Training Guide: Configuring Advanced Windows Server 2012 R2 Services

Orin Thomas
# Contents at a glance

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td></td>
<td>xvii</td>
</tr>
<tr>
<td>CHAPTER 1</td>
<td>Advanced Active Directory infrastructure</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td>Active Directory sites and replication</td>
<td>59</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td>Advanced DHCP and DNS</td>
<td>119</td>
</tr>
<tr>
<td>CHAPTER 4</td>
<td>Active Directory Certificate Services</td>
<td>205</td>
</tr>
<tr>
<td>CHAPTER 5</td>
<td>Backup and recovery</td>
<td>301</td>
</tr>
<tr>
<td>CHAPTER 6</td>
<td>Advanced file services and storage</td>
<td>373</td>
</tr>
<tr>
<td>CHAPTER 7</td>
<td>High availability</td>
<td>441</td>
</tr>
<tr>
<td>CHAPTER 8</td>
<td>Virtual machine and site resilience</td>
<td>505</td>
</tr>
<tr>
<td>CHAPTER 9</td>
<td>DAC and AD RMS</td>
<td>567</td>
</tr>
<tr>
<td>CHAPTER 10</td>
<td>Active Directory Federation Services</td>
<td>657</td>
</tr>
</tbody>
</table>

Index

715
This page intentionally left blank
## Contents

**Introduction**  

**Chapter 1  Advanced Active Directory infrastructure**  

<table>
<thead>
<tr>
<th>Lesson</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Before you begin</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Lesson 1: Configuring domains and forests</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Multidomain Active Directory environments</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Multiforest Active Directory environments</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Upgrading existing domains and forests</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>User principal name (UPN) suffixes</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Lesson summary</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Lesson review</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>Lesson 2: Configuring trusts</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Trusts</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>SID filtering</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Name suffix routing</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Lesson summary</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Lesson review</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Practice exercises</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Exercise 1: Prepare a domain controller to host a child domain</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>with a contiguous namespace</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exercise 2: Create a child domain with a contiguous namespace</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Exercise 3: Prepare domain controller to host the wingtiptoy.com</td>
<td>30</td>
</tr>
<tr>
<td></td>
<td>tree in the contoso.com forest</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exercise 4: Promote domain controller for new tree in contoso.com</td>
<td>31</td>
</tr>
</tbody>
</table>

---

What do you think of this book? We want to hear from you!  
Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:  

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5: Prepare a domain controller to host a new forest</td>
<td>32</td>
</tr>
<tr>
<td>6: Create new forest</td>
<td>33</td>
</tr>
<tr>
<td>7: Prepare to configure a forest trust relationship</td>
<td>34</td>
</tr>
<tr>
<td>8: Begin creating a forest trust relationship</td>
<td>37</td>
</tr>
<tr>
<td>9: Complete the creation of the forest trust relationship between contoso.com and margiestravel.com</td>
<td>40</td>
</tr>
<tr>
<td>10: Configure name suffix routing</td>
<td>43</td>
</tr>
<tr>
<td>11: Configure selective authentication</td>
<td>45</td>
</tr>
<tr>
<td>12: Configure additional UPN suffixes</td>
<td>50</td>
</tr>
<tr>
<td>13: Configure a shortcut trust</td>
<td>50</td>
</tr>
</tbody>
</table>

Suggested practice exercises .................................................. 54

Answers. .................................................................................... 55

<table>
<thead>
<tr>
<th>Lesson</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>2</td>
<td>56</td>
</tr>
</tbody>
</table>

**Chapter 2  Active Directory sites and replication** 59

Before you begin. ................................................................. 59

**Lesson 1: Configuring sites** ........................................... 59

- Configure sites and subnets | 60
- Manage SRV record registration | 68
- Moving domain controllers | 69

Lesson summary | 70
Lesson review | 71

**Lesson 2: Active Directory replication** 72

- Active Directory partitions | 72
- Understanding multi-master replication | 73
- RODC replication | 76
- Configure RODC password replication | 77
- Monitor and manage replication | 81
- Repadmin | 83
- Upgrade SYSVOL replication | 85

Lesson summary | 86
Lesson review | 86

Practice Exercises ............................................................. 88
Lesson summary
Lesson review

Lesson 3: Deploying and managing IPAM ........................................ 143
  Introduction to IPAM ........................................ 144
  Deploy IPAM ........................................ 144
  Configure IPAM database storage ........................................ 144
  Configure server discovery ........................................ 145
  Managing the IP address space ........................................ 148
  IP address tracking ........................................ 150
  IPAM administration ........................................ 152
  Lesson summary ........................................ 153
  Lesson review ........................................ 153

Practice exercises .................................................................. 154
  Exercise 1: Configure MEL-DC ........................................ 155
  Exercise 2: Configure DNSSEC ........................................ 156
  Exercise 3: Configure the name resolution policy .................. 158
  Exercise 4: Increase the size of the DNS socket pool ............ 161
  Exercise 5: Modify DNS Cache Locking ........................................ 161
  Exercise 6: Create and manage a GlobalNames zone ............ 163
  Exercise 7: Configure and view the DNS event log ............... 165
  Exercise 8: Verify netmask ordering and disable recursion ...... 167
  Exercise 9: Install and activate the DHCP role .................... 168
  Exercise 10: Create a DHCP superscope ............................ 173
  Exercise 11: Create a split scope .................................... 177
  Exercise 12: Configure DHCP Name Protection .................. 180
  Exercise 13: Create new multicast scopes .......................... 182
  Exercise 14: Configure DHCP failover ............................... 184
  Exercise 15: Install the IPAM feature .................................. 186
  Exercise 16: Configure IPAM GPOs and server discovery ....... 187
  Exercise 17: Configure servers to be managed by IPAM ....... 189
  Exercise 18: Manage servers using IPAM ........................... 194
  Exercise 19: Use IPAM to create a DHCP scope ................. 196
  Exercise 20: Use IPAM to manage IP addresses .................. 197

Suggested practice exercises ............................................. 199
Chapter 4 Active Directory Certificate Services 205

Before you begin ................................................ 205

Lesson 1: Installing and configuring
Active Directory Certificate Services ...................... 205
  Installing certificate authorities .......................... 206
  CRL distribution points ..................................... 212
  Online Responders ......................................... 214
  Administrative role separation ............................ 215
  CA backup and recovery ................................... 216
  Lesson summary .............................................. 218
  Lesson review ................................................. 219

Lesson 2: Manage certificates ................................ 220
  Certificate templates ....................................... 221
  Certificate revocation ...................................... 222
  Certificate renewal ........................................ 224
  Autoenrollment ............................................. 225
  Key archiving and recovery ............................... 227
  Lesson summary .............................................. 229
  Lesson review ................................................. 230

Practice exercises ............................................. 231
  Exercise 1: Deploy and configure an enterprise root CA 232
  Exercise 2: Deploy an enterprise subordinate CA ............. 241
  Exercise 3: Install a standalone subordinate CA ............. 246
  Exercise 4: Configure a standalone CA ...................... 250
  Exercise 5: Configure a CRL distribution point ............. 253
  Exercise 6: Configure an Online Responder ................. 257
  Exercise 7: Configure administrative role separation .......... 264
  Exercise 8: Configure a key recovery agent certificate template 268
  Exercise 9: Request a key recovery agent certificate ........... 273
  Exercise 10: Configure key recovery ........................ 277
Exercise 11: Configure a certificate template for autoenrollment and key recovery 279
Exercise 12: Configure Group Policy to support autoenrollment, credential roaming, and automatic renewal 282
Exercise 13: Configure a certificate template to support private key archival and recovery and reenroll all certificate holders 287
Exercise 14: Perform certificate revocation 288
Exercise 15: Perform certificate recovery 292

Suggested practice exercises ................................................. 296

Answers .......................................................... 297
Lesson 1 297
Lesson 2 299

Chapter 5 Backup and recovery 301

Before you begin .......................................................... 301
Lesson 1: Configuring and managing backups ......................... 301
  Windows Server Backup 302
  Windows Azure Backup 306
  Role-specific and application-specific backups 312
  Vssadmin 313
  Data Protection Manager 316
  Lesson summary 317
  Lesson review 317
Lesson 2: Recovering servers .............................................. 318
  Restore from backups 318
  Recover servers using Windows Recovery Environment 321
  Safe mode and Last Known Good Configuration 322
  Configure the Boot Configuration Data store 324
  Lesson summary 325
  Lesson review 325
Practice exercises ......................................................... 326
  Exercise 1: Prepare MEL-DC and CBR-DC for exercises 326
  Exercise 2: Install Windows Server Backup 327
  Exercise 3: Configure CBR-DC for local backup 330
  Exercise 4: Perform a backup to a local volume 334
Contents

Exercise 5: Perform a backup over the network ........................................ 336
Exercise 6: Use Vssadmin ........................................................................ 338
Exercise 7: Perform a full volume recovery using Windows Server Backup .............................................................. 341
Exercise 8: Prepare for Windows Recovery Environment ........................... 344
Exercise 9: Perform full server recovery over the network ....................... 345
Exercise 10: Boot into Safe Mode .............................................................. 348
Exercise 11: Modify Boot Configuration Data store ................................ 350
Exercise 12: Configure a standalone computer for use with Windows Azure Backup .............................................................. 354
Exercise 13: Configure Windows Azure Backup ....................................... 358
Exercise 14: Backup data to Windows Azure Backup ............................... 362
Exercise 15: Restore data from Windows Azure Backup ........................... 367

Suggested practice exercises ................................................................. 369

Answers .............................................................................................. 370
Lesson 1 .............................................................................................. 370
Lesson 2 .............................................................................................. 371

Chapter 6  Advanced file services and storage ......................................... 373

Before you begin .................................................................................. 373

Lesson 1: Configuring advanced file services ......................................... 373
File screens .......................................................................................... 374
Quotas ................................................................................................. 377
Server for NFS ..................................................................................... 379
BranchCache ........................................................................................ 380
File classification ................................................................................ 384
File access auditing ............................................................................ 385
Lesson summary .................................................................................. 387
Lesson review ....................................................................................... 387

Lesson 2: Configuring and optimizing storage ....................................... 388
iSCSI target and initiator ....................................................................... 389
iSNS server ........................................................................................ 392
Thin provisioning and trim .................................................................. 394
Features on Demand ............................................................................ 396
Tiered storage ....................................................................................... 398
Failover and preference settings 452
Continuously available shares 454
Active Directory detached clusters 454
Lesson summary 455
Lesson review 455
Lesson 2: Understanding Network Load Balancing 456
Network Load Balancing 457
Network Load Balancing prerequisites 458
NLB cluster operation modes 459
Managing cluster hosts 461
Port rules 462
Filtering and affinity 463
Upgrading an NLB cluster 464
New NLB PowerShell cmdlets 465
Lesson summary 466
Lesson review 466
Practice exercises 467
Exercise 1: Prepare ADL-DC, MEL-DC, and CBR-DC for exercises 468
Exercise 2: Install the Network Load Balancing feature on ADL-DC, CBR-DC, and MEL-DC 469
Exercise 3: Create a three-node NLB cluster 470
Exercise 4: Configure port rules and affinity 473
Exercise 5: Remove an NLB cluster 475
Exercise 6: Create shared storage for failover clustering 477
Exercise 7: Connect potential cluster nodes to shared storage 479
Exercise 8: Install failover cluster features 483
Exercise 9: Validate cluster configuration 484
Exercise 10: Create a two-node failover cluster 485
Exercise 11: Add a cluster node 486
Exercise 12: Change the quorum configuration 488
Exercise 13: Install and configure a highly available file server 489
Exercise 14: Configure a highly available file share 491
Exercise 15: Configure failover settings, failback settings, and move node 493
Chapter 8 Virtual machine and site resilience

Before you begin ................................................................. 505
Lesson 1: Virtual machine movement ........................................ 505
  Virtual machine failover clustering ....................................... 506
  Shared Nothing Hyper-V live migration ............................... 509
  Storage migration .................................................................. 512
  Virtual machine import and export ..................................... 515
  Lesson summary ..................................................................... 516
  Lesson review ......................................................................... 517
Lesson 2: Site-level fault tolerance ........................................... 518
  Hyper-V Replica .................................................................... 518
  Hyper-V Replica Broker ...................................................... 525
  Multisite clustering ................................................................ 526
  Lesson summary ..................................................................... 528
  Lesson review ......................................................................... 528
Practice exercises .................................................................... 529
  Exercise 1: Install the Hyper-V role on MEL-HV-1 and MEL-HV-2 531
  Exercise 2: Configure identical virtual switches on MEL-HV-1 and MEL-HV-2 536
  Exercise 3: Prepare servers for live migration .......................... 538
  Exercise 4: Prepare servers for replication ............................... 541
  Exercise 5: Create two virtual machines on MEL-HV-1 .............. 544
  Exercise 6: Configure TEST-ONE for replication .................... 547
  Exercise 7: View replication health and perform planned failover of TEST-ONE to MEL-HV-2 550
  Exercise 8: Configure Hyper-V to support live migration .......... 552
  Exercise 9: Perform live migration of TEST-TWO .................... 553
  Exercise 10: Perform storage migration .................................... 556
Chapter 9  DAC and AD RMS  567

Before you begin. ................................................. 567

Lesson 1: Implementing Dynamic Access Control (DAC). .............. 567
   Introduction to Dynamic Access Control  568
   Configuring Group Policy to support DAC  569
   Configuring user and device claims  569
   Configuring resource properties  571
   Central access rules  573
   Central access policies  575
   Staging  576
   Access Denied Assistance  577
Lesson summary  578
Lesson review  579

Lesson 2: Installing and configuring
Active Directory Rights Management Services (AD RMS) .............. 580
    Installing AD RMS  580
    AD RMS certificates and licenses  582
    AD RMS templates  583
    AD RMS Administrators and Super Users  586
    Trusted user and publishing domains  587
    Exclusion policies  589
    Apply AD RMS templates automatically  590
    Backing up AD RMS  591
Lesson summary  592
Lesson review  592
Chapter 10  Active Directory Federation Services  657

Before you begin. .................................................. 657

Lesson 1: Implementing Active Directory Federation Services .......... 657

AD FS Components 658
Claims, claim rules, and attribute stores 658
Claims provider 659
Relying party 660
Relying party trust 660
Claims provider trust 661
Configuring certificate relationship 662
This Training Guide is designed for information technology (IT) professionals who support, or plan to support, Windows Server 2012 R2 networks, and are ramping up on the latest technology. It is assumed that before you begin using this guide, you have a solid, foundation-level understanding of Microsoft Windows client and server operating systems, and common Internet technologies. This guide provides job-role training for the job role that is covered by the Microsoft certification exam 70-412. Use this book to enhance your job skills or to prepare for an upgrade to Windows Server 2012 R2. You can also use it to complement your exam preparation plan if you are preparing for certification.

When Microsoft Learning puts together exam objectives, it doesn’t randomly select pages from TechNet. Instead, in conjunction with subject matter experts and representatives of the product team, it puts together a list of tasks and areas of knowledge that represents what someone in a specific job role would do and need to know on a day-to-day, a weekly, or even a monthly basis.

