Lesson 8: Configuring DNS Zones

MOAC 70-411: Administering Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 3.1: Configure DNS Zones
- Understanding DNS
- Configuring and Managing DNS Zones
- Using the Dnscmd Command to Manage Zones

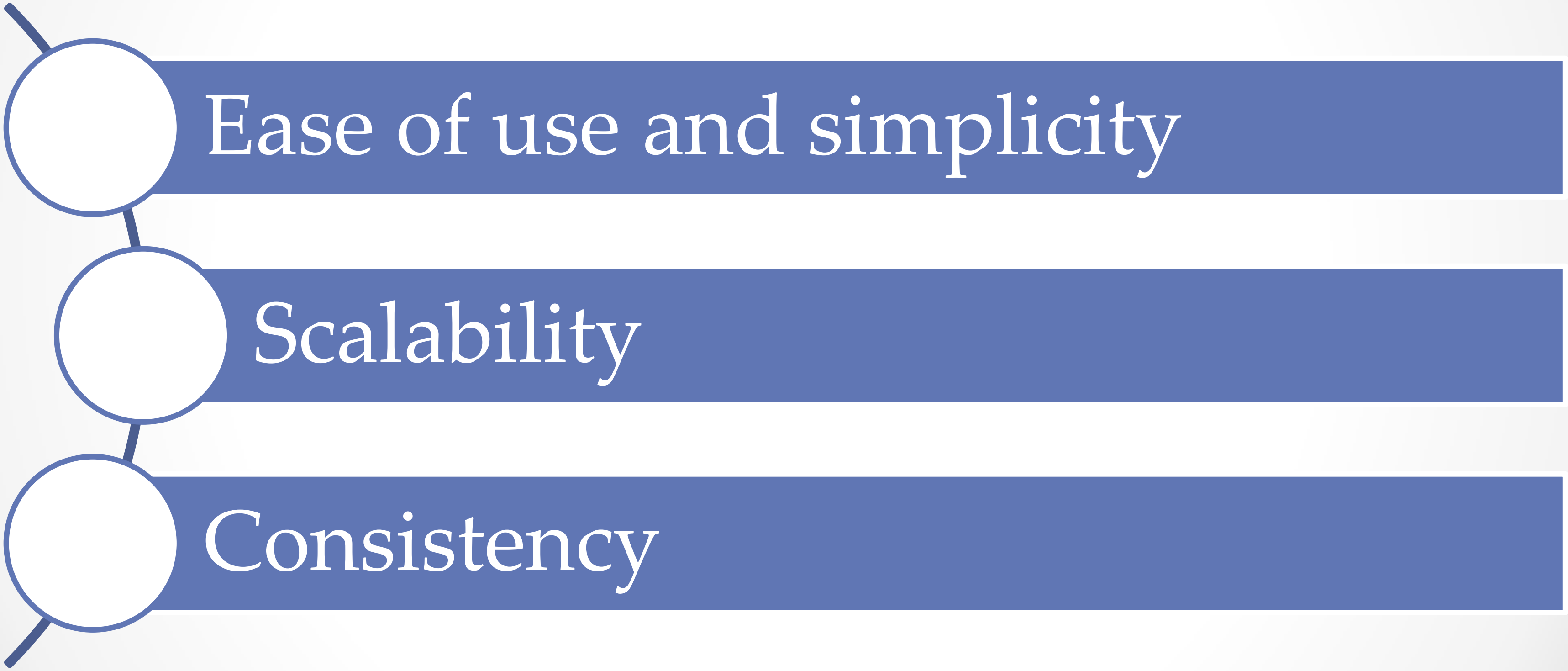
Understanding DNS

Lesson 8: Configuring DNS Zones

Understanding DNS

- ***Domain Name System (DNS)*** is a naming service used by TCP/IP networks and is an essential service used by the Internet.
- Translates URLs to IP addresses.
- Early TCP/IP networks performed name resolution using hosts files stored locally on each computer.

Benefits of DNS

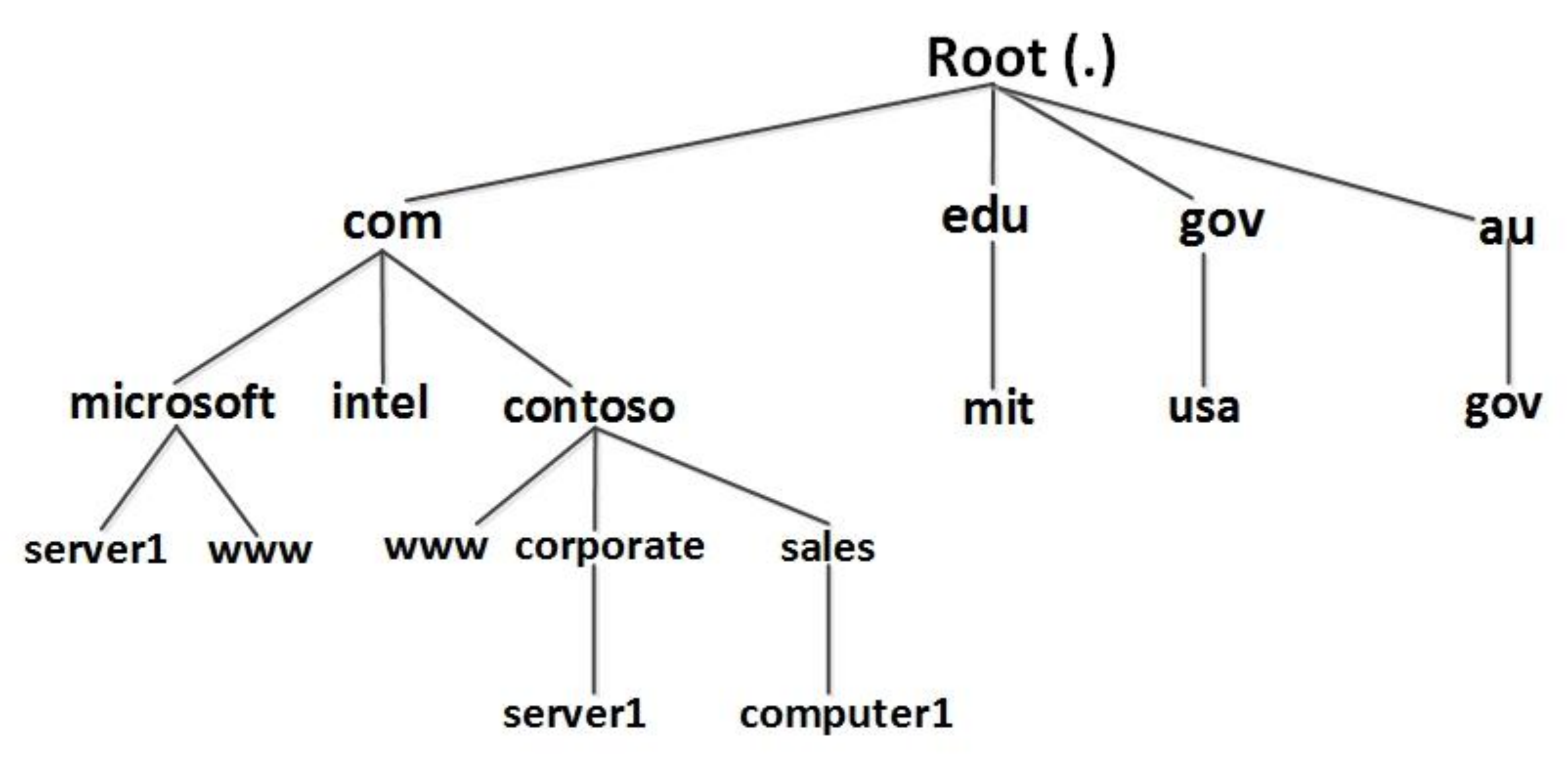


- Ease of use and simplicity
- Scalability
- Consistency

Understanding DNS Names and Zones

- ***Fully qualified domain names (FQDNs)*** map a host name to an IP address.
- Example:
  - computer1.sales.microsoft.com represents an FQDN
  - computer1 host is located in the sales domain, which is located in the Microsoft second-level domain, which is located in the .com top-level domain

DNS Hierarchy

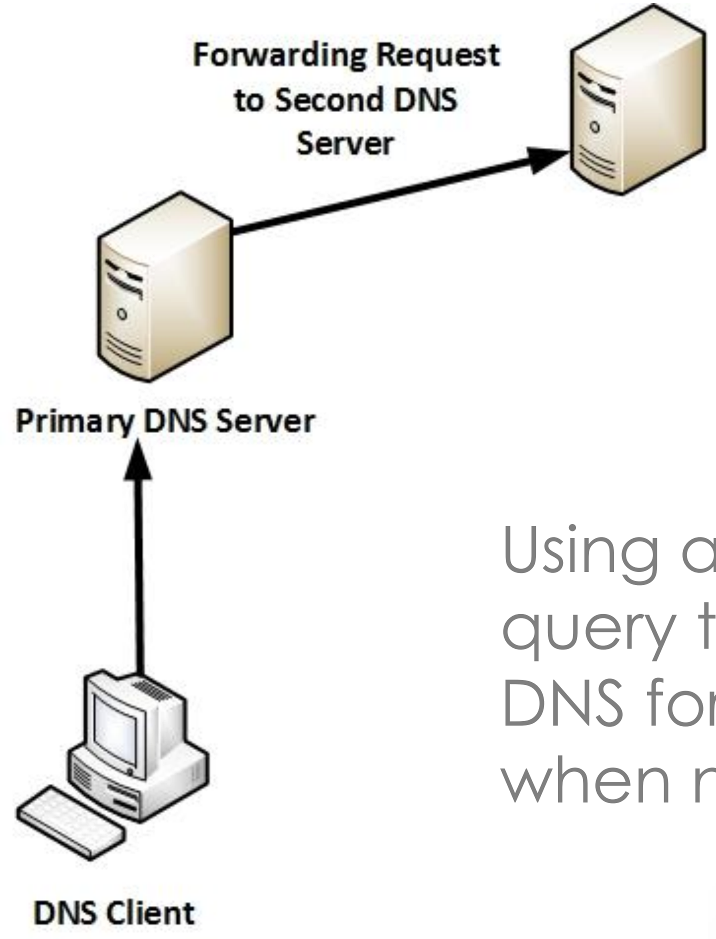


© 2013 John Wiley & Sons, Inc.

DNS Terms

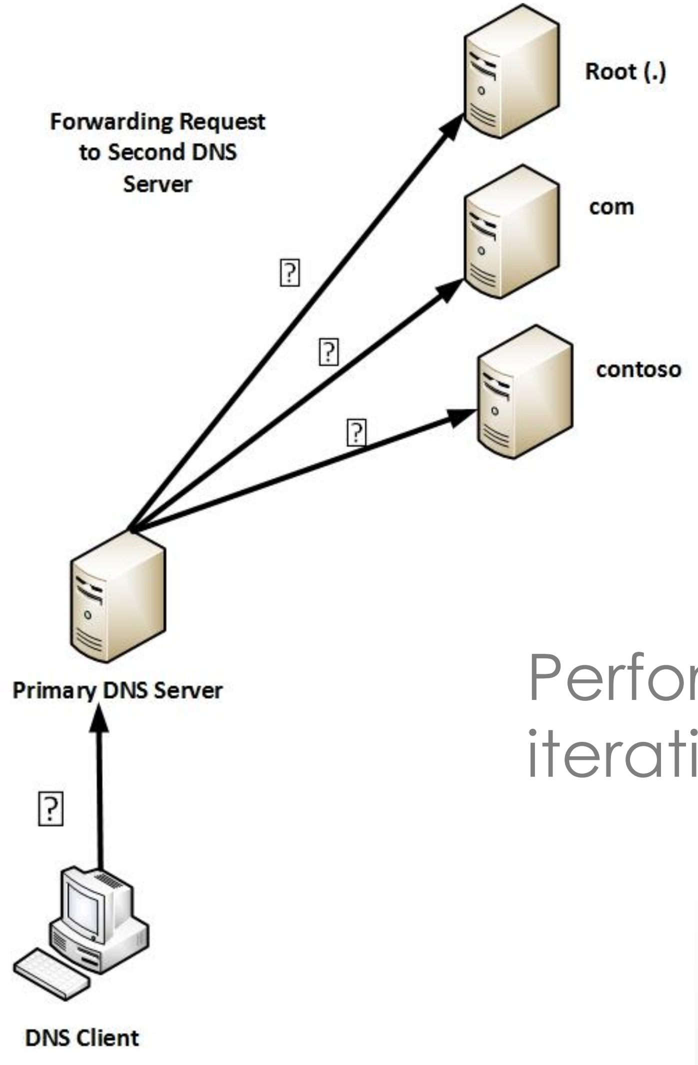
- Each node or leaf in the domain name tree is a **resource record (RR)**, which holds information associated with the domain name.
- **Top-level domains** consist of generic top-level domains and international country codes.
- **Second-level domains** are registered to individuals or organizations.
- A **host** is a specific computer or other network device in a domain.

