

# Lesson 9: Configuring DNS Records

MOAC 70-411: Administering  
Windows Server 2012

# Overview

- Exam Objective 3.2: Configure DNS Records
- Configuring DNS Record Types
- Using the DNSCMD Command to Manage Resource Records
- Troubleshooting DNS Problems

# Configuring DNS Record Types

Lesson 9: Configuring DNS Records

# DNS Records

- A **DNS zone database** is made up of a collection of resource records, which are used to answer DNS queries.
- Each **resource record (RR)** specifies information about a particular object.
- Each record has a type, an expiration time limit, and some type-specific data.

# DNS Records

Many of the resource records are automatically created:

- Clients or the DHCP servers create the host and Pointer (PTR) records.
- When you install a DNS server, NS records are usually created.
- When you install domain controllers, Service Location (SRV) records are created.

# Creating and Configuring DNS Resource Records

Different properties define different accounts:

- First name, last name, and login name for a user account
- Name of the printer and location for a printer in Active Directory

Just as you have different types of objects in Active Directory, you also have different types of resource records in DNS, with different fields.

# Creating and Configuring DNS Resource Records

When you create a new zone, two types of records are automatically created:

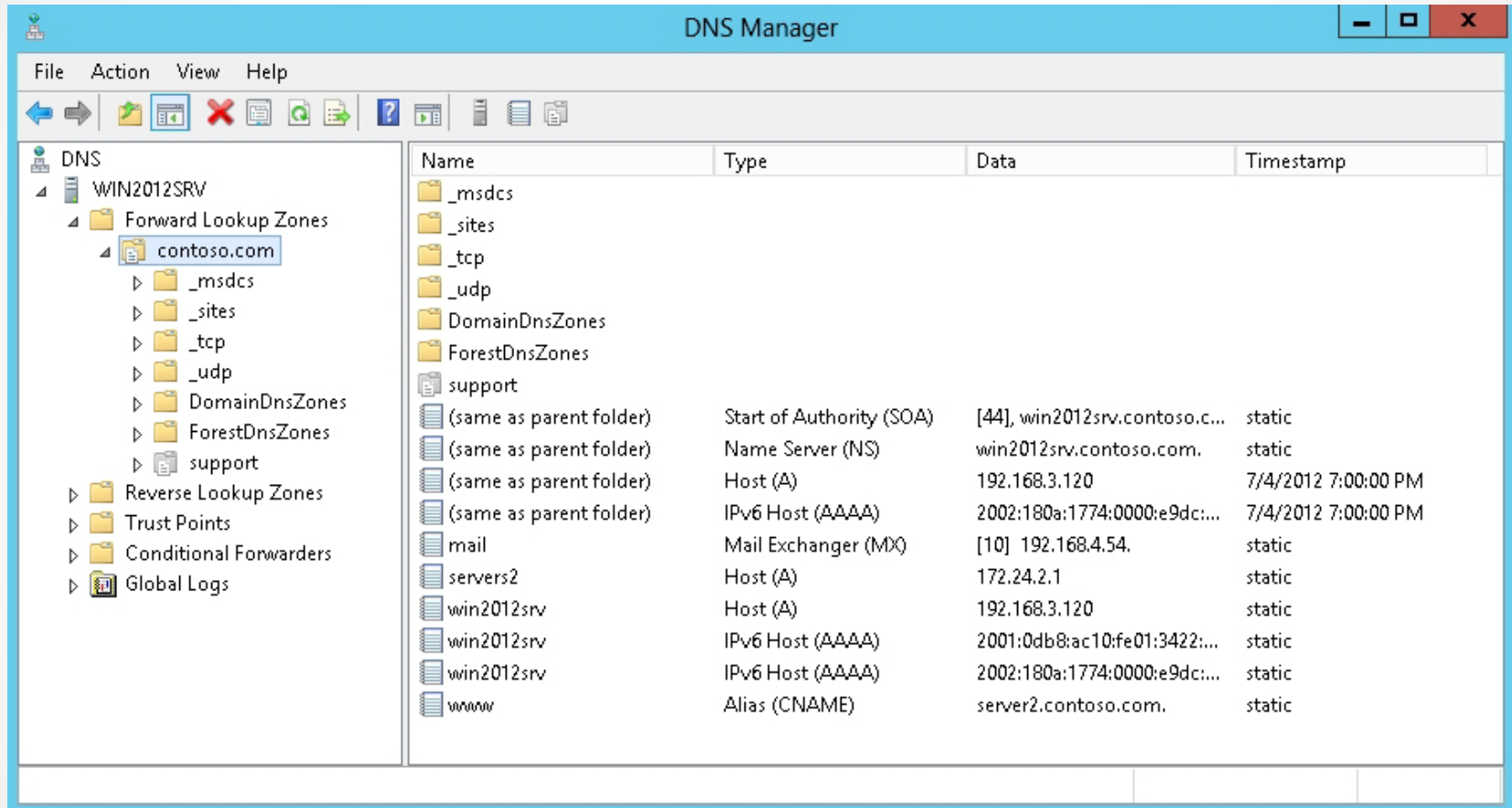
SOA

- Specifies authoritative information about a DNS zone

NS

- Specifies an authoritative name server for the host

# Creating and Configuring DNS Resource Records



The screenshot shows the DNS Manager console for the contoso.com zone. The left pane displays the tree structure, and the right pane shows a list of resource records.

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
support			
(same as parent folder)	Start of Authority (SOA)	[44], win2012srv.contoso.c...	static
(same as parent folder)	Name Server (NS)	win2012srv.contoso.com.	static
(same as parent folder)	Host (A)	192.168.3.120	7/4/2012 7:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	2002:180a:1774:0000:e9dc:...	7/4/2012 7:00:00 PM
mail	Mail Exchanger (MX)	[10] 192.168.4.54.	static
servers2	Host (A)	172.24.2.1	static
win2012srv	Host (A)	192.168.3.120	static
win2012srv	IPv6 Host (AAAA)	2001:0db8:ac10:fe01:3422:...	static
win2012srv	IPv6 Host (AAAA)	2002:180a:1774:0000:e9dc:...	static
www	Alias (CNAME)	server2.contoso.com.	static

Viewing the zone with common resource records



# Most Common Resource Records

- **Host (A and AAAA) record:** Maps a domain/host name to an IP address.
- **Canonical Name (CNAME) record:** Sometimes referred to as an Alias, maps an alias DNS domain name to another primary or canonical name.
- **Pointer (PTR) record:** Maps an IP address to a domain/host name.
- **Mail Exchanger (MX) record:** Maps a DNS domain name to the name of a computer that exchanges or forwards e-mail for the domain.
- **Service Location (SRV) record:** Maps a DNS domain name to a specified list of host computers that offer a specific type of service, such as Active Directory domain controllers.