Each exam maps to a different job role. The objectives for the 70-412 exam are a list of tasks and areas of knowledge that describe what an advanced administrator of the Windows Server 2012 and Windows Server 2012 R2 operating systems with several years of on-the-job experience (managing other server operating systems as well as Windows Server 2012 and Windows Server 2012 R2) does and understands. These topics include some that experienced administrators may not have encountered before or have limited experience with, such as Active Directory Rights Management Services and Active Directory Federation Services.

This book covers the majority of the topics and skills that are the subject of the Microsoft certification exam 70-412. The idea behind this book is that by reading it and by performing the extensive practice exercises at the end of each chapter in your own lab, you can learn how to perform tasks with the technologies addressed by the exam. By performing the tasks yourself in a test environment you’ll learn enough about how these technologies work that you’ll be able to leverage that knowledge in your real-world role as a Windows Server 2012 or Windows Server 2012 R2 administrator. Reading and performing the practice exercises in this book will assist you in preparing for the exam, but it’s not a complete exam preparation solution. If you are preparing for the exam, you should use additional study materials, such as practice tests and the 70-412 Configuring Advanced Windows Server 2012 Services Exam Ref to help bolster your real-world experience.
By using this training guide, you will learn how to do the following:

- Configure and manage high availability
- Configure file and storage solutions
- Implement business continuity and disaster recovery
- Configure network services
- Configure the Active Directory infrastructure
- Configure access and information protection solutions

**System requirements**

The following are the minimum system requirements your computer needs to meet to complete the practice exercises in this book. This book is designed assuming you will be using Hyper-V—either the client version available with some editions of Windows 8.1, or the version available in Windows Server 2012 R2. You can use other virtualization software instead, such as VirtualBox or VMWare Workstation, but the practice setup instructions later in this introduction assume that you are using Hyper-V. The exercises in Chapter 8 require the version of Hyper-V available in Windows Server 2012 R2 and involve functionality specific to this version of the product.

**Hardware requirements**

If you choose to use virtualization software, you need only one physical computer to perform the exercises in this book, except for in Chapter 8, which requires two identical computers. The physical host computer must meet the following minimum hardware requirements:

- x64-based processor that includes both hardware-assisted virtualization (AMD-V or Intel VT) and hardware data execution protection. (On AMD systems, the data execution protection feature is called the No Execute or NX bit. On Intel systems, this feature is called the Execute Disable or XD bit.) These features must also be enabled in the BIOS. (Note: You can run Windows Virtual PC without Intel-VT or AMD-V.) If you want to use Hyper-V on Windows 8 or Windows 8.1, you need a processor that supports Second Layer Address Translation (SLAT).
- 8 gigabytes (GB) of RAM (more is recommended).
- 250 GB of available hard disk space.
- Internet connectivity.
Software requirements

The following software is required to complete the practice exercises:


Virtual machine setup instructions

This set of exercises contains abbreviated instructions for setting up the SYD-DC, MEL-DC, ADL-DC, and CBR-DC computers used in the practice exercises in all chapters of this training kit. To perform these exercises, first install Windows Server 2012 R2 Standard edition using the default configuration, setting the administrator password to Pa$$w0rd.

Exercise 1: SYD-DC to function as a Windows Server 2012 R2 domain controller

1. Log on to the first computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password Pa$$w0rd.

2. Open an elevated PowerShell prompt and issue the following command:
   
   `cmd`

3. Enter the following command:
   
   `Netsh interface ipv4 set address "Ethernet" static 10.10.10.10`

4. Enter the following command:
   
   `netdom renamecomputer %computername% /newname:SYD-DC`

5. Restart the computer and log back on using the Administrator account.

6. Open an elevated PowerShell prompt and issue the following command:
   
   `Add-WindowsFeature AD-Domain-Services -IncludeManagementTools`
7. Open the Server Manager console. Click the Refresh icon.
8. Click the Notifications icon and then click Promote This Server To Domain Controller.
9. On the Deployment Configuration page, choose Add A New Forest. Type **Contoso.com** as the root domain name and then click Next.
10. On the Domain Controller Options page, configure the following settings and then click Next:
   - Forest Functional Level: **Windows Server 2012 R2**
   - Domain Functional Level: **Windows Server 2012 R2**
   - Specify Domain Controller Capabilities: **Domain Name System (DNS) Server And Global Catalog**
   - DSRM Password: **Pa$$w0rd**
11. On the DNS Options page, click Next.
12. On the Additional Options page, click Next.
13. Accept the default settings for the Database, Log Files, and SYSVOL locations, and click Next.
15. On the Prerequisites Check page, click Install.
16. The computer will restart automatically.

**Exercise 2: Prepare Active Directory Domain Server (AD DS)**

1. Log on to server SYD-DC using the Administrator account.
2. Using Active Directory Users And Computers, create a user account named **don_funk** in the Users container and assign the account the password **Pa$$w0rd**. Configure the password to never expire. Add this user account to the Enterprise Admins, Domain Admins, and Schema Admins groups.
3. Open the DNS console and create a primary IPv4 Reverse Lookup Zone for the subnet 10.10.10.x. Ensure that the zone is stored within AD DS and is replicated to all DNS servers running on domain controllers in the forest and allows only secure dynamic updates.
Exercise 3: Prepare ADL-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the second computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password Pa$$w0rd.
3. Open an elevated PowerShell prompt and issue the following commands:
   ```
cmd
Netsh interface ipv4 set address "Ethernet" static 10.10.10.20
Netsh interface ipv4 set dnsservers "Ethernet" static 10.10.10.10 primary
   ```
4. Enter the following command:
   ```
   netdom renamecomputer %computername% /newname:ADL-DC
   ```
5. Restart the computer and then log on again using the Administrator account.
6. Shut down the computer.

Exercise 4: Prepare CBR-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.
2. Log on to the third computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password Pa$$w0rd.
3. Open an elevated PowerShell prompt and issue the following commands:
   ```
cmd
Netsh interface ipv4 set address "Ethernet" static 10.10.10.30
Netsh interface ipv4 set dnsservers "Ethernet" static 10.10.10.10 primary
   ```
4. Enter the following command:
   ```
   netdom renamecomputer %computername% /newname:CBR-DC
   ```
5. Restart the computer and then log on again using the Administrator account.
6. Shut down the computer.
Exercise 5: Prepare MEL-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.

2. Log on to the third computer on which you have installed Windows Server 2012 R2 using the Administrator account and the password Pa$$w0rd.

3. Open an elevated PowerShell prompt and issue the following commands:
   ```
   cmd
   Netsh interface ipv4 set address "Ethernet" static 10.10.10.40
   Netsh interface ipv4 set dnsservers "Ethernet" static 10.10.10.10 primary
   ```

4. Enter the following command:
   ```
   netdom renamecomputer %computername% /newname:MEL-DC
   ```

5. Restart the computer and then log on again using the Administrator account.

6. Shut down the computer.

Exercise 6: Checkpoint all virtual machines

1. Checkpoint all virtual machines. This is the state that they need to be in prior to performing exercises. Checkpoints were termed snapshots in prior versions of Hyper-V.

Acknowledgments

I’d like to thank the following people for their dedication and help in getting this book written: Telmo Sampaio, Troy Mott, and Christina Rudloff. I’d also like to thank Oksana and Rooslan for their patience with me during the writing process.

Errata, updates, and book support

We’ve made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

   http://aka.ms/TG412R2

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at mspinput@microsoft.com.
We want to hear from you

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

http://aka.ms/tellpress

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.
CHAPTER 3

Advanced DHCP and DNS

Windows Server 2012 and Windows Server 2012 R2 include several tools that increase the functionality, security, and manageability of name and Internet Protocol (IP) address spaces. It is important to be able to efficiently manage the name and address space because of the increase in computers on organizational networks that use dynamically assigned names and addresses. This chapter discusses IP address management (IPAM), a technology that simplifies the centralized management of Dynamic Host Control Protocol (DHCP) and Domain Name System (DNS) servers. Maintaining the integrity of the DNS is also important, and in recent years there have been an increase in attacks against DNS infrastructure. In this chapter you discover several different methods that enable you to harden your organization’s DNS infrastructure.

Lessons in this chapter:

- Lesson 1: Implementing an advanced DNS solution
- Lesson 2: Implementing an advanced DHCP solution
- Lesson 3: Deploying and managing IPAM

Before you begin

To complete the practice exercises in this chapter, you need to have deployed computers SYD-DC, MEL-DC, CBR-DC, and ADL-DC as described in the Introduction, using the evaluation edition of Windows Server 2012 R2.

Lesson 1: Implementing an advanced DNS solution

DNS is one of those core network services to which many administrators pay little attention. It’s possible to manage a Windows Server 2012 R2 Active Directory implementation without having to open the DNS Manager console. In some environments, especially those that have stricter than average security requirements, you might need to go beyond the default configuration to make your organization’s DNS implementation more secure. In this lesson, find out about Domain Name System Security Extensions (DNSSEC), how to log DNS traffic, and how to configure a GlobalNames Zone. You read about several steps that you can take to harden a DNS server against attack by nefarious third parties.
After this lesson, you will be able to:

- Configure DNSSEC
- Configure DNS logging
- Configure a GlobalNames Zone
- Configure recursion
- Configure DNS socket pool
- Enable cache locking
- Configure netmask ordering
- Configure delegated administration
- View DNS server statistics

Estimated lesson time: 30 minutes

**DNSSEC**

DNSSEC provides clients with a way of verifying the integrity of the results of a DNS query. DNSSEC accomplishes this by cryptographically signing DNS zone data. When a client queries a record in a zone signed using DNSSEC, the DNS server returns both the record and the record’s digital signature that enables the client to validate that record as shown in Figure 3-1.

![Resource Record Signature (RRSIG) record](image)

**FIGURE 3-1** View the Resource Record Signature (RRSIG) record
When you sign a zone, the following new resource records are created:

- **Resource Record Signature (RRSIG) record**  This record is stored in the DNS zone, and each one is associated with an individual zone record. When a DNS query against the secure zone is performed, the DNS server returns both the record queried and the associated RRSIG record.

- **DNSKEY**  This special record allows for cryptographic verification of the RRSIG records.

- **Next Secure (NSEC/NSEC3) record**  This record provides proof that a queried record does not exist. For example, if a DNS client is querying the record unicorn.contoso.com and there is no unicorn.contoso.com host record hosted in the contoso.com zone, the DNS server returns an NSEC record.

When you implement DNSSEC, the following additional cryptographic keys are created:

- **Trust anchor**  This is a special public cryptographic key associated with a specific zone. The DNSKEY record is validated against this key. When you use DNSSEC with an Active Directory Integrated Zone, the trust anchor is replicated to all DNS servers hosted on domain controllers in the forest.

- **Key Signing Key (KSK)**  This special cryptographic key is used to sign all DNSKEY records. This key is created by a computer that hosts the DNSSEC Key Master role. The DNSSEC Key Master is a computer, usually the first DNS server on which DNSSEC is implemented, that generates and manages signing keys for a DNSSEC protected zone. A single DNS server can function as a DNSSEC Key Master for multiple zones.

- **Zone Signing Key (ZSK)**  This special cryptographic key is used to sign zone data, such as individual host records. The ZSK is created using the DNSSEC Key Master.

You can configure the Group Policy to ensure that clients only accept records from a DNS server for a specific zone if those records have been signed using DNSSEC. You do this by configuring the Name Resolution Policy Table (NRPT), which is located in the Computer Configuration\Policies\Windows Settings\Name Resolution Policy node of a GPO. Figure 3-2 shows configuring Group Policy in such a way that clients who are querying records in the contoso.com zone only accept those records as valid if they are correctly signed using DNSSEC.
DNSSEC is appropriate for high-security environments, such as those where Internet Protocol Security (IPSec) and authenticating switches are also in use. DNSSEC protects against attacks where clients are fed false DNS information. In many small-sized to medium-sized environments, the likelihood of such an attack is minimal. In high-security environments, enabling DNSSEC is a prudent precaution.

MORE INFO  DNSSEC
To learn more about DNSSEC zone, consult the following article:

DNS event logs
The DNS server log is located in the Applications And Services Logs folder in Event Viewer. Depending upon how you configure event logging on the Event Logging tab of the DNS server’s properties, as shown in Figure 3-3, this event log records information including:
Configure the DNS event logs

- Changes to the DNS service. For example when the DNS Server service is stopped or started.
- Zone loading and signing events.
- Modifications to DNS server configuration.
- DNS warning and error events.

By default the DNS server records all of these events. It’s also possible to configure the DNS server to only log errors, or errors and warning events. The key with any type of logging is that you should only enable logging for information that you might need to review at some time. Many administrators log everything “just in case” even though they will only ever be interested in a specific type of event.

In the event that you need to debug how a DNS server is performing, you can enable debug logging on the Debug Logging tab of the DNS server’s properties dialog box as shown in Figure 3-4. Debug logging is resource intensive, and you should only use it when you have a specific problem related to the functionality of the DNS server. You can configure debug logging to use a filter so that only traffic from specific hosts is recorded, rather than traffic from all hosts that interact with the DNS server.
GlobalNames zones

GlobalNames zones provide single-label name resolution. Single-label name resolution allows single names to be translated to IP addresses, such as Windows Server Update Services (WSUS), rather than requiring fully qualified domain names (FQDN) such as wsus.contoso.com. In the past, single-label name resolution has been handled by Windows Internet Name Service (WINS), a service that translates NetBIOS names to IPv4 addresses. GlobalNames zones are hosted on DNS servers and are intended as a replacement technology for WINS. You use alias (CNAME) records when populating a GlobalNames zone, which maps the single-label name to an existing FQDN as shown in Figure 3-5.
Consider using GlobalNames zones in the following circumstances:

- You need to provide single-label name resolution when your network uses IPv6 addressing. WINS does not support IPv6, whereas a single-label record in the GlobalNames zone are mapped to A or AAAA records, allowing both IPv4 and IPv6 name resolution.

- You need to provide single-label name resolution for a small number of hosts. An advantage of WINS is that it’s dynamically populated. You must populate the GlobalNames zone manually by creating CNAME records.

**MORE INFO  GLOBALNAMES ZONE**

To learn more about the GlobalNames zone, consult the following article:


To deploy the GlobalNames zone, you need to do the following:

- Create a new Active Directory integrated forward lookup zone named GlobalNames that you have configured to replicate throughout the forest.

- Manually activate the GlobalNames zone on each DNS server in the forest by running the following Windows PowerShell command (substituting DNSServerName name for the FQDN of the DNS server):

```
Set-DNSServerGlobalNameZone -ComputerName DNSServerName -Enable $True
```
Quick check

- What type of DNS records does a GlobalNames zone host?

Quick check answer

- A GlobalNames zone hosts CNAME, also known as alias, records.

