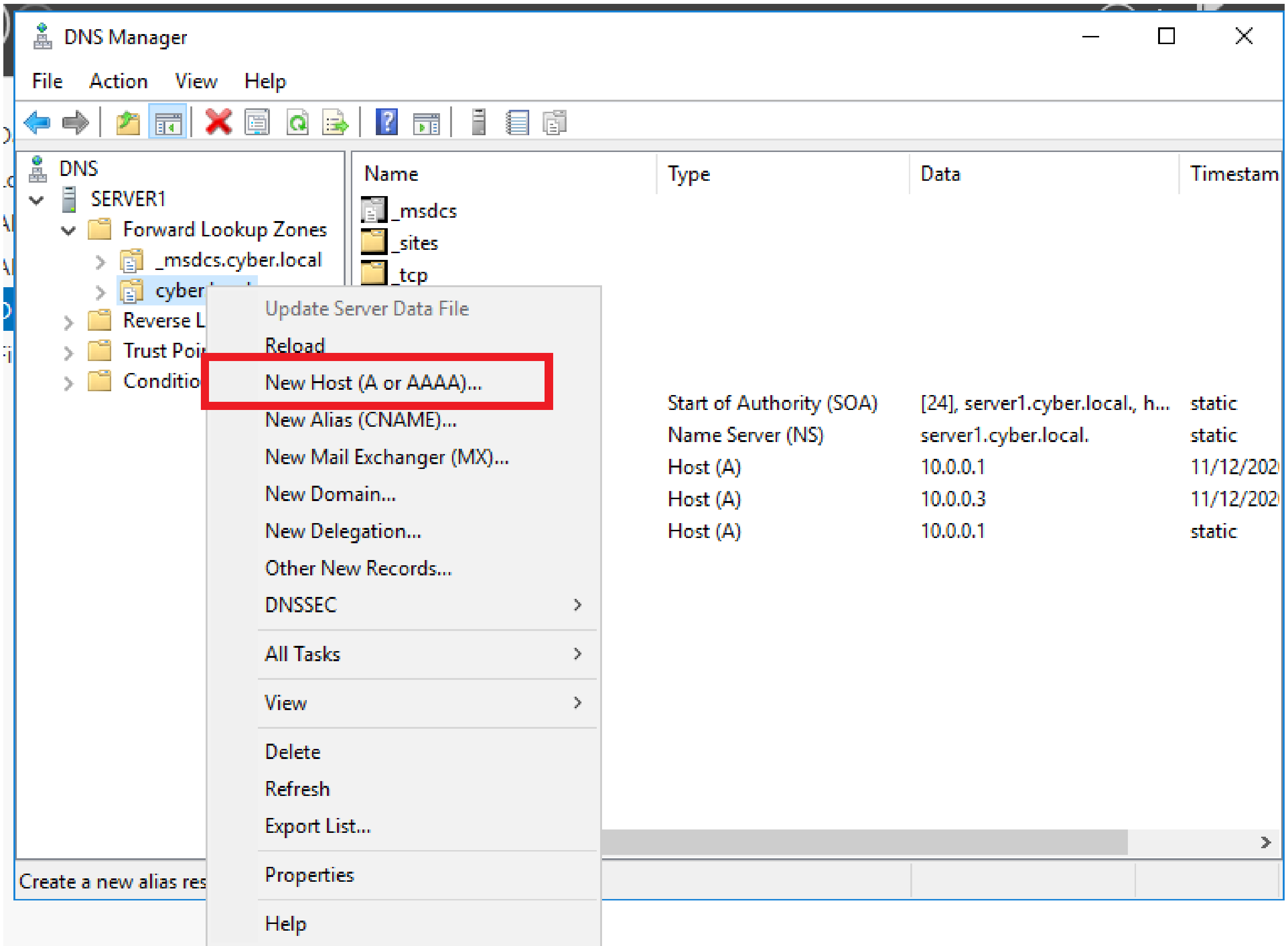
The DNS server is waiting for Active Directory Domain Services (AD DS) to signal
been completed. The DNS server service cannot start until the initial synchronizat
yet be replicated onto this domain controller. If events in the AD DS event log inc
resolution, consider adding the IP address of another DNS server for this domain
properties of this computer. This event will be logged every two minutes until AD

2 Expand ***SERVER1*** > ***Forward Lookup Zones*** > ***cyber.local***.



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[24], server1.cyber.local., h...	static
(same as parent folder)	Name Server (NS)	server1.cyber.local.	static
(same as parent folder)	Host (A)	10.0.0.1	11/12/202
Client7	Host (A)	10.0.0.3	11/12/202
server1	Host (A)	10.0.0.1	static

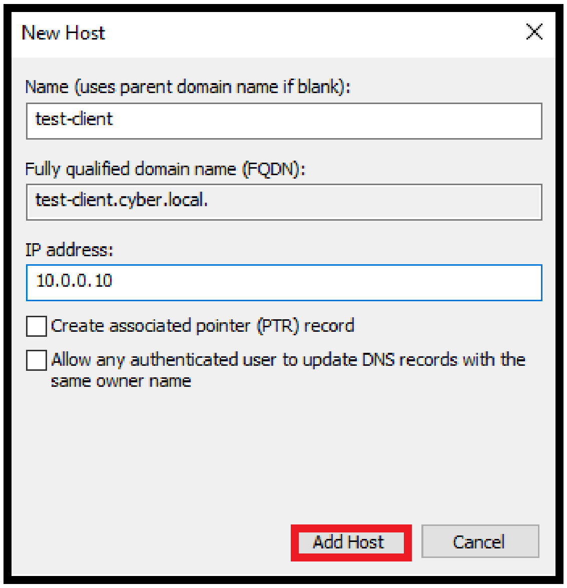
3 Right-click *cyber.local* and choose ***New Host (A or AAAA)...***



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
	Start of Authority (SOA)	[24], server1.cyber.local., h...	static
	Name Server (NS)	server1.cyber.local.	static
	Host (A)	10.0.0.1	11/12/202
	Host (A)	10.0.0.3	11/12/202
	Host (A)	10.0.0.1	static

Create a new alias res

4 For *Name*, enter **test-client**; for *IP Address*, enter **10.0.0.10**; and click **Add Host**. Click **OK** when prompted.



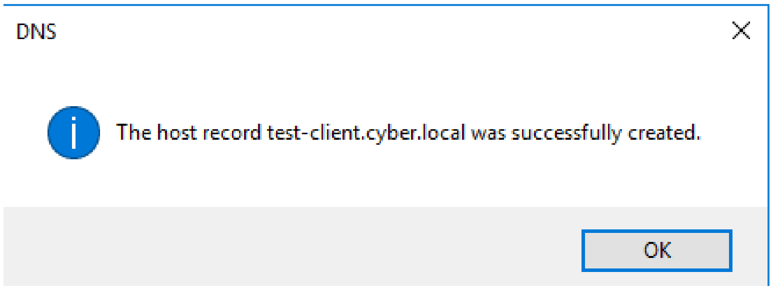
Name (uses parent domain name if blank): test-client

Fully qualified domain name (FQDN): test-client.cyber.local.

IP address: 10.0.0.10

□ Create associated pointer (PTR) record

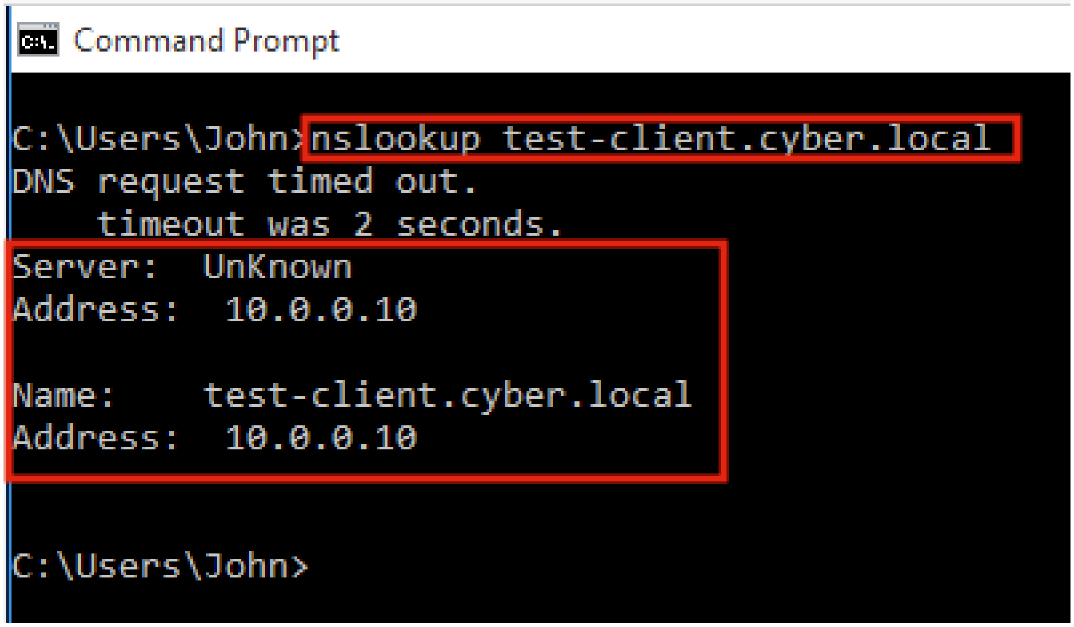
□ Allow any authenticated user to update DNS records with the same owner name



The host record test-client.cyber.local was successfully created.

