CIS 101B Lesson Plan

|  |  |
| --- | --- |
| **Week 2 Class 4** **Thursday 1-5:00 PM Thursday 6-10:00 PM** | **Chapter 9 – System Management**  **(Chapter 9.7 to 9.15)** |

Hands On

|  |  |
| --- | --- |
| **Use the lab PCs to try Windows Utilities**  **Create a MMC, adding Local Users and Groups, and Computer Management  Start/Search/MMC – Enter File/Add-Remove Snap-Ins**  **Create users and groups, using Local Users and Groups Create a new group, create a second user, put the user in that group, show assigning group permissions to a folder or a file**  **Run Performance Monitor, add some counters, generate a report**  **Change UAC settings**  **Use Remote Desktop to connect to other lab pcs Remember you have to log in with credentials on the machine you are connecting to, NOT your local credentials Enable Remote Desktop first: Win-Pause\Remote Settings**  **Run Windows Backup and Restore**  **Create a restore point Win-Pause\System Protection\Create**  **Restore from a Restore Point Win-Pause\System Protection\System Restore** | **Create a Windows 7 Recovery Disc Boot with Window 7 Recovery Disc**  **Create System Restore Point Load back to a previous Restore Point**  **Run Command Prompt from Windows 7 Recovery Disc, run SFC /scannow Then at the same prompt Run bootrec command with the following switches:  /fixmbr: Repairs the master boot record. /fixboot: Repairs the boot sector. /rebuildbcd: Rebuilds the boot configuration data**  **Run net start command to see what services are started, use net start to start a service, net stop to stop a service. net stop themes net start themes**  **Run msconfig to see what programs are starting up with Windows and control programs and services start up behavior**  **Reboot and press F8 before the Windows 7 start screen, look at all options for Advanced Boot Menu Select Safe Mode, look at the environment you get with Safe Mode** |

9.7 Linux Application Management

9.7.4 Linux Application Management Facts

When installing software on a Linux system, you usually install a precompiled application or service from a software *package*. Packages contain executables (and other files) that have been precompiled and configured for a specific hardware architecture and Linux distribution.

Use the shell commands listed in the following table to manage the applications and processes on Linux:

|  |  |
| --- | --- |
| **Command** | **Description** |
| yum | The yum command installs packages on Linux systems that use the Red Hat Package Manager (RPM). The yum command can automatically locate and download RPM packages for you by searching one or more repositories on the Internet. It can install the package and all of its dependencies at the same time.  The syntax for using yum is as follows:   * **yum install *package\_name*** installs the specified package. * **yum remove *package\_name*** uninstalls the specified package. * **yum list installed** lists all packages installed. * **yum list installed *package\_name*** checks to see if the specified package is installed. * **yum list available** displays a list of all packages available for installation within the Internet repositories yum is configured to use. * **yum list updates** generates a list of updates available for all installed packages. * **yum update *package\_name*** installs updates for the specified package. * **yum info *package\_name*** displays information about the specified package, including its version and dependencies. * **yum search *keyword*** searches for any packages that contain the specified keyword in the description, summary, or package name fields within the Internet repositories yum is configured to use. |
| apt-get | The apt-get command installs packages on Linux systems that use the Debian Package Manager (dpkg). The apt-get command can automatically locate and download Debian packages for you by searching one or more repositories on the Internet. It installs the package and all of its dependencies at the same time.  The syntax for using apt-get is as follows:   * **apt-get install *package\_name*** installs the specified package. * **apt-get remove *package\_name*** uninstalls the specified package. * **apt-get update** displays information about all packages available within the Internet repositories apt-get is configured to use. * **apt-get dist-upgrade** upgrades all installed packages to the newest version. |
| ps | The ps utility is used to display running processes on a Linux system. Many options can be used with the ps command. Several commonly used options include:   * **ps** displays only those processes associated with the current shell session. * **ps -e** displays all processes running on the system. * **ps -f** displays extended information about processes. This option can be combined with the **-e** option to display extended information about all of the processes running on the system. * **ps -l** displays information about processes in long format. This option can be combined with the **-e** and **-f**options to display extended process information in long format.   The following fields can be displayed in the output of the ps command, depending upon which options are included with the command:   * **PID** displays the process ID of the process. * **TTY** displays the name of the shell session the process is running within. * **TIME** displays the amount of CPU time used by the process. * **CMD** displays the name of the command that was run to create the process. * **UID** displays the user ID that owns the process. * **PPID** displays the PID of the process's parent. * **C** displays the amount of CPU utilization consumed by the process. * **STIME** displays the time that the process started. * **F** displays any flags associated with the process. * **S** displays the current state of the process. * **PRI** displays the priority of the process. * **NI** displays the nice value of the process. * **SZ** displays the size of the process in RAM. |

Use the **man *utility\_name*** command at the shell prompt to view the syntax along with all of the options that can be used with these commands.

9.8 Digital Content Management

9.8.3 Digital Content Management Facts

PC administrators need to be familiar with the following digital content management issues:

* Software licensing
* Digital Rights Management (DRM)

**Software Licensing**

It is important to understand how software licensing works because violating software license agreements could potentially expose your organization to litigation. There are two general software licensing models that you need to be familiar with:

|  |  |
| --- | --- |
| **License Type** | **Description** |
| Proprietary | The proprietary licensing model used by many software vendors. Each vendor you purchase a proprietary license from should provide an End User License Agreement (EULA) that dictates the specific terms for that particular software title.  There are several key facts that you need to remember about proprietary software licensing:   * When you purchase this type of software, you are not purchasing the software itself. Instead, you are purchasing a license to *use* the software. * You are not allowed to access the software's source code and make modifications. Usually, the source code is not made available to customers. A EULA does not typically allow you to reverse engineer the software to recreate the source code. * The license usually only permits you to install the software on a fixed number of computers. Installation limits are commonly enforced by the software vendor using online software activation. If you try to use the same activation code too many times, the software will not activate and can't be used.   Two different, general types of licenses are usually offered by software vendors:   * *Personal licenses* are intended for home and small business customers. Usually, they only allow the software to be installed on 1-3 systems. Because they are limited in the number of allowed installs, personal licenses are usually less expensive than other alternatives. However, personal licenses many not be the best choice for large organizations, which may need to purchase hundreds or even thousands of licenses for a given software title. * *Enterprise licenses* (which are also sometimes called *volume licenses*) are intended for medium and large organizations. Enterprise licenses allow the customer to install the software without restriction using the same activation code (typically until a maximum cap is reached). Because of the volume involved, the customer is usually able to purchase an enterprise license for much less than the cost of purchasing individual personal licenses. Enterprise licenses are usually too expensive for most home or small business users. |
| Open Source | Open Source software used to be exclusive to Linux and Unix operating systems. However, many Open Source applications are now available for Windows and Mac operating systems. Open Source licensing is very different from proprietary licensing:   * Open Source software is usually freely distributed. You can typically download, install, and use the software without paying a license fee. * Most Open Source software is distributed under the GNU General Public License (GPL), which requires that the source code for the software to be freely distributable to anyone who wants it. This means you can download the source code for an application, modify it, recompile it, and then use the modified version of the software. In fact, you could even post it for others to use as long as you make your source code freely available as well.   Organizations that release open source applications typically use a variety of means to generate revenue so they can keep developing new products:   * Contributions. Some Open Source projects ask you to contribute financially if you use their software. * Added functionality. Some Open Source projects release a base version of their software for free, but then charge a fee for highly desirable add-ons. * Support contracts. Some Open Source projects release their software for free, but then charge a fee for technical support. * Training contracts. Like support contracts, some Open Source projects also provide training for a fee. * Partnerships. Sometimes an Open Source project will partner with a commercial organization. In this situation, two versions of an application will be created, one that is proprietary and one that is Open Source. The proprietary version is typically used to finance the development of the free version. * Subscriptions. Sometimes an Open Source project will sell subscriptions for online accounts or server access. |

