Instructor Notes

Presentation: 1 hour 10 minutes
This module provides students with the knowledge and ability to manage and monitor Domain Name System (DNS).

Lab: 25 minutes
After completing this module, students will be able to:

- Manage the properties of DNS records.
- Test DNS server configuration.
- Monitor DNS server performance.

Required materials
To teach this module, you need Microsoft® Office PowerPoint® file 2277C_06.ppt

Important It is recommended that you use PowerPoint 2002 or later to display the slides for this course. If you use PowerPoint Viewer or an earlier version of PowerPoint, some features of the slides may not be displayed correctly.

Preparation tasks
To prepare for this module:

- Read all of the materials for this module.
- Complete all practices and the lab.
- Review prerequisite courses and modules.
How to Teach This Module

Explain to the students how the practices and labs are designed for this course. A module includes two or more lessons. Most lessons include a practice. After completing all of the lessons for a module, students finish the module with a lab.

Practices

This course does not include instructor demonstrations, but you should demonstrate many of the administrative tasks as you teach them. After you have covered the contents of the lesson, explain that a practice will give students a chance for hands-on learning of all the tasks discussed in the lesson.

Labs

At the end of each module, the lab enables the students to practice the tasks that are discussed and applied in the module.

Using scenarios that are relevant to the job role, the lab gives students a set of instructions in a two-column format. The left column provides the task (for example, “Create a group”). In the right column are specific instructions that the students will need to perform the task (for example, “From Active Directory Users and Computers, double-click the domain node”).

An answer key for each lab exercise is located on the Student Materials CD, in case the students need step-by-step instructions to complete the lab. They can also refer to the practices and How To pages in the module.
### Lesson: Managing DNS Records

This section describes the instructional methods for teaching this lesson.

#### What Is the Time to Live?
- Define the Time to Live (TTL) value.
- Explain the purpose of a TTL.
- Describe how a TTL value works. Refer to the slide.
  - This topic has an animated slide, so be sure to review the slide prior to class.

#### What Are Aging and Scavenging Parameters?
- Define aging and scavenging.
- Explain the purpose of aging and scavenging.
- Explain what the aging and scavenging parameters are, by referring to the slide.
- Explain the purpose of the no-refresh and refresh intervals.

#### How Aging and Scavenging Work
- Describe how aging and scavenging work.
- Provide an example of how aging and scavenging work. Refer to the slide.
  - This topic has an animated slide, so be sure to review the slide prior to class.

#### Practice: Managing DNS Records
- Direct the students to complete the following practice tasks:
  - Modify the default TTL for a zone.
  - Modify the TTL for a record.
  - Configure aging and scavenging.
- Reconvene class after all students have completed the practice and discuss the results of the practice.

### Lesson: Testing the DNS Server Configuration

This section describes the instructional methods for teaching this lesson.

#### What Are Simple and Recursive Queries?
- Explain the purpose of simple and recursive queries.
- Explain what a simple query is.
- Explain what a recursive query is.
- Describe how simple and recursive queries work. Refer to the example in the slide.
  - This topic has an animated slide, so be sure to review the slide prior to class.

#### Why Verify That a Resource Record Exists?
- Explain the purpose of verifying resource records.
- Discuss the tools that administrators can use to monitor, manage, and troubleshoot DNS, including Nslookup, Dnscmd, and Dnslint.
What Is Nslookup?
- Define Nslookup.
- Explain the purpose of Nslookup.
- Discuss how students can use Nslookup for verifying resource records and for many other tasks. Discuss some of the other tasks that can be done by using Nslookup.
- Explain that there are two modes for Nslookup: interactive and no interactive.
- Discuss the Nslookup syntax.
- Provide an example of the command-line output for an Nslookup session. Refer to the slide.

What Is Dnscmd?
- Define Dnscmd.
- Explain the purpose of Dnscmd.
- Discuss how students can use Dnscmd for verifying resource records and for many other tasks. Discuss some of the other tasks that can be done by using Dnscmd.
- Discuss the Dnscmd parameters.
- Provide an example of Dnscmd by referring to the slide.

What Is Dnslint?
- Define Dnslint.
- Explain the purpose of Dnslint.
- Discuss how students can use Dnslint for verifying resource records and for many other tasks. Discuss some of the other tasks that can be done by using Dnslint.
- Discuss the Dnslint functions and syntax.
- Provide an example of Dnslint output for a scan by referring to the slide.

Practice: Testing the DNS Server Configuration
- Direct the students to read the scenario.
- Direct the students to complete the following practice tasks:
  - Test DNS by using a simple and recursive query.
  - Verify records by using Nslookup.
  - View DNS zone information by using Dnscmd.
  - Test DNS by using Dnslint.
- Reconvene class after all students have completed the practice and discuss the results of the practice.
Lesson: Monitoring DNS Server Performance

This section describes the instructional methods for teaching this lesson.

- Explain that monitoring DNS server performance can help by:
  - Providing a baseline.
  - Help in troubleshooting DNS servers by using the performance data.
  - See the Microsoft Windows Server™ 2003 Help documentation for information about DNS performance.
- Discuss how to apply the guidelines.

### Guidelines for Monitoring DNS Server Performance by Using the Performance Console

- Define DNS event log.
- Explain the purpose of a DNS event log.
- Explain what a DNS event log file is.
- Discuss common types of DNS events.
- Provide examples of common DNS events by referring to the slide.

### What Is a DNS Event Log?

- Define DNS debug logging.
- Explain the purpose of DNS debug logging.
- Discuss characteristics of DNS debug logging.
- Discuss DNS debug logging options.
- Provide an example of DNS debug logging by referring to the slide.

