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 DNSSCMD 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.
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

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

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

```plaintext
Name Servers | Start of Authority (SOA) | Zone Transfers
-------------|--------------------------|------------------
WIN5         |                          |                  

To add name servers to the list, click Add.

**Name servers:**

<table>
<thead>
<tr>
<th>Server Fully Qualified Domain Name (FQDN)</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>win2012srv.acme.com.</td>
<td>Unknown</td>
</tr>
</tbody>
</table>

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

© 2013 John Wiley & Sons, Inc.
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

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:
  o 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

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.com 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

Viewing the MX resource record
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:
  o Forward lookup zones
  o 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

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

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

Showing the IP configuration
Clearing the DNS Cache

Using the `Nslookup` command
Clearing the DNS Cache

Using `Nslookup help`
Clearing the DNS Cache

Showing MX records in *Nslookup* interactive mode
Test a DNS Server

To verify the configuration of the server, you can perform manual or automatic testing.

Select a test type:
- [ ] A simple query against this DNS server
- [x] A recursive query to other DNS servers

To perform the test immediately, click Test Now.

Perform automatic testing at the following interval:

- Test interval: 1 minutes

Test results:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Simple Query</th>
<th>Recursive Query</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/4/2012</td>
<td>8:25:17 PM</td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>7/4/2012</td>
<td>8:25:15 PM</td>
<td>Pass</td>
<td>Pass</td>
</tr>
</tbody>
</table>

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.