Address Resolution Mechanism



Using a recursive query to perform DNS forwarding, when needed

Address Resolution Mechanism



Performing an iterative query

Configuring and Managing DNS Zones

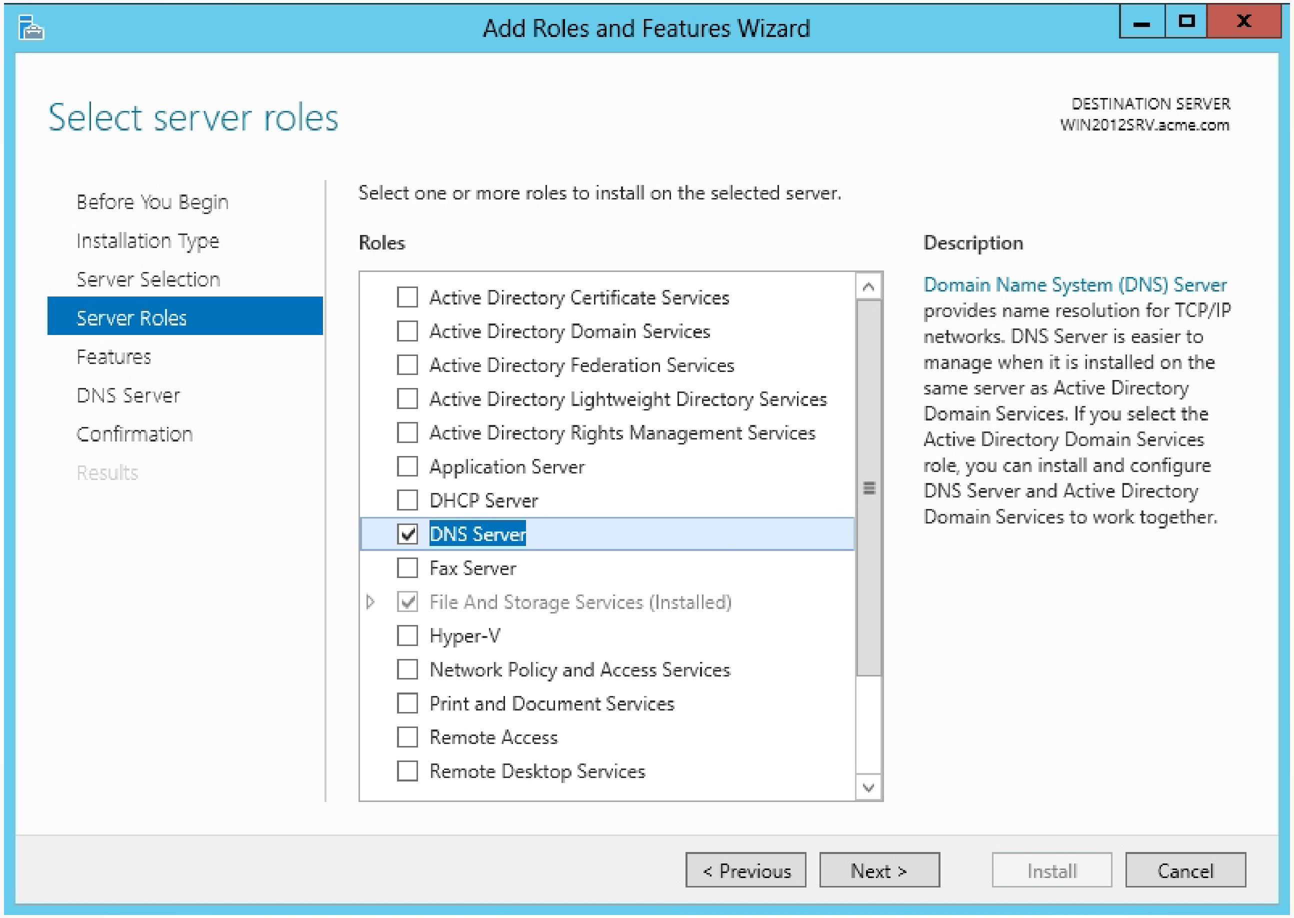
Lesson 8: Configuring DNS Zones

Deploying DNS

Steps in deploying DNS:

1. Install DNS on one or more servers.
2. Configure the DNS server, if necessary.
3. Create forward and reverse lookup zones.
4. Add resource records to the forward and reverse lookup zones.
5. Configure the clients to use the DNS servers.

Install DNS



Select server roles

DESTINATION SERVER
WIN2012SRV.acme.com

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

Roles

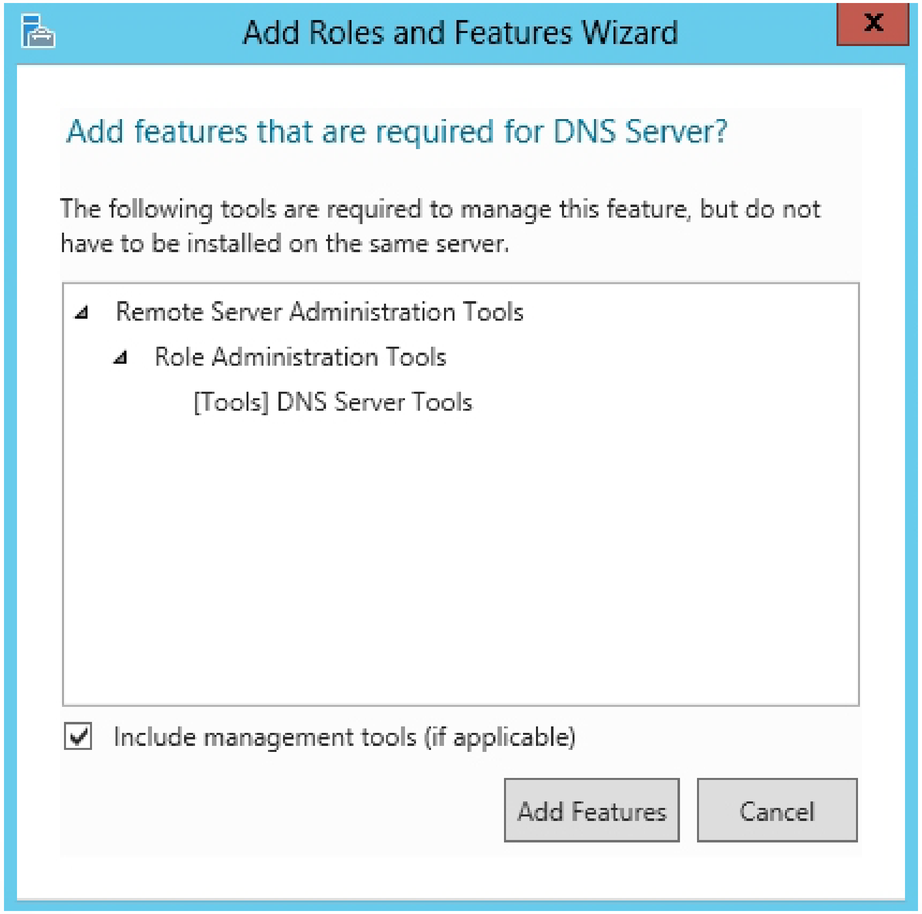
- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server
- □ Fax Server
- ☑ File And Storage Services (Installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.

Selecting DNS Server to install

Install DNS



Add Roles and Features Wizard

Add features that are required for DNS Server?

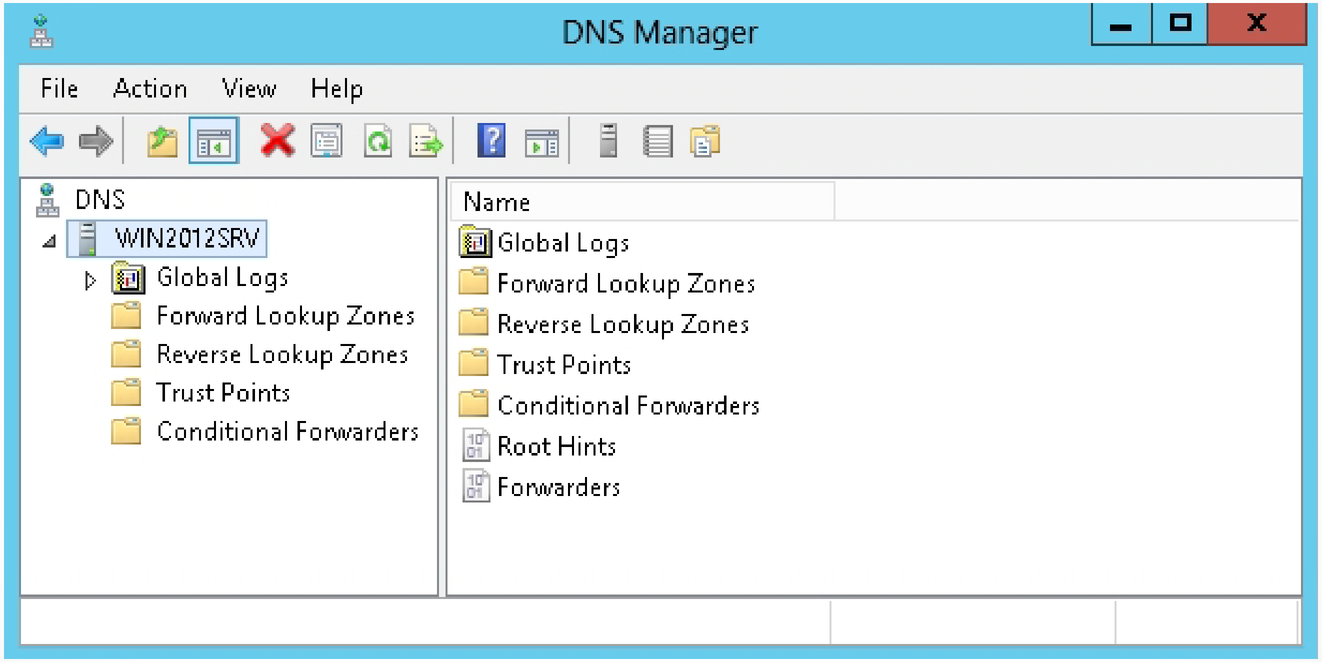
The following tools are required to manage this feature, but do not have to be installed on the same server.

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

☑ Include management tools (if applicable)

Adding roles and features

Install DNS



Viewing the DNS Manager console

Primary and Secondary Zones

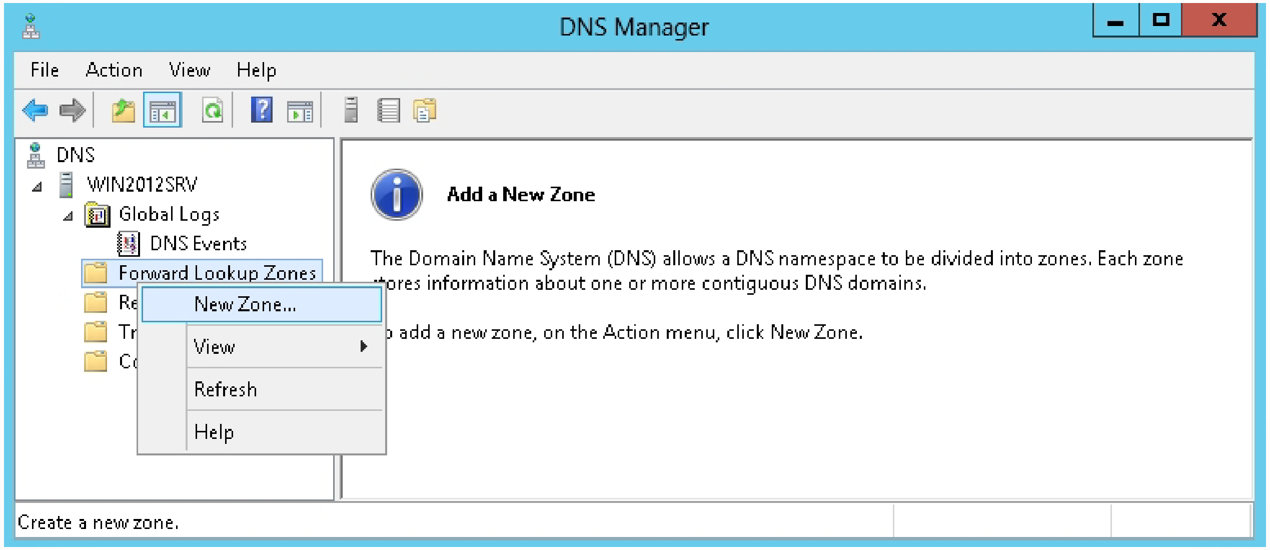
- **Primary zone**: Provides an authoritative, read-write copy of the zone.
- **Secondary zone**: Provides an authoritative, read-only copy of the primary zone.
- **Forward lookup zone**: Contains most of the resource records for a domain. Used primarily to resolve host names to IP addresses.
- **Reverse lookup zone**: Used to resolve IP addresses to host names.

