Microsoft

Configuring Advanced Windows Server 2012 R2 Services

Exam Ref 70-412

J.C. Mackin
Orin Thomas

Microsoft

Exam Ref 70-412: Configuring Advanced Windows Server 2012 R2 Services

J.C. Mackin
Orin Thomas

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2014931891
ISBN: 978-0-7356-7361-8

Printed and bound in the United States of America.

First Printing

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

Acquisitions Editor: Anne Hamilton
Developmental Editor: Karen Szall
Editorial Production: Box Twelve Communications
Technical Reviewer: Brian Svidergol
Cover: Twist Creative • Seattle

Contents at a glance

Contents

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:

www.microsoft.com/learning/booksurvey/

Introduction

Unlike other exams in the MCSA track, the Microsoft 70-412 certification exam deals with advanced topics such as Active Directory Rights Management Services and Active Directory Federation Services. Much of the exam comprises topics that even experienced systems administrators encounter less frequently than they encounter core infrastructure technologies, like Active Directory Domain Services and Windows Deployment Services.

Candidates for this exam are Information Technology (IT) Professionals who want to validate their advanced Windows Server 2012 R2 operating system configuration skills and knowledge. To pass this exam, candidates require strong understanding of how to configure and manage Windows Server 2012 R2 high availability, file and storage solutions, business and disaster recovery, network services, Active Directory infrastructure, and access and information protection solutions. To pass this exam, candidates require a thorough theoretical understanding as well as meaningful practical experience implementing the technologies involved. If you lack this experience, consider using the Microsoft Press companion title, *Training Guide: Configuring Advanced Windows Server 2012 R2 Services*, which contains extensive practical lab exercises.

This Exam Reference book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the links you'll find in text to find more information and take the time to research and study the topic. Great information is available on TechNet as well as in product team blogs and online forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *http://www.microsoft.com/learning/en/us/certification/cert-default.aspx*.

Errata & book support

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

http://aka.ms/ER412R2/errata

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

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

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

We want to hear from you

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

http://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*.

Preparing for the exam

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

CHAPTER 3

Implement business continuity and disaster recovery

This domain refers to the essential functions of backing up, restoring, and recovering servers. Understanding the topics covered in this domain requires a deep understanding of new technologies that you might not have implemented in your own environment. You should supplement the information in this chapter with some hands-on practice so that you can develop an understanding of how you can use these technologies to address real world scenarios and solve problems in an advanced server environment.

Objectives in this chapter:

- Objective 3.1: Configure and manage backups
- Objective 3.2: Recover servers
- Objective 3.3: Configure site-level fault tolerance

Objective 3.1: Configure and manage backups

This objective deals with preparing for data loss. Performing backups with the Windows Server Backup feature is the simplest and most obvious way to prepare for disaster recovery, but that doesn't mean that it's the most likely topic in this objective to appear on the exam. Windows Server Backup—at least at the basic level in which people most often use it— is actually too simple to lend itself well to exam questions. If you see a question about Windows Server Backup on the 70-412 exam, the question will address deeper configuration issues, such as configuring VSS or performance settings.

The exam question writers will likely have an easier time creating questions at an appropriate level of difficulty for the other topics covered in this objective, such as backup user rights, VSSAdmin, and Windows Azure Backup.

This objective covers how to:

- Use the Windows Server Backup feature
- Understand Backup Operators
- Use the Shadow Copies feature (Previous Versions)
- Configure online backups (Windows Azure Backup)

Using the Windows Server Backup feature

Windows Server Backup is the server backup feature in Windows Server 2012 and Windows Server 2012 R2. Its graphical console (Wbadmin.msc) is installed by default, but you can't use this console perform any local backups until you actually install the feature itself. To install the Windows Server Backup feature, you can, of course, use the Add Roles and Features Wizard, but if you prefer to use Windows PowerShell, type the following at a Windows PowerShell prompt:

```
Install-WindowsFeature Windows-Server-Backup
```

After you install Windows Server Backup, two backup wizards become available in the Windows Server Backup console: The Backup Schedule Wizard and the Backup Once Wizard. The links to open these wizards are shown in Figure 3-1. To prepare for Objective 3.1 on the 70-412 exam, you need to understand (among other things) all of the configuration options available in these two wizards. Fortunately, the wizards are very similar, and there aren't many options to learn.

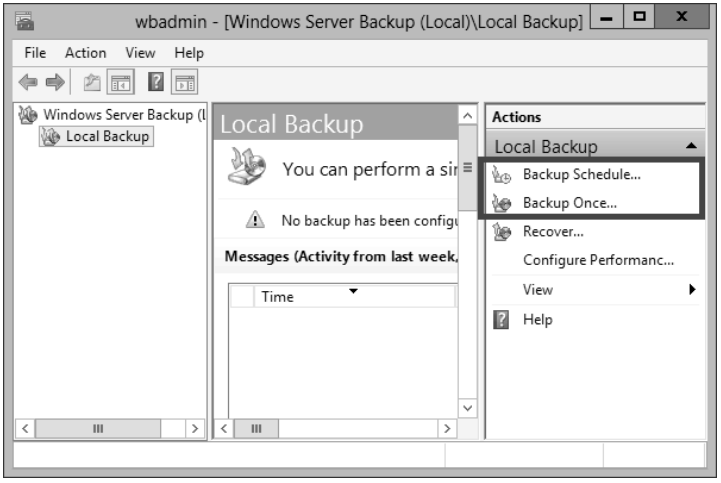

FIGURE 3-1 The Windows Server Backup console

Backup Options page

The Backup Options page appears only in the Backup Once Wizard, not the Backup Schedule Wizard. This first page gives you two options for performing a backup now: The first option is available only if you've already configured a scheduled backup for the local server. When available, this option lets you make an immediate backup of the same items you've already configured for the scheduled backup. All settings you've configured for that scheduled backup are also used, including the location at which you've chosen to save the backup data. The second backup option is to perform an immediate backup with options that haven't been configured for the scheduled backup on the local server. In Figure 3-2, the option to choose the scheduled backup options is, in fact, grayed out because no scheduled backup has been configured for the local server.

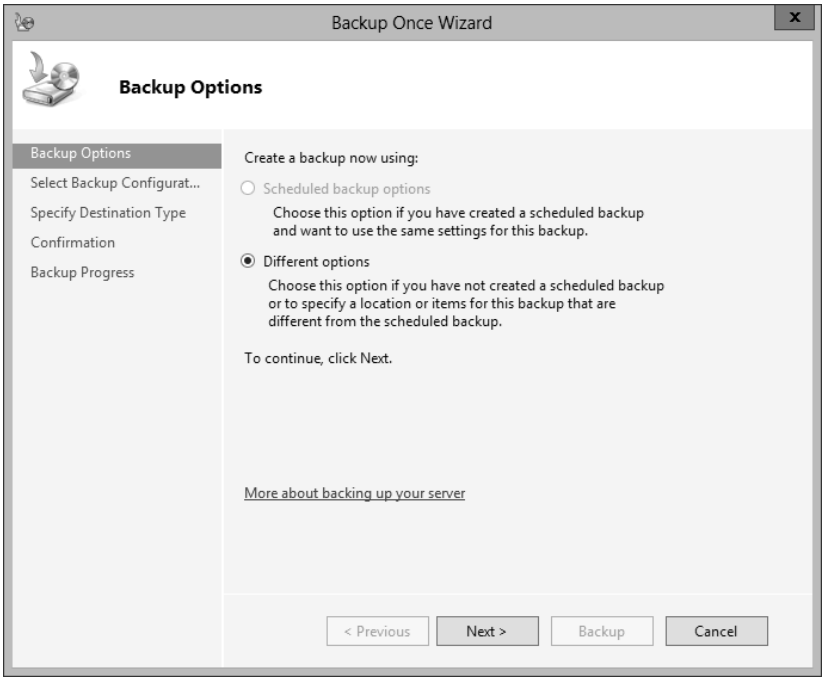

FIGURE 3-2 General options for immediate backup

Select Backup Configuration page

This page is shown in in the top left portion of Figure 3-3. Here you decide whether to perform a full server backup or a custom backup. As you might expect, a full server backup, includes all data on the system and lets you perform any type of recovery, including a system state or bare metal recovery. A custom backup can be a full backup or any subset of volumes, folders, or files. A custom backup also allows you to make some advanced configuration choices, such as creating exclusions or changing VSS settings for the backup.

If you are testing backup functionality for the purpose of exam preparation, make sure you choose the Custom option so that you can see all available backup options.

Select Items For Backup page

The Select Items For Backup page is shown in the bottom-right portion of Figure 3-3. On this page, click Add Items to choose which items to back up. Click Advanced Settings to adjust some default configuration settings for the backup.

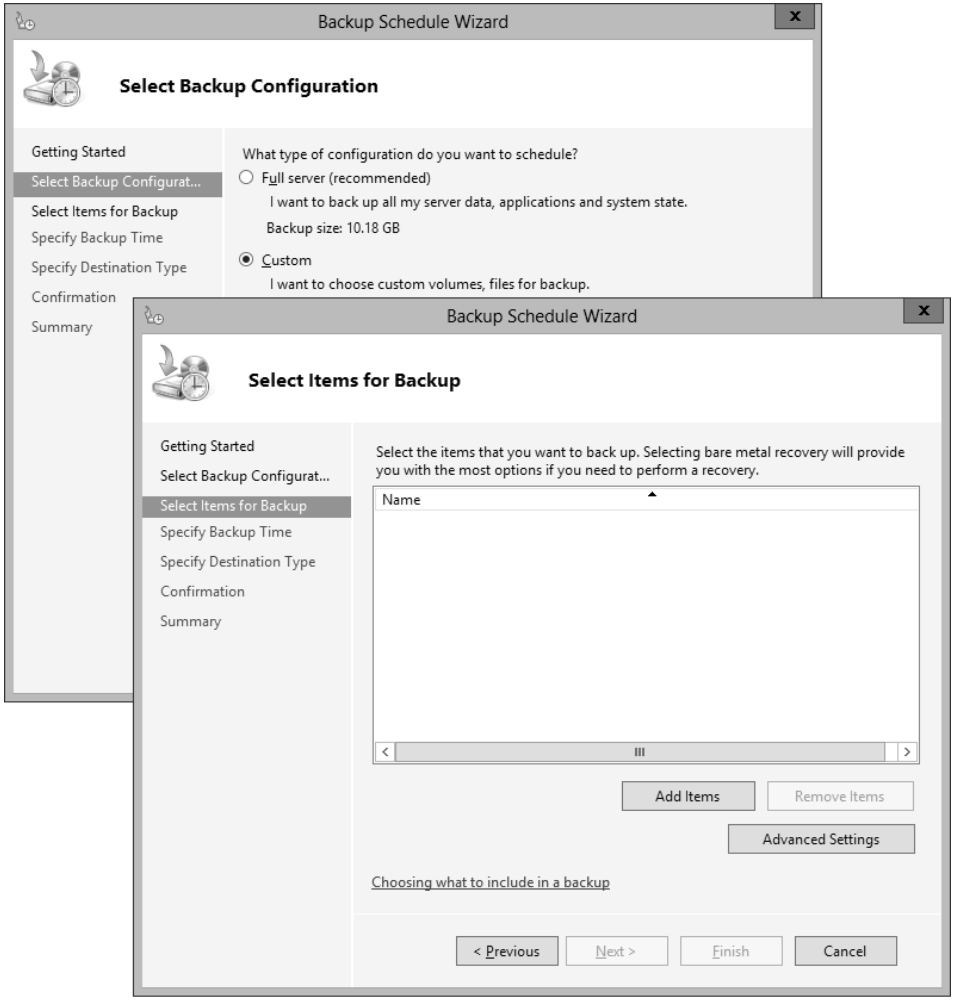

FIGURE 3-3 Choosing a backup type and items for backup

Add Items

Clicking Add Items on the Select Items For Backup page opens the Select Items dialog box, shown in Figure 3-4.

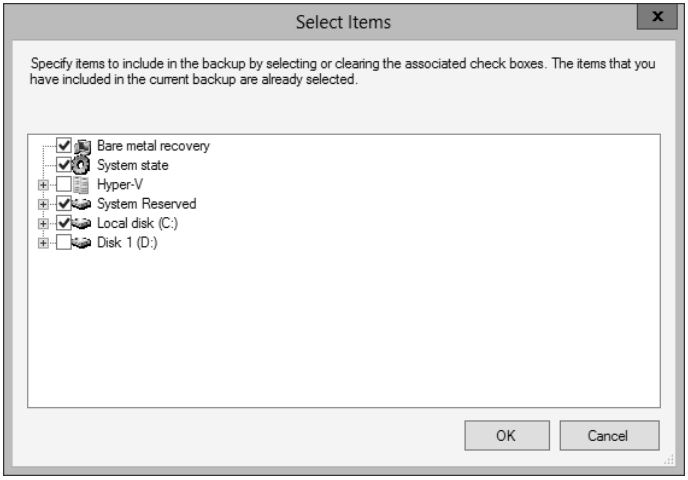

FIGURE 3-4 Selecting items to back up

Of these options, make sure you understand the following:

- **Bare Metal Recovery** This item in the Select Items dialog box is not a data component but a shortcut that selects the components required for a bare metal recovery. When you select Bare Metal Recovery, as shown in Figure 3-4, the System State and system disk (typically C:) are automatically selected, along with any System Reserved partition that the local system might include. Backing up these Bare Metal Recovery components lets you later boot a restored version of the local system on a server that is not loaded with any software at the outset. The bare metal server can be the original system with newly formatted disks or it can be another, identical system.
- **System State** System State contains only the system files and configuration data of the local server. By restoring these files, you would restore the configuration state of the server as it existed at the time the backup was performed. If the operating system on your server becomes corrupted, you can also use the system state data to repair a system and get it to a bootable state. System state always includes the following components:
  - Registry
  - COM+ class registration database
  - Boot files, including system files
  - System files under Windows File Protection

If the server is a domain controller, the following two components are also included in the system state:

- Active Directory service
- SYSVOL directory
- Certain server roles, such as the DHCP, AD CS and DNS roles and their associated databases, are also included in system state data.

- **Hyper-V** If the local server is a Hyper-V host, you will be able to select each hosted VM for backup.
- **Individual files and folders** Windows Server Backup in Windows Server 2012 and Windows Server 2012 R2 allows you to select individual volumes, folders, or files for backup.

Advanced Settings

If you click Advanced Settings on the Select Items For Backup page of the Backup Once Wizard or Backup Schedule Wizard (as shown in Figure 3-3), the Advanced Settings dialog box opens.

CONFIGURING EXCLUSIONS

It's possible that you'll see a question on the 70-412 exam that requires some understanding of backup exclusions. Such a question might set up a scenario in which you need to perform a backup more quickly, or with less space, or with less network traffic, than the current backup set. The "correct answer" might be to exclude a folder or files that match a particular filename pattern with some unneeded data in the current backup set. You do this on the Exclusions tab of the Advanced Settings dialog box, as shown in Figure 3-5.

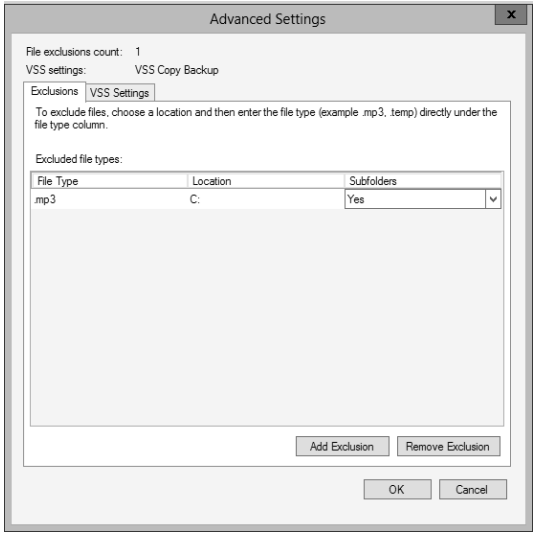

FIGURE 3-5 Excluding .mp3 files from a backup set

CONFIGURING VSS SETTINGS

The other tab—VSS Settings—is shown in Figure 3-6. *Volume Shadow Copy Service (VSS)* is the background service that, among other important functions, allows Windows Server Backup to create backups of all files, even ones which are locked by applications. All backups performed by Windows Server Backup are VSS backups, so these settings are always applied when the backup you're currently defining is performed.

The two options are:

- **VSS Full Backup** With this setting, the files you back up are marked as backed up in the application log file. This option is appropriate when you are not using any other backup application.
- **VSS Copy Backup** This is the default selection. With this option, the backed-up files are not marked up as backed up, so the backup doesn't interfere with any other backup applications.

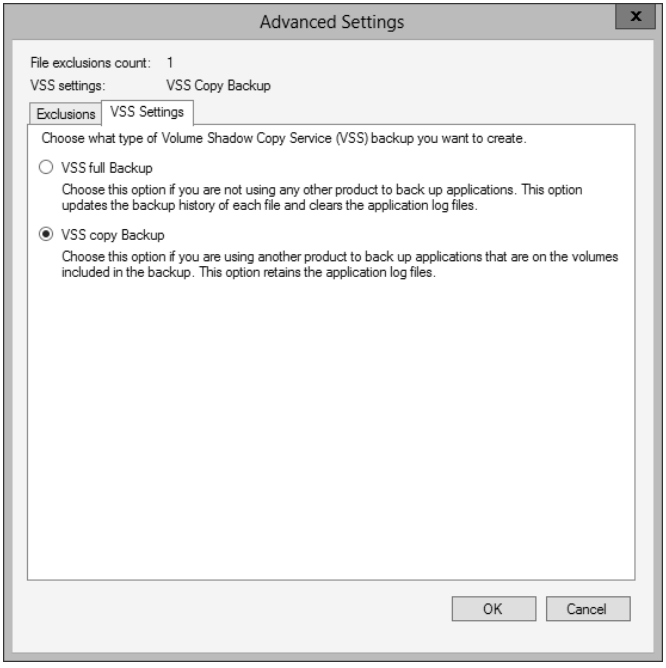

FIGURE 3-6 Choosing the type of VSS backup

Destination type

After you choose which items to back up and make any desired exclusions and changes to VSS settings, you need to specify a location to store the backup.

