WILEY

SYBEX
A Wiley Brand

MCA: Windows Server Hybrid Administrator Study Guide: AZ-800 & AZ-801

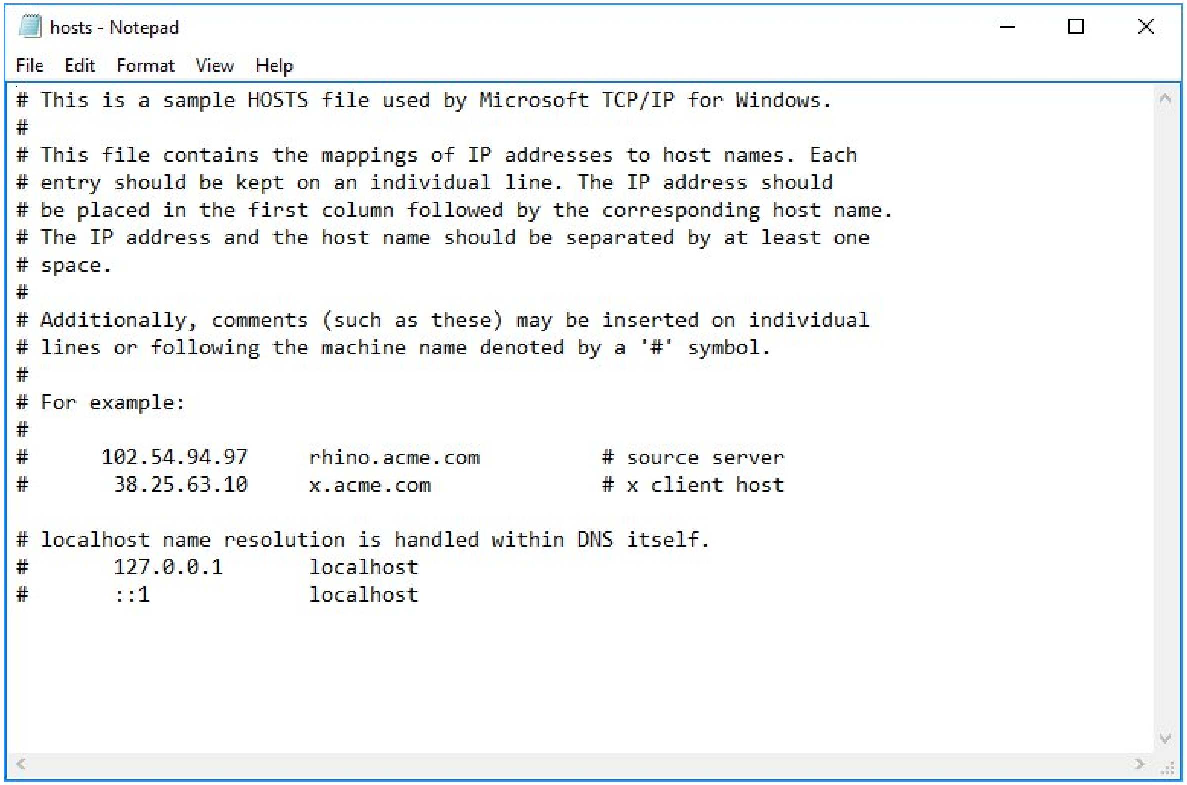
Chapter 5: Implementing DNS

Introduction to DNS

- The Domain Name System (DNS) is a service designed to resolve Internet Protocol (IP) addresses to and from hostnames.
- An IP address is a logical number that uniquely identifies a computer on a TCP/IP network.

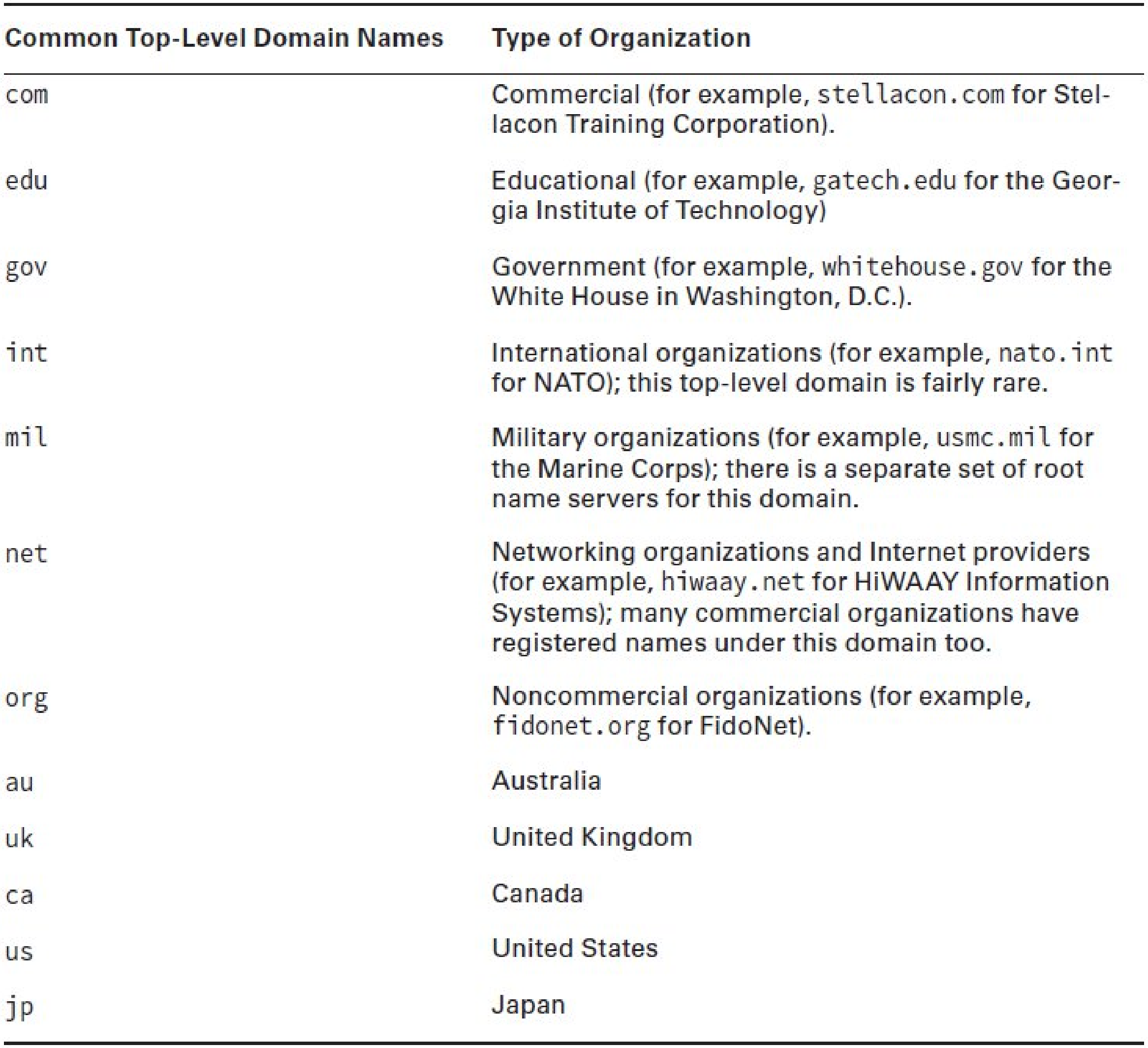
HOSTS File

- In order to resolve friendly names (hostnames) to TCP/IP addresses that the network stack can use, you must have some method for mapping them.
- Originally, ASCII flat files (often called HOSTS file) were used for this purpose.