5 Log into the Windows 10 client VM.

6 Open CMD and run the command ***nslookup test-client.cyber.local***

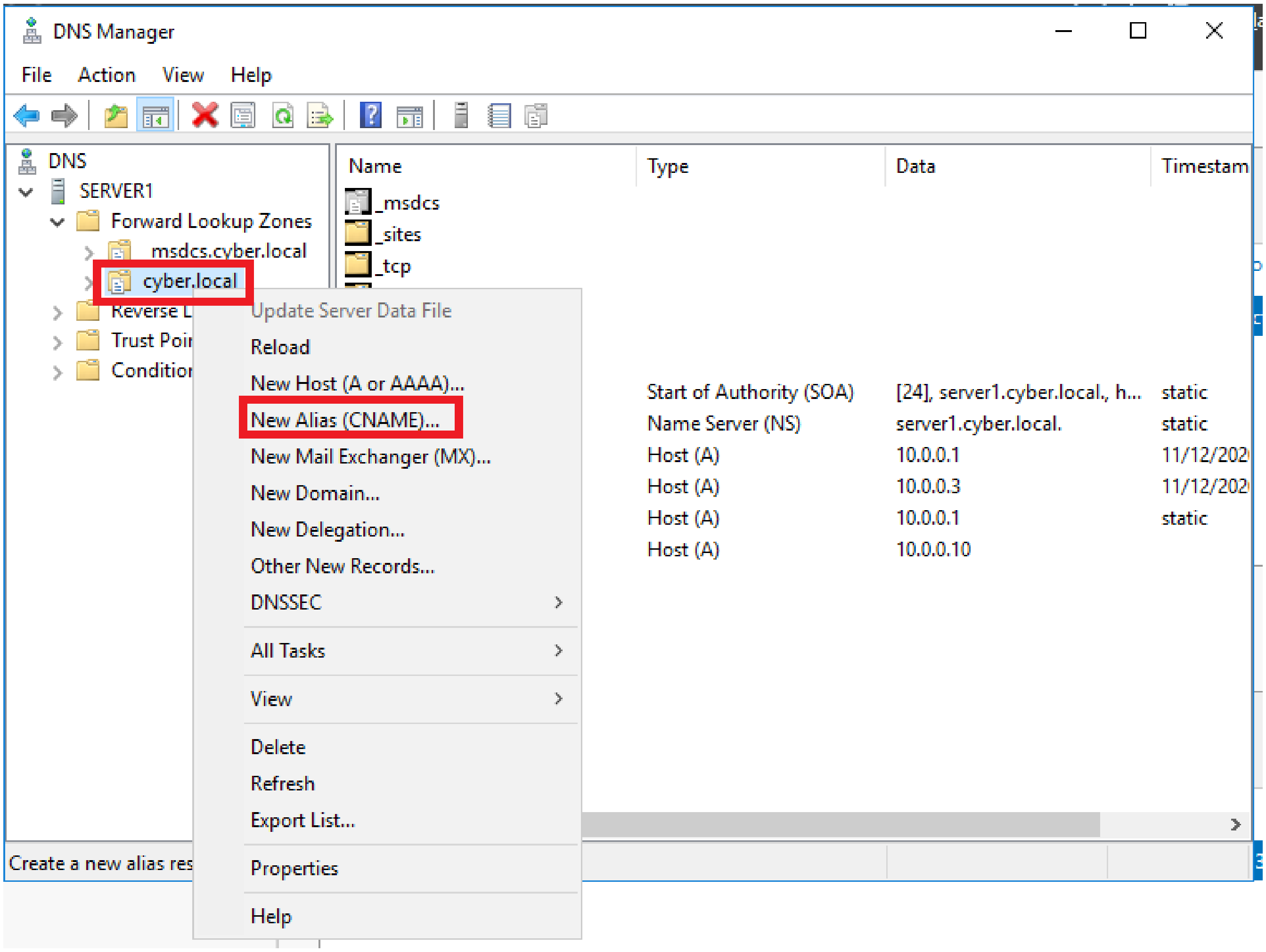


```
C:\Users\John>nslookup test-client.cyber.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10.0.0.10

Name:    test-client.cyber.local
Address:  10.0.0.10


C:\Users\John>
```

7 On ***SERVER1***, in **Server Manager**, click **Tools** and select ***DNS***.

8 Expand ***SERVER1*** > ***Forward Lookup Zones*** > ***cyber.local***.

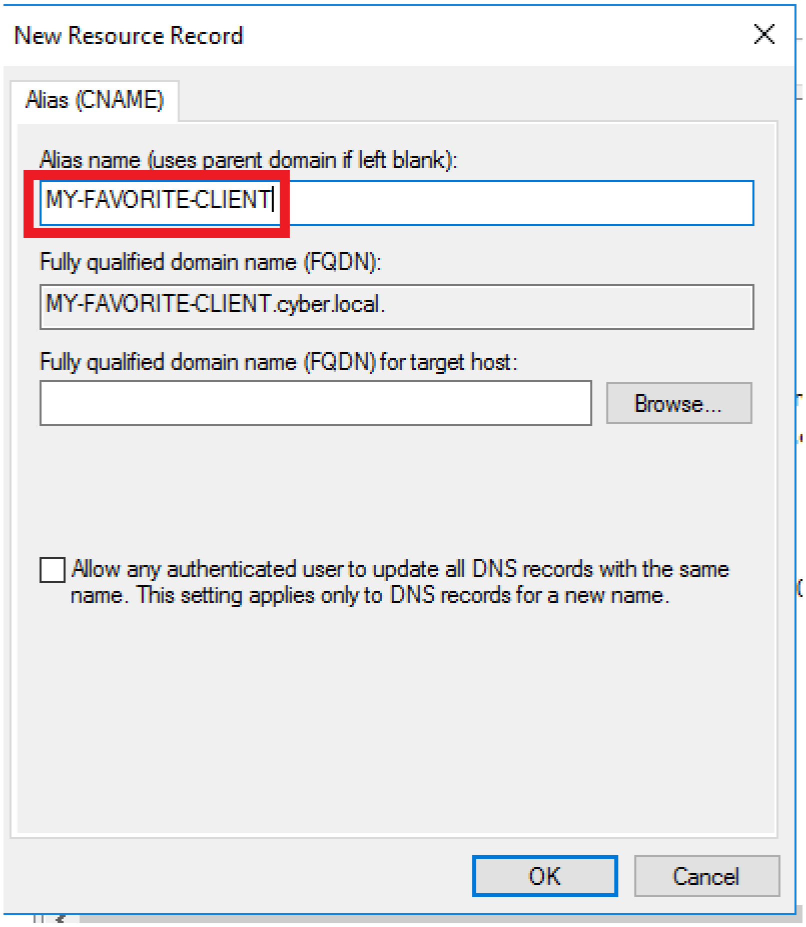
9 Right-click ***cyber.local*** and choose ***New Alias (CNAME)...***



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
	Start of Authority (SOA)	[24], server1.cyber.local., h...	static
	Name Server (NS)	server1.cyber.local.	static
	Host (A)	10.0.0.1	11/12/202
	Host (A)	10.0.0.3	11/12/202
	Host (A)	10.0.0.1	static
	Host (A)	10.0.0.10	