- **Back Up To A Dedicated Hard Disk** This option is available only for scheduled backups. If you have a spare physical hard disk, this option offers the best performance

for storing backups. Writing to the dedicated disk doesn't interfere with any other I/O operations.

- **Back Up To A Volume** This option is also available only for scheduled backups and applies to non-dedicated volumes and mapped network drives, not optical drives such as DVD drives.
- **Local Drives** This option is available only with the Backup Once option. It is similar to the Back Up To A Volume option, except that you can also burn the backup to an optical drive.
- **Remote Shared Folder** This option is available for both the scheduled backups and immediate backups. An important limitation of saving to a remote shared folder is that you can only store one backup at the remote location. Any existing backups found at the network path are overwritten by the new backup.

EXAM TIP

Remember that backing up to a remote shared folder overwrites the previous backup.

Performance settings

Performance settings are configured in the Windows Server Backup console, not the Backup Schedule Wizard or the Backup Once Wizard. The performance settings allow you to make backup operations quicker, at the expense of a longer restore operation. To view performance settings, click Configure Performance Settings in the Actions pane of the console, as shown in Figure 3-7. This opens the Optimize Backup Performance dialog box, shown in Figure 3-8.

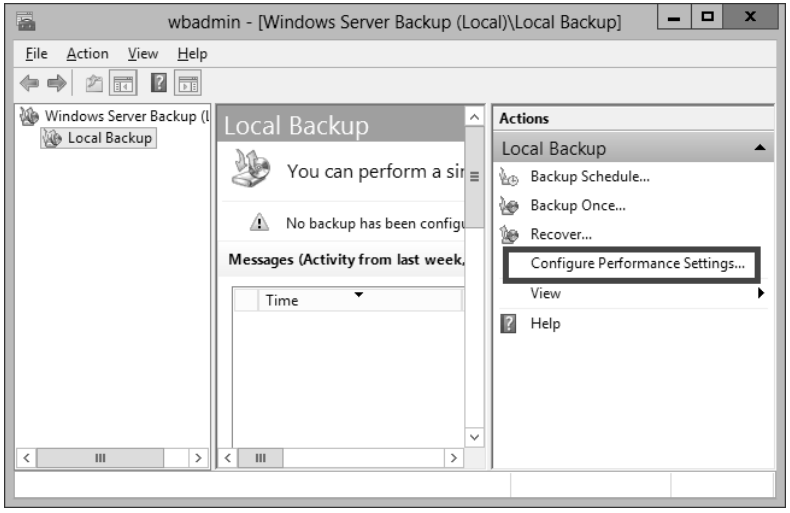

FIGURE 3-7 Configuring performance settings

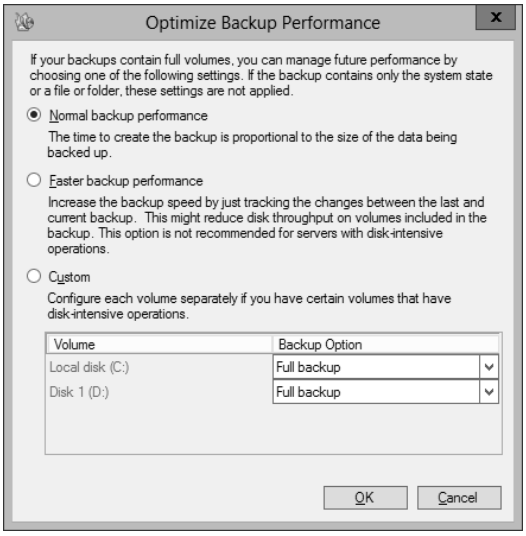

FIGURE 3-8 Configuring performance settings

By default, Normal Backup Performance is selected. With this option, full backups are performed. (The complete source data is backed up to the destination storage location, regardless of whether the blocks of data have changed.)

If you select Faster Backup Performance, incremental backups are performed 14 times in a row or 14 days in a row (whichever is sooner) before each full backup is performed. With incremental backups, only the blocks of data that have been modified since the last backup are copied to the destination storage location. The backup procedure is usually faster as a result, but the restore operation is typically longer.

To apply different backup methods to different volumes, select the Custom option. The choice for each volume is displayed as Full Backup or Incremental Backup.

Command-line tools for backup

Although backups you've reviewed where backup options are found in the GUI, it's also a good idea to look at how you can perform or configure backups from the command line. Windows Server 2012 and Windows Server 2012 R2 include two command-line tools to configure and perform backups: the *Wbadmin.exe* utility and Windows PowerShell.

Wbadmin.exe offers basic backup functionality and is installed when you install the Windows Server Backup feature of Windows Server 2012 and Windows Server 2012 R2. To see the commands available in Wbadmin.exe, type **Wbadmin /?** at a command prompt after you've installed Windows Server Backup feature.

Windows PowerShell includes a much more complete command-line administration interface for server backups. To see the Windows PowerShell cmdlets for backups in Windows Server 2012 or Windows Server 2012 R2, type the following at a Windows PowerShell prompt:

```
Get-Command -Module WindowsServerBackup
```

Understanding Backup Operators

Only members of the local Administrators group and the local Backup Operators group have the right to perform backups of files and directories on a given machine. Backup Operators are also granted the rights to restore files and directories and the right to shut down the system.

All three of these rights (backing up, restoring, and shutting down the system) are rights that can be assigned separately through User Rights Assignment in Local Computer Policy or Group Policy. If, for example, you want to grant a user the right to back up files and directories but not the right to restore files and directories, you need to assign the user that specific user right through Local Computer Policy or Group Policy. Don't add the user to the Backup Operators group because you will be granting that user unwanted privileges.

EXAM TIP

For the 70-412 exam, remember that Backup Operators have more rights than just backing up a system. They can back up, restore, shutdown the system, log on locally, and access the computer from the network. If you want to assign a user just a few of those privileges, you should assign that user those rights through Local Computer Policy or Group Policy instead of adding her to the Backup Operators group.

Using the Shadow Copies feature (Previous Versions)

The Volume Shadow Copy Service provides the software framework not only for Windows Server backups but for the Shadow Copies feature and its related Previous Versions feature.

You can enable shadow copies of volumes in the properties of those volumes, after which snapshots of the volume are taken regularly (twice per day by default). You can also access these settings by right-clicking a volume and selecting Configure Shadow Copies on the shortcut menu. After you have enabled shadow copies on a volume, users can use the Previous Versions feature to restore to a previous snapshot any file or folders the users own on that volume. This functionality is shown in Figure 3-9. In the figure, shadow copies are enabled on volume D:\. When you then right-click a file on that volume, the shortcut menu shows an option to restore previous versions.

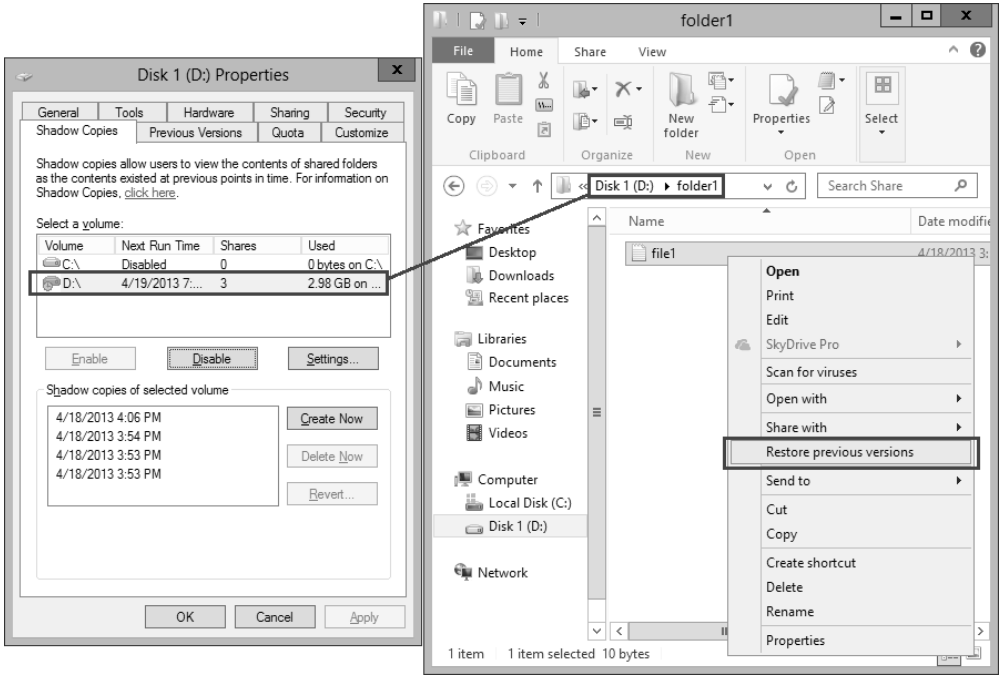

FIGURE 3-9 In this example, shadow copies are enabled on Volume D:\, allowing a user to restore a previous version of a file stored on that same volume

If you select the Restore Previous Versions option shown in Figure 3-9, the Previous Versions tab of the File Properties dialog box opens. This tab is shown in Figure 3-10. To restore a previous snapshot of the file, users can select the desired file version and then click the Restore button.

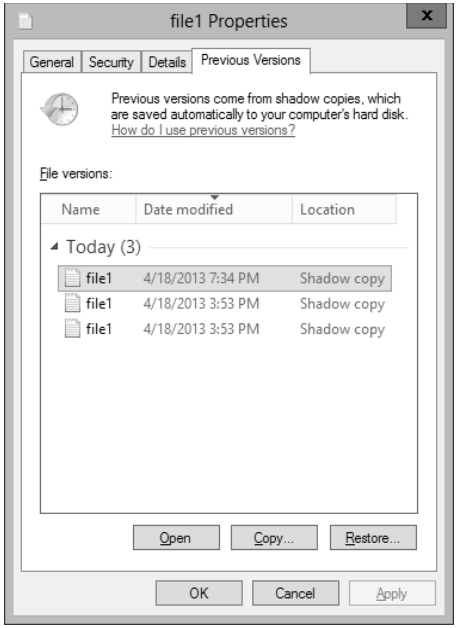

FIGURE 3-10 Restoring a previous version of a file

VSSAdmin is the command-line utility used for managing shadow copies and the Previous Versions feature. For example, you can create a new shadow copy (snapshot) of a volume by typing **VSSAdmin Create Shadow** at an elevated command prompt. To list available snapshots, type **VSSAdmin List Shadows**. To revert a volume to a previous snapshot, type **VSSAdmin Revert Shadow**. To delete a snapshot, type **VSSAdmin Delete Shadow**. To review other administrative options made available through VSSAdmin, type **VSSAdmin /?**.

EXAM TIP

You need to remember that VSSAdmin is the command-line tool used to manage shadow copies and the Previous Versions feature.

Configuring Windows Azure Backup

Microsoft provides an online backup feature—*Windows Azure Backup*—that lets you perform individual server backups to the cloud. Because it's an online service, Windows Azure Backup is capable of changing more than built-in features of Windows Server 2012 are. Make sure you consult online references about this service before you take the exam, so you know you have the most up-to-date information.

MORE INFO **ONLINE BACKUPS**

One good source of recent information about Microsoft online backups are the video screencasts about the service found at *http://technet.microsoft.com/en-US/video/ff832960.aspx?category=Robert%20Mitchell*.

Create a Windows Azure account

The first step in configuring online backups is to create Windows Azure account and then create a backup vault. You can create a backup vault directly through the Windows Azure management console at *http://manage.windowsazure.com*, as shown in Figure 3-11.

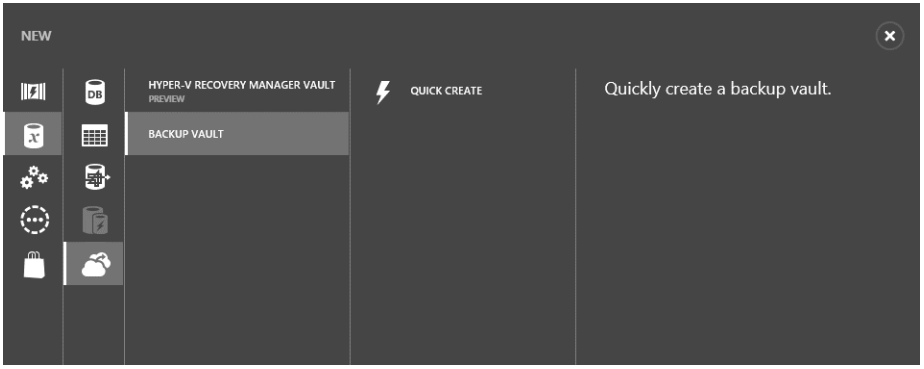

FIGURE 3-11 Creating a backup vault

Create a vault and add a certificate

In your Windows Azure portal, navigate to the recovery services and create a recovery vault in which to store your backups. After you create a vault, you need to upload management certificate to Windows Azure. You can obtain this certificate from a public certification authority (CA) or from a CA managed by your organization (such as Active Directory Certificate Services). Alternatively, you can create a self-signed client certificate by using the Makecert.exe command-line utility. Makecert.exe is included in Microsoft Visual Studio Express, the most recent version of which is a free download at *http://microsoft.com/download*.

NOTE **MAKECERT.EXE SYNTAX**

If you use Makecert.exe to create a self-signed certificate, use the following syntax:

```
makecert.exe -r -pe -n CN=<certName> -ss my -sr localmachine -eku
1.3.6.1.5.5.7.3.2 -e 12/12/2018 -len 2048 <CertificateName>.cer
```

Download and install the Windows Azure Backup Agent

After you create an account on the Windows Azure Backup website, create your vault, and upload your client certificate, you can download the Windows Azure Backup Agent and install it locally on the server. The Backup Agent appears similar to the Windows Server Backup console and is shown in Figure 3-12. This agent can be used to back up a single server to Windows Azure or it can be used to allow System Center 2012 R2 Data Protection Manager to perform backups to Windows Azure.

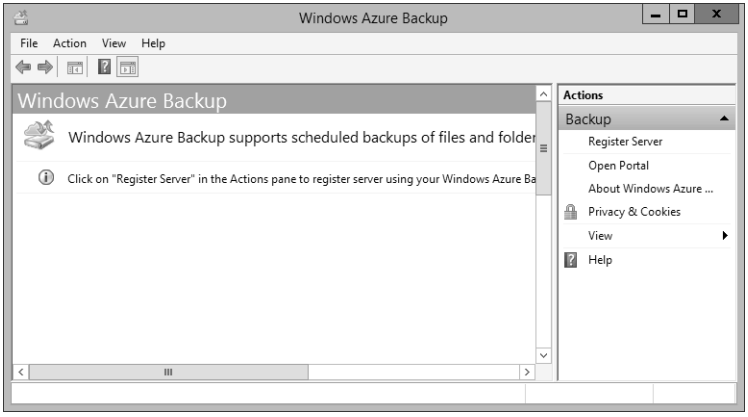

FIGURE 3-12 Using the Windows Azure Backup console

Register your server

The next step is to register your server. Registering a server enables you to perform backups from that same server only, though you can register multiple servers with the same recovery vault hosted with the same Windows Azure account.

The Register Server Wizard includes a few configuration steps. First, you are given an opportunity to specify a proxy server if desired. Second, you are asked to specify the certificate again and choose the Windows Azure vault to which you want to save your backups, as shown in Figure 3-13.

FIGURE 3-13 Registering a server

Finally, you need to specify a passphrase that will be used to encrypt your backup data. You must also specify a location to save this passphrase in a file. You need to provide this passphrase when you perform a restore operation, so it's essential that you don't lose it. (Microsoft doesn't maintain a copy of your passphrase.) A Generate Passphrase option creates the passphrase for you automatically.

After you register a server, new options for online backups appear in the Actions pane, including Schedule Backup, Recover Data, Change Properties, and Open Portal.

EXAM TIP

Remember this sequence of configuration steps: Create a Windows Azure account, upload the management certificate, download and install the agent, and then register the server.

Create a schedule

To start the Schedule Backup Wizard, click Schedule Backup in the Actions pane. The items you can select to backup in the Schedule Backup Wizard are shown in Figure 3-14.

