Module 2

Configuring and Troubleshooting DNS

Contents:
Lesson 1: Installing the DNS Server Role 2-3
Lesson 2: Configuring the DNS Server Role 2-9
Lesson 3: Configuring DNS Zones 2-20
Lesson 4: Configuring DNS Zone Transfers 2-27
Lesson 5: Managing and Troubleshooting DNS 2-32
Lab: Configuring and Verifying a DNS Solution 2-39
Module Overview

- Installing the DNS Server Role
- Configuring the DNS Server Role
- Configuring DNS Zones
- Configuring DNS Zone Transfers
- Managing and Troubleshooting DNS

This module explains how to configure, manage, and troubleshoot Domain Name System (DNS) server and zone properties that you will use in a secure environment.
Lesson 1
Installing the DNS Server Role

- Overview of the Domain Name System Role
- Overview of the DNS Namespace
- DNS Improvements for Windows Server 2008
- Demonstration: Installing the DNS Server Role
- Considerations for Deploying the DNS Server Role

The DNS Server role is a critical component of a Windows Server® 2008 domain infrastructure. This lesson provides information about the DNS role and how the DNS name space works. This lesson also provides details about what has changed in the DNS role for Windows Server 2008 and identifies the considerations for deploying the DNS role.
Overview of the Domain Name System Role

Domain Name System is a hierarchical distributed database

- DNS is the foundation of the Internet naming scheme
- DNS supports accessing resources by using alphanumeric names
- InterNIC is responsible for managing the domain namespace
- DNS was created to support the Internet’s growing number of hosts

Key Points
DNS is a name-resolution service that resolves names to numbers. The DNS service is a hierarchical distributed database. This means that the database is separated logically, allowing many different servers to host the worldwide database of DNS names.

Additional Reading
- DNS Overview
- Understanding zones and zone transfer
Overview of the DNS Namespace

Key Points
The DNS Namespace facilitates how a DNS client locates a computer. It is organized hierarchically or in layers to distribute information across many servers.

Additional Reading
- DNS Namespace Planning
- Designing a DNS Namespace
DNS Improvements for Windows Server 2008

Key Points
You will realize some of the advantages of using Windows Server 2008 with the new features that it includes for the DNS server role. These features include background zone loading, support for IPv6 and for read-only domain controllers, and global single names.

Additional Reading
- What's New in DNS in Windows Server 2008
- AD DS: Read-Only Domain Controllers
- DNS Server Role
Demonstration: Installing the DNS Server Role

In this demonstration, you will see how to install the DNS Server role
Considerations for Deploying the DNS Server Role

- The user account must be a member of the local administrators group or equivalent
- Manually configuring the server to use a static IP address is recommended
- Manually editing the server and boot files is not recommended
- Use the DNS console or dnscmd
- Active Directory integrated DNS zones cannot be administered using a text editor

Key Points
The DNS Server role is critical in the configuration of Active Directory and Windows Network infrastructure. When planning to deploy DNS, there are several considerations that need to be reviewed:

- Server capacity planning
- Where to place DNS servers
- Service availability

Additional Reading
- Help topic: Planning DNS Servers
Lesson 2
Configuring the DNS Server Role

- What Are the Components of a DNS Solution?
- DNS Resource Records
- What are Root Hints?
- What is a DNS Query?
- What Are Recursive Queries?
- What Are Iterative Queries?
- What is a Forwarder?
- What is Conditional Forwarding?
- How DNS Server Caching Works
- Demonstration: Configuring the DNS Server Role

The DNS infrastructure is the basis for name resolution on the Internet and in Windows Server 2008 Active Directory domains. This lesson provides guidance and information about what is required to configure the DNS server role, and explains the basic functions of a DNS server.
What Are the Components of a DNS Solution?

Key Points
The components of a DNS solution include DNS servers, DNS servers on the Internet, and DNS clients.