Create a new alias res

10 Under *Alias name*, enter **MY-FAVORITE-CLIENT**.



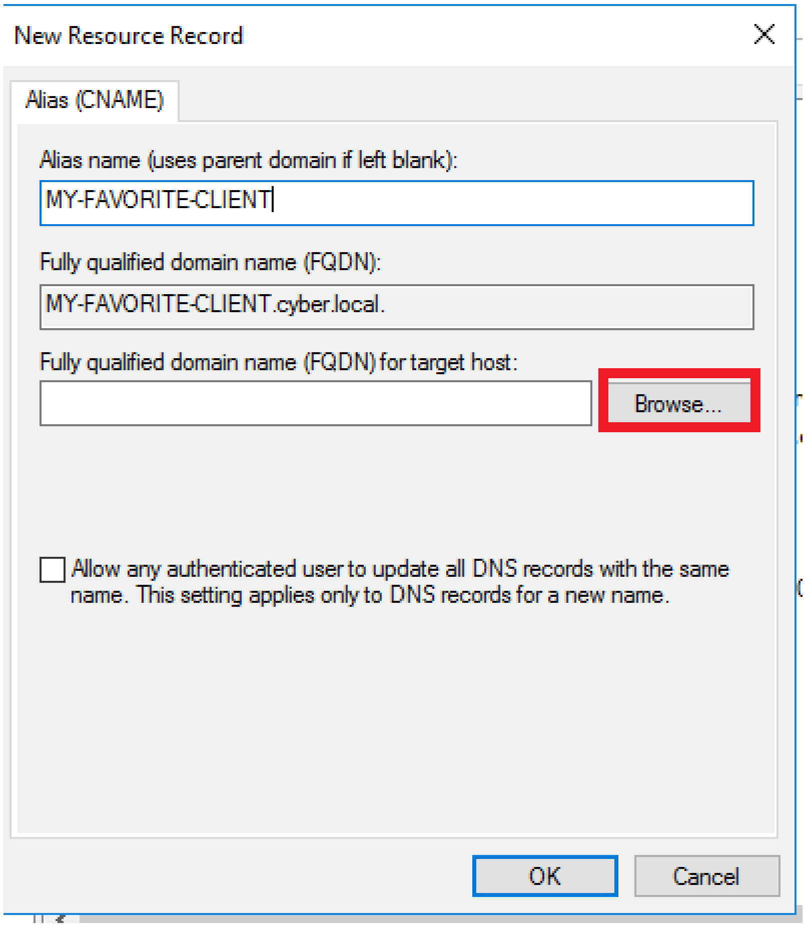
Alias name (uses parent domain if left blank): MY-FAVORITE-CLIENT

Fully qualified domain name (FQDN): MY-FAVORITE-CLIENT.cyber.local.

Fully qualified domain name (FQDN) for target host:

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

11 Click **Browse…** on the right, double-click ***SERVER1***, double-click ***Forward Lookup Zones***, then double-click ***cyber.local***, and choose ***test-client***. Enter **test-client.cyber.local** in the ***Fully qualified domain name*** field, then click **OK**.


New Resource Record

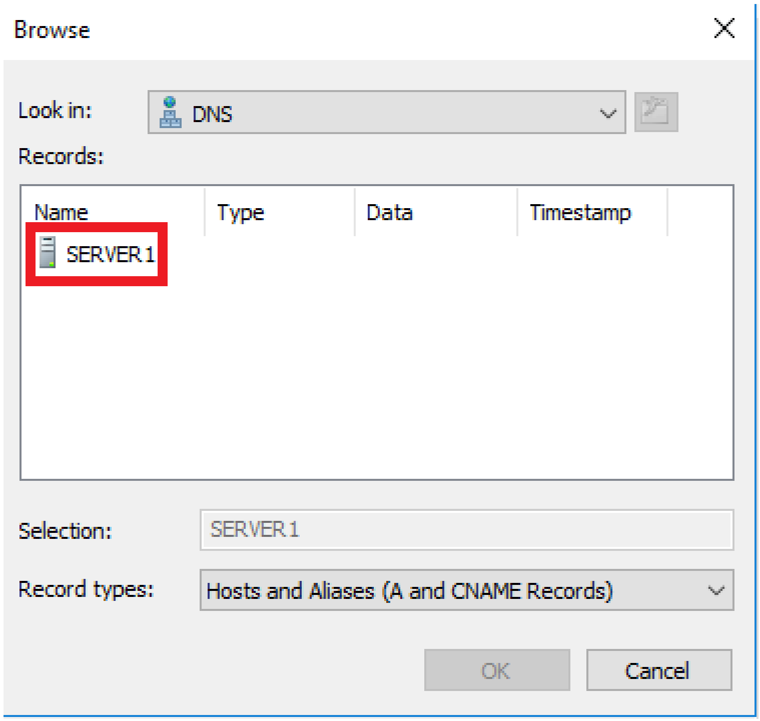
Alias (CNAME)

Alias name (uses parent domain if left blank):
MY-FAVORITE-CLIENT

Fully qualified domain name (FQDN):
MY-FAVORITE-CLIENT.cyber.local.

Fully qualified domain name (FQDN) for target host:

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.



Browse

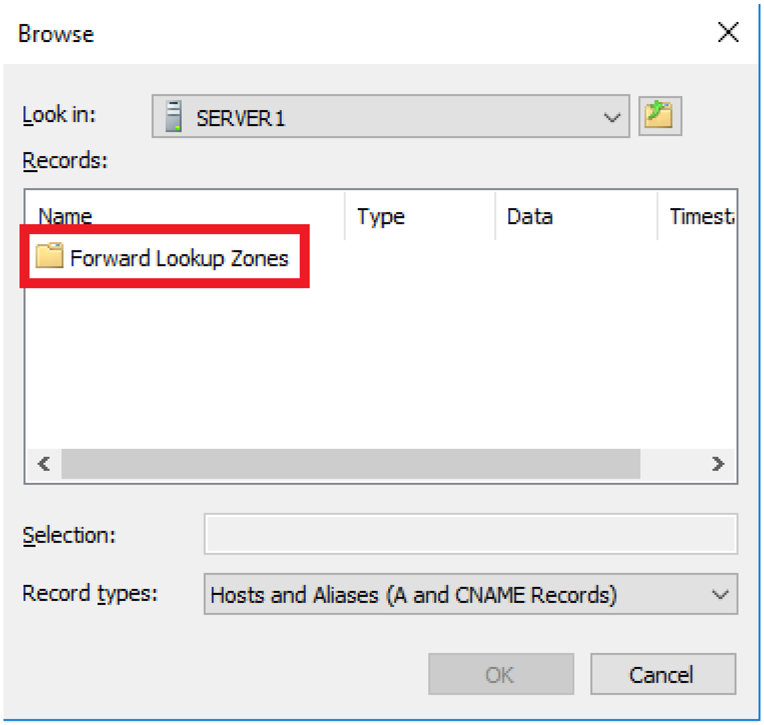
Look in: DNS

Records:

Name	Type	Data	Timestamp
SERVER1			

Selection: SERVER1

Record types: Hosts and Aliases (A and CNAME Records)



Browse

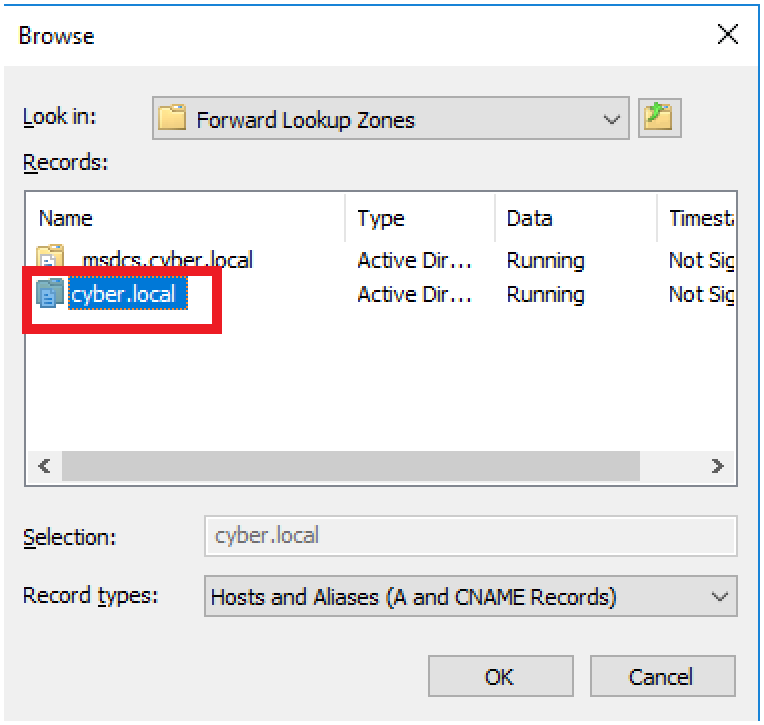
Look in: SERVER1

Records:

Name	Type	Data	Timest
Forward Lookup Zones			

Selection:

Record types: Hosts and Aliases (A and CNAME Records)



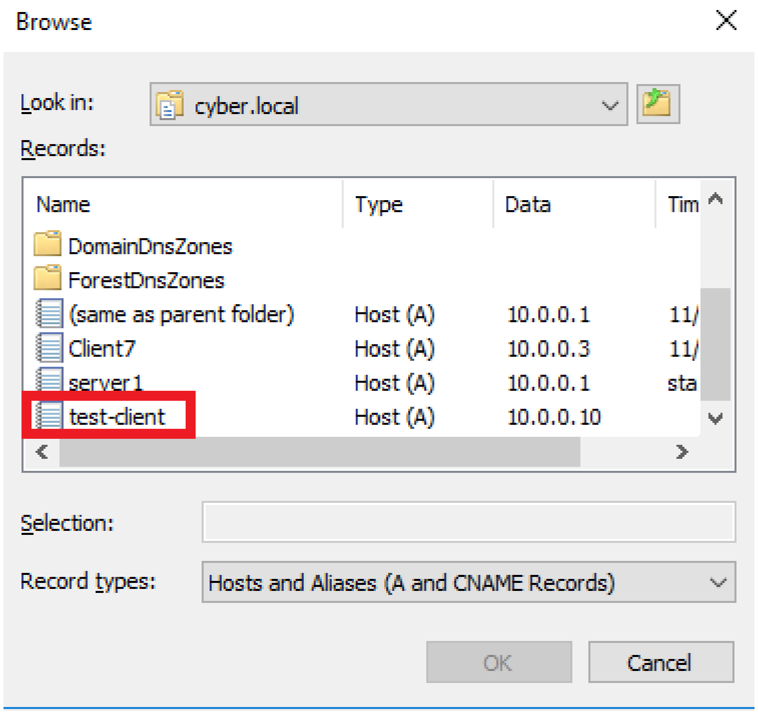
Look in: Forward Lookup Zones

Records:

Name	Type	Data	Timest
_msdcs.cyber.local	Active Dir…	Running	Not Sig
cyber.local	Active Dir…	Running	Not Sig

Selection: cyber.local

Record types: Hosts and Aliases (A and CNAME Records)



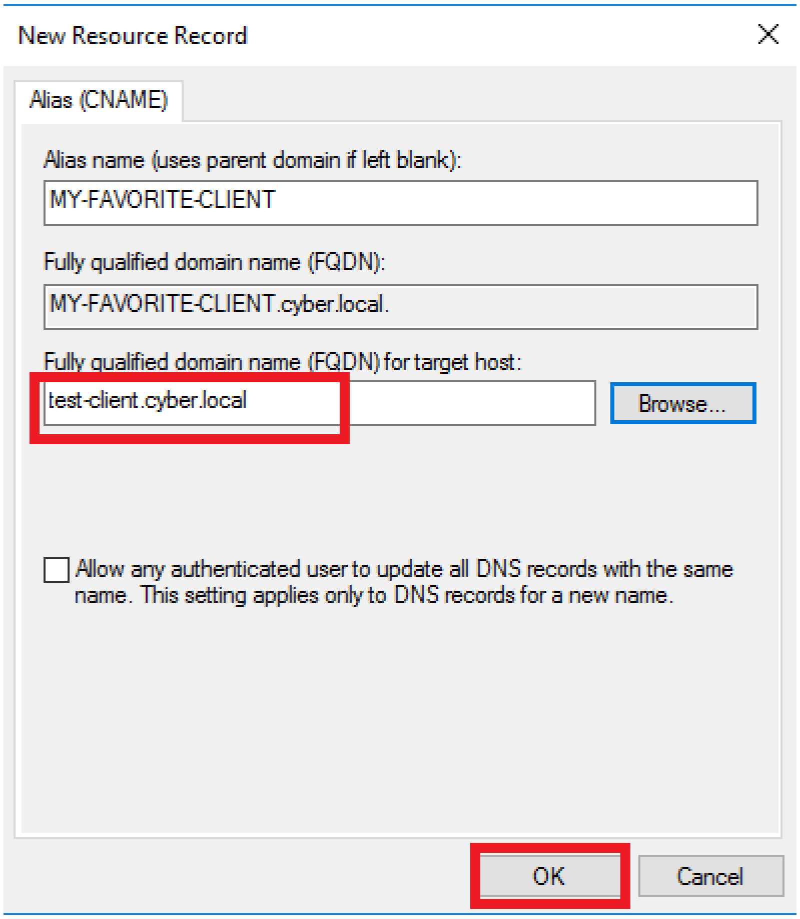
Look in: cyber.local

Records:

Name	Type	Data	Tim
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Host (A)	10.0.0.1	11/
Client7	Host (A)	10.0.0.3	11/
server1	Host (A)	10.0.0.1	sta
test-client	Host (A)	10.0.0.10	

Selection:

Record types: Hosts and Aliases (A and CNAME Records)



Alias name (uses parent domain if left blank): MY-FAVORITE-CLIENT

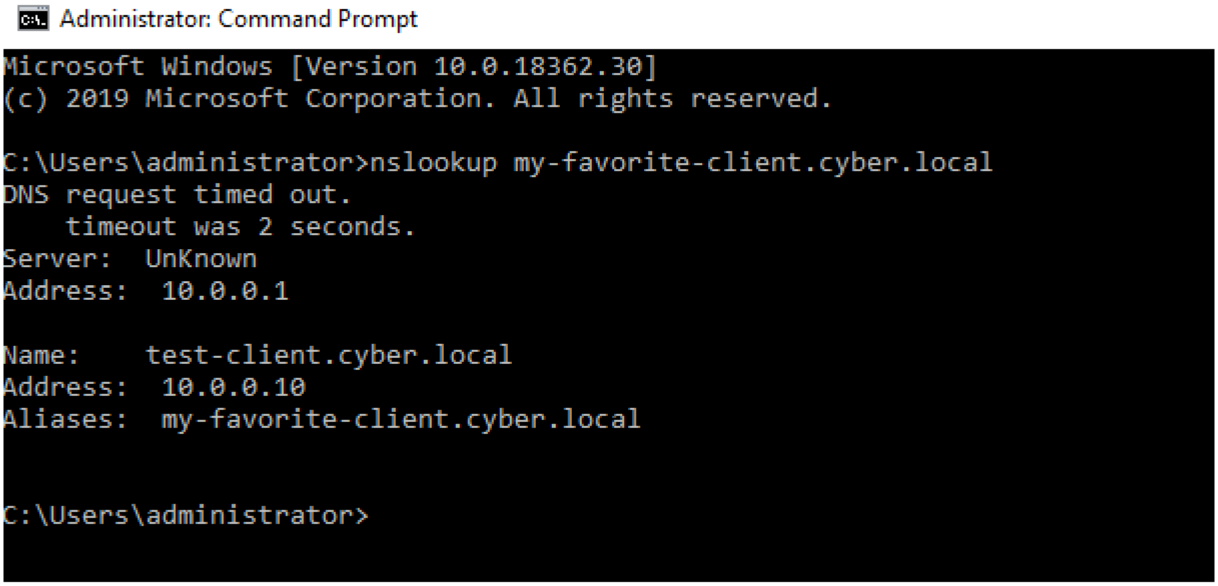
Fully qualified domain name (FQDN): MY-FAVORITE-CLIENT.cyber.local.