# Start of Authority (SOA) Records

SOA record fields:

- Authoritative server
- Responsible person
- Serial number
- Refresh shows
- Retry
- Expire
- Minimum TTL

# SOA Record

The screenshot shows the 'contoso.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The 'General' sub-tab is also active. The fields are as follows:

Field	Value	Unit	Action
Serial number:	1		Increment
Primary server:	win2012srv.acme.com.		Browse...
Responsible person:	hostmaster.acme.com.		Browse...
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	(DDDD:HH.MM.SS)

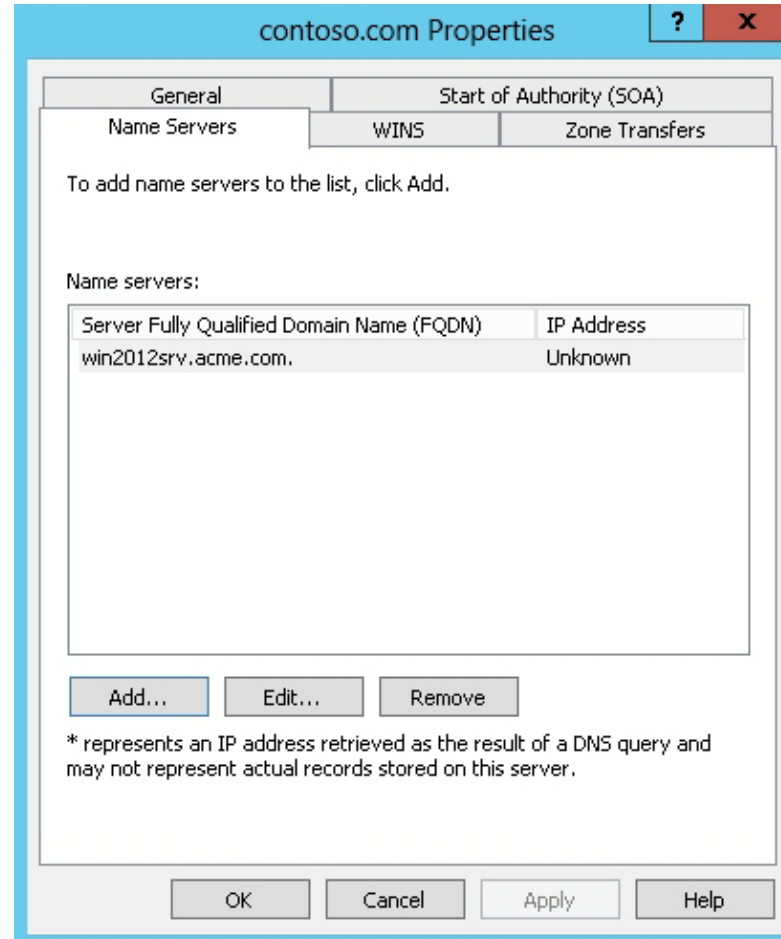
Buttons at the bottom: OK, Cancel, Apply, Help.

Viewing the SOA resource record

# Name Server (NS) Records

- The Name Server (NS) resource record identifies a DNS server that is authoritative for a zone including the primary and secondary copies of the DNS zone.
- Because a zone can be hosted on multiple servers, there is a single record for each DNS server hosting the zone.
- The Windows Server DNS Server service automatically creates the first NS record for a zone when the zone is created.

# NS Record



Viewing the NS resource record

# Host (A and AAAA) Records

- DNS Host records: A and AAAA
- The "A" stands for address.
- The A record maps a domain/host name to an IPv4 address.
- The AAAA record maps a domain/host name to an IPv6 address.

# Host Record

New Host

Name (uses parent domain name if blank):  
server1

Fully qualified domain name (FQDN):  
server1.contoso.com.

IP address:  
192.168.3.52

Create associated pointer (PTR) record:

Add Host Cancel

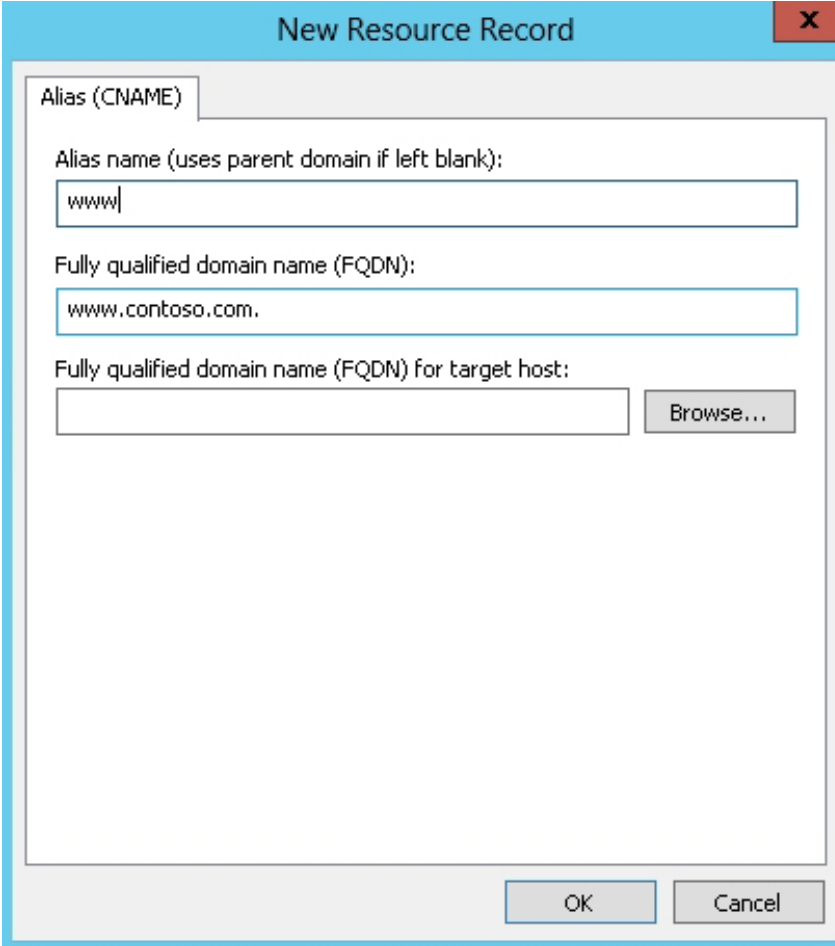
Viewing the Host resource record

# Canonical Name (CNAME) Records

- The Canonical Name (CNAME) resource record is an alias for a host name.
- It used to hide the implementation details of your network from the clients that connect to it, particularly if you need to make changes in the future.
- Example:
  - Instead of creating a Host record for www, you can create a CNAME that specifies the web server that hosts the www websites for the domain. If you need to change servers, you just point the CNAME to another server's Host record.



# CNAME Record



The image shows a Windows-style dialog box titled "New Resource Record" with a close button (X) in the top right corner. The dialog is divided into a tabbed area with "Alias (CNAME)" selected. Inside the tab, there are three text input fields and one button. The first field is labeled "Alias name (uses parent domain if left blank):" and contains the text "www". The second field is labeled "Fully qualified domain name (FQDN):" and contains the text "www.contoso.com.". The third field is labeled "Fully qualified domain name (FQDN) for target host:" and is currently empty, with a "Browse..." button to its right. At the bottom of the dialog, there are "OK" and "Cancel" buttons.