Advanced DNS options

In high-security environments there are a number of steps that you can take to make a DNS server more secure from attackers who attempt to spoof the server so that it provides records that redirect clients to malicious sites. Although DNSSEC provides security for zones hosted on the server, most DNS server traffic involves retrieving information from remote DNS servers and then passing that information on to clients. In this section you find out about settings that you can configure to ensure that the information relayed to clients retains its integrity in the event that a nefarious third party attempts to spoof your organization’s DNS servers.

DNS socket pool

DNS socket pool is a technology that makes cache-tampering and spoofing attacks more difficult by using source port randomization when issuing DNS queries to remote DNS servers. To spoof the DNS server with an incorrect record, the attacker needs to guess which randomized port was used as well as the randomized transaction ID issued with the query.

A DNS server running on Windows Server 2012 or Windows Server 2012 R2 uses a socket pool of 2,500 by default. You can use the dnscmd command-line tool to vary the socket pool between 0 and 10,000. For example, to set the socket pool size to 4,000, issue the following command:

```
dnscmd /config /socketpoolsize 4000
```

You must restart the DNS service before the reconfigured socket pool size is used.

MORE INFO DNS SOCKET POOL

To learn more about the DNS socket pool, consult the following article:


DNS cache locking

DNS cache locking enables you to control when information stored in the DNS server’s cache can be overwritten. For example, when a recursive DNS server responds to a query for a record that is hosted on another DNS server, it caches the results of that query so that it doesn’t have to contact the remote DNS server if the same record is queried again within the TTL (Time to Live) value of the resource record. DNS cache locking prevents record data in a
DNS server’s cache from being overwritten until a configured percentage of the TTL value has expired. By default, the DNS cache locking value is set to 100, but you can reset it using the Set-DNSServerCache cmdlet with the LockingPercent option. For example, to set the cache locking value to 80 percent, issue the following command and then restart the DNS server service:

```
Set-DNSServerCache -LockingPercent 80
```

**MORE INFO DNS CACHE LOCKING**

To learn more about the DNS Cache Locking zone, consult the following article:


**DNS recursion**

DNS servers on Windows Server 2012 or Windows Server 2012 R2 perform *recursive queries* on behalf of clients by default. This means that when the client asks the DNS server to find a record that isn’t stored in a zone hosted by the DNS server, the DNS server goes out and finds the result of that query and passes it back to the client. It’s possible for nefarious third parties to use recursion as a denial-of-service (DoS) attack vector, slowing a DNS server to the point where it becomes unresponsive. You can disable recursion on the Advanced tab of the DNS server’s properties as shown in Figure 3-6.

**FIGURE 3-6 Configure advanced DNS properties**
MORE INFO  DNS RECURSION

To learn more about the DNS recursion, consult the following article:

Netmask ordering

Netmask ordering ensures that the DNS server returns the host record on the requesting client’s subnet if such a record exists. For example, imagine that the following host records existed on a network that used 24-bit subnet masks:

- 10.10.10.105  wsus.contoso.com
- 10.10.20.105  wsus.contoso.com
- 10.10.30.105  wsus.contoso.com

If netmask ordering is enabled and a client with the IP address 10.10.20.50 performs a lookup of wsus.contoso.com, it is always returned the record 10.10.20.105 because this record is on the same subnet as the client. If netmask ordering is not enabled, then the DNS server returns records in a round robin fashion. If the requesting client is not on the same network as any of the host records, then the DNS server also returns records in a round robin fashion. Netmask ordering is useful for services such as Windows Server Update Services (WSUS) that you might have at each branch office. When you use it, the DNS server redirects the client in the branch office to a resource on the local subnet when one exists.

Netmask ordering is enabled by default on Windows Server 2012 and Windows Server 2012 R2 DNS servers. You can verify that netmask ordering is enabled by viewing the advanced properties of the DNS server as shown in Figure 3-7.
REAL WORLD  DEFAULTS ARE USUALLY GOOD

For the most part, the defaults such as netmask ordering and round robin are going to be suitable for your environment, and you probably won’t need to change them. When both are enabled, netmask ordering takes priority over round robin, meaning that a record on the same subnet will be returned where appropriate and in a round robin manner if no such record exists. The one that you’re likely to want to enable is automatic scavenging of stale records. This is especially useful if you have a DNS zone that services a large number of mobile clients. If you don’t enable scavenging, the zone becomes populated with the records of computers that might have touched your network a long time ago but never returned.

Delegated administration

In some larger environments, you might want to separate administrative privileges so that the people who are responsible for managing your organization’s DNS servers don’t have other permissions, such as the ability to create user accounts or reset passwords. By default, members of the Domain Admins group are able to perform all DNS administration tasks on DNS servers within a domain. Members of the Enterprise Admins group are able to perform all DNS administration tasks on any DNS server in the forest.

You can use the DNSAdmins domain local group to grant users the ability to view and modify DNS data as well as server configuration of DNS servers within a domain. You add users to this group when you want to allow them to perform DNS administration tasks without giving them additional permissions. You can assign permissions that allow users or security groups to manage a specific DNS server using the Security tab of the server’s properties as shown in Figure 3-8.
You can also configure permissions at the zone level. You do this by assigning a security principal permissions on the Security tab of the zone’s properties as shown in Figure 3-9. You might do this when you want to allow a specific person to manage host records without assigning them any other permissions. Today most organizations allow DNS records to be updated dynamically. This means that the only zones where you might need to configure special permissions to allow manual management are special ones, such as those that are accessible to clients on the Internet.
Analyze zone level statistics

You can understand how a DNS zone is being utilized by clients, by viewing DNS statistics. You can do this on computers running the Windows Server 2012 R2 operating system by using the Get-DnsServerStatistics cmdlet. Some of the information that you can view using this cmdlet includes:

- **Cache statistics**  View information about the number of requests that the DNS server satisfies from cache.
- **DNSSEC statistics**  Provides data about successful and failed DNSSEC validations.
- **Error statistics**  Detailed information about the number of errors, including bad keys, bad signatures, refusals, and unknown errors.
- **Master statistics**  Contains information about zone transfer statistics.
- **Query statistics**  Information about queries made to the DNS server.
- **Record statistics**  Data about number of records in the cache and memory utilization.
- **Recursion statistics**  Information about how the DNS server solves recursive queries.

You can view statistics related to a specific zone by using the –Zonename parameter. For example, if you wanted to view the statistics of the australia.adatum.com zone, you would issue the following command from an elevated Windows PowerShell prompt on a computer that hosts the DNS server role:

`Get-DnsServerStatistics -Zonename australia.adatum.com`
Lesson summary

- DNSSEC uses digital signatures to allow clients to verify the integrity of DNS records returned from a DNS server.
- The NRPT enables you to configure whether a client requires a specific zone to be signed using DNSSEC.
- A DNS event log records DNS events such as service startup and shutdown as well as errors.
- Debug logging enables you to record DNS traffic and events more thoroughly, though this has an effect on performance.
- GlobalNames zone provides single-label DNS resolution and can serve as a replacement for WINS.
- The DNS socket pool allows for port randomization with DNS requests as a way of protecting against spoofing attacks.
- DNS cache locking blocks a record stored in the DNS server’s cache from being overwritten until a specified percentage of the record’s TTL has expired.
- You can enable DNS recursion as a way of hardening a DNS server against attacks that use recursion as a way of denying service.
- Netmask ordering allows the DNS server to return a DNS record that is on the same IP subnet as the client, if such a record exists.
- You can analyze zone level statistics using the Get-DnsServerStatistics cmdlet.

Lesson review

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

1. The contoso.com zone hosts DNS records that map FQDNs of hosts in the zone to their IPv6 addresses. You have configured a GlobalNames zone and want to allow single-label name resolution of the name WSUS to the appropriate IPv6 address. Which type of record should you create in the GlobalNames zone to accomplish this goal?

   A. Host (AAAA)
   B. Alias (CNAME)
   C. Mail Exchanger (MX)
   D. Pointer (PTR)
2. You have deployed WSUS servers to each of your organization’s branch offices. Each branch office is located on its own subnet. You have created DNS records that use the same name, wsus.contoso.com, for each of the WSUS servers in these different branch offices. You want to ensure that when a client makes a name request for the record wsus.contoso.com, the DNS server returns the record that corresponds to an IP address on the client’s local subnet. Which of the following DNS options do you configure to accomplish this goal?
   A. Socket pool
   B. Cache locking
   C. Recursion
   D. Netmask ordering

3. The DNS server that hosts your organization’s external address space is under attack from nefarious third parties who are slowing it down by constantly launching DNS queries against the server for hosts in zones not hosted on the server. The DNS server should only return data for zones that it hosts directly. Which of the following settings should you configure to stop it responding to queries for hostnames located in zones that it does not host?
   A. Recursion
   B. Netmask ordering
   C. Cache locking
   D. Socket pool

4. You want to ensure that a record stored in the DNS server’s cache cannot be overwritten until 90 percent of its TTL period has expired. Which of the following DNS server settings would you configure to accomplish this goal?
   A. Netmask ordering
   B. Recursion
   C. Socket pool
   D. Cache locking

5. You want to increase the number of ports available that can be used when the DNS server makes a query. Which of the following DNS server settings should you configure to accomplish this goal?
   A. Socket pool
   B. Netmask ordering
   C. Recursion
   D. Cache locking
Lesson 2: Implementing an advanced DHCP solution

Like DNS, DHCP is another network service that most administrators barely pay attention to after they’ve configured it. The main concern that most administrators have with DHCP is that up until the release of Windows Server 2012, it’s been difficult to configure as a highly available service. Although DNS became highly available through being able to be hosted on any domain controller, the problem with making DHCP highly available was ensuring that when multiple DHCP servers were in play, duplicate addresses weren’t assigned to separate clients. In this lesson you find out about superscopes and multicast scopes. You also see how you can make DHCP more fault tolerant by implementing split scopes or by deploying DHCP failover.

After this lesson, you will be able to:

- Create and manage DHCP superscopes
- Implement and maintain multicast scopes
- Create DHCP split scopes
- Configure DHCP Name Protection
- Implement DHCP failover
- Configure DNS registration

Estimated lesson time: 30 minutes

Superscopes

A superscope is a collection of individual DHCP scopes. You might create a superscope when you want to bind existing scopes together for administrative reasons. For example, you might have a subnet in a building that is close to fully allocated. You add a second subnet to the building and then bind them together into a superscope. The process of binding several separate logical subnets together on the same physical network is known as multinetting. Figure 3-10 shows a superscope.
There needs to be at least one existing scope present on the DHCP server before you can create a superscope. After you have created a superscope, you can add new subnets to, or remove subnets from, that scope. It’s also possible to deactivate subnets within a scope, while keeping others active. You might use this technique when migrating clients from one IP address range to another, having both the source and destination scopes part of the same superscope, activating the new scope, and deactivating the original scope as necessary when performing the migration.

**MORE INFO SUPERSCOPES**


**Multicast scopes**

A *multicast address* is an address that allows many communications on a network. When you use multicast, multiple hosts on a network listen for traffic on a single multicast IP address. Multicast addresses are in the IPv4 range of 224.0.0.0 through to 239.255.255.255. *Multicast scopes* are collections of multicast addresses. You can configure a Windows Server 2012 or Windows Server 2012 R2 DHCP server to host multicast scopes. Multicast scopes are also known as MADCAP (Multicast Address Dynamic Client Allocation Protocol) scopes as applications that require access to multicast addresses support the MADCAP application programming interface (API). Figure 3-11 shows a multicast scope.
FIGURE 3-11 A multicast scope

MORE INFO MULTICAST SCOPES

To learn more about multicast scopes consult the following article:

Windows Deployment Services are the most common use of multicast addresses in infrastructures that use the default configurations of Windows Server 2012 or Windows Server 2012 R2. You can, however, configure the Windows Deployment Services (WDS) server with its own set of multicast addresses, and you don’t need to configure a special multicast scope in DHCP to support this role.

Quick check

■ What is the range of multicast IP addresses?

Quick check answer

■ Multicast IP addresses are in the range of 224.0.0.0 through 239.255.255.255

Split scopes

Split scope is one method of providing fault tolerance for a DHCP scope. The idea behind a split scope is that you host one part of the scope on one DHCP server, and a second smaller part of the scope on a second DHCP server. Usually this split has 80 percent of the addresses on the first DHCP server, and 20 percent of the addresses on the partner server. In this scenario, the DHCP server that hosts the 20 percent portion of the address space is usually located on a remote subnet. In this scenario you use a DHCP Relay Agent configured with a delay so that the majority of addresses are leased from the DHCP server that hosts 80 percent of the address space. Split scopes are most likely to be used in scenarios where your DHCP servers aren’t running on the Windows Server 2012 operating system. If you want to provide
fault tolerance for scopes hosted on servers running Windows Server 2012 or Windows Server 2012 R2, you should instead implement DHCP failover.

**MORE INFO SPLIT SCOPES**


### DNS registration

You can configure a DHCP server running the Windows Server 2012 or Windows Server 2012 R2 operating system to register a host’s name in DNS when that DHCP server leases an address to a client. When you do this, you ensure that addresses stored in the DNS zone match the IP addresses leased by the DHCP server. This is useful in environments where hosts are often changing IP addresses because it ensures that the DNS server has the most up-to-date name/IP address mapping. You configure DNS registration at the DHCP server level or at the individual DHCP scope level. Figure 3-12 shows the DNS registration page of a DHCP scope named ALPHA where dynamic registration is configured.

![FIGURE 3-12 DNS registration](image)

You can configure the following DNS registration options:

- **Enable DNS Dynamic Updates According To The Settings Below**
  
  This setting allows you to configure the DHCP server to only update DNS records when requested...
by the client (the default value). You can also configure registration to always
dynamically update DNS records each time the DHCP server leases an address.

- **Discard A And PTR Records When Lease Is Deleted** Enabled by default, the
  DHCP server will instruct the DNS server to remove any associated host and reverse
  lookup records when a DHCP lease expires and is deleted. Use this option in scopes
  that support transient clients, such as those that only infrequently connect to a specific
  network.

- **Dynamically Update DNS Records For DHCP Clients That Do Not Request
  Updates** Enabling this setting will ensure that DNS records are always updated when
  the DHCP server leases an address. Selecting this option configures the DHCP server to
  perform registration in a manner similar to when the Always Dynamically Update DNS
  records option is enabled.

- **Disable Dynamic Updates For DNS PTR Records** This option configures the DHCP
  server to update host (A) records, but does not update records in a reverse lookup
  zone. This option is useful for organizations that haven’t configured reverse lookup
  zones where attempts to register PTR records cause errors in the event log.

**Name Protection**

DHCP *Name Protection* is a feature that enables you to ensure that the hostnames that a
DHCP server registers with a DNS server are not overwritten in the event that a non-Windows
operating system has the same name. DHCP Name Protection also protects names from
being overwritten by hosts that use static addresses that conflict with DHCP-assigned
addresses.

For example, in the contoso.com domain there is a computer running the Windows 8.1
operating system that has the name Auckland. It receives its IP address information from a
Windows Server 2012 DHCP server. The DHCP server registers this name in DNS, and a record
associating the name Auckland.contoso.com with the IP address assigned to the computer
running Windows 8.1 is now present in the contoso.com DNS zone. A newly installed
computer running on a distribution of Linux is also assigned the name Auckland. Because
Name Protection has been enabled, this new computer is unable to overwrite the existing
record with a record associating the name Auckland.contoso.com with the Linux computer’s
IP address. If Name Protection had not been enabled, it’s possible that the record would have
been overwritten.

