Lesson 9: Recovering Servers

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft Official Academic Course

WILEY

Overview

- Objective 3.2 – Recover servers.
  - Restore from backups, perform a bare metal restore (BMR)
  - Recover servers using Windows Recovery Environment (WinRE) and safe mode
  - Apply system restore snapshots
  - Configure the Boot Configuration Data (BCD) store

Preparing for Windows Server 2012 Restores

Lesson 9: Recovering Servers

Windows Server 2012 Restores

A written server recovery plan that outlines roles and responsibilities as well as the steps necessary to recover your servers is critical to reducing the overall downtime and loss of productivity in your organization.

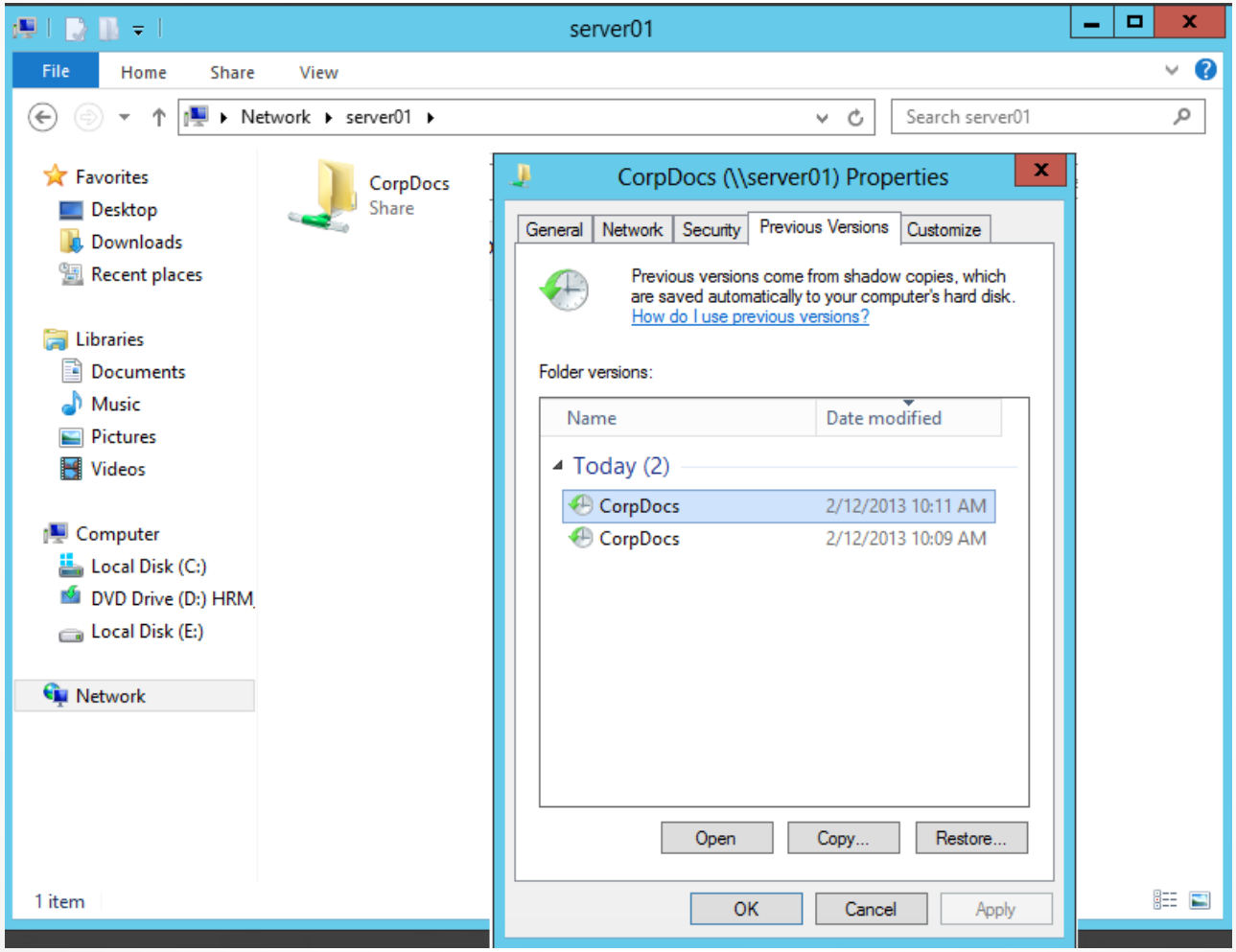
Preparing for Windows Server 2012 Restores

1. Who will be on the recovery team from IT and what will each of their recovery responsibilities be?
2. Do you know how many servers you have and where they are located (main office, branch office, and so on)?
3. Do you have a current network topology map that shows all critical servers, roles/features, IP addressing information, and network connections?
4. Do you have the specs on each server (memory, drive space, and volume info)—the information you need to know to rebuild the server from scratch?
5. Which server(s) will you need to recover first?
6. What is the step-by-step procedure for the data recovery process on each?
7. How will you know/test that things are back to normal after the restore?
8. When is the last time you performed a test restore to make sure your backups were working correctly?