**Digital Rights Management**

System administrators are frequently responsible for ensuring that intellectual property rights are observed on the computers and mobile devices they are responsible for. To protect the intellectual property rights of publishers, several Digital Rights Management (DRM) technologies have been implemented over the years. The goal of these technologies is to restrict the use of copyrighted works to only those who have paid the necessary licensing fees:

|  |  |
| --- | --- |
| **DRM Technology** | **Description** |
| Software activation | Many proprietary software vendors use online software activation. Before the user can run a newly installed application, it must be activated online with the software vendor. The software vendor tracks how many times each license code is activated and will block further activations after the license limit has been met. For personal software licenses, the limit is usually 1-3 activations. Enterprise license limits are governed by the enterprise license agreement. For example, an organization may purchase a 100-user license from the software vendor.  Two different forms of online software activation are used by software vendors:   * *One-time activation*. With one-time activation, the license is activated once, usually right after the product is installed. Once activated, the product remains activated. * *Persistent activation*. With persistent activation, the license is continuously re-activated online at a preconfigured interval. This allows the software vendor to deactivate installations if the conditions of the license agreement have been violated.   Using online activation helps software vendors ensure their products are used in compliance with the license agreement. However, it also has several drawbacks:   * Online activation mechanisms can fail if an internet connection isn't available. * A small system change can deactivate the software. For example, adding RAM to the system or upgrading the CPU could cause the activation system to think the application has been illegally copied to a new computer system. The customer typically has to contact the vendor to reactive the software. * Operating system upgrades or migrations can deactivate the software. |
| Media DRM | DRM has commonly been used with digital media files, including books, music, and videos. In the late 2000's most online digital media vendors implemented DRM to encrypt media files. Without the appropriate key, the files couldn't be decrypted and played by the customer.  In recent years, however, there has been a movement away from DRM on the part of many large digital media vendors. This has occurred because of several key shortcomings of DRM, including:   * A lack of portability. For example, DRM-protected digital files from a given vendor would only play using software or hardware from that same vendor. * A lack of backup support. DRM protection frequently made it such that protected digital files could not be backed up. * Weak encryption. Many applications are available on the Internet that can strip DRM protection from digital files. * Obsolescence could cause older digital files to no longer be playable on newer hardware. * Excessive management overhead. Trying to manage DRM for legally purchased digital files required an excessive amount of management overhead on the part of the digital media vendor. Small system errors on the vendor's network could cause customers to lose access to digital files that were legally purchased.   To address these shortcomings, many vendors have adopted DRM alternatives such as:   * Encouraging customers to not illegally share digital files * Making digital files so inexpensive and easy to access that it doesn't make sense to make illegal copies |

9.9 Updates

9.9.3 Update Facts

Updates are periodically released to:

* Fix bugs (errors) in programming code
* Patch security vulnerabilities
* Add features or provide support for new hardware

There are two types of Windows updates:

|  |  |
| --- | --- |
| **Update Type** | **Description** |
| Hotfix | A *hotfix* is an operating system patch that fixes bugs and other vulnerabilities in the software.   * Hotfixes may be released on a regular basis as fixes are created. * For the highest level of security, apply hotfixes as they are released (after you verify that the hotfix will not cause additional problems). * Microsoft identifies each hotfix by a number. This number also identifies a Knowledge Base (KB) article that describes the issues addressed by the hotfix. |
| Service pack (SP) | A *service pack* (SP) is a collection of hotfixes and other system enhancements.   * A service pack includes all hotfixes released to that time. If you install the service pack, you do not need to install individual hotfixes. Installing a service pack also includes all previous service packs. * Service packs might include additional functionality beyond simple bug fixes. |

Windows Update is a feature of the Windows operating system that helps you keep your computer up to date.

* By default, Windows automatically checks for updates, downloads them, and installs them during the automatic maintenance window (which is 2:00 AM by default).
* Updates are classified as Important, Recommended, and Optional. By default, Important and Recommended updates are installed automatically.
* Windows Update can install both hotfixes and service packs. For example, after installing a new version of Windows, Windows Update will download and install the latest service pack.
* Windows Update includes updates for the following:
  + Windows operating system and utilities
  + Drivers that have passed Microsoft certification and that are made available through Windows Update
* You can turn off automatic downloading or installation of updates. For example, on Windows 7 and Windows 8 you can configure your computer to:
  + Not check for updates (you can manually check for updates at any time)
  + Notify you of updates, but require your permission to download or install them
  + Download updates, but ask your permission to install them
* You can view a list of installed updates and remove any updates.
* For additional updates, you can use Microsoft Update in conjunction with Windows Update. Microsoft Update includes updates for Microsoft applications, such as Office applications.

You should be aware of the following facts when working with updates:

* Non-Microsoft applications and many drivers are not updated through Windows Update.
* To manually check for updates for applications or drivers, go to the manufacturer's website.
* Many applications include a feature that automatically checks the manufacturer's website periodically for updates. These programs typically ask your permission to install updates.
* Hardware devices, such as the BIOS or many networking devices, store code in a special hardware ROM chip. This software is referred to as *firmware*. Updates are done by *flashing* (replacing or updating) the code stored on the chip.
  + Always follow the instructions when performing firmware updates.
  + Many updates are performed through a browser; some updates can only be performed by booting to special startup disks while outside of Windows.
  + Turning off the device or interrupting the update process could permanently damage the device.
* Both hotfixes and service packs are specific to an operating system version. For example, a hotfix for Windows 8 will not work on Windows 10. However, a hotfix for Windows 10 Home will typically also apply to Windows 10 Professional.
* In a business environment, it is wise to test updates in an isolated lab environment (called a *sandbox*) before rolling them out to production systems.

9.10 System Backup

9.10.2 Backup Facts

A *backup* is a copy of data that is archived and which can be used to restore corrupt or lost data in the event of a hardware or system failure. Backups must be performed while the system is in good working order. In other words, you must plan for disasters ahead of time and take the necessary actions to protect your system before there is a problem.

Backup tools may be used to protect different types of data:

* *System state* data includes all of the files required to boot and run the computer. System state data includes the operating system files, the registry, drivers, and any configuration files.
* *User data* includes all data files saved and modified by users or applications that users run. The user data is the most important data for a company. Because user data changes constantly, back up the user data frequently and on a regular schedule.
* *Application data* includes files installed by an application and application configuration files. Application data changes only following the installation of an application or following a configuration change. Depending on the system you are using, a backup of system state data might include backing up all application files as well.

