

Lesson 8: Configuring and Managing Backups

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Overview

- Objective 3.1: Configure and Manage backups.
 - Configure Windows Server backups
 - Configure Windows Online backups
 - Configure role-specific backups
 - Manage VSS settings using VSSAdmin
 - Create system restore points

Configuring and Managing Backups

Lesson 8: Configuring and Managing Backups

Backups

- When an organization loses data, the results can range from a loss of productivity to an entire meltdown of the company itself.
- Having a solid backup strategy along with the systems, processes, and tools to execute the strategy is the key to your ability to recover.

The best method to data recovery is Backup, Backup, Backup.

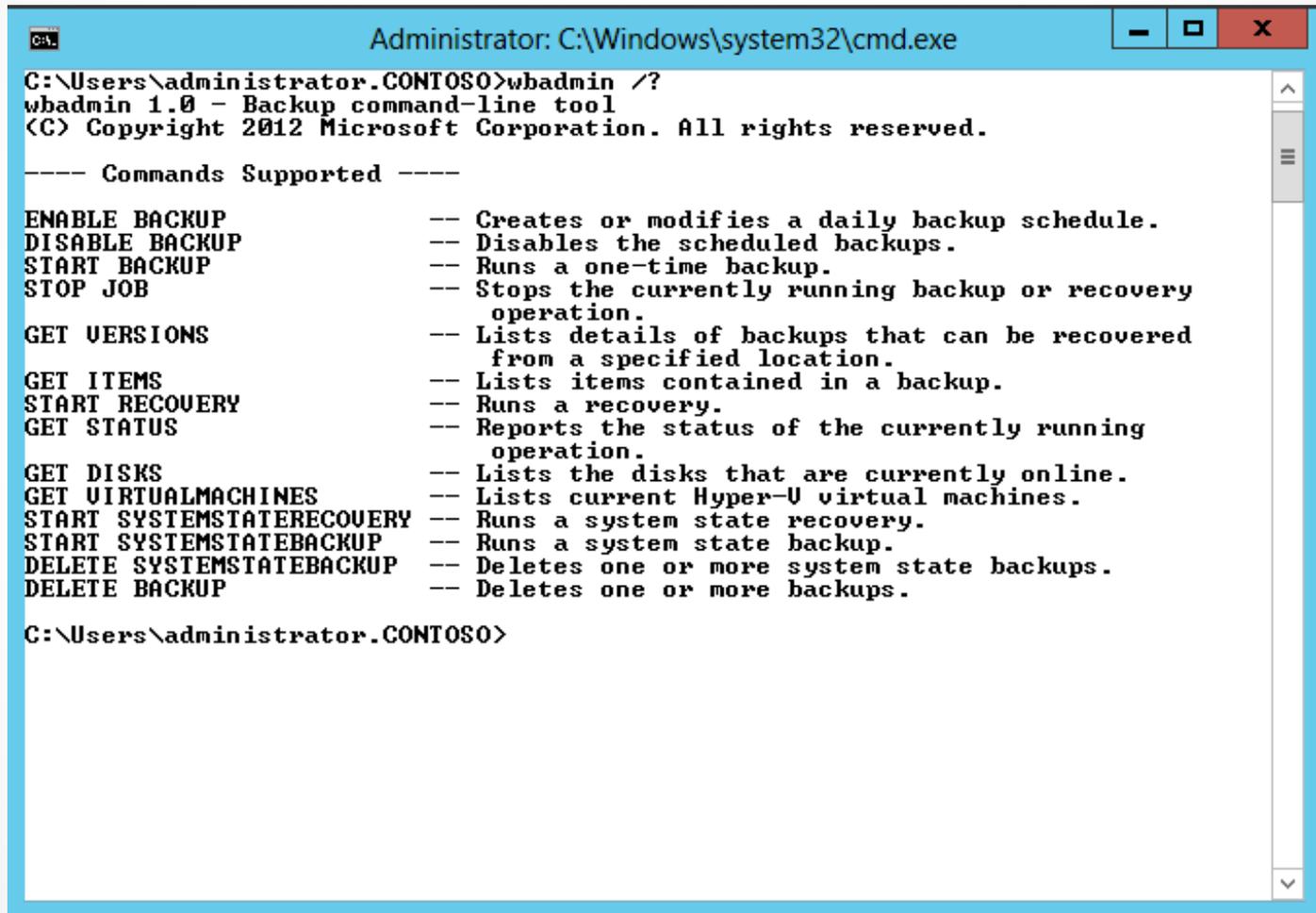
Lost Data

- If you've been administering servers for any length of time, you most likely have experienced or heard of someone who lost data due to:
 - Hardware failure
 - Software failure
 - Human error
 - Computer virus
 - Theft
 - Natural disaster (flooding, earthquakes, severe weather, and so on)
 - Fire

Windows Server Backup Feature

- **Windows Server Backup**, *wbadmin*, and Windows PowerShell cmdlets provide the tools to back up and restore your critical data and servers.
- To run backups on Server Core installations, use either the command-line tool *wbadmin* or the Windows PowerShell cmdlets, or manage them remotely from another computer using the Windows Server Backup MMC.
 - You can also use the Windows 8 Remote Server Administration Tools (RSAT).

Wbadmin



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator.CONTOSO>wbadmin /?
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2012 Microsoft Corporation. All rights reserved.

---- Commands Supported ----

ENABLE BACKUP           -- Creates or modifies a daily backup schedule.
DISABLE BACKUP          -- Disables the scheduled backups.
START BACKUP            -- Runs a one-time backup.
STOP JOB                -- Stops the currently running backup or recovery
                        operation.
GET VERSIONS            -- Lists details of backups that can be recovered
                        from a specified location.
GET ITEMS               -- Lists items contained in a backup.
START RECOVERY          -- Runs a recovery.
GET STATUS              -- Reports the status of the currently running
                        operation.
GET DISKS               -- Lists the disks that are currently online.
GET VIRTUALMACHINES     -- Lists current Hyper-U virtual machines.
START SYSTEMSTATERECOVERY -- Runs a system state recovery.
START SYSTEMSTATEBACKUP -- Runs a system state backup.
DELETE SYSTEMSTATEBACKUP -- Deletes one or more system state backups.
DELETE BACKUP           -- Deletes one or more backups.