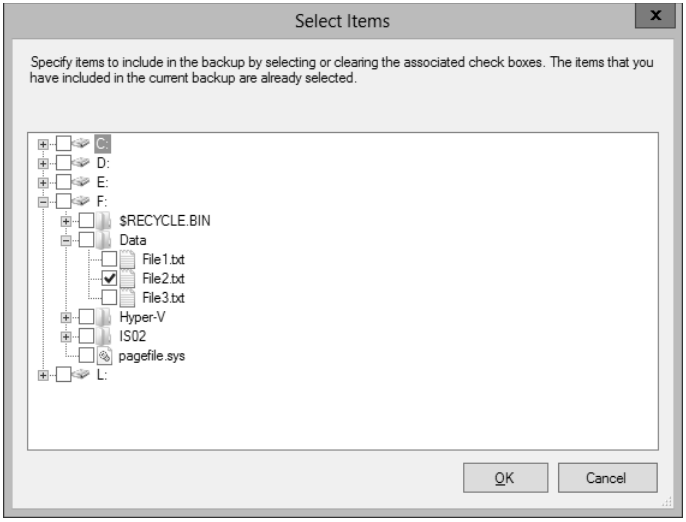

FIGURE 3-14 Selecting backups for an online backup

SPECIFYING RETENTION SETTINGS

Another feature especially relevant for the exam can be found on the Specify Retention Setting page of the Schedule Backup Wizard, shown in Figure 3-15. The *retention setting*, also called the *retention range*, is simply the number of days that the backup cannot be overwritten or deleted to make space for another backup. You can set the retention range for a backup at 7 days (the default), 15 days, or 30 days.

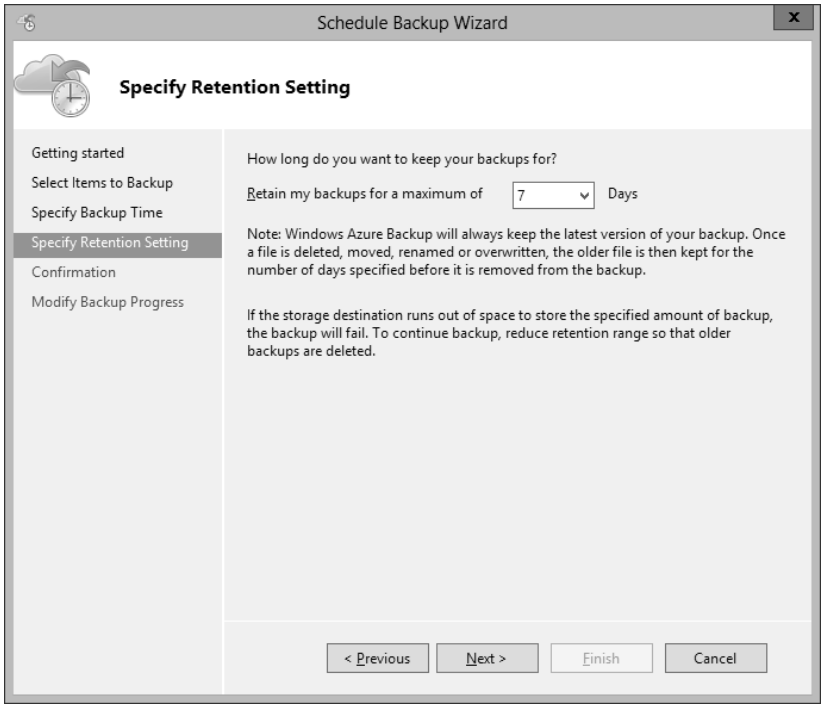

FIGURE 3-15 Configuring backup retention settings

Configure the Back Up Now option

The Back Up Now option appears in the Actions pane for online backups, as shown in Figure 3-16, but it does so only after you first complete the Schedule Backup Wizard. As stated earlier, Back Up Now for online backups allows you to perform additional online backups only of online backup sets that have been previously defined and scheduled. You *can't* use this option to select a new set of volumes, folders, or files and then perform an online backup of that new set.

Aside from this critical difference, the Back Up Now option for online backups resembles the Back Up Once option for local backups.

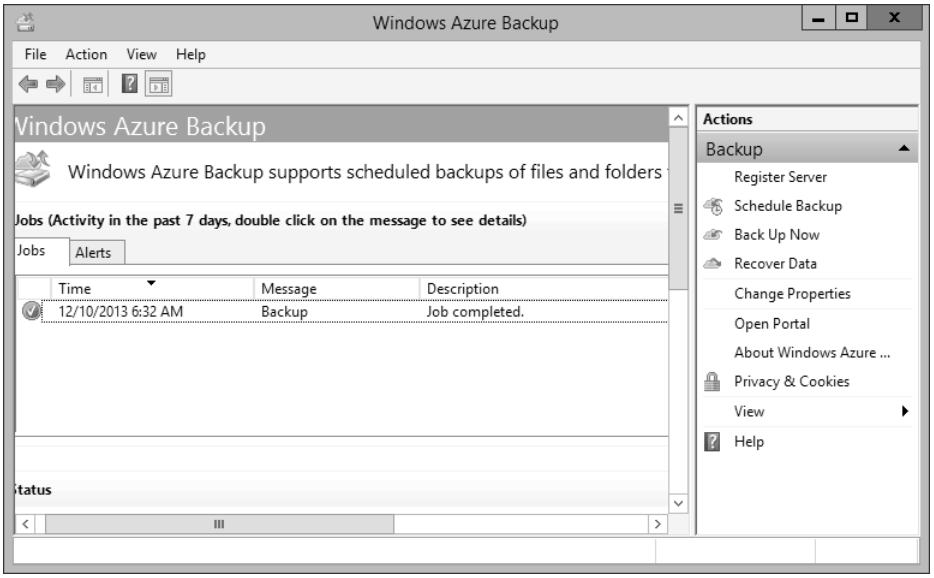

FIGURE 3-16 Viewing a backup job in the Windows Azure Backup console

Choose a Recover Data option

To restore data that has been backed up, choose the Recover Data option in the Actions pane. As Figure 3-17 shows, there isn't anything new or unusual about this option that would likely confuse you in the real world or in the exam world. However, it's worth remembering that you can restore online backups to another server.

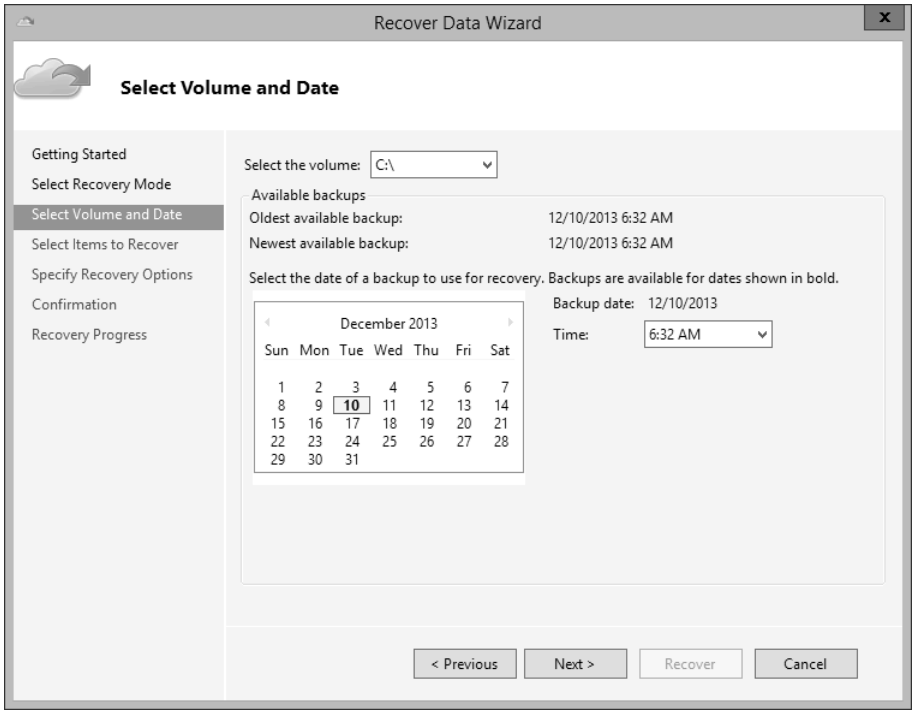

FIGURE 3-17 Recovering data

Enable bandwidth throttling

You can restrict the amount of bandwidth used during your online backup operations in a way that depends on when the backup occurs. To enable bandwidth throttling, click Change Properties in the Actions Pane, select the Throttling tab, and then select Enable Internet Bandwidth Usage Throttling For Backup Operations, as shown in Figure 3-18.

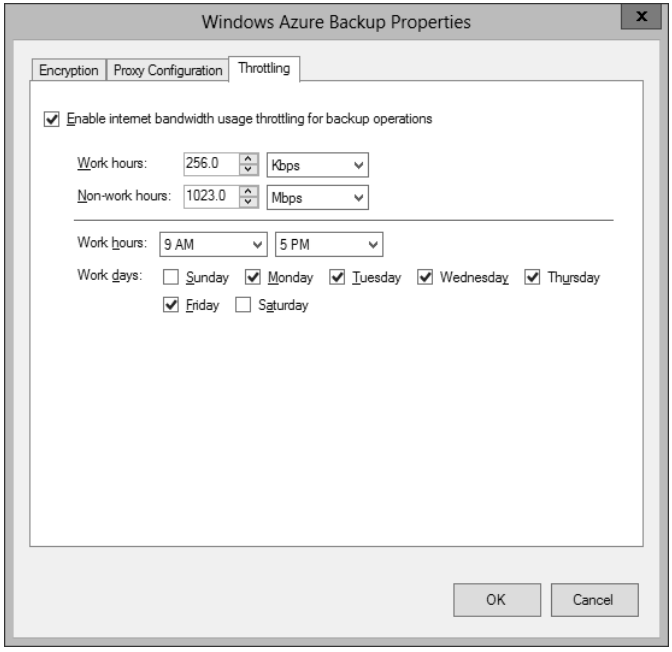

FIGURE 3-18 Configuring bandwidth throttling for online backups

Bandwidth throttling works by letting you set different bandwidth speeds for work and non-work hours. First you define the hours that should be considered work hours and for which days of the week. Then you specify how much Internet bandwidth you want to use for online backup operations during both these work hours and during the remaining non-work hours.

Bandwidth throttling might be the most likely feature about online backups to appear on the exam. For example, you could see a question that displays the Throttling tab and an accompanying scenario in which you need to adjust these settings in a way that reduces the impact of online backups on your users. In such a case, you might need to redefine the work hours (perhaps by lengthening the work day). Alternatively, you might need to decrease the bandwidth currently assigned to work hours if you want to prevent workday disruption. Or you might want to increase the bandwidth currently assigned to non-work hours if you want the online backups to be performed as quickly as possible.

Thought experiment

Using Windows Azure Backup at Adatum's branch offices

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

You are in the process of developing a solution to ensure that important server data hosted at remote Adatum branch offices is backed up in a reliable manner. In the last few years, backups have been written to attached USB storage devices. The problem is that these devices have been found to be unreliable, with the failure of the device only becoming apparent when an attempt to restore data has been performed. One solution that you are investigating is using Windows Azure Backup so that backed up data is stored within Windows Azure. With this in mind, you need to answer several questions before you proceed with the pilot program.

1. **What steps do you need to take prior to downloading the Windows Azure Backup agent?**
2. **What is the maximum retention period for data backed up to Windows Azure using Windows Azure Backup?**
3. **In addition to your Windows Azure account, what do you need access to if you want to recover data from Windows Azure Backup?**

Objective summary

- Windows Server Backup is the GUI-based backup tool in Windows Server 2012. Windows Server Backup lets you back up individual files, folder, and volumes; the system state data; the System Reserved partition; and the individual VMs hosted in Hyper-V. The command-line tool for performing backups in Windows Server 2012 is Wbadmin.exe.
- Backup Operators have the right to back up files and directories, restore files and directories, shut down the system, log on locally, and access the computer from the network.
- You can enable shadow copies on individual volumes. Snapshots of the volumes are then automatically taken by default twice per day. Users connecting to shared folders on these volumes will see previous versions of files in the shares available through the Previous Versions tab of the share properties. You can manage this Shadow Copy feature with the VSSAdmin tool.
- Windows Server 2012 provides an option to let you back up selected volumes, folders, and files of the local server over the Internet to cloud storage on Microsoft-owned

premises. This functionality is provided by an optional add-on service called Windows Azure Backup.

- To prepare to use Windows Azure Backup, you first create a Windows Azure account, then create a vault in which to store backups, then upload a certificate, and finally download and install the Windows Azure Backup Agent.

Objective review

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

1. Your network includes a file server named FileSrv1 that is running Windows Server 2012. You want to allow a user named User1 to back up FileSrv1. You also want to minimize the administrative privileges assigned to User1.

   What should you do?

   A. Assign User1 to the Backup Operators group on FileSrv1.

   B. Assign User1 to the Power Users group on FileSrv1.

   C. Assign User1 the user right to back up files and directories.

   D. Assign User1 the user rights to back up and restore files and directories.

2. Your network includes a file server named FileSrv2. FileSrv2 is running as a server core installation of Windows Server 2012. You want to create an immediate snapshot of volume E:\ so that users connecting to file shares will be able to revert files to the now-current version of the files in those shares. You want to perform this task with the least amount of administrative effort.

   Which tool should you use?

   A. VSSAdmin

   B. Shadow

   C. Get-VMSnapshot

   D. Wbadmin

3. You configure a Hyper-V host running Windows Server 2012 named VHost01 to perform a Windows Azure Backup at 11 P.M. every Wednesday. The organization's Internet connection isn't used for any other operations until 8 A.M. the following day. After running the online backup for the first time, you discover that the backup operation completes at 10:00 A.M. Thursday, after the start of the workday. You open the bandwidth throttling settings for the server and see the configuration shown in Figure 3-19.

   You want the online backup of VHost01 to complete before 8 A.M. on Thursday. Which of the following solutions is most likely to help you accomplish your goal with a minimum disruption for workers?

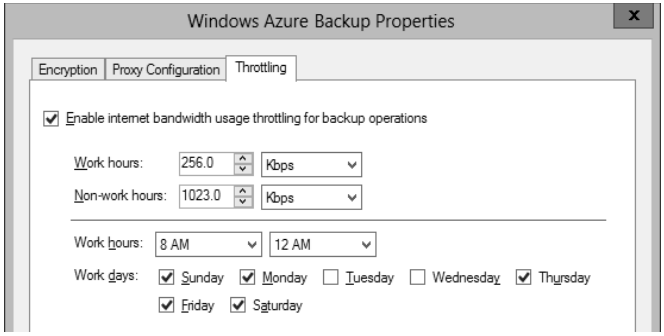

FIGURE 3-19 Configuring bandwidth throttling settings on FS01

A. Change the bandwidth setting assigned to work hours.

B. Change the bandwidth setting assigned to non-work hours.

C. Change the hours defined as work hours.

D. Change the days defined as work days.

4. You have a Windows Azure Backup account with a storage quota of 300 GB. You use this account to configure a single weekly backup of a file server running Windows Server 2012 named FileSrv01. The total amount of data on FileSrv01 does not significantly change from week to week. No other backups are configured with your account.

The online backup of FileSrv01 completes successfully on the first week, but on the second week, the backup fails. You receive an error indicating that the usage associated with your Windows Azure Backup account has exceeded its quota.

The Windows Azure Backup console displays the information shown in Figure 3-20 about the backup.

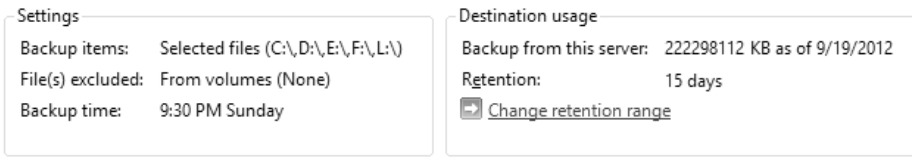

FIGURE 3-20 Viewing backup settings and destination usage

You want to be able to perform the weekly backup of FileSrv01 without failure. Which of the following actions is most likely to allow you to accomplish your goal?

A. Configure an exclusion for C:\Windows\Temp and choose to exclude its subfolders.

B. Configure an exclusion for C:\Windows\Temp and choose not to exclude its subfolders.

C. Change the retention range to 7 days.

D. Change the retention range to 30 days.

5. You want to configure a file server running Windows Server 2012 and named FS02 to perform a daily Windows Azure Backup at 3 AM. You also want to ensure that if the online backup operation extends into the beginning of the next workday at 9 AM, it will have a minimal impact on network performance for users. The workweek in your organization runs from Monday through Friday.

   You enable Internet bandwidth usage throttling for backup operations and find the default settings shown in Figure 3-21. What should you do next?

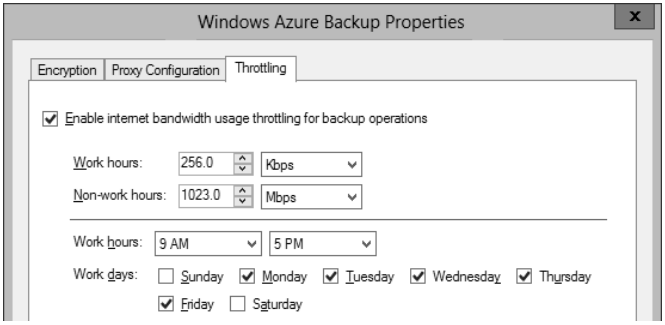

FIGURE 3-21 Configuring bandwidth throttling settings on FS02

   A. Leave the default settings.

   B. Increase the bandwidth setting assigned to work hours.

   C. Increase the bandwidth setting assigned to non-work hours.

   D. Change the selected workdays.

Objective 3.2: Recover servers

You have three topics to learn about for this objective, all of which are straightforward. First, learn the purpose of every advanced boot option and how to select these options. Then learn when and how to perform a system image recovery. Finally, learn a few command-line tools useful for troubleshooting in the Windows Recovery Environment.