Use the following tools to protect Windows systems:

|  |  |
| --- | --- |
| **Windows Version** | **Tools** |
| Windows 7 | On Windows 7 systems, the backup process is managed using the Backup and Restore console in Control Panel. The Backup and Restore console supports two types of backups:   * A *system image backup* backs up everything on the system to a .vhd file, including the operating system, installed programs, drivers, and user data files. A system image backup is the most complete type of backup, but also takes the longest time to create. * A *file backup* backs up specific files and folders up to a compressed file. File backups do not include system files, program files, encrypted files, files in the Recycle Bin, user profile settings, or temporary files.   The Backup and Restore console leverages the shadow copy feature of the Windows file system to allow files to be backed up even if they are open when the backup runs. The initial backup process backs up all of the files specified in the job. However, subsequent backups will evaluate the state of the file system and only backup files that have changed since the last backup was run. As a result, the first backup will take quite some time to complete, but subsequent backups will run much faster.  On Windows 7, backups can be saved to several different types of storage media:   * Secondary internal hard drives * External hard drives * Optical drives * USB flash drives * Network shares   Backup files cannot be saved to:   * The same disk that is being backed up * A disk containing the Windows operating system * A tape drive   System images created with the Backup and Recovery Console cannot be saved to:   * Flash memory * A tape drive * A recordable DVD   On Windows 7, file backups occur every Sunday at 7:00 pm by default. However, the backup schedule can be customized. A system image backup cannot be scheduled, but a system image backup can be included within a scheduled file backup. |
| Windows 8.x | The Backup and Restore console used to backup data on Windows 7 is not included in Windows 8.1. Instead, *File History* is used in Windows 8.1 to backup user profiles. A profile backup includes all of the information stored in the user’s library folders:   * User data files, such as documents, music, and videos * User preferences, such as the desktop background, screensaver, color schemes, contacts, browser favorites, and so on * User account details, such as the username, password, and so on   File History does not back up the entire system. Only the data in a user’s profile is backed up. However, a user can add folders to a library to back them up using File History. File history backs up files in the background. Once every hour, File History creates a shadow copy of user account files. This creates a snapshot of user account's files at a particular point in time. After creating the shadow copy, Windows keeps track of the prior versions of those files. Once done, users can browse and restore previous versions of files.  File History is disabled by default. When enabling File History, the location for storing the backup must be specified. A drive other than the drive the user files are already on must be specified. At least two drives must be implemented system to use File History. A best practice is to use a second internal hard disk drive. However, external flash drives or hard disks can also be used. In this configuration, File History must be disabled before disconnecting the external drive.  When File History is enabled, Windows monitors users' libraries, desktop, contacts, and Internet Explorer favorites. By default, File History checks once an hour to see if any data has changed since the last check. If it has, File History saves copies of the changed files to the configured location. Once done, a previous version of a file can be restored if a file gets lost or corrupted.  Like Windows 7, Windows 8.1 also supports the creation of system images. Where File History only backs up user files, a system image backs up the entire system, including operating system files, registry settings, installed applications, and so on. Keep the following considerations in mind:   * To protect user data, File History is the best option because lost or corrupted files can be quickly restored. * To protect the system itself, a system image is the best choice because it can be used to restore the entire computer. Individual files can't be restored from a system image backup. |
| Windows 10 | Windows 10 includes many backup tools used in earlier versions of Windows:   * The Backup and Restore console tool that was removed from Windows 8.1 has been restored in Windows 10. * Windows 10 includes File History, as found in Windows 8.1. * Windows 10 includes the option to create a System Image Backup, as found in Windows 7 and Windows 8.1. |

Keep the following facts in mind when configuring backups:

* Back up user data more often than system state data (it changes more frequently).
* Backup system state data and applications (or make a restore point) before you make a system change.
* During a system state backup, all system configuration information is backed up (system data cannot be backed up selectively in portions).
* Be sure to test your backup and restore strategy. It does no good to back up your data if you can't restore it.
* Backup media should be stored offsite to prevent the same disaster from affecting the network and the backup media.
* Backups can be scheduled using the tools within the backup utility, or by creating a new task in the Scheduled Tasks folder in the Control Panel.

9.11 System Protection

9.11.4 System Protection Facts

The following tools can be used to protect a Windows system:

|  |  |
| --- | --- |
| **Tool** | **Description** |
| System Restore | System Restore automatically takes snapshots (called *restore points*) of your system. You can use these restore points to roll back your computer to a specific point-in-time configuration.   * Restore points take snapshots of system files, registry settings, program files, and other batch, script, or executable files. Restore points do not protect user data files. * Automatic restore points are created in the background at regular intervals (by default once a day) as well as before configuration changes are made such as installing an application, installing an unsigned driver, or making other system changes. You can also manually create a restore point. * When you restore your system to a restore point, previous settings are restored, while subsequent changes are removed. For example, any applications installed after the restore point are no longer installed. * User data is not modified when restoring to a restore point. You cannot use a restore point to recover user data, and any changes made since a restore point are retained following the restore. * System Restore works only on NTFS partitions. Restore points are automatically saved to the same disk using up to 15% of the available disk space by default. You can customize the amount of disk space used for restore points. * System Restore is enabled automatically on the system hard drive where Windows is installed. |
| Previous Versions | Previous Versions (also called Shadow Copies) takes snapshots of files and folders and protects against accidental deletion or modification of user data files.   * Previous Versions is available in the Business, Ultimate, and Enterprise editions of Windows 7. **It has been replaced by the File History feature in Windows 8 and Windows 10.** * It is turned on by default, and takes regular backups of files that have changed. * Backups are saved on the same disk. Previous Versions does not protect against disk failure. * Previous Versions works on entire folders as well as individual files. * When you view a previous version of a file, it is opened in Read-only mode. You can browse through a previous version of a folder, navigating the directory structure. * When you restore previous versions, you can copy the previous version to a new location, or restore it to the same location (overwriting the existing version). * Previous Versions works only on NTFS partitions. |

9.12 System Recovery

9.12.8 System Recovery Facts

System recovery procedures are necessary when you are unable to boot the computer, or when other problems prevent it from working properly. Before using recovery tools, try other methods to resolve the problem including:

* Removing problematic hardware or software
* Updating drivers, applications, and operating system files
* Booting into Safe Mode to disable devices or roll back drivers

If these steps do not resolve the problem, use the following tools to recover the system:

|  |  |
| --- | --- |
| **Method** | **Description** |
| System Restore | You can use a restore point to revert your system to a previous point in time when it was working properly. When using a restore point:   * System changes made since the restore point was taken are undone. Any applications, device drivers, or patches installed since the restore point was taken will be removed when the system is reverted to that restore point. * User data is not affected; any files that have been changed since the restore point was taken will remain unchanged when the system is reverted to that restore point.   Start System Restore using one of the following methods:   * If the system can boot into Windows, open Control Panel and go to **System and Security** > **System** >**System Protection** > **System Restore**. * If the system can't boot into Windows, boot the computer from the Windows installation disc and repair the installation. Select **Troubleshoot** > **Advanced Options** > **System Restore**. |
| Startup Repair | If Windows won't boot, you can use the Startup Repair option to automatically fix problems. Boot the system from the Windows installation disc and repair the installation. Select **Troubleshoot** > **Advanced Options** >**Startup Repair**. The repair process does the following:   * Inspects and repairs the boot sector * Verifies that Windows boot files exist and are correctly configured * Compares the checksum for all Windows system files to make sure that they match what's on the installation disc |
| Command Prompt | The Windows Recovery Environment provides a Command Prompt option that you can use to manually diagnose and repair system problems. Boot the system from the Windows installation disc and repair the installation. Select **Troubleshoot** > **Advanced Options** > **Command Prompt**. You can use the Command Prompt option in the Recovery Environment to:   * Read boot logs * Enable and disable services * Read and write data to the hard disk drive * Overwrite corrupt or incorrect files (such as repairing a corrupt registry or restoring corrupt operating system files) * Format and partition drives * Repair a corrupted master boot record   When using the Command Prompt to troubleshoot problems, you should first research your problem at the Microsoft Website and print the exact instructions for performing recovery procedures. The Command Prompt provides dozens of commands to display information and make changes. You can access a complete description of these commands and their syntax by typing **help** or **help / [command]** at the Command Prompt. |
| System Image Recovery | If you are unable to repair a system using a restore point, automatic repair, or from the Command Prompt, you can restore the system from a system image backup.   * The restore process reformats hard drives, destroying all existing data. * The restore process restores all of the volumes you selected during the system image backup, including all user data on those volumes. However, any changes made since the last time the system image was created will be lost. * You cannot restore individual files from a system image backup. * You can use the following options to restore from a system image backup:   + If the system is bootable, open Control Panel, then select System and Security > Backup and Restore.   + If the system is not bootable, boot the system from the Windows installation disc and repair the installation. Select **Troubleshoot** > **Advanced Options** > **System Image Recovery**. |
| Refresh or Reset This PC | Windows 8 and Windows 10 both provide advanced recovery options for malfunctioning systems:   * Windows 8:   + **Reset Your PC**: Resetting your PC reinstalls Windows on the system. No configuration settings or user files will be preserved. All apps installed by the user will be removed. Only the apps that came with the PC will be reinstalled.   + **Refresh Your PC**: Refreshing your PC also reinstalls Windows, but your user files and settings are preserved. It also retains the apps that came with the PC as well as any apps you installed from the Windows Store. * Windows 10:   + **Reset This PC**: Refreshing PC also reinstalls Windows, but your user files and settings are preserved. It also retains the apps that came with the PC as well as any apps you installed from the Windows Store.   To use one of these options, boot the computer from the Windows installation disc and repair the installation. Select **Troubleshoot** and then the refresh or reset option you want to use.  The **Reset** option behaves differently on Windows 8 versus Windows 10. |
| Recovery disc/partition | If you purchased your system from a major PC manufacturer, it may include a recovery partition on the hard drive.   * Using the recovery disc/partition restores the system to the state it was in when shipped. * The recovery process typically restores a Windows image, which erases the hard drive. * Any applications and user data files added since the system was shipped will be lost. If possible, back up any data accessible on the hard disk before performing the recovery. * If the system has a recovery partition, the partition might not be visible from within the operating system. To use the recovery partition, edit the BIOS or boot using a special key combination as dictated by the manufacturer.   Because using the factory recovery option removes configuration settings and user data, it should only be used as a last resort and only in combination with a good backup. |

Use the following methods to recover lost data files:

|  |  |
| --- | --- |
| **Method** | **Description** |
| Previous Versions | In Windows 7, you can use the Previous Versions feature to restore files. Using Previous Versions is often the fastest way to recover lost, modified, or corrupt files.   * To restore a file to a previous version, edit the file properties and use the Previous Versions tab to select the version you want to restore. * To restore a deleted file, view the properties of the folder containing the file. On the Previous Versions tab, open a previous version of the folder to view its contents at that time. * You can restore the original file overwriting the existing file, or restore it to a different location. |
| Backup and Restore | **In Windows 7 and Windows 10**, you can use Backup and Restore from within Control Panel to restore files from a backup set. When you restore files from a backup, you restore the file as it existed when the backup was taken. **You can restore individual files or complete folders from the backup.** |
| File History | **In Windows 8 and Windows 10**, you can use File History from within Control Panel to restore files or folders. When you restore files using File History, you restore the file as it existed when the snapshot was taken. |

9.13 Virtual Memory

9.13.3 Virtual Memory Facts

*Virtual* memory is simulated memory that is implemented as a page file on a hard drive. Virtual memory is used by operating systems to simulate physical RAM using hard disk space. The process of moving data from RAM to disk (and back) is known as *swapping* or *paging*. **The Virtual Memory Manager (VMM) is in charge of swapping data between physical memory and the hard disk.** The VMM follows the following steps to manage applications:

1. The VMM assigns virtual addressing to an application. This is known as *logical segmentation*.
2. The application is then loaded into physical RAM (absolute address space). The process doesn't recognize its location in physical RAM; it only recognizes its virtual space.
3. As the user launches other applications, the VMM will allocate space to those applications in true physical RAM.
4. When there is no more space in physical RAM, the VMM will take the application that hasn't been used for the longest period of time and place it in the *page file* on the hard drive. This is known as *paging out*. Likewise, when an application is moved from the page file back into physical RAM, it is known as *paging in*.
5. If the system needs access to an application that has been paged out from physical RAM, this causes a problem known as a *page fault*. When this happens, the VMM will page out the program in the physical RAM that hasn't been used for the longest period of time to the page file on the hard drive, and will page in the application currently being accessed back to the physical RAM.

Some things to remember when working with virtual memory are:

* Accessing data stored in RAM is faster than accessing data on disk (or in virtual memory).
* Symptoms of low physical memory include slow system performance when running applications, or slow response when switching between applications.
* Disk thrashing occurs when the amount of physical memory is so low that data must constantly be moved from physical RAM, to disk, and then back again.
  + Symptoms of disk thrashing include high disk access statistics and the hard drive light being lit constantly when no data is being written to or read from the hard disk.
  + To prevent disk thrashing, either run fewer applications or add more physical RAM.
* Manage virtual memory performance using the System Control Panel applet (use the **Advanced** tab).
* By default, the Windows operating system manages virtual memory settings. The automatic settings are usually adequate. However, the maximum size of the virtual memory paging file and the disk where the paging file is stored can be manually configured.
* The most common recommended minimum page file size is about 1 times the amount of physical RAM plus an additional 256 MB to 512 MB. However, there are exceptions to this rule:
  + Systems that have a very small amount of physical RAM installed may require a page file that is 2 times the size of the installed RAM.
  + Systems with a moderate amount of physical RAM installed may require a page file that is 1.5 times the size of the installed RAM.
  + Systems with very large amounts of physical RAM installed typically don't require a large page file.
* To increase performance, move the page file to a different physical disk than that used by the operating system.
* If the paging file is on the system drive, Windows creates a memory dump file if the system crashes. Support personnel might be able to use this file to help identify what caused the system crash. To save a memory dump, the paging file must reside on the system partition.