Restoring Files and Folders

- If a user accidentally deletes or overwrites a file or folder on a network share, you have two options for restoring the data:
  - Access the share and restore the previous version.
  - Use Windows Server Backup to restore the data.

Restoring a File with Shadow Copies for Shared Volumes (SCSV)



Restoring Volumes

- The approach used to restore a volume depends on the type of volume being recovered.
- Data volumes can be restored using Windows Server Backup.
- To restore a system volume, use the ***Windows Recovery Environment (WinRE)*** and the Windows installation media.

Restoring the System State

- The system state includes the operating system configuration files. What is included in the system state differs depending on the role(s) performed by the server. This also impacts the process used to restore the system state when the time comes.
- The system state is included in these backup configuration options:
  - Full backups (recommended)
  - Bare metal recovery backups
  - System state backups

Restoring the System State

- Recovering the system state of a member server can be performed via the Windows Server Backup program.
- Recovering the system state of a domain controller requires that you boot into ***Directory Service Restore Mode (DSRM)***.
  - DSRM is a special boot mode that is used to repair and recover Active Directory.

Booting to DSRM

- There are two ways to configure your server to boot into DSRM:
  1. Use msconfig to configure the server to reboot into DSRM.
  2. Enter the following at a command prompt:

     bcdedit /set safeboot dsrepair

     - With the bcdedit command, you can return the server to normal boot by entering this command:

     bcdedit /deletevalue safeboot

Non-Authoritative Restores

- If you don't select the "perform an authoritative restore of Active Directory files" option, you're performing a ***non-authoritative restore***.
- The restored domain controller will then use normal replication with other replication partners (domain controllers) to gather information that was changed after the backup was taken.
- These changes overwrite the state you restored and bring the domain controller up to date with the current copy of the Active Directory database.

Authoritative Restores

- Performing an ***authoritative restore*** gives you the ability to increment the version number of the object in Active Directory that you want to restore.
- This object will then appear to be newer than the existing version of the same object being held by the other replication partners (domain controllers).
- Because the object appears as newer, it will be replicated to the other domain controllers and overwrite their data.

Authoritative Restores

- To perform an authoritative restore, boot into DSRM and use the Ntdsutil.exe tool.
- ***Ntdsutil.exe*** is a command-line tool used to access and manage an Active Directory database.
- The authoritative restore consists of two steps:
  1. Perform the non-authoritative restore from your backup.
  2. Perform the authoritative restore of the deleted object(s).

Authoritative Restores

After the non-authoritative restore of the system state completes and the server reboots into DSRM mode, open a command window and enter the following to restore an OU named *Sales* and all objects beneath it in the Contoso.com domain. (Press *Enter* after each command.)

```
C:>Ntdsutil
Ntdsutil: Activate Instance NTDS
Ntdsutil: Authoritative Restore
Restore subtree "cn=OU,dc=contoso,dc=com"
```