This objective covers how to:

- Use the Advanced Boot Options menu
- Recover servers with the Windows installation media

Using the Advanced Boot Options menu

The Advanced Boot Options menu gives you an important set of troubleshooting tools to fix a faulty Windows installation if the system at least begins the process of loading. Advanced Boot Options is especially useful when Windows doesn't start successfully, but it also provides

options to repair the system if the system boots but behaves erratically (for example, after an application or driver install).

To get the menu to appear, press F8 just as the system is starting. If you are already in Windows and want to access the Advanced Boot Options menu the next time the system starts without pressing F8, you can use the **Shutdown /r /o** command or hold down the Shift key as you click Restart. These last two options shut down the system and then open a special Choose An Option screen, as shown in Figure 3-25. To restart the system into the Advanced Boot Options menu, click Troubleshoot, Startup Settings, Restart.

The Advanced Boot Options menu is shown in Figure 3-22.

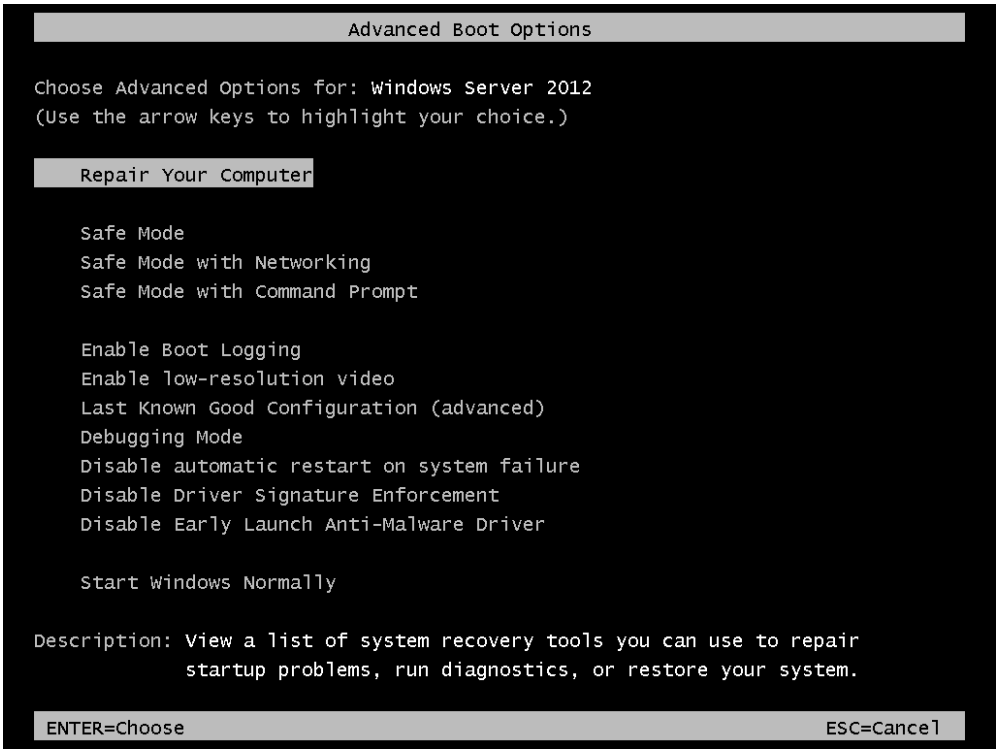

FIGURE 3-22 The Advanced Boot Options menu

EXAM TIP

For the 70-412 exam, you need to understand when to use all of the advanced boot options, but some options are more important to know for the exam than others. The most important advanced boot options for the exam are all three Safe Mode options (including the alternative methods to open them with Bcdedit and Msconfig), Last Known Good Configuration, and Disable Driver Signature Enforcement.

The available options are:

- **Repair Your Computer** Use this option to perform system image recovery. With this option, you can completely restore your computer from an earlier backup or image file.
- **Safe Mode** This option lets you boot the operating system with only minimal drivers, files, and services. The only drivers loaded are for the mouse, keyboard, storage, and video. This limited footprint allows you to get into the GUI operating system to remove applications or drivers or change any settings that are otherwise disrupting the system.
- **Safe Mode With Networking** This option is almost the same as Safe Mode, but it also adds networking drivers and services. With this option you can connect to the Internet or the local network to download files needed to fix the system.
- **Safe Mode With Command Prompt** This option is almost the same as Safe Mode, but the system boots into a command prompt instead of a GUI. No networking capabilities are provided.
- **Enable Boot Logging** This option attempts a normal boot into Windows Server 2012 and logs the boot procedure. For example, you can use this option to see which file is the last to load before a system freezes. The log file generated is named Ntbtlog.txt and is found in the Windows directory. If you can't boot into Windows, you can access and open Ntbtlog.txt if you boot with another operating system, such as a Windows PE 5.0 disk.

MORE INFO **WINDOWS PE 5.0**

To learn more about Windows PE 5.0, visit *http://technet.microsoft.com/en-us/library/hh825110.aspx*.

- **Enable Low-Resolution Video** This option starts the system with 640x480 display resolution. You might use this feature when the display settings you chose in the operating system are incompatible with your hardware and prevent you from seeing anything on the screen.
- **Last Known Good Configuration** This option is useful when a configuration change has prevented the system from starting. When you select this option, the system boots with the set of registry settings that were in place the last time the system booted successfully.

  For example, you could use this option when you install a device driver or application and you cannot successfully start the system immediately afterwards.
- **Debugging Mode** This mode can be used by developers who are troubleshooting operating system bugs.
- **Disable Automatic Restart on System Failure** This option prevents the system from rebooting after a system crash. It is useful when you want to prevent an endless loop of system restarts.

- **Disable Driver Signature Enforcement** By default, Windows Server 2012 will not load any kernel-mode software that isn't digitally signed. *Kernel mode software* refers to programs or drivers that run in the most protected parts of the operating system. *Digitally signed software* refers to programs and (especially) drivers that have been tested by Microsoft and whose bits have not been altered since they were approved.

  Windows will normally warn you before you install unsigned software, but in some cases, you might need to install and use unsigned drivers or applications. For example, your organization might develop software that is not yet signed but that needs to be used temporarily.

  For such occasions, choose the Disable Driver Signature Enforcement option to allow the software to load. Make sure you understand this option for the 70-412 exam.

- **Disable Early Launch Anti-Malware Driver** Malicious software that can load transparently before the operating system has proliferated in recent years. Instances of such malware, called *rootkits*, are difficult for traditional anti-malware software to detect. To remedy this problem, Windows Server 2012 introduces a new feature called Secure Boot. *Secure Boot* keeps unauthorized firmware, operating systems, and drivers from running at boot time by requiring the boot manager to be signed and pre-approved. If a problem is detected with the boot manager on the system and cannot be fixed, you will see a message indicating a Secure Boot Violation and the system will not start.

  Secure Boot is enabled by the early launch anti-malware driver. When you choose Disable Early Launch Anti-Malware Driver from the Advanced Boot Options menu, the computer will start in Safe Mode without first running the system's early-launch malware detection.

MORE INFO **SECURE BOOT**

To learn more about Secure Boot, search for "Secure Boot" on TechNet or visit *http://technet.microsoft.com/en-us/library/hh824987.aspx*.

Booting into Safe Mode: Alternatives with Bcdedit and Msconfig

If you are already in Windows, you can configure the system to boot into any of the three Safe Modes the next time the system starts. You can use either the Bcdedit command at the command prompt or the System Configuration Utility (Msconfig) in the GUI of Windows Server 2012 to make this configuration change.

In Bcdedit, type one of the following commands to boot the system on the next startup into Safe Mode, Safe Mode with Networking, or Safe Mode with Command Prompt, respectively:

```
Bcdedit /Set SafeBoot Minimal

Bcdedit /Set SafeBoot Network
```

```
Bcdedit /Set SafeBootAlternateShell True
```

To return to normal booting, then type the following:

```
Bcdedit /DeleteValue SafeBoot
```

To accomplish the same thing in Msconfig, select the Boot tab and then check Safe Boot, as shown in Figure 3-23. The next time the system starts, it will boot into the option you select here. Minimal is Safe Mode, Alternate Shell stands for Safe Mode with Command Prompt, and Network refers to Safe Mode with Networking. (The Active Directory Repair option refers to Directory Services Restore Mode, which is used on domain controllers to bring the Active Directory database offline for repairs.)

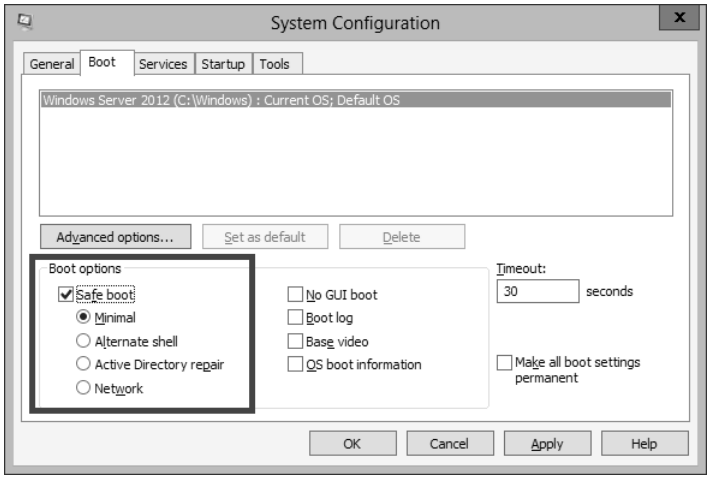

FIGURE 3-23 Booting into Safe Mode from Msconfig

Recovering servers with the Windows installation media

The Advanced Boot Options menu discussed in the previous section presents useful recovery options when Windows Server 2012 or Windows Server 2012 R2 can at least begin the process of loading. Other times, however, Windows doesn't even begin to load. On these occasions, you can boot with Windows Server 2012 or Windows Server 2012 R2 installation media and enter into Setup. When you get to the Windows Setup screen shown in Figure 3-24, choose the Repair Your Computer option. This step launches the Windows Recovery Environment, also called Windows RE. The Windows Recovery Environment (RE) runs on the Windows PE operating system. Windows PE is a version of Windows that is small enough to run on a DVD or a USB drive.

EXAM TIP

Windows RE is based on the Windows PE operating system. When you boot from Windows Server installation media, a text file named Startnet.cmd is read that includes commands used to launch the Windows PE operating system and load network resources. By using your own media, you can create and save a custom version of Windows RE that includes additional commands saved in this Startnet.cmd text file. For example, you can add a Net Use command to map a network drive if you want to make a network drive available in your Windows RE.

FIGURE 3-24 Recovering a server by using the Windows Server 2012 installation media

The Choose An Option screen of the Windows Recovery Environment is shown in Figure 3-25.

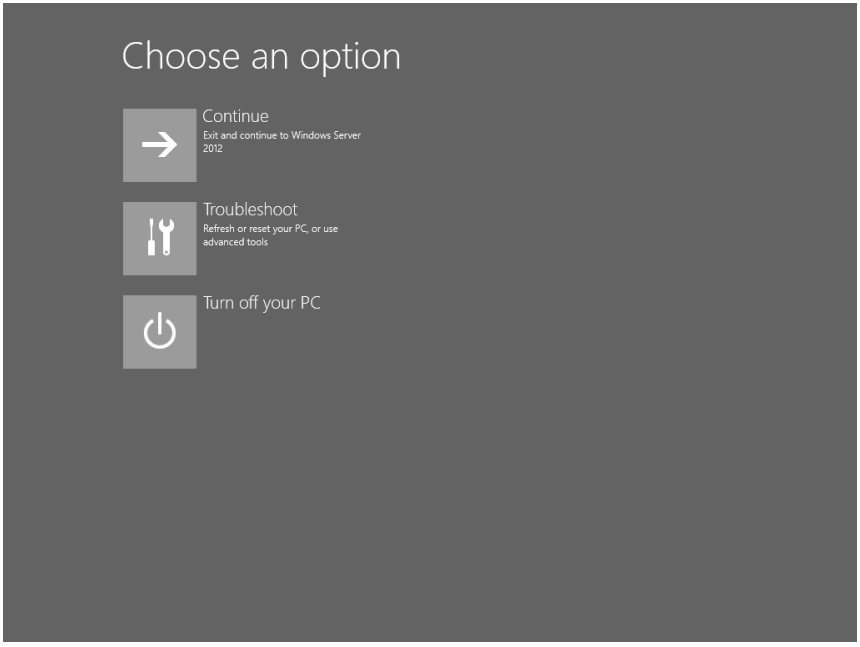

FIGURE 3-25 The Choose An Option screen in Windows RE

Click Troubleshoot to present the default troubleshooting options on the Advanced Options screen, shown in Figure 3-26.

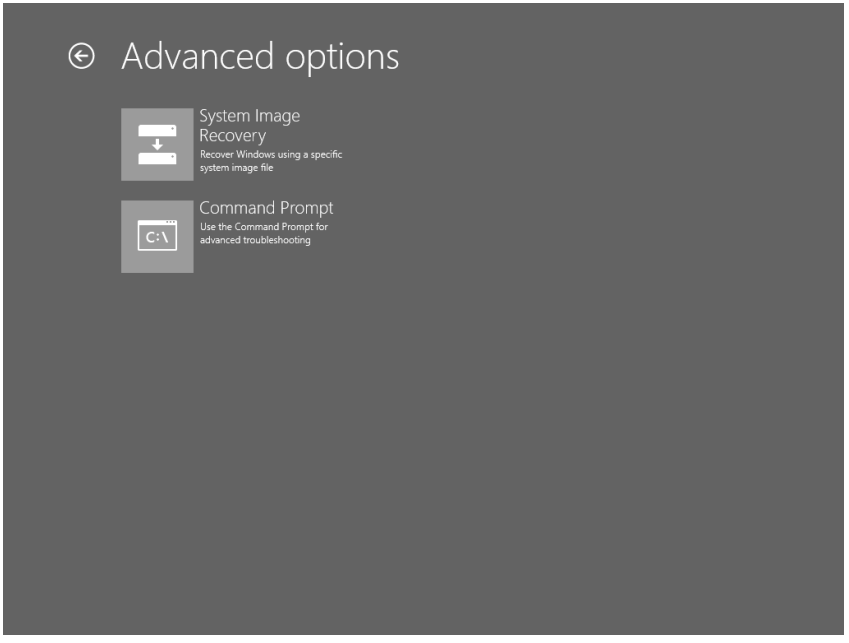

FIGURE 3-26 The Advanced Options screen in Windows RE

As you can see in Figure 3-26, the two built-in troubleshooting tools provided in the Windows Recovery Environment are System Image Recovery and Command Prompt. You can use System Image Recovery to restore a full server backup on a server that doesn't boot. You can use Command Prompt to repair the boot record by using Bootrec, Startrep, or other commands (or to perform any other troubleshooting).

Configuring System Image Recovery

When you select System Image Recovery after booting with Windows installation media, your disks are scanned for a Windows image backup (VHD or VHDX file). If one or more backup is found, you are given an opportunity to restore the most recent. If none is found, you can select one manually, as shown in Figure 3-27.

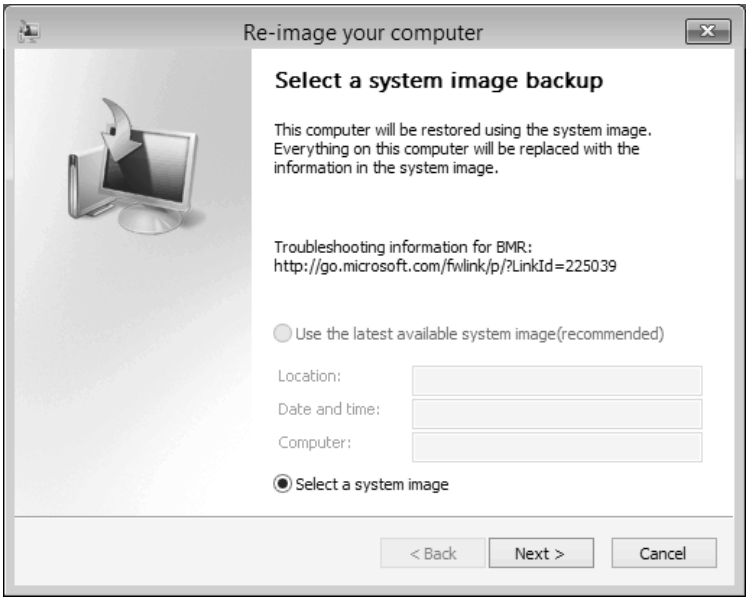

FIGURE 3-27 Recovering from a backed up system image

You should perform System Image Recovery from Windows installation media when you have a backup of your Windows Server 2012 R2 installation and either of the following is also true:

- You want to move the image to a new computer. (The hardware on the new computer should be identical to the old one so that the drivers contained in the image will work with the new hardware.)
- The disks or disk array on your server has been replaced (for example, because of hardware failure or data corruption).

MORE INFO **CUSTOMIZING WINDOWS RE**

To learn more about customizing Windows RE, visit *http://technet.microsoft.com/en-us/library/hh825125.aspx*.

Using command-line recovery tools

The Windows RE command prompt opens at the X:\Sources path by default. From this prompt, you can use a number of command-line tools to recover a Windows Server installation, such as Startrep, Bootrec, and Bcdedit.

EXAM TIP

Make sure you remember all of these command-line recovery tools for the 70-412 exam.

STARTREP

If the registry has become so corrupted that the system cannot start, you can use Startrep.exe to perform an automatic startup repair. Startrep.exe is located in the X:\Sources\Recovery directory, so you have to enter the command **cd recovery** before you can use Startrep.

BOOTREC

To understand the function of this utility, you first need to understand the difference between the boot sector, the Master Boot Record (MBR), and the Boot Configuration Data (BCD) store.