Fully qualified domain name (FQDN) for target host: test-client.cyber.local

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

12 Log into the Windows 10 client VM.

13 Open CMD and run the command ***nslookup my-favorite-client.cyber.local***



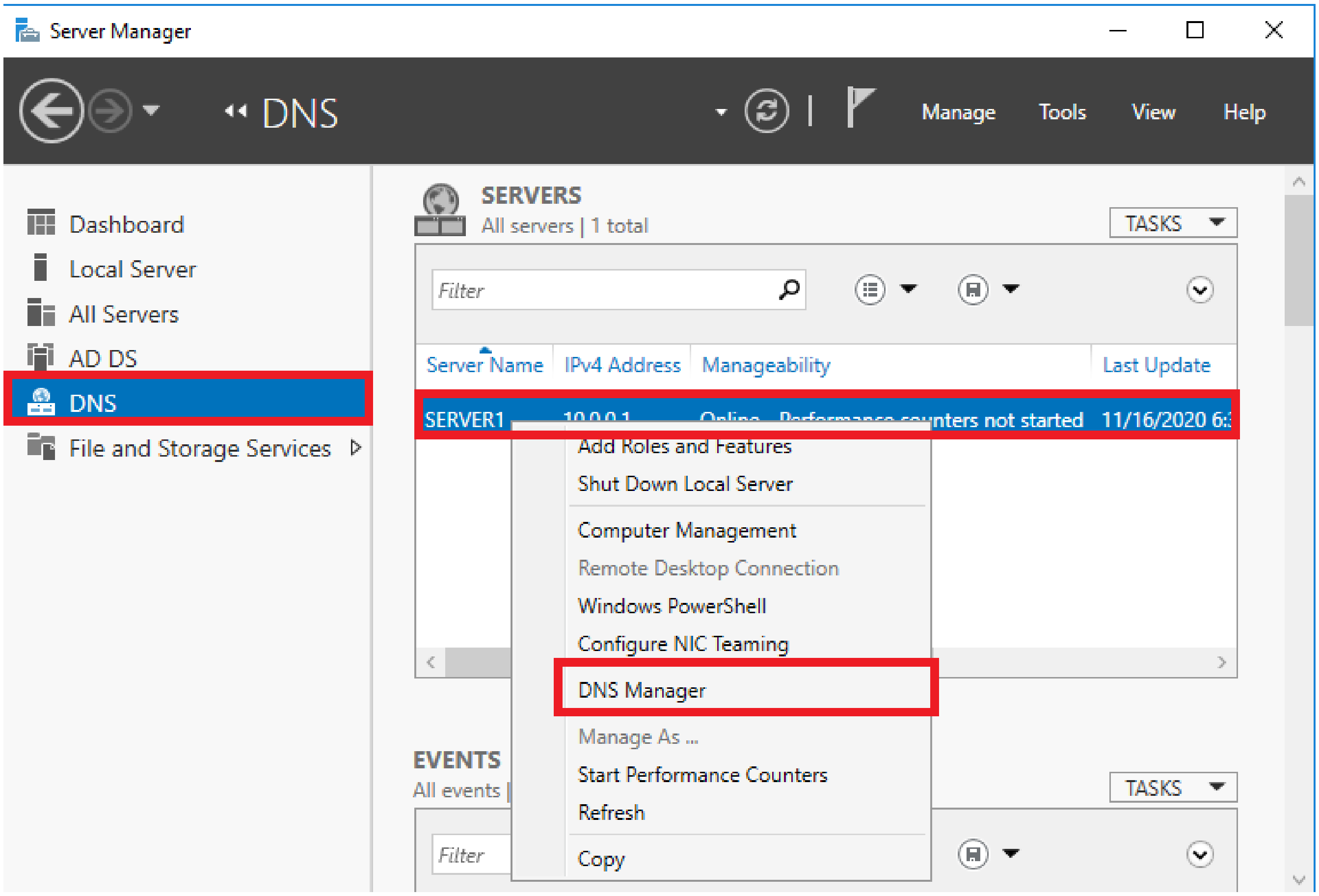
```
Microsoft Windows [Version 10.0.18362.30]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\administrator>nslookup my-favorite-client.cyber.local
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  10.0.0.1

Name:    test-client.cyber.local
Address:  10.0.0.10
Aliases:  my-favorite-client.cyber.local


C:\Users\administrator>
```

14 Why do we need CNAME records?

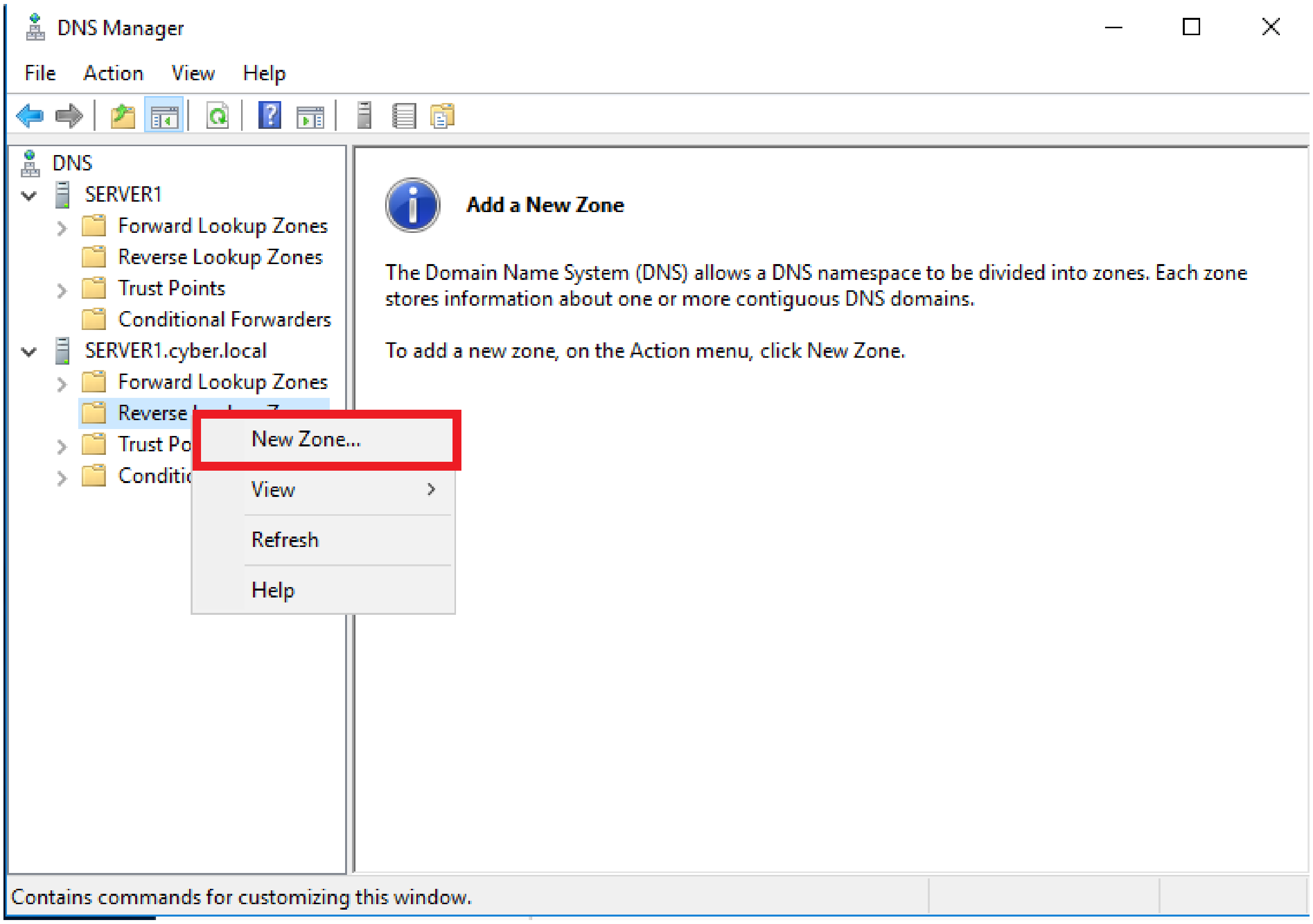
Lab Task 2: Bonus

Configure a PTR record on ***SERVER1***.

1 On ***SERVER1***, navigate to the DNS Servers section, right-click ***SERVER1*** on the server panel as shown, and select ***DNS Manager***.