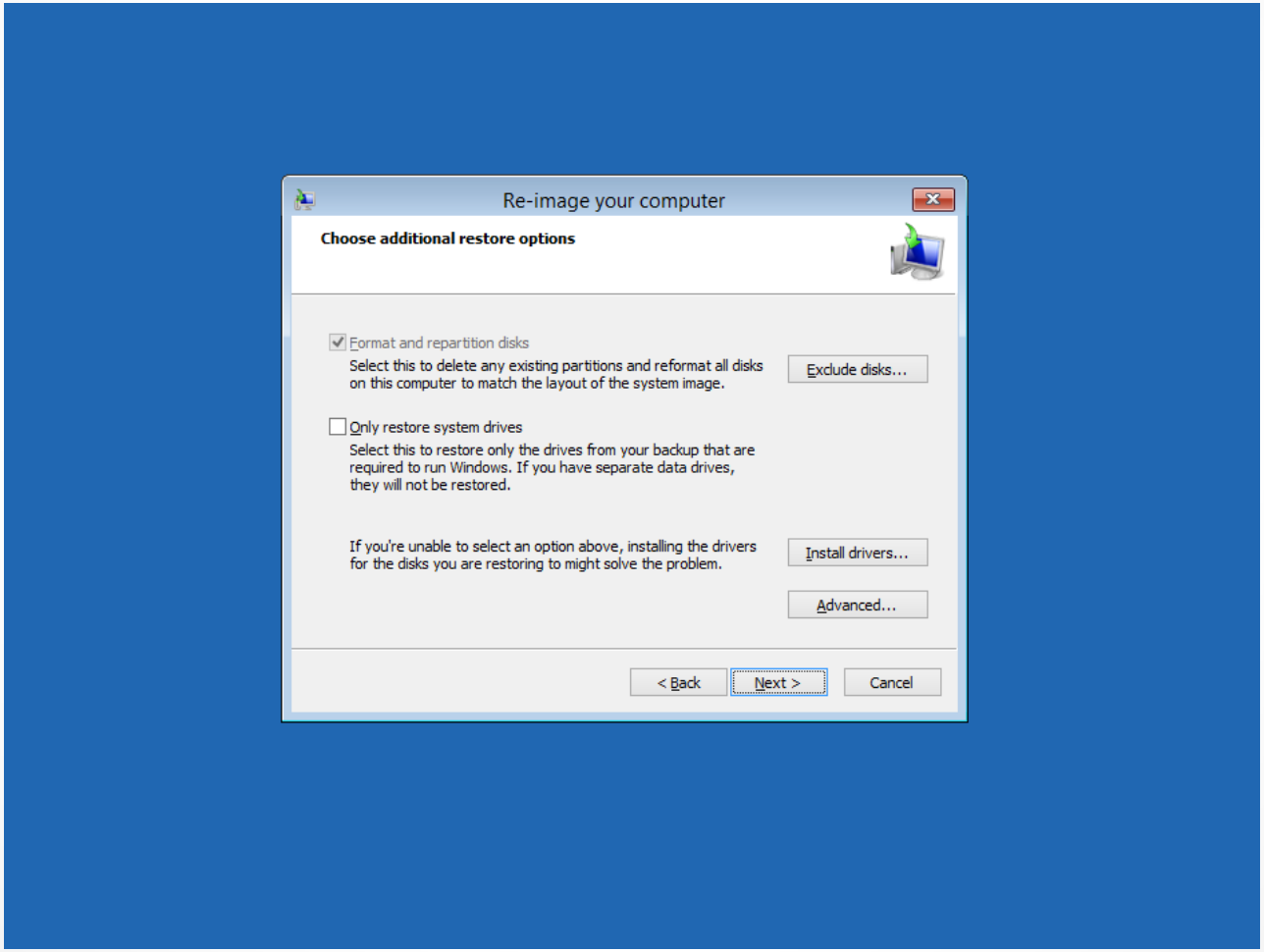
Active Directory Recycle Bin

- In Windows Server 2012, you can avoid performing lengthy authoritative restores using ntdsutil if you have the ***Active Directory Recycle Bin*** enabled before any Active Directory objects are deleted.
- Active Directory Recycle Bin restores objects and their attributes in their entirety.
- This is possible due to a new Active Directory state that replaces tombstone states that were in previous versions of Active Directory.
- Active Directory keeps tombstone objects for 180 days.

Performing a Bare Metal Recovery Restore

- A bare metal recovery restore allows you to restore the server without having to load the operating system beforehand.
- It does require that you have your Windows installation media from which to boot.

Performing a Bare Metal Recovery Restore



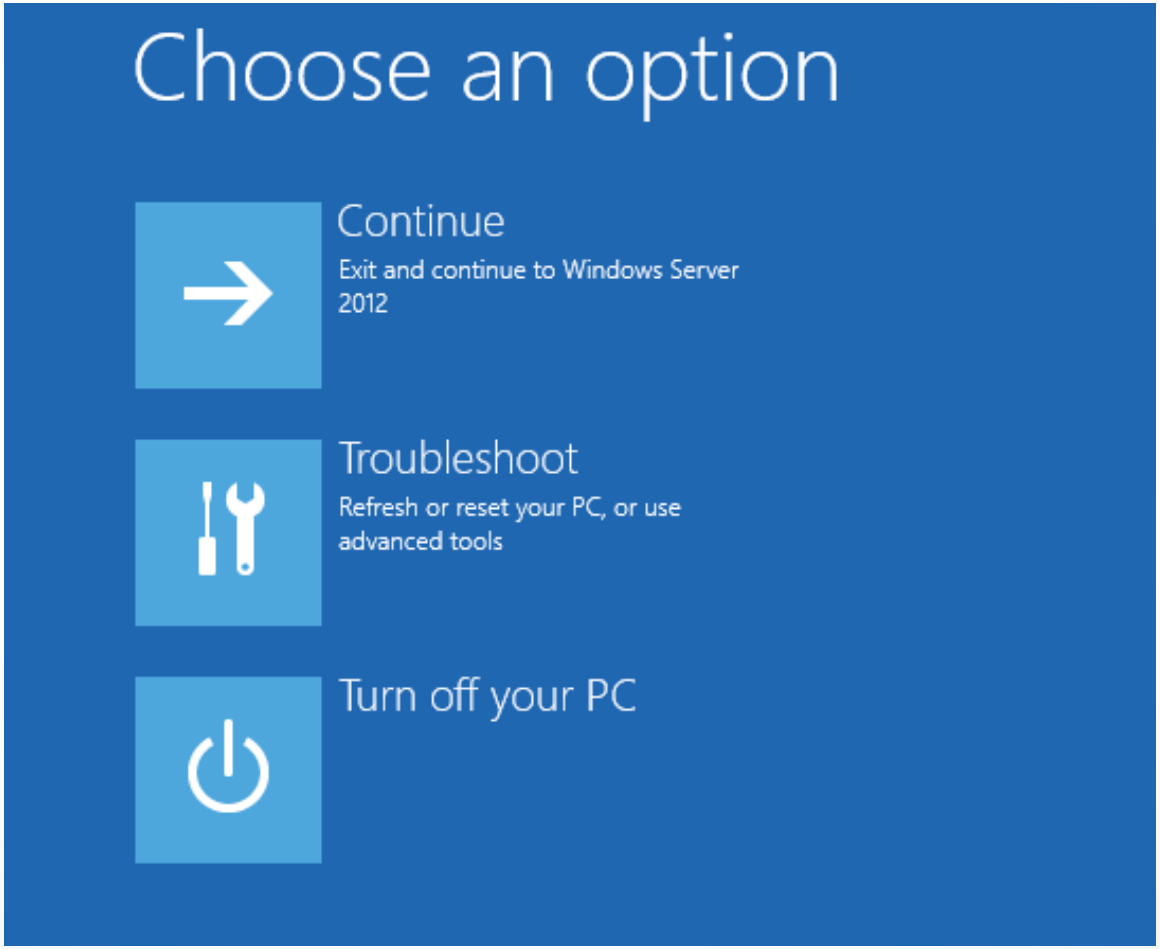
Recovering Servers Using WinRE and Safe Mode

If you experience problems that prevent Windows Server 2012 from booting, use the Windows Recovery Environment (WinRE) to troubleshoot and repair the system.

