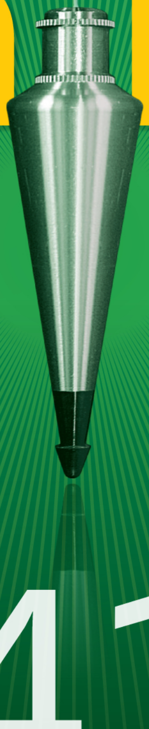
Microsoft

Designing and Implementing a Server Infrastructure

Steve Suehring

Exam Ref



EXAM

70-413

Exam Ref 70-413

Prepare for Exam 70-413—and help demonstrate your real-world mastery of enterprise server design and implementation. Designed for experienced, MCSA-certified professionals ready to advance their status—*Exam Ref* focuses on the critical-thinking and decision-making acumen needed for success at the MCSE level.

Focus on the expertise measured by these objectives:

- Plan and Deploy a Server Infrastructure
- Design and Implement Network Infrastructure Services
- Design and Implement Network Access Services
- Design and Implement an Active Directory Infrastructure (Logical)
- Design and Implement an Active Directory Infrastructure (Physical)

Exam Ref features:

- Organized by exam objectives
- Strategic, what-if scenarios
- 15% exam discount from Microsoft. Offer expires 12/31/2017. Details inside.

Designing and Implementing a Server Infrastructure

ABOUT THE EXAM

Exam 70-413 focuses on the planning, configuration, and implementation of Windows Server® 2012 services.

Exam 70-413 is a requirement for MCSE: Server Infrastructure certification, along with Exam 70-414 and MCSA: Windows Server 2012 certification.

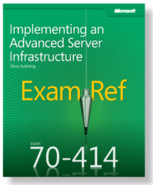
CERTIFICATION

The new **Microsoft Certified Solutions Expert (MCSE)** certifications validate your ability to design and build technology solutions in the cloud and on premises.

Professionals who achieve **MCSE: Server Infrastructure** certification can build comprehensive server infrastructure solutions. Show you have the skills needed to run a highly efficient and modern data center, with expertise in identity management, systems management, virtualization, storage, and networking.

See full details at:
microsoft.com/learning/certification

ALSO SEE



ISBN: 9780735674073
Coming Soon

ABOUT THE AUTHOR

Steve Suehring has worked extensively with the Windows Server product family since Windows® NT, with recent experience leading a large-scale deployment at a Fortune 1000 company. He has written several books on programming, security, and enterprise administration.

ISBN: 978-0-7356-7367-0
9 780735 673670 90000

U.S.A. $39.99
Canada $41.99
[Recommended]

*Certification/
Windows Server*

Windows Server 2012

Microsoft®

Microsoft

Exam 70-413: Designing and Implementing a Server Infrastructure

Exam Ref

Steve Suehring

ISBN: 978-0-7356-7367-0

2 3 4 5 6 7 8 9 10 QG 8 7 6 5 4 3

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author’s views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation,
nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions and Developmental Editor: Ken Jones

Production Editor: Holly Bauer

Editorial Production: Box Twelve Communications

Technical Reviewer: Brian Svidergol

Copyeditor: Susan Shaw Dunn

Indexer: Ginny Munroe

Cover Design: Twist Creative • Seattle

Cover Composition: Zyg Group, LLC

Illustrator: Rebecca Demarest

[2013-05-10]

To Rebecca.

Contents at a Glance

Contents

Introduction

This *Exam Ref* is designed to assist you with studying for the MCITP exam 70-413, "Designing and Implementing a Server Infrastructure." This exam focuses on both the use of server technologies to solve particular design objectives as well as the implementation of those designs to meet certain objectives. The exam has network-related objectives and calls on your experience with Windows Server and related technologies such as DirectAccess, VPNs, DNS, and DHCP.

The 70-413 exam is meant for large, enterprise-scale organizations and their needs. Passing the exam demonstrates your knowledge and experience with enterprise server technologies.

This book will review every concept described in the following exam objective domains:

- Plan and deploy a server infrastructure
- Design and implement network infrastructure services
- Design and implement network access services
- Design and implement an Active Directory infrastructure (logical)
- Design and implement an Active Directory infrastructure (physical)

Even though this book covers all the technologies involved in each exam objective, it's not meant to be a brain dump of questions that you'll see on the exam. In fact, this book is meant to be used as a supplement to your own experience with and a study of the relevant technologies in each objective. As you read the book, if you come across areas that you are less familiar with, you should follow up on that area to obtain additional knowledge. In many cases, the book provides links to the relevant areas in TechNet, but you should also pursue this area using every available tool at your disposal, including other areas of Microsoft's website, forums, and first-hand experience. In fact, you should deploy your own infrastructure for this exam to match the recommended lab scenarios covered not only in this book but also in the documentation from Microsoft on these subject areas. Microsoft offers trial versions of all software involved in this exam, and you can create a virtualized infrastructure to help your study of the exam objectives.

Microsoft Certified Professional Program

Microsoft certifications provide the best method for proving your command of current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies. Computer professionals who become Microsoft certified are recognized as experts and are sought after throughout the industry. Certification brings various benefits to the individual and to employers and organizations.

MORE INFO **OTHER MICROSOFT CERTIFICATIONS**

For a full list of Microsoft certifications, go to *www.microsoft.com/learning/mcp/default.asp*.

Acknowledgments

This book would not have been possible without my wife's support. She assumed nearly all responsibility for a 9-month-old and a 4-year-old so that I could focus on getting this book written. Ken Jones and Neil Salkind also worked out the details to make the book possible. Even though they didn't offer to do any diaper changes, I'll still thank them anyway.

And the requisite thanks to Tim and Rob from Partners, as well as Jim Oliva and John Eckendorf. Thanks to Bob, Mike, Ernie, and Tim for getting the band back together. It hasn't been that long since I wrote an acknowledgments section, but I can't remember the list of people that I usually thank, so here's to you, person that I can't remember when I'm writing this early on a Sunday morning: consider yourself thanked!

One person I can't forget to thank is you, the reader, not only for reading this acknowledgments section, but also for reading this book. I invite you to contact me, either through my website or on Twitter. Thank you!

Support & Feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

> *http://www.microsoftpressstore.com/title/9780735673670*

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

We Want to Hear from You

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

> *http://www.microsoft.com/learning/booksurvey*

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in Touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

Preparing for the Exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam ref and another study guide for your "at home" preparation, and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 2

Design and implement network infrastructure services

A network infrastructure consists of those basic services like Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Internet Protocol (IP) address management. Windows Server 2012 provides all these services. New to Windows Server 2012 is a service called IPAM, short for IP address management. IPAM gives an organization a single location from which the addressing for the entire organization can be managed and monitored.

Objectives in this chapter:

- Objective 2.1: Design and maintain a Dynamic Host Configuration Protocol (DHCP) solution
- Objective 2.2: Design a name resolution solution strategy
- Objective 2.3: Design and manage an IP address management solution

Objective 2.1: Design and maintain a Dynamic Host Configuration Protocol (DHCP) solution

Dynamic Host Configuration Protocol (DHCP) supplies Internet Protocol (IP) addresses and other network configuration information to devices on a network. Most clients and client devices in an enterprise use DHCP to obtain network information.

This objective covers the following topics:

- Design considerations, including a highly available DHCP solution that includes split scope, DHCP failover, DHCP failover clustering, DHCP interoperability, and DHCPv6
- How to implement DHCP filtering
- How to implement and configure a DHCP management pack
- How to maintain a DHCP database

Designing a highly available DHCP solution

DHCP is a vital service on an enterprise network. Without it, clients can't obtain IP addresses and information such as DNS servers. For this reason, DHCP is frequently deployed in a highly available manner so that if one server becomes unavailable, another can take over. This section examines the considerations involved in designing a high availability solution for DHCP.

MORE INFO **TERMINOLOGY AND BASIC DHCP DESIGN**

This section concentrates on DHCP design at the enterprise level and assumes that you have requisite knowledge of DHCP itself, along with basic deployment and management of DHCP. See *http://technet.microsoft.com/library/dd283016* for more information on DHCP, including terminology and basic design.

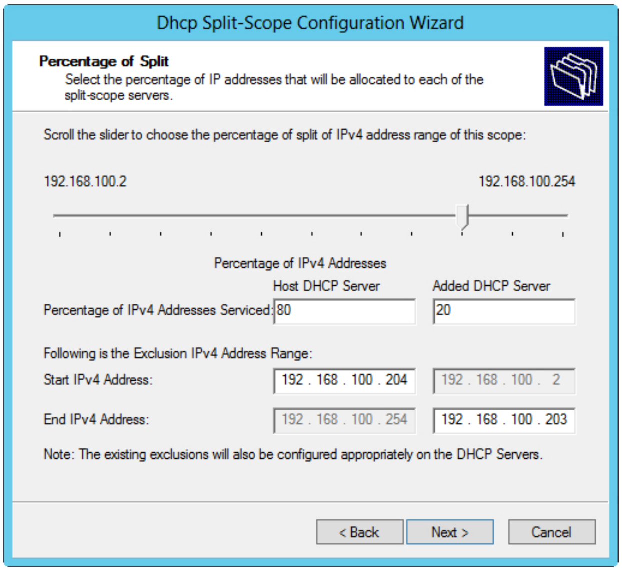
The two goals for highly available DHCP are as follows:

- Provide DHCP service at all times.
- When one DHCP server is no longer available, enable clients to extend their lease by contacting a different DHCP server.

When designing a highly available DHCP solution, you should consider whether to provide split-scope DHCP or failover clustering.

Split scope

With split-scope DHCP, two servers provide address and network information using a portion of the address space or DHCP scope. For example, if an organization assigns addresses from the 192.168.100.0/24 subnet, a split-scope DHCP scenario might call for 80 percent of the addresses to be assigned by one server and the other 20 percent by another server. This is known as the "80/20" rule for DHCP scope assignment, and organizations sometimes place the server with 80 percent of the scope nearest to the clients. However, you don't need to figure out the 80/20 split; the Dhcp Split-Scope Configuration Wizard includes a step to help configure the split (see Figure 2-1).



Dhcp Split-Scope Configuration Wizard

Percentage of Split

Select the percentage of IP addresses that will be allocated to each of the split-scope servers.