Primary and Secondary Zones

A server can host all primary zones, all secondary zones, or a mix of primary and secondary zones as follows:

- **Primary name servers**: Servers that host primary zones.
- **Secondary name servers**: Servers that host secondary zones.

Create a Standard Forward Lookup Primary Zone



Add a New Zone

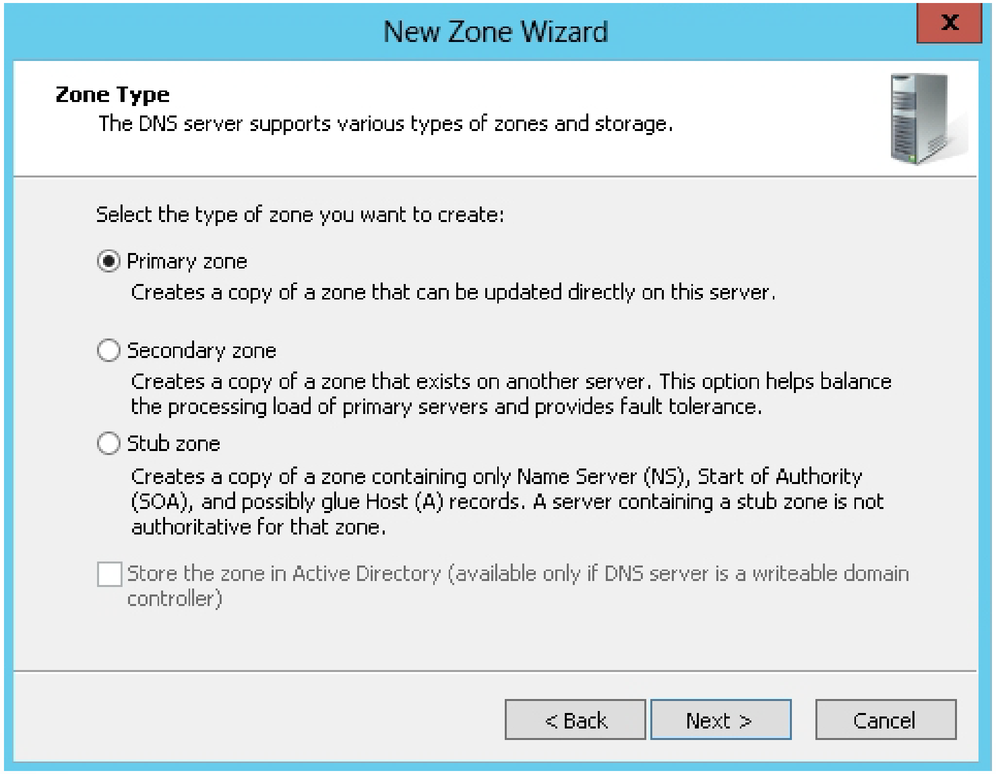
The Domain Name System (DNS) allows a DNS namespace to be divided into zones. Each zone stores information about one or more contiguous DNS domains.

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

Create a new zone.

Creating a new forward lookup zone

Create a Standard Forward Lookup Primary Zone



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.

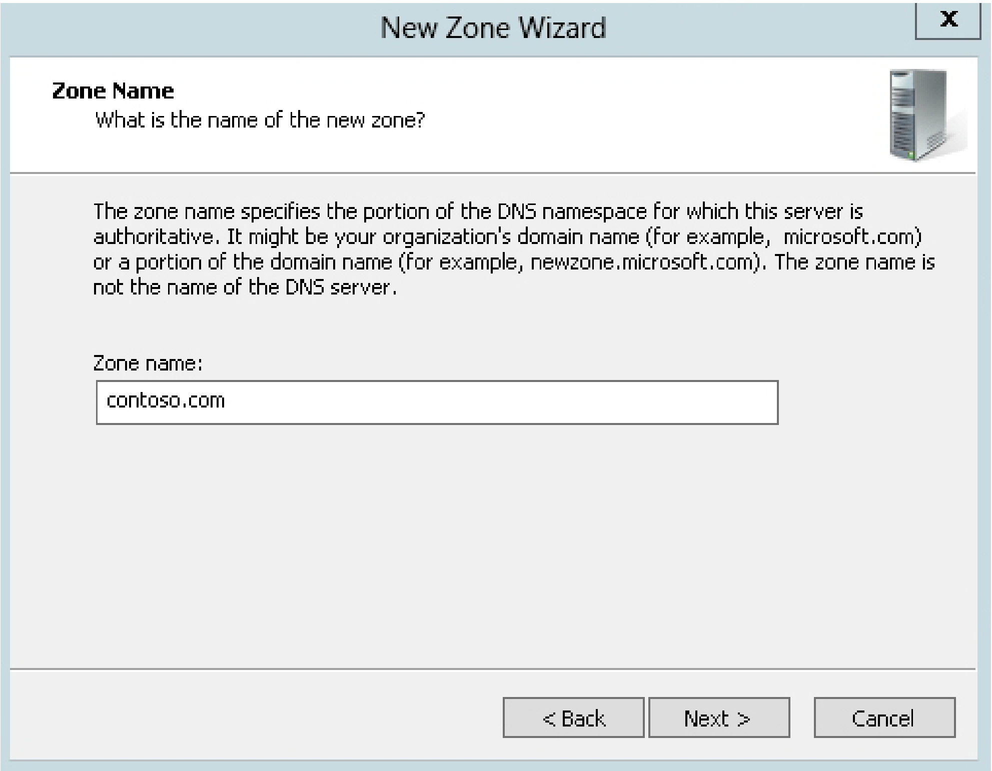
○ Stub zone

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)

Selecting the zone type

Create a Standard Forward Lookup Primary Zone



Zone Name

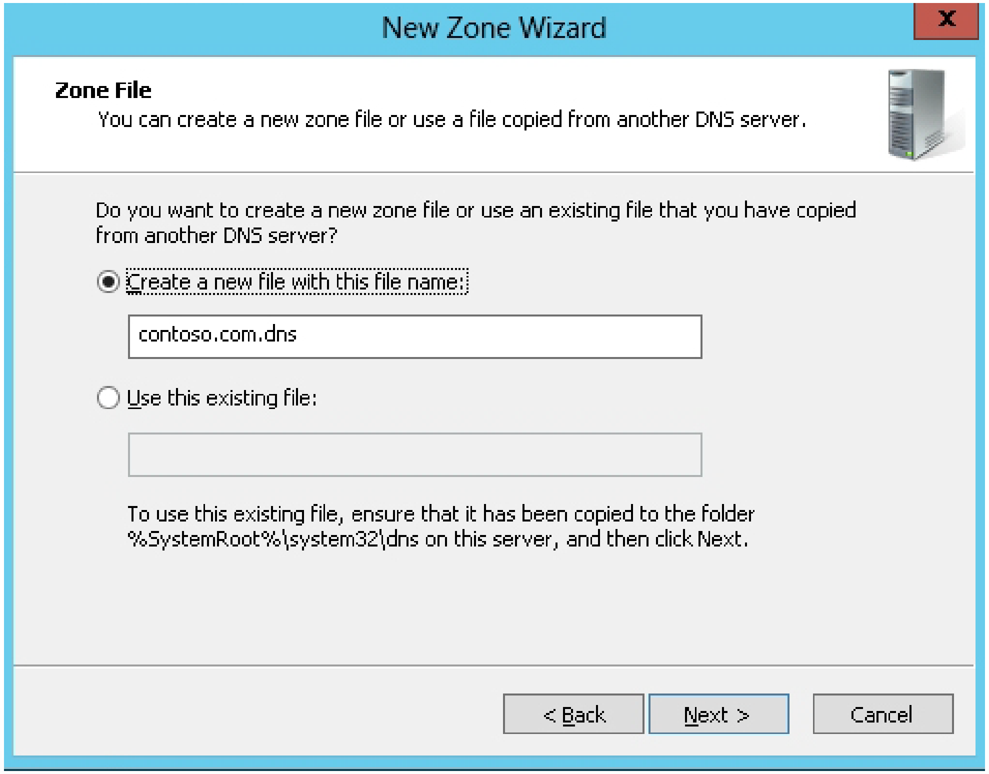
What is the name of the new zone?

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: contoso.com

Specifying the zone name

Create a Standard Forward Lookup Primary Zone



New Zone Wizard

Zone File

You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

● Create a new file with this file name:

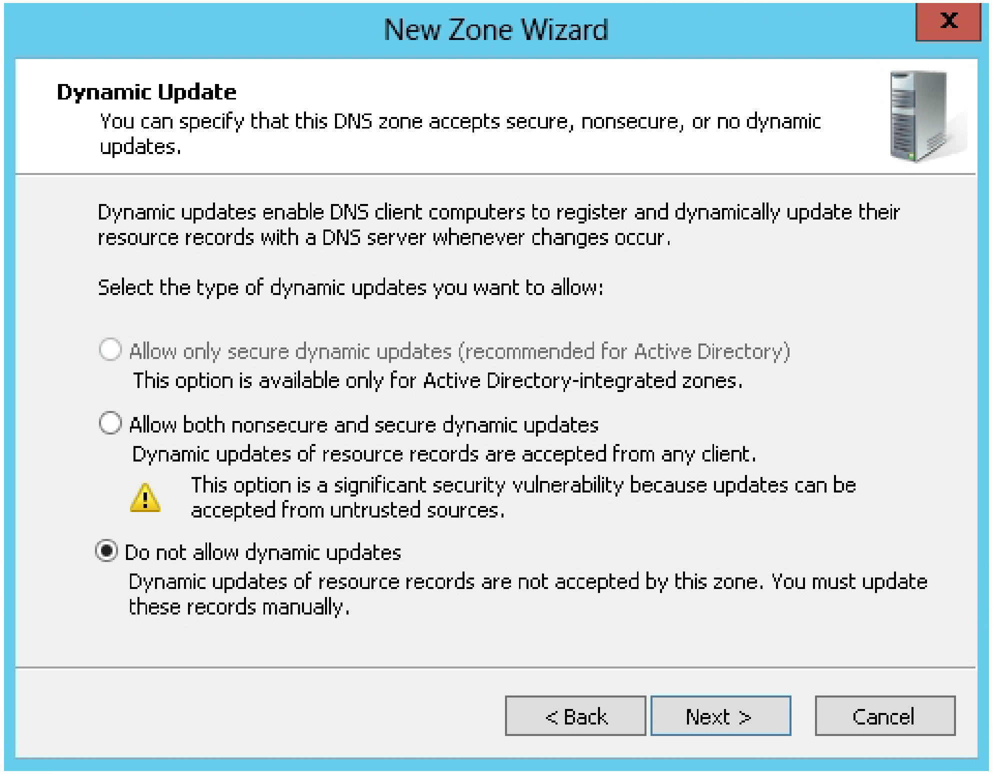
contoso.com.dns

○ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

Creating a zone file

Create a Standard Forward Lookup Primary Zone



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:

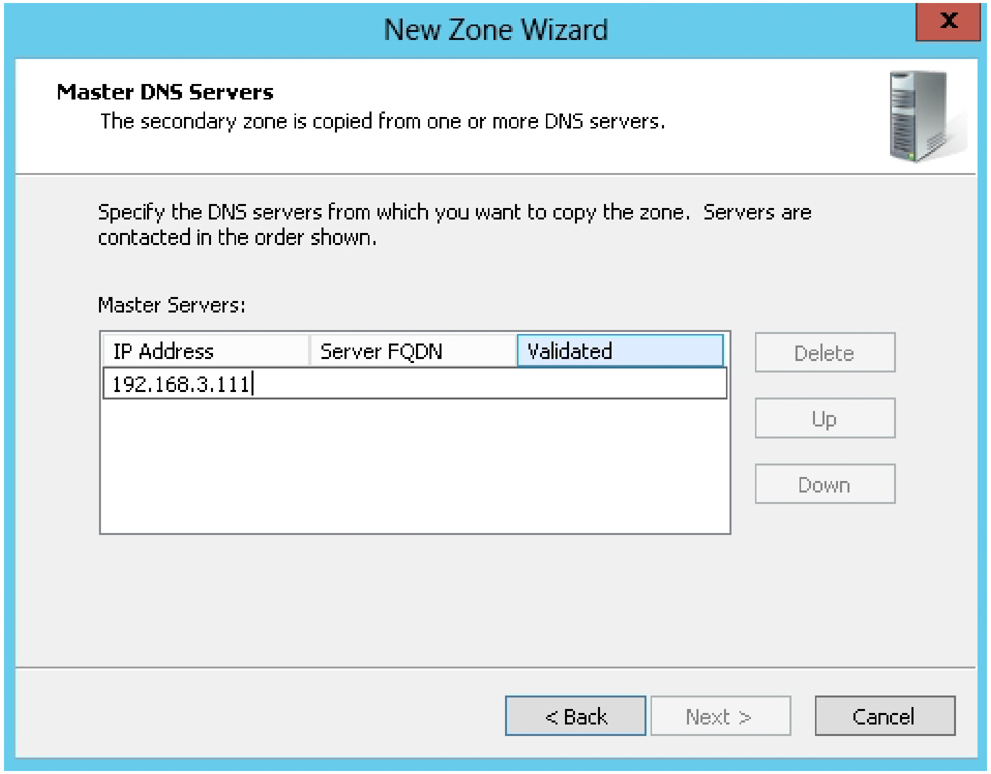
○ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ 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.