9.14 Operating System Troubleshooting

9.14.4 Application Troubleshooting Facts

When troubleshooting applications, it is always best to check a knowledge base on the manufacturer's website or search on the Internet for an answer to the problem first. The following table contains guidelines for troubleshooting common application issues:

|  |  |
| --- | --- |
| **Problem** | **Troubleshooting Method** |
| Shortcut malfunction | Installation of an application may create a shortcut on the desktop. The *shortcut* is a pointer file that identifies the location of the executable file that runs the application.   * During install you can often choose to add shortcuts for only the current user or all users. * Shortcuts will cease to work if the file to which they point is moved or altered, or if a drive has been remapped to a different drive letter (which can happen when working with removable media). * Some issues can be resolved by fixing the shortcut instead of re-installing the application. * Edit the properties of the shortcut to correct many application-related issues:   + Use the **Target** field to point to the executable location.   + Use the **Start in** field to identify a working directory for the application. |
| Installation issues | Application installation involves more than just copying the executable files to the computer. Installation typically modifies the registry, creates shortcuts, creates Start menu tiles, and configures other settings required by the application.  Users must have the appropriate permissions to install applications. The ability to install applications depends on the user's group membership and the operating system:   * Users who are members of just the Users group are not allowed to install applications. * On older versions of Windows, users who were members of the Power Users group could install applications as long as the installer did not modify system files. On modern versions of Windows, Power Users cannot install applications at all. * Users who are members of the Administrators group can install applications.   If an application's files get deleted or become corrupted after installation, they can be repaired by doing one of the following:   * Some applications provide the Repair option in Programs and Features. When selected, the Repair option inspects all of the application's files and replaces files that are missing or corrupt. * If an application does not provide the Repair option in Programs and Features, it must be first uninstalled and then reinstalled to repair missing or corrupt application files. |
| Windows compatibility | Because some applications use elements that are specific to a certain version of an operating system, you may run into problems when trying to use these same programs on newer operating systems. Windows Compatibility Mode is designed to correct this problem by creating an environment that emulates the operating system for which the application was originally intended.  In compatibility mode, you choose a target operating system (such as Windows Vista). When the application runs, it appears as if the application is running on the target operating system. To configure Compatibility Mode for an application, edit the properties of its shortcut or executable file. On the Compatibility tab, configure the following as appropriate:   * Operating system compatibility mode * Reduced color mode * Run in 640x480 screen resolution * Disable display scaling on high DPI settings * Run the program as an administrator   If you're not sure which settings to use, you can run the Compatibility Troubleshooter from the Compatibility tab. This utility will probe the application and automatically determine the correct compatibility settings.  Windows 7 Enterprise and Ultimate editions also provide *Windows XP Mode*. This feature is not included with the operating system and must be downloaded separately. Windows XP Mode provides a Windows Virtual PC containing a pre-installed copy of Windows XP Professional. You can use this virtual machine to run older applications that don't run correctly on Windows 7. The applications running within the virtual environment are accessed using the Remote Desktop Protocol and thus appear to be running on the Windows 7 host operating system itself. |
| Permissions | On older versions of Windows, applications ran with the privileges associated with the user who ran the application. But on modern versions of Windows, applications run by default as a standard user, even if the user who launches the application is an administrator. This is done to contain damage that could potentially result if the end user launches a poorly-written or malicious application. However, some applications need to run with administrative privileges to be able to complete necessary tasks.  Be aware of the following permission-related issues when running applications:   * Using UAC in modern versions of Windows, applications run with standard user privileges by default. The user will be prompted if the application requires elevated permissions. * Older applications written for previous versions of Windows may not be compatible with UAC. They may assume that they can run with administrator-level privileges. * Applications with insufficient permissions might not run, or they might run but not function correctly (or some features might not be available). If this happens, you can run the application:   + In compatibility mode. You can mark the **Run this program as an administrator** option on the Compatibility tab to automatically elevate privileges when the application is run.   + As administrator. To do this, right-click the application shortcut or executable file and choose **Run as administrator** * Many applications create data files as they run. They may also create temporary files. The user running the application must have sufficient file system permissions to the directories where these files will be created. |
| Error reporting | Windows Error Reporting is a feature of Windows that enables Microsoft to be notified of application faults, system unresponsiveness, and kernel defects. Microsoft uses these error reports to diagnose the cause for common problems, then, if possible, improve upon their product or supply troubleshooting techniques. Each time an error occurs, a dialog box will appear that prompts you to report the problem to Microsoft. If you are connected to the Internet and you choose to report the problem, technical information about the problem is sent to Microsoft. If known information about the problem you have experienced is available, you will receive a link to a Web page that contains information about the problem. |
| Service fails to start | During or shortly after startup, you might see an error message stating that a service has failed to start.   * Check the Event Viewer for additional information about which service failed to start and the reason why it did not load. * Try using the Services console or the NET START command to manually start the service. * If the service is not required, you can change its startup type to Manual in the Services console to prevent it from trying to load during startup. * If the service is necessary, use the Services console to make sure that any dependent services are configured to start and have started successfully. * Verify that the service is configured with a valid user account and that the password has not changed. If an account other than the Local System account is used, make sure that the service is configured with the correct password (when you change the user account password, you must also change the password configured by the services that use that account). |
| Hung Applications | If an application hangs and won't exit properly, you can use Task Manager to force it to close. This can be done in two ways:   * Select the hung application on the Processes tab and click **End Task**. * Right-click the hung application on the Processes tab and select **Go to Details**. Then, with the application's process selected on the Details tab, click **End Task**. |
| Process priority | By default, the Windows operating system kernel tries to evenly distribute access to system resources to all processes running on the system. However, if a process needs to run with a higher priority than the other processes on the system, its priority can be manually configured. Right-click on the process in Task Manager, select **Set Priority**, and then select a priority level. |
| Processor affinity | In a multicore or multiprocessor system, the Windows operating system kernel will automatically distribute processes across all available processes. However, a process can be constrained to run only on certain processors. Right-click on the process in Task Manager, select **Set Affinity**, and then mark the processors that the process is allowed to run on. |

9.14.6 System Errors Facts

Errors, lockups, and system crashes are typically caused by the following:

* Software bugs (errors in an application, the operating system, or driver code)
* Corrupt or missing operating system files
* Incorrect, corrupt, or incompatible device drivers
* Overheated hardware
* Failing hardware (memory, hard disk, or other component)

A *Blue Screen of Death* (BSOD), also called a stop error, is an error that is so severe that Windows can no longer continue to function. When this type of error occurs, the system will stop and display a blue screen with information related to the error. **On Mac OS, you may see the cursor turn into a pinwheel and you can't do anything. This is sometimes called the *Pinwheel of Death*.**

When a problem occurs, use basic troubleshooting to identify and isolate the problem. With system errors, often the cause is difficult to locate. Use the following suggestions:

* Identify the conditions when the error occurs. Does the error happen only when running a specific program or accessing a particular hardware device? Does it only happen after running the system for a while? Identify running programs and loaded device drivers.
* Capture any error messages displayed. A smart phone is a great tool for doing this. Then check Event Viewer for recent events. Use the Internet to search for solutions based on the error.
  + The vendor's site will usually provide the best knowledge-base. If you have the exact error message captured, search for the error message text.
  + If the vendor's site doesn't provide a solution, you may want to consider using Google to see if there are other recorded instances of your problem.
  + Windows Reporting is a feature that reports application errors to Microsoft. If known information about the problem you have experienced is available, you will receive a link to a Web page that contains information about the problem.
* Start with recently installed or updated hardware or software. If necessary, remove the new component and see if the problem goes away.
* Update operating system files, applications, and device drivers that are related to the error condition.
* Inspect the system hardware.
  + Make sure that cables are plugged in, that there aren't any bent pins, and that cards are properly seated in expansion slots.
  + Look for worn or frayed cables that might be causing a short.
  + Check status lights on components that indicate whether the device is receiving power or functioning normally.
  + Check components for dark spots that might indicate electrical shorts.
  + Listen as the system is running. Can you hear the fans running? Are there any unusual sounds?
  + If you see smoke or smell something burning, shut off the system immediately to prevent damage or hazards.
  + Look for dust buildup on components. Clean components as necessary.
* Run utilities to diagnose hardware components.
  + Monitor the system temperature to ensure components are not overheating.
  + Use a memory tester to verify that the memory modules are functioning properly.
  + Use Scan Disk to check hard disks for bad clusters.
  + View S.M.A.R.T. data to see if hard disks are failing.
* When troubleshooting operating system problems, the system log files can be an invaluable resource for identifying exactly what happened. For example, Event Viewer displays messages generated by the Windows operating system and by applications running on the system. Each entry is categorized according to the severity of the issue it describes:
  + Information
  + Warning
  + Error
  + Audit success/failure

Windows stores these messages in the following logs:

* + The Application log contains application-related events.
  + The Security log contains security-related events.
  + The Setup log contains events related to an application installation.
  + The System log contains system-related events, such as system modifications, malfunctions, and errors.