Additional Reading
- DNS defined
- Server Features
- Client Features
- DNS Server Role
DNS Resource Records

DNS resource records include:

- SOA: Start of Authority
- A: Host Record
- CNAME: Alias Record
- MX: Mail Exchange Record
- SRV: Service Resources
- NS: Name Servers
- AAAA: IPv6 DNS Record

Key Points
The DNS zone file stores resource records. The next lesson examines zone files in more detail. Resource records specify a resource type and the IP address to locate the resource. The most common resource record is an A resource record. This is a simple record that matches a hostname to an IP address. The host can be a workstation, server, or another network device, such as a router.

Additional Reading
- Resource records reference
What are Root Hints?

Root hints are the list of the 13 servers on the Internet that the Internet Assigned Numbers Authority maintains and that the DNS server uses if it cannot resolve a DNS query by using a DNS forwarder or its own cache. The root hints are the highest servers in the DNS hierarchy and can provide the necessary information for a DNS server to perform an iterative query to the next lowest layer of the DNS namespace.

Key Points

Root hints are the list of the 13 servers on the Internet that the Internet Assigned Numbers Authority maintains and that the DNS server uses if it cannot resolve a DNS query by using a DNS forwarder or its own cache. The root hints are the highest servers in the DNS hierarchy and can provide the necessary information for a DNS server to perform an iterative query to the next lowest layer of the DNS namespace.

Additional Reading

- Update root hints on the DNS server
- Disable recursion on the DNS server
### What is a DNS Query?

A query is a request for name resolution and is directed to a DNS server.

- **Queries are recursive or iterative**
- **DNS clients and DNS servers both initiate queries**
- **DNS servers are authoritative or non-authoritative for a namespace**

#### An authoritative DNS server for the namespace will either:

- Return the requested IP address
- Return an authoritative "No"

#### A non-authoritative DNS server for the namespace will either:

- Check its cache
- Use forwarders
- Use root hints

### Key Points

A DNS query is the method that you use to request name resolution in which a query is sent to a DNS Server. There are two types of DNS queries: authoritative and non-authoritative.

It is important to note that DNS servers also can act as DNS clients and send DNS queries to other DNS servers.
What Are Recursive Queries?

A recursive query is sent to a DNS server and requires a complete answer.

Key Points
A recursive query can have two possible results:

- It returns the IP address of the host requested
- The DNS server cannot resolve an IP address

For security reasons, it sometimes is necessary to disable recursive queries on a DNS server. In doing so, the DNS server in question will not attempt to forward its DNS requests to another server. This can be useful when you do not want a particular DNS server communicating outside its local network.
What Are Iterative Queries?

Key Points
Iterative queries provide a mechanism for accessing domain name information that resides across the DNS system, and enable servers to quickly and efficiently resolve names across many servers.

Additional Reading
- How DNS query works
What is a Forwarder?

A forwarder is a DNS server designated to resolve external or offsite DNS domain names.

Key Points
A forwarder is a network DNS server that forwards DNS queries for external DNS names to DNS servers outside that network. You also can use conditional forwarders to forward queries according to specific domain names.

Additional Reading
- Microsoft TechNet: Understanding forwarders
- Help topic: Understanding Forwarders
- Help topic: Using Forwarders
What is Conditional Forwarding?

Key Points
A conditional forwarder is a DNS server on a network that forwards DNS queries according to the query’s DNS domain name.
How DNS Server Caching Works

Key Points
DNS caching increases the performance of the organization's DNS system by decreasing the time it takes to provide DNS lookups.

When a DNS server resolves a DNS name successfully, it adds the name to its cache. Over time, this builds a cache of domain names and their associated IP addresses for the most common domains that the organization uses or accesses.