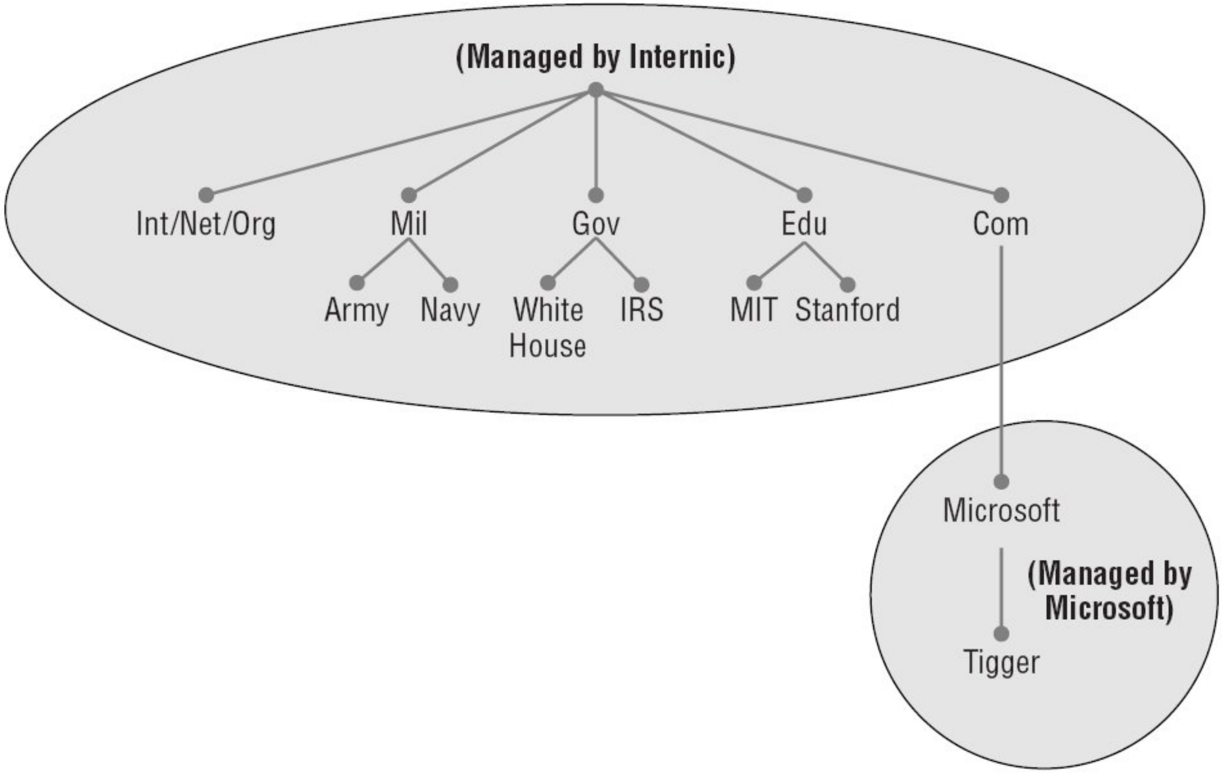
```
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

Common Top-Level DNS Domains



Common Top-Level Domain Names	Type of Organization
com	Commercial (for example, stellacon.com for Stellacon Training Corporation).
edu	Educational (for example, gatech.edu for the Georgia Institute of Technology)
gov	Government (for example, whitehouse.gov for the White House in Washington, D.C.).
int	International organizations (for example, nato.int for NATO); this top-level domain is fairly rare.
mil	Military organizations (for example, usmc.mil for the Marine Corps); there is a separate set of root name servers for this domain.
net	Networking organizations and Internet providers (for example, hiwaay.net for HiWAAY Information Systems); many commercial organizations have registered names under this domain too.
org	Noncommercial organizations (for example, fidonet.org for FidoNet).
au	Australia
uk	United Kingdom
ca	Canada
us	United States
jp	Japan

The DNS Hierarchy



Understanding Servers, Clients, and Resolvers

- DNS Server
  - Any computer providing domain name services is a DNS name server.
- DNS Clients
  - A DNS client is any machine issuing queries to a DNS server.
- DNS Resolvers
  - Resolvers are software processes, sometimes implemented in software libraries, that handle the actual process of finding the answers to queries for DNS data.
- Query
  - A request for information that is sent to a DNS server for address resolution (examples include recursive, inverse, and iterative queries).

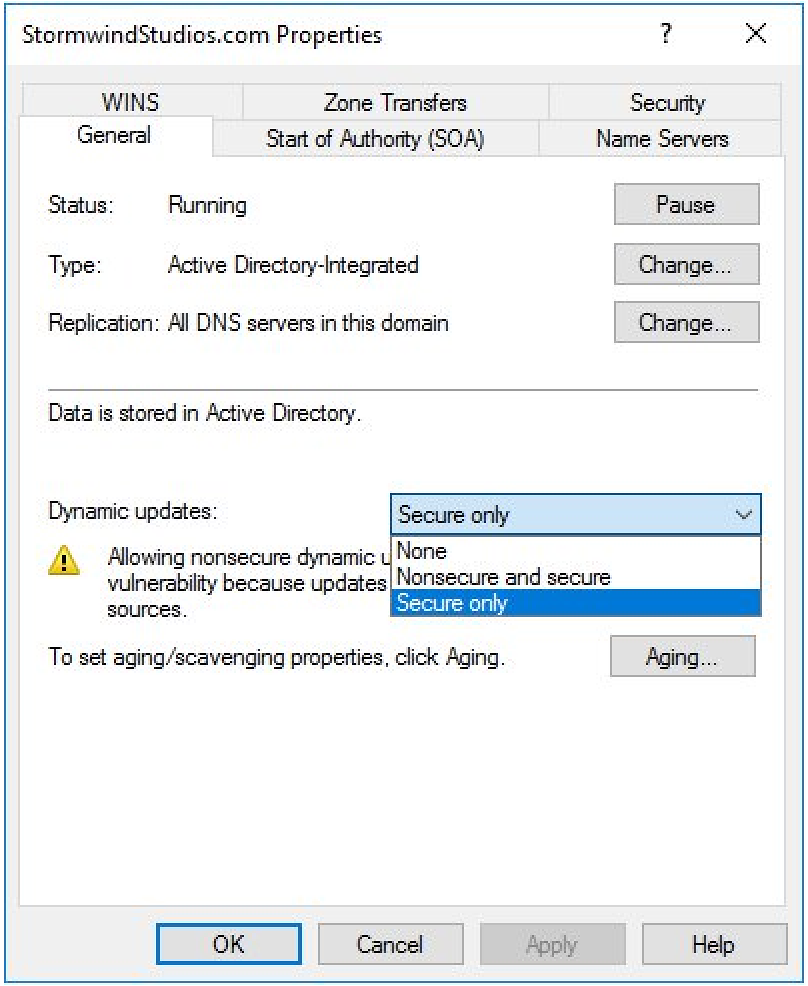
Dynamic DNS vs. Non-Dynamic DNS

- Dynamic DNS (DDNS)
  - Described in RFC 2136, allows DNS clients to automatically update information in the DNS database files (i.e. Windows 2022 DHCP server updates DNS with IP addresses)
- Non-Dynamic DNS (NDDNS)
  - Does not automatically populate the DNS database (records are typically updated manually).

Dynamic DNS (DDNS) Options (1/2)

- When setting up dynamic updates on your DNS server, you have three options
  - None
    - This means your DNS server is Non-Dynamic.
  - Nonsecure and secure
    - This means that any machine (even if it does not have a domain account) can register with DNS. Using this setting could allow rogue systems to enter records into your DNS server.
  - Secure only
    - This means that only machines with accounts in Active Directory can register with DNS. Before DNS registers any account in its database, it checks Active Directory to make sure that account is an authorized domain computer.

Dynamic DNS (DDNS) Options (2/2)



StormwindStudios.com Properties

Status: Running

Type: Active Directory-Integrated

Replication: All DNS servers in this domain

Data is stored in Active Directory.