### What Is DNS Debug Logging?

- Direct the students to read the scenario.
- Direct the students to complete the following practice tasks:
  - Monitor DNS by using the Performance console.
  - Monitor DNS by using event logs.
  - Configure DNS debug logging.
- Reconvene class after all students have completed the practice and discuss the results of the practice.

### Practice: Monitoring DNS Server Performance

Lab: Managing and Monitoring DNS

Remind the students that they can review the module for assistance in completing the lab. Tell students that a detailed answer key for each lab is provided in the Labdocs folder on the Student Materials CD.
Overview

Domain Name System (DNS) servers are critical to a network; therefore, you must manage and monitor them to ensure that they are functioning properly and to optimize network performance.

Important For more information about securing DNS, see the Microsoft® Windows Server™ 2003 Enterprise Edition Help documentation.

Objectives

After completing this module, you will be able to:

- Manage the properties of DNS records.
- Test the DNS server configuration.
- Monitor DNS server performance.
Lesson: Managing DNS Records

- What Is the Time to Live?
- What Are Aging and Scavenging Parameters?
- How Aging and Scavenging Work
- Practice: Managing DNS Records

Introduction
As a part of managing DNS, you can configure the Time to Live (TTL) value on resource records. The TTL value is used to determine how long clients should cache records they have recently resolved. You can configure aging and scavenging settings to allow outdated records to be automatically removed from the DNS database.

Lesson objectives
After completing this lesson, you will be able to:
- Describe how the TTL value works.
- Configure the TTL value.
- Explain what aging and scavenging parameters are.
- Describe how aging and scavenging work.
- Manage DNS records.
What Is the Time to Live?

The Time to Live (TTL) value indicates how long a record should be cached by clients and other DNS servers. The TTL is a time-out value expressed in seconds that is included with DNS records that are returned in a DNS query. The TTL value tells the recipients how long to hold or use the resource record or any of its included data before allowing the data to expire and discarding it.

The TTL process is as follows:

1. The records in the zone are sent to other DNS servers and DNS clients as responses to queries.
2. Records are cached based on the TTL period supplied in the record.
3. When the TTL expires, the record is removed from the cache.

If the TTL is set too short, DNS query traffic increases because the DNS clients may request name resolution for the expired records.

---

**Definition**
The Time to Live (TTL) value indicates how long a record should be cached by clients and other DNS servers. The TTL is a time-out value expressed in seconds that is included with DNS records that are returned in a DNS query. The TTL value tells the recipients how long to hold or use the resource record or any of its included data before allowing the data to expire and discarding it.

**How a TTL value works**
The TTL value for a zone is applied to all records that are created in that zone. The TTL value for a record is applied to that record and overrides the TTL applied to the zone.

**Note** To see the TTL value on a resource record, you must enable the Advanced option from the View menu in the DNS Management console.
If the TTL is set too long for a record, the DNS clients may cache outdated records.

The TTL value for a zone can be adjusted only on the server that hosts the primary zone. If records are modified infrequently, you may want to increase the TTL value to cause the records to be cached longer. This, in turn, will reduce DNS queries to your DNS server. The default TTL for a zone is one hour.

**Example**

You may want to increase the TTL value on the resource record for a Web server whose IP address does not change. This would cause other clients and DNS servers on the Internet to cache the record for a greater period of time and, in turn, reduce the number of DNS queries to your DNS server.
What Are Aging and Scavenging Parameters?

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>No-Refresh Interval</td>
<td>DNS server does not accept refresh attempts</td>
<td>7 days</td>
</tr>
<tr>
<td>Refresh Interval</td>
<td>DNS server does accept refresh attempts</td>
<td>7 days</td>
</tr>
</tbody>
</table>

Definitions

The *aging* process allows a DNS server to determine whether a stale DNS resource record should be removed from the DNS database.

*Scavenging* is the process of cleaning and removing outdated or extinct names data from the DNS database.

Purpose of aging and scavenging

Aging and scavenging help keep zone data current by automatically removing outdated zone data. The process of aging and scavenging is of particular importance in a DNS environment that supports dynamic updates. Because resource records can automatically be modified by clients, in some cases these records are not automatically removed when computers are removed from the network. For example, if a computer registers its own host resource record at startup but is later improperly disconnected from the network, its host resource record might not be deleted from DNS. If your network has mobile users and computers, this situation can occur frequently.

In addition, stale resource records take up space in the DNS database and can cause unnecessarily long zone transfers. These outdated resource records may be sent as responses to queries and may cause name resolution problems for DNS clients.

To remove outdated resource records from the DNS database, Windows Server 2003 DNS server can scavenge outdated resource records by searching the database for resource records that have aged for a specified period and deleting those records from the database.
Aging and scavenging parameters for a zone

To determine when to scavenge records, DNS uses the time stamp for each record, along with the aging and scavenging parameters. Aging and scavenging must be enabled on both the DNS server and the DNS zone. There are two configurable options for aging and scavenging:

- **No-refresh interval.** During this span of time, a DNS server does not accept refresh attempts.
- **Refresh interval.** During this span of time, a DNS server accepts refresh attempts.

In a refresh attempt, a computer requests to renew its DNS record. A refresh attempt occurs when the client that owns the DNS record attempts to reregister the resource record when no information has changed in the record.