Scroll the slider to choose the percentage of split of IPv4 address range of this scope:

192.168.100.2 192.168.100.254

Percentage of IPv4 Addresses

	Host DHCP Server	Added DHCP Server
Percentage of IPv4 Addresses Serviced:	80	20

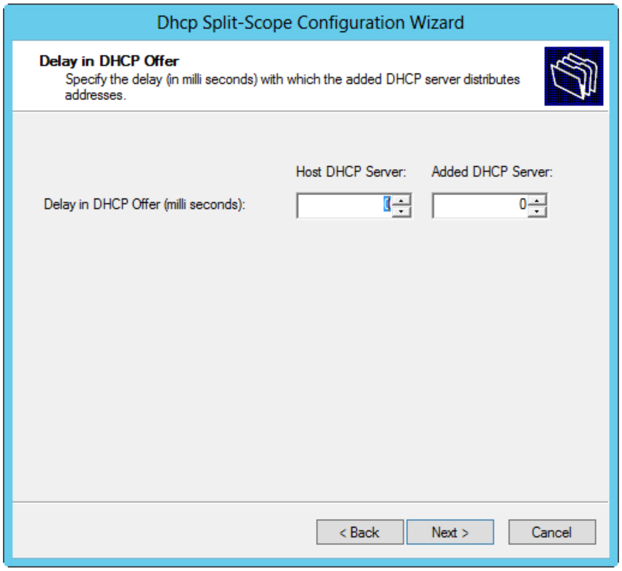
Following is the Exclusion IPv4 Address Range:

Start IPv4 Address:	192 . 168 . 100 . 204	192 . 168 . 100 . 2
End IPv4 Address:	192 . 168 . 100 . 254	192 . 168 . 100 . 203

Note: The existing exclusions will also be configured appropriately on the DHCP Servers.

FIGURE 2-1 Configuring a split-scope percentage in the Dhcp Split-Scope Configuration Wizard.

Split scope enables traffic to be split among participating servers while also providing redundancy for clients should one of the two servers fail. However, clients accept the first DHCP response they receive, so you can't guarantee from which server clients will receive a DHCP response. If the servers are split across a network boundary, you need to configure a DHCP relay agent on a router and introduce a delay at that point so as to prevent the secondary server from responding before the primary server. The Dhcp Split-Scope Configuration Wizard also includes an opportunity to add a delay to one of the servers involved in the split scope, as shown in Figure 2-2.

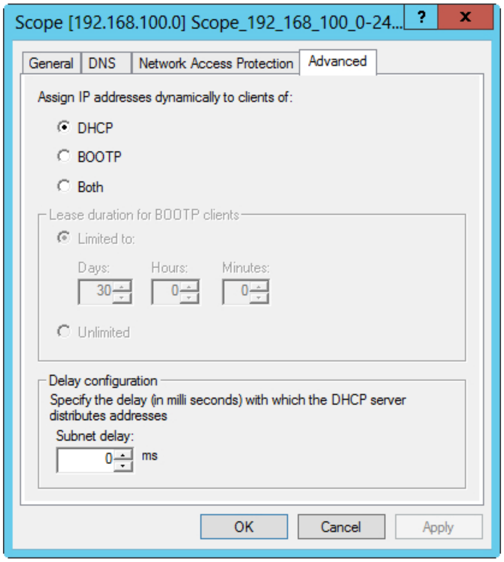

Dhcp Split-Scope Configuration Wizard

Delay in DHCP Offer
Specify the delay (in milli seconds) with which the added DHCP server distributes addresses.

	Host DHCP Server:	Added DHCP Server:
Delay in DHCP Offer (milli seconds):	0	0

FIGURE 2-2 Adding a delay in a split scope can help ensure that network information comes from the correct server.

Alternatively, a delay can be configured into the scope itself through the Advanced tab in the Scope Properties sheet, as shown in Figure 2-3.


Scope [192.168.100.0] Scope_192_168_100_0-24...

Assign IP addresses dynamically to clients of:

● DHCP
○ BOOTP
○ Both

Lease duration for BOOTP clients

● Limited to:

Days:	Hours:	Minutes:
30	0	0

○ Unlimited

Delay configuration
Specify the delay (in milli seconds) with which the DHCP server distributes addresses
Subnet delay: 0 ms

FIGURE 2-3 Configuring a delay for the DHCP server response can help in a split-scope scenario.

NOTE **SPLIT SCOPE**

Split scope is available only for IPv4 scopes.

DHCP failover

A new feature of Windows Server 2012, DHCP failover means that two servers are configured with the same DHCP configuration. Windows Server 2012 has two modes for failover: hot standby and load sharing. These modes of DHCP failover are different from failover clustering, which is discussed later.

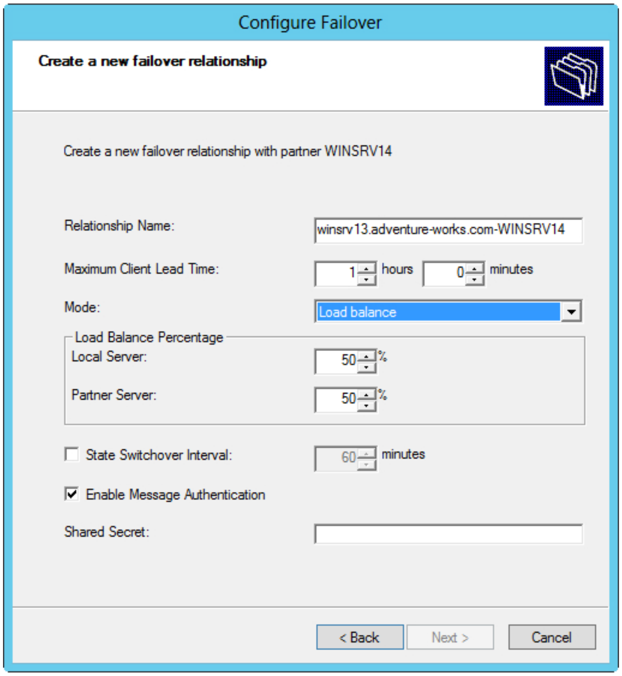
NOTE **TWO NODES**

DHCP failover is limited to two nodes.

With DHCP failover, each server has a replicated version of the entire scope, including lease information. This means that either server can offer addresses for the entire scope. The practical implication of scope and lease replication is to enable both modes of operation. With a hot standby operation, one server provides DHCP information while the other server maintains a replicated version of the DHCP lease information, ready to take over if the primary server fails. In a load-sharing mode, each server assigns DHCP information and updates the shared lease information database.

Hot standby mode is useful for organizations that have a remote location with DHCP clients, sometimes called a hub-and-spoke topology. The remote location acts as the primary server; a server at the central data center acts as a backup. If the remote server goes offline, the secondary server at the data center can take over. The primary and secondary assignment is done at the subnet level, rather than the scope level. This means that a server can be primary for one subnet and secondary for another subnet.

Load-sharing mode is helpful for data center or centralized DHCP scenarios in which two servers operate within a single site. In load-sharing mode, each server assigns DHCP information to clients based on a load ratio. You set the load balance percentage at configuration time, as shown in Figure 2-4.


Configure Failover

Create a new failover relationship

Create a new failover relationship with partner WINSRV14

Relationship Name: winsrv13.adventure-works.com-WINSRV14

Maximum Client Lead Time: 1 hours 0 minutes

Mode: Load balance

Load Balance Percentage

Local Server: 50 %

Partner Server: 50 %

□ State Switchover Interval: 60 minutes

☑ Enable Message Authentication

Shared Secret:

FIGURE 2-4 Configuring the load balance percentage in a DHCP failover architecture.

You can edit the load balance percentage after initial configuration from the partner server.

NOTE **LIMITATIONS**

DHCP failover is limited to IPv4 scopes and configuration.

DHCP failover clustering

A redundant architecture available prior to Windows Server 2012 is failover clustering. With failover clustering, the primary DHCP server offers DHCP information, and the secondary server takes over if the first server fails. In this scenario, the DHCP servers share the same storage, thus making a single point of failure at the storage level.

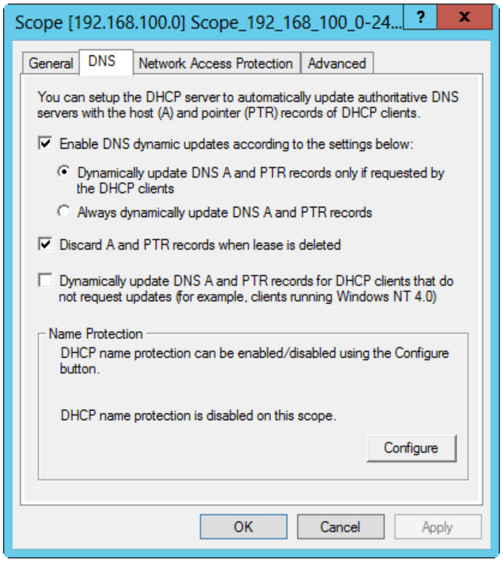
MORE INFO **FAILOVER CLUSTERING**

See *http://technet.microsoft.com/library/ee405263* for more information on failover clustering.

DHCP Interoperability

The term *interoperability* refers to the relationship between DHCP and other Microsoft technologies such as Routing and Remote Access, Network Access Protection (NAP), Active Directory Domain Services (AD DS), and other related technologies, rather than interoperability between the Microsoft DHCP implementation and the DHCP implementation from other vendors.

DHCP clients can register dynamic DNS entries upon address assignment. To do so, the DHCP server depends on a directory services domain controller to be available, and the DHCP server must be authorized to make such entries into the DNS. This can be configured on the DNS tab of the Scope Properties sheet (see Figure 2-5).


Scope [192.168.100.0] Scope_192_168_100_0-24...
?
x
General
DNS
Network Access Protection
Advanced
Configure
OK
Cancel
Apply

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

☑ Enable DNS dynamic updates according to the settings below:

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

○ Always dynamically update DNS A and PTR records

☑ Discard A and PTR records when lease is deleted

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

Name Protection

DHCP name protection can be enabled/disabled using the Configure button.