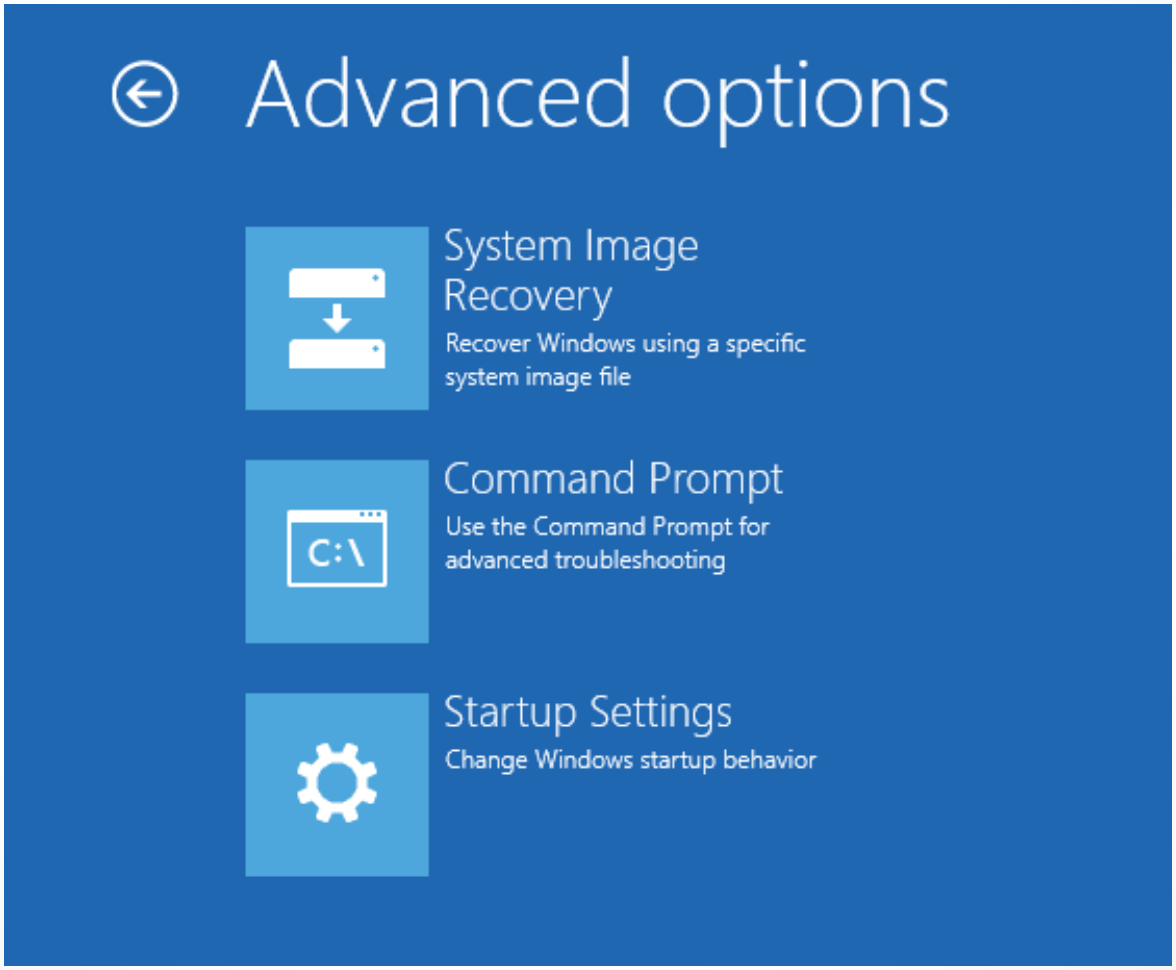
Recovering Servers Using WinRE and Safe Mode

- There are several ways to access the Windows Recovery Environment (WinRE) in Windows Server 2012:
  - The server enters WinRE in situations after two consecutive failed attempts to start Windows, after two consecutive shutdowns that were unexpected, or due to secure boot errors.
  - Select *Settings* from the Charms bar, choose *Power*, and click *Restart* while holding down the SHIFT key.
  - Boot the server from Windows installation media and select *Repair Computer*.
  - Enter the command **`shutdown /r /o`** from a command prompt.