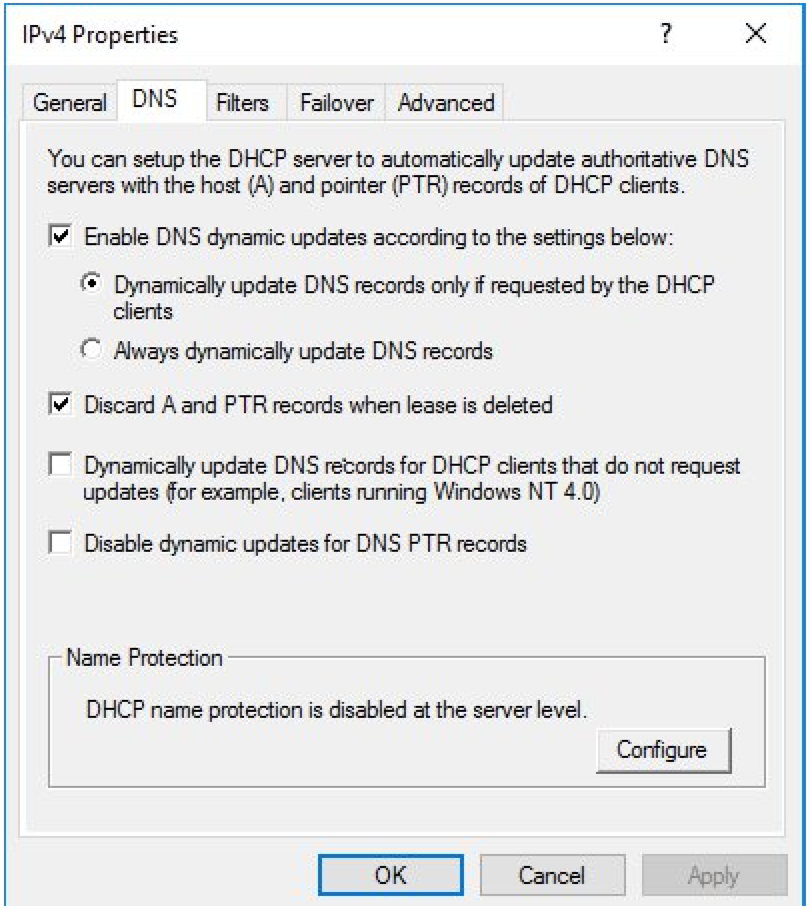
Dynamic updates: Secure only

Allowing nonsecure dynamic u vulnerability because updates sources.

To set aging/scavenging properties, click Aging.

How DNS Dynamically Updates

- Static – administrators manually enter the TCP/IP information into the database.
- Dynamic (using DHCP) – DHCP sends any new IP address/machine name combination to the DNS database.



You can setup the DHCP server to automatically update authoritative DNS servers with the host (A) and pointer (PTR) records of DHCP clients.

☑ Enable DNS dynamic updates according to the settings below:

● Dynamically update DNS records only if requested by the DHCP clients

○ Always dynamically update DNS records

☑ Discard A and PTR records when lease is deleted

□ Dynamically update DNS records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0)

□ Disable dynamic updates for DNS PTR records

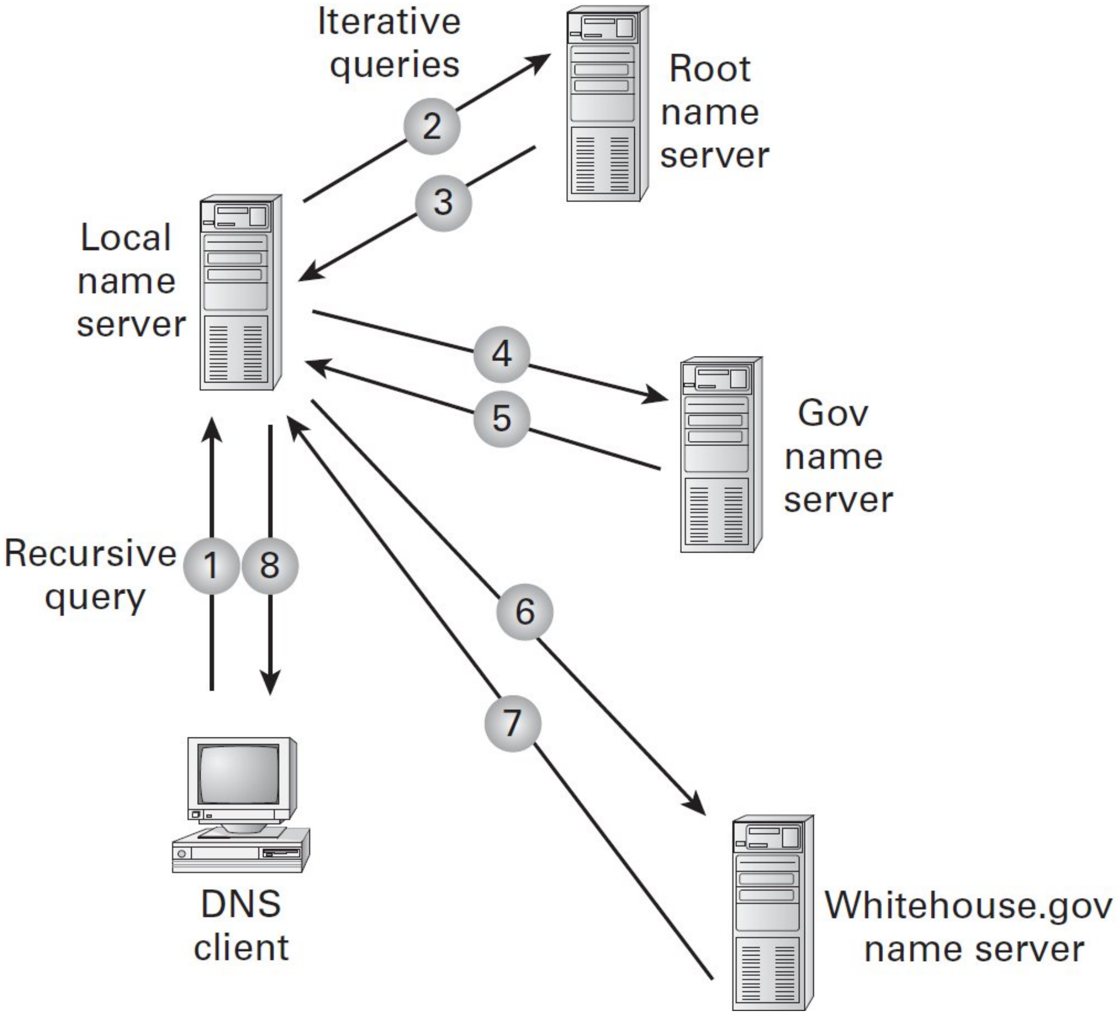
Name Protection

DHCP name protection is disabled at the server level.

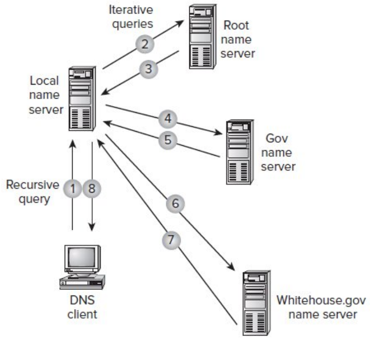
DNS Queries

- Iterative queries
  - A client asks the DNS server for an answer, and the server returns the best answer
  - The server never sends out an additional query in response to an iterative query
  - If the server doesn’t know the answer, it may direct the client to another server through a referral
- Recursive queries
  - In a recursive query, the client sends a query to a name server, asking it to respond either with the requested answer or with an error message
  - The error states one of two things:
    - The server can’t come up with the right answer
    - The domain name doesn’t exist
- Inverse queries
  - Inverse queries use PTR records
  - Instead of supplying a name and then asking for an IP address, the client first provides the IP address and then asks for the name

DNS - Iterative Queries



Iterative Queries



Here's what happens to resolve the request:

1. The resolver sends a recursive DNS query to its local DNS server asking for the IP address of www.whitehouse.gov. The local name server is responsible for resolving the name, and it cannot refer the resolver to another name server.