2 Right-click ***Reverse Lookup Zones*** and select ***New Zone...***



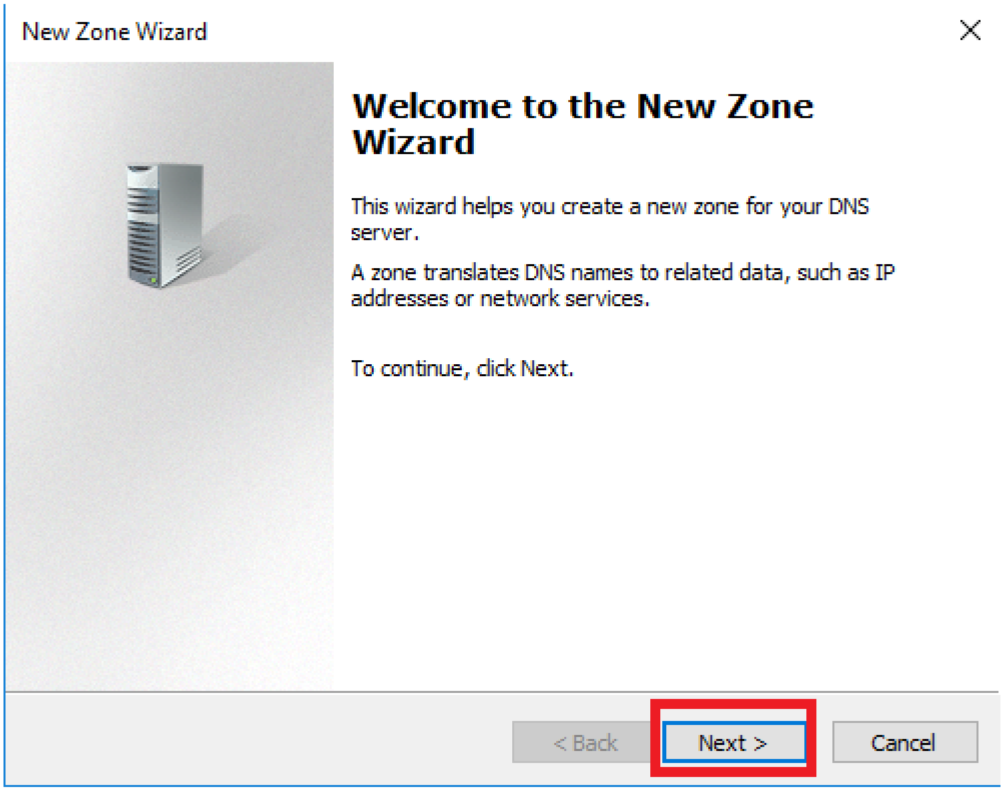
Add a New Zone

The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.

To add a new zone, on the Action menu, click New Zone.

Contains commands for customizing this window.

3 Click **Next** and select ***Primary zone***.



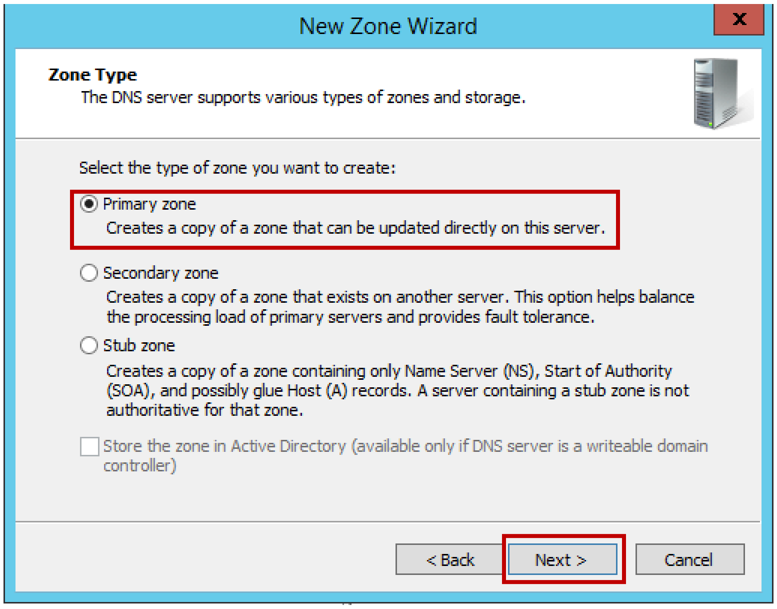
New Zone Wizard

Welcome to the New Zone Wizard

This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.



New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

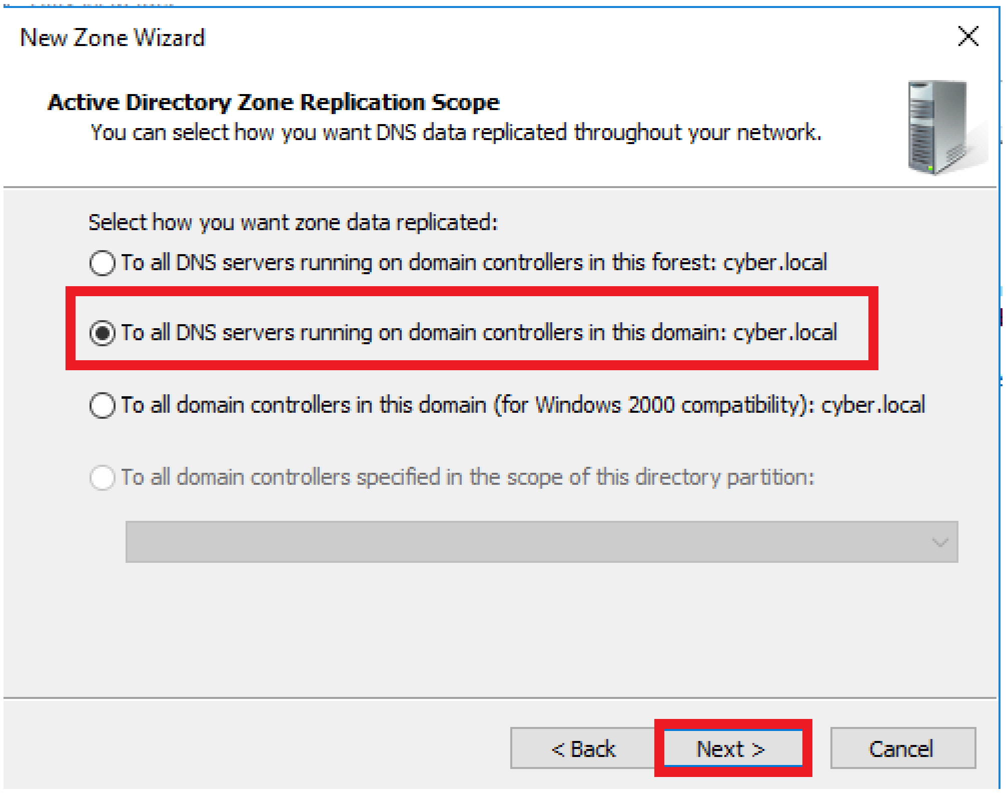
● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

□ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

4 In **Active Directory Zone Replication Scope**, select ***To all DNS servers running on domain controllers in this domain***: ***cyber.local*** and click **Next**.



New Zone Wizard

Active Directory Zone Replication Scope

You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

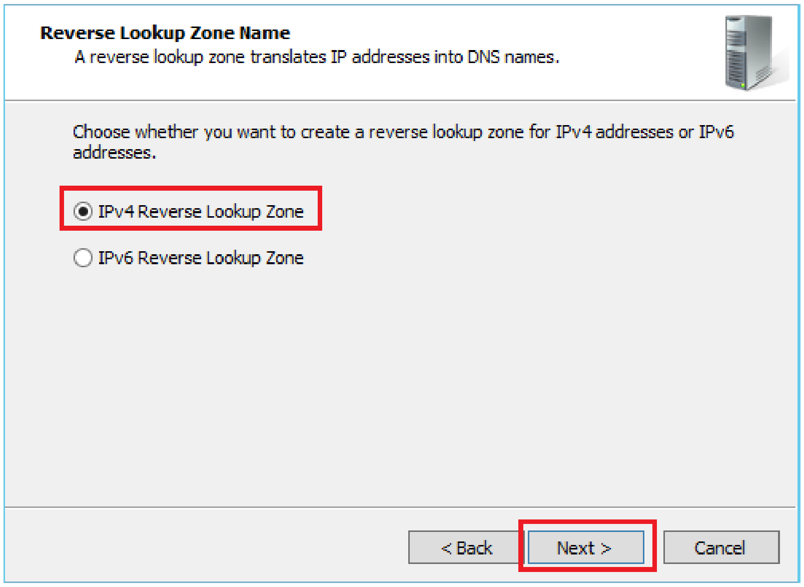
○ To all DNS servers running on domain controllers in this forest: cyber.local

● To all DNS servers running on domain controllers in this domain: cyber.local

○ To all domain controllers in this domain (for Windows 2000 compatibility): cyber.local