Alias (CNAME)

Alias name (uses parent domain if left blank):

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) for target host:

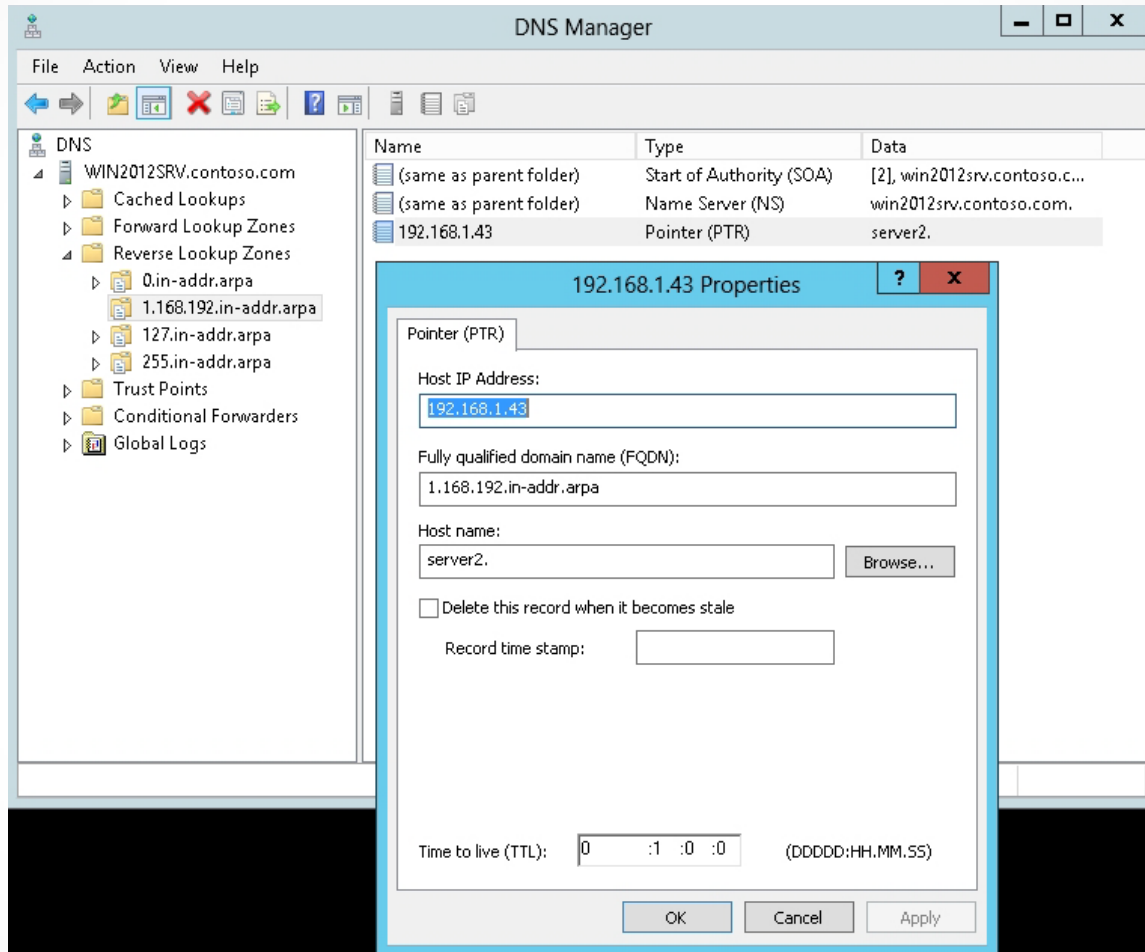
Viewing the CNAME resource record

# Pointer (PTR) Records

- The Pointer records (PTR) resolve host names from an IP address.
- Different from the Host record, the IP address is written in reverse.
- For example, the IP address 192.168.3.41 that points to server1.sales.contoso is:

```
41.3.168.192.in-addr.arpa. IN PTR  
server1.sales.contoso.com
```

# PTR Record



Viewing the PTR resource record

# Mail Exchanger (MX) Records

- The Mail Exchanger (MX) resource record specifies an organization's mail server, service, or device that receives mail via Simple Mail Transfer Protocol (SMTP).
- For fault tolerance, you can designate a second mail server.
- Although each external mail server requires an MX record, the primary server is designed with a lower priority number.

# Mail Exchanger (MX) Records

- For example, if you have three mail servers that can receive e-mail over the Internet, you would have three MX records for the contoso.com domain:
  - @ IN MX 5 mailserver1.contoso.com.
  - @ IN MX 10 mailserver2.contoso.com.
  - @ IN MX 20 mailserver3.contoso.com.
- The primary mail server is the first one because it has a lower priority number.

# MX Record

The image shows a Windows-style dialog box titled "New Resource Record" with a close button (X) in the top right corner. The dialog has a tab labeled "Mail Exchanger (MX)". Inside the dialog, there are several input fields and a text block:

- Host or child domain:** A text box containing the text "mail".
- Text block:** A paragraph of text: "By default, DNS uses the parent domain name when creating a Mail Exchange record. You can specify a host or child name, but in most deployments, the above field is left blank."
- Fully qualified domain name (FQDN):** A text box containing the text "mail.contoso.com."
- Fully qualified domain name (FQDN) of mail server:** An empty text box followed by a "Browse..." button.
- Mail server priority:** A text box containing the number "10".

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

Viewing the MX resource record

# Service Location (SRV) Records

- SRV resource records are used to find specific network services.
- The format for an SRV record:  
`Service_Protocol.Name [TTL] Class SRV  
Priority Weight Port Target`

# Service Location (SRV) Records

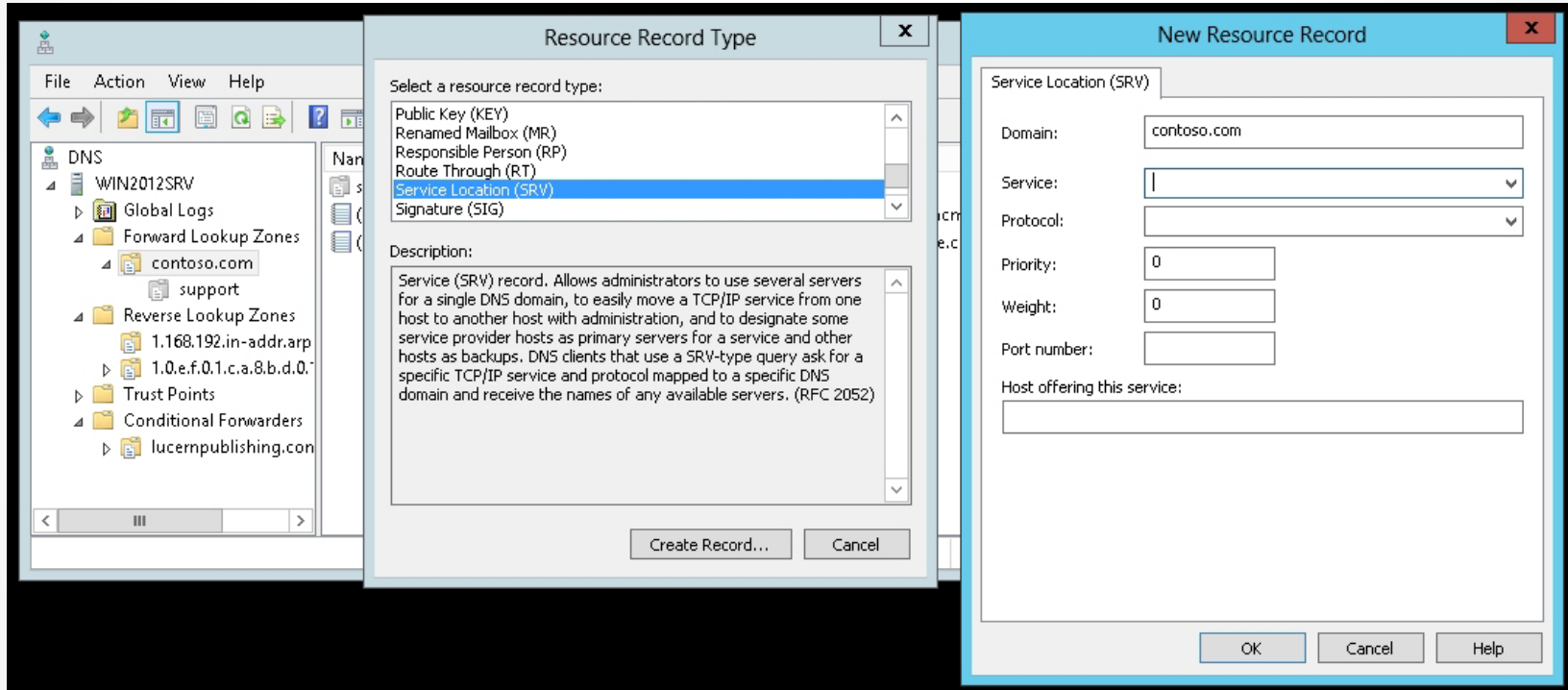
- For example, to log in with Lightweight Directory Access Protocol (LDAP), you could have the following SRV records for two domain controllers:

```
ldap._tcp.contoso.com. IN SRV 0 0 389  
dc1.contoso.com.
```

```
ldap._tcp.contoso.com. IN SRV 10 0 389  
dc2.contoso.com.
```