2. The local name server checks its zones, and it finds no zones corresponding to the requested domain name.
3. The root name server has authority for the root domain and will reply with the IP address of a name server for the .gov top-level domain.
4. The local name server sends an iterative query for www.whitehouse.gov to the Gov name server.
5. The Gov name server replies with the IP address of the name server servicing the whitehouse.gov domain.
6. The local name server sends an iterative query for www.whitehouse.gov to the whitehouse.gov name server.
7. The whitehouse.gov name server replies with the IP address corresponding to www.whitehouse.gov.
8. The local name server sends the IP address of www.whitehouse.gov back to the original resolver.

Queries

- Inverse query - uses pointer (PTR) records. Instead of supplying a name and then asking for an IP address, the client first provides the IP address and then asks for the name.
- Recursive query – The name server may be required to send out several queries to find the definitive answer. Name servers, acting as resolvers, are allowed to cache all of the received information during this process; each record contains information called *time to live (TTL)*. The TTL specifies how long the record will be held in the local cache until it must be resolved again.

Choosing Appropriate TTL Values

Choosing an appropriate TTL depends on a number of factors, including the following:

- Amount of change anticipated for the records within the zone.
- Amount of time that can withstand an outage that might require changing an IP address.
- Amount of traffic that you believe the DNS server can handle.

Primary DNS Zone (1/2)

- The primary zone is responsible for maintaining all of the records for the DNS zone.
- Contains the primary copy of the DNS database.
- All record updates occur on the primary zone.
- There are two types of primary zones:
  - Primary zone
  - Primary zone with Active Directory Integration (Active Directory DNS)

Primary DNS Zone (2/2)

- Primary DNS zones get stored locally in a file (with the suffix .dns) on the server.
- Disadvantages:
  - Lack of Fault Tolerance
  - Additional Network Traffic
  - No Security

Secondary DNS Zones

- Secondary zones are non-editable copies of the DNS database.
- They are used for *load balancing* (also referred to as *load sharing*) - a way of managing network overloads on a single server.
- A secondary zone gets its database from a primary zone.

Secondary Zone Advantages

Secondary zones have the following advantages:

- provides fault tolerance, so if the primary zone server becomes unavailable, name resolution can still occur using the secondary zone server.
- also increase network performance by offloading some of the traffic that would otherwise go to the primary server.

Configure Zone Delegation

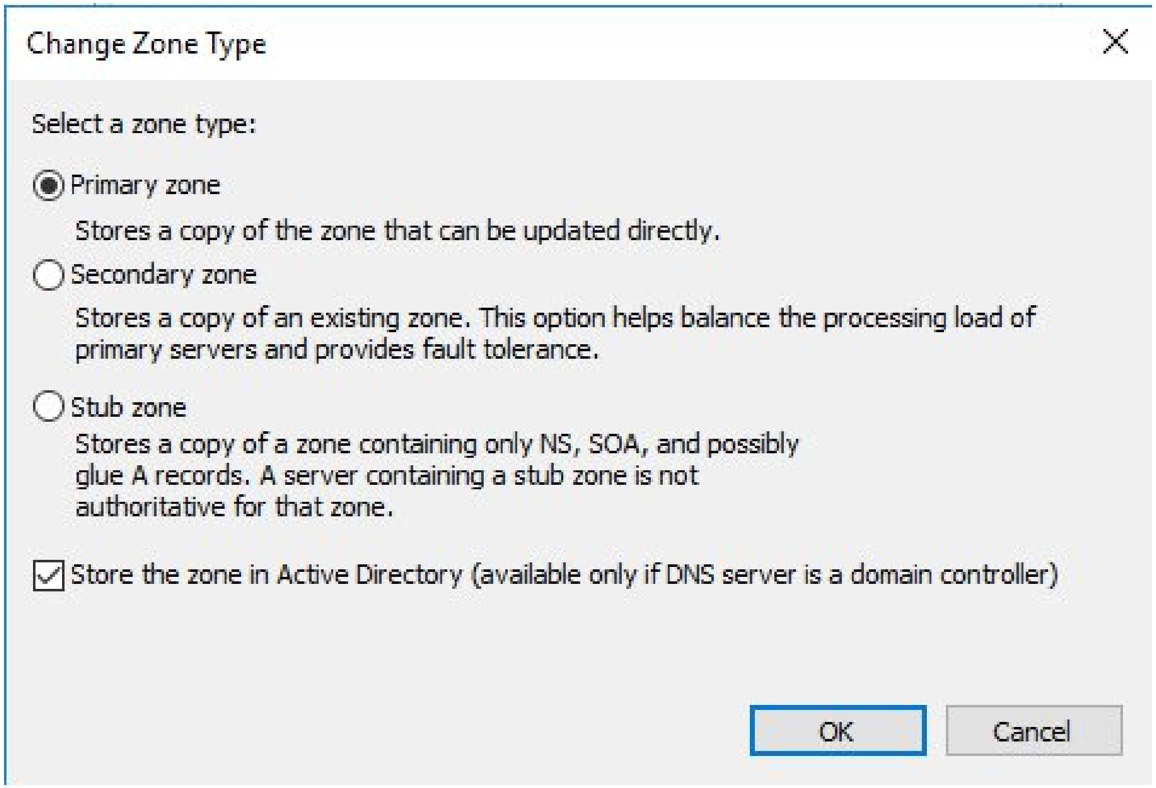
To create a new zone delegation, you would complete the following steps:

1. Open the DNS console.
2. In the console tree, right-click the applicable subdomain and then click New Delegation.
3. Follow the instructions provided in the New Delegation Wizard to finish creating the newly delegated domain.

Active Directory Integrated DNS Zones

- Database stored in Active Directory
- DNS server must reside on a domain controller
- Advantages of an AD Integrated Zone
  - Full Fault Tolerance
  - No Additional Network Traffic
  - DNS Security
    - An Active Directory Integrated Zone can use secure dynamic updates
    - An Active Directory Integrated Zone stores and replicates its database through Active Directory replication
  - Background zone loading

DNS Zone Type Selection



Change Zone Type

Select a zone type:

● Primary zone

Stores a copy of the zone that can be updated directly.

○ Secondary zone

Stores a copy of an existing zone. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone

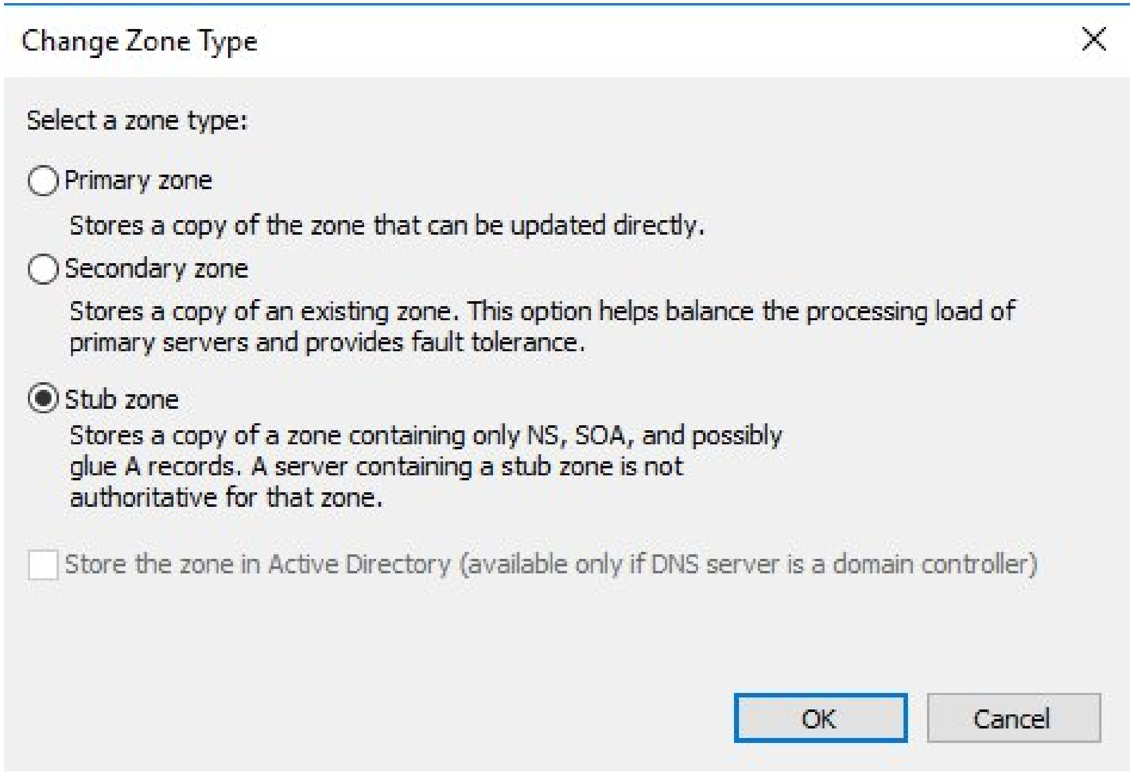
Stores a copy of a zone containing only NS, SOA, and possibly glue A records. A server containing a stub zone is not authoritative for that zone.