C:\Users\administrator.CONTOSO>
```

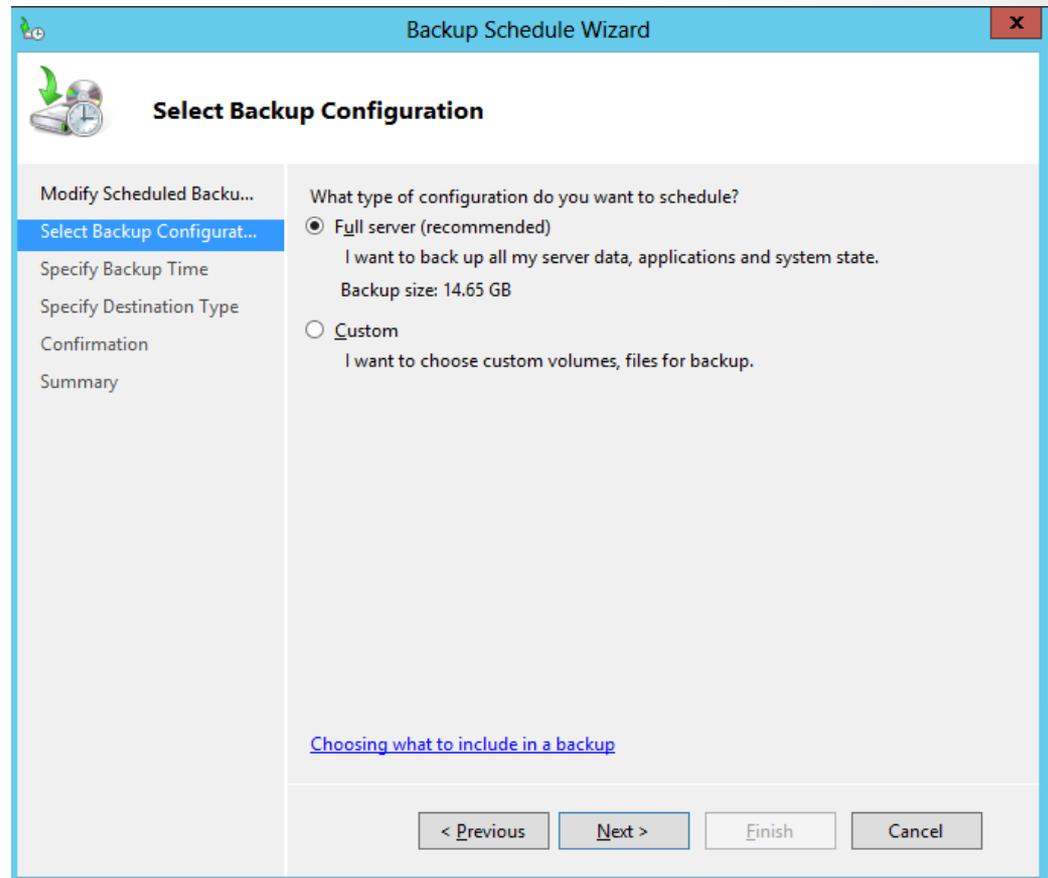
Windows Server Backups

- The Windows Server Backup feature provides full server, bare metal recovery, system state, system reserved, and local/remote volume backup capabilities.
- **Recovery Time Objective (RTO)**: The maximum amount of time you have to bring a system back online before it has a significant impact on your organization.
- **Recovery Point Objective (RPO)**: The amount of data you can afford to lose before it has a significant impact on your organization.

Backup Configuration Options

When configuring your backup, select either:

- Full server (recommended)
- Custom



Custom Backup Configuration

- The **Custom** option allows you to specify the items you want to back up. The options include:
 - **Bare metal recovery:** Recover your server from a hard drive failure to a machine running the same/different hardware.
 - It does not support cross-architecture (x86 to x64) and requires Windows Server installation media to start the recovery process.
 - It automatically includes system state, system reserved, and the critical volumes that are necessary for the operating system to run.

Custom Backup Configuration