○ To all domain controllers specified in the scope of this directory partition:

5 Under **Reverse Lookup Zone Name**, select ***IPv4 Reverse Lookup Zone***, and click **Next**.



Reverse Lookup Zone Name

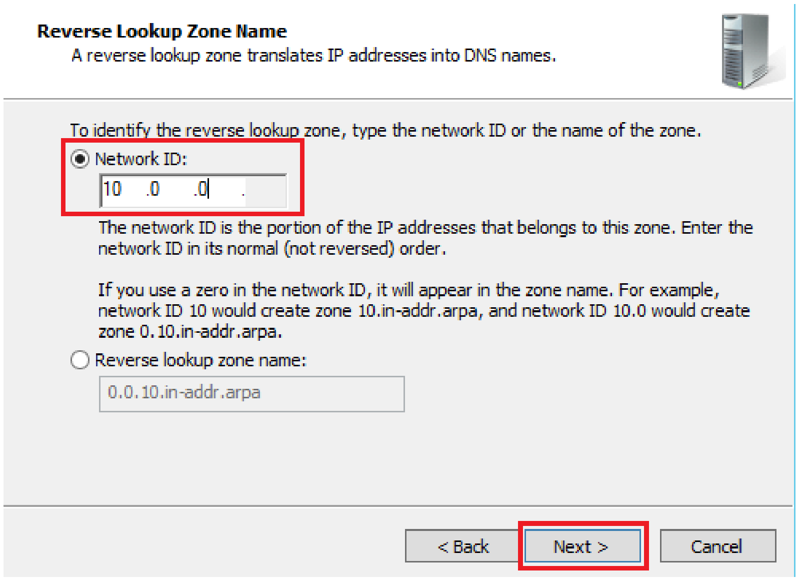
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

● IPv4 Reverse Lookup Zone

○ IPv6 Reverse Lookup Zone

6 For the network ID, enter ***10.0.0***, leave the rest empty, and click **Next**.



Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

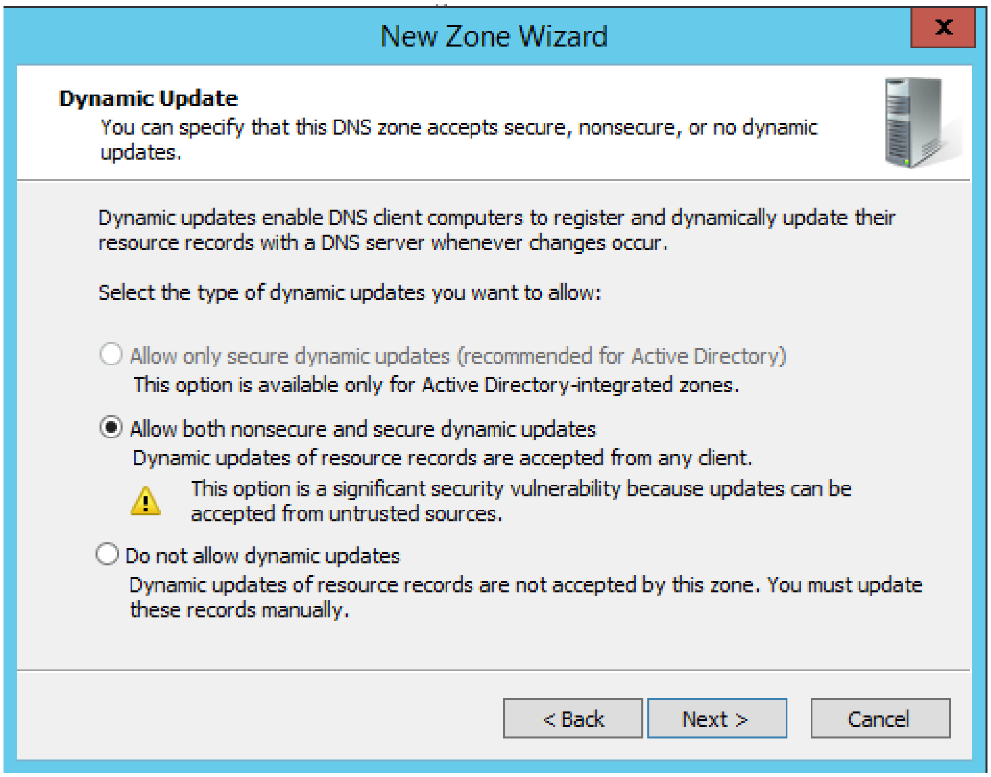
● Network ID:
10 .0 .0 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:
0.0.10.in-addr.arpa

7 On the **Dynamic Update** window, select ***Allow both nonsecure and secure dynamic updates***, and click **Next**.



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.

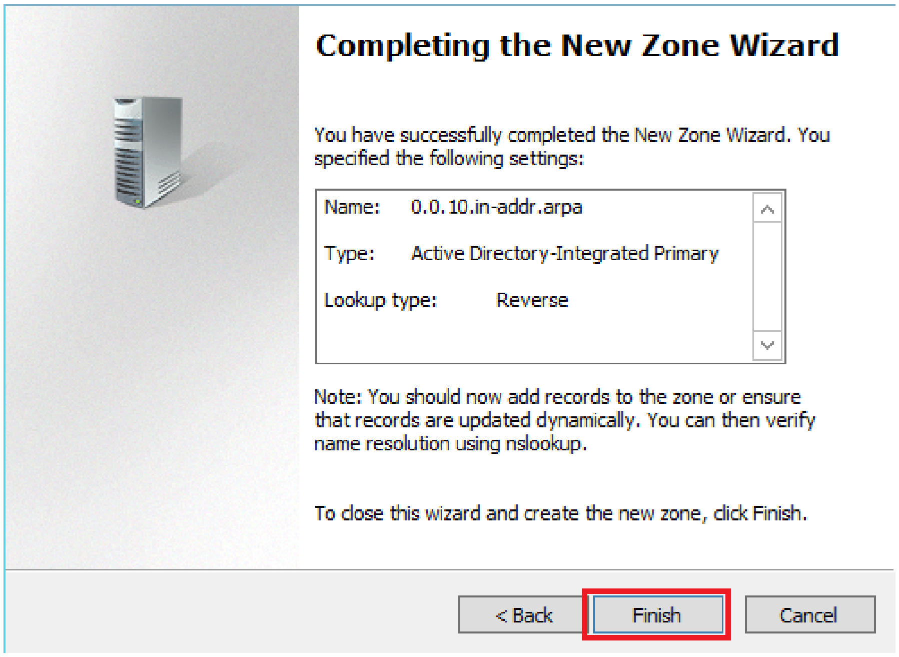
Select the type of dynamic updates you want to allow:

○ 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.