Note  
Manually entered DNS resource records have a time stamp of zero, which means they never age. When manually entering a DNS resource record, you can subject that record to aging and scavenging by setting a valid time stamp. To configure a manually created record for aging and scavenging, enable the Advanced option from the View menu in the DNS Management console, access the properties of the record, and then select Delete this record when it becomes stale.

Purpose of the no-refresh and refresh intervals

You can configure the no-refresh and refresh intervals to reduce DNS replication in an infrastructure that uses DNS dynamic updates.

By default, a DNS client refreshes its name and IP address information every 24 hours. Other events on the system may also trigger a refresh event. Every time DNS refreshes a DNS database entry, even when it does not modify the host name or IP address, it modifies the DNS attribute on that record. The modified attribute needs to be replicated to all DNS servers that host the zone.

The purpose of the no-refresh interval is to prevent clients from refreshing their records when information is unchanged. This helps reduce unnecessary zone replication traffic. By default, the no-refresh interval for a zone is 7 days. After the no-refresh interval has elapsed, the DNS server will accept refresh attempts from clients. Clients must refresh their records during the refresh interval. If a record is not refreshed during the refresh interval, the record is considered to be stale and can be removed from the database the next time the scavenging process occurs. By default, the refresh interval is 7 days.
How Aging and Scavenging Work

A sample DNS host, DEN-CL1.contoso.msft, registers its host (A) resource record at the DNS server for a zone where aging and scavenging is enabled for use.

1. When registering the resource record, the DNS server places a time stamp on the record, based on the server’s current time.

2. After the resource record’s time stamp is written, the DNS server does not accept refreshes for this resource record during the zone’s no-refresh interval. It can, however, accept updates prior to that interval.

   For example, if the IP address for DEN-CL1.contoso.msft changes, the DNS server can accept the update. In this case, the server also updates (resets) the resource record time stamp.

3. Upon expiration of the no-refresh period, the server begins to accept attempts to refresh this resource record.

   After the initial no-refresh period ends, the server does not suppress attempts to refresh the resource record for its remaining life span.

4. During the refresh period, if the server receives a refresh request for the resource record, it processes the request. Any updates to the record will reset the time stamp for the resource record, as described in step 2.
6. When the server performs subsequent scavenging for the Contoso.msft zone, the server examines the resource record and all other zone records. Each resource record is compared to the current time on the server on the basis of the following formula to determine whether the resource record should be removed:

\[
\text{resource record time stamp + no-refresh interval for zone + refresh interval for zone}
\]

7. If the sum of this formula is greater than current server time, no action is taken, and the resource record continues to age in the zone. If the sum is less than current server time, the resource record is deleted from the zone.

Example

In the preceding illustration, a host record is registered and time-stamped in DNS on January 1. The DNS server and the DNS zone are both configured for aging and scavenging. The no-refresh interval is 7 days, and the refresh interval is 7 days. After the initial 7-day TTL expires, the refresh interval provides an additional 7 days. On January 15, the TTL expires and the record can be scavenged from the DNS database.
Practice: Managing DNS Records

In this practice, you will:

- Modify the default TTL for a zone
- Modify the TTL for a record
- Configure aging and scavenging

Objectives

In this practice, you will:

- Modify the default TTL for a zone.
- Modify the TTL for a record.
- Configure aging and scavenging.

Instructions

Ensure that the DEN-DC1 virtual machine is started.

Practice

► Change the default TTL for the Contoso.msft zone

1. Log on to DEN-DC1 as Contoso\Administrator, with the password of Pa$$w0rd.
2. Click Start, point to Administrative Tools, and then click DNS.
3. In the DNS console tree, expand DEN-DC1, expand Forward Lookup Zones, and then select Contoso.msft.
4. Right-click Contoso.msft and then click Properties.
5. On the Start of Authority (SOA) tab, change the value of the Minimum (default) TTL to 30 minutes and then click OK.

► Modify the TTL for a record

1. In the console tree, right-click Contoso.msft and then click New Host (A).
2. In the Name field, type TTLTest. In the IP address field, type 10.10.10.10. Click Add Host, click OK, and then click Done.
3. In the View menu, click Advanced.
4. In the Contoso.msft zone, right-click the **TTLTest** record and then click **Properties**. What is the TTL for the record?
   
   *30 Minutes*

5. In the Time to live (TTL) field, change the value to **15 minutes** and then click **OK**.

**Configure aging and scavenging**

1. In the console tree, right-click **DEN-DC1** and then click **Properties**.
2. On the **Advanced** tab, click **Enable automatic scavenging of stale records** and then click **OK**.
3. In the console tree, right-click **Contoso.msft** and then click **Properties**.
4. On the **General** tab, click **Aging**.
5. Click **Scavenge stale resource records**, click **OK**, and then click **OK** again.
6. In the console tree, right-click **Contoso.msft** and then click **Refresh**.
7. Right-click **Contoso.msft** and then click **Properties**.
8. On the **General** tab, click **Aging**. Notice the default no-refresh and refresh intervals.
9. Click **OK** twice.
10. Close the DNS console.
Lesson: Testing the DNS Server Configuration

Introduction
Whenever the DNS server configuration changes, it is important to test the DNS server to ensure that the configuration still functions properly. This lesson introduces various tools for this purpose.

Lesson objectives
After completing this lesson, you will be able to:
- Describe how simple and recursive queries work.
- Explain the purpose of verifying that resource records exist.
- Explain what Nslookup is.
- Explain what Dnscmd is.
- Explain what Dnslint is.
- Test DNS server configuration.
What Are Simple and Recursive Queries?

Introduction
You can test a DNS server by performing two types of queries: simple and recursive.