- **System state:** Backs up all the files needed to recover Active Directory, including the registry, boot files, the COM+ class registration database, the Active Directory database (ntds.dit) and its associated log files, the Active Directory Certificate Services database, the SYSVOL folder, and system files under the protection of Windows Resource protection.
- **System reserved:** Contains the Windows Recovery Environment (WinRE) files and can be used to boot the server in situations where the operating system becomes corrupted or fails to boot.
- **Local disk (x:):** Represents local disks and volumes on the server.

Manual Backups

- You can run a manual backup (one-time backup) by using the Backup Once Wizard, which can be accessed via the Actions pane in the Windows Server Backup console.
- These types of backups can also be initiated using wbadmin and Windows PowerShell.
- Never use manual backups as a replacement for your regularly scheduled backup.

Storing the Backups

Windows Server Backup provides three options to select from when deciding where to store your backups. These options include backing up to:

- Hard disk(s) (recommended)
- A volume
- A shared network folder

Backup Folder and File Structure

- When your backup starts, Windows Server Backup creates a folder structure in the target location you specified:
 - Backup <Date> <ID number>
 - Catalog
 - Logs
 - SPPMetadataCache
 - MediaID
- The Catalog folder contains information about the volumes backed up and where your backups are stored.

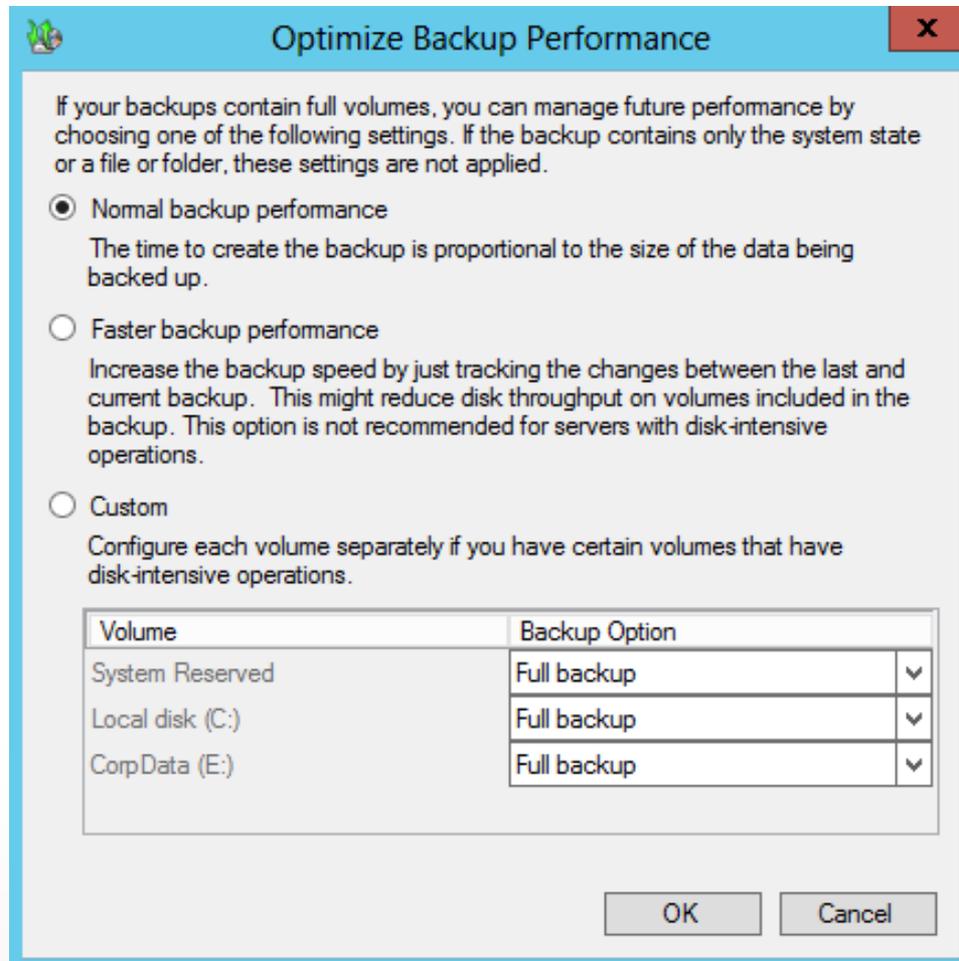
Full versus Incremental

- After the first full backup, you can then automatically run incremental backups, which saves only the data that has changed from the last backup.
- By default, Windows Server Backup creates incremental backups, which function much like full backups, allowing you to restore from a single backup.
 - In the past, you had to restore a full backup followed by the necessary incremental backup(s) to complete the restore process.

Optimizing Backups

- Windows Server Backup also provides performance enhancements by using block-level technology and Volume Shadow Copy Service (VSS).
- Block-level backup technology improves performance by bypassing the files and file system.
- **Volume Shadow Copy Service (VSS)** takes a snapshot of the volume's current data, which is used by Windows Server Backup to back up the data. The snapshot, or shadow copy, is then deleted when the backup completes.

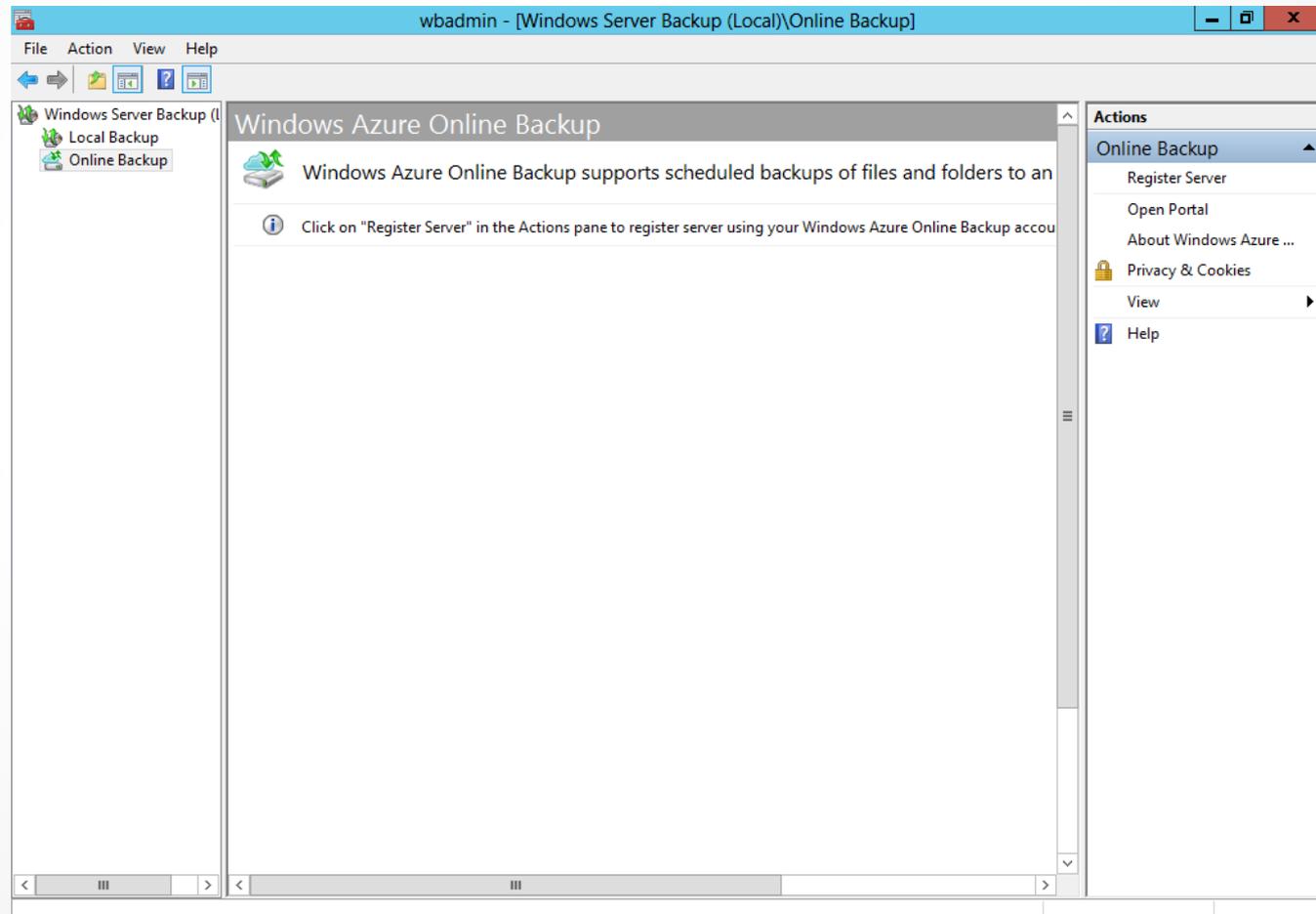
Optimizing Backups



Windows Azure Online Backup

- Storing your backups in the cloud allows you to retrieve them from any location where you have Internet access and provides you with an offsite storage location to protect against disasters.
- **Windows Azure Online Backup** is a Windows Server 2012 feature that allows you to back up your files and folders to the Windows Azure Online Backup service.