Specifying Dynamic Update settings

Create a Standard Forward Lookup Secondary Zone



New Zone Wizard

Master DNS Servers
The secondary zone is copied from one or more DNS servers.

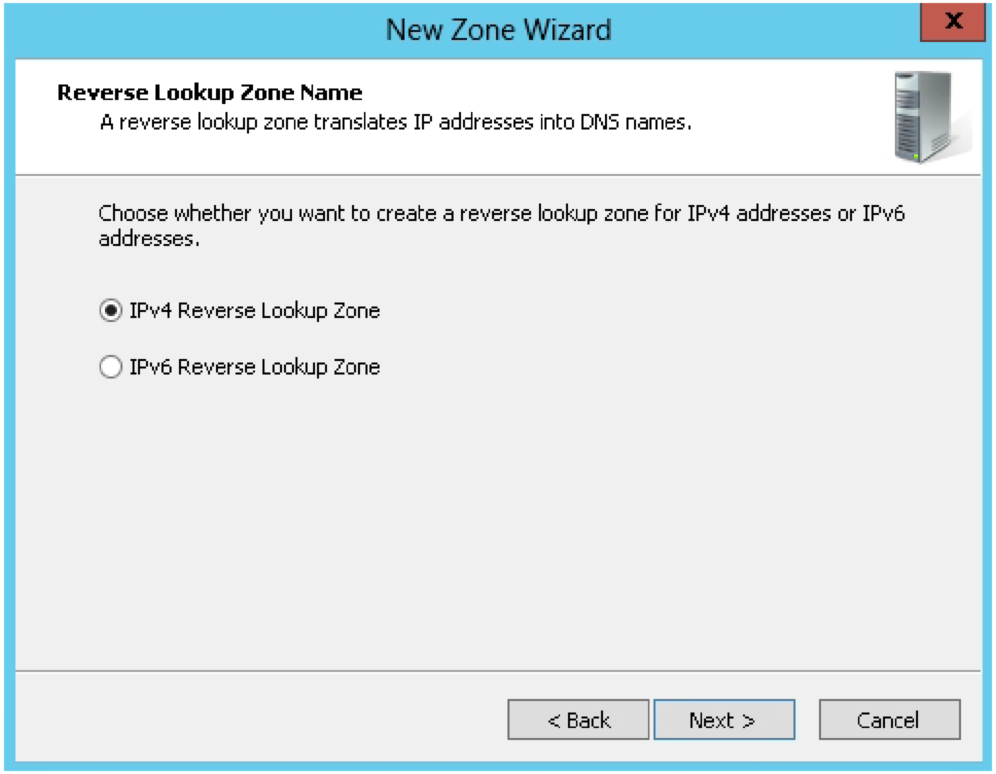
Specify the DNS servers from which you want to copy the zone. Servers are contacted in the order shown.

Master Servers:

IP Address	Server FQDN	Validated
192.168.3.111		

Entering the IP address on the Master DNS Servers page

Create a Standard Reverse Lookup Primary Zone for an IPv4 Subnet



Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

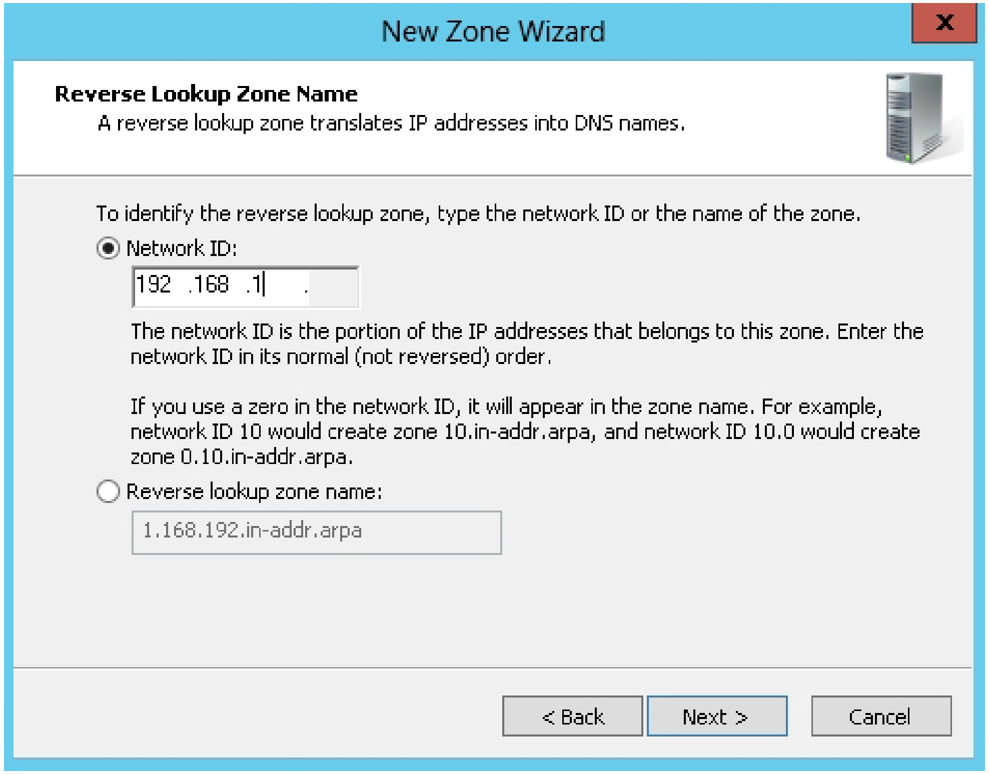
Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

● IPv4 Reverse Lookup Zone

○ IPv6 Reverse Lookup Zone

Selecting the IPv4 reverse lookup zone type

Create a Standard Reverse Lookup Primary Zone for an IPv4 Subnet



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:

192 .168 .1 .

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.

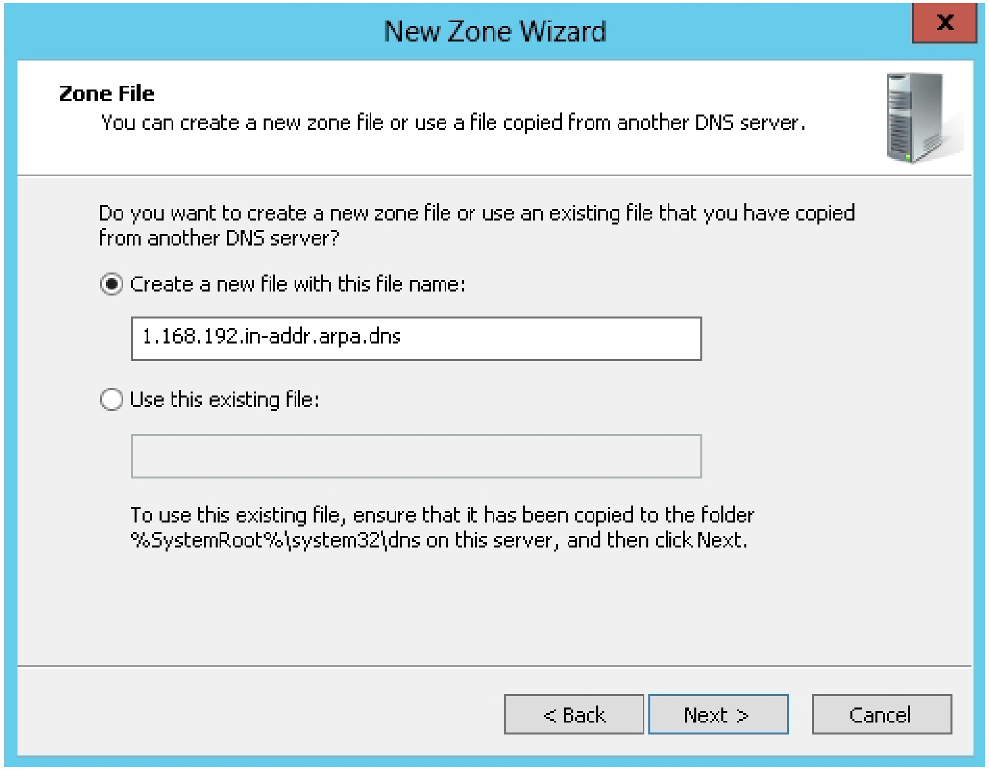
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

○ Reverse lookup zone name:

1.168.192.in-addr.arpa

Specifying the reverse lookup zone name

Create a Standard Reverse Lookup Primary Zone for an IPv4 Subnet



Zone File

You can create a new zone file or use a file copied from another DNS server.

Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

● Create a new file with this file name:

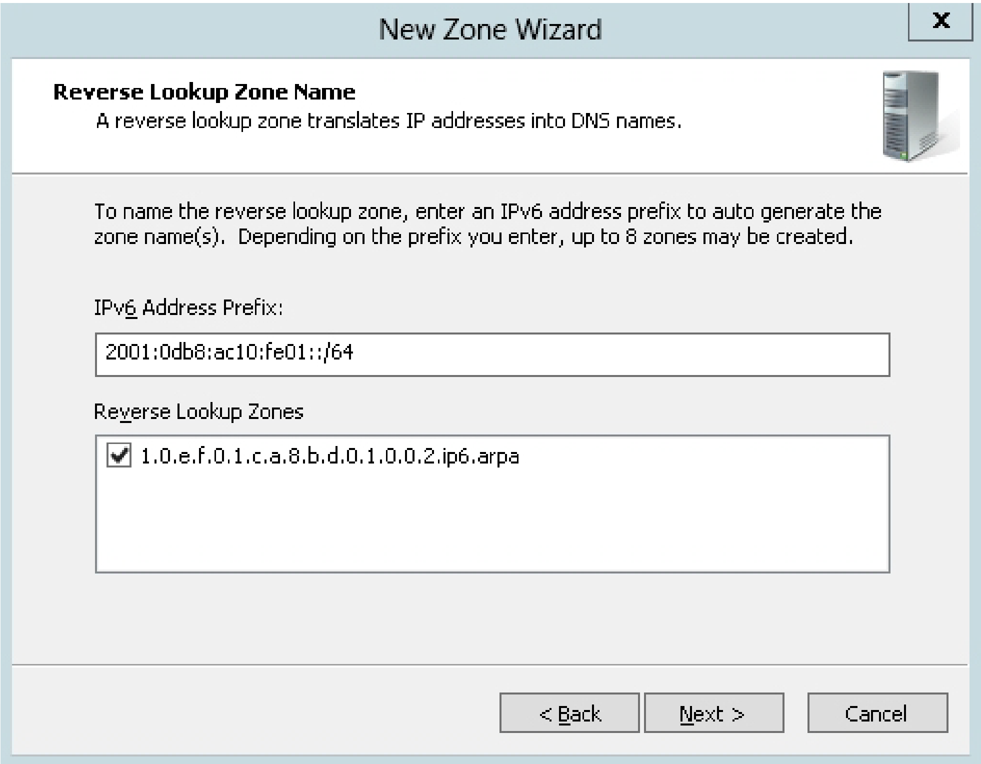
1.168.192.in-addr.arpa.dns

○ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

Specifying the Zone File page

Create a Standard Reverse Lookup Primary Zone for an IPv6 Subnet



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

To name the reverse lookup zone, enter an IPv6 address prefix to auto generate the zone name(s). Depending on the prefix you enter, up to 8 zones may be created.