Be aware of the following common problems and causes:

* To prevent corrupt system files, ensure that end users shut their systems down cleanly.
* Sometimes a system may seem to be locked up, but in reality the system is just running slowly. This condition may be caused by several factors:
  + The processor is over-utilized. Give the system time to finish some tasks, or close unnecessary applications to see if the unresponsive program resumes.
  + The system is infected with malware. To prevent this, run full antimalware scans on a regular basis.
  + The system has inadequate memory installed. If this is the case, add more memory to the system.
  + The system has inadequate video hardware. Avoid using integrated video adapters. A video adapter board with adequate video memory will perform much better.
  + The page file configuration has not been optimized. You can improve performance by moving the page file to a disk other than the system disk. Creating page files on multiple storage devices can also increase system performance.
  + The hard disk is overly full and heavily fragmented. Upgrade to a bigger disk and keep it defragged regularly.
  + There are unnecessary applications being loaded at system startup. Use Task Manager turn off startup applications that aren't used frequently. Uninstall applications on the system that aren't needed.
* If you have a specific application that stops responding, you can use Task Manager to end or stop the application. Be aware that you might lose any data generated by the application.
* Spontaneous reboot can be caused by a bad power supply, device driver, or an overheated CPU.
* Intermittent system crashes without any other apparent cause can be caused by overheated components.
* A noisy fan might be caused by something rubbing on the fan (such as a cable inside the case). If there is nothing touching the fan, then the bearings could be going bad. Replace the fan before it stops working.
* A clicking noise when reading or writing data from the hard disk is an early sign of a failing drive. Move data from the drive as soon as possible.
* A blue screen error that continually references the same memory address could indicate memory that is starting to fail.
* If an error message indicates that a DLL file associated with an application is corrupt or missing, do one of the following:
  + Manually copy a known-good copy of the DLL back into the appropriate location in the file system.
  + Repair the installation (if possible) using the application installer.
  + Uninstall the application and then reinstall it.
  + Restore the system to a prior restore point.
* If an error message indicates that an operating system DLL file is corrupt or missing, do one of the following:
  + Manually copy a known-good copy of the DLL back into the appropriate location in the file system.
  + Restore the system to a prior restore point.
  + Run the system file checker utility from the command prompt. The command is **sfc /scannow**. This utility scans all system files and replaces missing, corrupt, or incorrect versions of these files.

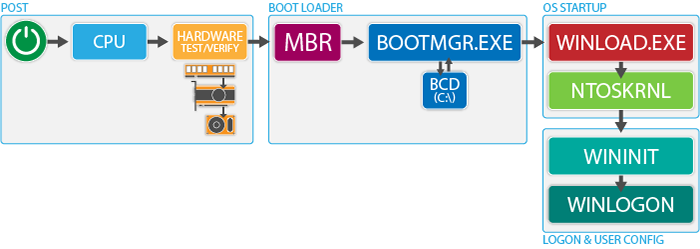
9.15 Windows Boot Errors

9.15.2 Boot Process Facts

Windows systems can boot using either a Legacy BIOS or a UEFI boot sequence. By understanding each of these boot sequences, you can focus troubleshooting efforts on the most likely errors.

**Legacy BIOS Boot**

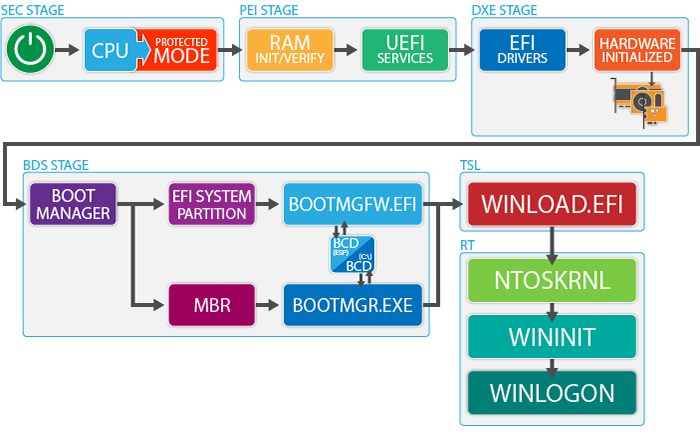
The following diagram and table describe the four basic stages of the Legacy BIOS boot sequence:



|  |  |
| --- | --- |
| **Stage** | **Process** |
| POST (power-on self-test) | On a system using BIOS, the following steps take place:   1. Power is supplied to the CPU. The CPU is hard-coded to look at a special memory address that contains a pointer (or jump program), which instructs the CPU where to find the BIOS program. 2. The CPU loads the BIOS program. The first BIOS process to run is the POST, which performs the following tasks:    1. Verifies the integrity of the BIOS code.    2. Tests and initializes the following hardware devices one by one:       * Locates, sizes, and verifies system memory       * Verifies and initializes video card (output displayed on monitor)       * Identify available hard disks 3. After POST tests complete, the BIOS identifies other system devices. It uses CMOS settings and information supplied by the devices themselves to identify and configure hardware devices. Plug and play devices are allocated system resources. The system typically displays information about the keyboard, mouse, and SATA drives in the system. Following this summary, you will also see information about devices and system resources. 4. The BIOS then searches for a boot drive (using the boot order specified in the CMOS).   During this sequence, system information is displayed on the screen and the option to enter the CMOS setup to configure system parameters is available. |
| Boot loader | During the boot loader stage, the following process occurs:   1. On the boot device, the BIOS searches for and loads the boot code in the master boot record (MBR). The MBR is located in the first sector on the disk. 2. The MBR boot code uses the partition table to identify the active disk partition. 3. On the active partition, it looks for and loads the bootmgr.exe program. 4. The bootmgr.exe program looks for the BCD store in either the C:\ directory or the System Reserved partition. The BCD store contains a list of all Windows installations on the disk. 5. If only one installation exists, bootmgr.exe automatically loads the OS. If multiple installations exist, a list of bootable operating systems is displayed.   This stage occurs after the BIOS information screen disappears, but before the Windows loading screen is shown. |
| OS startup | During this stage, the operating system is started. The operating system configures system devices and loads necessary files. The following process occurs:   1. The operating system loader winload.exe is started. At this stage, advanced startup options can be access by pressing the F8 key (e.g., Safe Mode). 2. Winload.exe then loads the following:    * System registry    * Ntoskrnl.exe    * Essential device drivers 3. Control of the system is passed to ntoskrnl.exe. 4. At this point, the Windows logo is displayed and ntoskrnl.exe:    * Loads device drivers.    * Starts services.    * Configures the OS environment. |
| Logon and user configuration | After the operating system and devices are configured, the system waits for user logon. Following logon, the operating system is configured with user-specific settings.   1. The wininit and winlogon programs run to allow user logon. At this point, the Welcome or user logon screen is displayed. 2. Following logon, all remaining device drivers and user settings are loaded. In addition, the current configuration profile is copied to the Last Known Good Configuration registry. |