- The *boot sector* is the first sector of a bootable drive. The boot sector provides instructions about how to boot from that drive.
- The *MBR* is a type of boot sector used only in disks partitioned in the MBR partition style. This record contains information about the partitions on the drive. It also contains instructions about how to load the operating system.
- The *BCD store* is a binary file that contains the boot configuration data in Windows. The BCD maintains a record of the operating systems installed on the local disks and controls how operating systems load, in which order (and in which manner) they are presented in the boot menu, and which operating system is set as the default.

The *Bootrec.exe* utility is useful in performing basic repairs of the boot sector, the MBR, and the BCD store. It's used with four options, described below:

- **Bootrec /FixBoot** This option writes a new boot sector to the system partition. Use this option if the boot sector has been damaged or if a version of Windows earlier

than Windows Vista or Windows Server 2008 has been installed on the system after Windows Server 2012 or Windows Server 2012 R2.

- **Bootrec /FixMbr** This option should be used only with disks partitioned with an MBR partition style, not with disks partition with a GUID Partition Table (GPT) partition style. (GPT disks are very common in Windows Server 2012 systems.) For MBR-type disks, the /FixMbr option writes an MBR to the system partition. Use this option to repair master boot record corruption issues or to remove nonstandard code from the MBR.
- **Bootrec /ScanOs** This option scans all disks for Windows installations, including those that aren't currently listed in the BCD store.
- **Bootrec /RebuildBcd** This option scans all disks for Windows installations and lets you add detected installations to the BCD store.

BCDEDIT

Bcdedit.exe is the main command-line editor of the BCD store. One of the main reasons to use Bcdedit is so you can modify boot entries, which are the options that define each operating system available on the boot menu. You don't normally need to edit the boot entries from Windows RE unless the BCD store has become corrupted or improperly modified. If you've used the Bcdedit /export command to back up a functioning version of the BCD store, you can use the Bcdedit /import command in Windows RE to restore store that backed up version if necessary.

BCDBOOT

You can use Bcdboot to quickly rebuild a new BCD store if the old one has become corrupted and you don't have a backed up version to restore.

Thought experiment

Configuring server recovery at Contoso

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

You are in the process of developing documentation to assist in the diagnosis and recovery of servers running the Windows Server 2012 R2 operating system which have been deployed on physical hardware. You are working on the section related to choosing boot options and need to answer the following questions before you can proceed:

1. **Which boot option would you enable to determine the last service or driver to load before the system freezes?**
2. **What is the name of the file that records this information and where is it located?**
3. **Which boot option should you select to start the system using the configuration that was in place the last time a successful sign-on occurred?**

Objective summary

- You can troubleshoot a Windows installation that at least begins the process of loading by using advanced boot options. To access the Advanced Boot Options menu, press F8 as the system is starting.
- The Advanced Boot Options menu includes Safe Mode, which loads only minimal drivers; Last Known Good Configuration, which loads the last version of the Registry that allowed a system to completely start; and Disable Driver Signature Enforcement, which allows Windows to load unsigned drivers.
- If Windows doesn't even begin to start, you can recover the system by booting from Windows Server 2012 or Windows Server 2012 R2 installation media. You can then click Troubleshooting to enter the Windows Recovery Environment.
- If you want to recover your installation from backup onto a bare-metal system in the Windows Recovery Environment, choose the option to perform a System Image Recovery.
- If you want to troubleshoot your installation in the Windows Recovery Environment, choose the Command Prompt option. From there, you can use command-line tools such as Startrep to perform automatic startup repair; Bootrec to repair the boot sector, MBR, or BCD store; Bcdedit to restore a backed up version of the BCD store; or Bcdboot to quickly rebuild the BCD store.

Objective review

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

1. You want to ensure that a server running Windows Server 2012 R2 boots into Safe Mode the next time it starts.

   Which commands can you use to achieve this goal? (Choose all that apply.)

   A. Bootrec

   B. Bcdedit

   C. Startrep

   D. Msconfig

2. Your company is preparing to migrate a server named Server1 from Windows Server 2003 to Windows Server 2012 R2. A developer at your company is working to update a kernel mode driver installed on Server1 that has been developed in-house. He installs the driver for testing on TestServer1. TestServer1 is running Windows Server 2012 R2 and has hardware that is identical to that of Server1. After he installs the program, TestServer1 fails to start. You need to ensure that he can test the driver on TestServer1. You also want to minimize the security risk on the machine. Which option should you choose from the Advanced Boot Options menu?

   A. Safe Mode

   B. Last Known Good Configuration

   C. Disable Driver Signature Enforcement

   D. Disable Early Launch Anti-Malware Driver

3. You are a network administrator for Contoso.com. All servers in the company network are running Windows Server 2012 R2.

   The disk array fails on a file server named FileSrvA. You replace the disk array. You now need to recover the server as quickly as possible and allow users to connect to the file shares on FileSrvA. What should you do?

   A. Start FileSrvA in the Last Known Good Configuration

   B. Start FileSrvA from the Windows Server 2012 R2 installation media

   C. Start FileSrvA in Safe Mode with Command Prompt

   D. Initiate a network boot of FileSrv to connect to a WDS server.

Objective 3.3: Configure site-level fault tolerance

Hyper-V Replica is a Windows Server 2012 and Windows Server 2012 R2 feature introduced in that allows you to create a replica of a virtual machine running on Hyper-V on either of these platforms. If the primary VM fails, you can fail over to the replica VM. Hyper-V Replica can thus provide fault tolerance for a VM even if an entire host site should go offline.

Unlike a failover cluster, Hyper-V Replica doesn't rely on shared storage between the VMs. The replica VM instead begins with its own copy of the primary VM's virtual hard disk. The primary VM then sends updates of its changes (called *replication data* and this data is repeatedly saved by the replica VM. Replication frequency is every 5 minutes for Hyper-V on Windows Server 2012 and either 30 seconds, 5 minutes, or 15 minutes when Hyper-V is running on Windows Server 2012 R2.

This objective covers how to:

- Configure Hyper-V physical host servers
- Configure VMs
- Perform Hyper-V Replica failover
- Use Hyper-V Replica in a failover cluster
- Configure Hyper-V Replica Extended Replication
- Use Global Update Manager
- Recover multi-site failover clusters

Configuring Hyper-V physical host servers

It's important to understand the sequence of steps in configuring Hyper-V Replica. The first step is to configure the server-level replication settings for *both* physical Hyper-V hosts, called the primary server and the replica server. You can access these settings in Hyper-V Manager by right-clicking a host server in the navigation pane, selecting Hyper-V Settings, and then selecting Replication Configuration in the left column of the Hyper-V Settings dialog box, as shown in Figure 3-28. By default, replication is not enabled, and no options are selected or configured.

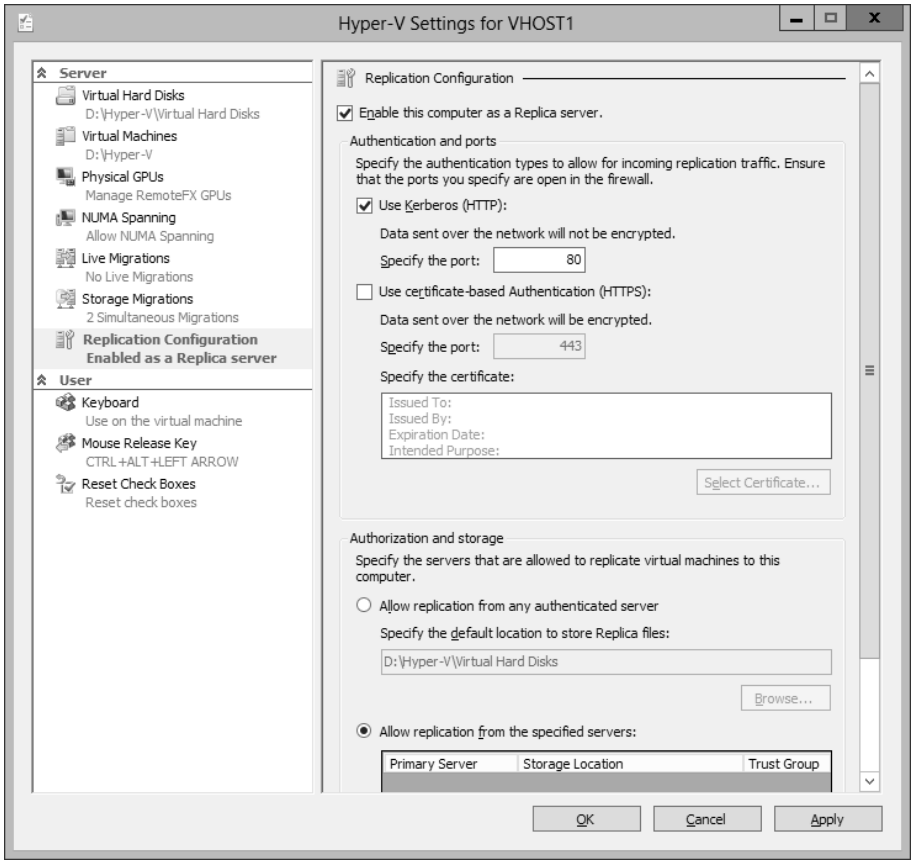

FIGURE 3-28 The host server settings for Hyper-V Replica

To enable a physical host for Hyper-V Replica, first select the Enable This Computer As A Replica Server check box. Then, configure settings in the Authentication And Ports area and the Authorization And Storage area shown in Figure 3-28. You need to repeat these configuration steps on both primary and replica servers before configuring a VM for replication.

- **Authentication And Ports** In this area you choose which authentication methods you want to be available later as options when you configure a locally hosted VM for replication. You can enable Kerberos (HTTP), Certificate-Based Authentication (HTTPS), or both.
  - **Use Kerberos (HTTP)** You can enable Kerberos (HTTP) only if the local server is domain-joined. The advantage of choosing Kerberos is that it requires no further configuration. The two disadvantages are first that it doesn't encrypt data sent over the network, and second that it can be used for authentication only when the remote host server is located in a trusted domain. Note also that when you choose this authentication protocol, you need to enable the firewall rule named Hyper-V Replica HTTP Listener (TCP-In).

- **Use Certificate-Based Authentication (HTTPS)** You can enable Certificate-Based Authentication (HTTPS) regardless of whether the local server is domain-joined. In fact, when the local server is a standalone server, it is the only authentication protocol option. The two advantages of enabling Certificate-Based Authentication (HTTPS) are that it encrypts replication data and that it allows you to replicate with a remote host when there is no trust relationship with that host through Active Directory. The disadvantage of this authentication method is that it is more difficult to configure: It requires you to provide an X.509v3 certificate for which Enhanced Key Usage (EKU) must support both Client Authentication and Server Authentication (through the Computer certificate template, for example) and that specifies (typically) the fully qualified domain name (FQDN) of the local server in the subject name field. The certificate can be self-signed or issued through a public key infrastructure (PKI). When you choose this authentication protocol, you need to enable the firewall rule named Hyper-V Replica HTTPS Listener (TCP-In).

It's important to remember that Windows Server 2012 doesn't automatically enable the firewall rules you need for the authentication protocols you choose. Depending on which protocol(s) you have enabled, you also need to enable the firewall rule Hyper-V Replica HTTP Listener (TCP-In), Hyper-V Replica HTTPS Listener (TCP-In), or both. You can enable a rule either in Windows Firewall with Advanced Security or by using the Enable-NetFirewallRule -DisplayName command in Windows PowerShell followed by the name of the rule (including quotation marks).

EXAM TIP

Remember that encrypted replication of a VM requires the host servers to have installed a certificate including both Client Authentication and Server Authentication extensions for EKU.

MORE INFO **CONFIGURING CERTIFICATE-BASED AUTHENTICATION WITH HYPER-V REPLICA**

To learn more about configuring certificate-based authentication with Hyper-V Replica, search for Hyper-V Replica - Prerequisites for certificate-based deployments or visit *http://blogs.technet.com/b/virtualization/archive/2012/03/13/hyper-v-replica-certificate-requirements.aspx*.

When configuring replication, you must also configure the following settings:

- **Authorization And Storage** This area allows you to configure security settings on the local server that are used when the local server acts as a replica server. More specifically, your choice here determines the remote primary servers from which the local server will accept replication data. Even if you are configuring your local server as the primary server, the settings here are required so that—if you ever need to fail over to a remote replica—you can later fail back to the local server.

You need to choose one of two security options, both of which also provide a default path you can modify to store replication data:

- **Allow Replication From Any Authenticated Server** This option is somewhat less secure. When you choose this option, the local server can receive replication data from any authenticated server.
- **Allow Replication From The Specified Servers** This option requires you to specify the primary server(s) authorized for the local replica server. You can add multiple entries to authorize different primary servers by DNS name. To add an entry authorizing a primary server address, click Add as shown in Figure 3-29. This step opens the Add Authorization Entry dialog box shown in Figure 3-30.

For each entry, a default storage path (the middle field) is already provided, but the other two fields must be filled in manually. In the Specify The Primary Server field, you enter an FQDN that can include a wildcard character (for example, "*.adatum.com"). You also have to provide a tag called a trust group. If you want to allow replication traffic from a set of primary servers, you should assign those primary servers the same trust group name.

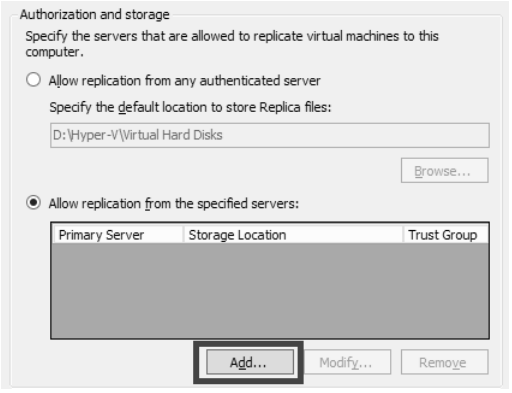

FIGURE 3-29 Authorizing primary servers for the local replica server

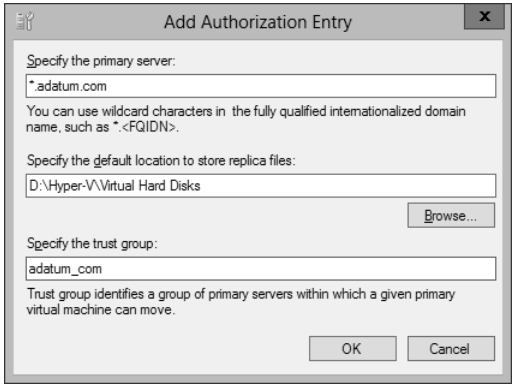

FIGURE 3-30 Adding an authorized primary server address

How might these settings in the Authorization And Storage area appear on the 70-412 exam? One could imagine a question based on an unsuccessful failover. In such a question, authorization settings might not be configured at all on the replica server. Or the FQDN provided in the Specify The Primary Server field in Figure 3-30 might be configured incorrectly, and the correct answer fixes that problem. Another possible question could involve a new organizational requirement that security be tightened on a replica server. Incorrect answer choices might refer to IPSec or other security-tightening methods, but the correct answer will refer to adding an authorization entry on the replica server.

Configuring VMs

After you configure both physical host servers, the next step in configuring Hyper-V Replica is to configure the chosen VM for replication on the primary server. Begin by right-clicking the VM and selecting Enable Replication, as shown in Figure 3-31.

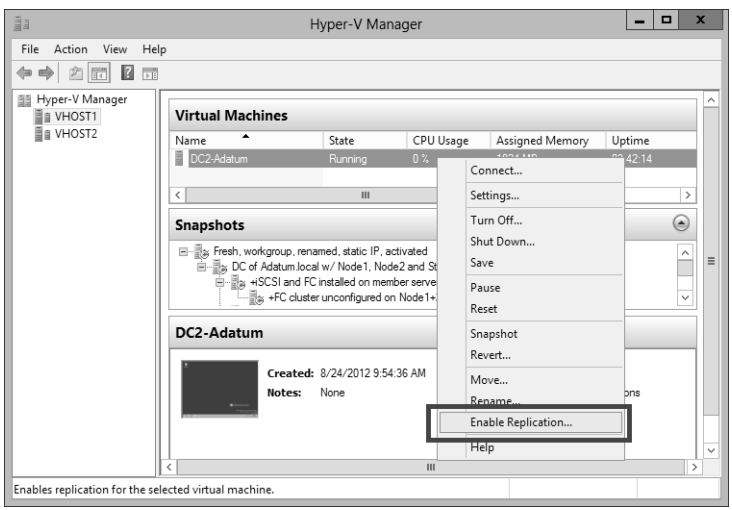

FIGURE 3-31 Creating a replica of a virtual machine

This step opens the Enable Replication wizard. The wizard includes the following five configuration pages:

- **Specify Replica Server** Use this page to specify the remote replica server by name.
- **Specify Connection Parameters** This page, shown in Figure 3-32, asks you to specify which of the authentication types enabled at the server level in Hyper-V Settings you want to use to support this replicated VM. If you have enabled only one of these two authentication methods at the server level, that same method is the only option here. Naturally, the replica server must support the same authentication method.

  This page also provides an option that lends itself fairly well to an exam question: the Compress The Data That Is Transmitted Over The Network check box. This compression option reduces bandwidth requirements for replication at the expense of increased processor usage. If this option does appear on the exam, this trade-off is likely to be the key to getting the right answer.