IPv6 Address Prefix:

2001:0db8:ac10:fe01::/64

Reverse Lookup Zones

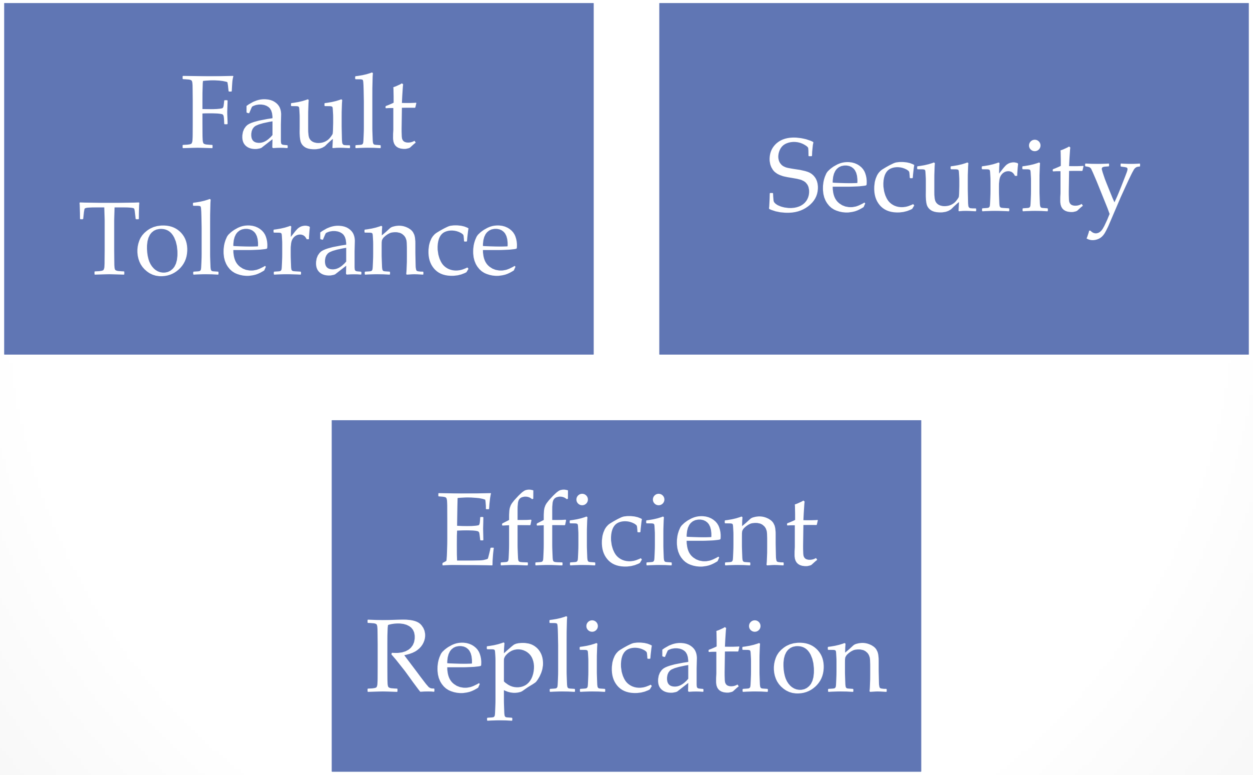
☑ 1.0.e.f.0.1.c.a.8.b.d.0.1.0.0.2.ip6.arpa

Specifying the reverse lookup zone name for IPv6

Active Directory-Integrated Zones

- DNS can be stored in and replicated with Active Directory, as an ***Active Directory-integrated zone***.
- By using Active Directory-integrated zones, DNS follows a multi-master model:
  - Each server enables all DNS servers to have authoritative read-write copies of the DNS zone.
- A change made on one DNS server replicates to other DNS servers.

Benefits of Using Active Directory to Store DNS



Fault Tolerance

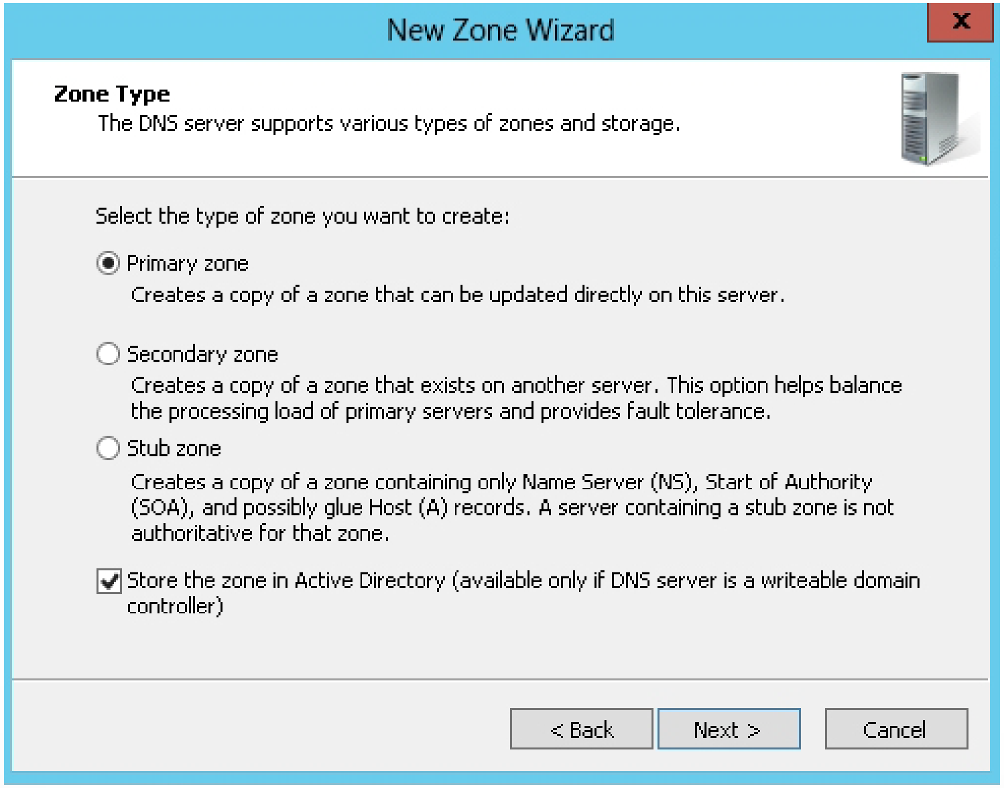
Security

Efficient Replication

Replication Scopes

- To all domain controllers in the domain
- To all domain controllers that are DNS servers in the local domain (default)
- To all domain controllers that are also DNS servers in the entire forest

Create an Active Directory-Integrated Standard Forward Lookup Primary Zone



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.

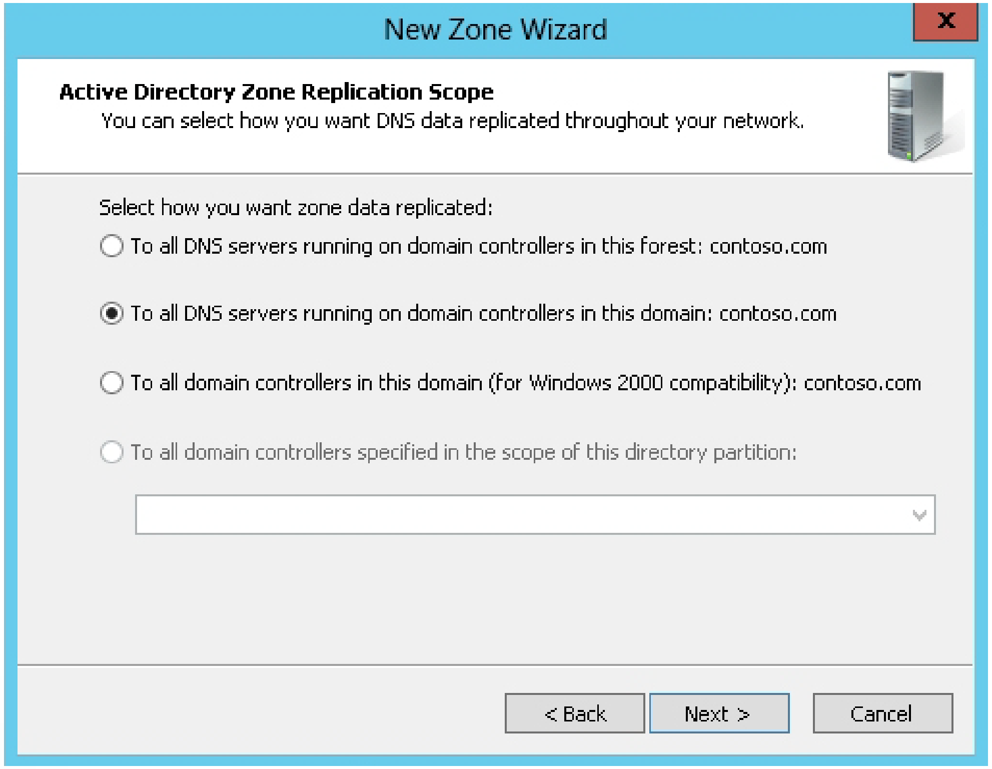
○ Stub zone

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)

Selecting the zone type

Create an Active Directory-Integrated Standard Forward Lookup Primary Zone



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: contoso.com

● To all DNS servers running on domain controllers in this domain: contoso.com

○ To all domain controllers in this domain (for Windows 2000 compatibility): contoso.com

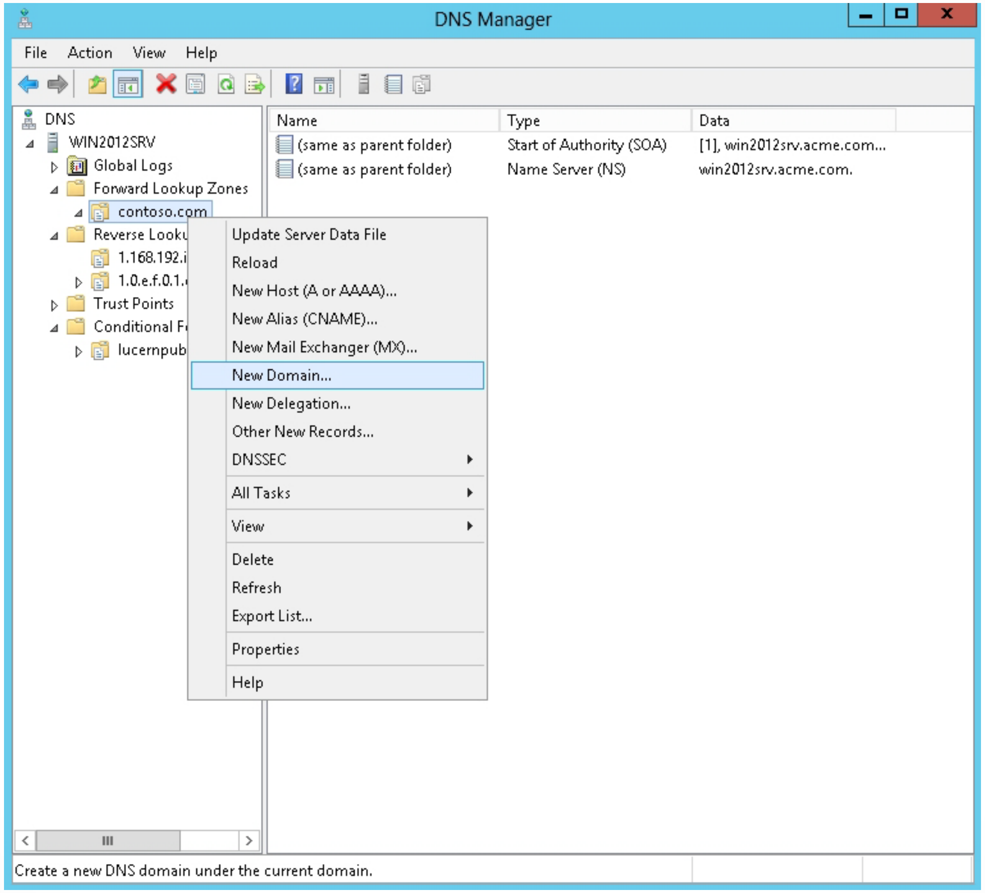
○ To all domain controllers specified in the scope of this directory partition:

Specifying the Active Directory zone replication scope

Configuring Zone Delegation

- A DNS ***subdomain*** is a child domain that is part of a parent domain and has the same domain suffix as the parent domain.
- Subdomains allow you to :
  - Assign unique names to be used by a particular department, subsidiary, function, or service within the organization.
  - Break up larger domains into smaller, more manageable domains.

Create a Subdomain

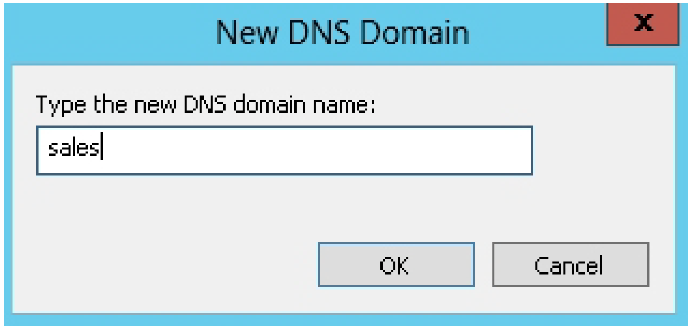


Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], win2012srv.acme.com...
(same as parent folder)	Name Server (NS)	win2012srv.acme.com.

Create a new DNS domain under the current domain.