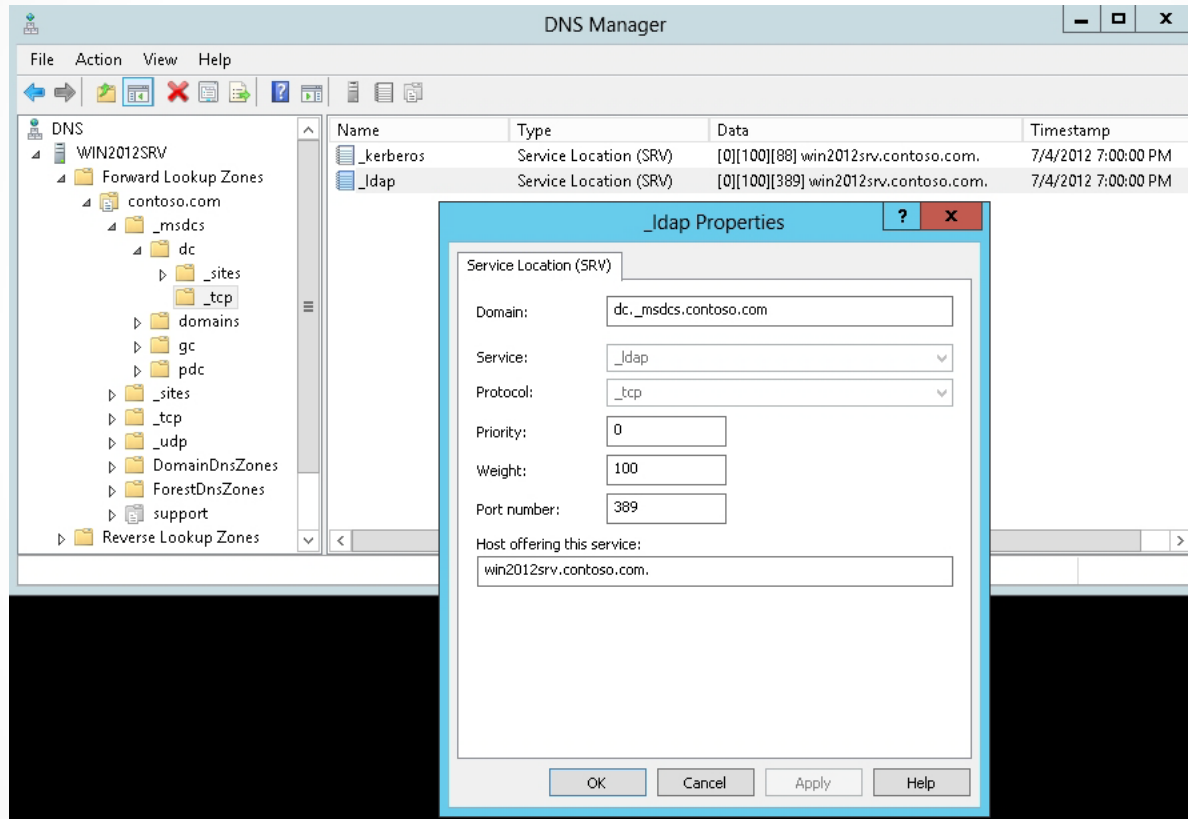


# SRV Record



Viewing the SRV record

# SRV Record

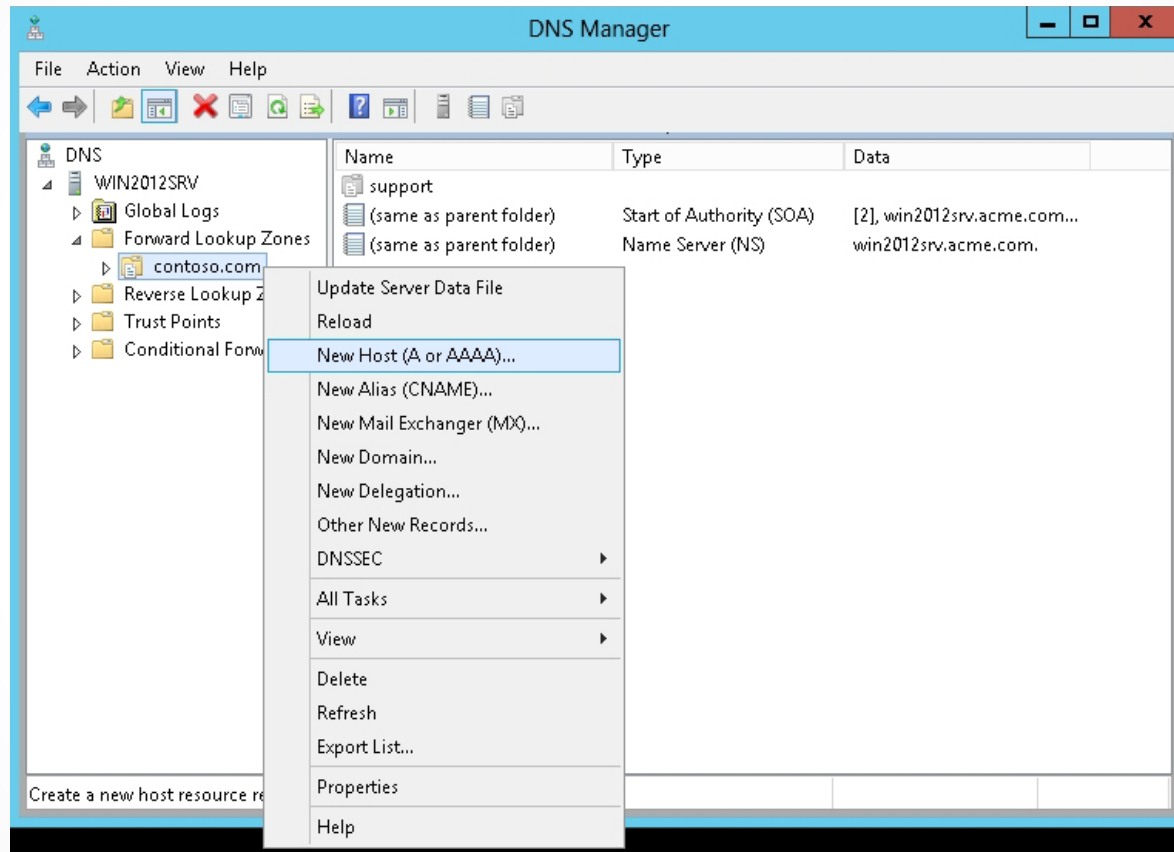


Viewing the SRV resource record for a domain

# Configuring Record Options

- The DNS console provides a GUI interface for managing resources for Windows servers.
- Before you can create resource records, you need to first create the appropriate:
  - Forward lookup zones
  - Reverse lookup zones