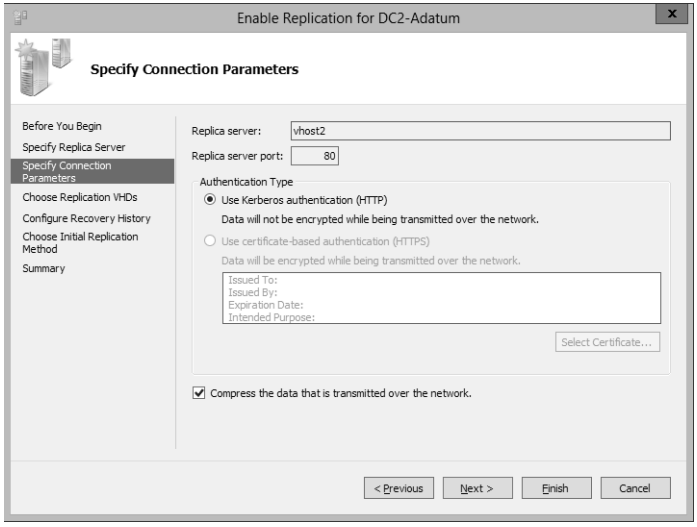

FIGURE 3-32 Selecting authentication and compression settings for a replicated VM

EXAM TIP

If both authentication types are available for the VM and you want to change the authentication type later to certificate-based authentication, you have to remove replication and complete the Enable Replication wizard again. Before you do, however, make sure that certificate-based authentication is also enabled in the Hyper-V Settings on the remote host server.

- **Choose Replication VHDs** By default, all virtual hard disks (VHDs) attached to the VM are enabled for replication. You can use this page to deselect any VHDs that you don't want to be replicated.
- **Configure Additional Recovery Points** This page, shown in Figure 3-33, includes the settings to Configure Additional Recovery Points. These are among the most likely of all Hyper-V Replica settings to appear on the 70-412 exam. As shown in the figure, you can configure Only The Latest Recovery Point or Additional Recovery Points.

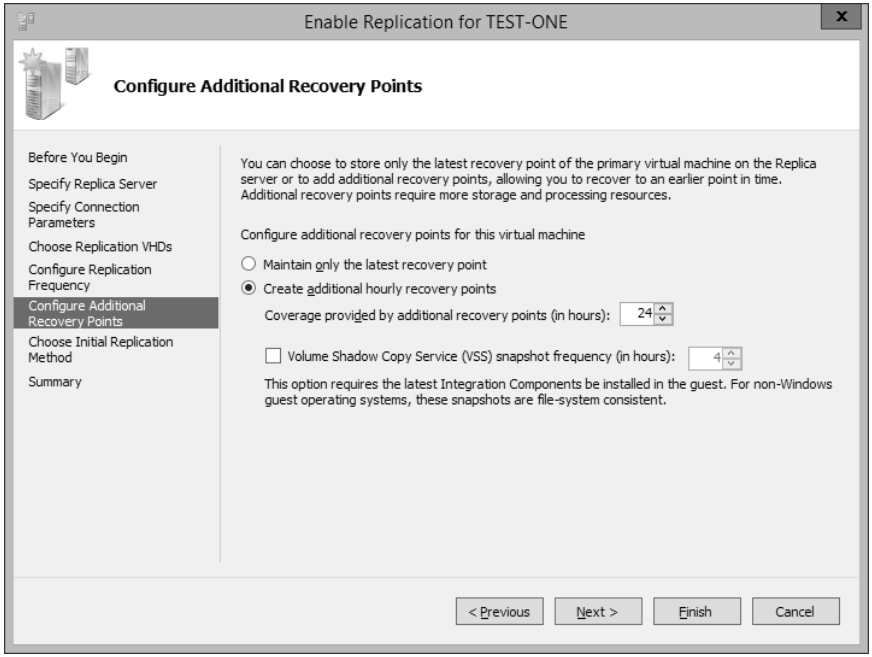

FIGURE 3-33 Configuring additional recovery points

Recovery points are VM snapshots saved on a replica server. Replication traffic sends a new snapshot from the primary to the replica server every 5 to 15 minutes, but only the latest is saved on the replica by default. Selecting the Additional Recovery Points option configures the replica server to keep one extra snapshot per hour. If you later perform a failover operation at the replica server, you then have the option of recovering either the most recent version of the VM, which is always available, or one of these earlier, hourly snapshots. Windows Server 2012 R2 increases the number of maximum recovery points to 24 from the 16 that are available in Windows Server 2012.

A menu of available recovery points on a replica server is shown in Figure 3-34. If the Configure Recovery History page were left at the default setting (Only The Latest Recovery Point), only the first option named Latest Recovery Point would appear in this menu.

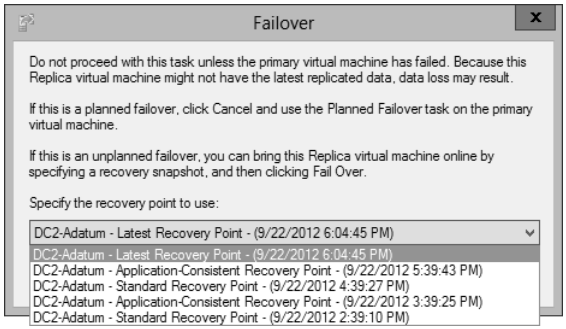

FIGURE 3-34 Specifying the latest recovery point and previous hourly snapshots of a VM that can be restored in a failover on the replica server

When you enable the Additional Recovery Points option on the Configure Recovery History page, the replica server by default will keep an hourly snapshot for each of the past four hours in addition to the latest recovery point. However, you can change this setting if you want to store more (or fewer) of these recovery points on the replica server. The main drawback to keeping many recovery points is the use of storage resources required to do so.

The last configuration settings on the Configure Recovery History page relate to *incremental Volume Shadow Copy Service (VSS) copies*, also known as *application-consistent recovery points*. These are high-quality snapshots taken during moments in which the VM momentarily "quiesces" (gracefully pauses) activity in VSS-aware applications such as Microsoft Exchange and SQL Server. The advantage of these snapshot types is that they help ensure that the failover will be free of errors in these applications. The disadvantage is that they are more processor-intensive and cause important applications to pause briefly. (However, it should be noted that the pause is normally too brief for users to detect.)

You enable incremental VSS copies by selecting the Replicate Incremental VSS Copy Every check box, and then selecting the frequency of the application-consistent recovery point. (You can see these options in Figure 3-33.) If you leave the default frequency of 1 hour, then every recovery point will be an application-consistent recovery point. If you select a frequency of 2 hours, then the standard recovery point will be replaced by an application-consistent recovery point every 2 hours, and so on. Figure 3-35 shows the snapshots stored on a replica server for which incremental VSS copies are scheduled every two hours.

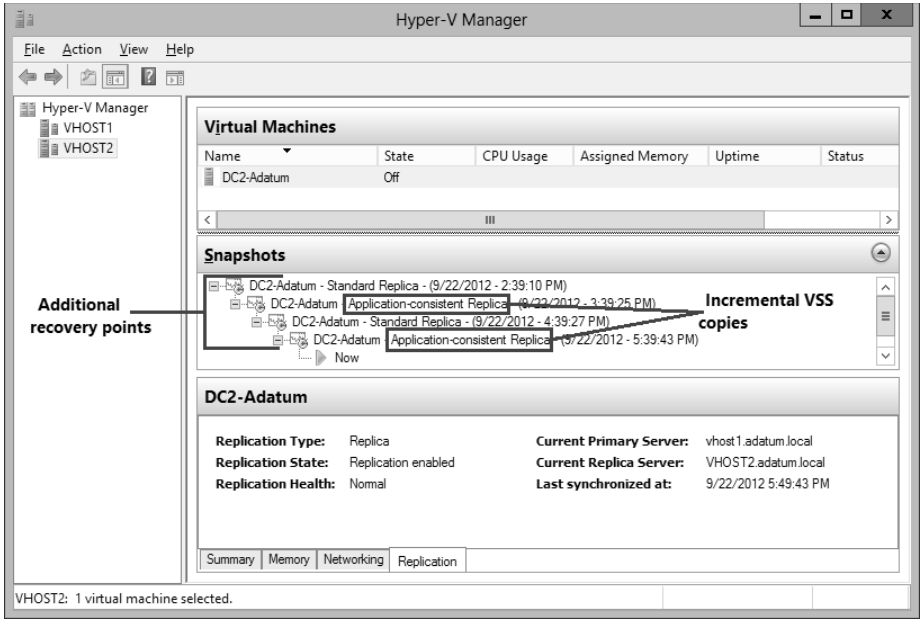

FIGURE 3-35 Viewing incremental VSS copies and standard recovery points

EXAM TIP

Be prepared to answer a question about application-consistent snapshots on the 70-412 exam.

- **Choose Initial Replication Method** This page, shown in Figure 3-36, allows you to specify how the initial copy of the VHDs attached to the primary VM will be sent to the replica server. By default, the VHDs are sent over the network. Sending very large files over a network such as the Internet isn't always a realistic option, however. As an alternative, you can choose the second option, to export the VHDs to external media (and then physically transport them to the replica server). The final option is to use an existing VM on the replica server as the initial copy. You can choose this option if you have restored an exact copy of the VM and its VHDs on the replica server.

  This page also allows you to configure the initial network transfer to take place at a specified future time. You can use this option to minimize user disruption.

NOTE **BANDWIDTH**

Typically, the initial transfer of the VHD is far more bandwidth-intensive than the updates sent through replication are. After the initial copies of the VHDs are sent, only the changes (deltas) to these VHDs are sent during replication, which occurs every 5 to 15 minutes.

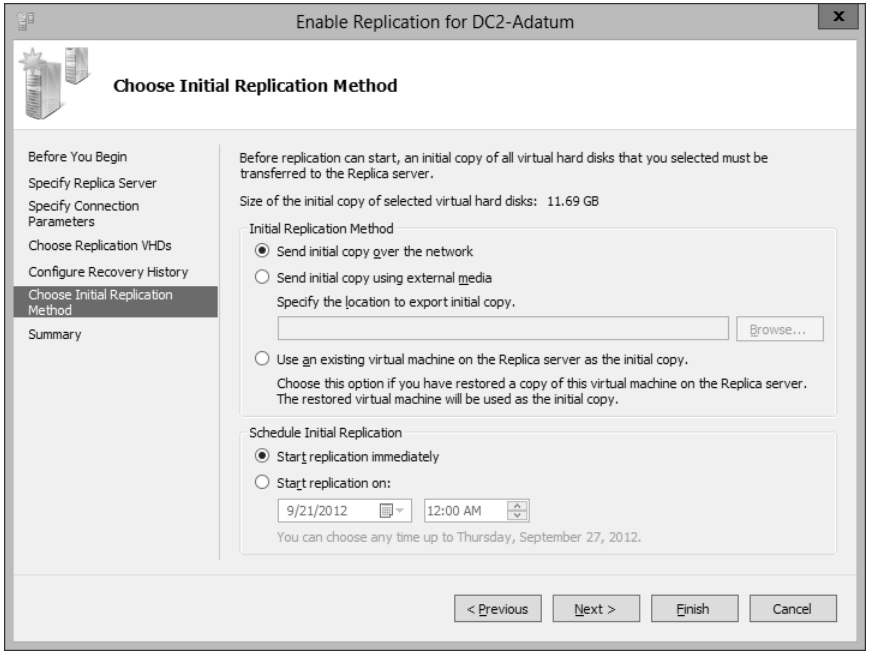

FIGURE 3-36 Determining how to send the base copy of the VHDs attached to a primary VM

Configuring failover TCP/IP settings

After you enable replication on a VM, you might need to specify the TCP/IP settings that will apply to the replica VM after failover. By default, the replica VM will inherit the same IPv4 and IPv6 configuration as the primary VM. In many cases, however, the replica VM will need a different IP configuration to communicate in its environment.

To assign a different IP configuration to the replica VM, in Hyper-V Manager on the replica server, right-click the replica VM and select Settings from the shortcut menu. In the Settings dialog box, expand Network Adapter in the left column and then select Failover TCP/IP, as shown in Figure 3-37. In the right pane, assign the new IP configuration as appropriate.

Then, on the primary server, assign the original IP configuration in the same settings area. Otherwise, the replica settings will persist if you fail back to the original location. (Remember this last point for the exam.)

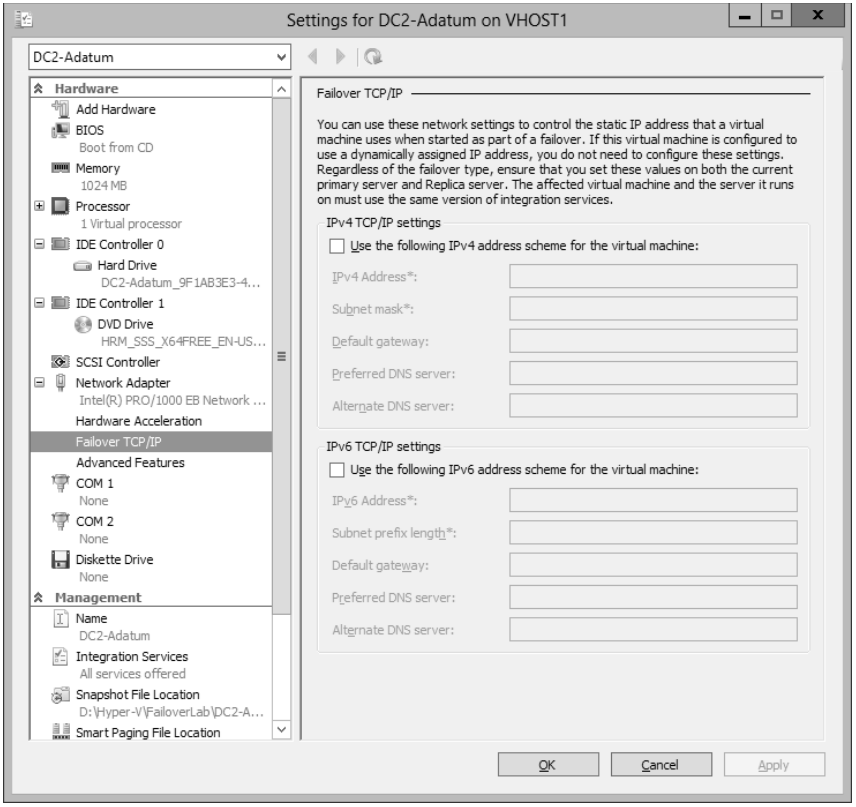

FIGURE 3-37 Assigning a different IP configuration to a replica VM

Resynchronizing the primary and replica VMs

After you complete the Enable Replication wizard, you can modify the replication settings for a VM in the Settings dialog box for that VM. Replication settings appear in the Management category in the menu on the left, as shown in Figure 3-38.

One configuration setting appears here that does not appear in the Enable Replication wizard: Resynchronization. Resynchronization is a highly resource-intensive operation that is performed occasionally between a primary and replica VM. By default, resynchronization can occur at any time. You have the option, however, to restrict resynchronizations to selected off-peak hours. Alternatively, you can opt to perform resynchronization manually.

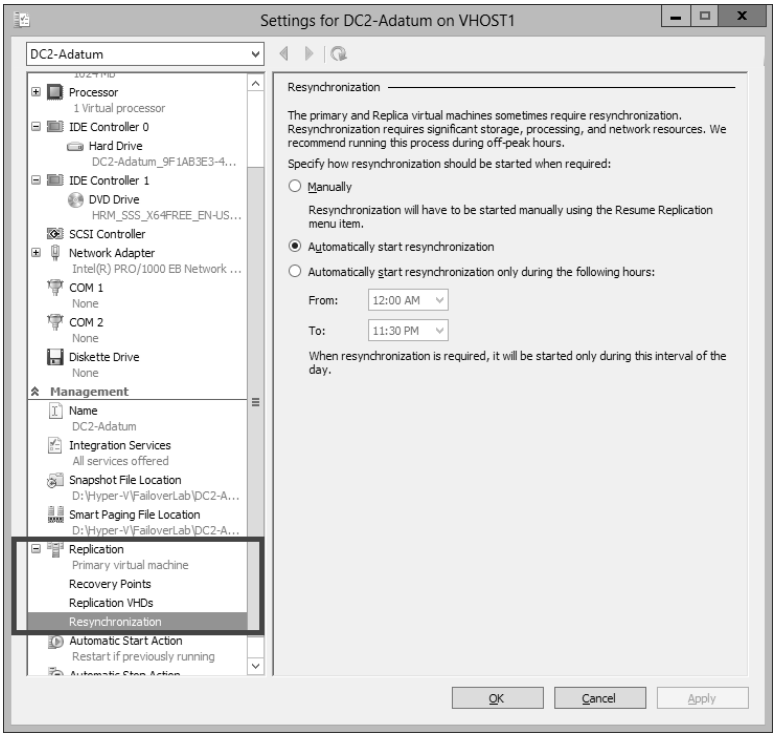

FIGURE 3-38 Replication settings for a VM

Performing Hyper-V Replica failover

You can perform three types of failovers with Hyper-V Replica after it is configured: planned failovers, unplanned failovers, and test failovers. It's somewhat likely you'll see an exam question in which you need to understand the difference among them and when they are used.

Planned failover

A *planned failover* is the only failover you initiate from the primary server. You use this method whenever you can manually shut down the primary VM, and the primary and replica servers can still communicate.

A planned failover is the preferred failover type because no data is lost. In fact, you cannot even use this option to fail over to the latest recovery point or to any earlier recovery point. With a planned failover, only an exact copy of the current primary VM and its VHDs can be failed over to the replica server.