Purpose of simple and recursive queries
Whenever the DNS server configuration changes, it is important to test the DNS server to ensure that the configuration still functions properly. By using the testing query functions on the DNS server, you can verify that the DNS queries are functioning. This is useful when you are troubleshooting DNS name resolution problems. By testing the DNS server configuration in this manner, you can narrow down where the name resolution problem resides. You can configure automatic testing to occur at regularly scheduled intervals.

Simple query
A simple query performs a local test on the DNS server by using the local DNS client to issue a query. Because this test is local, no network connectivity is required between the DNS server and other network components. This type of test directs the DNS server to perform a simple or iterative query locally. This localized query uses the DNS client resolver on the DNS server to query the local DNS service. This query does not generate any network traffic. If the simple query fails, it indicates a critical problem with the local DNS service. The DNS service may need to be restarted or reinstalled on the server.

Recursive query
A recursive query tests a DNS server by forwarding a query to another DNS server. This type of test specifies that the DNS server must perform a recursive query. This test is similar (in its initial query processing) to the simple query in that it uses the local DNS client resolver to query the local DNS server, which is located on the same computer.
In this test, however, the client asks the server to use recursion to resolve an NS-type query for the root of the DNS domain namespace. This type of query typically requires additional recursive processing and can be helpful in verifying that server root hints or zone delegations have been properly configured.

If this query fails, it indicates that the DNS server is unable to resolve names by using root hints or forwarders. To resolve this issue, ensure that your server is properly configured for root hints and forwarders. Additionally, network connectivity problems may also cause the recursive query to fail.

**Example**

In the preceding illustration, the DNS client resolver on the DNS server sends a simple query to the local DNS service. The simple query either passes or fails.

The DNS client resolver on the DNS server sends a recursive query to the local DNS server, which then forwards the query to the authoritative DNS server for resolution. The recursive query either passes or fails.
Why Verify That a Resource Record Exists?

Verifying that a resource record exists is a basic function of monitoring and troubleshooting DNS. If the DNS server contains outdated, stale, or incorrect host name–to–IP address mappings, the clients cannot connect to network services. With the amount of dynamic change that occurs in the DNS service, it is important to be able to verify that DNS resource records are both correct and updated.

To identify problems with your DNS solution, you can verify:

- Missing records.
- Incomplete records.
- Incorrectly configured records.

You can use the following three tools to monitor DNS:

- Nslookup
- Dnscmd
- Dnslint

The next section focuses on using these tools to verify resource records, which is only one of the many tasks that these tools can accomplish.
What Is Nslookup?

**Nslookup is a command-line tool used to diagnose DNS infrastructure**

*Definition*

Nslookup is a command-line tool that is used to help diagnose problems with the DNS infrastructure. Nslookup is installed on all computers that run Microsoft Windows® 2000 or later.

*Purpose of Nslookup*

Nslookup provides the ability to perform query testing of DNS servers and to obtain detailed responses. This information is useful in troubleshooting name resolution problems, in verifying that resource records are added or updated correctly in a zone, and in debugging other server-related problems.

*Nslookup syntax*

Nslookup has two modes:

- **Interactive.** This mode allows you to type commands in Nslookup and view the results in a Command Prompt window. Use the interactive mode when you need more than one piece of data.

- **Noninteractive.** This mode allows you to execute an Nslookup command in a single step, which can either be run on its own from the command prompt or inserted into a batch file. Noninteractive mode provides a single piece of data as output. The output can be stored in a text file for later viewing. This mode is useful when you configure a performance alert to run a batch file.
To enter Nslookup in interactive mode, type `nslookup` at the command prompt. The following table describes the Nslookup syntax in interactive mode.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-option...</code></td>
<td>Specify one or more Nslookup commands. For a list of available commands, type a question mark (<code>?</code>). Nslookup commands include:</td>
</tr>
<tr>
<td></td>
<td>• Exit</td>
</tr>
<tr>
<td></td>
<td>• Help</td>
</tr>
<tr>
<td></td>
<td>• Set type</td>
</tr>
<tr>
<td></td>
<td>• View</td>
</tr>
<tr>
<td><code>computer_to_find</code></td>
<td>If you specify the IP address of a computer, Nslookup returns the host name. If you specify the host name of a computer, Nslookup returns the IP address. If the host name that you are querying for does not have a trailing period, the default DNS domain name is appended to the name. To find a computer outside the current DNS domain, append a period to the name. For example, find a host record by using the following set option:</td>
</tr>
<tr>
<td></td>
<td><code>Set type=a</code></td>
</tr>
<tr>
<td></td>
<td>DEN-SRV1</td>
</tr>
<tr>
<td></td>
<td>These commands would return the IP address for DEN-SRV1.</td>
</tr>
<tr>
<td><code>-server</code></td>
<td>Specify the server to use as the DNS server. If you omit the server, the currently configured default DNS server is used; for example: <code>Server.DEN-DC1.contoso.msft</code>.</td>
</tr>
</tbody>
</table>

**Note** For Nslookup to work properly, a pointer (PTR) resource record on the server must be the subject of the lookup. At startup, Nslookup performs a reverse lookup on the IP address of the server that is running the DNS Server service. Nslookup reports an error if it cannot resolve the address to a name. This error does not hinder the normal performance of Nslookup for diagnostics.

**Examples**

The illustration in the PowerPoint slide provides an example of the command-line output for an Nslookup session. This session is used to verify the existence of both the host (A) record for DEN-SRV1 and the service locator (SRV) resource records, which are registered by Windows Server 2003 domain controllers. In this example, the domain controller DEN-DC1 is registered for the Contoso.msft domain.