Additional Reading
- Help topic: Install a Caching-only DNS Server
Demonstration: Configuring the DNS Server Role

In this demonstration, you will see how to:

- Update root hints on a DNS server
- Configure a DNS server to use a forwarder
- Clear the DNS server cache by using the DNS console
- Clear the DNS server cache by using the DNSScmd command
Lesson 3
Configuring DNS Zones

- What Is a DNS Zone?
- What Are the DNS Zone Types?
- What Are Forward and Reverse Lookup Zones?
- What are Stub Zones?
- Demonstration: Creating Forward and Reverse Lookup Zones
- DNS Zone Delegation

DNS zones are an important concept in DNS infrastructure. They allow for DNS domains to be logically separated and managed. This lesson provides the foundation for understanding how zones relate to DNS domains and information about the different types of DNS zones that are available in the Windows Server 2008 DNS role.
What Is a DNS Zone?

Key Points
A DNS zone hosts all or a portion of a domain and its subdomains. The slide illustrates how subdomains can belong to the same zone as their parents or be delegated to another zone. The Microsoft.com domain is separated into two zones. The first zone hosts www.microsoft.com and ftp.microsoft.com. Example.microsoft.com is delegated to a new zone, which hosts the example.microsoft.com and its subdomains ftp.example.microsoft.com and www.example.microsoft.com.

Additional Reading
- Understanding zones and zone transfer
What Are the DNS Zone Types?

<table>
<thead>
<tr>
<th>Zones</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>Read/write copy of a DNS database</td>
</tr>
<tr>
<td>Secondary</td>
<td>Read-only copy of a DNS database</td>
</tr>
<tr>
<td>Stub</td>
<td>Copy of a zone that contains only records used to locate name servers</td>
</tr>
<tr>
<td>Active Directory integrated</td>
<td>Zone data is stored in Active Directory rather than in zone files</td>
</tr>
</tbody>
</table>

Key Points
There are four DNS zone types:

- Primary
- Secondary
- Stub
- Active Directory integrated

Additional Reading

- Help topic: Understanding Zone Types
What Are Forward and Reverse Lookup Zones?

Key Points
The forward lookup zone resolves host names to IP addresses, and hosts the common resource records: A, CNAMEs, SRV, MX, SOA, and NS.

The reverse lookup zone resolves an IP address to a domain name, and hosts SOA, NS, and PTR records.

Additional Reading
- Help topic: Understanding Zone Types
What are Stub Zones?

Key Points
A stub zone is a copy of a zone that contains only those resource records necessary to identify that zone’s authoritative DNS servers. A stub zone resolves names between separate DNS namespaces, which may be necessary when a corporate merger requires that the DNS servers for two separate DNS namespaces resolve names for clients in both namespaces.

Additional Reading
- Help topic: Understanding Zone Types
Demonstration: Creating Forward and Reverse Lookup Zones

In this demonstration, you will see how to:

- Create a forward lookup zone
- Create a reverse lookup zone
DNS Zone Delegation

Key Points
DNS is a hierarchical system, and zone delegation connects the DNS layers together. A zone delegation points to the next hierarchical level down and identifies the name servers responsible for lower-level domain.

Additional Reading
- Delegating Zones
Lesson 4

Configuring DNS Zone Transfers

- What is a DNS Zone Transfer?
- How DNS Notify Works
- Securing Zone Transfers
- Demonstration: Configuring DNS Zone Transfers

DNS zone transfers are how the DNS infrastructure moves DNS zone information from one server to another. This lesson covers the different methods that the DNS Server role uses when transferring zones.
What is a DNS Zone Transfer?

A DNS zone transfer is the synchronization of authoritative DNS zone data between DNS servers.

Key Points
A zone transfer occurs when you transfer the DNS zone that is on one server to another DNS server.

Zone transfers keep primary DNS server zones and secondary DNS Server zones synchronized. This is how DNS builds its resilience on the Internet. It is important that DNS zones remain updated on primary and secondary servers. Discrepancies in primary and secondary zones can cause service outages and host names that are resolved incorrectly.

Additional Reading
- Understanding zones and zone transfer
- Initiate a zone transfer at a secondary server
- Reload or transfer a stub zone
- Adjust the refresh interval for a zone
- Adjust the retry interval for a zone
How DNS Notify Works

A DNS notify is an update to the original DNS protocol specification that permits notification to secondary servers when zone changes occur.