A planned failover is a good option in the following situations:

- You want to perform host maintenance on the primary server and temporarily want to run the VM from the replica.
- Your primary site is anticipating a possible power outage and you want to move the VM to the replica site.

- You are expecting a weather emergency, such as a flood, and you want to ensure business continuity.
- Your compliance requirements mandate that you regularly run your workloads for certain periods of time from the replica site.

To perform a planned failover, you begin by *shutting down the primary VM*. You then right-click the VM in Hyper-V Manager, click Replication, and then click Planned Failover, as shown in Figure 3-39. The latest updates are then sent to the replica server, the VM is failed over, and the replica VM is automatically started on the remote server. At the end of this operation, the replication relationship is reversed, so what was the replica server becomes the primary server, and vice versa.

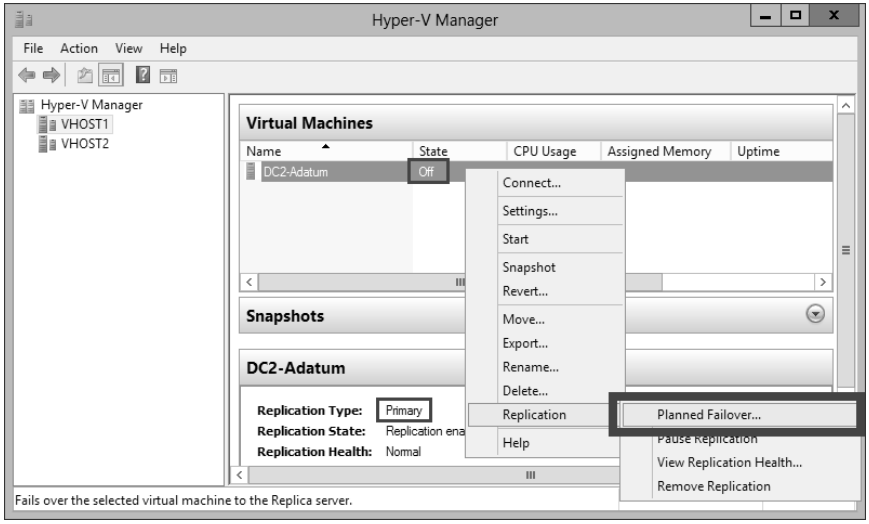

FIGURE 3-39 Performing a planned failover from the primary server

Unplanned failover

This type of failover is called an *unplanned failover* in the Windows Server 2012 and Windows Server 2012 R2 documentation, but in the actual interface, it's called just "failover." On the 70-412 exam, you might see it referred to either way.

An unplanned failover is performed at the replica server. You perform this failover type when the primary VM fails suddenly and cannot be brought back online. An unplanned failover is a good option in the following situations:

- Your primary site experiences an unexpected power outage or a natural disaster.
- Your primary site or VM has had a virus attack, and you want to restore your business quickly with minimal data loss by restoring your replica VM to the most recent recovery point before the attack.

To perform an unplanned failover, in Hyper-V Manager on the replica server, right-click the replica VM, click Replication, and then click Failover, as shown in Figure 3-40.

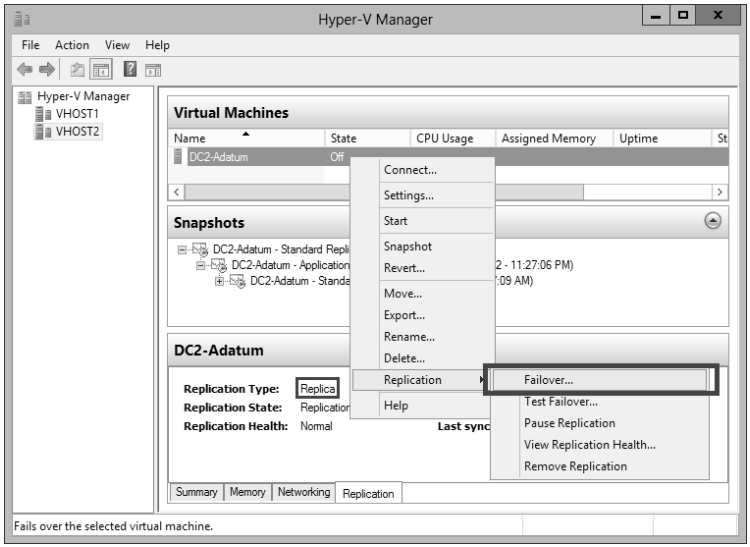

FIGURE 3-40 Performing an unplanned failover on the replica server

When you perform an unplanned failover, you have to choose a recovery point, as shown earlier in Figure 3-34. The VM is then started on the replica server.

After the replica VM is started, the replica relationship with the primary VM is broken, and replication stops. If at some later point you can bring the original primary VM online, you can resume replication by reversing the replication relationship. After you perform this operation, the local replica server becomes the new primary, and the remote primary becomes the new replica. To reverse replication in this way, right-click the VM on the replica server, click Replication, and then click Reverse Replication, as shown in Figure 3-41. This step starts the Reverse Replication Wizard, which allows you to reenter the settings for the replica.

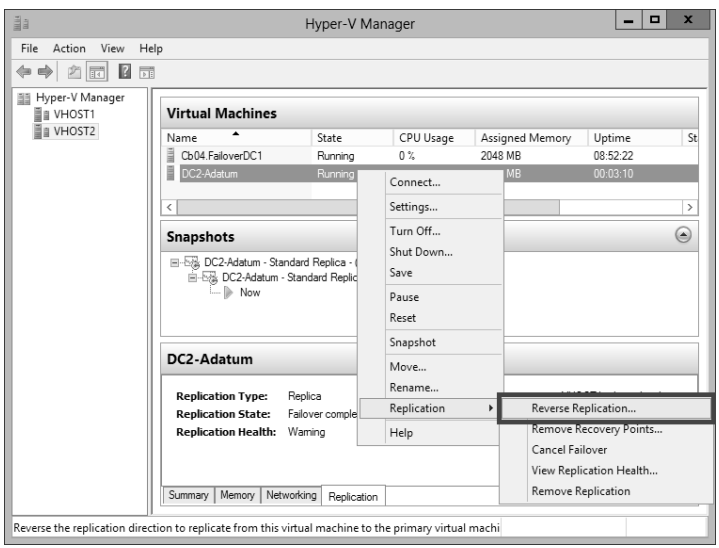

FIGURE 3-41 Reversing replication

Another option you can see on the Replication submenu in Figure 3-41 is Cancel Failover. You can safely choose this option after you perform an unplanned failover as long as no changes have been made to the replica. After you cancel a failover, you have to manually resume replication on the primary VM by right-clicking it and selecting Resume Replication. Cancelling a failover is a good idea if you quickly discover after performing an unplanned failover that the primary VM can be brought online.

EXAM TIP

Remember the Reverse Replication option and the Cancel Replication option for the exam.

Test failover

A *test failover* is the only failover operation you can perform while the primary VM is still running. The purpose of this failover type is to simulate an unplanned failover so that you can ensure that it will function as planned in case of an emergency.

To perform a test failover, in Hyper-V Manager on the replica server, right-click the replica VM, click Replication, and then click Test Failover. You then have to select a recovery point, just as you do with an unplanned failover. Next, a local, disposable copy of the replica VM is created on the replica server. The new copy of the VM appears in Hyper-V Manager in a stopped state with the tag "- Test." For example, a test failover of a VM named "MyVM1" would result in a new VM called "MyVM1 - Test". You can then start the new VM manually to see if it works as expected.

By default, the virtual network adapters of the test VM are disconnected from all virtual switches. If desired, you can preattach the adapter(s) of the test VM to a virtual switch of your choice. To do so, open the settings of the base replica VM, expand Network Adapter, and then click Test Failover, as shown in Figure 3-42. Make sure you choose a virtual switch that will not create any conflicts in a production network.

After you examine the functioning of the test VM, you can safely delete it in Hyper-V Manager.

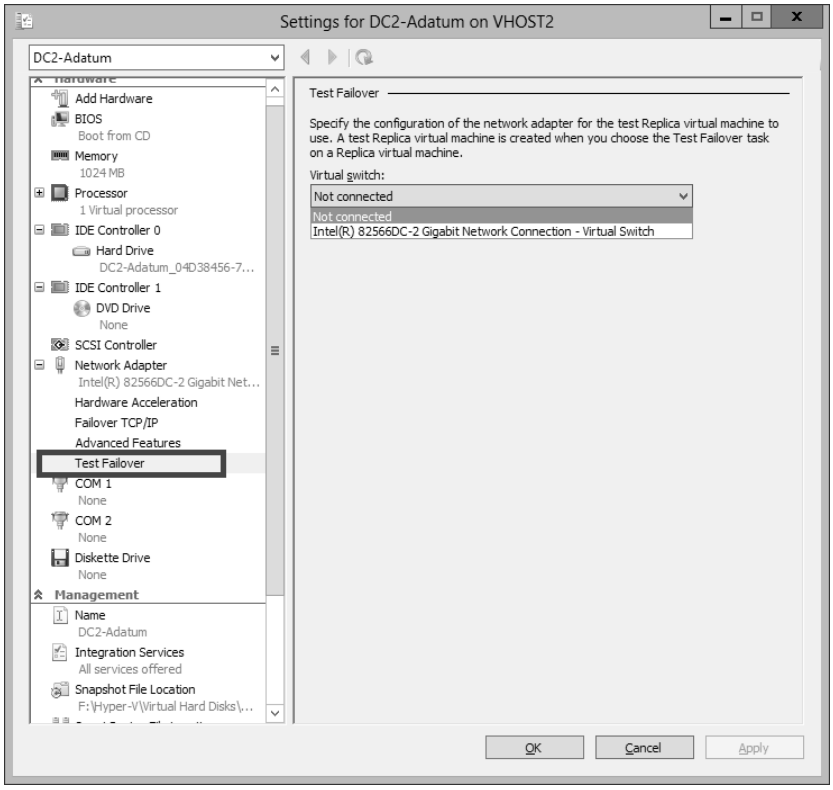

FIGURE 3-42 Preattaching the network adapter of a failover test VM to a virtual switch

Using Hyper-V Replica in a failover cluster

The configuration steps previously described apply to VMs that are not hosted in a failover cluster. However, you might want to provide an offsite replica VM for a clustered VM. In this scenario, you would provide two levels of fault tolerance. The failover cluster is used to provide local fault tolerance, for example, if a physical node fails within a functioning data center. The offsite replica VM, on the other hand, could be used to recover only from site-level failures, for example, in case of a power outage, weather emergency, or natural disaster.

The steps to configure a replica VM for a clustered VM differ slightly from the normal configuration, but they aren't complicated. The first difference is that you begin by opening Failover Cluster Manager, not Hyper-V Manager. In Failover Cluster Manager, you then have to add a failover cluster role named *Hyper-V Replica Broker* to the cluster.

To add the Hyper-V Replica Broker role, right-click the Roles node in Failover Cluster Manager and select Configure Role. This step opens the High Availability Wizard. In the High Availability Wizard, select Hyper-V Replica Broker, as shown in Figure 3-43.

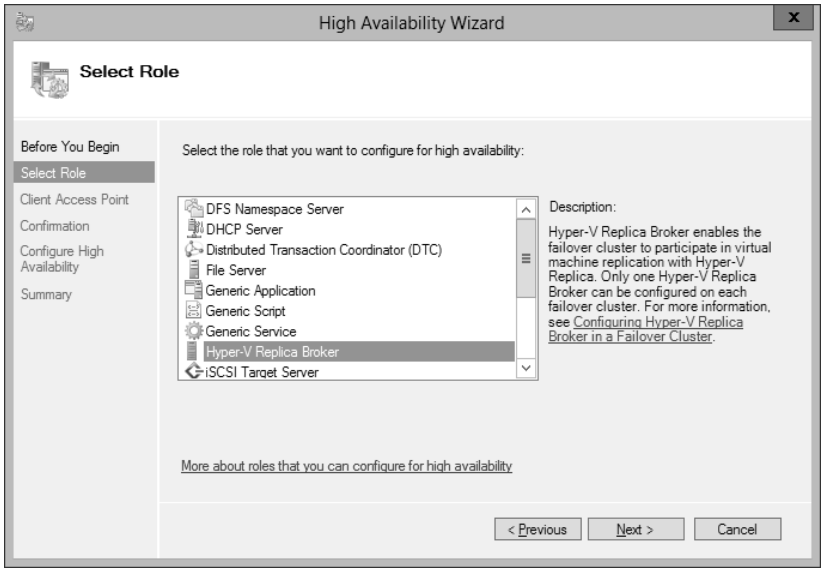

FIGURE 3-43 Adding the Hyper-V Replica Broker role to a failover cluster

When you choose this role, the High Availability Wizard will then ask you to provide a NetBIOS name and IP address to be used as the connection point to the cluster (called a *Client Access Point*, or *CAP*). This step is shown in Figure 3-44.

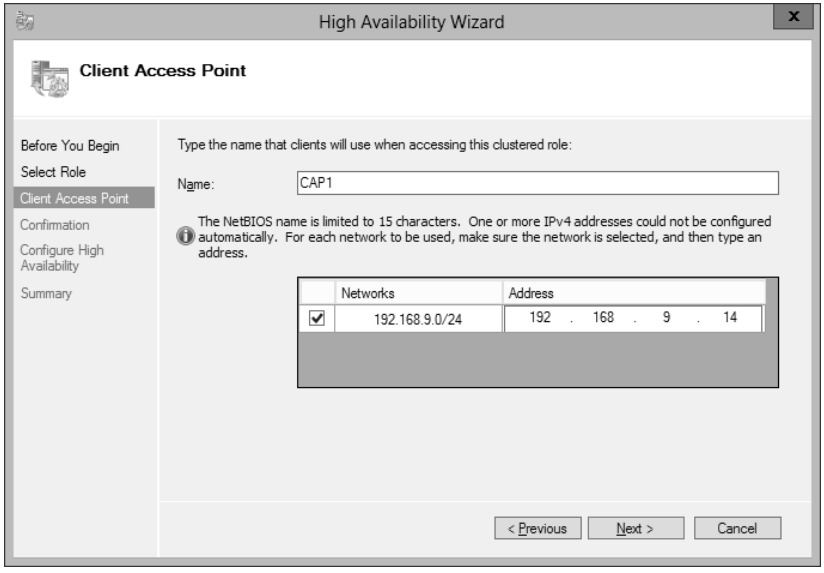

FIGURE 3-44 Providing a name and address for the Client Access Point

Next, you configure the equivalent of the server replication settings shown earlier in Figure 3-28. To do so, right-click the Hyper-V Replica Broker node in Failover Cluster Manager and

select Replication Settings from the shortcut menu, as shown in Figure 3-45. The difference between the settings here and the settings in Figure 3-28 is that in this case, the settings apply to the entire cluster as a whole.

FIGURE 3-45 Configuring replication settings for the cluster

On the remote Replica server, you configure replication as you normally would, by configuring Hyper-V Settings in Hyper-V Manager as described in the earlier section named "Configuring Hyper-V physical host servers." However, if you want the remote Replica also to be a multi-node failover cluster, then you would need to configure that remote failover cluster through Failover Cluster Manager (by adding and configuring the Hyper-V Replica Broker role).

After you configure the host server settings, you can configure replication on the VM in Failover Cluster Manager just as you would in Hyper-V Manager. Right-click the clustered VM, click Replication, and then click Enable Replication, as shown in Figure 3-46.

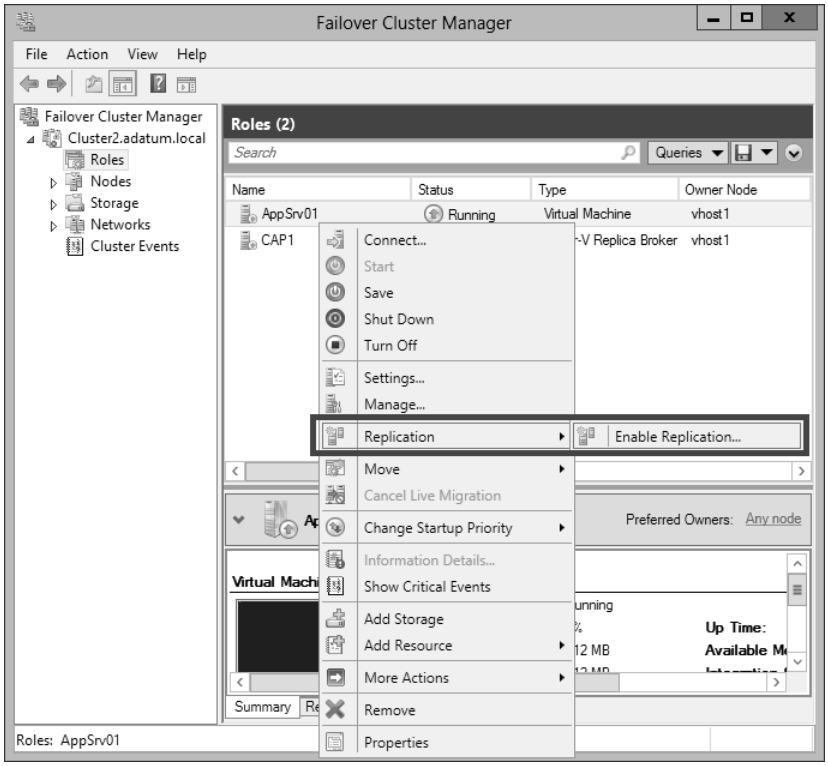

FIGURE 3-46 Enabling replication on a clustered VM

This step opens the same Enable Replication wizard that you see when you configure replication on a nonclustered VM. The remaining configuration steps are therefore identical.