**UEFI Boot**

The following diagram and table describe the different stages of the UEFI boot sequence:



|  |  |
| --- | --- |
| **Stage** | **Process** |
| SEC (Security) | Immediately after the system is powered on, the SEC sequence begins.   1. Power is supplied to the CPU. 2. The CPU switches from 16-bit Real Mode to 64-bit Protected Mode. 3. The CPU executes a specific set of instructions to prepare the system for PEI to run. |
| PEI (Pre-EFI Initialization) | PEI initializes the system and prepares for the DXE.   1. The CPU and chipset are verified and fully initialized. 2. System memory is initialized, verified, and allocated. 3. PEI modules are loaded to allocate system resources. 4. The DXE is initialized, and the system is prepared to transition to DXE. |
| DXE (Driver Execution Environment) | DXE initializes configured devices, mounts drives, and prepares to boot the OS.   1. Device drivers are loaded into memory. 2. Hardware devices are initialized simultaneously (e.g., video card, network card, USB controllers). 3. System drives are mounted and initialized. 4. The EFI boot manager is initialized. |
| BDS (Boot Device Selection) | The BDS stage runs the EFI boot manager, which identifies the system's boot configuration settings and decides how to boot the system.   1. If an EFI System Partition (ESP) exists, the following process occurs:    1. On the ESP in the \EFI\Microsoft directory, the boot manager looks for and runs the bootmgfw.efi file.    2. The bootmgfw.efi looks for the BCD store in the same directory, which contains a list of all Windows installations.    3. If only one installation exists, UEFI automatically loads it. If multiple installations exist, a list of bootable operating systems is displayed. 2. If no ESP exists, the boot manager uses Legacy BIOS mode to complete the boot sequence:    1. The MBR looks for and loads the bootmgr.exe program.    2. The bootmgr.exe program looks for the BCD store in either the C:\ directory or the System Reserved partition.    3. If only one installation exists, bootmgr.exe automatically loads the OS. If multiple installations exist, a list of bootable operating systems is displayed.   At the beginning of the BDS stage, the UEFI interface is executed and the option to load the EFI Shell or enter the UEFI configuration is available. |
| TSL (Transient System Load) | During TSL stage, the operating system loader is located and booted.   1. The BCD store is used to identify the location of the operating system loader (for Windows, the default location is C:\Windows\system32\winload.efi). 2. The operating system loader winload.efi is started. 3. Winload.efi then loads the following elements:    1. System registry    2. Ntoskrnl.exe    3. Essential device drivers |
| RT (Run Time) | After the operating system and devices are configured, the system waits for user logon. Following logon, the operating system is configured with user-specific settings.   1. Control of the system is passed to ntoskrnl.exe. 2. At this point, the Windows logo is displayed and ntoskrnl.exe:    * Loads device drivers.    * Starts services.    * Configures the OS environment. 3. The wininit and winlogon programs run to allow user logon (at this point, the Welcome screen is displayed). 4. Following logon, all remaining device drivers and user settings are loaded. In addition, the current configuration profile is copied to the Last Known Good Configuration registry. |

Even though it seems to have more stages, the UEFI boot sequence is considerably faster than the BIOS boot sequence.

9.15.6 Windows Boot Options

If your system will not start, or if it is having significant problems, then you can boot your system in a variety of modes that may help you get your system up and running. There are two main ways you can select an alternate boot mode:

* Access the Settings app and select one of the following:
  + Windows 8: **Update and Recovery** > **Recovery** > **Restart Now**
  + Windows 10: **Update and Security** > **Recovery** > **Restart Now**
* Run the **msconfig.exe** utility to specify which boot mode you would like to use, then reboot the system.

Only a subset of advanced boot options are available in **Msconfig**.

The following table describes the different startup modes:

|  |  |
| --- | --- |
| **Mode** | **Description** |
| Enable Debugging | This option starts Windows in an advanced troubleshooting mode. This option is typically used by programmers, not system administrators. |
| Enable Boot Logging | This option creates a log file named **Ntbtlog.txt** in C:\Windows during startup. This file contains an entry for each driver loaded during the boot process. If the system does not complete a regular boot, you can look at this file to see the last driver to load before the failure occurred. |
| Enable Low-Resolution Video | This option loads Windows using your current video driver, but configures it to use low resolution settings and a slow refresh rate. This option is useful when the wrong video configuration settings have been used, causing the screen to be unreadable. Selecting this option gives you the ability to restore the correct video settings. |
| Enable Safe Mode | When a computer boots in Safe Mode, only essential drivers and services are loaded (e.g., generic mouse, monitor, base storage device, keyboard, video drivers, and the Event Log service). This allows you to troubleshoot misbehaving applications, services, and drivers. |
| Enable Safe Mode with Networking | Safe Mode with Networking is a variation of Safe Mode that also loads a network driver and protocol so the system can communicate on the network. This option is useful in situations where an updated driver needs to be downloaded from the Internet and installed on the system to correct a problem. |
| Enable Safe Mode with Command Prompt | Safe Mode with Command Prompt starts the computer in Safe Mode and displays a command prompt. |
| Disable Driver Signature Enforcement | Selecting this option causes Windows to not require a digital signature when loading a driver. |
| Disable Early Launch Anti-Malware Protection | This prevents the early launch antimalware driver from loading when the system is booted. This could increase the system's exposure to rootkit malware packages. |
| Disable Automatic Restart on System Failure | By default, Windows is configured to reboot whenever a critical system error occurs (Blue Screen of Death).   * When the error occurs, you will have only a short time before the system reboots. This might not be sufficient time to read and record the error information. * If the error occurs while you are away from your computer, you will see a message that the system has restarted, but won't have seen the error. * If the error occurs during startup, the system might continually reboot.   Use the **Disable automatic restart on system failure** option on the advanced boot menu to stop the automatic reboots. |
| Launch Recovery Environment | Use this option to access system recovery tools, such as:   * Reset This PC * System Restore * System Image Recovery * Startup Repair * Command Prompt * Go Back to the Previous Build |

Use the following recommendations to troubleshoot startup errors with the advanced boot options:

* Boot into Safe Mode and then use the appropriate tool to undo any recent changes. For example, you can:
  + Use Device Manager to roll back drivers or disable devices that might be causing the problem.
  + Use Add or Remove Programs to uninstall software that has just been added.
  + Restore any settings that may have changed.
  + Disable unneeded services or applications that load at startup.
  + Use System Restore to restore the system to a known good restore point.
* After booting into Safe Mode, begin by undoing the most recent change to the system. For example, if the problem started after you installed a new device driver, roll back the driver and reboot.
* If undoing recent changes does not fix the problem, you could disable all unnecessary devices and services. If you can boot normally, you can identify which component was causing the problem by enabling devices and services one-by-one until the system becomes unstable.