# Create a Host Record



Creating a new Host record

# Changing a Resource Record

To change a resource record:

1. Double-click the resource record to display the *Properties* dialog box.
2. Make appropriate changes.

Changes to resource records must replicate to the other DNS servers for the domain.

# Advanced Options

To see additional options when managing and configuring the resource records:

1. Open the *View* menu.
2. Select the *Advanced* option in the DNS console.

# Views of a Resource Record

25d3bdb1-ce41-4f46-a185-2afe5ab88714 Prop... ? x

Alias (CNAME)

Alias name (uses parent domain if left blank):

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) for target host:

25d3bdb1-ce41-4f46-a185-2afe5ab88714 Prop... ? x

Alias (CNAME)

Alias name (uses parent domain if left blank):

Fully qualified domain name (FQDN):

Fully qualified domain name (FQDN) for target host:

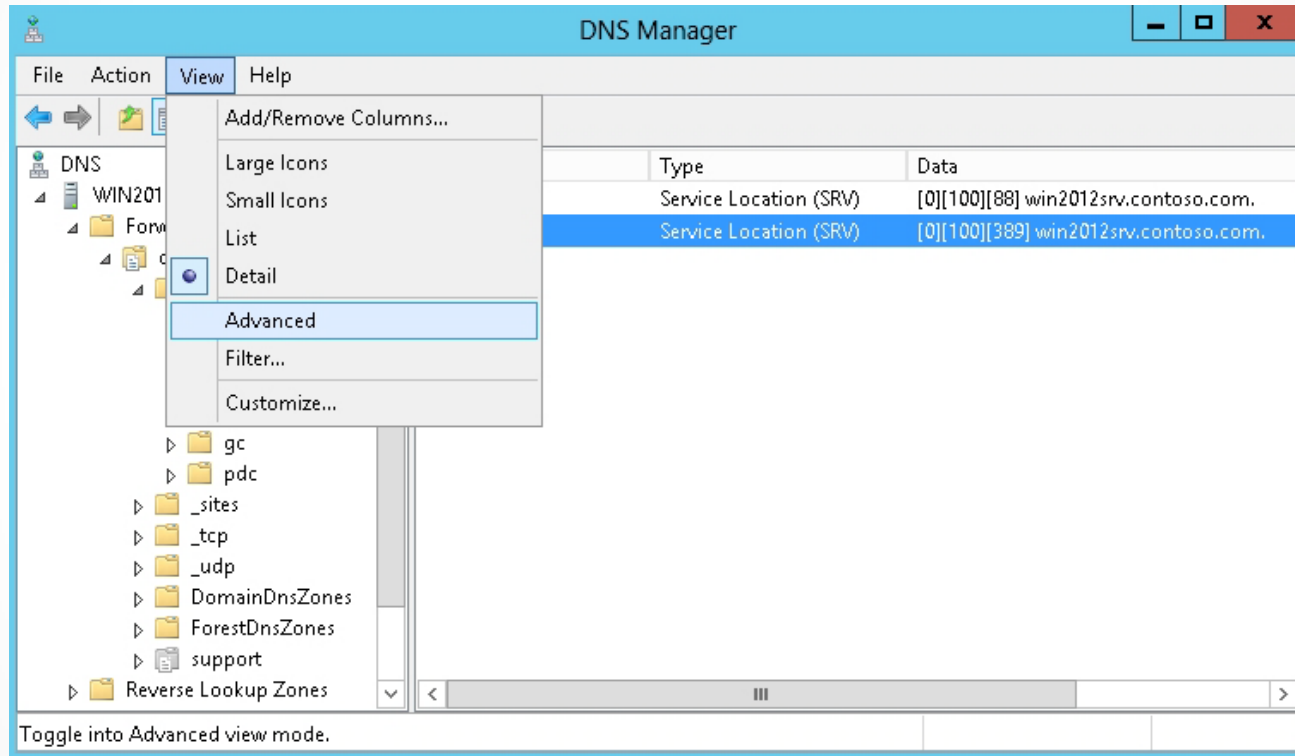
Delete this record when it becomes stale

Record time stamp:

Time to live (TTL):  :0 :10 :0 (DDDD:HH.MM.SS)

Viewing the Normal view and Advanced view for a resource record

# Modify the TTL Value for a Resource Record



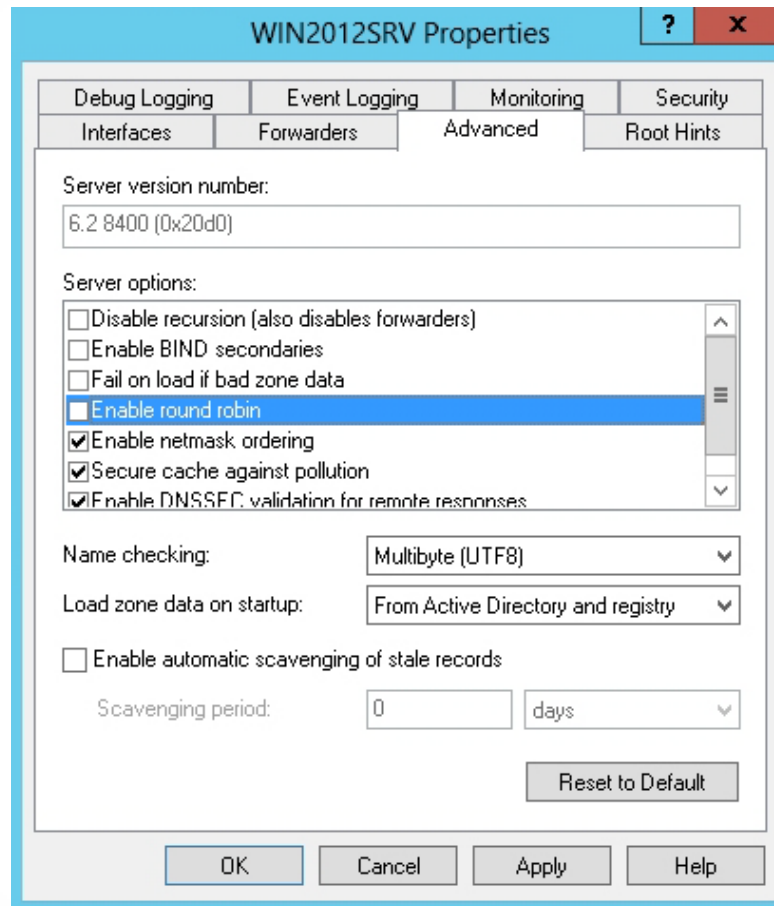
Selecting the Advanced option



# Configuring Round Robin

- **Round robin** is a DNS balancing mechanism that distributes network load among multiple servers by rotating resource records retrieved from a DNS server.
- By default, DNS uses round robin to rotate the resource records returned in a DNS query where multiple resource records of the same type exist for a query's DNS host name.
- Round robin can be enabled or disabled by opening the server properties within the DNS Manager console.