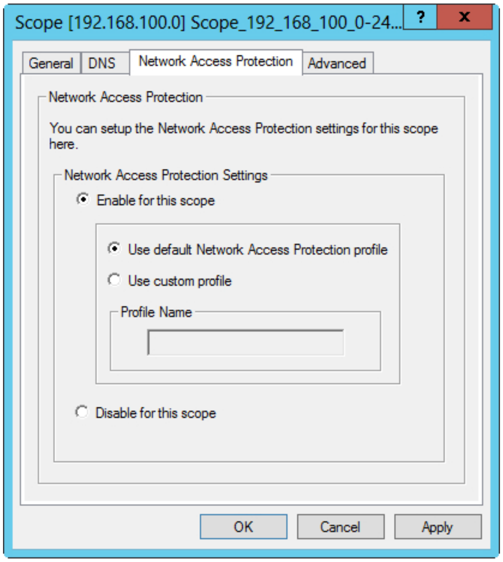
DHCP name protection is disabled on this scope.

FIGURE 2-5 Configuring dynamic DNS settings related to a DHCP scope.

The DHCP server can update both the pointer (PTR) and host address (A) record for the client. The Client FQDN option (DHCP option 81) is used for this purpose. Option 81 includes the Fully Qualified Domain Name (FQDN) and other information from the client. As Figure 2-5 shows, the server can be configured to update the DNS at all times or only if requested by the client. Older clients are also supported (ones that can't or don't send DHCP option 81) by selecting the Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates check box within this Properties sheet.

DHCP interoperability with AD DS is typically used to detect and authorize additional DHCP servers on the network. DHCP servers running Windows can be authorized into the AD DS schema and if not authorized, can be prevented from leasing IP addresses to clients. However, this authorization scheme works only for DHCP servers running Windows 2000 and above and doesn't work for a DHCP server running on Linux or a network device.

DHCP can work with NAP to limit client access unless the client is in a compliant state. Figure 2-6 shows the NAP-related configuration in a scope's Properties sheet.


Scope [192.168.100.0] Scope_192_168_100_0-24...
?
x
General
DNS
Network Access Protection
Advanced
OK
Cancel
Apply

Network Access Protection

You can setup the Network Access Protection settings for this scope here.

Network Access Protection Settings

● Enable for this scope

● Use default Network Access Protection profile

○ Use custom profile

Profile Name

○ Disable for this scope

FIGURE 2-6 Network Access Protection settings related to DHCP.

You can configure NAP at the individual scope level or for all scopes on a server.

MORE INFO **WORKING WITH NAP**

For more information on NAP, see *http://technet.microsoft.com/library/dd125338%28*.

DHCPv6 considerations

DHCP for IPv6 operates in stateless and stateful modes. In stateful mode, clients obtain both an address and information such as DNS servers from the DHCP server. In stateless mode, clients obtain ancillary information such as DNS servers but receive their addressing through IPv6 auto-configuration or as a static IP address.

Implementing DHCP filtering

DHCP filtering, sometimes called *link-layer filtering*, enables you to configure how the DHCP server responds to requests for address and network information. DHCP filtering enables the DHCP server to send information only to known clients or deny information to specific clients. This is especially important in a data-center scenario in which you likely want to control the devices allowed on the network.

DHCP filtering works with Media Access Control (MAC) addresses, which are sent by the DHCP client along with a DHCP request. Windows Server 2012 has two types of filters: Allow and Deny. An Allow filter sends network information only to those clients listed in the filter. A Deny filter excludes specific clients from obtaining information from the DHCP server.

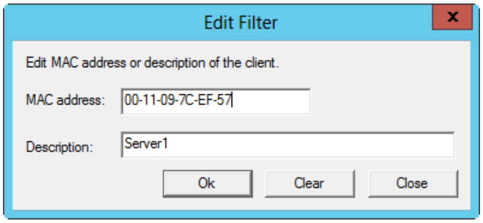
In an Allow scenario, each authorized MAC address needs to be specifically entered into the filter; otherwise, it can't obtain information from the DHCP server. Of course, this isn't an issue if the client is using an address that's statically assigned on the client itself.

Windows Server 2012 enables filtering with the full MAC address or by using wildcards. For example, these are all valid filters:

- 00-11-09-7c-ef-57
- 00-11-09-7c-ef-*
- 00-11-09-*-*-*
- 0011097cef57

Using wildcards enables you to configure a group of the same devices or devices from the same manufacturer as being allowed or denied. This saves the effort of entering each MAC address individually if a group of devices share the same MAC prefix.

DHCP filtering is configured with the DHCP MMC snap-in. Adding a filtered address is accomplished by right-clicking either Allow or Deny (depending on which type you want to set up) and then entering the MAC address details, as shown in Figure 2-7.



Edit MAC address or description of the client.

MAC address: 00-11-09-7C-EF-57

Description: Server1

FIGURE 2-7 Creating a DHCP filter.

You also need to enable filters at the overall filter (Allow or Deny) level rather than at the individual MAC address level. To enable the Allow or Deny filter, right-click Allow or Deny in the DHCP MMC snap-in and select Enable. You can also enable filters at the scope level.

Implementing and configuring a DHCP Management Pack

The DHCP Management Pack, part of the Operations Manager component of Microsoft System Center 2012, enables advanced logging and monitoring of the DHCP environment. For example, the DHCP Management Pack enables monitoring of the availability of the DHCP service, the filtering status, and the status of scopes to help prevent scope exhaustion.

Implementing a DHCP Management Pack requires Microsoft System Center 2012. The DHCP Management Pack is imported into Operations Manager. Creating a new management pack is recommended to incorporate any changes to the DHCP Management Pack without affecting the original configuration.

Table 2-1 outlines several scenarios for monitoring a DHCP infrastructure.

TABLE 2-1 Common scenarios for DHCP monitoring

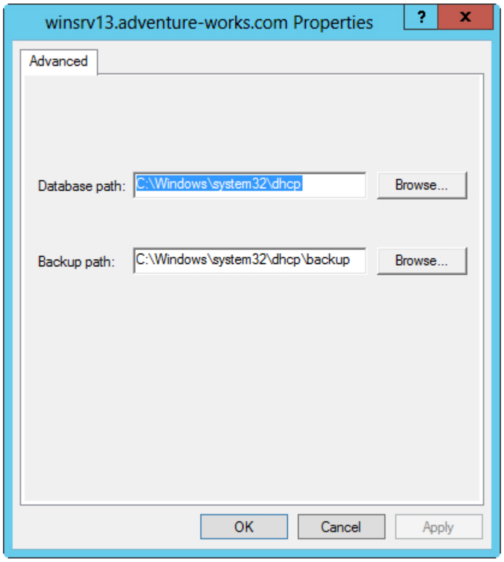
What to Monitor	Description
The servers themselves	Monitor for the availability of the service and detect unauthorized DHCP servers.
DHCP scopes	Monitor when a scope is nearing address exhaustion.
The DHCP database	Monitor when the database is having problems.
Performance	Monitor for excessive requests or queue length as well as the number of addresses in use, and related items.

MORE INFO **DHCP MANAGEMENT PACK**

See *http://technet.microsoft.com/library/cc180306.aspx* for more information on the DHCP Management Pack

Maintaining a DHCP database

Maintenance of a DHCP database involves backing up and restoring the database. The location of the database and its backup location can be configured at the server level within its Properties sheet, as shown in Figure 2-8.



winsrv13.adventure-works.com Properties

Advanced

Database path: C:\Windows\system32\dhcp

Backup path: C:\Windows\system32\dhcp\backup

FIGURE 2-8 Configuring the location of the DHCP database, as well as its backup location.

You can back up and restore the DHCP database through Actions at the server level in DHCP Manager. Also, to change an automated backup that runs every 60 minutes, set the

BackupInterval value in the registry at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

MORE INFO **COMPACTING WITH JETPACK**

You also can compact the DHCP database by using Jetpack. See *http://technet.microsoft.com/library/hh875589%28v=ws.10%29.aspx* for more information.

At times you may need to reconcile the database due to inconsistencies in client addressing between summary and detailed information. To do so, select Reconcile All Scopes from the address level (IPv4 or IPv6) or at the scope level by clicking Reconcile.

THOUGHT EXPERIMENT
Designing a DHCP topology

In the following thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You have a wide area network (WAN)–connected remote site with 150 clients that need to receive address information and a primary data center that provides DHCP information for 350 clients.

Describe the DHCP topology that should be designed for this site, including hot standby and failover architecture, if applicable.

Objective summary

- The DHCP server role in Windows Server 2012 provides for redundancy with split scope, failover through hot standby and load sharing, and failover clustering.
- Hot standby failover enables a server to take over should its counterpart fail.
- Load-sharing failover enables both servers to assign DHCP information.
- Failover clustering enables both servers to assign DHCP information by sharing the same DHCP database on a shared storage location.
- DHCP filtering configures how the server responds to clients by using link-layer MAC addresses.
- The DHCP Management Pack, part of System Center Operations Manager, enables monitoring and reporting of the DHCP service.
- The DHCP database is stored on the file system and needs to be reconciled occasionally to remove stale entries.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the “Answers” section at the end of this chapter.

1. You’re configuring a split-scope DHCP scenario between two servers. What’s the recommended percentage for a DHCP split scope configuration?

    A. 60/40

    B. 70/30

    C. 80/20

    D. 50/50

2. Which of the following are valid MAC filters in Windows Server 2012? (You can assume that the MAC addresses themselves are valid.)

    A. 00-11-09-*-*-*

    B. 001109001111

    C. 00:11:09:09:11:09

    D. 00-11-09-7c-ef-%

3. You need to move the DHCP database. Assuming a standard Windows directory and Program Files path structure and that you’ve changed the path in the DHCP Manager, what’s the default path where the DHCP database is found?

    A. C:\Windows\system32\dhcp

    B. C:\Program Files\Microsoft\DHCP\Data

    C. C:\Windows\system32\DHCP\Data

    D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DHCP

4. While implementing split scope, you notice that the secondary server is responding to numerous DHCP requests first. What’s the best way to handle this situation?

    A. Increase the split ratio so that the secondary server has more IP addresses from the scope.

    B. Introduce a delay for DHCP offers from the secondary using the DHCP management console.

    C. Reduce the load on the primary server so that it can respond faster.

    D. Place the secondary DHCP server on a different network segment to introduce a delay in the response.

Objective 2.2: Design a name resolution solution strategy

Name resolution typically involves Domain Name System (DNS) but can also include Windows Internet Name Service (WINS). This objective concentrates on design of the solution rather than its implementation.