Creating a new subdomain

Create a Subdomain

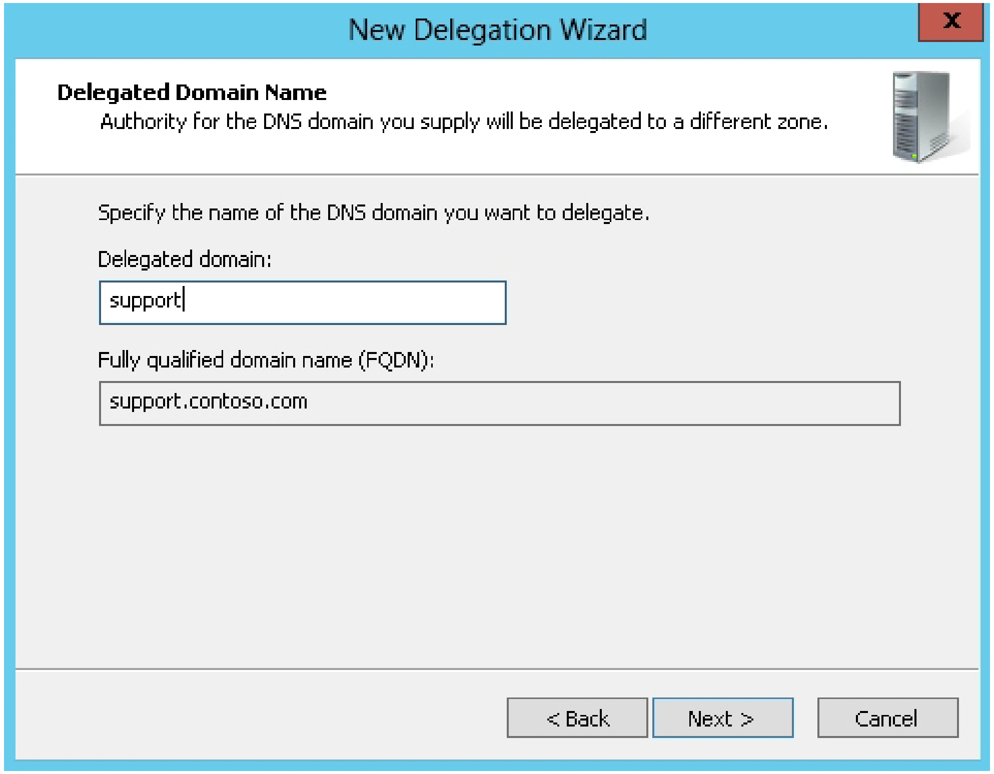


Type the new DNS domain name:

sales

Specifying the subdomain name

Delegate a DNS Domain



Delegated Domain Name

Authority for the DNS domain you supply will be delegated to a different zone.

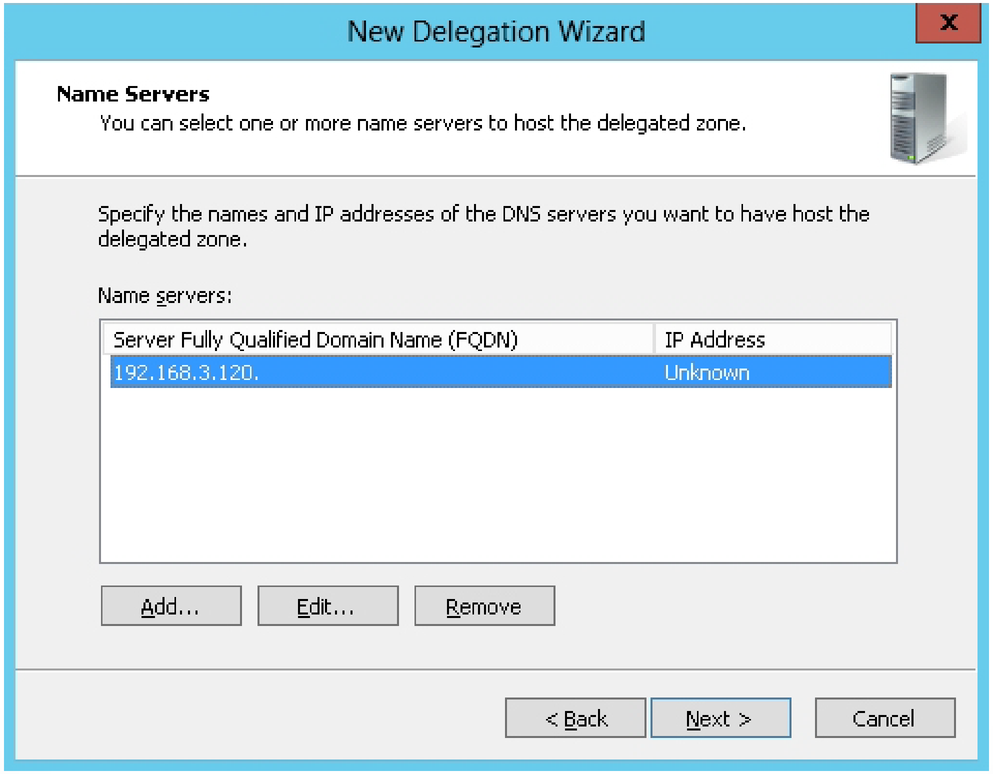
Specify the name of the DNS domain you want to delegate.

Delegated domain: support

Fully qualified domain name (FQDN): support.contoso.com

Entering the name of the delegated subdomain

Delegate a DNS Domain



New Delegation Wizard

Name Servers

You can select one or more name servers to host the delegated zone.

Specify the names and IP addresses of the DNS servers you want to have host the delegated zone.

Name servers:

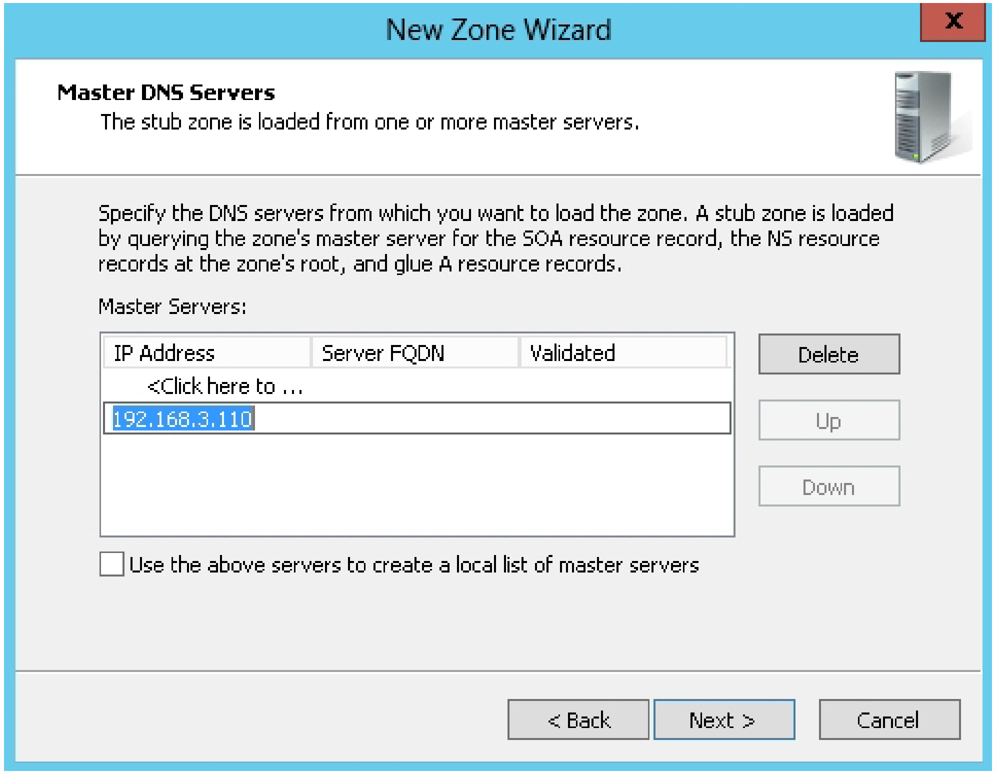
Server Fully Qualified Domain Name (FQDN)	IP Address
192.168.3.120.	Unknown

Specifying name servers for the delegated zone

Stub Zones

- A ***stub zone:***
  - Is a copy of a zone that contains only necessary resource records in the master zone and acts as a pointer to the authoritative name server.
  - Allows the server to forward queries to the name server that is authoritative for the master zone without going up to the root name servers and working its way down to the server.

Create a Stub Zone


New Zone Wizard

Master DNS Servers

The stub zone is loaded from one or more master servers.

Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.

Master Servers:

IP Address	Server FQDN	Validated
<Click here to ...		
192.168.3.110		

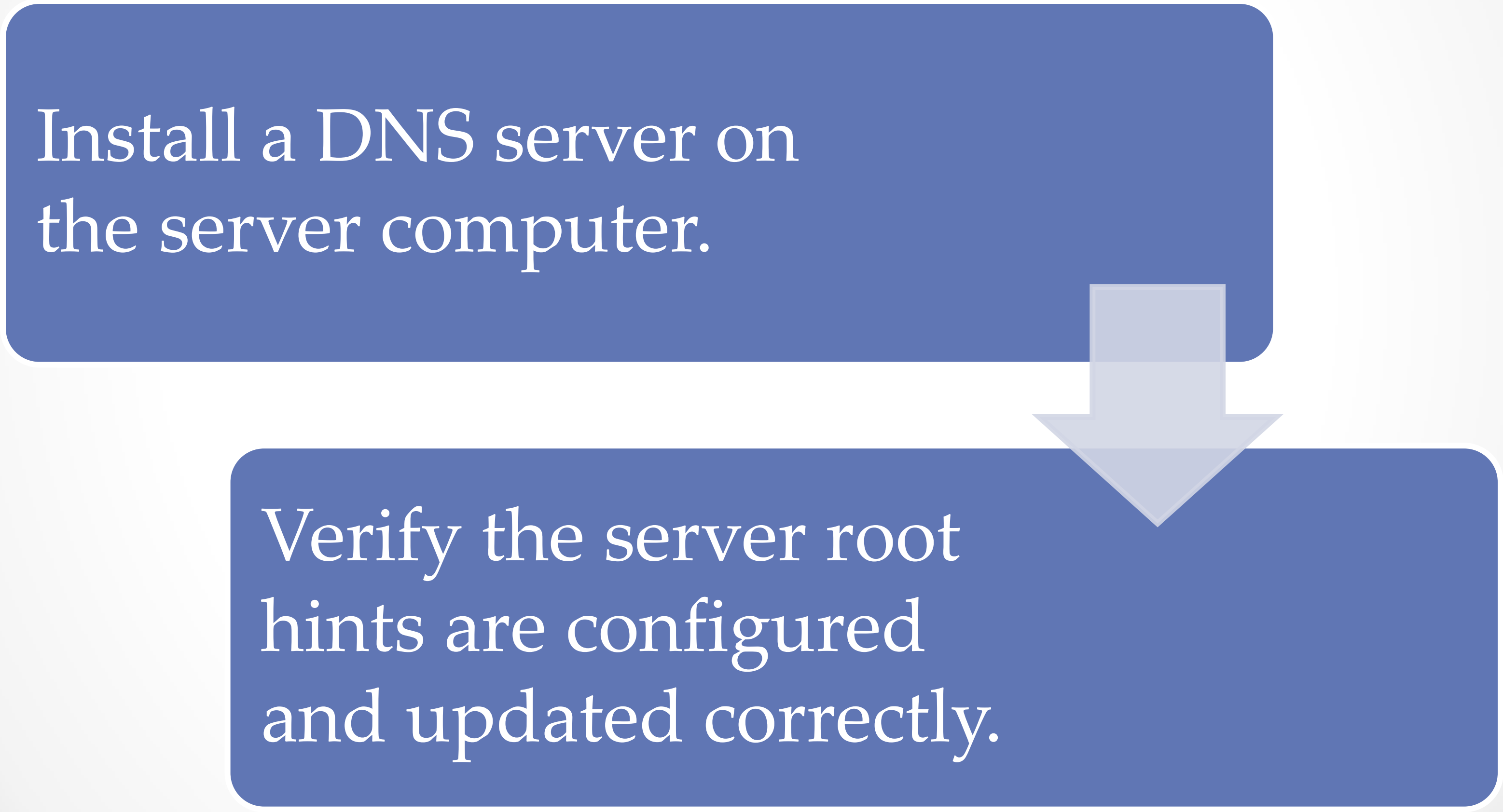
□ Use the above servers to create a local list of master servers

Specifying the master DNS server for a stub zone

Caching-Only Servers

- A ***caching-only server*** does not host any zones and is not authoritative for any domain.
- It receives client requests, and as the DNS servers fulfill DNS queries, the server adds the information to its cache.