# Disable Round Robin



Disabling round robin

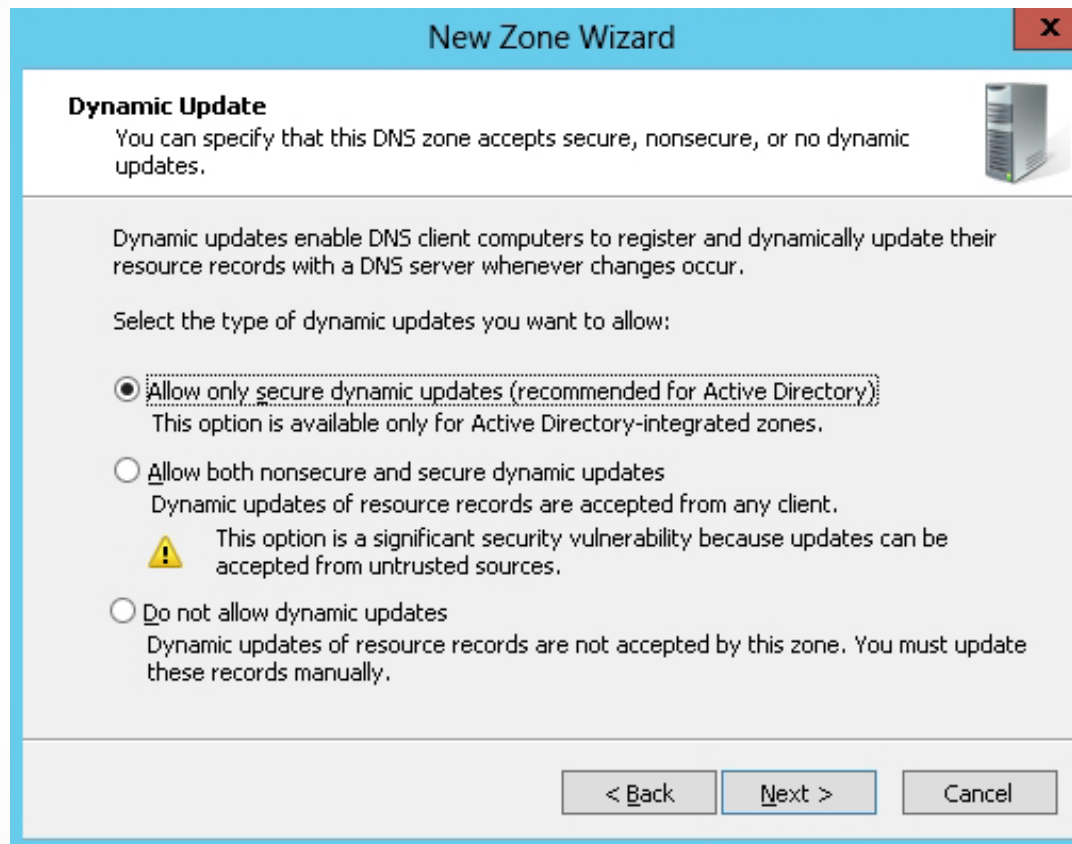
# Configuring Secure Dynamic Updates

- DNS supports **dynamic updates**, where resource records for the clients are automatically created and updated at the host's primary DNS server.
- For Active Directory-integrated zones, these records are automatically replicated to the other DNS servers.
- Because standard dynamic updates are insecure, Microsoft added secure dynamic updates.

# Configuring Secure Dynamic Updates

- Standard dynamic updates are not secure because anyone can update a standard resource record.
- If you enable **secure dynamic updates**, only updates from the same computer can update a registration for a resource record.

# Configuring Secure Dynamic Updates



Enabling secure dynamic updates

# Configuring Zone Scavenging

- By default, Windows updates its own resource record at startup time and every 24 hours after startup.
- As some records become stale and are not removed or updated, the DNS database becomes outdated.
- To help with stale data, you can configure zone scavenging to clean up the stale records.
- **Aging** in DNS is the process of using timestamps to track the age of dynamically registered resource records.
- **Scavenging** is the mechanism to remove stale resource records.

# Configuring Zone Scavenging

To enable aging and scavenging:

- Resource records must either be dynamically added to zones or manually modified to be used in aging and scavenging operations.
- Scavenging and aging must be enabled both at the DNS server and on the zone.

# Configuring Zone Scavenging

DNS scavenging depends on:

- **No-refresh interval:** The time between the most recent refresh of a record time stamp and the moment when the time stamp can be refreshed again.
- **Refresh interval:** The time between the earliest moment when a record time stamp can be refreshed and the earliest moment when the record can be scavenged.



# Enable Aging/Scavenging at the Server

**Server Aging/Scavenging Properties**

Scavenge stale resource records

**No-refresh interval**

The time between the most recent refresh of a record timestamp and the moment when the timestamp may be refreshed again.

No-refresh interval:

**Refresh interval**

The time between the earliest moment when a record timestamp can be refreshed and the earliest moment when the record can be scavenged. The refresh interval must be longer than the maximum record refresh period.

Refresh interval:

OK Cancel

Opening the Server Aging/Scavenging  
Properties dialog box

# Using the DNSCMD Command to Manage Resource Records

Lesson 9: Configuring DNS Records

# The dnscmd COMMAND

- To add a host record for a webserver with an IPv4 address of 10.0.0.5 on server1.contoso.com:

```
dnscmd server1.contoso.com /recordadd  
contoso.com webserver A 10.0.0.5
```

- To delete the same record:

```
dnscmd server1.contoso.com /recorddelete  
contoso.com webserver a
```

# The dnscmd COMMAND

- Because you are deleting a record, you are asked if you are sure that you want to delete the record. If you do not want to be asked, you can add the /f parameter:

```
dnscmd server1.contoso.com /recorddelete  
contoso.com webserver a /f
```

# Troubleshooting DNS Problems

## Lesson 9: Configuring DNS Records

# DNS Troubleshooting Tools

IPConfig  
command

NSLookup  
command

DNS  
Console

# IPConfig

- **ipconfig /all** displays the full TCP/IP configuration for all adapters including host name, DNS servers, and the physical address (or MAC address).
- **ipconfig /flushdns** flushes and resets the contents of the DNS client resolver cache.
- **ipconfig /displaydns** displays the contents of the DNS client resolver cache, which includes both entries preloaded from the local hosts file and any recently obtained resource records for name queries resolved by the computer.

# IPConfig

- `ipconfig /registerdns` initiates manual dynamic registration for the DNS names and IP addresses that are configured at a computer.