You can enable Name Protection on a scope by clicking Configure on the DNS tab of the
IPv4 or IPv6 properties dialog box as shown in Figure 3-13. You can also do this using the
Set-DhcpServerv4DnsSetting or the Set-DhcpServerv6DnsSetting cmdlet. For example, to
configure the DHCP server on computer MEL-DC so that Name Protection is enabled on all
IPv4 scopes, issue the command:

```
Set-DhcpServerv4DnsSetting –Computer MEL-DC –NameProtection $true
```
DHCP failover

DHCP failover enables you to configure DHCP to be highly available without using split scopes. DHCP failover is a feature new to Windows Server 2012. You have two options when configuring DHCP failover:

- **Hot standby mode**  This relationship is a traditional failover relationship and is shown in Figure 3-14. When you configure this relationship, the primary server handles all DHCP traffic unless it becomes unavailable. You can configure DHCP servers to be in multiple separate relationships, so it’s possible that a DHCP server can be the primary server in one relationship and a hot standby server in another relationship. When configuring this relationship, you specify a percentage of the address ranges to be reserved on the standby server. The default value is 5 percent. This 5 percent of addresses is available as soon as the primary server is unavailable. The hot standby server takes control of the entire address range when the figure specified by the state switchover interval is reached. The default value for this interval is 60 minutes.
**FIGURE 3-14** Configure a hot standby relationship

- **Load sharing mode**  This is the default mode when you create a DHCP failover relationship. In this mode both servers provide IP addresses to clients according to the ratio defined by the load balance percentage as shown in Figure 3-15. The default is for each server to share 50 percent of the load. The Maximum Client Lead Time is used to renew DHCP leases issued by the failed partner.
Prior to configuring DHCP failover, you need to remove any split scopes between the potential partners. You can also choose a shared secret to authenticate replication traffic, although you won’t have to enter this secret on the partner DHCP server.

**MORE INFO DHCP FAILOVER**

To learn more about DHCP failover consult the following article:


**Lesson summary**

- Superscopes enable you to combine existing DHCP scopes for the purpose of administration.
- Multicast scopes enable you to provide multicast address ranges to applications that require multicast addresses.
- Split scopes enable you to host parts of the same scope on different DHCP servers. Split scopes provide high availability if DHCP servers don’t run the Windows Server 2012 operating system.
- DNS registration allows you to have the DHCP server update DNS with the DHCP client’s name and IP address information.
Name Protection enables you to configure DHCP so that names registered on behalf of Windows clients in DNS can’t be overwritten by hosts using operating systems unrelated to Microsoft.

DHCP failover is a technology new to Windows Server 2012. It enables DHCP servers to be configured in a partner relationship. In hot standby mode, one DHCP server serves as a hot standby for another server, only taking over if the first server becomes unavailable. In load sharing mode, the DHCP servers share IP address allocation duties for the same scope.

Lesson review

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

1. Your organization has two DHCP servers at its central site. The first one is hosted on a computer running the Windows Server 2012 operating system. The second DHCP server is hosted on a computer running the Windows Server 2008 R2 operating system. You want to make a DHCP scope highly available so that clients can still obtain address leases if one of these DHCP servers fail. Which of the following strategies should you implement to accomplish this goal?
   A. Configure DHCP failover. Use hot standby mode.
   B. Configure DHCP failover. Use load sharing mode.
   C. Configure a split scope.
   D. Configure a superscope.

2. Your organization has two DHCP servers at its central site. Both DHCP servers are running on the Windows Server 2012 operating system. One DHCP server also hosts the company’s intranet site. You want to configure DHCP so that one DHCP server handles the majority of the organization’s DHCP traffic and the other DHCP server, installed on the server that hosts the intranet site, only leases addresses if the first one becomes unavailable. The second DHCP server should be able to lease addresses from the entire scope until such time as the first DHCP server is returned to service. Which of the following strategies should you implement to accomplish this goal?
   A. Configure DHCP failover. Use load sharing mode.
   B. Configure a split scope.
   C. Configure DHCP failover. Use hot standby mode.
   D. Configure a superscope.

3. You are about to add a large number of users and computers to one of the existing buildings at your company. Unfortunately the existing DHCP scope used at this building is close to exhaustion. You want to configure DHCP so that clients on this physical network can be leased addresses from either the original or an additional
Lesson 3: Deploying and managing IPAM

IP Address Management (IPAM) is a technology introduced with the release of Windows Server 2012 that simplifies the process of managing multiple DHCP and DNS servers. Rather than having to keep detailed records to track scopes and DHCP servers, IPAM enables you to view and manage this information centrally. In this lesson you find out about the functionality of the IPAM feature and how you can deploy IPAM to manage your organization’s DHCP and DNS servers.

After this lesson, you will be able to:

- Configure IPAM
- Configure server discovery
- Create and manage IP blocks and ranges
- Track IP addresses
- Delegate IPAM administration
- Configure IPAM database storage

Estimated lesson time: 45 minutes
Introduction to IPAM

IPAM enables you to centralize the management of DHCP and DNS servers. Rather than managing each server separately, you can use IPAM to manage them from a single console. You can use a single IPAM server to manage up to 150 separate DHCP servers and up to 500 individual DNS servers. A single IPAM server is able to manage 6,000 separate DHCP scopes and 150 separate DNS zones. You can perform tasks such as creating address scopes, configuring address reservations, and managing DHCP and DNS options globally, rather than having to perform these tasks on a server-by-server basis.

You can also use IPAM to search stored IP address lease data, MAC address data, and corresponding user sign on and sign off information. Microsoft estimates that the Windows Internal Database (WID) used by IPAM is able to store three years of IP address utilization data for an organization that has 100,000 users before data must be purged.

MORE INFO  IPAM
To get more of an overview of IPAM, consult the following article:

Deploy IPAM
You can only install the IPAM feature on a computer that is a member of an Active Directory domain. IPAM is also limited so that you can only use it to manage DHCP and DNS servers that are members of the same Active Directory forest. You can’t use IPAM to manage standalone servers or servers that are members of different forests. You can have multiple IPAM servers within a single Active Directory forest. You are likely to do this if your organization is geographically dispersed.

It’s important to note IPAM cannot manage a locally installed DHCP or DNS server. For this reason you should install the IPAM feature on a server that doesn’t host the DNS or DHCP roles. IPAM is also not supported on computers that host the domain controller server role. Additionally, if you want to use the IPAM server to manage IPv6 address ranges, you need to ensure that IPv6 is enabled on the computer that will host the IPAM server.

MORE INFO  DEPLOYING THE IPAM SERVER
To learn more about deploying the IPAM server, consult the following TechNet document:

Configure IPAM database storage
You could only use the version of IPAM that shipped with Windows Server 2012 with the Windows Internal Database (WID). The version of IPAM available in Windows Server 2012 R2 supports using a SQL Server 2012 instance for hosting IPAM data. This allows you to host the
IPAM database on a host that is separate from the IPAM server. Microsoft recommends that the SQL Server instance be devoted to hosting the IPAM database. You should not host other databases on this instance.

**Configure server discovery**

*Server discovery* is the process where the IPAM server checks with Active Directory to locate domain controllers, DNS servers, and DHCP servers. You select which domains to discover in the Configure Server Discovery dialog box, as shown in Figure 3-16.

![Configure Server Discovery](image)

**FIGURE 3-16** Configure server discovery

After you've completed server discovery, you need to run a special PowerShell cmdlet that creates and provisions Group Policy objects that allow the servers to be managed by the IPAM server. When you set up the IPAM server, you choose a GPO name prefix as shown in Figure 3-17. You use this prefix when executing the Invoke-IpamGpoProvisioning Windows PowerShell cmdlet that creates the appropriate GPOs.
FIGURE 3-17  Select a provisioning method

If you use the GPO prefix IPAM, the three GPOs are named:

- IPAM_DC_NPS
- IPAM_DHCP
- IPAM_DNS

Until these GPOs apply to the discovered servers, these servers are listed as having an IPAM Access Status of Blocked. After the GPOs are applied to the discovered servers, the IPAM Access Status changes to Unblocked as shown in Figure 3-18.
When the discovered service has an IPAM Access Status set to Unblocked, you can edit the properties of the server and set it to Managed as shown in Figure 3-19. After you do this, you can use IPAM to manage the selected services on the server.
Managing the IP address space

The benefit of IPAM is that it enables you to manage all of the IP addresses in your organization. IPAM supports the management of IPv4 public and private addresses whether they are statically or dynamically assigned. IPAM enables you to detect if there are overlapping IP address ranges defined in DHCP scopes on different servers. It also enables you to determine IP address utilization and whether there are free IP addresses in a specific range, and create DHCP reservations centrally without having to configure them on individual DHCP servers. IPAM also enables you to create DNS records based on IP address lease information.

IPAM separates the IP address space into blocks, ranges, and individual addresses. An IP address block, shown in Figure 3-20, is a large collection of IP addresses that you use to organize the address space used in your organization at the highest level. An organization might only have one or two address blocks: one for its entire internal network and another smaller block that represents the public IP address space used by the organization.

![An IPv4 address block](image)

**FIGURE 3-20** An IPv4 address block

An IP address range is part of an IP address block. An IP address range cannot map to multiple IP address blocks. Generally an IP address range corresponds to a DHCP scope. Figure 3-21 shows an IP address range.
An IP address maps to a single IP address range. As Figure 3-22 shows, an IP address includes information about an associated MAC address, how the address is assigned, and when that assignment expires.
More Info  Managing IP Address Space

To learn more about managing IP address space, consult the following article:

IP address tracking

One of the most important features of IPAM is its ability to track IP addresses by correlating DHCP leases with user and computer authentication events on managed domain controllers and Network Policy Servers (NPS). IP address tracking enables you to figure out which user was associated with a specific IP address at a particular point of time, something that can be important when trying to determine the cause of unauthorized activity on the organizational network.

As Figure 3-23 shows, you can search for IP address records using one of the following four parameters:

- **IP address**  Track by IPv4 address, but IPAM does not support tracking on the basis of IPv6 address.
- **By client ID**  Track IP address activity on the basis of media access control (MAC) address.
- **By host name**  Track by the computer’s name as registered in DNS.
Lesson 3: Deploying and managing IPAM

By user name  Track a user name by providing a host name.

![Server Manager](image)

**FIGURE 3-23**  IP address tracking

**MORE INFO  IP ADDRESS TRACKING**

To learn more about IP address tracking, consult the following article:


You can track only data that has been recorded since IPAM has been deployed. So although it is possible to store several years of data in the Windows Internal Database that IPAM uses, you're limited to being able to retrieve only events that have been recorded after IPAM was configured.

**Quick check**

- You want to determine which IP addresses a computer with a particular MAC address was assigned to over a specific period. What IP address tracking category would you use to determine this information?

**Quick check answer**

- You would track by client ID when you have a computer’s MAC address and want to extract additional information from IPAM address tracking.
IPAM administration

You can delegate administrative permissions by adding user accounts to one of five local security groups on the IPAM server. By default, members of the Domain Admins and Enterprise Admins groups are able to perform all tasks on the IPAM server. The five local security groups, shown in Figure 3-24, enable you to delegate the following permissions:

- **IPAM Users**  Members of this group are able to view IPAM server information such as address space and operational event information, but they are unable to view IP address tracking information.

- **IPAM MSM Administrators**  MSM stands for multi-server management. Users added to this group have all the rights of the IPAM Users group and are able to perform common IPAM management tasks such as managing server inventory. They have read-only access to the IP address space. They are unable to view or perform IP address tracking tasks.

- **IPAM ASM Administrators**  ASM stands for address space management administrator. Users added to this group are able to perform all tasks that can be performed by members of the IPAM Users group, but they are also able to manage the IP address space. They cannot perform monitoring tasks and are unable to perform IP address tracking tasks.

- **IPAM IP Audit Administrators**  Members of this group are able to manage server inventory and perform common management tasks, but they have read-only access to the IP address space and IP address tracking information.

- **IPAM Administrators**  Members of this group are able to perform all tasks on the IPAM server including viewing IP address tracking information.

![Computer Management](image)

**FIGURE 3-24**  IPAM local user groups

**MORE INFO**  IPAM ADMINISTRATION

To learn more about IPAM administration, consult the following article:  
Lesson summary

- IPAM enables you to centrally manage DHCP and DNS servers.
- You cannot deploy the IPAM server on a domain controller. You should not deploy a DNS or DHCP server on the IPAM server if you want to manage those servers using IPAM.
- The IPAM server must be a member of an Active Directory domain and can only manage DHCP and DNS servers that are members of the same forest.
- You can use IP address tracking to search the IPAM database on the basis of IP address, MAC address, computer name, or user name.
- Members of the Domain Admins and Enterprise Admins groups have full administrative access to the IPAM server. There are five local security groups on the IPAM server that you can use to delegate administrative privileges.
- The IPAM role available with Windows Server 2012 R2 can use a SQL Server 2012 instance to host the IPAM database.

Lesson review

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

1. You need to give a user the ability to view IP address tracking information stored in your organization’s IPAM server without adding him or her to the IPAM Administrators group. To which of the following IPAM-related security groups could you add this user to grant this privilege?
   A. IPAM Users
   B. IPAM IP Audit Administrators
   C. IPAM MSM Administrators
   D. IPAM ASM Administrators

2. You need to give a user the ability to manage the IP Address Space on an IPAM server without adding the user to the IPAM Administrators group. To which of the following IPAM-related security groups could you add this user to grant this privilege?
   A. IPAM MSM Administrators
   B. IPAM Users
   C. IPAM ASM Administrators
   D. IPAM IP Audit Administrators

3. You want to use IPAM’s IP address tracking feature to determine which IP addresses a computer with a specific MAC address was assigned by your organization’s DHCP servers during a particular week. Which of the following categories should you search on to accomplish this goal?
A. IP address
B. Client ID
C. Host name
D. User name

4. You are in the process of configuring IPAM. You have run the discovery process and discovered three servers that host the DHCP server role. The server’s IPAM Access Status is listed in the IPAM Server Inventory as Blocked. Which of the following steps should you take so that this status changes to unblocked? (Choose two.)

A. Ensure that you have provisioned the GPOs using the Invoke-IpamGPOProvisioning cmdlet.
B. Verify that Group Policy is applied correctly to the server hosting the IPAM server role.
C. Verify that Group Policy is applied correctly to the three servers hosting the DHCP server role.
D. Restart the IPAM server.