Windows Recovery Environment (Win RE)



Windows Recovery Environment (Win RE)



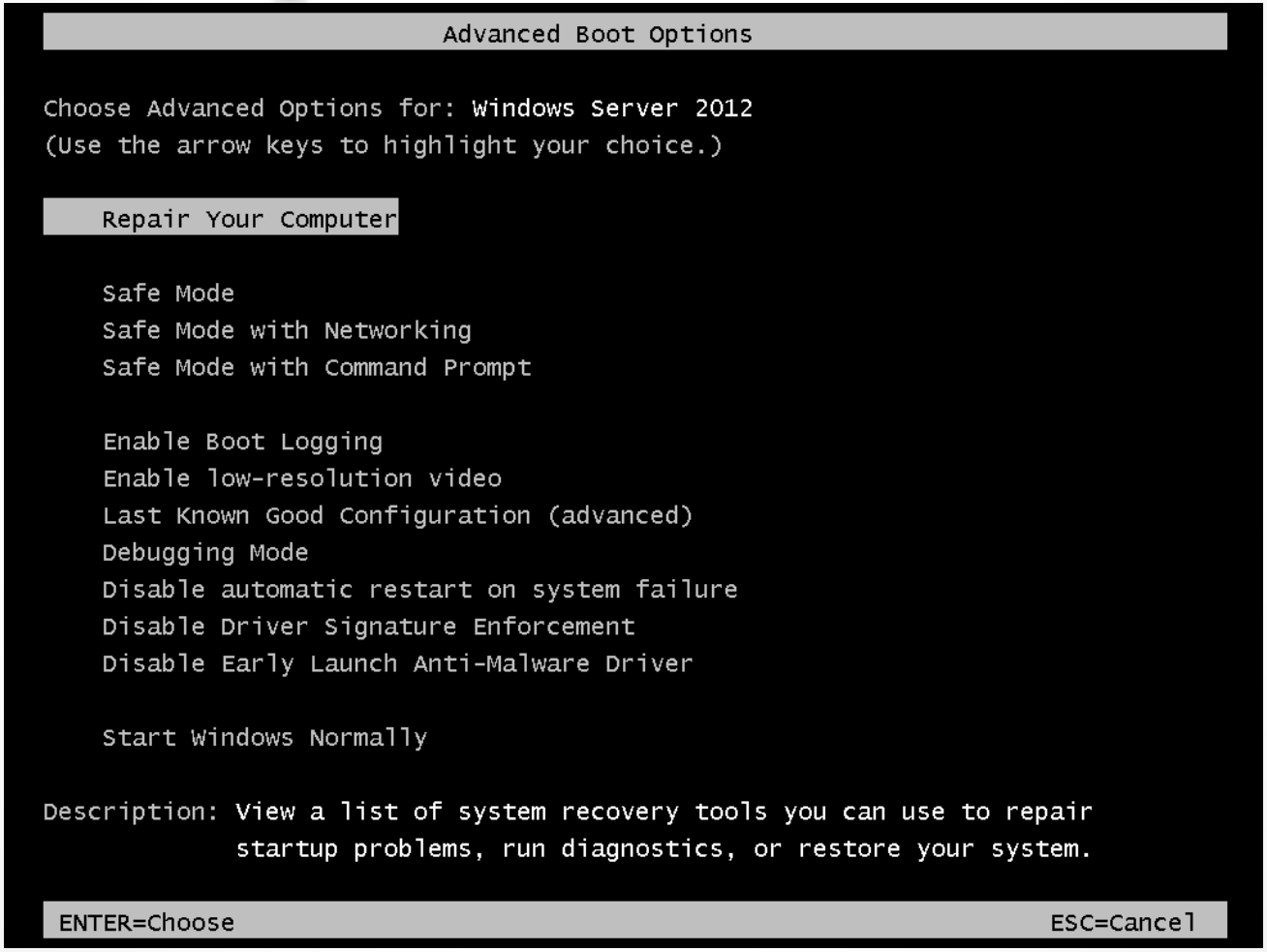
Advanced Boot Options Menu

- On the Advanced Boot Options menu, you can select from the following:
  - **Repair Your Computer:** Provides a list of system recovery tools that you can use to repair your system, run diagnostics, or restore your system.
  - **Safe Mode:** Starts Windows using only the core drivers and services. This option should be used when you cannot boot after the installation of a new driver and/or device.
  - **Safe Mode with Networking:** Similar to safe mode but with networking support. Use this option to create a network connection to gain access to files on servers, connect and compare settings on other computers, and use the Internet to download updates.
  - **Safe Mode with Command Prompt:** Similar to safe mode but opens a command prompt.

Advanced Boot Options Menu

- **Enable Boot Logging:** Creates ntbt.log.txt that lists all of the drivers that are loaded during setup. This includes the last driver loaded before the system failed. It's stored in the %systemroot%.
- **Enable low-resolution video:** Starts Windows in low-resolution display mode; allows you to set or reset the display resolution.
- **Last Known Good Configuration (advanced):** Starts Windows using the settings from the last time that Windows booted successfully.
- **Debugging Mode:** Enables the Windows kernel debugger.
- **Disable automatic restart on system failure:** The settings here prevent Windows from automatically rebooting after a crash.
- **Disable Driver Signature Enforcement:** Allows drivers containing improper signatures to be loaded.
- **Disable Early Launch Anti-Malware Driver:** Allows drivers to initialize without being measured by the anti-malware driver.