# ipconfig /all

```
Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN2012SRU
Primary Dns Suffix . . . . . : contoso.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : contoso.com

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . :
Description . . . . . : Qualcomm Atheros AR8152 PCI-E Fast Ethernet
Controller (NDIS 6.30)
Physical Address. . . . . : E8-40-F2-72-C9-21
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:db8:ac10:fe01:3422:3244:2333:5634(Preferred)
IPv6 Address. . . . . : 2002:180a:1774:0:e9dc:84f5:3789:857b(Preferred)
Link-local IPv6 Address . . . . . : fe80::e9dc:84f5:3789:857b%12(Preferred)
IPv4 Address. . . . . : 192.168.3.120(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80:c2c1:c0ff:fe38:18ac%12
DHCPv6 IAID . . . . . : 266879218
DHCPv6 Client DUID. . . . . : 00-01-00-01-17-77-A6-5C-E8-40-F2-72-C9-21
DNS Servers . . . . . : ::1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 11:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

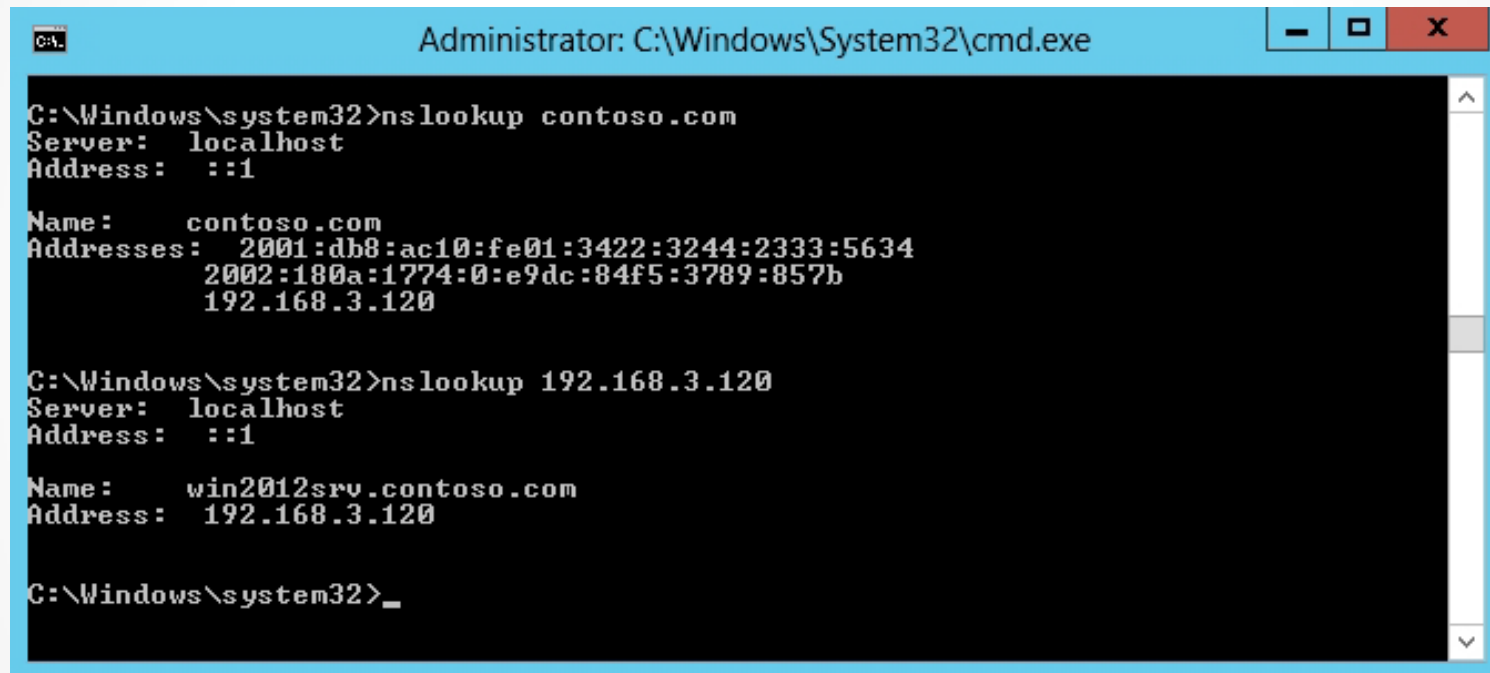
Tunnel adapter isatap.{D620AE03-720B-4584-B74F-853E26FA8FD1}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Windows\system32>_
```

Showing the IP configuration

# Clearing the DNS Cache



```
Administrator: C:\Windows\System32\cmd.exe

C:\Windows\system32>nslookup contoso.com
Server: localhost
Address: ::1

Name: contoso.com
Addresses: 2001:db8:ac10:fe01:3422:3244:2333:5634
           2002:180a:1774:0:e9dc:84f5:3789:857b
           192.168.3.120

C:\Windows\system32>nslookup 192.168.3.120
Server: localhost
Address: ::1

Name: win2012srv.contoso.com
Address: 192.168.3.120

C:\Windows\system32>_
```

Using the Nslookup command

# Clearing the DNS Cache

```
Administrator: C:\Windows\System32\cmd.exe - nslookup

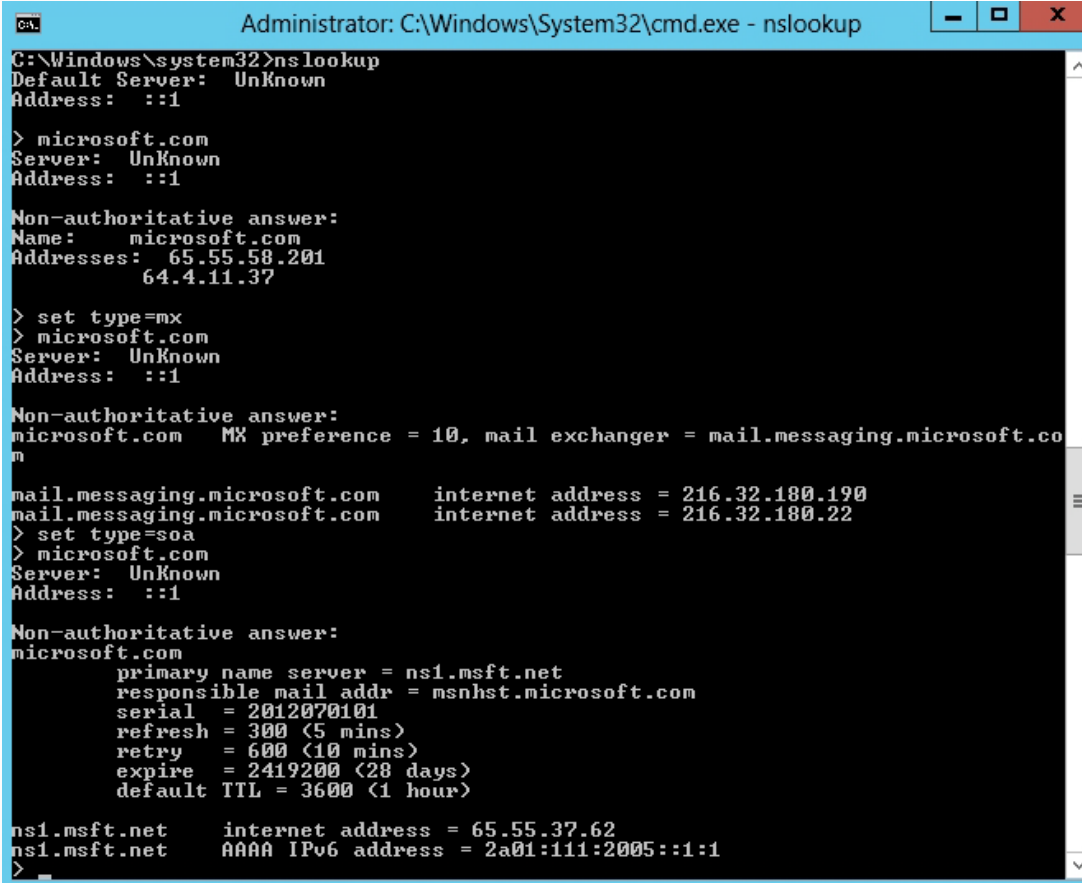
C:\Windows\system32>nslookup
Default Server: UnKnown
Address: ::1

> help
Commands:  (identifiers are shown in uppercase, [] means optional)
NAME      - print info about the host/domain NAME using default server
NAME1 NAME2 - as above, but use NAME2 as server
help or ? - print info on common commands
set OPTION - set an option
  all      - print options, current server and host
  [no]debug - print debugging information
  [no]d2    - print exhaustive debugging information
  [no]defname - append domain name to each query
  [no]recurse - ask for recursive answer to query
  [no]search - use domain search list
  [no]vnc  - always use a virtual circuit
  domain=NAME - set default domain name to NAME
  srchlist=N1[,N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
  root=NAME - set root server to NAME
  retry=X  - set number of retries to X
  timeout=X - set initial time-out interval to X seconds
  type=X   - set query type (ex. A,AAAA,A+AAAA,ANY,CNAME,MX,NS,PTR,
SOA,SRU)
  querytype=X - same as type
  class=X    - set query class (ex. IN <Internet>, ANY)
  [no]msxfr - use MS fast zone transfer
  ixfrver=X  - current version to use in IXFR transfer request
server NAME - set default server to NAME, using current default server
lserver NAME - set default server to NAME, using initial server
root        - set current default server to the root
ls [opt] DOMAIN [ > FILE] - list addresses in DOMAIN (optional: output to FILE)
  -a      - list canonical names and aliases
  -d      - list all records
  -t TYPE - list records of the given RFC record type (ex. A,CNAME,MX,NS,
PTR etc.)
view FILE - sort an 'ls' output file and view it with pg
exit      - exit the program

> _
```