Key Points

DNS notify is an update to the original DNS protocol specification that permits notification to secondary servers when zone changes occur.

This is useful in a time-sensitive environment, where data accuracy is important.
Securing Zone Transfers

Key Points
Zone information provides organizational data, so you should take precautions to ensure it is secure from malicious access and that it cannot be overwritten with bad data (known as DNS poisoning). One way in which you can protect the DNS infrastructure is to secure the zone transfers and use secure dynamic updates.

Additional Reading
• Help topic: Checklist: Secure Your DNS Server
Demonstration: Configuring DNS Zone Transfers

In this demonstration, you will see how to:

- Configure DNS zone transfers
- Configure a secondary zone
Lesson 5
Managing and Troubleshooting DNS

- What is Time to Live, Aging, and Scavenging?
- Demonstration: Managing DNS Records
- Testing the DNS Server Configuration
- Tools That Identify Problems With DNS
- Demonstration: Testing the DNS Server Configuration
- Monitoring DNS using the DNS Event Log and Debug Logging

DNS is a crucial service in the Active Directory infrastructure. When the DNS service experiences problems, it is important to know how to troubleshoot them and identify the common issues that can occur in a DNS infrastructure. This lesson covers the common problems that occur in DNS, the common areas for gathering DNS information, and the tools that you can use to troubleshoot problems.
What is Time to Live, Aging, and Scavenging?

<table>
<thead>
<tr>
<th><strong>Feature</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Time to Live (TTL)</td>
<td>Indicates how long a DNS record will remain valid</td>
</tr>
<tr>
<td>Aging</td>
<td>Occurs when records that have been inserted into the DNS server reach their expiration and are removed</td>
</tr>
<tr>
<td>Scavenging</td>
<td>Performs DNS server resource record grooming for old records in DNS</td>
</tr>
</tbody>
</table>

Key Points
Time to Live (TTL), aging, and scavenging help manage DNS resource records in the zone files. Zone files can change over time, so there needs to be a way to manage DNS records that are updated or which are not valid because the hosts they represent are no longer on the network.

Additional Reading
- Enable automatic scavenging of stale resource records
- Start immediate scavenging of stale resource records
- Use Aging and Scavenging
- Help topic: Use Aging and Scavenging
Demonstration: Managing DNS Records

In this demonstration, you will see how to:

- Configure TTL
- Enable Scavenging
- Configure Aging
Testing the DNS Server Configuration

You can test the DNS server configuration by using:

- A simple query to ensure that the DNS service is answering
- A recursive query to ensure that the DNS server can communicate with the upstream DNS service

Key Points

In the DNS server Monitoring tab, you can configure a test that allows the DNS server to determine whether it can resolve simple local queries and perform a recursive query to ensure that the server can communicate with upstream servers.
Tools That Identify Problems With DNS

<table>
<thead>
<tr>
<th>Tool</th>
<th>Used to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nslookup</td>
<td>Troubleshoot DNS problems</td>
</tr>
<tr>
<td>Dnscmd</td>
<td>Edit the DNS configuration</td>
</tr>
<tr>
<td>Dnslint</td>
<td>Diagnose common DNS issues</td>
</tr>
</tbody>
</table>

Key Points

Issues can occur when you do not configure the DNS server, and its zones and resource records, properly. When resource records are causing issues, it can sometimes be more difficult to identify the issue because configuration problems are not always obvious.

Additional Reading

- Description of the DNSLint utility
- Help topic: Troubleshooting DNS Servers
- Troubleshooting DNS
Demonstration: Testing the DNS Server Configuration

In this demonstration, you will see how to test the DNS server configuration by using:

- Simple queries
- Recursive queries
- Nslookup
- Dnscmd
- Dnslint
Monitoring DNS using the DNS Event Log and Debug Logging

- **Monitor DNS events in the event log to:**
  - Monitor zone transfer information
  - Monitor computer events
- **Enable DNS debug logging to view granular verbose information about DNS activities**

**Key Points**

The DNS server has its own category in the event log. As with any event log in Windows Event Viewer, you should review the event log periodically.