This objective covers just this topic:

- Design considerations, including secure name resolution, DNSSEC, DNS socket pool, cache locking, disjoint namespaces, DNS interoperability, migration to application partitions, IPv6, Single-Label DNS Name Resolution, zone hierarchy, and zone delegation

Designing a name resolution strategy

You need to keep several things in mind when designing a complex name resolution strategy at the enterprise level. These include prioritizing security while at the same time providing a reliable and robust infrastructure for the organization. Several features of Windows Server 2012 can be used to create this robust and reliable design.

In addition to the features you can use to create a robust and reliable design, you should also be intimately familiar with DNS for the exam. This includes being familiar with the DNS protocol as well as the tools and concepts surrounding implementation of DNS in an enterprise. Many of these tools and concepts have existed for quite some time and aren't directly called out as objectives on the exam. As an enterprise administrator, you are expected to have the prerequisite knowledge of a primary protocol such as DNS.

MORE INFO **ADDITIONAL REFERENCES**

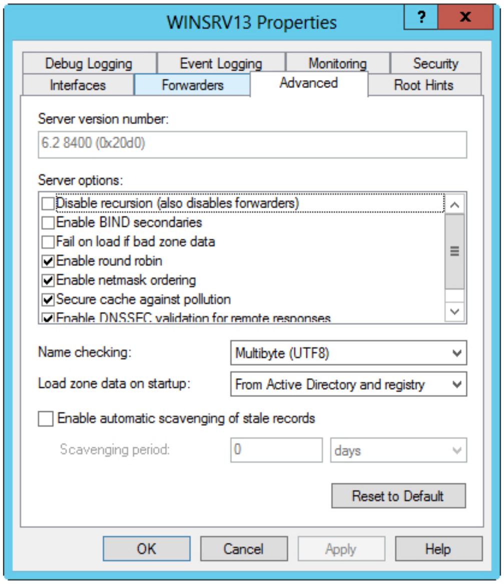
Table 2-2 provides links to additional reference information for these concepts, but you're encouraged to pursue supplemental DNS information beyond that which is listed here and on the exam objectives.

TABLE 2-2 Additional resources

Concept	More Information
Conditional forwarding	*http://technet.microsoft.com/library/0104be3c-0405-4455-b011-6950875c0446*
DNS zone types	*http://technet.microsoft.com/library/cc771898*
DNS server placement	*http://technet.microsoft.com/library/cc737361*
Troubleshooting DNS	*http://technet.microsoft.com/library/cc753041*
DNS Technical Reference	*http://technet.microsoft.com/library/dd197461*

Secure name resolution

Ensuring secure name resolution includes making sure that the name server and DNS server have been secured. The Advanced tab in the DNS server Properties sheet, shown in Figure 2-9, contains several check boxes relevant to secure name resolution.



Server version number:
6.2 8400 (0x20d0)

Server options:
☐ Disable recursion (also disables forwarders)
☐ Enable BIND secondaries
☐ Fail on load if bad zone data
☑ Enable round robin
☑ Enable netmask ordering
☑ Secure cache against pollution
☑ Enable DNSSEC validation for remote responses

Name checking: Multibyte (UTF8)
Load zone data on startup: From Active Directory and registry

☐ Enable automatic scavenging of stale records
Scavenging period: 0 days

FIGURE 2-9 Advanced DNS properties for the DNS Server service.

Among the options relevant to DNS security is Secure Cache Against Pollution, which randomizes the source port for requests, and Enable DNSSEC Validation For Remote Responses, which is discussed in the "DNSSEC" section later in this chapter.

Several other design considerations should be examined when looking at the name resolution strategy. If clients will resolve external DNS names, such as for Internet hosts, you can configure a group of DNS servers in the forest root domain to forward queries to external DNS servers or by using root hints so that any child domain servers forward queries to the forest root domain servers.

This is essentially what you'll do by disabling recursion on a child DNS server. You can disable recursion for DNS servers that are authoritative for DNS zones but don't need to provide general DNS resolution to clients on the network. A good example of this is an enterprise scenario in which the domain controllers are separate from the DNS servers that clients use for normal Internet name resolution. In such a scenario, recursion should be disabled on the domain controllers. If your domain has both types of records, you should consider splitting the DNS namespace between external and internal servers.

Zone transfers should be disabled by default and enabled only to allowed hosts.

DNSSEC

DNSSEC, defined primarily by RFCs 4033, 4034, and 4035, adds security to DNS. Windows Server 2012 enhances support for DNSSEC (DNS Security Extensions). DNSSEC provides new resource records and also provides for data integrity, origin authority, and authenticated denial of existence. DNSSEC operates using public key cryptography whereby clients receive cryptographically signed responses to queries. The clients have the public key of the server signing the response and can therefore ensure the validity of the response, and that it hasn't been tampered with.

DNSSEC can also sign entire zones via the dnscmd.exe tool. With Windows Server 2012, you can now deploy DNSSEC in Active Directory–integrated zones with dynamic updates. This is a change from previous versions of Windows and its support for DNSSEC.

DNSSEC establishes a chain of trust with a trust anchor at the root zone that enables a chain of trust to be built to ensure that responses are trustworthy. Therefore, when planning to use DNSSEC, you need to determine the location for the trust anchors. This also means that the validity of not only individual resource records can be verified, but also the actual server itself can be verified as being the correct authoritative server.

A signed zone contains RRSIG, DNSKEY, and NSEC records in addition to the normal DNS records in that zone. NSEC provides authenticated denial of existence for DNS. Windows Server 2012 supports NSEC and NSEC3, an extended version of the standard. NSEC3 helps to prevent zone enumeration whereby an attacker can send repeated queries across a zone to determine targets.

MORE INFO **DEPLOYING DNSSEC**

For a step-by-step demonstration for deploying DNSSEC, visit *http://technet.microsoft.com/library/hh831411*.

DNS socket pool

The DNS socket pool enables randomization of queries to prevent cache poisoning attacks. Security update MS08-037 enables this feature by default, and it is enabled by default in Windows Server 2012. The DNS socket pool uses several source ports for issuing queries.

Both the number of source ports to be used and any exclusions or ports not to be used for issuing queries can be configured. Unfortunately, this feature can't be controlled using the DNS management tool and must instead be configured by using either the dnscmd tool or the registry.

MORE INFO **CONFIGURING THE DNS SOCKET POOL**

See *http://technet.microsoft.com/library/ee649174.aspx* for more information on configuring the socket pool.

Cache locking

Another method for preventing cache poisoning is with cache locking. Cache locking prevents cached responses from being overwritten during their Time to Live (TTL). Cache locking is configured as a percentage of the TTL. So if the TTL is 3600 seconds, a cache-locking percentage of 50 would prevent the cached value from being overwritten for 1800 seconds, or 50 percent of the TTL. You can configure cache locking by using the CacheLockingPercent registry key or the dmscmd tool.

MORE INFO **CONFIGURING CACHE LOCKING**

See *http://technet.microsoft.com/library/ee649148.aspx* for more information on configuring cache locking.

Disjoint namespaces

A disjoint namespace has a different Active Directory domain and DNS domain suffix. For example, a DNS suffix of corp.adventure-works.com with an Active Directory domain of int.corp .adventure-works.com is in a disjoint namespace. Domain members register resource records in the domain in which they're members—int.corp.adventure-works.com in the example. The domain controller then registers both global and site-specific service (SRV) records into the DNS domain. The SRV records are also placed in the _msdcs zone.

Disjoint namespaces are used when business rules dictate that namespace separation needs to occur. However, applications to be used in a disjoint namespace should be tested because they may expect that the domain and DNS suffix match and therefore may not work. Disjoint namespaces require additional administration overhead because of the manual processes involved to manage the DNS and Active Directory information.

The following configurations support disjoint namespaces:

- In a multi-domain Active Directory forest with a single DNS namespace or zone
- In a single Active Directory domain that's split into multiple DNS zones

On the other hand, a disjoint namespace won't work in the following configurations:

- When a suffix matches an Active Directory domain in the current or another forest
- When a certification authority (CA) domain member changes its DNS suffix

DNS interoperability

Microsoft's implementation of DNS complies with the relevant DNS-related RFCs, thus making interoperability possible with other servers. The Enable BIND Secondaries check box on the Advanced tab of the DNS server Properties sheet enables the Windows-based DNS server to interact with a server running the BIND name server. Refer to Figure 2-9 for a screenshot of this tab.

Migration to application partitions

Application partitions enable certain data to be replicated along partition lines. Specifically, application partitions assist with control of the replication's scope—for instance, to enable certain DNS zones to be replicated.

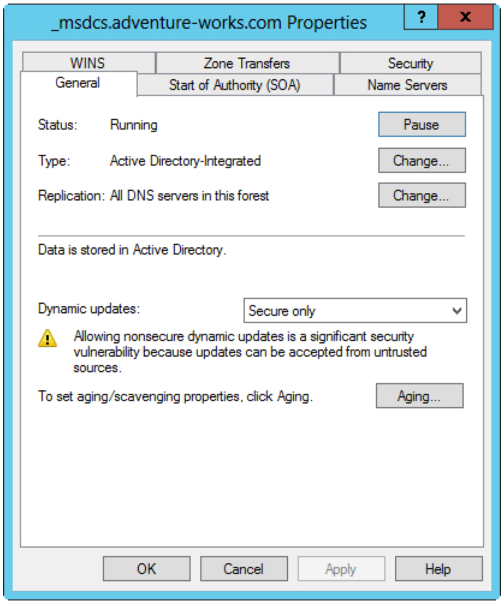
An application partition is created with the dnscmd command-line tool:

```
dnscmd <ServerName> /CreateDirectoryPartition <Fully Qualified Domain Name>
```

After the partition is created, servers are enlisted with this command:

```
dnscmd <ServerName> /EnlistDirectoryPartition <Fully Qualified Domain Name>
```

After the directory partition is created, you can change zone replication in the Properties sheet for the given zone. On the General tab of the zone's Properties sheet, you change the replication configuration by clicking Change. Figure 2-10 shows the General tab.



Status: Running

Type: Active Directory-Integrated

Replication: All DNS servers in this forest

Data is stored in Active Directory.