Advanced Boot Options Menu



Command-Line Tools

- **Bootrec**: Troubleshoots and repairs the master boot record, boot sector, and Boot Configuration Data (BCD) store.
- **Bcdedit:** Displays how Windows is configured to boot and can also be used to troubleshoot issues with the Windows Boot Manager.
- **Format:** Formats partitions.

Command-Line Tools

- **System File Checker**: Checks the integrity of your hard drive. If a file is missing or corrupt, it can be restored with this tool. SFC validates the digital signatures of all the Windows system files and restores any it finds that are incorrect.
  - **Sfc /scannow:** Scans all of your protected system files and repairs problems by replacing incorrect versions with the correct Microsoft versions.
  - **Sfc /verifyonly:** Scans for integrity of all protected system files but does not perform a repair operation.
- **Diskpart:** Loads the Windows Disk management program. Using this program, you can shrink, expand, create, and delete existing partitions as well as gather information about your hard drives.

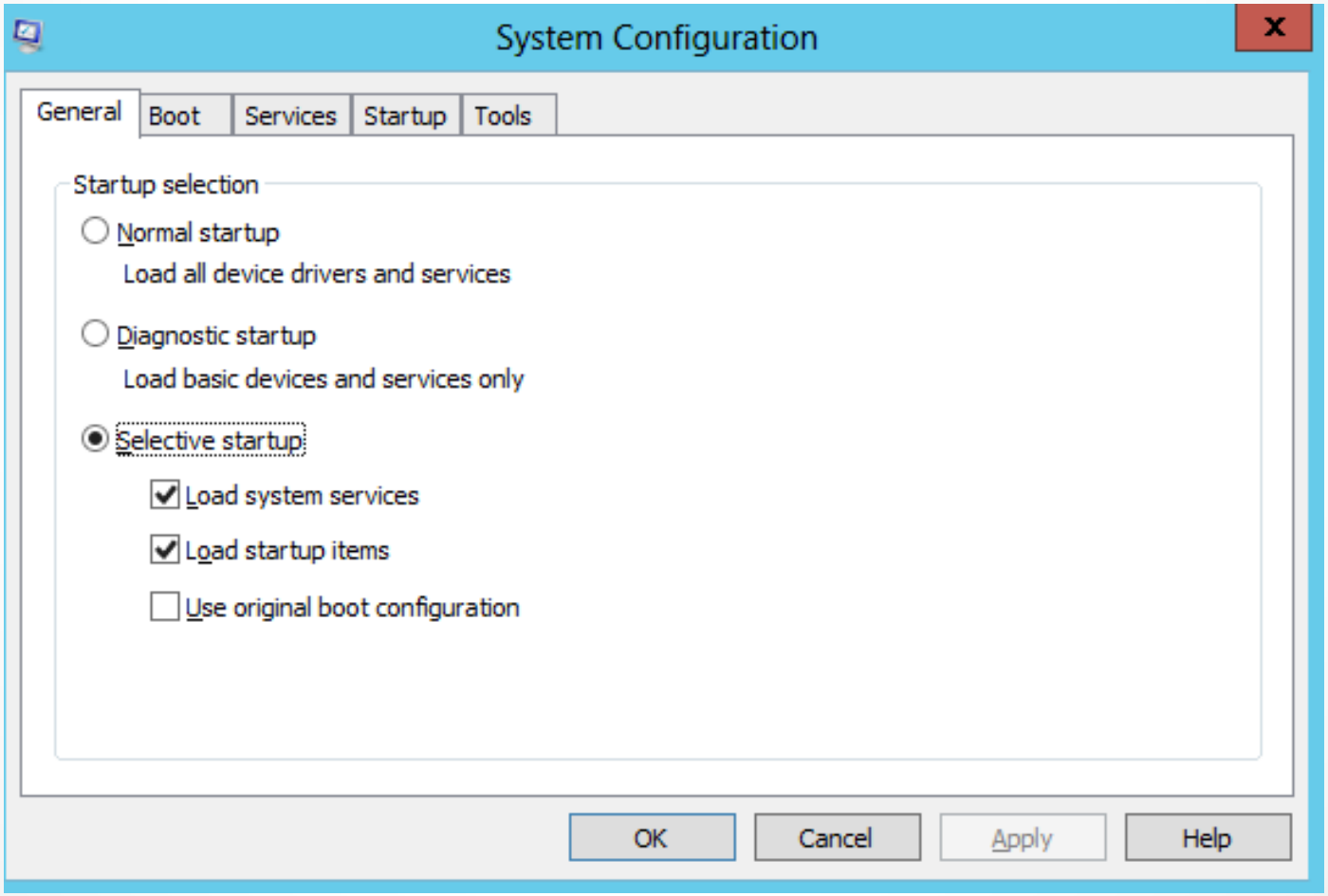
Safe Mode

- Starting in ***safe mode*** allows you to troubleshoot situations where you cannot access the system due to faulty hardware, software, device drivers, and virus infections.
- Safe mode loads a minimal set of drivers and services
- If you can boot into safe mode but can't boot normally, the system most likely has a conflict with hardware settings, services, drivers, or some type of registry corruption.