**Note** Some commands issued by Nslookup perform zone transfers. If zone transfers are not allowed to the system where the command is being run, a query-refused message will appear. To resolve this problem, allow zone transfers to the system when Nslookup is run. The `-ls` option in Nslookup can be used to retrieve records through zone transfers.
What Is Dnscmd?

Dnscmd is a command-line tool that is included in the support tools on the Windows Server 2003 CD. Dnscmd allows an administrator to complete many of the DNS administrative tasks on the DNS server from a Command Prompt window.

By using Dnscmd, you can check dynamic registration of DNS resource records, including secure DNS updates, in addition to deregistration of resource records.

Dnscmd can be useful when you have to accomplish a DNS configuration task for numerous DNS servers. Instead of using the DNS administrative tool, you can use the command-line tool.

Dnscmd is also useful when you need to modify DNS server settings remotely. By creating a batch file, which includes the `dnscmd` command, you can send the batch to a DNS server and execute it remotely.

**Dnscmd parameters**

The syntax of the `dnscmd` command is as follows:

```
dnscmd ServerName Command [Command Parameters]
```

The following table lists some Dnscmd commands and their descriptions.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/Info</td>
<td>Displays general DNS server configurations</td>
</tr>
<tr>
<td>/enumzones</td>
<td>Lists the zones on the server</td>
</tr>
<tr>
<td>/clearcache</td>
<td>Clears the DNS server cache</td>
</tr>
<tr>
<td>/zoneinfo zone name</td>
<td>Displays information about a zone</td>
</tr>
<tr>
<td>/enumrecords zone name</td>
<td>Lists records for a specific zone; can be filtered to display specific types of records such as NS or CNAME</td>
</tr>
</tbody>
</table>
Example

In the slide, the Dnscmd tool is used to view all the zones on DNS server 192.168.1.17. In this example, the initial `dnscmd` command allowed the administrator to view the switches that are associated with each zone.

The final `dnscmd` command displays DNS zone information on the Nwtraders.msft zone by using the zone name that is reported in the initial `dnscmd` command.
What Is Dnslint?

Dnslint is a command-line tool that is included in the support tools on the Windows Server 2003 CD. The Dnslint tool can run a series of queries to help diagnose common DNS name resolution problems.

Verifying the existence or consistency of a particular set of DNS records on multiple DNS servers can help diagnose and fix problems that are caused by missing or incorrect DNS records.

For example, if clients are experiencing problems logging on to the domain, verifying that the SRV records (which clients use to find Lightweight Directory Access Protocol [LDAP] and Kerberos servers) are available and accurate can help you ascertain whether DNS is a cause of the problem.

Another example scenario occurs when you receive reports that customers are having problems accessing your Web site. It would be beneficial to have a tool that quickly checks all of the DNS records that are involved with the Web farm on each of the DNS servers that are supposed to contain these records. You could then quickly determine whether there are missing or incorrect DNS records that may be related to the problem.

In a third scenario, you are experiencing problems with e-mail delivery: You can send e-mail, but you are not receiving any. Name resolution could be the problem. To confirm this hypothesis (or to eliminate it as a possibility), you need to check all of the DNS records on all of the DNS servers that are used to resolve the e-mail server’s IP address.
Dnslint has three functions that verify DNS records and generate a Hypertext Markup Language (HTML) report:

- **Dnslint /d** diagnoses potential causes of lame delegation and other related DNS problems. *Lame delegation* occurs when a DNS subdomain is configured to be delegated to a DNS server that either does not exist or does not act authoritatively for that subdomain.

- **Dnslint /ql** verifies a user-defined set of DNS records on multiple DNS servers.

- **Dnslint /ad** verifies DNS records that are specifically used for Active Directory® directory service replication.

The syntax for Dnslint is as follows:


- Use the /d switch to request domain name tests. This switch is useful when you troubleshoot lame delegation problems.
- Use the /ad switch to request Active Directory tests.
- Use the /ql switch to request DNS query tests from a list. You create a sample input file by running the `dnslint /ql autocreate` command.
- Use the /e switch to request connectivity tests on e-mail servers.
- To prevent the report from automatically opening, use the /no_open switch, which is useful in scripts.
- Use the /r switch to specify the name of the report file that is created.
- Use the /s switch to bypass an InterNIC whois lookup. You can specify a DNS server IP address instead of querying InterNIC for one.
- Use the /t switch to request output to a text file.
- Use the /test_tcp switch to request a test of Transmission Control Protocol (TCP) port 53. By default, only User Datagram Protocol (UDP) port 53 is tested.
- Use the /v switch to request verbose output to the screen.
- Use the /y switch to overwrite an existing report file without the user being prompted. The /y switch is useful in scripts.

**Note** The /d, /ad, and /ql switches for Dnslint must be used separately.

**Example**

The illustration in the slide provides an example of Dnslint HTML output for the Contoso.msft domain. The HTML report shows the command that was issued to generate the report and the name server that is authoritative for Contoso.msft.
Practice: Testing the DNS Server Configuration

In this practice, you will:
- Test DNS using a simple and recursive query
- Verify records by using Nslookup
- View DNS zone information by using Dnscmd
- Test DNS by using Dnslint

Ensure that the DEN-DC1 virtual machine is started.