Sometimes it may be necessary to get more details about a DNS problem than the Event viewer provides. In this instance, you can use debug logging to provide additional information.
Lab: Configuring and Verifying a DNS Solution

- Exercise 1: Configuring a DNS Infrastructure
- Exercise 2: Monitoring and Troubleshooting DNS

Logon information

<table>
<thead>
<tr>
<th>Virtual machines</th>
<th>NYC-DC1, NYC-SVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Administrator</td>
</tr>
<tr>
<td>Password</td>
<td>Pa$$wOrd</td>
</tr>
</tbody>
</table>

Estimated time: 60 minutes

Objectives:
- Configure a DNS Infrastructure to include a secondary zone, stub zone, and secure zone transfers
- Monitor DNS
**Exercise 1: Implementing a DNS Infrastructure**

**Scenario**
You are the primary DNS administrator for Woodgrove Bank. You have received a request to create two new DNS zones. The Nwtraders.msft zone is for a division in the bank that requires its own DNS domain. This division will also have a group of administrators that administer the zone’s resource records. Contoso is a company that Woodgrove Bank recently acquired. To begin integration testing, you must define a DNS domain called contoso.msft and test different zone configurations. You also need to test the zone to ensure it is resilient to failure.

**Exercise Overview:**
In this exercise, you will configure the DNS server role on a member server, and configure the contoso.msft and nwtraders.msft zones. You then will create secondary zones for each domain and create a stub zone for Nwtraders.msft.

The main tasks are as follows:

1. Start the **6421A-NYC-DC1** and **6421A-NYC-SVR1** virtual machines, and log on as **admin** with a password of **Pa$$w0rd**.
2. Configure the DNS Server role on **NYC-SVR1**.
3. Configure the Contoso.msft zone on **NYC-SVR1**.
4. Configure the Nwtraders.msft zone on **NYC-DC1**.
5. Configure zone transfer security.
6. Configure secondary zones for each domain on **NYC-SVR1** and **NYC-DC1**.
7. Configure a stub zone for Nwtraders.msft on **NYC-SVR2**.
8. Configure administrative options for the Nwtraders.msft domain.

▶ **Task 1: Start the 6421A-NYC-DC1, and 6421A-NYC-SVR1 virtual machines**
1. Start **6421A-NYC-DC1** and log on as **Administrator** using the password **Pa$$w0rd**.
2. Start **6421A-NYC-SVR1** and log on as **Administrator** using the password **Pa$$w0rd**.
Task 2: Configure the DNS Server role on NYC-SVR1
- On NYC-SVR1, in the Server Manager console, add the DNS Server role.

Task 3: Configure the Contoso.msft zone on NYC-SVR1
1. On NYC-SVR1, open the DNS console (found in Administrative Tools).
2. Create a primary forward lookup zone named Contoso.msft.
3. Use the default options in the New Zone Wizard.

Task 4: Configure the nwtraders.msft zone on NYC-DC1
1. On NYC-DC1, open the DNS console (found in Administrative Tools).
2. Create an Active Directory Integrated primary forward lookup zone named nwtraders.msft.
3. Use the default options in the New Zone Wizard.

Task 5: Configure zone transfers
1. On NYC-DC1 configure nwtraders.msft to allow zone transfers to NYC-SVR1:
   - NYC-SVR1 IP address is: 10.10.0.24.
2. On NYC-SVR1 configure contoso.msft to allow zone transfers to NYC-DC1.
   - NYC-DC1 IP address is: 10.10.0.10.
3. Answer the following question:

Question: Why do you need to configure the zone transfers?
Task 6: Configure secondary zones for each domain
1. On NYC-DC1, use the DNS console to configure a secondary forward zone for Contoso.msft:
   - The address of the primary zone server for Contoso.msft: 10.10.0.24.
2. On NYC-SVR1, use the DNS console to configure a secondary forward zone for nwtraders.com:
   - The address of the primary zone server for nwtraders.com: 10.10.0.10.