8 Click **Finish**.



Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name: 0.0.10.in-addr.arpa

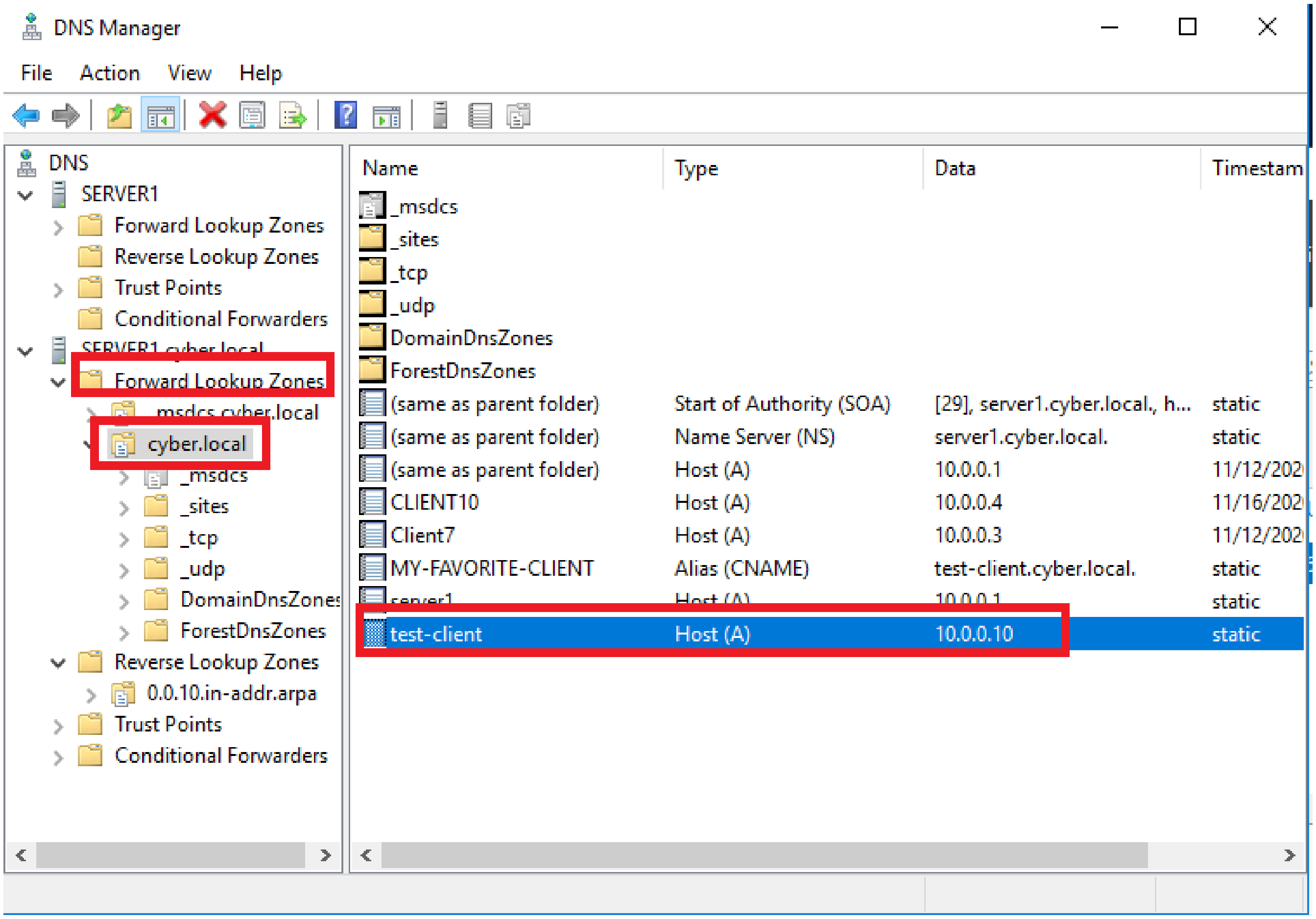
Type: Active Directory-Integrated Primary

Lookup type: Reverse

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

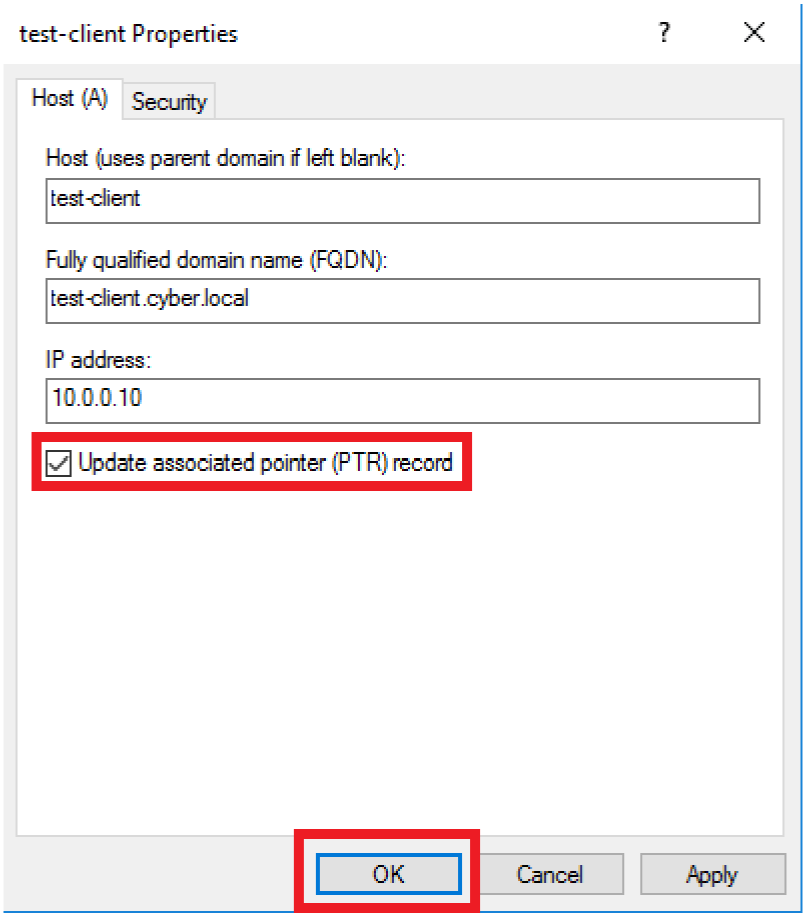
To close this wizard and create the new zone, click Finish.

9 Expand ***Forward Lookup Zones*** and select ***cyber.local***. Double-click ***test-client***.



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[29], server1.cyber.local., h...	static
(same as parent folder)	Name Server (NS)	server1.cyber.local.	static
(same as parent folder)	Host (A)	10.0.0.1	11/12/202
CLIENT10	Host (A)	10.0.0.4	11/16/202
Client7	Host (A)	10.0.0.3	11/12/202
MY-FAVORITE-CLIENT	Alias (CNAME)	test-client.cyber.local.	static
server1	Host (A)	10.0.0.1	static
test-client	Host (A)	10.0.0.10	static

10 Select ***Update associated pointer (PTR) record*** and click **OK**.


test-client Properties

Host (A) | Security

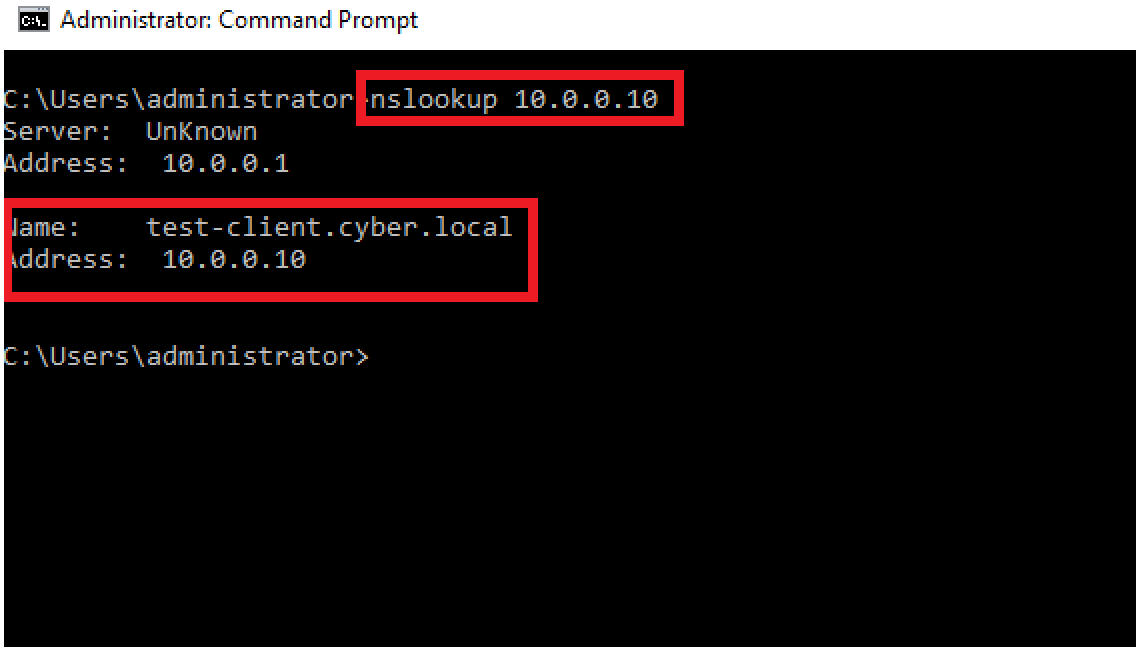
Host (uses parent domain if left blank):
test-client

Fully qualified domain name (FQDN):
test-client.cyber.local

IP address:
10.0.0.10

☑ Update associated pointer (PTR) record

11 From the client machine, resolve the ***10.0.0.10*** IP using the ***nslookup*** command. What are the results?



```
C:\Users\administrator>nslookup 10.0.0.10
Server:  UnKnown
Address:  10.0.0.1

Name:    test-client.cyber.local
Address:  10.0.0.10


C:\Users\administrator>
```