Test DNS using a simple and recursive query
1. If necessary, log on to DEN-DC1 as Contoso\Administrator, with the password of Pa$$w0rd.
2. Click Start, point to Administrative Tools, and then click DNS.
3. From the DNS console tree, right-click DEN-DC1 and then click Properties.
4. On the Monitoring tab, click A simple query against this DNS server and A recursive query to other DNS servers.
5. Click Test Now.
   What are the results?
   **Simple query passes, recursive query fails**

   What can explain the results of the recursive query?
   The DNS service is running on the local computer, so the simple query succeeds. The DNS server is not configured with a forwarder, and cannot communicate with the root servers, so the recursive query fails.

6. Click OK.

   ► **Verify records by using Nslookup**

   1. Click Start, point to All Programs, point to Windows Support Tools, and then click Command Prompt.
   2. At the command prompt, type Nslookup and then press ENTER.
   3. Type set type=soa and then press ENTER.
   4. Type Contoso.msft and then press ENTER. What is the serial number for the SOA record?
      **Answers will vary.**

   5. Type Set type=NS and then press ENTER.
   6. Type Contoso.msft and then press ENTER. What are the name servers for Contoso.msft?
      **Den-dc1.contoso.msft**

   7. Type set type=a and then press ENTER.
   8. Type DEN-DC1.contoso.msft and then press ENTER. What is the IP address of DEN-DC1?
      **10.10.0.2**

   9. Type Exit and then press ENTER.
   10. To view records by using Nslookup in noninteractive mode, at the command prompt, type nslookup -type=soa contoso.msft and then press ENTER.
   11. At the command prompt, type nslookup -type=ns contoso.msft and then press ENTER.
View DNS zone information by using Dnscmd

1. At the command prompt, type `dnscmd /info` and then press ENTER. What is the scavenging interval for the server?
   
   168 hours

2. At the command prompt, type `dnscmd /enumzones` and then press ENTER. What type of zone is Contoso.msft?
   
   Primary, AD-Domain

3. At the command prompt, type `dnscmd /enumrecords contoso.msft @` and then press ENTER.
   
   What type of record is TTLTest?
   
   Host or A record

   What is the TTL for TTLTest?
   
   900 seconds

Test DNS by using Dnslint

1. At the command prompt, type `dnslint /d contoso.msft /s 10.10.0.2` and then press ENTER. Click OK at the Microsoft Internet Explorer prompt.
   
   What is the refresh period on the SOA record?
   
   3600 seconds

   What is the default (minimum) TTL for Contoso.msft?
   
   1800 seconds

   What is the mail server for Contoso.msft?
   
   none listed

2. Close Internet Explorer.
3. Close all open windows.
Lesson: Monitoring DNS Server Performance

Introduction
As an administrator, you can provide useful baseline data and troubleshoot DNS issues by using the Performance console to monitor the performance of a DNS server.

In addition, there are several tools built into a DNS server running Windows Server 2003 to help monitor DNS events and data. These tools include DNS Event Viewer and DNS debug logging.

Lesson objectives
After completing this lesson, you will be able to:

- Apply guidelines for monitoring DNS server performance when using the Performance console.
- Define a DNS event log.
- Define DNS debug logging.
- Describe how DNS debug logging works.
- Use logging to monitor DNS server performance.
Guidelines for Monitoring DNS Server Performance by Using the Performance Console

<table>
<thead>
<tr>
<th>Performance counter</th>
<th>What to look for after a baseline is established</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Update Rejected</td>
<td>Any increase over the baseline may be cause for further investigation</td>
</tr>
<tr>
<td>Recursive Queries/sec</td>
<td>If this counter goes dramatically up or down, it should be further investigated</td>
</tr>
<tr>
<td>AXFR Request Sent</td>
<td>If this counter dramatically increases or decreases, it should be investigated</td>
</tr>
</tbody>
</table>

Introduction

Because DNS servers are critically important in most environments, their performance must be monitored. Some practices that support effective monitoring are:

- Providing a useful baseline for predicting, estimating, and optimizing DNS server performance.
- Troubleshooting DNS servers where server performance has degraded—either over time or during periods of peak activity.

As you begin your DNS server monitoring, you can review sample test results (for DNS servers running Windows Server 2003) that were collected during product development and testing. You can use this information as a starting reference as you begin to monitor your DNS servers to measure and define baseline performance.

Note

For more information about the sample test results collected during product and testing for DNS servers running Windows Server 2003, see the Windows Server 2003 Help documentation for DNS performance.

Windows Server 2003 also provides a set of DNS server performance counters that can be used with System Monitor to measure and monitor various aspects of server activity.
It is recommended that you monitor the critical phases of DNS activity, such as dynamic update, notify, incremental and full zone transfers, queries, and the health of the DNS server. The following table includes some common performance counters that can be helpful in monitoring DNS.

<table>
<thead>
<tr>
<th>Performance counters</th>
<th>What data is collected</th>
<th>What the data means</th>
<th>What to look for after baseline is established</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dynamic Update Rejected</strong></td>
<td>The total number of dynamic updates that the DNS server rejects.</td>
<td>A high number of rejections to a DNS server configured to allow secure updates could mean that unauthorized computers are attempting to update.</td>
<td>Any increase over the baseline may be cause for investigation.</td>
</tr>
<tr>
<td><strong>Recursive Queries/sec</strong></td>
<td>The average number of recursive queries received by a DNS server in each second.</td>
<td>This counter provides a view of the query load on the DNS server.</td>
<td>Dramatic increases or decreases should be investigated.</td>
</tr>
<tr>
<td><strong>AXFR Request Sent</strong></td>
<td>The total number of full zone transfer requests sent by the DNS Server service when operating as a secondary server for a zone.</td>
<td>The DNS server hosting the secondary zone is requesting full zone transfers. If this number is high, a lot of changes are happening on the primary zone.</td>
<td>Dramatic increases above the baseline could reflect a need to review the number of changes in the zone and the configuration of zone transfers.</td>
</tr>
</tbody>
</table>
What Is a DNS Event Log?