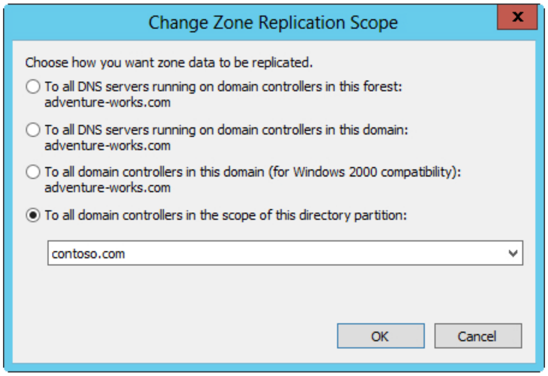
Dynamic updates: Secure only

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

To set aging/scavenging properties, click Aging.

FIGURE 2-10 You configure replication on the General tab of a zone's Properties sheet.

When you click Change, the Change Zone Replication Scope dialog box appears, as in Figure 2-11.



Choose how you want zone data to be replicated.

○ To all DNS servers running on domain controllers in this forest:
adventure-works.com

○ To all DNS servers running on domain controllers in this domain:
adventure-works.com

○ To all domain controllers in this domain (for Windows 2000 compatibility):
adventure-works.com

● To all domain controllers in the scope of this directory partition:

contoso.com

FIGURE 2-11 Replicating to a directory partition.

IPv6

Windows Server 2012 supports IPv6 DNS hosting. Address records are known as AAAA in IPv6 rather than the A record for IPv6 DNS hosts. Designing IPv6 DNS typically means a coexistence strategy of some nature whereby both IPv4 and IPv6 DNS is supported on a network.

MORE INFO USING IPV6 IN WINDOWS

See *http://technet.microsoft.com/network/bb530961.aspx* for more information on IPv6 in Windows.

Windows Internet Name Service (WINS) doesn't support IPv6, so keep this limitation in mind when planning an IPv6 deployment. You can use an ISATAP router to provide translation services for WINS.

MORE INFO USING ISATAP

See *http://technet.microsoft.com/library/dd379548%28.aspx* for more information on using ISATAP for this purpose.

Single-label DNS name resolution

Single-label domains are missing a top-level domain (TLD) and the normal dot (.) notation associated with domain names. For example, a normal domain is adventure-works.com, whereas a single-label domain is adventure-works.

You find single-label names on networks with legacy Windows Internet Name Service (WINS) deployments. However, as WINS is retired, administrators must plan for providing name resolution for older, legacy WINS-based applications and important resources. Windows has a GlobalNames Zone (GNZ) that can be used to provide name resolution for single-label names. GNZ can be deployed in a single forest or across multiple forests to provide static name resolution.

GNZ helps in the transition from WINS to the multi-label standard DNS zones and can therefore be part of a planning strategy for name resolution. You should understand how GNZ varies from domain suffixes and how it has improved performance over multiple domain suffixes in single-label resolution scenarios with several domains. Windows Server 2012 looks first in the GNZ when a single-label resolution query is received. If a record is in the GNZ, it can't participate in dynamic updates, and dynamic update requests for that record will be refused.

MORE INFO WORKING WITH THE GNZ

See *http://technet.microsoft.com/library/cc794961.aspx* for more information, including the exact steps required to configure a GlobalNames Zone. See also *http://technet.microsoft.com/en-us/library/cc816610* for a discussion around the ways in which GNZ can help with resolution.

Zone hierarchy and zone delegation

The zone hierarchy is the tree-like structure of DNS, in which the root of the zone is represented by a single dot (.). Up the tree from that root are top-level domains (TLDs) such as .com, .net, and .org. The tree branches out into the private domains that you recognize, like microsoft.com and adventure-works.com.

Zone delegation refers to the ability to respond to queries authoritatively by using a portion of a zone. For example, in the hierarchical nature of DNS, the root servers are responsible for the root of the zone and delegate authority for TLDs to TLD servers who then delegate responsibility for domains such as adventure-works.com to private corporate nameservers. When a query arrives for www.adventure-works.com, the query begins at the root server, which refers the query to the responsible server for the .com TLD, which then refers to the responsible server for the domain being queried.

In much the same way that root servers delegate to TLD servers, which then delegate to corporate nameservers, you can also delegate portions of corporate domains such as adventure-works.com to other nameservers so that they become authoritative for that part of the zone. For example, you may want to create an authoritative zone for corp.adventure-works.com so that queries are sent to a different server for hosts in that domain.

Zone delegation is configured in the DNS Manager by right-clicking the zone to be delegated and then selecting New Delegation. Doing so invokes the New Zone Delegation Wizard so that the portion of the zone, such as the corp subdomain in the corp.adventure-works.com scenario, can be delegated.

THOUGHT EXPERIMENT
Troubleshooting primary and secondary servers

In the following thought experiment, apply what you’ve learned about the “Design a Name Resolution Solution Strategy” objective. You can find answers to these questions in the “Answers” section at the end of this chapter.

You’ve configured a secure primary DNS server with a single zone, contoso.com, at a central data center and are deploying a new secondary server at a remote site. The secondary server has its DNS service configured but isn’t receiving updates for the contoso.com DNS zone.

1. **Describe troubleshooting steps that you can take on the secondary server as well as any additional configuration that may be necessary for this scenario to be successful.**
2. **Describe troubleshooting steps that you can take on the primary server as well as any additional configuration that may be necessary for this scenario to be successful.**

MORE INFO **DNS HIERARCHY AND DELEGATION**

See *http://technet.microsoft.com/library/cc731879* for more information on the hierarchy and delegation concepts of DNS.

Objective summary

- The DNS service supports configurations to enhance security including DNSSEC, DNS socket pool, and cache locking.
- DNS socket pool randomizes the source port for DNS queries, and cache locking prevents cached entries from being overwritten for a certain percentage of their Time to Live (TTL) value.
- Microsoft's DNS implementation supports disjoint namespaces, in which the DNS name suffix varies from the Active Directory Domain Services (AD DS) domain name suffix.
- Zone delegation enables a different server to be authoritative for a given zone. This, coupled with zone hierarchy and application partitions, enables complex name service architectures for an organization.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Which of the following are supported disjoint namespace configurations in Windows Server 2012?

   A. When a suffix matches an Active Directory domain in the current or another forest

   B. In a multi–Active Directory domain forest with a single DNS namespace or zone

   C. In a single Active Directory domain that's split into multiple DNS zones

   D. When a certification authority (CA) domain member changes its DNS suffix

2. Which command creates an application partition?

   A. dnscmd <FQDN> /CreateDirectoryPartition <ServerName>

   B. dnscmd <ServerName> /CreateApplicationPartition <FQDN>

   C. dnscmd <ServerName> /CreateDirectoryPartition <FQDN>

   D. dnscmd <FQDN> /CreateApplicationPartition <ServerName>

3. Which feature of Microsoft's DNS implementation helps prevent cache poisoning?

    A. DNS socket pool

    B. Cache lock pooling

    C. Cache poisoning prevention

    D. DNS pool randomization

4. You've configured cache locking and have received reports that clients are receiving stale DNS query responses. Which registry key do you need to change in order to change the TTL ratio that remains locked?

    A. TTLRatioPercent

    B. CacheResetValue

    C. TTLLockingValue

    D. CacheLockingPercent

Objective 2.3: Design and manage an IP address management solution

Windows Server 2012 introduces a new feature called IP address management (IPAM) that helps administrators organize the infrastructure and hosts on the network. IPAM is a powerful tool that can be used to manage both IPv4 and IPv6 network infrastructure as well as provide auditing of an IP address space.

This objective covers the following topics:

- Design considerations, including IP address management technologies such as IPAM, Group Policy based, and manual provisioning, as well as distributed vs. centralized placement
- How to configure role-based access control
- How to configure IPAM auditing
- How to migrate IPs
- How to manage and monitor multiple DHCP and DNS servers
- How to configure data collection for IPAM

Design considerations for IP address management

When managing an IP address infrastructure, your overall goal is to reduce the administrative burden and overhead of managing the address space. For example, many organizations use something as simple as a spreadsheet for managing their address space. This makes tracking who makes changes to the address space difficult. Common tasks such as determining which devices use which IP need to be done manually and then updated manually. All this manual intervention for IP address management introduces errors, not to mention the overhead of having to do it in the first place.

In an ideal world, the IP address spaces in use would manage themselves as much as possible while requiring as little administrator intervention as possible. IP address management (IPAM) in Windows Server 2012 helps alleviate some of that overhead with several key features such as discovery, auditing, reporting, and monitoring.

IPAM enables IP address tracking for Windows Server 2008 and above domain controllers and network policy servers, enables some configuration and monitoring of DNS servers, and enables scope monitoring and configuration of DHCP servers. IPAM attempts to discover domain controllers, DNS servers, DHCP servers, and network policy servers at a regular interval. The servers themselves can be managed by IPAM or left unmanaged. However, to enable discovery, the server needs to allow communication from the IPAM server at the firewall level, and other security settings also need to allow the discovery to take place. All servers must reside in one Active Directory forest and must be domain members to be used with IPAM.

Designing an IPAM solution involves determining where to house the servers, whether at a central location or in a distributed fashion with an IPAM server at each site. IPAM servers don't communicate or share information with each other, but you can customize each server's scope to limit discovery to that site. The practical implication of this design choice is that you can allocate certain scopes in a multi-site environment so that they can be managed by a team local to that environment. In other environments, a centralized approach works best, but you can split IP address management as needed by your organization.