Task 7: Configure a stub zone for WoodgroveBank.com
1. On NYC-SVR1, use the DNS console to configure a stub zone for WoodgroveBank.com:
   - The address of the primary zone server for WoodgroveBank.com: 10.10.0.10.
2. Click WoodgroveBank.com and take note of the records listed.
3. On NYC-DC1, in the DNS console, click WoodgroveBank.com and verify that there are additional records that are not included in a stub zone.
4. Answer the following question:

   Question: Why use a stub zone instead of conditional forwarders?

Task 8: Configure administrative options for the nwtraders.msft domain
1. On NYC-DC1, use the DNS console to add the DL Nwtraders DNS Admins group to the nwtraders.msft access control list.
2. Grant the Read, Write, Create all Child objects, and Delete all child objects permissions to the DL Nwtraders DNS Admins group.
Exercise 2: Monitoring and Troubleshooting DNS

Scenario
Some users have complained that they are having trouble resolving domain names. You have to analyze the DNS infrastructure to ensure that there are no problems.

Exercise Overview
In this exercise, you will perform several tests to ensure the DNS infrastructure is working properly. You will use several DNS troubleshooting tools to validate DNS configuration and responses.

The main tasks are as follows:
1. Test simple and recursive queries.
2. Verify SOA records by using Nslookup.
3. Use the Dnslint command to verify name server records.
4. View performance statistics by using the Performance console.
5. Verify DNS replication.
6. Close all virtual machines and discard undo disks.

▶ Task 1: Test simple and recursive queries
- On NYC-DC1, in the DNS console, use the DNS Server Monitoring function to perform A simple query against this DNS Server.

▶ Task 2: Verify SOA records by using Nslookup
1. On NYC-DC1, open a command prompt and type nslookup.exe.
2. Configure a query type of SOA (Start of Authority).
3. Look up the SOA resource records for nwtraders.msft and contoso.msft.
Task 3: Use the Dnslint command to verify name server records
1. On NYC-DC1, open a command prompt and run the dnslint.exe command for the nwtraders.msft domain on the 10.10.0.10 IP address:
   - The dnslint.exe file is located in d:\Labfiles\dnslint.
2. Generate a Dnslint report html file:
   - The /s switch specifies that Dnslint will not refer to the Internet for the specified domain.
   - The /d switch specifies the domain to be searched.

Note: Consult the Help documentation if you need guidance.

Task 4: View performance statistics by using the Performance console
1. On NYC-DC1, use the Computer Management console to open Performance Monitor.
2. Add the A simple query against this DNS Server and A recursive query against this DNS Server DNS counters.
3. Use the Monitoring feature in the DNS Server properties to generate requests to the DNS server.
4. Review the data that the requests generate in Performance Monitor. Alternate between the graph view and the report view.
Task 5: Verify DNS replication
1. On NYC-DC1, use the DNS console to add an A resource record called Test to the nwtraders.msft zone. Use the IP address of 10.10.0.15.
2. Verify that the A resource record created on NYC-DC1 has replicated on NYC-SVR1.
3. If the A resource record does not appear, manually force replication to occur.

Task 6: Close all virtual machines and discard undo disks
1. On the host computer, click Start, point to All Programs, point to Microsoft Virtual Server, and then click Virtual Server Administration Website.
2. Under Navigation, click Master Status. For each virtual machine that is running, click the Virtual Machine Name, and in the context menu, click Turn off Virtual Machine and Discard Undo Disks. Click OK.
Module Review and Takeaways

- Review Questions
- Common Issues and Troubleshooting Tips
- Real-world Issues and Scenarios
- Best Practices
- The DNS Console
- Command-line Tools
- Monitoring Tools

Review Questions

1. You are conducting a presentation for a potential client about the advantages of using Windows Server 2008. What are the new features that you would point out when discussing the Windows Server 2008 DNS server role?