A DNS event log is a system log that is configured to log only DNS events. The DNS event log contains basic events logged by the DNS Server service. For example, when the DNS server starts or stops, a corresponding event message is written to this log. Some additional critical DNS service events are also logged here, such as when the server starts but cannot locate initializing data such as zones or boot information stored in the Windows Server 2003 registry or (in some cases) Active Directory.

The following table is a partial listing of common events that are recorded in the DNS server log.

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>The DNS server has started.</td>
</tr>
<tr>
<td>3</td>
<td>The DNS server has shut down.</td>
</tr>
<tr>
<td>3150</td>
<td>The data in the DNS zone has updated.</td>
</tr>
<tr>
<td>6522</td>
<td>A change in the zone serial number prompted a zone transfer.</td>
</tr>
</tbody>
</table>

You can use the DNS console to change the type of events to be logged by DNS servers. For example, you can configure the server to log errors only, errors and warnings, all events, or no events. Keep in mind that detailed logs help in the troubleshooting process but may hinder server performance. The default setting logs all events. To change the logging level, go to the properties of the server in the DNS console and modify the Event Logging settings.

The illustration on the PowerPoint slide provides an example of what you might see when viewing an event log through the Event Viewer.
**What Is DNS Debug Logging?**

**Definition**

*DNS debug logging* is an optional logging tool for DNS that collects DNS data that you select. DNS debug logging allows for detailed DNS statistics and information to be gathered to further help in troubleshooting.

Because logging takes resources from the server, debug logging is not enabled by default. Debug logging is configured at the DNS server level, and therefore the debug logging settings affect all of the zones hosted on the DNS server.

**Purpose of DNS debug logging**

If you want to obtain very specific information about the DNS server and its operations, you can enable DNS debug logging. You can collect specific DNS data in the Dns.log file by using DNS debug logging. For example, if you want to know what types of queries a computer has sent to the DNS server, you could configure DNS debug logging to collect just the inbound DNS queries by using the UDP or TCP from a certain Internet Protocol (IP) address.

**DNS debug logging**

Debug logging can be resource intensive, affecting overall server performance and consuming disk space. Therefore, it should be used only temporarily, when more detailed information about server performance is needed.

DNS debug logging will gather and log information about DNS traffic that fits the debug logging criteria.

The storage of debug logging data is restricted by specified file size limits or storage capacity limits. When file limits are reached, the logging process overwrites the oldest entries.
The following table lists and describes the options that are available when you configure DNS debug logging.

<table>
<thead>
<tr>
<th>Options</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet direction</td>
<td>Outgoing</td>
<td>Packets that the DNS server sends are logged in the DNS server log file.</td>
</tr>
<tr>
<td></td>
<td>Incoming</td>
<td>Packets that the DNS server receives are logged in the log file.</td>
</tr>
<tr>
<td>Packet contents</td>
<td>Standard queries</td>
<td>Specifies that packets containing standard queries are logged in the DNS server log file.</td>
</tr>
<tr>
<td></td>
<td>Updates</td>
<td>Specifies that packets containing dynamic updates are logged in the DNS server log file.</td>
</tr>
<tr>
<td></td>
<td>Notifies</td>
<td>Specifies that packets containing notifications are logged in the DNS server log file.</td>
</tr>
<tr>
<td>Transport protocol</td>
<td>UDP</td>
<td>Specifies that packets sent and received over UDP are logged in the DNS server log file. UDP is used when clients issue queries to a DNS server.</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>Specifies that packets sent and received over TCP are logged in the DNS server log file. TCP is used to perform zone transfers.</td>
</tr>
<tr>
<td>Packet type</td>
<td>Request</td>
<td>Specifies that request packets are logged in the DNS server log file.</td>
</tr>
<tr>
<td></td>
<td>Response</td>
<td>Specifies that response packets are logged in the DNS server log file.</td>
</tr>
<tr>
<td>Other options</td>
<td>Enable filtering based on IP address</td>
<td>Provides additional filtering of packets logged in the DNS server log file. This option allows logging of packets that are sent from specific IP addresses to a DNS server or from a DNS server to specific IP addresses.</td>
</tr>
<tr>
<td></td>
<td>File name</td>
<td>Specifies the name and location of the DNS server log file.</td>
</tr>
<tr>
<td></td>
<td>Log file maximum size limit</td>
<td>Sets the maximum file size for the DNS server log file.</td>
</tr>
</tbody>
</table>
Practice: Monitoring DNS Server Performance

In this practice, you will:
- Monitor DNS by using the Performance console
- Monitor DNS by using event logs
- Configure DNS debug logging

Objectives

In this practice, you will:
- Monitor DNS by using the Performance console.
- Monitor DNS by using event logs.
- Configure DNS debug logging.

Instruction

Ensure that the DEN-DC1 virtual machine is started.