Using Nslookup help

# Clearing the DNS Cache



```
Administrator: C:\Windows\System32\cmd.exe - nslookup
C:\Windows\system32>nslookup
Default Server: UnKnown
Address: ::1

> microsoft.com
Server: UnKnown
Address: ::1

Non-authoritative answer:
Name:    microsoft.com
Addresses: 65.55.58.201
          64.4.11.37

> set type=mx
> microsoft.com
Server: UnKnown
Address: ::1

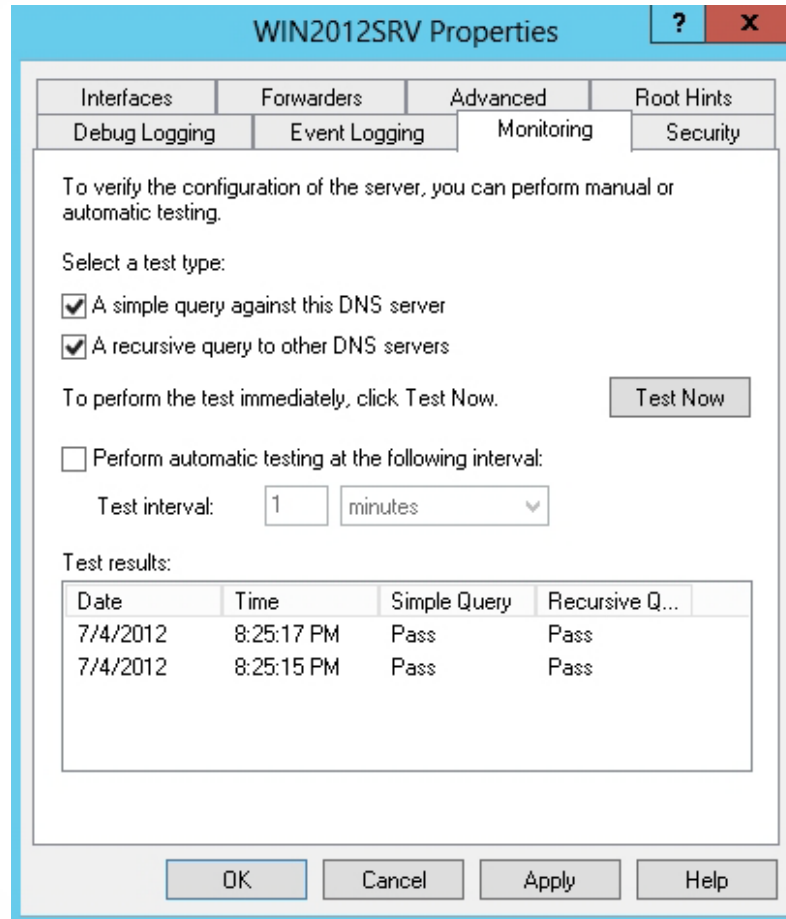
Non-authoritative answer:
microsoft.com  MX preference = 10, mail exchanger = mail.messaging.microsoft.com
mail.messaging.microsoft.com  internet address = 216.32.180.190
mail.messaging.microsoft.com  internet address = 216.32.180.22
> set type=soa
> microsoft.com
Server: UnKnown
Address: ::1

Non-authoritative answer:
microsoft.com
    primary name server = ns1.msft.net
    responsible mail addr = msnhst.microsoft.com
    serial = 2012070101
    refresh = 300 (5 mins)
    retry = 600 (10 mins)
    expire = 2419200 (28 days)
    default TTL = 3600 (1 hour)

ns1.msft.net  internet address = 65.55.37.62
ns1.msft.net  AAAA IPv6 address = 2a01:111:2005::1:1
>
```

Showing MX records in Nslookup interactive mode

# Test a DNS Server



Testing simple and recursive queries for a DNS server

# Lesson Summary

- A DNS zone database is made up of a collection of resource records, which are used to answer DNS queries.
- Start of Authority (SOA) records specify authoritative information about a DNS zone.
- Name Server (NS) records specify an authoritative name server for the host.
- Host A and Host AAAA records map a domain or host name to an IP address.
- Alias (CNAME) records map an alias DNS domain name to another primary or canonical name.
- Pointer (PTR) records map an IP address to a domain or host name.
- Mail exchanger (MX) records map a DNS domain name to the name of a computer that exchanges or forwards mail for the domain.
- Service location (SRV) records map a DNS domain name to a specified list of host computers that offer a specific type of service.

# Lesson Summary

- Minimum TTL specifies a default Time to Live (TTL) value, which defines the default time a resource record remains in a DNS cache after a DNS query has retrieved a record.
- DNS supports dynamic updates, whereas resource records for the clients are automatically created and updated at the host's primary DNS server.
- Round robin is a DNS balancing mechanism that distributes network load among multiple servers by rotating resource records retrieved from a DNS server.
- Aging in DNS is the process of using timestamps to track the age of dynamically registered resource records.
- Scavenging is the mechanism to remove stale resource records.
- Microsoft provides several tools to help you troubleshoot DNS problems, including the `IPConfig` command, the `NSLookup` command, and the DNS console.

**Copyright 2013 John Wiley & Sons, Inc.**

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.