- Windows Azure is a cloud-based storage service managed by Microsoft.

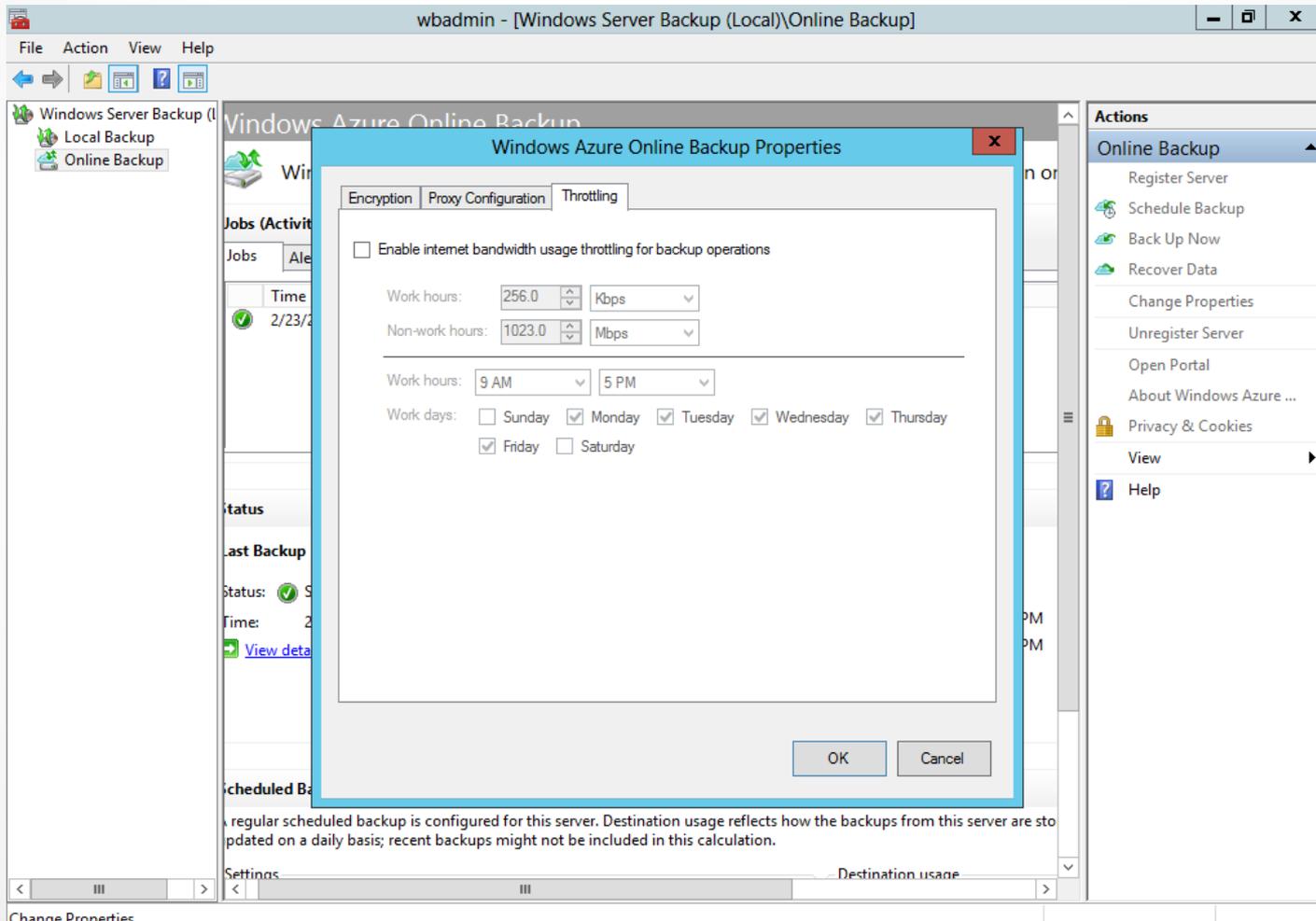
Windows Azure Online Backup



Optimizing Online Backups

- During the backup process, Windows uses your network along with Internet bandwidth.
- Just as with any backup, it's always a good idea to run it outside of your normal work hours. If that is not an option, you can make some adjustments to control how the Windows Azure Backup Agent uses the bandwidth during certain days and times.

Windows Azure Online Backup Properties



Change Properties.

Backing Up DHCP

- The Dynamic Host Configuration Protocol (DHCP) database contains information about IP address leases, reservations, scopes, scope options, and DHCP registry key settings.
- It's backed up automatically at 60-minute intervals to the `%systemroot%\System32\Dhcp\Backup` directory. It is also backed up as part of a system state or full backup and by using the DHCP Manager console.

Backing Up DNS

- Active Directory-integrated DNS zone configuration information is stored in the registry; therefore, it's also backed up as part of the system state and during full backups.
- An alternative is to use DNSCMD with the /zoneexport switch to export the Active Directory-integrated zones to a file you can back up:

```
DNSCMD /zoneexport contoso.com  
  \backup\contoso.com.dns.bak
```
- The XCOPY command can be used to back up primary and secondary zone files to a backup folder you specify:

```
XCOPY %systemroot%\system32\dns c:\backups\dns /y
```

Backing Up WINS

- The Windows Internet Name Service (WINS) maintains a distributed database used to register and query dynamic mappings of NetBIOS names for computers and groups.
- It maps NetBIOS names to IP addresses.
- Although the database is backed as part of system state and full backups, you can also back up the WINS database from the WINS console.

Backing Up Certificate Services

- Certificate Services stores a database in the C:\Windows\system32\Certlog location by default.
- When certificates are issued to users and computers, the associated information is maintained in the Certificate Services database.

Backing Up Active Directory Domain Services

Active Directory is backed up as part of system state and full backups. These components are included in the system state:

- **System startup (boot) files**
- **System registry**
- **COM+ Class registration database**
- **System volume (SYSVOL)**
- **Active Directory**

Active Directory Recycle Bin

- To use Active Directory Recycle Bin, your forest functional level should be set to at least Windows Server 2008 R2 or greater and all domain controllers must be running Windows Server 2008 R2 or Windows Server 2012.
- This can be confirmed by selecting *Server Manager > Tools > Active Directory Administrative Center*.

Protecting Active Directory Objects from Deletion

- To further protect against the accidental deletion of objects in Active Directory (Computers, OUs, and Users), Windows Server 2012 provides the “protect from accidental deletion” option.
- This setting can be found by opening the Active Directory Administration Center, right-clicking the object, and selecting *Properties*.

VSS Settings and VSSAdmin

- Use the *Volume Shadow Copy Administrative Command-line Tool (VSSAdmin)* to
 - Create and delete volume shadow copies/associations.
 - List shadow copy providers and writers.
 - Resize a volume shadow storage association.
- VSSAdmin is used to manage VSS.

VSS Components

- The VSS components communicate with each other via the VSS Framework to both create and restore your shadow copies. These are the tasks performed by each component:
 - ***VSS requester***
 - ***VSS writer***
 - ***VSS provider***
 - ***Source volume***
 - ***Storage volume***

Creating System Restore Points

- Shadow Copies for Shared Volumes (SCSV) and Hyper-V snapshots provide you with the ability to return to a specific point in time.
- You enable SCSV on a per-volume basis by selecting *Server Manager > Tools > Computer Management*.
- You need at least 300 MB of free space to create a shadow copy on the selected volume.

Shadow Copies for Shared Volumes

The screenshot shows the Windows Server Backup console. The left pane displays the navigation tree with 'Disk Management' selected. The main pane shows the 'Volume' tab for the 'E:' drive, which is a shared NTFS volume. The 'Backup (E:) Properties' dialog box is open, showing the 'Shadow Copies' tab. The dialog includes a table for selecting a volume and a list of existing shadow copies.

Volume	Next Run Time	Shares	Used
\\?\Vol...	Disabled	0	0 bytes on \...
C:\	2/7/2013 7:0...	0	488 MB on ...
E:\	2/7/2013 7:0...	0	2.27 GB on ...

Shadow copies of selected volume

2/6/2013 1:33 PM	Create Now
	Delete Now
	Revert...

Backing Up Hyper-V Virtual Machines

- VMs, created using Hyper-V, are stored as files on your hard disk.
 - These files contain the VHDs, saved state files, snapshot files, and configuration files.
- VSS writers are responsible for preparing their data in order to make the shadow copy and are instructed by VSS to quiesce (pause) its associated application to ensure a consistent backup is made.
- By using the Microsoft Hyper-V VSS writer, Windows Server Backup can create the snapshots while the VM is running.

Hyper-V Snapshots

- **Hyper-V snapshots** offer another way to capture the state, data, and hardware configurations for a VM at a specific point in time.
- These snapshots, which can be taken when the VM is running or stopped, are created in the Hyper-V Manager.
- The snapshot includes the configuration and network settings for the VM as well as the current state of the VHD(s) attached to the machine and any saved state information.
- Hyper-V uses the VSS to make a copy of the guest machine's hard disk.
- By default, a Hyper-V snapshot's data is stored in an automatic VHD (.avhd) file and then it's attached to the VM.
- When you take a snapshot of a VM, you are basically converting its VHD into a differencing disk.

Exploring Enterprise Backup Solutions

- If you are looking for an enterprise backup solution, then consider System Center 2012 Data Protection Manager:
 - It provides the ability to back up to disk and to tape.
 - It can be used to protect and recover Exchange (2007, 2010, 2013), SQL (2008, 2008 R2, 2012), SharePoint (2013, 2010), Windows SharePoint Server 3.0, Microsoft Office SharePoint Server 2007, Windows desktops/laptops (Windows 7/8, Windows Vista), virtual servers (Hyper-V Windows Server 2008/2008 R2, Windows Server 2012), and file servers (Windows Server 2008/2008 R2, Windows Server 2012) within and across Active Directory domains.

Exploring Enterprise Backup Solutions

- DPM also provides you with the ability to manage system state and bare metal recovery from a central location.
- The following vendors provide enterprise backup solutions for Windows Server 2012:
 - Acronis Backup and Restore
 - Symantec Backup Exec 2012 and NetBackup
 - IBM Tivoli Storage Manager
 - Carbonite
 - CA Technologies ARCserve
 - Commvault Simpana

Lesson Summary

- Hardware/software failures, human error, computer viruses, theft, natural disasters, and fire can result in data loss; therefore, you need to have a backup strategy in place and be prepared to execute it.
- When the Windows Server Backup feature is installed, it includes the Windows Server Backup console, wbadmin, and Windows PowerShell cmdlets that can be used to back up your server.
- Windows Server Backup on Windows Server 2012 does not support backing up to tape, but you can still use System Center 2012 Data Protection (DPM) Manager to perform a disk-to-disk-to-tape (D2D2T) and third-party software if necessary.

Lesson Summary

- Windows Server Backup offers both full server (recommended) and custom backup configuration options. Custom options include bare metal recovery, system state, system reserved, and local disk.
- Bare metal recovery backups can be used to recover your server from a hard drive failure to a machine running the same/different hardware, but it does not support cross-architecture (x86 to x64) restores.
- Manual backups should not be a replacement for regularly scheduled backups.

Lesson Summary

- Windows Server provides three options when deciding where to store your backups: hard disk, volumes, and shared network folders. When backing up to hard disk, the best practice is to dedicate them to the Windows Server Backup job set and use a rotation schedule to take disks offsite for additional protection.
- Backups to shared network folders are overwritten with each subsequent backup.
- Backups are stored in a *WindowsImageBackup* folder under the name of the server being backed up (e.g.,
\\<server>\<sharedfolderpath>\WindowsImageBackup\<serverbackedup>).

Lesson Summary

- Backup performance is enhanced through the use of block-level technology and Volume Shadow Copy Service (VSS). Block-level technology bypasses the files and file system and reads the blocks in the order they appear on the disk. VSS takes snapshots of the volume's current data allowing users and applications to continue to use the volume without interruption.
- Backups of full server volumes can be optimized by selecting the faster backup performance setting (incremental backups) available in the Configure Performance Settings.
- File classification allows you to configure automatic procedures for defining a desired property on a file, based on the conditions specified in classification rules.

Lesson Summary

- Windows Online Backups, a feature available with Windows Server 2012, allows you to back up your files and folders to the Windows Azure Online Backup service. It does not support system drivers/system state backups. This involves setting up a Windows Azure Online account, installing a software agent, registering the server, and then scheduling the backup to occur. You can also monitor the health of the online service with the Windows Azure dashboard.
- As part of your overall backup strategy, take into consideration the roles installed on each of your servers. Depending on the roles performed, how you approach the backup and eventually restore the system may be impacted.

Lesson Summary

- The Volume Shadow Copy Administrative Command-line tool (VSSAdmin) can be used to manage VSS. VSS consists of VSS requesters, writers, and providers that work with each other using the VSS Framework.
- Shadow Copies for Shared Volumes (SCSV) uses the capability of VSS to capture and store copies of folders located on shared network resources at a specific point in time. End users can use these to restore their own files, which can reduce the time and costs associated with file recovery.
- Hyper-V snapshots can be used to capture the state, data, and hardware configurations for a virtual machine (VM) at a specific point in time.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make backup copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.