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

Stub DNS Zones

- Stub zones work a lot like secondary zones—the database is a non-editable copy of a primary zone
- The difference is that the stub zone's database contains only the information necessary (3 record types only) to identify the authoritative DNS servers for a zone
  - Name Server (NS) records
  - Start of Authority (SOA) records
  - Glue host (A) records
- Stub zone should not be used to replace secondary zones
- Stub zones are not used for redundancy and load balancing

DNS Stub Zone Types



Change Zone Type

Select a zone type:

○ Primary zone

Stores a copy of the zone that can be updated directly.

○ Secondary zone

Stores a copy of an existing zone. This option helps balance the processing load of primary servers and provides fault tolerance.

● Stub zone

Stores a copy of a zone containing only NS, SOA, and possibly glue 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 domain controller)

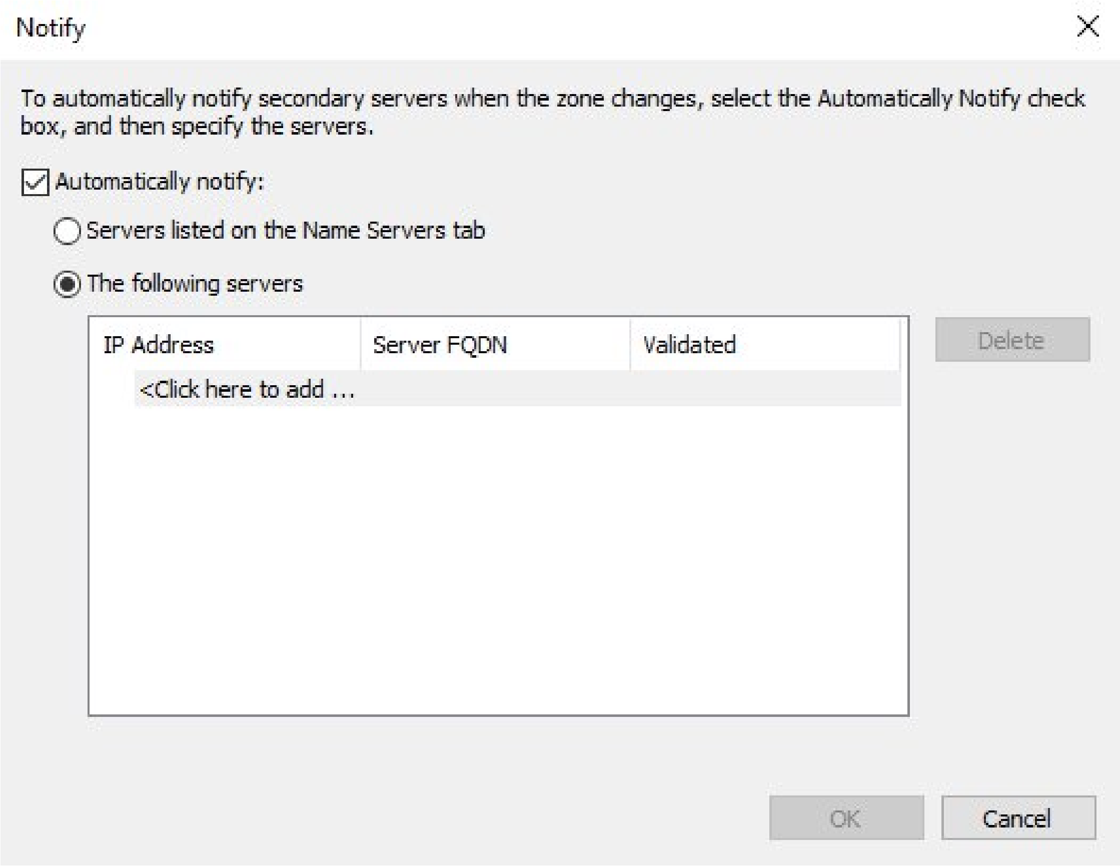
GlobalName Zones

- Windows Server 2022 DNS supports *GlobalName zones*. Use single-label names (DNS names that do not contain a suffix such as .com, or .net).
- Are not intended to support peer-to-peer networks and workstation name resolution, and they don’t support dynamic DNS updates.
- Are designed to be used with servers. Because GlobalName zones are not dynamic, an administrator has to enter the records into the zone database manually.

DNS Notify

- Windows Server 2022 supports DNS Notify.
- *DNS Notify* is a mechanism that allows the process of initiating notifications to secondary servers when zone changes occur (RFC 1996).
- Uses a push mechanism for communicating to a select set of secondary zone servers when their zone information is updated.
- DNS Notify does not allow you to configure a notify list for a stub zone.