2. You are deploying DNS servers into an Active Directory domain, and your customer requires that the infrastructure is resistant to single points of failure. What must you consider while planning the DNS configuration?

3. What is the difference between recursive and iterative queries?

4. What must you configure before you can transfer a DNS zone to a secondary DNS server?
5. You are the administrator of a Windows Server 2008 DNS environment. Your company recently acquired another company. You want to replicate their primary DNS zone. The acquired company is using Bind 4.9.4 to host their primary DNS zones. You notice a significant amount of traffic between the Windows Server 2008 DNS server and the Bind server. What is one possible reason for this?

6. You must automate a DNS server configuration process so that you can automate the deployment of Windows Server 2008. What DNS tool can you use to do this?

**Common Issues and Troubleshooting Tips**

- To resolve DNS resource record resolution problems:
  - If the change to the resource record is recent, it may not be replicated to all DNS servers.
  - In larger organizations where DNS is integrated with Active Directory, convergence can take longer.
  - The client can sometimes cache invalid DNS records. Therefore, you should clear the local DNS cache.
  - Servers on the Internet may need additional time to update information in their own cache and organization before any changes you have made begin to work properly.

- To resolve issues with DNS zone transfers:
  - Ensure that the server trying to transfer the zone is permitted in the primary zone configuration.
  - Ensure that the server to which the zone is transferring supports the zone transfer features in Windows Server 2008. It may be necessary to turn off some features.
  - Ensure that a firewall or other port-management devices that reside between the two DNS servers are not blocking Port 53 UDP.
• To resolve problems when the DNS Server responds slowly to requests:
  • Verify that other programs are not impacting the server with the DNS Server role.
  • Use Performance Monitor to identify the load on the server that DNS requests generate. It may be necessary to split the load or create additional subzones.
  • Ensure that there are not a large number of stale resource records.

**Real-world issues and scenarios**

• Reverse DNS zones
  
  Typically, administrators do not create reverse DNS zones in their DNS infrastructure. This will not cause any obvious issues at first. However, many applications use reverse DNS to resolve name information about hosts on which they are running.

  Some applications require that a reverse zone and pointer resource records are defined. Many e-mail security devices and software routinely check for a reverse DNS record for the IP address communicating with it.

• DNS and Active Directory trusts
  
  When creating trusts between two Active Directory domains, the ability for domain A to lookup records in domain B (and vice versa) is tied to the configuration of the DNS infrastructure. Active Directory domains are accessible rarely on the Internet. Therefore, you need conditional forwarders, stub zones, or secondary zones to replicate the DNS infrastructure across domains and forests.

• Secure zones against zone dumping
  
  By default, zone transfers are disabled in Windows Server 2008. When configuring zone transfers, it is a best practice to specify the IP address of the servers to which you want to transfer zone data. We recommend strongly that the Allow zone transfer to Any Server is not selected, especially if the server is on the Internet. With this option enabled, it is possible to dump the entire zone, which can provide a significant amount of information about the network to possible attackers.
Best Practices

- Enter the correct e-mail address of the responsible person for each zone you add to, or manage on, a DNS server. Applications use this field to notify DNS administrators for a variety of reasons. For example, query errors, incorrect data returned in a query, and security problems are a few ways in which this field can be used. While most Internet e-mail addresses contain the “@” symbol to represent the word “at” in e-mail, this symbol must be replaced with a period (.) when entering an e-mail address for this field. For example, instead of “administrator@microsoft.com”, you would use “administrator.microsoft.com”.

For more information on configuring the responsible person for a zone, see Modify the start of authority (SOA) record for a zone at http://technet2.microsoft.com/WindowsServer/en/library/e1f77652-7e1f-4902-9107-6b863cc843501033.mspx.

- Be conservative when adding alias records to zones

Avoid using CNAME resource records (RRs) to alias a host name used in a host (A) resource record if they are unnecessary. Also, ensure that no other RRs use any alias names you use.