Configuring Caching-Only Servers



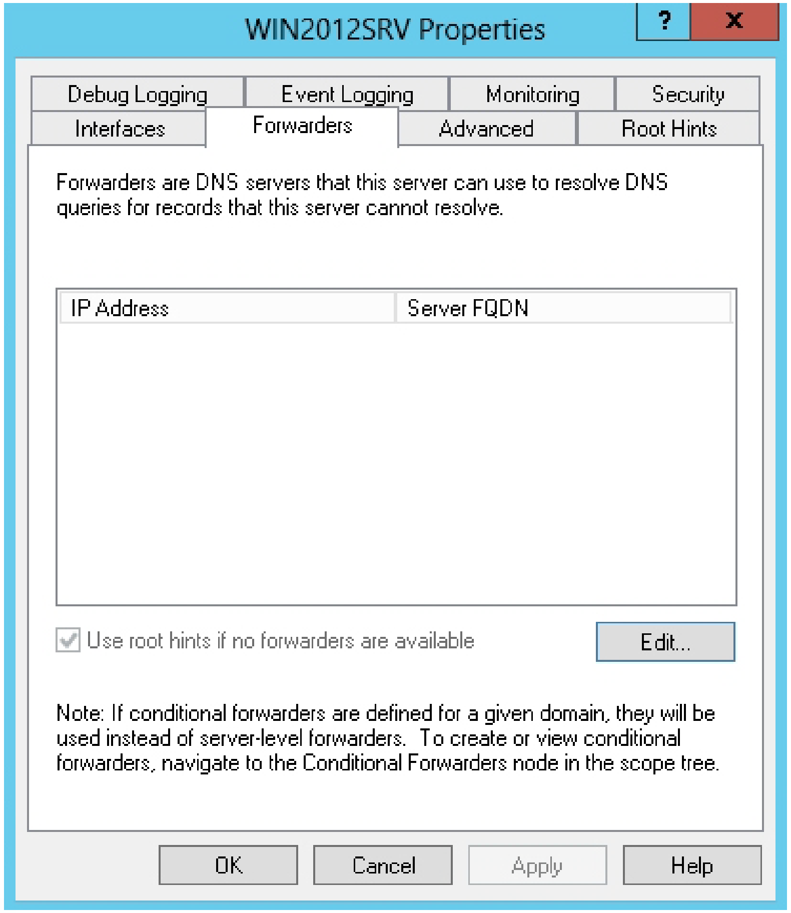
Install a DNS server on the server computer.

Verify the server root hints are configured and updated correctly.

Configuring Forwarding/ Conditional Forwarding

- When a client contacts a DNS server and the DNS server does not know the answer, it performs an iterative query to find the answer.
- DNS servers can be configured to be forwarded to another DNS server or a conditional forwarder based on the domain name queried.
- A ***forwarder*** controls name resolution queries and traffic.
  - Can improve the efficiency of name resolution on a network.

Configure Forwarders



Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

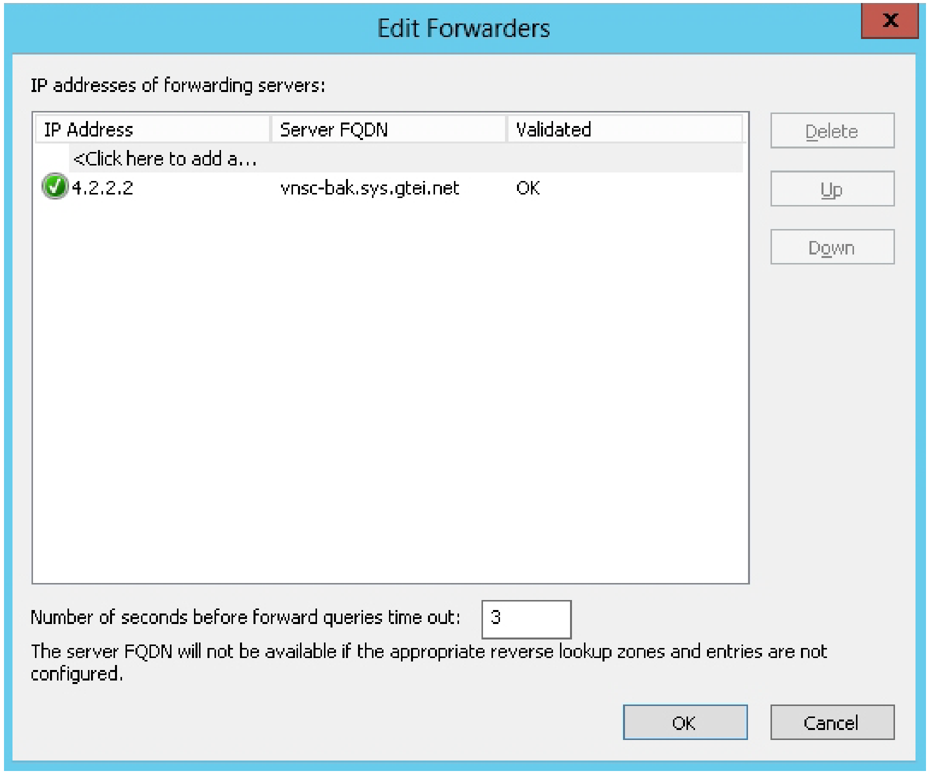
IP Address	Server FQDN

☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

Selecting the Forwarders tab

Configure Forwarders



Edit Forwarders

IP addresses of forwarding servers:

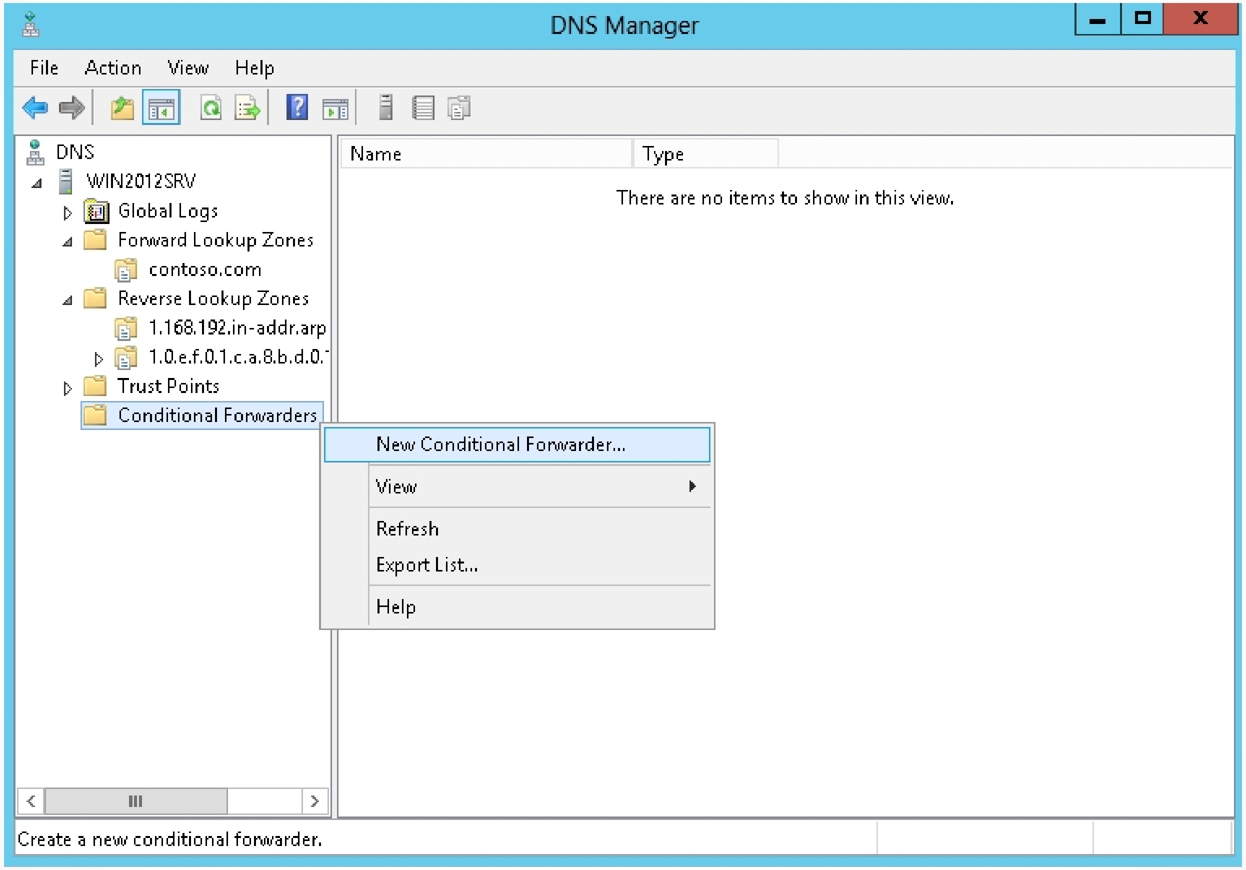
IP Address	Server FQDN	Validated
<Click here to add a...		
✓ 4.2.2.2	vnsc-bak.sys.gtei.net	OK

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.

Modifying the Forwarders list

Configure Conditional Forwarders

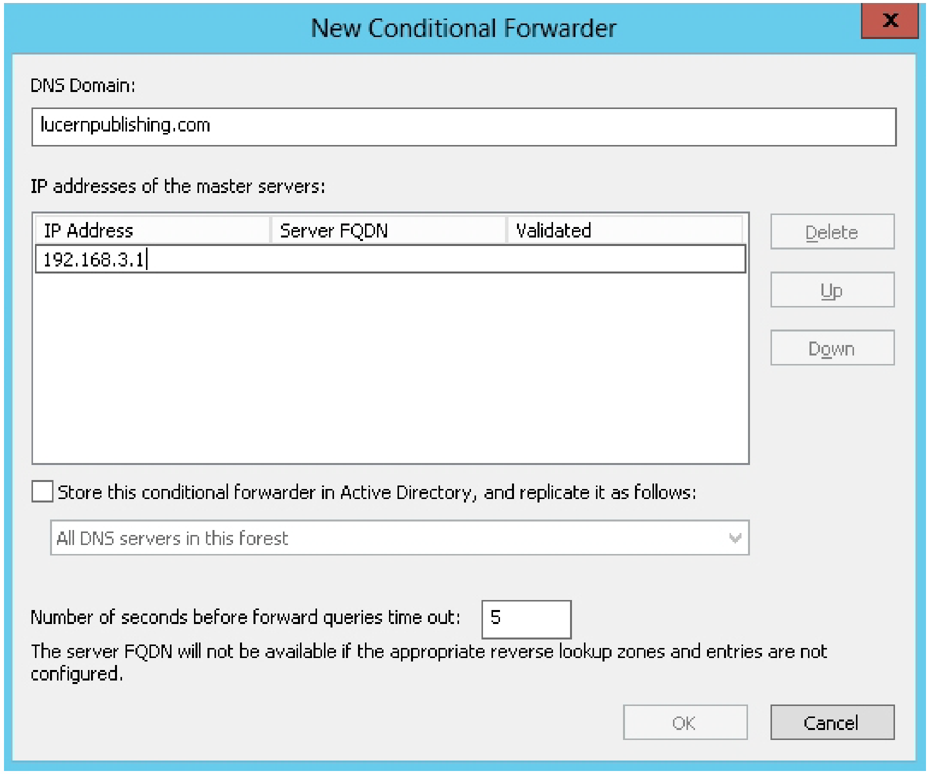


There are no items to show in this view.

Create a new conditional forwarder.

Creating a conditional forwarder

Configure Conditional Forwarders



New Conditional Forwarder

DNS Domain: lucernpublishing.com

IP addresses of the master servers:

IP Address	Server FQDN	Validated
192.168.3.1		

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

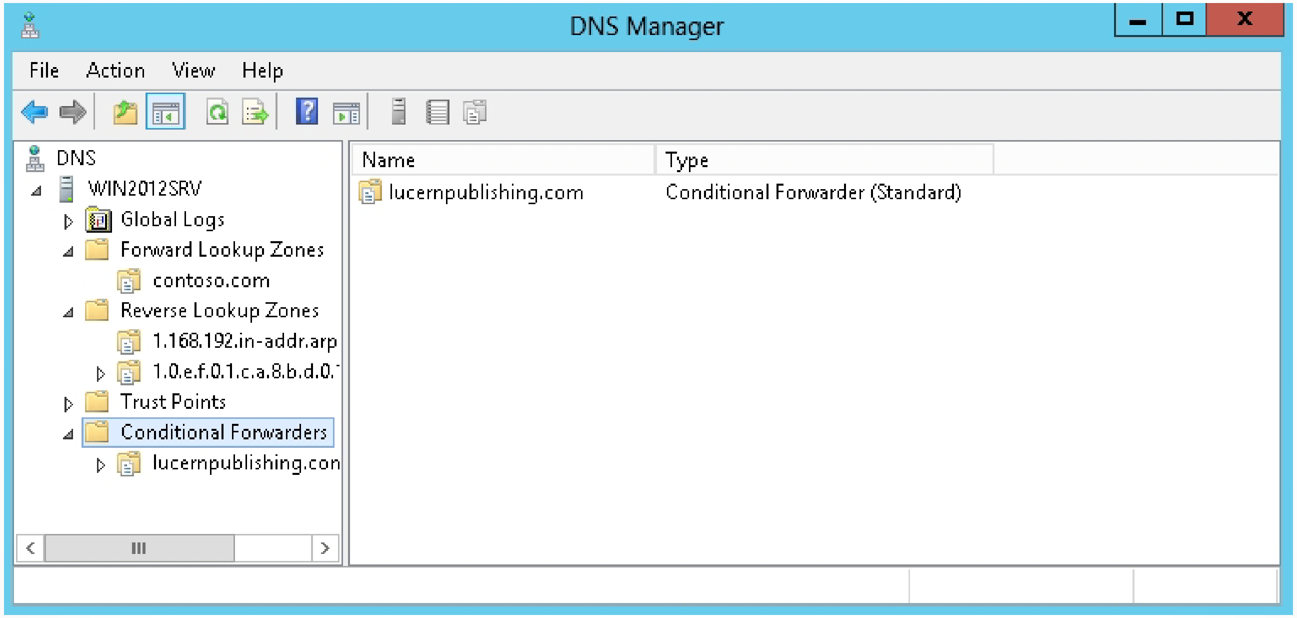
All DNS servers in this forest

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.