DNS Notify Dialog Box



Notify

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

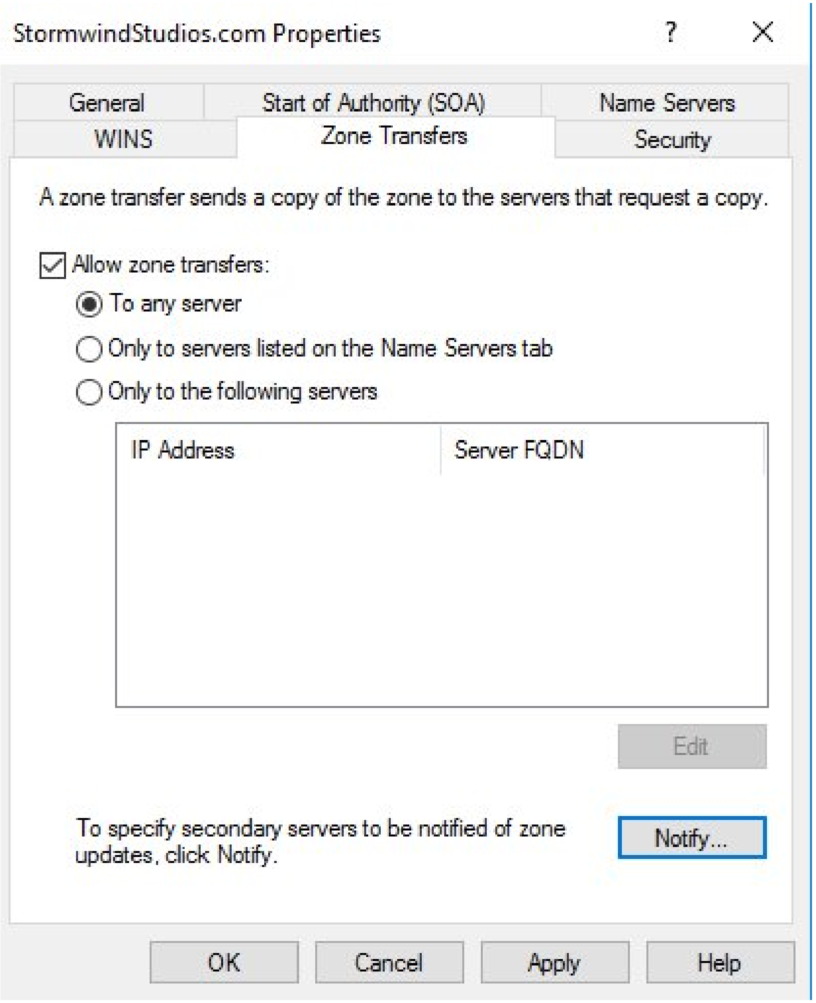
☑ Automatically notify:

○ Servers listed on the Name Servers tab

● The following servers

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

DNS Zone Transfer Tab



StormwindStudios.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

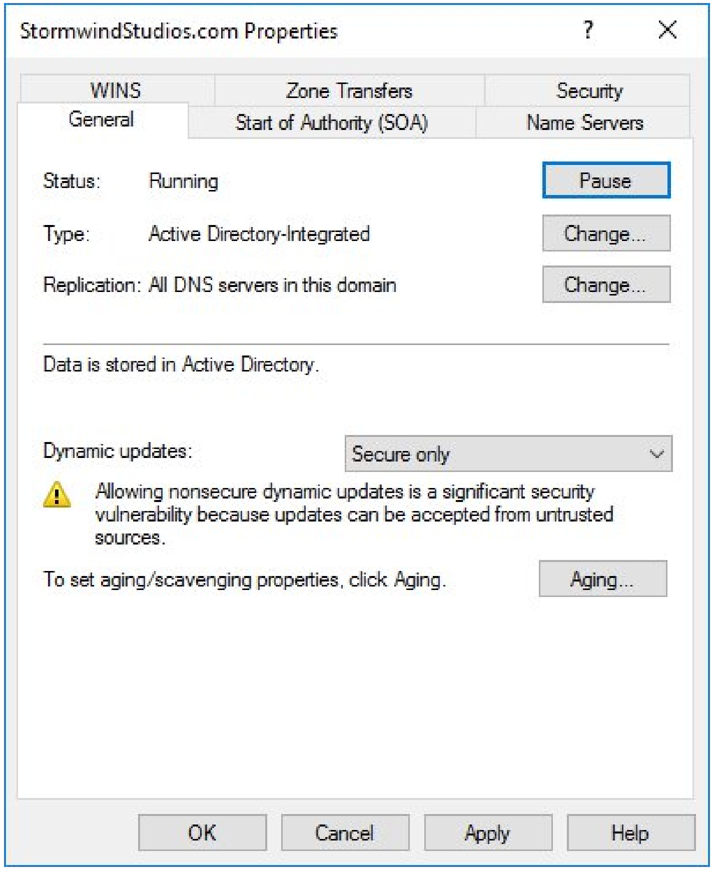
IP Address	Server FQDN

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

Configure Stub Zone Transfers with Zone Replication

To configure zone replication scope through the DNS snap-in:

1. Click Start ➢ Administrative Tools ➢ DNS.
2. Right-click the zone that you want to set up.
3. Choose Properties.
4. In the Properties dialog box, click the Change button next to Replication.
5. Choose the replication scope that fits your organization.



StormwindStudios.com Properties

Status: Running

Type: Active Directory-Integrated

Replication: All DNS servers in this domain

Data is stored in Active Directory.

Dynamic updates: Secure only

Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.

To set aging/scavenging properties, click Aging.

Advantages of DNS in Windows Server 2022

- Background zone loading
- Support for TCP/IP version 6 (IPv6)
- Read-only domain controllers
- GlobalName zone
- DNS socket pools
- DNS cache locking
- Response Rate Limiting (RRL)
- Unknown Record Support
- IPv6 Root Hints
- DNS Security Extensions (DNSSEC)
- DNS devolution
- Record weighting
- Netmask ordering
- DnsUpdateProxy group
- DNS Policies

DNS Socket Pool & DNS Cache Locking

- DNS Socket Pools helps reduce cache-tampering and spoofing attacks by randomizing which source port is used when issuing DNS queries to remote DNS servers.
- DNS Cache Locking allows an administrator to control when the information stored in the DNS server’s cache can be overwritten. Configured at a percent value.

Response Rate Limiting (RRL)

Allows you to help prevent the possibility of hackers using the corporate DNS servers to initiate a denial of service attack on corporate DNS clients. Can manipulate the following settings:

- Responses Per Second
- Errors Per Second
- Window
- Leak Rate
- TC Rate
- Maximum Responses
- White List Domains / White List Subnets
- White List Server Interfaces

Common DNS Record Types

- Start of Authority (SOA)
- Name Server (NS)
- Host Record (A)
- Alias (CNAME)
- Pointer (PTR)
- Mail Exchanger (MX)
- Service (SRV)

SOA Record Structure

Field	Meaning
Current zone	The current zone for the SOA. This can be represented by an `@` symbol to indicate the current zone or by naming the zone itself.
Class	This will almost always be the letters *IN* for the Internet class.
Type of record	The type of record follows. In this case, it’s SOA.
Primary master	The primary master for the zone on which this file is maintained.
Contact email	The Internet email address for the person responsible for this domain’s database file. There is no `@` symbol in this contact email address because `@` is a special character in zone files.
Serial number	This is the “version number” of this database file. It increases each time the database file is changed.
Refresh time	The amount of time (in seconds) that a secondary server will wait between checks to its master server to see whether the database file has changed and a zone transfer should be requested.
Retry time	The amount of time (in seconds) that a secondary server will wait before retrying a failed zone transfer.
Expiration time	The amount of time (in seconds) that a secondary server will spend trying to download a zone. Once this time limit expires, the old zone information will be discarded.
Time to live	The amount of time (in seconds) that another DNS server is allowed to cache any resource records from this database file.

NS Record Structure

Field	**Meaning**
Name	The domain that will be serviced by this name server. In this case I used `example.com`.
AddressClass	Internet (IN)
RecordType	Name server (NS)
Name Server Name	The FQDN of the server responsible for the domain

Host Record

- A host record (also called an A record for IPv4 and AAAA record for IPv6) is used to associate statically a host’s name to its IP addresses.

- The format is:

```
host_nameoptional_TTL IN  A  IP_Address
```

Alias Record

- Related to the host record is the alias record, or canonical name (CNAME) record.
- The syntax of an alias record is as follows:

```
aliasoptional_TTL  IN  CNAME  hostname
```

- Used to point more than one DNS record toward a host for which an A record already exists.

Pointer Record

- A or AAAA records are probably the most visible component of the DNS database because Internet users depend on them to turn FQDNs like www.microsoft.com into the IP addresses that browsers and other components require to find Internet resources.
- The format of a PTR record appears as follows:

```
    reversed_address.in-addr.arpa.
optional_TTL IN PTR targeted_domain_name
```

Mail Exchanger Record

- Used to specify which servers accept mail for this domain.

- Each MX record contains two parameters—a preference and a mail server, as shown in the following example:

```
domain IN MX preference mailserver_host
```

SRV Record Structure

Field	**Meaning**
Domain name	Domain for which this record is valid (`ldap.tcp.example.com.`).
TTL	Time to live (86,400 seconds).
Class	This field is always `IN`, which stands for Internet.
Record type	Type of record (`SRV`).
Priority	Specifies a preference, similar to the Preference field in an MX record. The SRV record with the lowest priority is used first (`10`).
Weight	Service records with equal priority are chosen according to their weight (`100`).