MSConfig

- ***MSConfig*** (also called *System Configuration*) is a tool used to troubleshoot the system startup process.
- It can be used to disable or enable software, device drivers, and services that run at startup.
- MSConfig can also be used to change boot parameters if necessary.

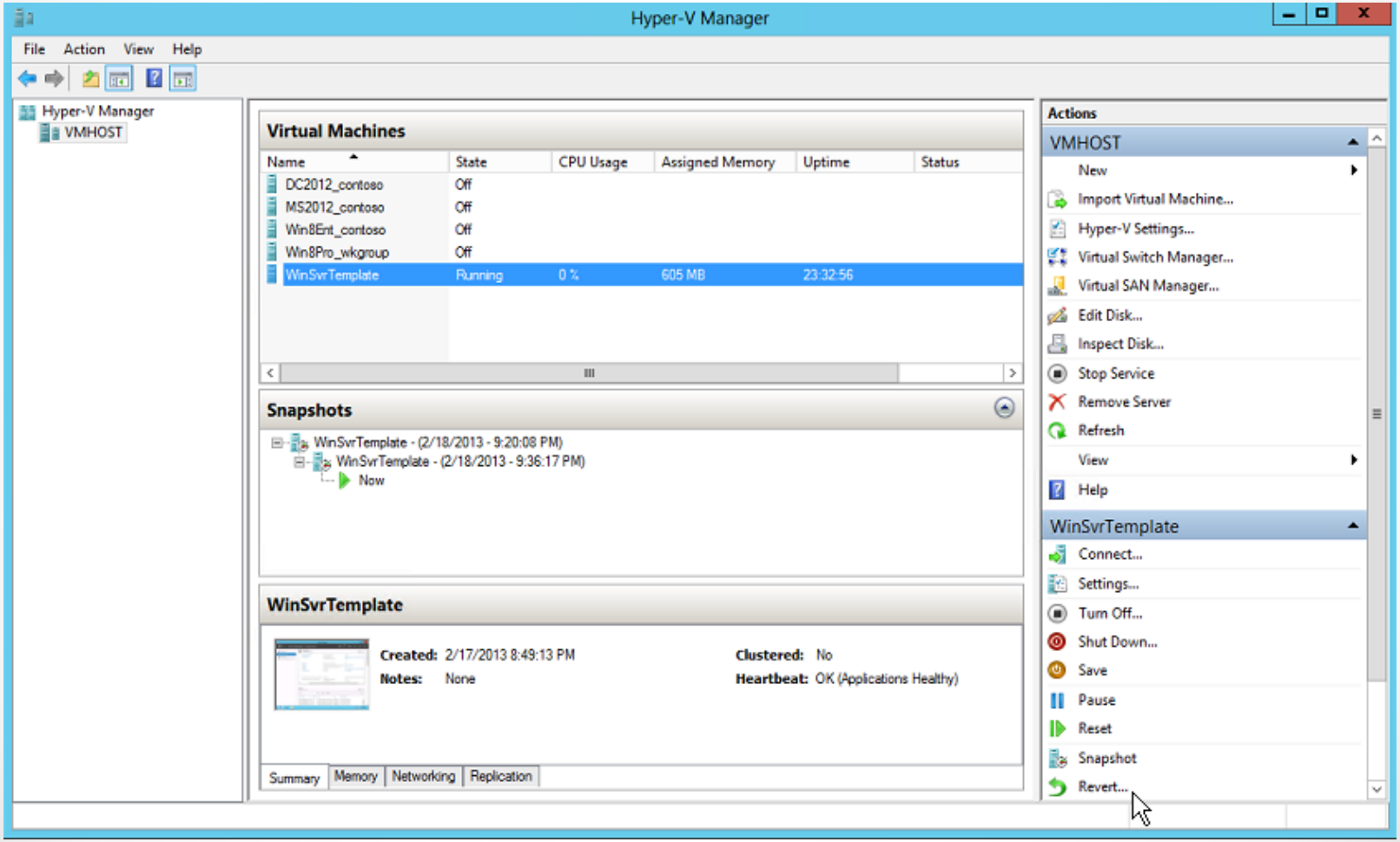
MSConfig



System Restore Snapshots

- SCSV, Hyper-V snapshots, and Virtual Machine Backups all offer options for returning files/folders and VMs to a known point in time.
- Remember that Windows 2008 and later server operating systems do not support the creation of system restore points.
- They do provide the ability to use the SCSV feature, Hyper-V snapshots, and VM backup/restore with Windows Server Backup as options for returning to a specific point in time.
- You can use the Revert option within Hyper-V Manager to return a VM to the previous snapshot (called ***reverting***) or to a selected snapshot and use Windows Server Backup to restore a VM.

System Restore Snapshots



Boot Configuration Data Store

- The ***Boot Configuration Data (BCD) store***:
  - Contains information that controls how your server boots.
  - Replaces the boot.ini text file that was used in Windows Server 2003 to manage the boot configuration information.
  - Is located in the \Boot\Bcd directory on BIOS-based operating systems.
  - Is located on the Extensible Firmware Interface (EFI) system partition on EFI-based systems.