**Practice exercises**

The goal of this section is to provide you with hands-on practice with the following:

- Configuring DNSSEC
- Configuring NRPT
- Creating GlobalNames zone
- Configuring advanced DNS server options
- Configuring a DHCP superscope
- Deploying a split scope
- Configuring DHCP Name Protection
- Setting up a multicast scope
- Enabling DHCP failover
- Configuring and deploying IPAM

To perform the exercises in this section, you need access to an evaluation version of Windows Server 2012 R2. You should also have access to virtual machines SYD-DC, MEL-DC, CBR-DC, and ADL-DC, the setup instructions for which are described in the Introduction. You should ensure that you have a checkpoint of these virtual machines that you can revert to at the end of the practice exercises. You should revert the virtual machines to this initial state prior to beginning these exercises.
Exercise 1: Configure MEL-DC

In this exercise, you configure MEL-DC to be a member of the contoso.com domain. To complete this exercise, perform the following steps:

1. Ensure that SYD-DC is started.
2. Start MEL-DC and sign on as Administrator with the password Pa$$w0rd.
3. On the Local Server node of the Server Manager console, verify that the local IP address is set to 10.10.10.40 and then click on the WORKGROUP link next to Workgroup.
4. On the Computer Name tab of the System Properties dialog box, click Change.
5. In the Computer Name/Domain Changes dialog box, click Domain and type contoso.com as shown in Figure 3-25 and then click OK.

![Figure 3-25 Join the domain](image)

6. In the Windows Security dialog box, type the user name don_funk and the password Pa$$word and then click OK.
7. On the Computer Name/Domain Changes dialog box, shown in Figure 3-26, click OK.

![Figure 3-26 Verify the domain join](image)
8. In the dialog box that informs you that you need to restart the computer to apply changes, click OK.
9. Click Close on the System Properties dialog box.
10. Click Restart Now on the Microsoft Windows dialog box.
11. When MEL-DC restarts, sign in as contoso\don_funk with the password `Pa$$w0rd`.

**Exercise 2: Configure DNSSEC**

In this exercise, you configure DNSSEC on the contoso.com zone. To complete this exercise, perform the following steps:

1. Ensure that you are signed on to SYD-DC as contoso\don_funk.
2. From the Tools menu of the Server Manager console, click DNS.
3. In the DNS Manager console, expand the SYD-DC\Forward Lookup Zones node and click the Contoso.com node.
4. Verify that the records present in the Contoso.com zone match those shown in Figure 3-27.

![Figure 3-27: The unsigned DNS zone](image_url)

5. On the Action menu, click DNSSEC and click Sign The Zone.
6. On the DNS Security Extensions (DNSSEC) page of the Zone Signing Wizard, click Next.
7. On the Signing Options page, click Use Default Settings To Sign The Zone as shown in Figure 3-28 and click Next.
8. On the DNS Security Extensions (DNSSEC) page, verify that the Key Master is set to SYD-DC as shown in Figure 3-29 and click Next.


10. On the Action menu of the DNS Manager console, click Refresh and verify the presence of the new DNS records as well as the DNSSEC icon on the zone as shown in Figure 3-30.
Exercise 3: Configure the name resolution policy

In this exercise, you configure the Group Policy so that clients will verify the integrity of DNS records in the contoso.com zone. To complete this exercise, perform the following steps:

1. Ensure that you are signed on to SYD-DC as contoso\don_funk.
2. On the Tools menu of the Server Manager console, click Group Policy Management.
3. In the Group Policy Management Console, expand the Forest: Contoso.com node, expand the Domains node, expand the Contoso.com node, and click Default Domain Policy as shown in Figure 3-31. Click OK on the Group Policy Management Console dialog box.
Practice exercises

CHAPTER 3  159

4. On the Action menu, click Edit.

5. In the Group Policy Management Editor, expand the Computer Configuration\Policies\Windows Settings node and click Name Resolution Policy.

6. In the Name Resolution Policy area, type **contoso.com** in the text box next to the Suffix drop-down menu, select the Enable DNSSEC in This Rule check box, and select the Require DNS Clients To Check That Name And Address Data Has Been Validated By The DNS Server as shown in Figure 3-32. Click Create.
7. In the Group Policy Management Editor, scroll down to view the Name Resolution Policy Table and verify that the settings match those shown in Figure 3-33. Click Apply.

![Name Resolution Policy Table](image1)

**FIGURE 3-33** Verify the Name Resolution Policy

8. Close the Group Policy Management Editor and the Group Policy Management Console.

9. On the taskbar, click the Windows PowerShell icon.

10. Type the following command and press Enter to force a Group Policy update:

    `Gpupdate /force`

11. Type the following command and press Enter to verify that an RRSIG record exists for mel-dc.contoso.com as shown in Figure 3-34:

    `resolve-dnsname mel-dc.contoso.com -server syd-dc -dnssecok`

![Windows PowerShell](image2)

**FIGURE 3-34** Verify the DNS record

Exercise 4: Increase the size of the DNS socket pool

In this exercise, you increase the size of the DNS socket pool. To complete this exercise, perform the following steps:

1. When signed on to SYD-DC as contoso\don_funk, right-click the Windows PowerShell icon on the taskbar and click Run As Administrator. Click Yes in the User Account Control dialog box.

2. Type the following command and press Enter to view the currently configured DNS socket pool site:
   
   `(Get-DNSServer).ServerSetting.SocketPoolSize`

3. Type the following command and press Enter to change the DNS socket pool size to 4,000:
   
   `Dnscmd /config /socketpoolsize 4000`

4. Type the following command and press Enter:
   
   `Restart-Service DNS`

5. Type the following command and press Enter to verify the new DNS socket pool size:
   
   `(Get-DNSServer).ServerSetting.SocketPoolSize`

Exercise 5: Modify DNS Cache Locking

In this exercise, you verify the current DNS Cache Locking setting, change this setting, and then verify the change. To complete this exercise, perform the following steps:

1. Ensure that you are signed on to SYD-DC as contoso\don_funk and have an elevated Windows PowerShell window open.

2. Type the following command and press Enter to verify the size of the current DNS cache locking setting as shown in Figure 3-35:

   `get-DNSServerCache`
3. Configure the cache locking percentage to 80 percent by typing the following command and pressing Enter:
   
   ```powershell
   Set-DNSServerCache -LockingPercent 80
   ```

4. Restart the DNS Server service to apply the changes by typing the following command and pressing Enter:
   
   ```powershell
   Restart-Service DNS
   ```

5. Verify the alterations to the cache locking by typing the following command as shown in Figure 3-36 and pressing Enter:
   
   ```powershell
   get-DNSServerCache
   ```
Practice exercises

CHAPTER 3  163

Exercise 6: Create and manage a GlobalNames zone

In this exercise, you configure single-name resolution by configuring a GlobalNames zone. You then create a record in the GlobalNames zone. To complete this exercise, perform the following steps:

1. While signed on to SYD-DC as contoso\don_funk, open the DNS Manager console by clicking DNS in the Tools menu of the Server Manager console.
2. In the DNS Manager console, click the Forward Lookup Zones node under SYD-DC.
3. On the Action menu, click New Zone.
4. On the Welcome page of the New Zone Wizard, click Next.
5. On the Zone Type page, click Primary Zone, ensure that Store The Zone In Active Directory is selected, and click Next.
6. On the Active Directory Zone Replication Scope page, click To All DNS Servers Running On Domain Controllers In This Forest: Contoso.com and click Next.
7. In the Zone Name page, type GlobalNames, as shown in Figure 3-37, and click Next.
8. On the Dynamic Update page, click Do Not Allow Dynamic Updates and click Next.
10. Switch to the elevated Windows PowerShell window, type the following command, and press Enter.
    ```powershell
    Set-DNSServerGlobalNameZone -ComputerName SYD-DC -Enable $True
    ```
11. Type the following command and press Enter to verify that the GlobalNameZone is enabled as shown in Figure 3-38:
    ```powershell
    Get-DNSServerGlobalNameZone
    ```
12. Switch to the DNS Manager console and click the GlobalNames zone under Forward Lookup Zones.


14. In the New Resource Record dialog box, configure the following information, as shown in Figure 3-39, and click OK:

- Alias Name (Uses Parent Domain If Left Blank): Bondi
- Fully Qualified Domain Name (FQDN) For Target Host: syd-dc.contoso.com

![Figure 3-39 The CNAME record](image)

**Exercise 7: Configure and view the DNS event log**

In this exercise, you configure event logging for the DNS service. To complete this exercise, perform the following steps:

1. While signed on to SYD-DC as contoso\don_funk, open the DNS Manager console.
2. In the DNS Manager console, right-click SYD-DC and click Properties.
3. On the SYD-DC Properties dialog box, click the Event Logging tab.
4. On the Event Logging tab, ensure that All Events are selected as shown in Figure 3-40 and click OK.
5. In the Tools menu of the Server Manager console, click Event Viewer.

6. In the Event Viewer Console, expand the Applications And Service Logs node and click DNS Server.

7. In the DNS Server log, look for Event ID 7646 which confirms that the zone contoso.com is now signed with DNSSEC as shown in Figure 3-41.
Exercise 8: Verify netmask ordering and disable recursion

In this exercise, you verify that netmask ordering is enabled on the DNS server hosted on SYD-DC. You also disable recursion. To complete this exercise, perform the following steps:

1. While signed on to SYD-DC as contoso\don_funk, switch to the DNS Manager console.
2. In the DNS Manager console, right-click the SYD-DC node and click Properties.
3. On the SYD-DC Properties dialog box, click the Advanced tab.
4. On the Advanced Tab of the SYD-DC Properties dialog box, select Disable Recursion (Also Disables Forwarders) and verify that Enable Netmask Ordering is enabled as shown in Figure 3-42.

8. View the DNS event in the event log.
5. Click OK to close the SYD-DC Properties dialog box.
6. Close the DNS Manager console.

**Exercise 9: Install and activate the DHCP role**

In this exercise, you install the DHCP role on MEL-DC and SYD-DC. To complete this exercise, perform the following steps:

1. Ensure that you are signed on to SYD-DC as contoso\don_funk.
2. In the Server Manager console on SYD-DC, click the All Servers node.
3. On the Manage menu, click Add Servers.
4. In the Add Servers dialog box, click Find Now.
5. In the Add Servers dialog box, click MEL-DC and click the arrow to add it to the Selected box as shown in Figure 3-43. Click OK.
6. Right-click SYD-DC and click Start Performance Counters.
7. Right-click MEL-DC and click Start Performance Counters.
8. In the Manage menu of the Server Manager console, click Add Roles And Features.
10. On the Select Installation Type Page, click Role-Based or Feature-Based Installation and click Next.
11. On the Select Destination Server page, click MEL-DC.contoso.com as shown in Figure 3-44 and click Next.
12. On the Select Server Roles page, click the DHCP Server check box.
13. In the Add Roles And Features Wizard dialog box, click Add Features.
14. On the Select Server Roles page, click Next three times and then click Install.
15. When the installation completes, click Close on the Installation Progress page of the Add Roles And Features Wizard.
16. On the Manage menu, click Add Roles And Features.
17. On the Before You Begin page of the Add Roles And Features Wizard, click Next twice.
18. In the Select Destination Server page, click SYD-DC.contoso.com and click Next.
19. On the Select Server Roles page, click the DHCP Server check box as shown in Figure 3-45.

**FIGURE 3-44** Select a server to manage
20. On the Add Roles And Features Wizard dialog box, click Add Features and then click Next three times. Click Install and then click Close.

21. In the Server Manager console on SYD-DC, click the DHCP Server node.

22. Next to the There Are 2 Jobs With New Notifications message, click More.

23. In the All Servers Task Details dialog box, shown in Figure 3-46, click the Complete DHCP Configuration link next to MEL-DC.
24. On the Description page of the DHCP Post-Install Configuration Wizard, click Next.

25. On the Authorization page, verify that the user credentials are set to CONTOSO\don_funk as shown in Figure 3-47, click Commit, and then click Close.
26. In the All Servers Task Details dialog box, click the Complete DHCP Configuration link next to SYD-DC.

27. On the Description page of the DHCP Post-Install Configuration Wizard, click Next.

28. On the Authorization page, verify that CONTOSO\don_funk is listed as the credentialed user, click Commit, and then click Close.

29. Verify that the Stage is listed as complete on the All Servers Task Details And Notifications dialog box as shown in Figure 3-48 and then click the close icon on the title bar.

![All Servers Task Details](image)

**FIGURE 3-48** Verify the completion of tasks

**Exercise 10: Create a DHCP superscope**

In this exercise, you create a DHCP superscope. To complete this exercise, perform the following steps:

1. Ensure that you are signed on to SYD-DC with the contoso\don_funk user account.
2. On the Tools menu of the Server Manager console, click DHCP.
3. In the DHCP console, expand Syd-dc.contoso.com and click IPv4 as shown in Figure 3-49.
5. On the Welcome To The New Scope Wizard page, click Next.
6. On the Scope Name page, in the Name text box, type **Scope-A** and click Next.
7. On the IP Address Range page, in the Start IP Address text box, enter the following information as shown in Figure 3-50 and click Next three times:
   - **Start IP Address**: 192.168.200.10
   - **End IP Address**: 192.168.200.230
   - **Length**: 24
   - **Subnet Mask**: 255.255.255.0
On the Configure DHCP Options page, verify that Yes, I Want To Configure These Options Now is selected and click Next.

9. On the Router (Default Gateway) page, type 192.168.200.1 as shown in Figure 3-51 and click Add. Click Next three times.

10. On the Activate Scope page, click No, I Will Activate This Scope Later, click Next, and then click Finish.

11. In the DHCP console, click the IPv4 node, and on the Action menu click New Scope.
12. On the Welcome To The New Scope Wizard page, click Next.

13. On the Scope Name page, in the Name text box, type **Scope-B** and click Next.

14. On the IP Address Range page, in the Start IP Address text box, enter the following information and click Next three times:
   - Start IP Address: **192.168.201.10**
   - End IP Address: **192.168.201.230**
   - Length: 24
   - Subnet Mask: **255.255.255.0**

15. On the Configure DHCP Options page, verify that the Yes, I Want To Configure These Options Now option is selected and click Next.

16. On the Router (Default Gateway) page, type **192.168.201.1** as shown in Figure 3-52 and click Add. Click Next three times.

17. On the Activate Scope page, click No, I Will Activate This Scope Later, click Next, and click Finish.

18. In the DHCP console, click the IPv4 node. On the Action menu, click New Superscope.


20. On the Superscope Name page, type the name **SYD-Superscope** and click Next.

21. On the Select Scopes page, hold the Ctrl key and click [192.168.200.0] Scope-A and [192.168.201.0] Scope-B as shown in Figure 3-53. Click Next.

23. In the DHCP console, click Superscope SYD-Superscope as shown in Figure 3-54, and on the Action menu, click Activate.

Exercise 11: Create a split scope

In this exercise, you configure a split scope that is hosted on SYD-DC and MEL-DC. To complete this exercise, perform the following steps:

1. In the DHCP console on SYD-DC, click the DHCP node, and on the Action menu click Add Server.

2. In the Add Server dialog box, click This Authorized DHCP Server and click Mel-dc.contoso.com as shown in Figure 3-55. Click OK.
3. In the DHCP console, expand Mel-dc.contoso.com and click the IPv4 node.