Port number	The port where the server is listening for this service (`389`).
Target	The FQDN of the host computer (`hsv.example.com` and `msy.example.com`).

Installing and Configuring DNS

1. Open Server Manager.
2. On the dashboard, click the Add Roles And Features link.
3. If a Before You Begin screen appears, click Next.
4. On the Selection type page, choose Role-Based Or Feature-Based Installation and click Next.
5. Click the Select A Server From The Server Pool radio button and choose the server under the Server Pool section. Click Next.
6. Click the DNS Server Item in the Server Role list. If a pop-up window appears telling you that you need to add additional features, click the Add Features button. Click Next to continue.
7. On the Add Features page, just click Next.

Installing and Configuring DNS - Continued

8. Click Next on the DNS Server information screen.
9. On the Confirm Installation screen, choose the Restart The Destination Server Automatically If Required check box and then click the Install button.
10. At the Installation progress screen, click Close after the DNS server is installed.
11. Close Server Manager.

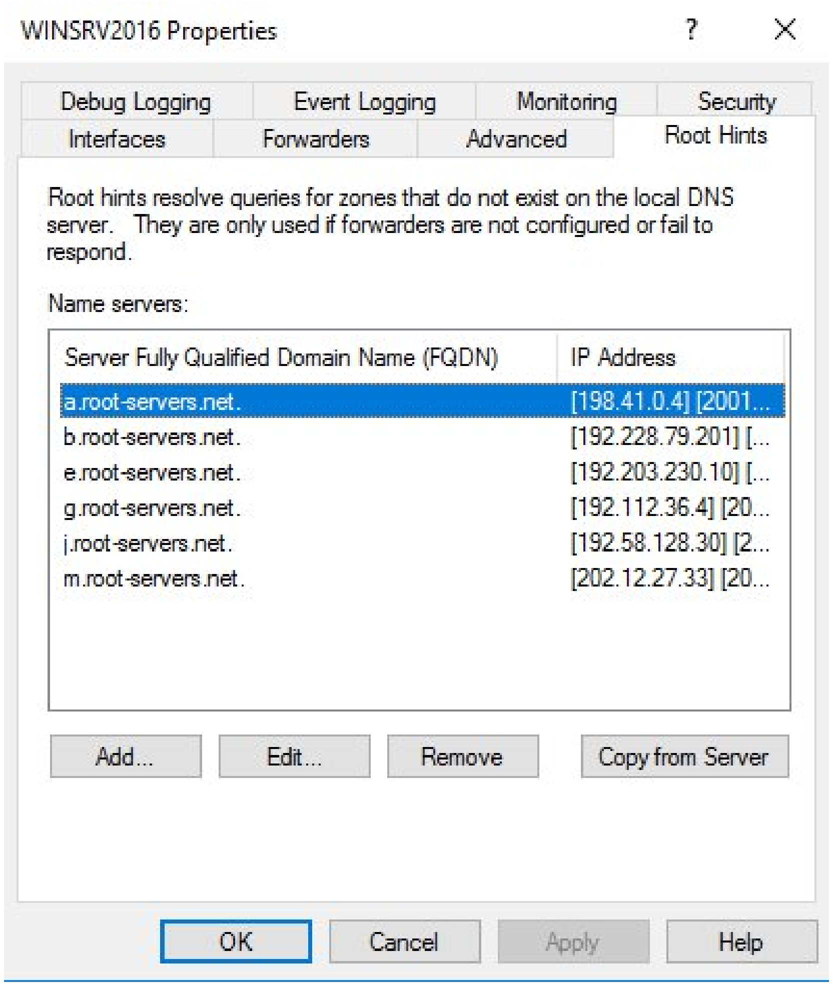
Load Balancing with Round Robin

- DNS supports load balancing through the use of round robin.
- Load balancing distributes the network load among multiple network hosts if they are available.
- You set up round-robin load balancing by creating multiple resource records with the same hostname but different IP addresses for multiple computers.
- Round robin is enabled by default.

Configuring a Caching-Only Server

- Caching-only servers are DNS name servers that only perform queries, cache the answers, and return the results.
- After installing the DNS service, simply make sure the root hints are configured properly.
  1. Right-click your DNS server and choose the Properties command.
  2. When the Properties dialog box appears, switch to the Root Hints tab.
  3. If your server is connected to the Internet, you should see a list of root hints for the root servers maintained by ICANN and the Internet Assigned Numbers Authority (IANA). If not, click the Add button to add root hints as defined in the cache.dns file.

DNS Server Properties – 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:

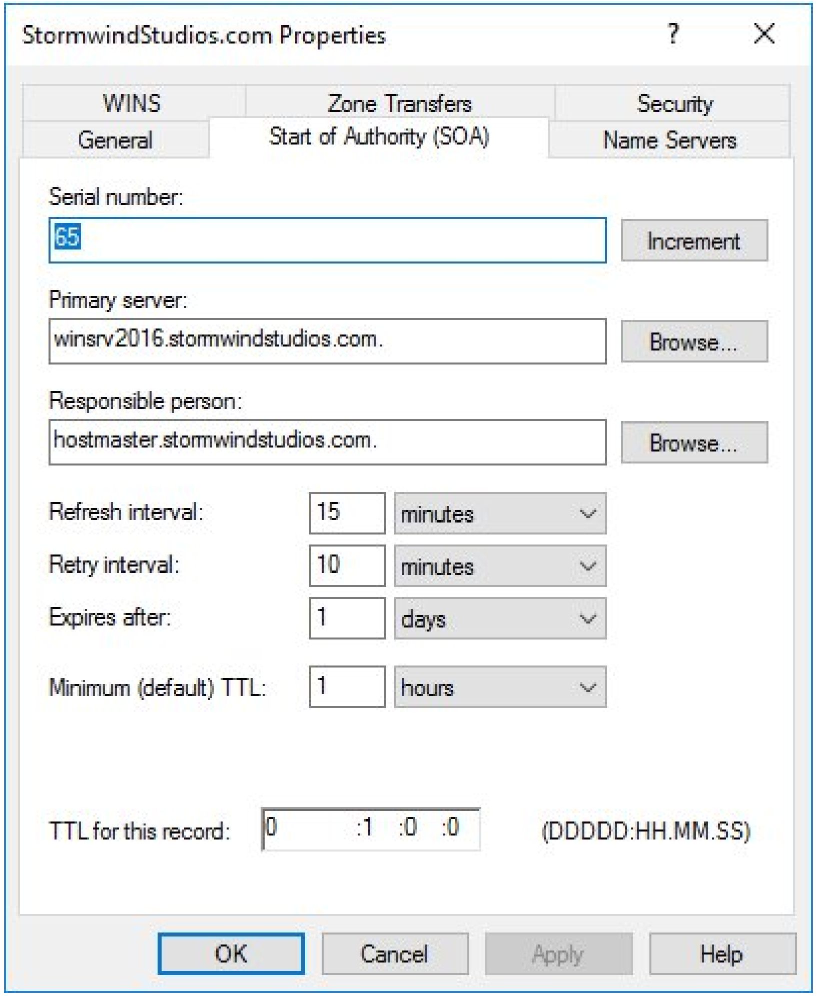
Server Fully Qualified Domain Name (FQDN)	IP Address
a.root-servers.net.	[198.41.0.4] [2001...
b.root-servers.net.	[192.228.79.201] [...
e.root-servers.net.	[192.203.230.10] [...
g.root-servers.net.	[192.112.36.4] [20...
j.root-servers.net.	[192.58.128.30] [2...
m.root-servers.net.	[202.12.27.33] [20...

Setting Zone Properties

There are six tabs on the Properties dialog box for a forward or reverse lookup zone. They are:

- General
- Start of Authority (SOA)
- Name Servers
- WINS
- Zone Transfers
- Security

Start Of Authority (SOA) Tab



StormwindStudios.com Properties

Serial number: 65

Primary server: winsrv2016.stormwindstudios.com.