When deploying IPAM, you should be aware of the limitations for a single server:

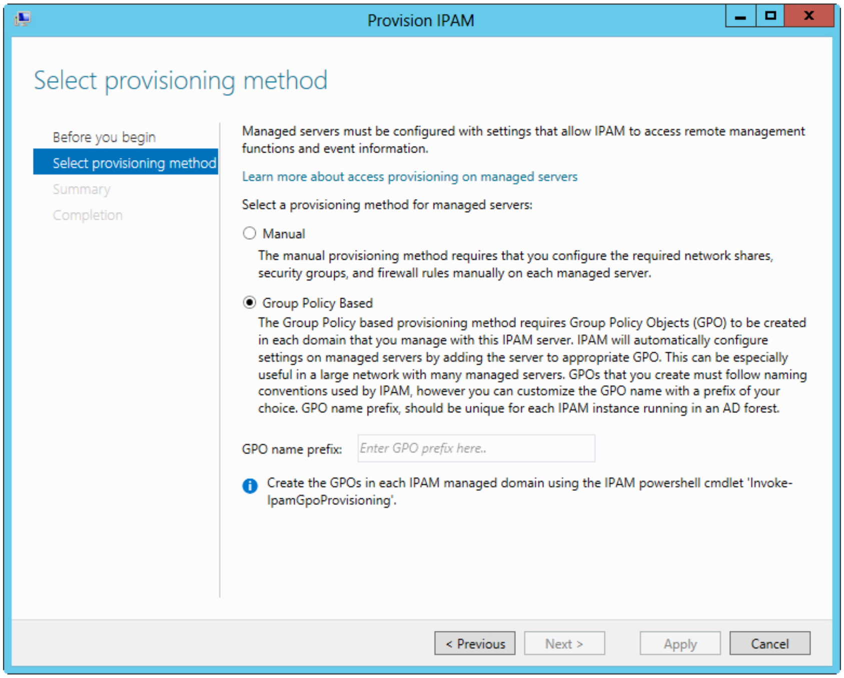
- 150 DHCP servers
- 500 DNS servers
- 6000 DHCP scopes
- 150 DNS zones

Also, non-Microsoft devices such as routers and switches aren't managed or monitored by IPAM.

MORE INFO **IPAM OVERVIEW**

See *http://technet.microsoft.com/library/hh831353* for an overview of IPAM, including additional limitations.

When installed, the IPAM server is provisioned manually or with Group Policy Objects (GPOs). The Provision IPAM Wizard walks through the provisioning process (see Figure 2-12). Note, however, that after you choose the provision method, you can't change it. Using the Group Policy Based option enables the servers to be marked as managed in a more automated fashion, and the GPOs can be removed when a server is marked as unmanaged.



Provision IPAM

Select provisioning method

- Before you begin
- Select provisioning method
- Summary
- Completion

Managed servers must be configured with settings that allow IPAM to access remote management functions and event information.

Learn more about access provisioning on managed servers

Select a provisioning method for managed servers:

○ Manual

The manual provisioning method requires that you configure the required network shares, security groups, and firewall rules manually on each managed server.

● Group Policy Based

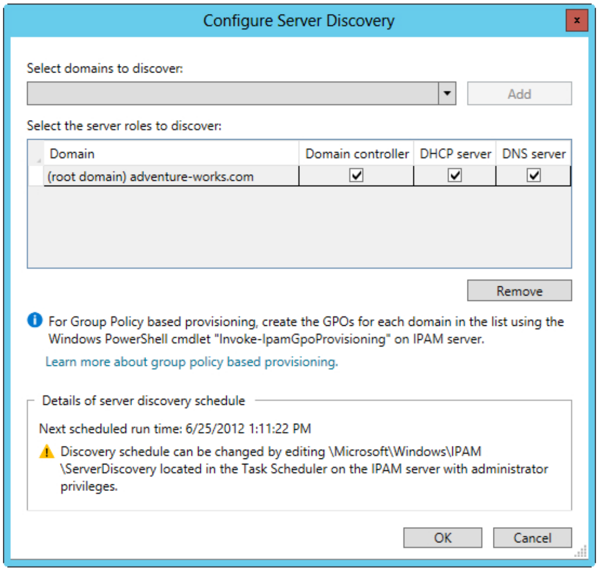
The Group Policy based provisioning method requires Group Policy Objects (GPO) to be created in each domain that you manage with this IPAM server. IPAM will automatically configure settings on managed servers by adding the server to appropriate GPO. This can be especially useful in a large network with many managed servers. GPOs that you create must follow naming conventions used by IPAM, however you can customize the GPO name with a prefix of your choice. GPO name prefix, should be unique for each IPAM instance running in an AD forest.

GPO name prefix: Enter GPO prefix here..

Create the GPOs in each IPAM managed domain using the IPAM powershell cmdlet 'Invoke-IpamGpoProvisioning'.

FIGURE 2-12 Configuring the IPAM provisioning method.

Through GPOs, you can add a Server Discovery task to the task scheduler but can also start it manually through the IPAM server manager. The types of servers to be discovered can also be configured, as shown in Figure 2-13.



Configure Server Discovery

Select domains to discover:

Select the server roles to discover:

Domain	Domain controller	DHCP server	DNS server
(root domain) adventure-works.com	☑	☑	☑

For Group Policy based provisioning, create the GPOs for each domain in the list using the Windows PowerShell cmdlet "Invoke-IpamGpoProvisioning" on IPAM server.

Learn more about group policy based provisioning.

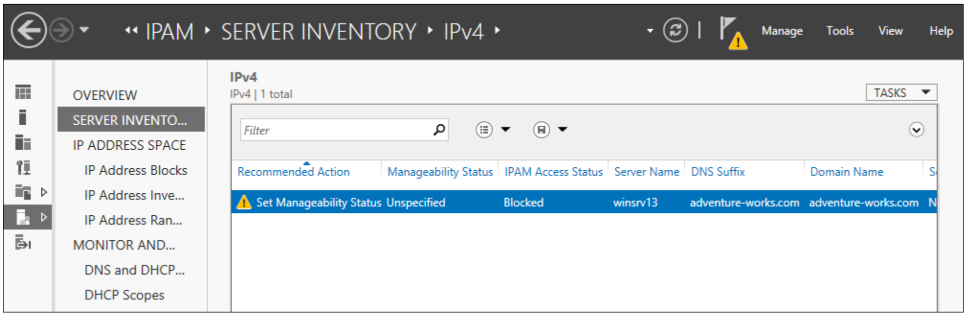
Details of server discovery schedule

Next scheduled run time: 6/25/2012 1:11:22 PM

Discovery schedule can be changed by editing \Microsoft\Windows\IPAM \ServerDiscovery located in the Task Scheduler on the IPAM server with administrator privileges.

FIGURE 2-13 Configuring the types of servers to be discovered by IPAM.

When servers are discovered, their IPAM Access Status shows them as blocked, and their manageability will be Unspecified, as shown in Figure 2-14.



Recommended Action	Manageability Status	IPAM Access Status	Server Name	DNS Suffix	Domain Name	S
⚠ Set Manageability Status	Unspecified	Blocked	winsrv13	adventure-works.com	adventure-works.com	N

FIGURE 2-14 You need to correct the manageability status of a recently discovered server to be able to manage the server.

To configure the server so that it is manageable, add the appropriate GPOs to the server by running the following Windows PowerShell command (as Administrator) from the IPAM server:

```
Invoke-IpamGpoProvisioning -Domain <domain> -GpoPrefixName <Prefix> -IpamServerFqdn
<IPAM Server Name>
```

This command results in three GPOs being created. For example, if you use a GPO name prefix of IPAM1 when provisioning IPAM, the following Group Policy Objects would be created, which can be verified in the Group Policy Management tool:

- IPAM1_DC_NPS
- IPAM1_DNS
- IPAM1_DHCP

When this is complete, each server to be managed needs to obtain the GPOs. Run the following command from within the server itself:

```
gpupdate /force
```

The final step to manage the server is to set the server status to Managed. Right-click the server, select Edit Server, and set the Manageability status to Managed.

Configuring role-based access control

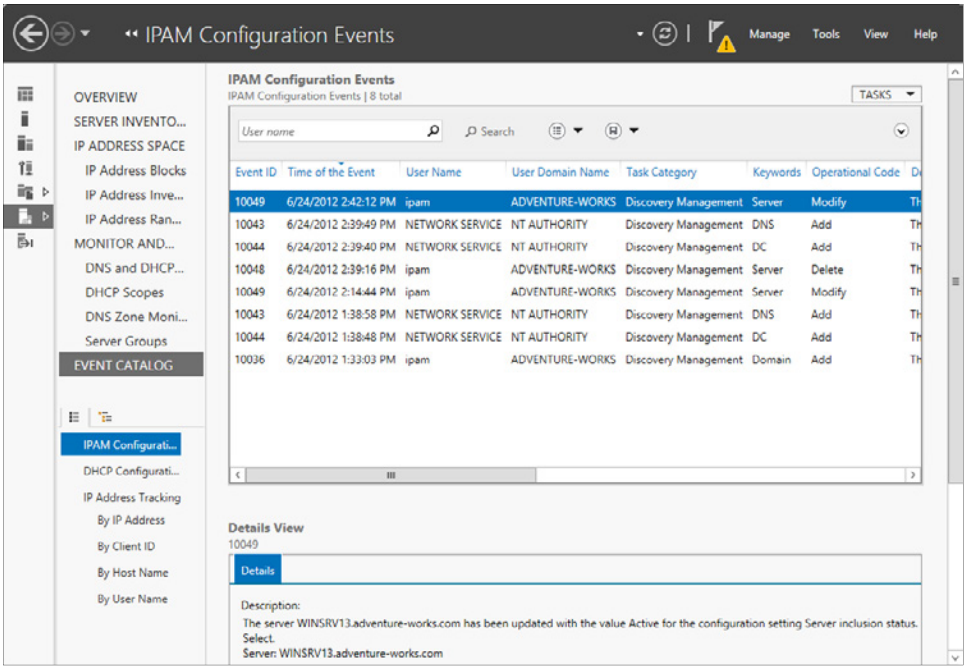
When installed, IPAM creates five security groups, as shown in Table 2-3. These groups are added during IPAM provisioning and can be used like other security groups in Windows. For example, adding users to one of these groups enables them to perform IPAM-related tasks according to the permissions for that group.

TABLE 2-3 Security groups created by IPAM

Security Group	Description
IPAM Users	Allows you to view information about the various areas being managed by IPAM with the exception of IP address-tracking information.
IPAM MSM Administrators	Includes the privileges in the IPAM Users group and adds the ability to manage the IPAM server.
IPAM ASM Administrators	Includes the privileges in the IPAM Users group and adds the ability to manage IP address space tasks and server management.
IPAM IP Audit Administrators	Views IP address-tracking information in addition to the privileges in the IMAP Users group.
IPAM Administrators	Makes up an overall administrative group that can perform all IPAM tasks.

Configuring IPAM auditing

IPAM can be used for auditing purposes to provide information on address utilization, policy compliance, and other information based on the type of servers being managed by IPAM. You use the Event Catalog to configure IPAM auditing (see Figure 2-15). The IP address audit functionality in IPAM collects user information along with the IP address, hostname, and client identifier (MAC address for IPv4 or DUID for IPv6). This information comes from managed DHCP servers, domain controllers, and network policy servers.