9.15.8 Startup Error Facts

The following table contains a description of common startup errors:

|  |  |
| --- | --- |
| **Error** | **Description** |
| System does not power on | If the system does not power on:   * Make sure the system is plugged in and the power strip or UPS is turned on. * Check the power switch and the power type (110 or 220 volts) on the back of the power supply. * If you have just installed a new system, make sure the system case power switch is connected to the motherboard.   When you turn on the computer, you should hear both the power supply fan and the CPU fan start to spin. |
| System powers on, but no display is visible | If the system powers on but there is nothing on the display, check the following:   * Verify that the monitor is connected to the computer, plugged in, and turned on. * Verify that the BIOS/UEFI is configured to use the correct video adapter. Most motherboards can be configured to use either the integrated video adapter or a PCIe video adapter installed in an expansion slot. * To display startup information on the screen, the computer needs at a minimum the CPU, memory, and a video card. Other components are not necessary. Verify that these three components are properly installed. * If necessary, reduce the system to the three components listed above and try starting the system. If that does not work, swap out components to identify the failed component.   Some computers will use a series of beeps to indicate specific problems when those messages cannot be shown on the screen. In this case, consult the BIOS documentation for the meaning of the audible messages. |
| Corrupt MBR or partition table | The master boot record (MBR) is responsible for locating the system (active) partition and loading the volume boot record (VBR). A corrupt or missing master boot record or a corrupt partition table prevents the system from loading the boot record code and finding the volume boot record and loading the boot loader program. Symptoms of a corrupt MBR or partition table include:   * The system hangs immediately after the BIOS information is shown. * Any of the following errors:   + MBR corrupt   + Invalid partition table   + Error loading operating system   + Missing operating system   To fix the problem, boot the system from the installation disc and repair the system. Select **Troubleshoot** >**Advanced Options** > **Startup Repair**. Alternatively, you can select the **Command Prompt** option and then run the **bootrec /FixMbr** command. The /FixMbr option causes the bootrec command to write the rewrite the master boot record without overwriting the existing partition table on the disk. |
| Corrupt boot sector | The boot sector (also called the volume boot record or volume boot code) is responsible for loading the operating system boot loader program (BOOTMGR). At this point in the process, the MBR has loaded, located an active partition, but there is a problem in loading the VBR, the VBR does not specify a boot loader program, or the boot loader specified in the VBR is missing or corrupt. Symptoms of a corrupt or missing boot sector include:   * System hangs following the BIOS information screen. * Any of the following errors:   + Non-system disk or disk error   + Remove disks or other media   + Invalid system disk   + Invalid media type   + Disk Boot failure   + A disk read error occurred   + BOOTMGR is missing   + Missing GRUB/LILO   To correct the problem you can check the following:   * Check the boot order in the BIOS/UEFI to make sure the system is booting from the correct storage device. * If the device is a removable media device, the drive should be empty (so the drive is skipped when checking for a boot disk), or the drive must have media that includes a bootable partition (for the system to boot from that drive). For example, leaving a USB device plugged in is a common cause of the non-system disk error. These errors can be avoided by disabling the **USB Device** option in the boot sequence or to set the integrated USB controller to **No Boot**. * Boot the system from the installation disc and repair the system. Select **Troubleshoot** > **Advanced Options** > **Startup Repair**. Alternatively, you can select the **Command Prompt** option and then run the **bootrec /FixBoot** command. The /FixBoot option causes the bootrec command to write a new boot sector in the system partition. |
| Inaccessible boot disk | The boot loader program uses the *boot configuration database* (BDC) to locate valid Windows installations to start. If the database points to a location that does not include any operating system files, you will see a message similar to the following:  Windows could not start because of a computer disk hardware configuration problem. Could not read from the selected boot disk. Check boot path and disk hardware.  To correct the problem, boot the system from the installation disc and repair the system. Select **Troubleshoot** >**Command Prompt** option and then run the **bootrec /RebuildBcd** command. The /RebuildBcd option causes the bootrec command to scan all storage devices for operating systems and add them to the BCD database. |
| Missing or corrupt file | If the boot manager cannot locate needed operating system files on the selected boot partition, you might see the following errors occur:   * Windows could not start because the following file is missing or corrupt: <filename> Please re-install a copy of the above file. * A blue screen error that describes a corrupt or missing file.   This problem is caused either by a corrupt disk, corrupt files, or missing files. To correct the problem, boot the system from the installation disc and repair the system. Select **Troubleshoot** > **Advanced Options** > **Startup Repair**. Alternatively, you can select the **Command Prompt** option and then use the **copy** command to replace the file referenced by the error message with a known good copy. |
| Blue screen or system hang after Windows splash screen is displayed | The most common cause of the errors at this stage are bad drivers or corrupt registry settings. To correct the problem, try the following (in this order):   * If the error includes any error codes or messages, check the Microsoft website for troubleshooting information. * Boot the system into Safe Mode. In Safe Mode, rollback drivers, remove drivers, or restore to a restore point. * To identify which driver is causing the problem, enable boot logging, then read the **Ntbtlog.txt** file to identify the last driver that the system tried to load. * If you cannot boot into Safe Mode, boot into the Recovery Environment and use System Restore to restore to a restore point that was created when the system was working correctly. |
| Service fails to start | If a service fails to start, you will see a message such as:  At least one service or driver failed during system startup. Use Event Viewer to examine the event log for details.  Use Event Viewer to view details about the service that did not start, then try starting the service manually. If necessary, re-enable or re-install the service. |
| Corrupt or missing DLL or system file | If you see errors about corrupt or missing DLLs or system files, either during startup or after Windows starts, boot the system from the installation disc and repair the system. Select **Troubleshoot** > **Advanced Options** >**Startup Repair**. Alternatively, you can select the **Command Prompt** option and then use the **sfc** command to run the System File Checker utility. The syntax to use with **sfc** is as follows:   * Use **sfc /scannow** to scan the integrity of all protected system files and repair any file that has problems. * Use **sfc /verifyonly** to scan the integrity of all protected system files, but not repair them. * Use **sfc /scanfile** to scan the integrity of a specific file and repair it if it has problems. * Use **sfc /verifyfile** to scan the integrity of a specific file, but not repair it. |
| Device fails to start | This message indicates that a hardware device could not be started. Begin by checking Device Manager for information about the device. If necessary, update the driver or disable the device. |
| Missing NTLDR | If you're still using Windows XP and your NTLDR is missing or corrupt. If this file gets corrupt, you're going to have to fix it. To fix the problem, do the following:   * Boot your system from your installation CD. * In the Windows XP setup menu, press **R** to repair Windows. * Log into Windows using your administrator user and password by pressing **1**. * Copy the NTLDR file located in the i386 directory on the installation disk to the root directory of the system's hard drive. * When you're done, remove the installation disk from the system and try rebooting. That should fix the problem if your original NTLDR file is missing or corrupted. |

If the system experiences a blue screen error during startup or after the system has started, the default behavior is to restart Windows automatically after displaying the error. With the default configuration, the system could restart, experience the same error, restart automatically, and enter a constant cycle of error and restart. To configure the system to display the blue screen error until you manually continue, access the advanced startup options menu and then select **Disable automatic restart on system failure** to stop the automatic reboot cycle.