Responsible person: hostmaster.stormwindstudios.com.

Refresh interval: 15 minutes

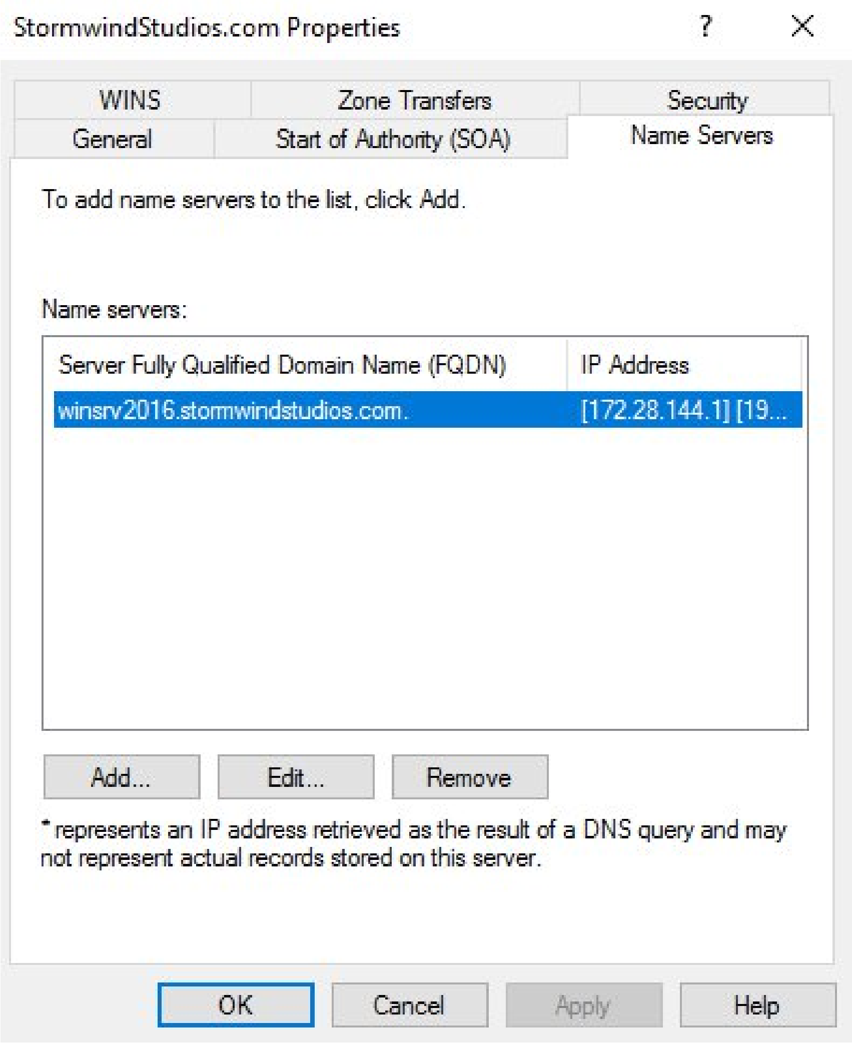
Retry interval: 10 minutes

Expires after: 1 days

Minimum (default) TTL: 1 hours

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

Name Servers Tab



StormwindStudios.com Properties

To add name servers to the list, click Add.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
winsrv2016.stormwindstudios.com.	[172.28.144.1] [19...

* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.

Delegating Zones for DNS

- A need to delegate management of part of your DNS name space to another location or department within your organization.
- A need to divide one large zone into smaller zones for distributing traffic loads among multiple servers, for improving DNS name resolution performance, or for creating a more fault-tolerant DNS environment.
- A need to extend the name space by adding numerous subdomains at once, such as to accommodate the opening of a new branch or site.

DNS Forwarding

If a DNS server does not have an answer to a DNS request, it may be necessary to send that request to another DNS server. This is called *DNS forwarding*.

Two main types of forwarding:

- External Forwarding
- Conditional Forwarding

Manually Creating DNS Records

There are only two important things to remember for manually creating DNS records:

- Must right-click the zone and choose either the New Record command or the Other New Records command.

- Must know how to fill in the fields of whatever record type you're using.

DNS Aging and Scavenging

- Windows Server 2022 DNS supports two features called *DNS aging* and *DNS scavenging*. These features are used to clean up and remove stale resource records.
- By default, DNS aging and scavenging is disabled by default.
- DNS aging and scavenging is done by using time stamps.

Install DNS Using PowerShell

- To install DNS on a regular Windows server:

```
Install-WindowsFeature DNS
–IncludeManagementTools
```

- To install DNS on a Nano server:

```
Install-NanoServerPackage
Microsoft-NanoServer-DNS-Package -
Culture en-us
```

PowerShell Commands for DNS

PowerShell Command	Description
Add-DnsServerClientSubnet	This command allows an administrator to add a client subnet to a DNS server.
Add-DnsServerConditionalForwarderZone	Administrators can use this command to add a conditional forwarder to a DNS server.
Add-DnsServerForwarder	This command allows an administrator to add forwarders to a DNS server.
Add-DnsServerPrimaryZone	Administrators can use this command to add a primary zone to a DNS server.
Add-DnsServerQueryResolutionPolicy	This command allows an administrator to add a query resolution policy to DNS.
Add-DnsServerResourceRecord	Administrators can use this command to add a resource record to a DNS zone.
Add-DnsServerResourceRecordA	This command allows an administrator to add an A record to a DNS zone.
Add-DnsServerResourceRecordAAAA	This command allows an administrator to add an AAAA record to a DNS zone.
Add-DnsServerResourceRecordCName	This command allows an administrator to add a CNAME record to a DNS zone.
Add-DnsServerResourceRecordDnsKey	Administrators can use this command to add a DNSKEY record to a DNS zone.
Add-DnsServerResourceRecordDS	This command allows an administrator to add a DS record to a DNS zone.
Add-DnsServerResourceRecordMX	This command allows an administrator to add a MX record to a DNS zone.
Add-DnsServerResourceRecordPtr	This command allows an administrator to add a PTR record to a DNS zone.
Add-DnsServerSecondaryZone	Administrators can use this command to add a secondary zone.
Add-DnsServerSigningKey	This command adds a KSK or ZSK to a signed zone.
Add-DnsServerStubZone	This command adds a stub zone to a DNS server.
Add-DnsServerTrustAnchor	Admins can use this command to add a trust anchor to a DNS server.

PowerShell Commands for DNS - Continued

PowerShell Command	Description
Add-DnsServerZoneDelegation	This command allows an administrator to add a new delegated DNS zone to an existing zone.
Clear-DnsServerCache	Administrators use this command to clear resource records from a DNS cache.
ConvertTo-DnsServerPrimaryZone	This command converts a zone to a primary zone.
Get-DnsServer	This command retrieves configuration information for a DNS server.
Get-DnsServerDsSetting	This command allows you to gather information about DNS Active Directory settings.
Get-DnsServerRootHint	Administrators use this command to view root hints on a DNS server.
Get-DnsServerScavenging	Administrators use this command to view DNS aging and scavenging settings.
Get-DnsServerSetting	This command allows you to view DNS server settings.
Get-DnsServerSigningKey	This command allows you to view zone signing keys.
Import-DnsServerResourceRecordDS	This command allows an administrator to import DS resource record from a file.
Import-DnsServerRootHint	This command imports root hints from a DNS server.
Remove-DnsServerZone	Administrators use this command to remove a DNS zone from a server.
Resume-DnsServerZone	This command allows you to resume resolution on a suspended zone.
Set-DnsServer	Administrators can use this command to set the DNS server configuration.
Set-DnsServerRootHint	This command allows an administrator to replace a server’s root hints.
Set-DnsServerSetting	Administrators can use this command to change DNS server settings.
Test-DnsServer	This command allows an administrator to test a functioning DNS server.