For the 70-412 exam, there's a good chance you'll be asked about basic concepts related to configuring replication on clustered VMs. First, remember that you use Failover Cluster Manager to configure replication for a clustered VM at the primary site but still use Hyper-V Manager at the Replica site (if the Replica VM isn't also clustered). Also, remember that in Failover Cluster Manager at the primary site, you need to add the Hyper-V Replica Broker role to the failover cluster, and that this role is used to configure Hyper-V Replica "server" settings for the cluster. Finally, you also need to remember that when you configure Hyper-V Replica in a failover cluster, the CAP name and address are used as the server name and address.

Configuring Hyper-V Replica Extended Replication

Extended Replication is a feature available in Windows Server 2012 R2 that allows you to extend replication beyond the host and replica server to a third site. For example, you may have configured Hyper-V replica so that a VM hosted in the Melbourne datacenter is automatically replicated to a computer running Windows Server 2012 R2 with the Hyper-V role installed in the Sydney datacenter. With Hyper-V Extended Replication, you could then configure

replication so that the replica in the Sydney datacenter is replicated on to an additional computer running Windows Server 2012 R2 with the Hyper-V role installed that is located in the Canberra datacenter.

MORE INFO **HYPER-V EXTENDED REPLICATION**

To learn more about Hyper-V Extended Replication, visit *http://blogs.technet.com/b/virtualization/archive/2013/12/10/hyper-v-replica-extend-replication.aspx*

Using Global Update Manager

When the state of a cluster is changes, for example when a node is taken offline, all of the other nodes in the cluster must acknowledge the change before the cluster will commit the change to the cluster database. *Global Update Manager* is the component that is responsible for managing cluster database updates. Windows Server 2012 R2 allows you to configure Global Update Manager settings through the (Get-Cluster).DatabaseReadWriteMode Windows PowerShell command. Using this command, you can configure the following options:

- **0 = All (write) And Local (Read)** This is the default setting in Windows Server 2012 R2 for all cluster workloads except Hyper-V. It requires that all cluster nodes acknowledge the update before the change is committed to the database. Database reads occur on the local node.
- **1 = Majority (Read And Write)** This is the default setting for Windows Server 2012 R2 Hyper-V failover clusters. Requires that only a majority of nodes acknowledge the update before the chance is committed to the database. Database read involves comparing the most recent timestamp from the majority of available nodes and using the most recent data.
- **2 = Majority (Write) And Local (Read)** This mode also requires the majority of cluster nodes acknowledge the update before committing the change to the database. The difference is that database read occurs on the local node, which means that the data may be stale.

Microsoft recommends that you not use mode 1 or 2 when you need to ensure that the cluster database is consistent, such as when using AlwaysOn availability groups with Microsoft SQL Server 2012 or Database Availability Groups with Microsoft Exchange Server 2010 or 2013.

MORE INFO **GLOBAL UPDATE MANAGER**

To learn more about the changes to Global Update Manager in Windows Server 2012 R2, visit *http://technet.microsoft.com/en-us/library/dn265972.aspx#BKMK_GUM*.

Recovering multi-site failover clusters

In some cases it can be necessary to force a cluster restart during a multi-site cluster failure. For example, you have a seven-node cluster, with four nodes in the first site and three nodes in the second site. A network outage disrupts inter-site communication. In this situation, the first site with the four nodes would remain operational and the cluster nodes in the second site would shut down because they would be unable to achieve quorum. However, what if the network outage happens to only impact external network communication to the first site and that the second site—the one with the cluster nodes that shut down—remains accessible to clients at other locations and to clients on the Internet? In that scenario, you'd force-start the cluster nodes in the second site using the cluster.exe command with the /fq switch. When you do this, everything will work fine until you restore network connectivity back to the first site, where the original four nodes still believe they have quorum. Then you have two collections of nodes which both believe they hold quorum. This scenario is termed a *partitioned cluster*, *split cluster*, or "*split brain*" *cluster*.

With Windows Server 2012 clusters, once you restored connectivity, you'd need to manually restart partitioned nodes in the first site using the cluster.exe command with the /pq switch. Windows Server 2012 R2 includes improvements that allow partitioned clusters to automatically reconcile when they detect "split brain" configuration. With Windows Server 2012 R2, the nodes that you started with the /fq switch are deemed authoritative and other cluster nodes will automatically restart using the /pq switch without requiring manual intervention.

MORE INFO **MULTI-SITE FAILOVER CLUSTERS**

To learn more about multi-site failover clusters, visit *http://technet.microsoft.com/en-gb/video/Hh133452*.

Thought experiment

Designing fault tolerance at Adatum

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

You are a network administrator for Adatum.com, an organization with headquarters in San Francisco and a branch office in Montreal. You are designing fault tolerance and business continuity for a new application server and VM that will be named AppVM1. AppVM1 will be hosted in the San Francisco office.

You want to meet the following goals:

- **You want to prevent any disruption of service and data loss in case an individual server fails unexpectedly.**
- **You want to be able to resume service with minimal data loss in case a catastrophe such as an earthquake brings the main office offline for an extended period.**
- **You always want to retain daily backups from the previous two weeks.**

With these goals in mind, answer the following questions:

1. **Which features in Windows Server 2012 can enable you to meet the first goal?**
2. **How might you design fault tolerance so that you can meet the first goal even after a catastrophe brings the main office offline for an extended period?**
3. **Describe two ways you might design fault tolerance for AppVM1 so that you can continue to meet the third goal even through a catastrophe that brings the main office offline for an extended period.**

Objective summary

- Hyper-V Replica is a new feature of Windows Server 2012 that creates an offline copy (replica) of a running VM and its storage. This replica can exist anywhere in the world. The online original (called the primary VM) sends the replica updates of any changes every 5 to 15 minutes. In case the primary VM fails, you can fail over to the replica and bring it online.
- To configure Hyper-V Replica, you first configure authentication and authorization settings for both physical host servers, called the primary server and replica server. Then, in Hyper-V Manager on the primary server, run the Enable Replication Wizard for the desired VM.
- By default, you can fail over only to the most recent recovery point, which is normally no more than 5 to 15 minutes old. However, you can choose to store additional, older recovery points that allow you to return to point-in-time snapshots of the primary VM.

- A planned failover is performed on the primary server after you shut down the primary VM. A planned failover brings the replica VM online with no loss of data. You can perform an unplanned failover on the replica server if the primary server fails without warning. With an unplanned failover, the replica VM recovers a copy of the primary VM that is normally no more than 5 to 15 minutes old. Finally, you can also perform a test failover while the primary VM is still running. A test failover brings a copy of the replica VM online in a state that is disconnected from the network.
- If you want to configure Hyper-V Replica for a VM that is hosted in a failover cluster, you need to add the Hyper-V Replica Broker role to the cluster. You also need to provide a CAP name and address for the cluster that will act as the server name.
- Global Update Manager is the component that is responsible for managing cluster database updates.

Objective review

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

1. You are configuring Hyper-V Replica on a VM that is hosting Microsoft Exchange. You want to help ensure that if you fail over to the replica VM, the application data will remain in a consistent state.

   What should you do? (Choose all that apply.)

   A. Configure the replica server to save additional recovery points.

   B. Configure the primary server to replicate incremental VSS copies.

   C. Configure a resynchronization schedule for the primary and replica VM.

   D. Configure Hyper-V Replica Broker.

2. You have configured Hyper-V Replica for a VM named AppSrv1, which is hosted on a primary server named VMhost1 in Cleveland. The replica server is named RepHost1 and is located in Denver.

   An unexpected power outage suddenly brings the entire Cleveland site offline. You perform a failover at the Denver site and start the replica VM on RepHost1. Power is returned to the Cleveland site after several hours, but only after changes have been made to AppSrv1.

   You are able to bring VMhost1 back online and now want to return AppSrv1 to its original host. Which step should you take next?

   A. Perform an unplanned failover.

   B. Choose the option to cancel the failover.

   C. Perform a planned failover.

   D. Choose the option to reverse replication.

3. Within your organization, a clustered VM named SQL1 is hosting SQL Server. The failover cluster hosting SQL1 is named Cluster1 and includes three nodes, named Node1, Node2, and Node3. Node1 is the preferred owner of the SQL1 VM. All three nodes are located in the same data center.

   You want to configure an offsite replica of SQL1 to protect the VM in case the entire failover cluster is brought down because of a power outage or other emergency.

   You deploy a physical server named RepSrv2 at a remote site. You want to configure RepSrv2 as the replica server. You install Windows Server 2012 and then the Hyper-V role on RepSrv2. You then connect the server to the Internet and establish a VPN connection between the two sites.

   Which of the following steps should you take? (Choose two.)

   A. At the primary site, configure Hyper-V Replica Broker and provide a CAP name.

   B. At the replica site, configure Hyper-V Replica Broker and provide a CAP name.

   C. In the replication settings on Cluster1, restrict authorization to the CAP.

   D. In the replication settings on RepSrv2, restrict authorization to the CAP.

Answers

This section contains the solutions to the "Thought experiments" and the "Objective review" questions in this chapter.

Objective 3.1: Thought experiment

1. You need to create a Windows Azure subscription, create a backup vault, and upload a management certificate.
2. The maximum retention period for data backed up to Windows Azure using Windows Azure Backup is 30 days.
3. You need a copy of a management certificate uploaded to the Windows Azure account and you'll need the passphrase used to protect the backed up data.

Objective 3.1: Review

1. **Correct Answer:** C
   - A. **Incorrect:** Backup Operators have the right to back up files and directories, restore files and directories, shut down the system, log on locally, and access the computer from the network. You want User1 only to able to back up the system.
   - B. **Incorrect:** Power Users do not have the right to back up the system.
   - C. **Correct:** By assigning the right to back up files and directories to User1, you can avoid assigning any other unnecessary privileges to the account.
   - D. **Incorrect:** The question does not state that User1 needs to be able to restore the system.
2. **Correct Answer:** A
   - A. **Correct:** VSSAdmin is the command-line tool used to manage shadow copies (snapshots) of disks.
   - B. **Incorrect:** Shadow is a command used to follow another user's session in Remote Desktop Services.
   - C. **Incorrect:** The Get-VMSnapshot cmdlet is used on a Hyper-V host to list all of the available snapshots of a VM.
   - D. **Incorrect:** Wbadmin is the command-line utility for Windows Server Backup. You can't use this utility to create a snapshot (shadow copy) of a disk.

3. **Correct Answer:** B

   A. **Incorrect:** Changing the bandwidth assigned to the work hours will not help you achieve your goal of having the backup operation complete before the work day begins at 8 AM.

   B. **Correct:** The bandwidth setting assigned to non-work hours is restricted to 1023.0 Kbps, which is much lower than the default setting of 1023 Mbps. This low setting could be unnecessarily limiting the bandwidth allowed at night. If you raise this value, the backup operation could proceed much more quickly (assuming more bandwidth is available).

   C. **Incorrect:** Adjusting the work hours could potentially cause disruption for workers, and it will not help you meet your goal of completing the backup operation before 9 A.M.

   D. **Incorrect:** The workdays are not currently affecting the backup because the backup is being performed outside of work hours. If you include Wednesday as a workday, you would actually apply bandwidth throttling to the first hour of the backup operation, and slow the procedure down for that hour.

4. **Correct Answer:** C

   A. **Incorrect:** This step would exclude the C:\Windows\Temp folder and its subfolders from the backup set, but it would not meet your goal of allowing the backup to be performed weekly. This folder is too small to reduce the size of the backup in any significant way.

   B. **Incorrect:** This step would exclude the C:\Windows\Temp folder but not its subfolders from the backup set, but it would not meet your goal of allowing the backup to be performed weekly. Too little data is stored in this folder to reduce the size of the backup in any significant way.

   C. **Correct:** This setting would allow the previous week's backup to be deleted in order to make space for the current week's backup. The size of the backup from the previous week is approximately 220 GB, and your storage quota is 300 GB. Consequently, you need to be able to remove the previous week's backup to make room for the current week's backup.

   D. **Incorrect:** This setting would not fix your problem. It would require all backups to be kept at least 30 days on Microsoft servers. If there is insufficient space to allow a new backup, as is the case in this scenario, the new backup will fail.

5. **Correct Answer:** A
   A. **Correct:** You don't need to modify the default settings. The bandwidth of the backup operation will be throttled to 256 Kbps beginning at 9AM every weekday.
   B. **Incorrect:** You don't want to increase the bandwidth settings assigned to work hours because this would increase the impact on network performance for users during work hours.
   C. **Incorrect:** Increasing the bandwidth setting assigned to non-work hours would not help you achieve your goal of minimizing impact on users if the backup operation proceeds into the work day.
   D. **Incorrect:** You don't need to adjust workdays because the current selection reflects the Monday - Friday schedule of the organization.

Objective 3.2: Thought experiment

1. You enable the Boot Logging option to track which services and drivers are loaded as a way of determining which was the last loaded before the system freezes.
2. The boot log is written to the file ntbtlog.txt and this file is located in the Windows folder.
3. You use Last Known Configuration to start the computer using the configuration that was in place the last time a successful sign-on occurred.

Objective 3.2: Review

1. **Correct Answers:** B, D
   A. **Incorrect:** Bootrec is used to repair the boot sector, the master boot record, and the BCD store. It cannot be used to configure a server to start in Safe Mode.
   B. **Correct:** You can use the Bcdedit /Set SafeBoot Minimal command to ensure that a computer running Windows Server 2012 will boot into Safe Mode the next time it starts.
   C. **Incorrect:** Startrep is used to before a startup repair of the local system. It cannot be used to configure a server to start in Safe Mode.
   D. **Correct:** You can use Msconfig in the GUI to configure a system to boot into Safe Mode the next time it starts. To do this, click the Boot menu, click Safe Boot, and then ensure that Minimal is selected.

2. **Correct Answer:** C

   A. **Incorrect:** Safe mode will never allow the device driver to load, so it will not allow testing of the new device driver.

   B. **Incorrect:** Last Known Good Configuration will revert to a version of the registry that did not include the driver that you need to test. You need to be able to test the driver.

   C. **Correct:** The problem is most likely caused by the fact that Windows Server 2012 does not load unsigned kernel mode drivers. To proceed with testing, you need to choose Disable Driver Signature Enforcement.

   D. **Incorrect:** This option will disable the defense against certain types of malware, but it will not allow you to load an unsigned driver.

3. **Correct Answer:** B

   A. **Incorrect:** This option is not available because Windows is not loaded on the disk array.

   B. **Correct:** You need to boot from the Windows installation media and then perform a System Image Recovery. This procedure will allow you to restore the system to its former state as quickly as possible.

   C. **Incorrect:** This option is not available because Windows is not loaded on the disk array.

   D. **Incorrect:** This option would to install a completely new deployment of Windows. You don't want a new deployment. You want to recover the old installation as quickly as possible.

Objective 3.3: Thought experiment

1. Only failover clustering can prevent any disruption of service and data loss in case of an individual server failure.

2. You can configure Hyper-V Replica on failover clusters in both the San Francisco and Montreal offices. The failover cluster in the San Francisco office can act as the primary server and the failover cluster in the Montreal office can act as the replica server.

3. One option is to use a cloud backup service such as Windows Azure Backup to back up AppVM1 daily and specify a retention range of 15 days. Another option is to perform daily backups of AppVM1 to local file storage on a file server that is itself a virtual machine. You can then configure this file server as a primary VM with a replica VM in the replica site (Montreal). In case of site-level failure at the primary site, the replica VMs of AppVM1 and the file server at the replica site will continue to operate as before with no loss of backup data.

Objective 3.3: Review

1. **Correct Answers:** A, B
   - **A. Correct:** You need to enable the option to save additional recovery points. This step allows you to configure some of these additional recovery points as incremental VSS copies, which are application-consistent.
   - **B. Correct:** Incremental VSS copies are snapshots that are application-consistent for VSS-aware applications like Microsoft Exchange.
   - **C. Incorrect:** Resynchronization does not affect the consistency of applications within recovery point snapshots.
   - **D. Incorrect:** Hyper-V Replica Broker is used for failover clustering, not for application consistency.
2. **Correct Answer:** D
   - **A. Incorrect:** You have already performed an unplanned failover. You cannot perform failover to the other site until replication is re-established between the two servers.
   - **B. Incorrect:** It's too late to cancel the failover because changes have already been made to AppSrv1.
   - **C. Incorrect:** You cannot perform a planned or unplanned failover to the other site until replication is re-established.
   - **D. Correct:** Choosing the option to reverse replication starts the Reverse Replication wizard. This wizard lets you re-establish replication between the two servers, with the local server in Denver acting as the new primary. After you complete this wizard, you can perform a planned failover to return the VM to the site in Cleveland.
3. **Correct Answers:** A, D
   - **A. Correct:** You need to configure the Hyper-V Replica Broker role for the failover cluster if you want to add an offsite replica to a clustered VM.
   - **B. Incorrect:** To configure Hyper-V Replica Broker at the replica site, you would need to create a failover cluster at the replica site. This step is unnecessary because you want to configure RepSrv2 as the replica server. Your goal is not to create a replica cluster.
   - **C. Incorrect:** In the replication settings for Cluster1, you want to restrict authorization to RepSrv2. However, this step is not immediately necessary. It would be required only if the VM were failed over to the replica site and you later wanted to fail back to the original site.
   - **D. Correct:** The server-level replication settings allow you to limit which remote servers can act as a primary server to the local replica server. In this case, you need to configure the Client Access Point as the name of the primary server.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z