5. On the Welcome To The New Scope Wizard page, click Next.

6. On the Scope Name page, type **SplitScope-A** and click Next.

7. On the IP Address Range page, enter the following as shown in Figure 3-56 and click Next three times:
   - Start IP Address: **192.168.210.100**
   - End IP Address: **192.168.210.180**
   - Length: **24**
   - Subnet Mask: **255.255.255.0**
8. On the Configure DHCP Options page, verify that the Yes, I Want To Configure These Options Now option is selected and click Next.

9. On the Router (Default Gateway) page, type **192.168.210.1** as shown in Figure 3-57 and click Add. Click Next three times.

   ![FIGURE 3-57 The default gateway address](image)

10. On the Activate Scope page, select the Yes, I Want To Activate This Scope Now option, click Next, and then click Finish.

11. In the DHCP console, click the IPv4 node under Syd-dc.contoso.com.


14. On the Scope Name page, type **SplitScope-B** and click Next.

15. On the IP Address Range page, enter the following and click Next three times:
   - Start IP Address: **192.168.210.181**
   - End IP Address: **192.168.210.200**
   - Length: **24**
   - Subnet Mask: **255.255.255.0**

16. On the Configure DHCP Options page, verify that the Yes, I Want To Configure These Options Now option is selected and then click Next.


18. On the Activate Scope page, select the Yes, I Want To Activate This Scope Now option, click Next, and then click Finish.

19. Verify that the DHCP console appears as shown in Figure 3-58.
Exercise 12: Configure DHCP Name Protection

In this exercise, you configure DHCP Name Protection using the graphical user interface (GUI) and using Windows PowerShell. To complete this exercise, perform the following steps:

1. In the DHCP console on SYD-DC, click the IPv4 node under the Syd-dc.contoso.com node.
2. On the Action menu, click Properties.
3. In the IPv4 Properties dialog box, click the DNS tab.
4. On the DNS tab, shown in Figure 3-59, click Configure.
5. On the Name Protection dialog box, check the Enable Name Protection check box as shown in Figure 3-60 and click OK.

6. Click OK to close the IPv4 Properties dialog box.

7. In an elevated Windows PowerShell window, type the following command as shown in Figure 3-61 and press Enter to verify the status of Name Protection on the DHCP server running on MEL-DC:

   `Get-DhcpServerv4DnsSetting -Computer MEL-DC`
8. In a Windows PowerShell window, type the following command and press Enter to enable Name Protection on the DHCP server hosted on mel-dc.contoso.com:

```
Set-DhcpServerv4DnsSetting -Computer MEL-DC -NameProtection $true
```

9. Verify that Name Protection is now enabled on MEL-DC by reissuing the following command as shown in Figure 3-62:

```
Get-DhcpServerv4DnsSetting -Computer MEL-DC
```

**Exercise 13: Create new multicast scopes**

In this exercise, you create a new multicast scope that will be hosted on the DHCP server SYD-DC. To complete this exercise, perform the following steps:

1. In the DHCP console on SYD-DC, click the IPv4 node under Syd-dc.contoso.com.
2. In the Action menu, click New Multicast Scope.
3. On the Welcome To The New Multicast Scope Wizard page, click Next.
4. On the Multicast Scope Name page, enter the name **Multicast-A** and click Next.
5. On the IP Address Range page, configure the following settings as shown in Figure 3-63 and click Next three times:
   - Start IP Address: **230.100.0.10**
   - End IP Address: **230.100.0.230**

   ![New Multicast Scope Wizard](image)

   **FIGURE 3-63** A new multicast range

6. On the Activate Multicast Scope page, shown in Figure 3-64, click Yes, click Next, and click Finish.

   ![New Multicast Scope Wizard](image)

   **FIGURE 3-64** Activate a multicast scope
Exercise 14: Configure DHCP failover

In this exercise, you configure DHCP failover. To complete this exercise, perform the following steps:

1. In the DHCP console on SYD-DC, expand the Syd-dc.contoso.com node and click the IPv4 node.
2. On the Action menu, click Configure Failover.
3. On the Introduction To DHCP Failover page of the Configure Failover Wizard, clear the Select All check box, hold down the Ctrl key and click 192.168.200.0 and 192.168.201.0 as shown in Figure 3-65. Click Next.

4. On the Specify The Partner Server To Use For Failover page, click Add Server.
5. In the Add Server dialog box, select This Authorized DHCP Server and click Mel-dc. contoso.com as shown in Figure 3-66. Click OK and then click Next.
6. On the Create A New Failover Relationship page, click the Mode drop-down menu and set it to Hot Standby. Enable the State Switchover Interval and set it to 60 Minutes as shown in Figure 3-67. Type the Shared Secret as **Pa$$w0rd**. Click Next, click Finish, and click Close.

7. In the DHCP console, click the IPv4 node under Syd-dc.contoso.com, and on the Action menu, click Properties.
8. On the Failover tab, verify that the settings listed match Figure 3-68 and click Delete.

![Figure 3-68](image)

**FIGURE 3-68** Delete a failover relationship


10. Click OK to close the IPv4 Properties dialog box.

**Exercise 15: Install the IPAM feature**

In this exercise, you join server ADL-DC to the domain and install the IPAM feature. To complete this exercise, perform the following steps:

1. Ensure that SYD-DC and MEL-DC remain powered on.
2. Turn on ADL-DC and sign on as Administrator with the password Pa$$w0rd.
3. Open a Windows PowerShell window by clicking the Windows PowerShell icon on the Desktop taskbar.
4. Type the following command and press Enter to join ADL-DC to the contoso.com domain.
   ```bash
   Netdom join ADL-DC /domain:contoso.com
   ```
5. Restart ADL-DC and sign on as contoso\don_funk.
6. Click on Add Roles And Features on the Manage menu of the Server Manager console.
8. On the Select Destination Server page, ensure that ADL-DC.contoso.com is selected and click Next twice.
9. On the Select Features page, click IP Address Management (IPAM) Server as shown in Figure 3-69.

![Add Roles and Features Wizard](image)

**FIGURE 3-69** Add the IPAM feature

10. On the Add Roles And Features Wizard dialog box, click Add Features, click Next, and then click Install. When the installation completes, click Close.

**Exercise 16: Configure IPAM GPOs and server discovery**

In this exercise, you configure IPAM-related GPOs. To complete this exercise, perform the following steps:

1. While signed on to ADL-DC, click the IPAM node in the Server Manager console.
2. On the IPAM Server Tasks section, click Provision The IPAM Server.
4. On the Select Provisioning Method page, click Group Policy Based, and in the GPO Name Prefix box type **IPAM** as shown in Figure 3-70. Click Next.
5. On the Summary page, click Apply and then click Close.

6. On the IPAM Server Tasks section of the Server Manager console, click Configure Server Discovery.

7. In the Configure Server Discovery dialog box, click Add as shown in Figure 3-71 and click OK.
8. On the IPAM Server Tasks section of the Server Manager console, click Start Server Discovery.

9. Wait 15 minutes for server discovery to complete before starting Exercise 17.

**Exercise 17: Configure servers to be managed by IPAM**

In this exercise, you configure servers so that they can be managed centrally by IPAM. To complete this exercise, perform the following steps:

1. On the IPAM Server Tasks section, click Select Or Add Servers To Manage And Verify IPAM Access.

2. Both SYD-DC and MEL-DC should be present as shown in Figure 3-72.
3. Right-click the Windows PowerShell icon on the taskbar and click Run As Administrator.

4. On the User Account Control dialog box, click Yes.

5. In the Windows PowerShell window, type the following command and press Enter:

   ```powershell
   Invoke-IpamGpoProvisioning -Domain contoso.com -GpoPrefixName IPAM -IpamServerFqdn ADL-DC.contoso.com -DelegatedGpoUser "contoso\don_funk"
   ```

6. When prompted, type Y for Yes, and press Enter.

7. Switch to SYD-DC and ensure that you are signed on as contoso\don_funk.

8. Open an elevated Windows PowerShell prompt, type the following command, and press Enter:

   ```powershell
   gpupdate /force
   ```


10. Expand the Contoso.com domain and click the Computers container.


12. On the New Object – Group dialog box, enter the following information as shown in Figure 3-73 and click OK:

   - Group Name: **IPAM_Managed_Servers**
   - Group Scope: **Universal**
   - Group Type: **Security**
13. Right-click the IPAM_Managed_Servers group and click Properties.


15. On the Select Users, Contacts, Computers, Service Accounts, Or Other Objects dialog box, click Object Types.

16. On the Object Types dialog box, select the Computers check box and click OK.

17. In the Select Users, Contacts, Computers, Service Accounts, Or Other Objects dialog box, type SYD-DC; MEL-DC, click Check Names, and click OK.

18. Verify that both MEL-DC and SYD-DC are listed as members of the group as shown in Figure 3-74 and click OK.
20. In the Group Policy Management Console, expand Forest: Contoso.com, Domains, Contoso.com, and click IPAM_DNS.
21. On the Group Policy Management Console pop-up box, click OK.
23. In the Select User, Computer, Or Group dialog box, type IPAM_Managed_Servers and click OK.
24. Verify that the Group Policy Management Console matches Figure 3-75.

![Figure 3-75 Group policy filtering](image)

25. Click the IPAM_DHCP policy and click OK to dismiss the Group Policy Management Console.
27. In the Select User, Computer, Or Group dialog box, type IPAM_Managed_Servers and click OK.
28. Click the IPAM_DC_NPS policy and click OK to dismiss the Group Policy Management Console.
30. In the Select User, Computer, Or Group dialog box, type IPAM_Managed_Servers and click OK.
31. Restart SYD-DC and MEL-DC to refresh the group membership of these computers.
32. Sign on to each computer as contoso\don_funk, open an elevated Windows PowerShell prompt and type the following command:

   Gpupdate /force

33. After you have updated the Group Policy, run the following command on SYD-DC and MEL-DC to verify that the IPAM-related Group Policy Objects apply to the computer as shown in Figure 3-76:

   Gpresult /r /scope computer

   ![Figure 3-76](image.png) Verify the Group Policy application

34. On ADL-DC, open the Server Manager console, click the IPAM node, and when Overview is selected, click Select Or Add Servers To Manage And Verify IPAM Access.

35. When IPv4 is selected, right-click SYD-DC, and click Refresh Server Access Status.


37. Wait until the task completes and then click the Refresh icon on the taskbar and verify that both servers are listed as Unblocked, as shown in Figure 3-77.
Exercise 18: Manage servers using IPAM

In this exercise, you configure SYD-DC and MEL-DC to be managed by IPAM. To complete this exercise, perform the following steps:

1. On ADL-DC, in the Server Manager console, with the Server Inventory section of the IPAM area selected, right-click Mel-dc, and click Edit Server.

2. In the Add Or Edit Server dialog box, set the Manageability Status to Managed as shown in Figure 3-78 and click OK.
3. Right-click SYD-DC, and click Edit Server.
4. In the Add Or Edit Server dialog box, set the Manageability Status to Managed, and click OK.
5. Verify that both servers now have the status of Managed and Unblocked as shown in Figure 3-79.

![Figure 3-78 Configure the server manageability](image)

**FIGURE 3-78** Configure the server manageability

![Figure 3-79 Verify successful configuration](image)

**FIGURE 3-79** Verify successful configuration
Exercise 19: Use IPAM to create a DHCP scope

In this exercise, you use IPAM to create a DHCP scope on MEL-DC. To complete this exercise, perform the following steps:

1. While signed on to ADL-DC as contoso\don_funk, click the IPAM node in the Server Manager console, and then click DNS and DHCP under Monitor and Manage.
2. Right-click Mel-dc.contoso.com, and click Create DHCP Scope.
3. In the Create DHCP Scope dialog box, enter the following information as shown in Figure 3-80 and click OK:
   - Scope Name: IPAM_Scope_A
   - Start IP Address: 192.168.250.10
   - End IP Address: 192.168.250.230
   - Subnet Mask: 255.255.255.0

![Create DHCP Scope dialog box]

FIGURE 3-80 Create a DHCP scope
Exercise 20: Use IPAM to manage IP addresses

In this exercise, you use IPAM to manage IP addresses, including creating address blocks, creating reservations, and managing DNS records. To complete this exercise, perform the following steps:

1. While signed on to ADL-DC as contoso\don_funk, click the IPAM node in the Server Manager console, and then click IP Address Blocks under IP Address Space.
2. Click Tasks, and click Add IP Address Block.
3. In the Add Or Edit IPv4 Address Block dialog box, enter the following information as shown in Figure 3-81 and click OK:
   - Network ID: **172.16.10.0**
   - Prefix Length: **24**
   - Description: **Perth Office**

![Add or Edit IPv4 Address Block](image)

**FIGURE 3-81** Add an IPv4 address block

4. Click the IP Address Inventory node. In the Tasks menu, click Add IP Address.
5. In the Add IPv4 Address dialog box shown in Figure 3-82, enter the following information and click OK:
   - IP Address: **172.16.10.20**
   - MAC Address: **AA-BB-CC-DD-EE-00**
   - Device Type: **Host**
   - Device Name: **PER-DC**
   - Forward Lookup Zone: **Contoso.com**
   - Forward Lookup Primary Server: **SYD-DC.contoso.com**
6. Right-click the PER-DC IP Address Inventory Record, and click Create DNS Host Record.

7. Click the Windows PowerShell icon on the taskbar.

8. In the Windows PowerShell window, type the following command to verify that the DNS record has been created as shown in Figure 3-83:

```
Resolve-dnsname per-dc.contosoc.com
```

![FIGURE 3-83 Verify the DNS record](image.png)
Suggested practice exercises

The following additional practice exercises are designed to give you more opportunities to practice what you’ve learned and to help you successfully master the lessons presented in this chapter.

- **Exercise 1**  Use IPAM to create a DHCP scope on SYD-DC for the 172.16.10.0 /24 IP Address Range.
- **Exercise 2**  Reset the DNS socket pool on SYD-DC to its original value.
- **Exercise 3**  Create a new DNS zone named Margiestravel.com and configure it to use DNSSEC.
Answers

This section contains the answers to the lesson review questions in this chapter.

Lesson 1

1. **Correct answer:** C

   A. **Incorrect.** This method cannot be used with a DHCP server hosted on the Windows Server 2008 R2 operating system. Hot standby mode has the primary DHCP server respond to DHCP clients except in the case when the primary server is unavailable, at which point the hot standby server begins leasing addresses.

   B. **Incorrect.** This method cannot be used with a DHCP server hosted on the Windows Server 2008 R2 operating system. Load sharing has each partner DHCP server lease addresses from the scope to DHCP clients. In the event that one DHCP server fails, the other DHCP server utilizes the whole scope after the maximum client lead time period has elapsed.

   C. **Correct.** In a split scope, part of the scope is hosted on one DHCP server, and a smaller part is hosted on a second DHCP server. Traditionally the split between the first and second DHCP servers is 80/20. Use this option when one or both DHCP servers are not running the Windows Server 2012 operating system.

   D. **Incorrect.** Superscopes enable you to combine existing scopes for administrative purposes. They are often implemented when there are multiple logical subnets used on the same physical network. Superscopes do not provide high availability.