IPAM Configuration Events
IPAM Configuration Events | 8 total

Event ID	Time of the Event	User Name	User Domain Name	Task Category	Keywords	Operational Code	D
10049	6/24/2012 2:42:12 PM	ipam	ADVENTURE-WORKS	Discovery Management	Server	Modify	Th
10043	6/24/2012 2:39:49 PM	NETWORK SERVICE	NT AUTHORITY	Discovery Management	DNS	Add	Th
10044	6/24/2012 2:39:40 PM	NETWORK SERVICE	NT AUTHORITY	Discovery Management	DC	Add	Th
10048	6/24/2012 2:39:16 PM	ipam	ADVENTURE-WORKS	Discovery Management	Server	Delete	Th
10049	6/24/2012 2:14:44 PM	ipam	ADVENTURE-WORKS	Discovery Management	Server	Modify	Th
10043	6/24/2012 1:38:58 PM	NETWORK SERVICE	NT AUTHORITY	Discovery Management	DNS	Add	Th
10044	6/24/2012 1:38:48 PM	NETWORK SERVICE	NT AUTHORITY	Discovery Management	DC	Add	Th
10036	6/24/2012 1:33:03 PM	ipam	ADVENTURE-WORKS	Discovery Management	Domain	Add	Th

Details View
10049

Details

Description:
The server WINSRV13.adventure-works.com has been updated with the value Active for the configuration setting Server inclusion status.
Select.
Server: WINSRV13.adventure-works.com

FIGURE 2-15 The Event Catalog in IPAM

By default, the IPAM configuration events are shown, but other events can be shown and can have reports created from the data within them. Included are query tools and a search box to help narrow the focus of the events displayed. Criteria can be added to a query filter, as shown in Figure 2-16.

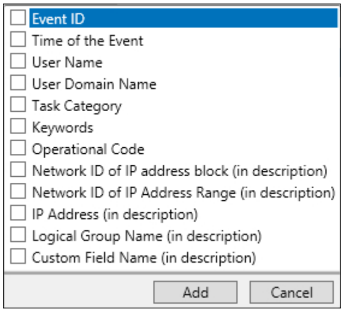

☐ Event ID
☐ Time of the Event
☐ User Name
☐ User Domain Name
☐ Task Category
☐ Keywords
☐ Operational Code
☐ Network ID of IP address block (in description)
☐ Network ID of IP Address Range (in description)
☐ IP Address (in description)
☐ Logical Group Name (in description)
☐ Custom Field Name (in description)

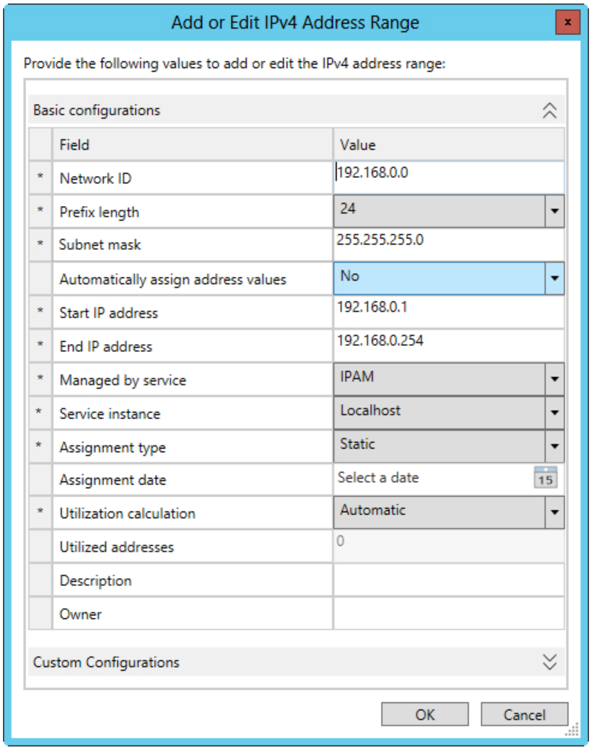
FIGURE 2-16 Additional filter criteria for IPAM auditing.

After the data is retrieved, it can be exported to a comma-separated value (CSV) file.

Migrating IP addresses

IPAM can help you manage IP addresses in a network. IPAM might be used to track utilization of IP addresses for a given site to ensure that enough addresses exist for clients at that site. IPAM defines IP address ranges as groups of contiguous IP addresses, and IP address blocks as groupings of IP address ranges.

When migrating IP addresses to be managed by IPAM, the addresses can be entered manually by address range, address block, and individually by address. You can also import IP addresses into IPAM with a CSV-formatted file. Figure 2-17 shows the Add Or Edit IPv4 Address Range dialog box.



Add or Edit IPv4 Address Range

Provide the following values to add or edit the IPv4 address range:

Basic configurations

	Field	Value
*	Network ID	192.168.0.0
*	Prefix length	24
*	Subnet mask	255.255.255.0
	Automatically assign address values	No
*	Start IP address	192.168.0.1
*	End IP address	192.168.0.254
*	Managed by service	IPAM
*	Service instance	Localhost
*	Assignment type	Static
	Assignment date	Select a date
*	Utilization calculation	Automatic
	Utilized addresses	0
	Description	
	Owner	

Custom Configurations

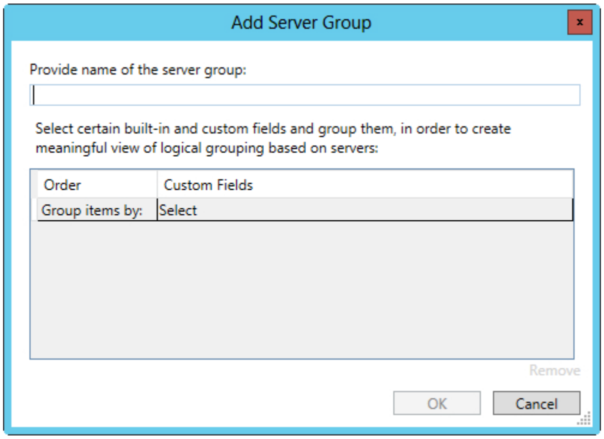
FIGURE 2-17 Adding and editing an IP address range in IPAM.

The Managed By Service drop-down list is helpful for migration planning. With this dialog box you can select how the address block or range is now being managed from choices like IPAM (as shown), a non-Microsoft DHCP solution, Microsoft Virtual Machine Manager (VMM), or another method. Choosing this correctly then enables you to import the IP address space within IPAM but still have address assignment done using the current method. When ready, the IP address can be moved under IPAM management as appropriate.

Managing and monitoring multiple DHCP and DNS servers

IPAM can use logical groupings of servers for configuration, monitoring, and management. This is useful for managing a group of servers that are located at a remote site or have some other common criteria for management and monitoring in IPAM. Server groups are configured within the Monitor and Manage section of IPAM.

Within server groups in IPAM, you add a server group with the Add Server Group dialog box, shown in Figure 2-18.



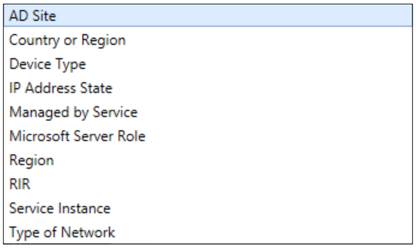
Provide name of the server group:

Select certain built-in and custom fields and group them, in order to create meaningful view of logical grouping based on servers:

Order	Custom Fields
Group items by:	Select

FIGURE 2-18 Adding a server group in IPAM.

As you see within Figure 2-18, you can also group servers by several criteria, as shown in Figure 2-19.



AD Site
Country or Region
Device Type
IP Address State
Managed by Service
Microsoft Server Role
Region
RIR
Service Instance
Type of Network

FIGURE 2-19 Criteria available for ordering the server group in IPAM.

Multi-filtering is available, such that you can choose to first group by one criterion and then additional criteria as needed to create a group with the necessary specificity.

After a server group is created, it can be found within the Server Groups section in the IPAM management console. Like other areas, server groups can be searched and their display order can be changed to locate the server group to be managed.

Configuring data collection

IPAM data-collection activities are scheduled using Task Scheduler and are run at regular intervals. The data collected depends on the items configured within IPAM. For example, if IPAM is being used to manage IP addresses, the data-collection activities include an IP address utilization scan for the IP addresses being managed. The length of time that it takes to collect data also varies accordingly.

The data-collection tasks are configured within the Task Scheduler Library under Microsoft | Windows | IPAM. Table 2-4 shows the task names and their default frequency.

TABLE 2-4 Default schedules for tasks in Task Scheduler

Task Name	Frequency
AddressExpiry	1 day
AddressUtilization	2 hours
Audit	1 day
ServerAvailability	15 minutes
ServerConfiguration	6 hours
ServerDiscovery	1 day
ServiceMonitoring	30 minutes

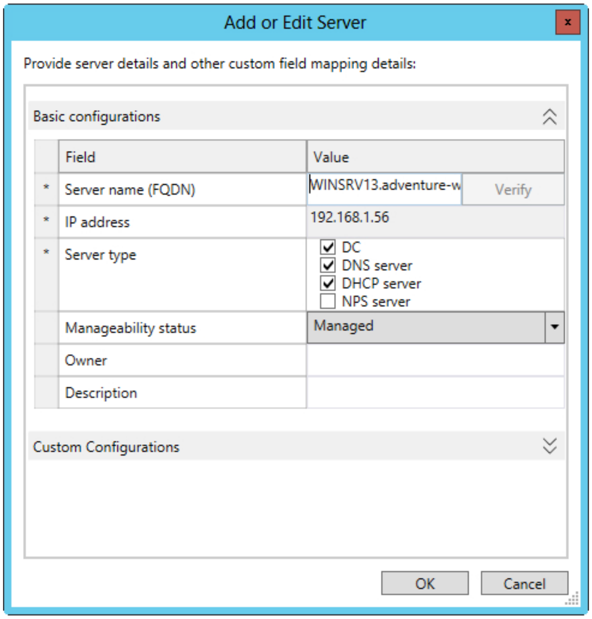
The type of server defines the data to be collected from that server. For example, DNS zones aren't collected from a DHCP server, and so on. You can change the data to be collected from a server within the Add Or Edit Server dialog box. Figure 2-20 shows this dialog box, within which the Server Type can be set according to the need for data collection.