Practice

▸ Monitor DNS by using the Performance console

1. If necessary, log on to DEN-DC1 as Contoso\Administrator, with the password of PaSSw0rd.
2. Click Start, point to Administrative Tools, and then click Performance.
3. In the Performance console tree, expand Performance logs and alerts, right-click Counter Logs, and then click New Log Settings.
4. In the Name field, type DNS and then click OK.
5. Click Add Counters.
6. Select DNS from the Performance Object list.
7. Add the following counters:
   - AXFR Request Received
   - AXFR Success Sent
   - IXFR Request Received
   - IXFR Success Sent
   - Zone Transfer Success
   - Zone Transfer Failure
8. Click Close.
9. Set the sample data interval to 1 second.
10. In the Run as field, type contoso\administrator and then click Set Password.
11. Set and confirm the password of Pa$$w0rd and then click OK.
12. On the Schedule tab, under the Start log section, click Manually and then click OK.
13. When prompted that the log file location does not exist, click Yes.

► Monitor DNS by using event logs
1. Click Start, point to Administrative Tools, and then click DNS.
2. In the DNS console tree, right-click DEN-DC1, point to All tasks, and then click Restart.
3. In the DNS console tree, expand DEN-DC1, expand Event Viewer, and then click DNS Events.
4. In the details pane, examine the events that have Event ID 2 and 3.
   When was the DNS service last started? __________________________

► Configure DNS debug logging
1. In the DNS console tree, right-click DEN-DC1 and then click Properties.
2. On the Debug Logging tab, click Log packets for debugging and then click OK.
3. Close all open windows.

► To Prepare for the lab
1. Ensure that the DEN-DC1 virtual machine is started.
2. Start the DEN-SRV1 virtual machine.
Lab: Managing and Monitoring DNS

In this lab, you will:
- Test simple and recursive queries
- Verify SOA records by using Nslookup
- Use Dnslint to verify name server records
- View performance statistics by using the Performance console
- Verify DNS replication

Objectives

In this lab, you will:
- Test simple and recursive queries.
- Verify SOA records by using Nslookup.
- Use Dnslint to verify name server records.
- View performance statistics by using the Performance console.
- Verify DNS replication.

Instructions

Ensure that the following virtual machines are running:
- DEN-DC1
- DEN-SRV1

Estimated time to complete this lab:
30 minutes
Exercise 1
Managing and Monitoring DNS

In this lab, you will manage and monitor DNS.

Scenario

You have decided to implement DNS on a new server in your organization. The server named DEN-SRV1 will be configured to host the zone Contoso.msft. You need to ensure that DEN-SRV1 is configured properly and that your environment will support name resolution. You will use various tools to test the environment, including several command-line tools.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific instructions</th>
</tr>
</thead>
</table>
| 1. Test simple and recursive queries on DEN-SRV1. | a. Log on to DEN-SRV1 as Administrator with the password of Pa$$w0rd.  
b. Test simple and recursive queries on DEN-SRV1.  
Why did the recursive query fail? ________________ |
| 2. Create a root zone on DEN-DC1. Configure DEN-SRV1 to use DEN-DC1 as a root hint server. | a. On DEN-DC1, create a forward lookup zone with the name “.”.  
b. On DEN-SRV1, in the DNS console, on the properties of DEN-SRV1, delete all root hints. Add a root hint for DEN-DC1.contoso.msft.  
c. On DEN-SRV1, test simple and recursive queries.  
Was the recursive query successful? ________________ |
| 3. Start the DNS counter log on DEN-DC1. | On DEN-DC1, use the Performance console to start the DNS counter log. |
| 4. Configure a secondary zone on DEN-SRV1 for Contoso.msft. | a. On DEN-DC1, allow zone transfers for the Contoso.msft zone to any server.  
b. Create a secondary zone on DEN-SRV1 for Contoso.msft. Use DEN-DC1 as the master server.  
c. Use Nslookup to view the SOA record of Contoso.msft on both DEN-SRV1 and DEN-DC1.  
Do both servers have the same serial number for the SOA record? ________________ |
| 5. Use Dnslint on DEN-SRV1 to verify the NS records for Contoso.msft. Ensure that NS records exist for all DNS servers for Contoso.msft. | a. On DEN-SRV1, use Dnslint with the /d and /s switches for Contoso.msft. Use 10.10.0.2 as the root server.  
Are both DEN-DC1 and DEN-SRV1 listed as name servers? ________________  
b. On DEN-DC1, on the Name Servers tab for the Contoso.msft zone, add DEN-SRV1 as a name server.  
c. Use Dnslint with the /d and /s switches for Contoso.msft. Use 10.10.0.2 as the root server.  
Are both DEN-DC1 and DEN-SRV1 listed as name servers? ________________ |
(continued)

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Specific instructions</th>
</tr>
</thead>
</table>
| 6. Use the Performance console to verify zone replication. | a. On DEN-DC1, stop the DNS counter log. Use System Monitor to load the logged data. Add the following counters:  
• AXFR Request Received ____________________  
• AXFR Success Sent _______________________  
• IXFR Request Received _____________________  
• IXFR Success Sent _________________________  
• Zone Transfer Success _____________________  
• Zone Transfer Failure ______________________  
  
b. View the counters by using the Report view, and note the values for each counter. |
| 7. Verify the last successful zone transfer to DEN-SRV1 by using the debugging log and the event log. | a. On DEN-DC1, open the debugging log to determine the last successful zone replication to DEN-SRV1. The DNS log can be found at C:\Windows\System32\DNS.  
  
b. Use the event log on DEN-SRV1 to verify the successful zone replication from DEN-DC1. |
| 8. Complete the lab exercise. | a. Close all programs and shut down all computers. Do not save changes.  
  
b. To prepare for the next module, start the DEN-DC1 and DEN-SRV1 virtual machines. |