DNS allows an owner name of a CNAME resource record to be used as the owner name of the other types of resource records, such as NS, MX, and TXT resource records.

For more information, see the Help topic: Managing resource records.

- If you are using Active Directory, use directory-integrated storage for your DNS zones. This offers increased security, fault tolerance, and simplified deployment and management.

By integrating zones, you can simplify network planning. For example, domain controllers for each of your Active Directory domains correspond in a direct one-to-one mapping to DNS servers. This can simplify planning and troubleshooting DNS and Active Directory replication problems because the same server computers are used in both topologies.
If you are using directory-integrated storage for your zones, you may select from the different replication scopes that replicate your DNS zone data throughout the directory. If your DNS infrastructure must support Windows 2000 DNS servers, you will use the directory-integrated storage method that replicates DNS zone data to all of a domain’s controllers. If your DNS infrastructure is composed of DNS servers running Windows Server 2003 only, you may also select from replication scopes that replicate your DNS zone data to all DNS servers in the Active Directory forest, all DNS servers in a specified Active Directory domain, or all domain controllers specified in a custom replication scope.

Any DNS server hosting a directory-integrated zone is a primary DNS server for that zone. This enables a multimaster model where multiple DNS servers may update the same zone data. A multimaster model eliminates a single point of failure associated with a conventional single-master DNS topology, where updates may be done only to a single DNS server for a given zone.

One of the important benefits of directory integration is the support for secure dynamic update of the names within a zone. For more information, see Dynamic update at http://technet2.microsoft.com/WindowsServer/en/library/e760737e-9e55-458d-b5ed-a1ae9e04819e1033.mspx.

- Consider the use of secondary zones to assist in off-loading DNS query traffic wherever appropriate.

You can use secondary servers as backups for DNS clients, which enables you to load balance DNS query traffic on your network and reserve your DNS-enabled primary servers for use only by those clients that need them to perform dynamic registration and updates of their A and PTR RRs.

Disable Recursion for servers that do not answer client queries or communicate using forwarders. As DNS servers communicate amongst themselves using iterative queries, this ensures that the server responds only to queries that are intended for it.

The DNS Console

The primary tool that you use to manage DNS servers is the DNS console, which is located in the Administrative Tools folder on the Start menu. You can use the DNS console alone or as a Microsoft Management Console (MMC), further integrating DNS administration into your total network management. It also is available in Server Manager on computers with the DNS Server role installed.
Command-Line Tools

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nslookup</td>
<td>Use to perform query testing of the DNS domain namespace.</td>
</tr>
<tr>
<td>Dnscmd</td>
<td>Use this command-line interface to manage DNS servers. This utility is useful in scripting batch files to help automate routine DNS management tasks or to perform simple unattended setup and configuration of new DNS servers on your network.</td>
</tr>
<tr>
<td>Ipconfig</td>
<td>Use this command to view and modify IP configuration details that the computer uses. This utility includes additional command-line options to provide help in troubleshooting and supporting DNS clients.</td>
</tr>
<tr>
<td>DNSlint</td>
<td>Provides several automated tests to verify that DNS servers and resource records are configured properly and pointing to valid services. You can download this command from Microsoft at <a href="http://support.microsoft.com/kb/321045">http://support.microsoft.com/kb/321045</a>.</td>
</tr>
</tbody>
</table>

Monitoring Tools

The Windows Server 2008 family includes the following options for monitoring DNS servers:

- Default logging of DNS server event messages to the DNS server log. DNS server event messages are separated and kept in their own system event log – the DNS server log – which you can view using the DNS console or Event Viewer.

- Optional debug options for trace logging to a text file on the DNS server computer. You also can use the DNS console to enable additional debug logging options for temporary trace logging of DNS server activity to a text-based file. The file that is created and used for this feature, Dns.log, is stored in the systemroot\System32\Dns folder.

- Windows Performance Monitor. You can monitor specific DNS performance counters in real time to diagnose DNS problems and resource-contention issues.