Boot Configuration Data Store

- Because the BCD store is a binary file, you can't modify it using a standard text editor such as Notepad.
- Using the ***Boot Configuration Data Editor (bcdedit.exe)*** tool from a command prompt, allows you to:
  - Add, modify, and delete entries in the BCD store.
  - Import/Export entries to/from a BCD store.
  - List the current settings of the BCD store.

Windows Boot Environment

- The boot environment (as shown in Figure 9-17) is split into two components:
  - ***Windows Boot Manager***: Makes it possible for you to choose which boot loader/application to load.
  - ***Windows Boot Loader***: Is a small program or application that moves the operating system into memory.

Bcdedit

- The multi-boot system is configured to boot to Windows 8 after 30 seconds. To change this setting to wait for only 10 seconds, enter the following command:

  `bcdedit /timeout 10`

- To create a backup of this BCD store to a folder named *BcdStore* on drive D:\, enter the following command:

  `bcdedit /export D:\BcdStore`

- You can use the following command to import and restore the backup that was just created using the /export switch:

  `bcdedit /import D:\BcdStore\bcdbackup`

- In the previous multi-boot example, Windows 8 is configured as the default operating system, and it launches if you don't make a selection after the time-out value is reached (e.g., 30 seconds). To make Windows 7 the default operating system to boot after the time-out value is reached, enter the following command:

  `Bcdedit /default {849ab759-2b7d-11e2-9a4d-10bf4879ebe3}`

Bootrec

- In Windows Server 2012, the boot loader (bootmgr) looks for the BCD store on the active partition. If the BCD store is missing or corrupt, you see the "Boot Configuration Data for your PC is missing or contains errors" message or a similar error during the boot process.
- The best approach to take is to rebuild the BCD using the ***Boot Recovery Tool (bootrec.exe)*** by entering the following command after booting to WinRE:

```
Bootrec /rebuildbcd
```

Bootrec

- To export the BCD store, use the following bcdedit.exe command:

```
Bcdedit /export c:\BCDStore
```

- After backing up the BCD store, remove the hidden, read-only, and system attributes from the BCD file so that you can modify it:

```
Attrib c:\boot\bcd -h -r -s
```

- After modifying the BCD file's attributes, rename the existing BCD store using the Ren command:

```
Ren c:\boot\bcd bcd.old
```

- Next, rebuild the BCD store by entering the following command:

```
Bootrec /rebuildbcd
```

- Once the rebuild of the BCD store has completed successfully, you should see that a Windows installation was identified and be prompted to add the installation to the boot list.
- After doing so, reboot the server, and you should be up and running.

Lesson Summary

- You should have a written plan when it comes to recovering your servers.
- Windows Server 2012 provides two options for restoring files and folders: previous versions and Windows Server Backup.
- There are two options for recovering previous versions of files: Copy the files to a new location, which means they will inherit the permissions of the target directory, or restore the files, which means the current version is deleted but the file's permission settings are retained.

Lesson Summary

- The approach used to restore a volume depends on the type of volume to recover. Data volumes can be restored using Windows Server backup, whereas system volumes require the WinRE and Windows installation media.
- WinRE provides a set of utilities that can assist you in troubleshooting and recovering a system that will not boot due to problems with the operating system files, services, and device drivers.

Lesson Summary

- The system state includes the operating system configuration files. Additional items might be included depending on the role of the server (e.g., domain controller's system state includes NTDS and SYSVOL). The system state is included in full backups, bare metal recovery backups, and system state backups.
- Recovering the system state of a domain controller requires you to boot into Directory Service Restore Mode (DSRM).

Lesson Summary

- Non-authoritative restores means you are returning the domain controller to the state it was in when the backup was performed; the restored domain controller will then use normal replication with replication partners to obtain updated information.
- Authoritative restores are used when you want to restore Active Directory object(s) that was accidentally deleted and the change has already replicated to other domain controllers. The goal of this type of restore is to overwrite the copies located on the other domain controllers.

Lesson Summary

- Ntds.util is used to perform an authoritative restore, whereas Active Directory Recycle Bin can be used to avoid the labor-intensive process of performing an authoritative restore if it is enabled prior to any Active Directory objects being deleted.
- Performing authoritative restores can impact passwords, home directory and profile paths, and group membership changes that occurred after the backup was made. To avoid these types of issues, always restore the smallest unit necessary to return your Active Directory to an operational state.

Lesson Summary

- A bare metal recovery restore allows you to restore a server without loading the operating system beforehand. By default, a bare metal restore includes only the system state, system reserved, and critical volumes (those that hold the boot files, operating system and registry, SYSVOL, Active Directory database, and Active Directory database log files) unless you add the data volumes as part of the setup.
- There are several ways to access the Windows Recovery environment to troubleshoot system boot problems: **`shut down /r /o`**; booting from the Windows installation media and selecting Repair Computer; and selecting Settings from the Charms bar, choosing Power, and clicking Restart while holding down the SHIFT key.

Lesson Summary

- Booting in safe mode allows you to troubleshoot situations where you cannot access the system due to faulty hardware, software, device drivers, and virus infections. Once booted into safe mode, you can check system/application logs, run msinfo32.exe to gather details, review the ntbtlog file, and use MSConfig to troubleshoot and repair your server.
- You can use the Revert option within Hyper-V Manager to return a VM to the previous snapshot (called reverting).