Identifying the name and IP address of a conditional forwarder

Configure Conditional Forwarders



Name	Type
lucernpublishing.com	Conditional Forwarder (Standard)

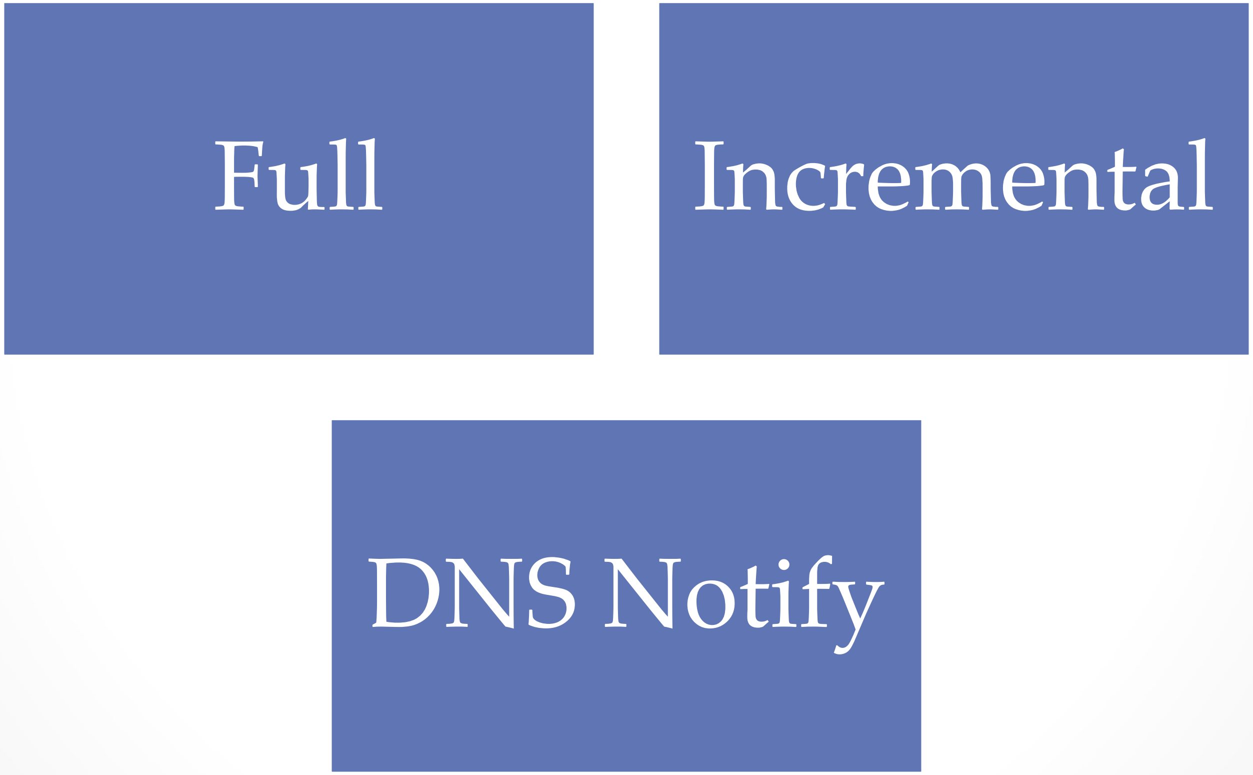
Viewing the conditional forwarders

Zone Transfers

Events that trigger a zone transfer:

- The initial transfer occurs when a secondary zone is created.
- The zone refresh interval expires.
- The DNS Server service is started at the secondary server.
- The master server notifies the secondary server that changes have been made to a zone.

Three Types of Zone Transfers

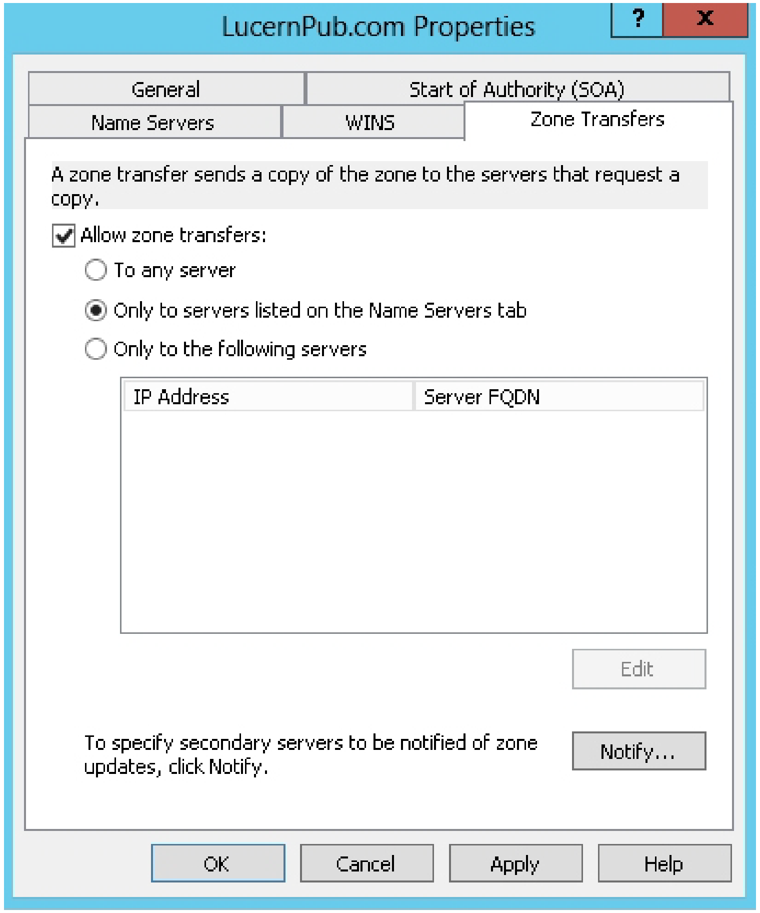


Full

Incremental

DNS Notify

Configure Zone Transfer Settings



LucernPub.com Properties

A zone transfer sends a copy of the zone to the servers that request a copy.

☑ Allow zone transfers:

○ To any server

● Only to servers listed on the Name Servers tab

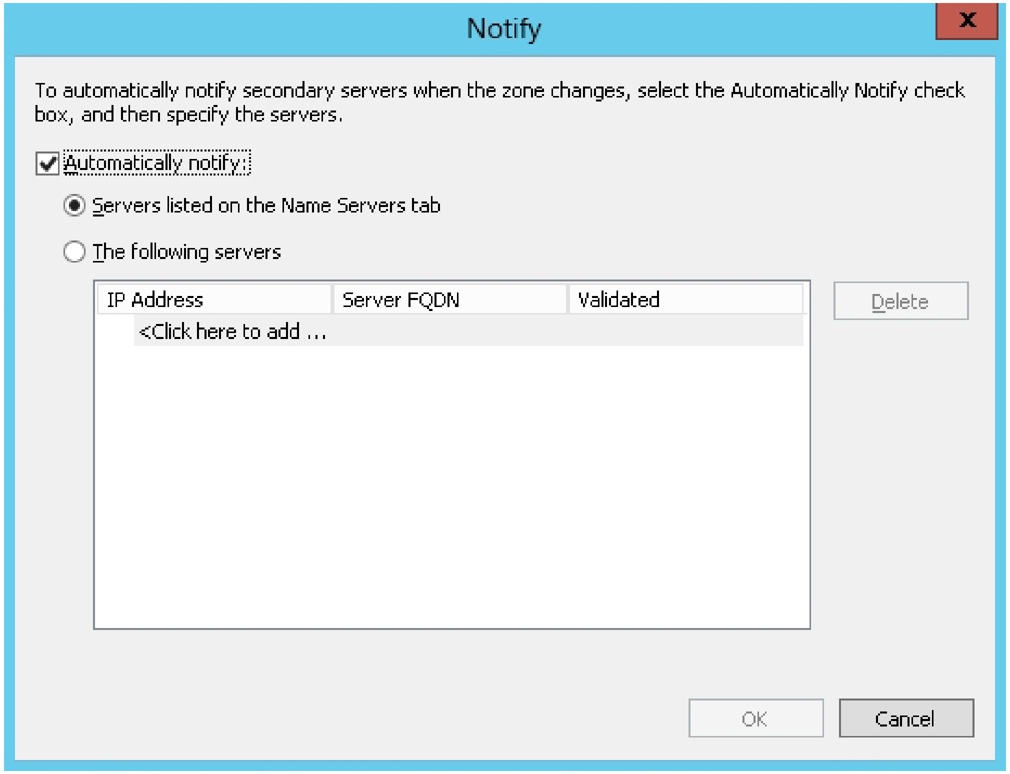
○ Only to the following servers

IP Address	Server FQDN

To specify secondary servers to be notified of zone updates, click Notify.

Viewing the Zone Transfers tab

Configure Zone Transfer Settings



Notify

To automatically notify secondary servers when the zone changes, select the Automatically Notify check box, and then specify the servers.

☑ Automatically notify:

● Servers listed on the Name Servers tab

○ The following servers

IP Address	Server FQDN	Validated
<Click here to add ...		

Configuring Notify options in the Notify dialog box

Using the Dnscmd Command to Manage Zones

• • •

Lesson 8: Configuring DNS Zones

dnscmd.exe Command

- Create, delete, and view zones and records
- Reset server and zone properties
- Perform zone maintenance operations, such as updating the zone, reloading the zone, refreshing the zone, writing the zone back to a file or to Active Directory, and pausing or resuming the zone
- Clear the cache
- Stop and start the DNS service
- View statistics

dnscmd.exe Examples

To view the zones on a DNS server called server1.contoso.com:

```
dnscmd server1.contoso.com /enumzones
```

To add an Active Directory-integrated primary zone called support.contoso.com on server1.contoso.com, execute the following command:

```
dnscmd server1.contoso.com /zoneadd
support.contoso.com /dsprimary
```

dnscmd.exe Examples

To create a secondary zone called support.contoso.com on server1.contoso.com, perform the following command from the primary zone located at 10.0.0.2:

```
dnscmd server1.contoso.com /zoneadd
support.contoso.com /secondary 10.0.0.2
```

To delete the secondary zone called support.contoso.com:

```
dnscmd server1.contoso.com /zonedelete
support.contoso.com
```

Lesson Summary

- Domain Name System (DNS) is a naming service used by TCP/IP network and is an essential service used by the Internet. DNS servers are often referred to as name servers.
- Each node or leaf in the tree is a resource record (RR), which holds information associated with the domain name.
- The primary zone provides an authoritative, read-write copy of the zone while the secondary zone provides an authoritative, read-only copy of the primary zone.
- A forward lookup zone contains most of the resource records for a domain and is used primarily to resolve host names to IP addresses.
- A reverse lookup zone is used to resolve IP addresses to host names.
- Today, DNS can be stored in and replicated with Active Directory as an Active Directory-integrated zone.
- A stub zone is a copy of a zone that contains only necessary resource records (SOA, NS, and an A record) in the master zone and acts as a pointer to authoritative name server.

Lesson Summary

- A forwarder helps control name resolution queries and traffic, which can improve the efficiency of name resolution for the computers in your network.
- Conditional forwarding expands on the idea of forwarding, where you forward those queries to other DNS servers based on the DNS domain names in the query.
- Zone transfers are the complete or partial transfer of DNS data from a zone on a DNS server to another DNS server.
- A full zone transfer (AXFR), which copies the entire zone, is used when you first bring a new DNS secondary server online for an existing zone. With large zones, full transfers can be very time-consuming and resource extensive.
- An incremental zone transfer (IXFR) retrieves only resource records that have changed within a zone.
- The DNS Notify method allows the primary DNS server to use a "push" mechanism to notify secondary servers that it has been updated and that the resource records need to be transferred.
- The `dnscmd.exe` command allows an administrator to display and change properties of the DNS servers, zones, and resource records.