2. **Correct answer:** C

   A. **Incorrect.** Load sharing has each partner DHCP server lease addresses from the scope to DHCP clients. In the event that one DHCP server fails, the other DHCP server utilizes the whole scope after the maximum client lead time period has elapsed. This does not meet the requirement that the second server not lease addresses unless the first is unavailable.

   B. **Incorrect.** In a split scope, part of the scope is hosted on one DHCP server, and a smaller part is hosted on a second DHCP server. Traditionally the split between the first and second DHCP servers is 80/20. Use this option when one or both DHCP servers are not running the Windows Server 2012 operating system. This does not meet the requirement that the second server be able to lease addresses from the entire scope if necessary.

   C. **Correct.** Hot standby mode has the primary DHCP server respond to DHCP clients except in the case when the primary server is unavailable, at which point the hot standby server begins leasing addresses.
D. Incorrect. Superscopes enable you to combine existing scopes for administrative purposes. They are often implemented when there are multiple logical subnets used on the same physical network. Superscopes do not provide high availability.

3. Correct answer: A

A. Correct. Superscopes enable you to combine existing scopes for administrative purposes. They are often implemented when there are multiple logical subnets used on the same physical network. Superscopes do not provide high availability.

B. Incorrect. Split scopes are high-availability solutions. In a split scope, part of the scope is hosted on one DHCP server, and a smaller part is hosted on a second DHCP server. Traditionally, the split between the first and second DHCP servers is 80/20. Use this option when one or both DHCP servers are not running the Windows Server 2012 operating system.

C. Incorrect. Load sharing mode is a high-availability solution. Load sharing has each partner DHCP server lease addresses from the scope to DHCP clients. In the event that one DHCP server fails, the other DHCP server utilizes the whole scope after the maximum client lead time period has elapsed.

D. Incorrect. Hot standby mode is a high-availability solution. Hot standby mode has the primary DHCP server respond to DHCP clients except in the case when the primary is unavailable at which point the hot standby server begins leasing addresses.

4. Correct answer: B

A. Incorrect. In a split scope, part of the scope is hosted on one DHCP server, and a smaller part is hosted on a second DHCP server. Traditionally the split between the first and second DHCP servers is 80/20. Use this option when one or both DHCP servers are not running the Windows Server 2012 operating system. This solution does not distribute IP addresses in a load-balanced manner.

B. Correct. Load sharing has each partner DHCP server lease addresses from the scope to DHCP clients. In the event that one DHCP server fails, the other DHCP server utilizes the whole scope after the maximum client lead time period has elapsed.

C. Incorrect. Hot standby mode has the primary DHCP server respond to DHCP clients except in the case when the primary server is unavailable, at which point the hot standby server begins leasing addresses. This solution does not distribute IP addresses in a load-balanced manner.

D. Incorrect. Superscopes enable you to combine existing scopes for administrative purposes. They are often implemented when there are multiple logical subnets used on the same physical network. Superscopes do not provide high availability.
Lesson 2

1. **Correct answer:** B
   
   A. **Incorrect.** Members of the IPAM Users group are unable to view IP address tracking information. This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

   B. **Correct.** This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

   C. **Incorrect.** Members of the IPAM MSM Administrators group are unable to view IP address tracking information. This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

   D. **Incorrect.** Members of the IPAM ASM Administrators group are unable to view IP address tracking information. This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

2. **Correct answer:** C

   A. **Incorrect.** Only members of the IPAM ASM Administrators group and the IPAM Administrators group are able to manage the IP address space on an IPAM server.

   B. **Incorrect.** Only members of the IPAM ASM Administrators group and the IPAM Administrators group are able to manage the IP address space on an IPAM server.

   C. **Correct.** Members of the IPAM ASM Administrators group are able to manage the IP address space on an IPAM server.

   D. **Incorrect.** Only members of the IPAM ASM Administrators group and the IPAM Administrators group are able to manage the IP address space on an IPAM server.

3. **Correct answer:** B

   A. **Incorrect.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

   B. **Correct.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

   C. **Incorrect.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

   D. **Incorrect.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

4. **Correct answers:** A and C

   A. **Correct.** These servers need to have the appropriate IPAM-related GPOs apply to them before their status can change to unblocked. This involves creating the GPOs.
using the Invoke-IpamGPOP Provisioning cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.

B. Incorrect. These servers need to have the appropriate IPAM-related GPOs apply to them before their status can change to unblocked. This involves creating the GPOs using the Invoke-IpamGPOP Provisioning cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.

C. Correct. These servers need to have the appropriate IPAM-related GPOs apply to them before their status can change to unblocked. This involves creating the GPOs using the Invoke-IpamGPOP Provisioning cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.

D. Incorrect. Restarting the IPAM server does not alter the blocked status of the servers that you want to manage. These servers need to have the appropriate IPAM-related GPOs apply to them. This involves creating the GPOs using the Invoke-IpamGPOP Provisioning cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.

Lesson 3

1. Correct answer: B

A. Incorrect. Members of the IPAM Users group are unable to view IP address tracking information. This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

B. Correct. This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

C. Incorrect. Members of the IPAM ASM Administrators group are unable to view IP address tracking information. This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

D. Incorrect. Members of the IPAM ASM Administrators group are unable to view IP address tracking information. This information can only be viewed by users that are members of the IPAM IP Audit Administrators and IPAM Administrators local groups.

2. Correct answer: C

A. Incorrect. Only members of the IPAM ASM Administrators group and the IPAM Administrators group are able to manage the IP Address space on an IPAM server.

B. Incorrect. Only members of the IPAM ASM Administrators group and the IPAM Administrators group are able to manage the IP Address space on an IPAM server.

C. Correct. Members of the IPAM ASM Administrators group are able to manage the IP address space on an IPAM server.
D. **Incorrect.** Only members of the IPAM ASM Administrators group and the IPAM Administrators group are able to manage the IP address space on an IPAM server.

3. **Correct answer:** B

A. **Incorrect.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

B. **Correct.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

C. **Incorrect.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

D. **Incorrect.** You track by client ID when you know a computer’s MAC address to determine which IP addresses the computer was assigned.

4. **Correct answers:** A and C

A. **Correct.** These servers need to have the appropriate IPAM-related GPOs applied to them before their status can change to unblocked. This involves creating the GPOs using the `Invoke-IpamGPOProvisioning` cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.

B. **Incorrect.** These servers need to have the appropriate IPAM-related GPOs applied to them before their status can change to unblocked. This involves creating the GPOs using the `Invoke-IpamGPOProvisioning` cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.

C. **Correct.** These servers need to have the appropriate IPAM-related GPOs applied to them before their status can change to unblocked. This involves creating the GPOs using the `Invoke-IpamGPOProvisioning` cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.

D. **Incorrect.** Restarting the IPAM server does not alter the blocked status of the servers that you want to manage. These servers need to have the appropriate IPAM-related GPOs applied to them. This involves creating the GPOs using the `Invoke-IpamGPOProvisioning` cmdlet and then ensuring that they apply to the servers that host the services that IPAM will manage.
Index

A

Access Denied Assistance  577–578
Active Directory And Trusts console  13
Active Directory Application Mode (ADAM)  663
Active Directory Certificate Services  205–300
    installing and configuring  205–218
Active Directory detached clusters  454–455
Active Directory Domains And Trusts console  4, 10
Active Directory Federation Services. See AD FS
Active Directory Lightweight Directory Services (AD LDS)  663
Active Directory Recycle Bin  6
    forest functional levels and  8
Active Directory Rights Management Services. See AD RMS (Active Directory Rights Management Services)
Active Directory Sites And Services console  92
Active Directory Users And Computers console  4
    selective authentication and  17
    UPN suffixes and  10
ADAM (Active Directory Application Mode)  663
AD CS Configuration Wizard  234
address block  148
address range  135, 139, 143, 148, 149
address space  119, 133, 136, 148, 150, 152
address tracking  150–153
Add Roles And Features Wizard dialog box  97, 243
AD FS  657–665
    attribute store  659
    claim  658
    claim rules  658
    claims provider  659
    claims provider trust  661
    claims rules  664–665
    configuring certificate relationship  662–663
    configuring Web Application Proxy  666–667
    multi-factor authentication  671
    relying party  660
    relying party trust  660
    Workplace Join  669–670
AD LDS (Active Directory Lightweight Directory Services)  663
administrative role separation
    certificate permissions and  215
    configuring  264–268
adprep.exe  9
AD RMS (Active Directory Rights Management Services)  580–591
Administrators  586
    apply templates automatically  590–591
    backing up  591
    certificates and licenses  582–583
    configuration database  591
    Exclusion policies  589–590
    installing and configuring  580–581
    Super Users  586–587
    templates  583–585
    Trusted publishing domains (TPDs)  588–589
    Trusted user domains (TUDs)  587–588
advanced DHCP solution implementation  134–135
    DHCP failover  139–140
    DNS registration  137–138
    Multicast scopes  135–136
    Name Protection  138–139
    Split scopes  136–137
    Superscopes  134–135
Advanced DNS options  126–129
    DNS cache locking  126
    DNS recursion  127
    DNS socket pool  126
    Netmask ordering  128
Advanced Encryption Services (AES). See AES
AES (Advanced Encryption Services)  6
affinity 463–464
AIA (Authority Information Access) distribution points 211
Allow Private Key To Be Exported (certificate template settings) 221
application partitions 73
Archive subject’s encryption private key 228
Archive Subject’s Encryption Private Key (certificate template settings) 221
@ symbol, using UPN suffixes and \text{10}
attribute store, AD FS 659
authentication
forest-wide 16
intraforest 4
policy silos 7
selective 16
Authentication Type for CES page (AD CS Configuration Wizard) 239
autoenrollment, certificate management 225–226
Autoenroll permission (certificates) 226
Automatic certificate renewal 224–225

B
backing up AD RMS. See AD RMS (Active Directory Rights Management Services)
backup, CAs (certificate authorities) 216–218
bidirectional trust 14
Branch Cache
Client configuration
Hosted Cache Server (Uses HTTPS) 384
Peer Discovery (Uses WSD) 384
BranchCache 61, 380–384
BranchCache for Network File Server 381–382
Client configuration 382–384
Configure Hosted Cache Servers 383
Content Retrieval (Uses HTTP) 383
Set BranchCache Hosted Cache Mode 383
Enable Automatic Hosted Cache Discovery By Service Connection Point 383
Hosted Cache Server Configuration 380–381

C
CA Compromise issue, revoking a certificate, 231
CA for CES page (AD CS Configuration Wizard) 239
CAs (certificate authorities)
backup and recovery 216–218
CA Type page (AD CS Configuration Wizard) 236
CDPs (CRL Distribution Points) 212–213
central access policies, (DAC) 575–576
central access rules, (DAC) 573
Certificate Enrollment Policy Web Service 207–208
Certificate Enrollment Web Service 208
Certificate Hold issue, revoking a certificate 231
Certificate Revocation List (CRL) Distribution Points 212
certificates
management
autoenrollment 225–226
key archiving and recovery 227–229
renewal 224–225
recovery, performing 292–296
revocation 223, 288–292
templates 221, 224, 287
Certificate Services 205–300
CA backup and recovery 216–218
CDPs (CRL Distribution Points) 212–213
certificate authority 206–208
installing and configuring 205–218
administrative role separation 215–216
online responders 214–215
management 224
autoenrollment 227
key archiving and recovery 227
renewal 224–225
Certificate Services Client-Auto-Enrollment group policy 226
Certification authority 207
Certification Authority Backup Wizard 216
Certification Authority Web Enrollment 207
Certutil-backup c:\backup command 217
Change of Affiliation issue, revoking a certificate 231
checkpoints 512
child domains 3
claim rules, AD FS 658
claims, AD FS 658
claims-based authentication 658
claims provider, AD FS 659
claims provider trust, AD FS 661
claims rules, AD FS 664–665
Cluster-Aware Updating (CAU) 449–451
Cluster networks 448–449
Cluster quorum modes 443–445
  Node and disk majority 443
  Node and file share majority 443
  Node majority 443
  No Majority: Disk Only 443
Cluster Shared Volumes 446–447, 506–510
Cluster Shared Volumes (CSVs) 506
Cluster storage and cluster shared volumes 445–446
Compatibility (certificate template settings) 221
Configure file access auditing
  Configure file access auditing 414–417
Configuring advanced file services 373–387
Configuring and managing backups 301–318
Configuring and managing failover clustering 441–455
Configuring and optimizing storage 388–397
Confirmation page (AD CS Configuration Wizard) 238
conflict resolutions 75
Constrained delegation 5
Continuously available file shares 454
Credential page (AD CS Configuration Wizard) 234
Credential Security Support Provider (CredSSP) 510
CRL (Certificate Revocation List) 212
  CRL Distribution Points (CDPs) and, 212–213
Cryptography for CA page (AD CS Configuration Wizard) 237

D

DAC (Dynamic Access Control) 567–579
  central access policies 575–577
  central access rules 573–574
  configuring
    Group Policy support 569
    resource properties 571–573
    user and device claims 569–570
    staging 576–577
Data Protection Manager 316–317
Delegated administration 129–130
Delta CRL list 212
device claims (DAC), configuring 570
DFS (Distributed File System) 61, 85
  replicating 5
DHCP failover 139–143
  Hot standby mode 139
  Load sharing mode 140
Distributed File System (DFS) 61, 85
  replicating 5
DNS cache locking 126–127, 132
DNS (Domain Name System)
  SRV record registration, managing 68
  zones, storing 5
DNS event logs 122–123
DNSKEY 121
DNS registration 134, 137, 141
DNSSEC 119–122, 126, 131–132
DNS socket pool 120, 126, 132
domain controllers
  functional levels 6
Domain Name System (DNS) See DNS
domain quarantine 21
domains
  configuring 1–11
  controllers, moving 69
  functional levels 4–8
  partitions 73
  trees 3
  trusting 14
  upgrading 9
Domains And Trusts (Active Directory) console 10
Dynamic Access Control. See DAC (Dynamic Access Control)
dynamic witness 527

E

Enroll permission (certificates) 226
Enterprise Admins group 7
enterprise root CA
  deploying and configuring 232–241
enterprise root CAs (certificate authorities) 209–212, 218
enterprise subordinate CA 210, 219
  deploying 241
enterprise subordinate CAs deployment 241–246
Exclusion policies. See AD RMS (Active Directory Rights Management Services)
external trusts 13, 17

F

Failover and preference settings 452–453
Failover clustering 442–443
Features on Demand 396–397
Federation server role 658
File access auditing 385–387
File classification 384–385
File Replication Service (FRS) 85
File screens 374–377
File Server Resource Manager (FSRM) 374
Filtering 463–464
Filtering and affinity 463–464
  Disable The Port Range 464
  Multiple Host 464
fine-grained password policies

Network 464
None 464
Single 464
Single Host 464
fine-grained password policies 6
force quorum resiliency 527
forests
configuring 1–11
functional levels 7
trusts 14, 16
upgrading 9
forest-wide authentication 16
FQDN (full qualified domain name) 3
FRS (File Replication Service) 85
fully qualified domain name (FQDN) 3
functional levels
domain 4–7
forest 7