THOUGHT EXPERIMENT
Configuring servers for IPAM management

In the following thought experiment, apply what you've learned about this objective. You can find answers to these questions in the "Answers" section at the end of this chapter.

You've installed the IPAM server role in a centralized placement and have configured it for GPO-based discovery. After the server discovery task, you see two servers available to manage.

Describe the steps involved to bring the servers under IPAM management.



Add or Edit Server

Provide server details and other custom field mapping details:

Basic configurations

	Field	Value
*	Server name (FQDN)	WINSRV13.adventure-w Verify
*	IP address	192.168.1.56
*	Server type	☑ DC ☑ DNS server ☑ DHCP server ☐ NPS server
	Manageability status	Managed
	Owner	
	Description	

Custom Configurations

FIGURE 2-20 The Add Or Edit Server dialog box is used to configure the Server Type in IPAM.

MORE INFO **CONFIGURING IPAM**

See *http://technet.microsoft.com/library/hh831622* for more information on configuring IPAM.

Objective summary

- IPAM has certain limitations on the number of servers that it can manage. These include 150 DHCP servers, 500 DNS servers, 150 DNS zones, and 6000 DHCP scopes.
- The IPAM server can locate servers to provision manually or by using Group Policy Objects (GPOs).
- IPAM servers can be distributed as appropriate for an organization's needs.
- IPAM creates several groups that can be used for role-based access control to the various functions in IPAM.
- IP addresses can be managed and audited in IPAM, and IPAM can be provisioned with IP addresses managed by other DHCP servers.
- Server groups help manage multiple servers in IPAM by creating logical groups as configured by administrators.
- Task Scheduler contains several tasks related to collection of data in IPAM, and data collection can be started manually.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You need to grant access for viewing audit information within IPAM. To which group should you add a user to, to grant that user the minimum level of permission for this task?

   A. IPAM Users

   B. IPAM IP Address Audit Admins

   C. IPAM Administrators

   D. IPAM IP Audit Administrators

2. When provisioning IPAM servers using GPOs, servers are discovered. After configuring them to be managed in IPAM, what command do you need to run on the server to be managed?

   A. Invoke-IpamAudit /server <ipam-servername> /domain

   B. gpupdate /reset

   C. Invoke-IpamAudit /server <ipam-servername> /configure

   D. gpupdate /force

3. What is the default data-collection interval for the ServerDiscovery task?

   A. 3 days

   B. 8 hours

   C. 1 day

   D. 1 hour

4. Which of the following isn't a valid criterion for grouping events (assuming you're not using a custom criterion)?

   A. Keywords

   B. Event Region

   C. User Name

   D. User Domain Name

5. When do IPAM servers exchange information on the servers under their respective management?

   A. When configured in a distributed scenario

   B. Never; IPAM servers don't exchange information

   C. When configured with System Center 2012

   D. When configured to use DNS

Chapter summary

- The DHCP server role in Windows Server 2012 provides for redundancy with split scope, failover through hot standby and load sharing, and failover clustering.
- Failover clustering enables both servers to assign DHCP information by sharing the same DHCP database on a shared storage location.
- DHCP filtering configures how the server to responds to clients by using link-layer MAC addresses.
- The DHCP Management Pack, part of System Center Operations Manager, enables monitoring and reporting of the DHCP service.
- The DNS service supports configurations to enhance security including DNSSEC, DNS socket pool, and cache locking.
- You can manage and audit IP addresses in IPAM. You also can provision IPAM with IP addresses that are managed by other DHCP servers.

Answers

This section contains the solutions to the thought experiments and answers to the objective review questions in this chapter.

Objective 2.1: Thought experiment

You would likely use Hot Standby Failover deploying two servers. The server at the primary location would normally service clients at the primary location, and a secondary server at a remote location would service requests for the remote site. In a Hot Standby scenario, if one of the servers fails, the other can service requests for its failed partner.

Objective 2.1: Review

1. **Correct answer:** C
    - A. **Incorrect:** This isn't the correct split as recommended.
    - B. **Incorrect:** This isn't the correct split as recommended.
    - C. **Correct:** An 80 percent/20 percent ratio for split scopes is good practice, with the primary server receiving 80 percent of the addresses and the secondary server receiving 20 percent.
    - D. **Incorrect:** This isn't the correct split as recommended.
2. **Correct answers:** A and B
    - A. **Correct:** 00-11-09-*-*-* is a valid filter using wildcards to match multiple MACs.
    - B. **Correct:** 001109001111 is a valid MAC filter.
    - C. **Incorrect:** 00:11:09:09:11:09 isn't a valid MAC filter; it uses colons as a separator.
    - D. **Incorrect:** 00-11-09-7c-ef-% isn't a valid MAC filter; it uses a percent sign as a wildcard indicator.
3. **Correct answer:** A
    - A. **Correct:** The path C:\Windows\system32\dhcp is the default location for the database. This is configured in the DHCP server's Properties sheet.
    - B. **Incorrect:** The path C:\Program Files\Microsoft\DHCP\Data doesn't exist.
    - C. **Incorrect:** The path C:\Windows\system32\DHCP\Data doesn't exist.
    - D. **Incorrect:** The registry key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DHCP doesn't house the DHCP database.

4. **Correct answer:** B

    A. **Incorrect:** Increasing the split ratio so that the secondary server has more IP addresses from the scope makes it only so that the secondary server can assign more addresses; it doesn't help alleviate the issue of the secondary server assigning addresses to clients at the primary location.

    B. **Correct:** Introducing a delay for DHCP offers from the secondary using the DHCP management console accomplishes this task by allowing the primary server to respond first but the secondary to respond after a period of time. Because DHCP clients accept the first response, this achieves the requirements.

    C. **Incorrect:** Reducing the load on the primary server so that it can respond faster may help, but because the scenario doesn't indicate that the primary server was overloaded, the secondary server may just be responding faster for other reasons.

    D. **Incorrect:** Placing the secondary DHCP server on a different network segment to introduce a delay in the response doesn't meet the requirement and may introduce connectivity problems for DHCP responses.

Objective 2.2: Thought experiment

1. On the secondary server, you should make sure that the primary server is reachable. This might be achieved with a simple ping command, assuming that ICMP echo requests and echo responses aren't blocked by a firewall. You could also use nslookup on the secondary server and point to the primary server to query for information on the contoso.com domain.

2. On the primary server, you should ensure network connectivity to the secondary server and—importantly—ensure that zone transfers are allowed to the secondary server. This is accomplished at the zone level within the Zone Transfers tab of the Properties sheet. Ensuring that the firewall allows both UDP and TCP ports 53 inbound is also a good idea.

Objective 2.2: Review

1. **Correct answers:** B and C.

    A. **Incorrect:** This isn't a supported configuration as defined by Microsoft.

    B. **Correct:** This is a supported configuration.

    C. **Correct:** This is a supported configuration

    D. **Incorrect:** This isn't a supported configuration.

2. **Correct answer:** C
    A. **Incorrect:** The dnscmd command syntax is incorrect.
    B. **Incorrect:** The dnscmd command syntax is incorrect.
    C. **Correct:** This is the correct syntax for this task.
    D. **Incorrect:** The dnscmd command syntax is incorrect.
3. **Correct answer:** A
    A. **Correct:** DNS socket pool randomizes source ports for queries.
    B. **Incorrect:** This isn’t a valid option.
    C. **Incorrect:** This isn’t a valid option.
    D. **Incorrect:** This isn’t a valid option.
4. **Correct answer:** D
    A. **Incorrect:** This isn’t a valid registry key.
    B. **Incorrect:** This isn’t a valid registry key.
    C. **Incorrect:** This isn’t a valid registry key.
    D. **Correct:** This is the correct registry key.

Objective 2.3: Thought experiment

You first need create the GPOs by using the Invoke-IpamGpoProvisioning command. Then, you need to run gpupdate /force on the servers to be managed. Finally, you need to set the server to Managed status within IPAM.

Objective 2.3: Review

1. **Correct answer:** D
    A. **Incorrect:** IPAM Users is a real group but doesn’t include the permission to view audit information.
    B. **Incorrect:** This isn’t a real group.
    C. **Incorrect:** The IPAM Administrators group has the privilege but isn’t the minimum level necessary for the task.
    D. **Correct:** IPAM IP Audit Administrators is the minimum privileges required for this task.

2. **Correct answer:** D
   - A. **Incorrect:** This isn't a real command.
   - B. **Incorrect:** Although gpupdate is a real command, the proposed answer shows an invalid switch for this operation.
   - C. **Incorrect:** This is an invalid command.
   - D. **Correct:** The gpupdate /force command retrieves the appropriate GPOs from the IPAM server.
3. **Correct answer:** C
   - A. **Incorrect:** This interval is invalid for this task.
   - B. **Incorrect:** This interval is invalid for this task.
   - C. **Correct:** The ServerDiscovery task runs once daily through Task Scheduler by default.
   - D. **Incorrect:** This interval is invalid for this task.
4. **Correct answer:** B
   - A. **Incorrect:** This is a valid criterion; refer to Figure 2-16.
   - B. **Correct:** Event Region isn't a valid criterion.
   - C. **Incorrect:** This is a valid criterion; refer to Figure 2-16.
   - D. **Incorrect:** This is a valid criterion; refer to Figure 2-16.
5. **Correct answer:** B
   - A. **Incorrect:** IPAM servers don't exchange information.
   - B. **Correct:** IPAM servers don't communicate to exchange information.
   - C. **Incorrect:** IPAM servers don't communicate using this protocol.
   - D. **Incorrect:** IPAM servers don't exchange information.

Index

About the Author

STEVE SUEHRING is a technology architect providing both vision and implementation assistance to organizations of all sizes. Steve specializes in large-scale, big-picture uses of technology to solve business problems with a focus on how to meet an organization's goals. His experience enables him to have a unique perspective on interoperability among the technologies available in today's enterprises. Steve has spoken at events around the world, served as an editor for a technology magazine, and authored several books on a wide range of subjects including programming, security, and enterprise administration. You can follow him at his web site *http://www.braingia.org* and *@stevesuehring* on Twitter.