G

Get-ADTrust cmdlet 21
GlobalNames zones 124–125
group managed service accounts 6

H

hardware security module (HSM) 212
hared Nothing Hyper-V live migration 509
hierarchies, CA 208–209
Hot standby mode (DHCP failover) 139
Hyper-V 6
Hyper-V hosting 518
Hyper-V Replica 518–526
Hyper-V Replica Broker 525–526

I

installation
AD RMS 581–582
Internet Protocol (IP) addresses 60
intraforest authentication 4
IPAM Administrators permissions 152
IPAM ASM Administrators permissions 152
IPAM (IP Address Management) 143–152
Configure IPAM database storage 144–145
Configure server discovery. See also Server discovery
Deploy IPAM 144

Introduction to IPAM 144
IPAM administration 152
Managing the IP address space 148
IPAM IP Audit Administrators 152
IPAM MSM Administrators permissions 152
IPAM Users permissions 152
IP (Internet Protocol) addresses 60
iSCSI initiator 392–394
iSCSI target and initiator 389–392
iSCSI targets 388–390
iSNS server 392–394
iSNS Server Properties dialog box 392, 428–429, 429
issuing CAs (certificate authorities) 208

J

K

KCC (knowledge consistency checker) 74
/kcc switch (repadmin) 84
KDC (key distribution center) 6
_kerberos record 68
Kerberos V5
authentication protocol 13
realm 20
key distribution center (KDC) 6
key recovery agent (KRA) certificate 229–231, 277
configuring 268–273
requesting 273–277
Key Signing Key (KSK) 121
knowledge consistency checker (KCC) 74

L

LastLogonTimestamp attribute 5
_ldap SRV record 68
Load sharing mode (DHCP failover) 140

M

Managing cluster hosts 461–462
Drainstop 461
Resume 462
Start 461
Stop 461
Suspend 462
Migrating and upgrading clusters 451–452
Move Server dialog box 70
multicast address 135, 141
Multicast scopes 135, 136, 141
multidomain environments 1–8
multi-factor authentication, AD FS 671–672
multiforest environments 1, 8
    multidomain environments and 2
multi-master replication 73
Multisite clustering, site-level fault tolerance 526–527

N
Name Protection 134, 138, 139, 142
name suffix routing 22
netdom.exe 13, 20
Netlogon service on domain controllers 69
Netmask ordering 128, 132, 133
Network Device Enrollment Service 207–209
Network Load Balancing (NLB) 457–458
Network Load Balancing prerequisites 458–459
New-ADReplicationSite Windows PowerShell cmdlet 62
New NLB PowerShell cmdlets 465–466
New Technology File System (NTFS) 568
Next Secure (NSEC/NSEC3) record 121
NLB cluster operation modes 459–460
    IGMP multicast 460
    Multicast mode 460
    Unicast mode 459
NLB clusters, upgrading 465

O
OCSP (Online Certificate Status Protocol) Response
    Signing Certificate template 214
offline root CA 211
Online Responder role service 207
    certificate revocation 214–215
        configuring 257–264

P
partitions, replicating 72
password policies 6
Password Replication Policy tab 77
passwords
    replacated ADL-DC, viewing 107
    RODC replication, configuring 77
perimeter networks, standalone subordinate CAs 211
policy silos 7
Port rules 462–463
practice exercises
    acquiring certificates for each server 691–694
    Add a cluster node 486–488
    apply RMS templates using file classification 649–651
    Backup data to Windows Azure Backup 362–367
    Begin creating a forest trust relationship 37–40
    Boot into Safe Mode 348–350
    Change the quorum configuration 488–489
    Cluster-Aware Updating 496–500
    Complete the creation of the forest trust relationship between contoso.com and margiestravel.com 40–42
    configure Access Denied Assistance 627–629
    Configure a certificate template for autoenrollment and key recovery 279–282
    Configure a certificate template to support private key archival and recovery and reenroll all certificate holders 287–288
    Configure a CRL distribution point 253–257
    Configure additional UPN suffixes 50
    Configure ADL-DC as an RODC 102–105
    Configure administrative role separation 264–268
    Configure a highly available file share 491–493
    Configure a key recovery agent certificate template 268–273
    Configure and view the DNS event log 165–166
    Configure an Online Responder 257–264
    configure application exclusions 648
    Configure a shortcut trust 50–53
    Configure a standalone CA 250–253
    Configure a standalone computer for use with Windows Azure Backup 354–358
    Configure BranchCache policies 431–435
    Configure CBR-DC for local backup 330–334
    Configure DHCP failover 184–186
    Configure DHCP Name Protection 180
    Configure DNSSEC 156–158
    Configure failover settings, failback settings, and move node 493–495
    Configure file classification 410–411
    Configure Group Policy to support autoenrollment, credential roaming, and automatic renewal 282–286
    Configure Hyper-V to support live migration 552–553
    Configure identical virtual switches on MEL-HV-1 and MEL-HV-2 536–538
Configure IPAM GPOs and server discovery  187–189
Configure key recovery  277–278
Configure MEL-DC  155–156
Configure MEL-DC as an additional domain controller  96–100
Configure name suffix routing  43–45
Configure port rules and affinity  473–475
Configure quota templates and quotas  402–407
configure resource properties for DAC  607–608
Configure RODC replication  105–107
Configure selective authentication  45–49
configure staging  629–631
configure template distribution  647–648
Configure TEST-ONE for replication  547–550
Configure the name resolution policy  158–160
configure user and device claims for DAC  602–607
Configure Windows Azure Backup  358–362
configuring a claims provider trust  702–703
configuring CA trust in each forest  689–691
configuring claim rules  705–714
configuring DNS forwarding  675–677
configuring relying party trust  699–701
Connect to an iSCSI target  421–423
create a central access policy  624–626
Create a child domain with a contiguous namespace  27–30
Create a copy of a running virtual machine  558–559
Create Active Directory sites  89–90
Create Active Directory subnets  91–92
Create a DHCP superscope  173–177
create AD RMS templates  642–646
create a file classification rule  611–618
Create and assign an iSCSI target  417–421
Create and manage a GlobalNames zone  163–165
Create a new storage pool and thin provisioned virtual disk  423–426
Create a split scope  177–180
Create a three-node NLB cluster  470–473
Create a two-node failover cluster  485–486
create central access rules  621–624
Create file groups, file screen templates, apply file screens, and apply file screen exceptions  407–410
Create new forest  33
Create new multicast scopes  182–183
Create shared storage for failover clustering  477–478
Create site links  93–94
create the AD RMS Super Users group  641–642
Create two virtual machines on MEL-HV-1  544–547
create users and groups for DAC  598–602
Deploy and configure an enterprise root CA  232–241
Deploy an enterprise subordinate CA  241–246
Deploy BranchCache on Windows Server 2012 R2  435–437
Deploy FSRM  401–402
deploying AD CS in each forest  678–680
deploying AD FS in each forest  694–699
Enable reverse replication  559–561
enabling Group Policy support for DAC  595–598
Increase the size of the DNS socket pool  161
Install and activate the DHCP role  168–173
Install and configure a highly available file server  489–491
install and configure the AD RMS server role  635–641
Install a standalone subordinate CA  246–250
Install failover cluster features  483–485
Install the Hyper-V role on MEL-HV-1 and MEL-HV-2  531–535
Install the IPAM feature  186–187
Install the iSNS server and register the initiator  426–429
Install Windows Server Backup  327–330
Manage servers using IPAM  194–195
Modify Boot Configuration Data store  350–354
Modify DNS Cache Locking  161–163
Modify site link cost and replication schedule  94–95
Monitor replication with repadmin  110–112
Install the Network Load Balancing feature on ADL-DC, CBR-DC, and MEL-DC  469–470
onnect potential cluster nodes to shared storage  479–483
Perform a backup over the network  336–338
Perform a backup to a local volume  334–335
Perform a full volume recovery using Windows Server Backup  341–345
Perform an unplanned failover  561
Perform a virtual machine export  558
Perform certificate recovery  292–296
Perform certificate revocation  288–291
Perform full server recovery over the network  345–348
Perform live migration of TEST-TWO  553–556
Perform storage migration  556–557
Prepare ADL-DC, MEL-DC, and CBR-DC for exercises  468–469
Prepare a domain controller to host a child domain with a contiguous namespace  25
Prepare a domain controller to host a new forest 32–33
Prepare domain controller to host the wingtiptoys.com tree in the contoso.com forest 30
Prepare for Windows Recovery Environment 344
prepare infrastructure for an AD RMS deployment 632–635
Prepare MEL-DC and ADL-DC 400–401
Prepare MEL-DC and CBR-DC for exercises 326–327
prepare separate forests 673–675
Prepare servers for live migration 538–541
Prepare servers for replication 541–544
Prepare to configure a forest trust relationship 34–37
preparing claim data 703–705
preparing MEL-DC and ADL-DC 594–596
preparing MEL-DC for certificate publication 684–688
preparing SYD-DC for certificate publication 680–684
preparing the server for file classification for DAC 609
Promote domain controller for new tree in contoso.com forest 31–32
Remove an NLB cluster 475–476
Remove feature files 429–431
Remove the RODC and reset accounts 113–114
Request a key recovery agent certificate 273–276
Restore data from Windows Azure Backup 367–369
run and verify the file classification 619
Simulate unplanned failure 495–496
Use IPAM to create a DHCP scope 196
Use IPAM to manage IP addresses 197–198
Use Vssadmin 338–340
Verify netmask ordering and disable recursion 167
Verify site placement and trigger replication 101
Verify the classification 413–414
View account passwords replicated to ADL-DC 107–110
View replication health and perform planned failover of TEST-ONE to MEL-HV-2 550–552
preferred owner 452–453
Private Key 217
Private Key page (AD CS Configuration Wizard) 237
private keys 287
Publish Certificate In Active Directory (certificate template settings) 221

Hard Quota 377
Soft Quota 378

R

RDS (Remote Desktop Services) 6, 17
read only domain controllers (RODC) 61, 76
replication, configuring 105
realm trusts 13, 20
Recovering servers 318–324
BCD (Boot Configuration Data store) 324
BCDEdit 324
Restore from backups 318–319
Restore from Windows Azure Backup 320–321
Restore to an alternative location 320
Safe mode, data recovery 322–323
Windows Recovery Environment 321–322
recovery, certificate management 216–218
Recycle Bin (Active Directory) 6
forest functional levels and 8
relative identifiers (RIDs) 2
relying party server, AD FS 660
relying party trust, AD FS 660
RemoteApp 6
Remote Desktop Services. See RDS
renewal, certificate management 224–225
Renewal Period (certificate template settings) 221
Repadmin tool 83–85
Replicate Now dialog box 101
/replswitch (repadmin) 85
replication 59–118, 72–88
monitoring and managing 81
multi-master 73
Resource Record Signature (RRSIG) record 120
/replsignobj switch (repadmin) 85
revocation, certificate management, 223–225
Revoked Certificates Properties, 257
Revoked Certificates Properties dialog box 223
RIDs (relative identifiers) 2
/rodcpwdrepl option (repadmin) 85
RODC (read only domain controllers) 61, 76
replication, configuring 105
Role specifc backups 312–313
root CAs (certificate authority) 208
tree enterprise root CA 232–241
offline root CAs 211
root domain names 3
Rsers And Computers (Active Directory) console
selective authentication, configuring 17

Q

/queue switch (repadmin) 85
Quotas 377–379
Safe mode, data recovery

S
Safe mode, data recovery 322–323
Safe mode 323
Safe mode with command prompt 323
Safe mode with networking 323
schemas
multiforest environments and 8
partitions 73
Security (certificate template settings) 221
selective authentication 5
configuring 16
Select Role Services to Configure page (AD CS Configuration Wizard) 234
Server discovery 145–148
Server for NFS 379–380
Server for NFS Data Store 379
SetADDomainMode Windows PowerShell cmdlet 4
Set-ADForestMode Windows PowerShell cmdlet 7
Setup Type page (AD CS Configuration Wizard) 236
Shared virtual hard disks 447–448
shortcut trusts 13, 18
/showutdvec switch (repadmin) 85
SID filtering 21
silos (policy) 7
site-level fault tolerance 518–529
dynamic witness 527
Force quorum resiliency 527
Hyper-V Replica 518–526
planned failover 523–524
unplanned failover 524–525
Hyper-V Replica Broker 525–526
multisite clustering 526–527
tie breaker for 50% node split 527
virtual machine network health detection 528
site links 64
bridges 66
sites 59–118
configuring 60–68
Split scopes 136, 137, 141
SRV records registration 68
staging (DAC) 576–577
standalone root CAs 210–211
configuring 250
subordinates 246
Storage tiers 398–399
subnets

counting 60–68
Superscopes 134, 135, 141
Superseded reason, revoking a certificate (certificate template settings) 231
Superseded Templates 221
System Center 2012 R2 Configuration Manager, Exchange Server 61
SYSVOL replication, upgrading 85

T
templates, AD RMS 583–584
thin provisioned virtual disk 396
Thin provisioning and trim 394–396
tie breaker for 50% node split 527
Tiered storage 398–399
token-decrypting certificates, AD FS 663
token-signing certificates, AD FS 663
transitive trust 14
trigger replication 101
Trim 396
Trust anchor 121
Trusted publishing domains (TPDs). See AD RMS (Active Directory Rights Management Services)
Trusted user domains (TUDs). See AD RMS (Active Directory Rights Management Services)
trusting domains/forests 14
trust relationships 4
trusts 13–21
two-way trust 14
U

Understanding Network Load Balancing 456–466
unidirectional trust 14
update sequence numbers (USNs) 75
Upgrading an NLB cluster 464–465
UPN (user principal names) suffixes 10
USB (Universal Serial Bus) ports 212
hardware security module (HSM) 212
user claims (DAC), configuring 570
user principal names (UPN) suffixes 10
Users And Computers (Active Directory) console 4
selective authentication and 17
UPN suffixes and 10
USNs (update sequence numbers) 75

V

Validity Period (certificate template settings) 221
Validity Period page (AD CS Configuration Wizard) 220
virtual desktops 6
virtual machine network health detection 528
virtual machines
movement 505–516
failover clustering 506–508
Hyper-V live migration 509–511
import/export 515–516
storage migration 512–514
Vssadmin 313–316

W

WAN (wide-area network) 61
Web Application Proxy 658
Web Application Proxy server 667–668
wide-area network (WAN) 61
Windows Azure Backup 306–315
  Backing up data 310
  Preparing 308
  Recovery Services 312
  Restore from 320–321
Windows PowerShell Credential pop-up 241
Windows Server 2003 domain functional level 5
Windows Server 2008 domain functional level 5
Windows Server 2008 R2 domain functional level 5, 6
Windows Server Backup 302–306
  Backing up data 306
  Backup locations 304

Z

Zone level statistics 131
Cache statistics 131
DNSSEC statistics 131
Error statistics 131
Master statistics 131
Query statistics 131
Record statistics 131
Recursion statistics 131