CIS 101B Lesson Plan

|  |  |
| --- | --- |
| **Week 2 Class 3****Wedsday 1-5:00 PMWedsday 6-10:00 PM** | **Chapter 9 – System ManagementChapter 9.1 to 9.6** |

Hands On

|  |  |
| --- | --- |
| **Use the lab PCs to try Windows Utilities****Create a MMC, adding Local Users and Groups, and Computer Management Start/Search/MMC – EnterFile/Add-Remove Snap-Ins****Create users and groups, using Local Users and GroupsCreate 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 pcsRemember you have to log in with credentials on the machine you are connecting to, NOT your local credentialsEnable Remote Desktop first:Win-Pause\Remote Settings****Run Windows Backup and Restore****Create a restore pointWin-Pause\System Protection\Create****Restore from a Restore PointWin-Pause\System Protection\System Restore** | **Create a Windows 7 Recovery DiscBoot with Window 7 Recovery Disc** **Create System Restore PointLoad back to a previous Restore Point****Run Command Prompt from Windows 7 Recovery Disc, run SFC /scannowThen at the same promptRun 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 themesnet 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 MenuSelect Safe Mode, look at the environment you get with Safe Mode** |

9.1 Windows System Tools

9.1.7 Windows Utilities Facts

You should be familiar with the following Windows tools and utilities.

|  |  |
| --- | --- |
| **Tool** | **Description** |
| Control Panel | Use the Control Panel to customize features of devices and to configure how a computer looks and behaves. Use the various applets within the Control Panel to perform configuration tasks for specific features or devices.* Use Ease of Access to modify the behavior of input and display devices to accommodate users with special needs.
* Use Fonts to view, remove, or add to all fonts that are currently installed on the computer.
* Use Devices and Printers to view, configure, add, or remove devices such as printers, scanners, and cameras.
* Use Clock, Language, and Region settings to configure various settings such as language preference, default currency symbols, and date and time notation.
* Use Hardware and Sound to view and configure the current system sound settings, installed audio devices, sound cards, printer settings, and other hardware settings.
* Use Windows Firewall to manage network traffic that is allowed or denied through the Windows host-based firewall.
* Use Security and Maintenance to review recent error messages and options for resolving issues.
* Use System and Security to configure Windows Update, manage Power Options, configure File History, configure Backup and Restore, configure Storage Spaces, and use Administrative Tools.
* Use Internet Options within Network and Internet to modify your Internet Properties.
	+ Use the General tab to modify your browser home page, startup window, tabs, history, and appearance.
	+ Use the Security tab to determine your security zone and security level.
	+ Use the Privacy tab to manage website privacy and enable and disable pop-ups and InPrivate Browsing.
	+ Use the Connections tab to set up Internet connections.
	+ Use the Programs tab to manage your default browser, add-ons, and other Internet programs and file associations.
	+ Use the Advanced tab to set and reset advanced browser settings.
 |
| Task Manager | Use Task Manager to view the current state of the system and running applications. Task Manager is made up of the following tabs:* Use the Processes tab to view the status of all current applications running on the computer. Use this tab to terminate unresponsive applications.
* Use the Performance tab to view system-wide processor, memory, disk, and network statistics.
* Use the App History tab to monitor Windows Store apps running on the system.
* Use the Startup tab to enable or disable applications that start automatically when the system boots.
* Use the Users tab to monitor users currently logged on to the system.
* Use the Details tab to view the status of all current processes running on the computer and the CPU and memory resources they use. Use this tab to modify the priority of a process or terminate unwanted processes.
* Use the Services tab to view a list of services running on the computer. You can use this tab to start and stop a particular service.
 |
| Microsoft Management Console (MMC) | The Microsoft Management Console (MMC) is a framework that provides a common user interface for performing system administration tasks. Management of a set of related features is done by adding snap-ins to the console. The MMC provides the shell for running these snap-ins, while the snap-ins provide the details for performing specific management tasks. Microsoft provides snap-ins for managing:* Local Users and Groups
* Device Manager
* Disk Management
* Print Management
* Component Services
* Windows Firewall with Advanced Security

To open a blank console, type **mmc** in the Run box. You can then add snap-ins to work with the configuration of your system. The console consists of two or three panes:* The tree pane (on the left) organizes objects in a hierarchy.
* The results pane (in the middle) shows objects and configuration options.
* The actions pane (on the right) lists the actions you can take on objects. (The actions pane was new with Windows Vista.)

You can save a console that includes the snap-ins you use most (saved consoles have the **.msc** extension). Microsoft provides a number of preconfigured consoles that include snap-ins for common tasks. |
| Computer Management | Computer Management is a saved MMC console that includes common snap-ins used to manage your computer. Some common ways to start Computer Management include:* Right-click the Start menu and select **Computer Management**.
* Click **Start** > **All Apps** > **Windows Administrative Tools** > **Computer Management**.
* Search for **Computer Management**.
* Double-click **Computer Management** in Administrative Tools in Control Panel.
 |
| Event Viewer | Use Event Viewer to view logs about programs, system events, and security. Each entry is listed as a warning, error, or information event. Events are added to the following logs:* The Application log contains a list of all application-related events such as application installations, un-installations, and application errors.
* The System log contains a list of all system-related events such as system modifications, malfunctions, and errors.
* The Security log contains a list of all security-related events such as security modifications and user login events.

Additional logs might be added by applications or services. |
| Services | A *service* is a program that processes requests from other applications or users. Services can start automatically and stay constantly running in the background, waiting for service requests. Use the Services snap-in to view and manage running services. The service startup behavior determines how the service is started.* When set to Automatic, the service is started automatically by Windows when the system boots.
* When set to Manual, the service must be manually started.
* When Disabled, the service will not run.
 |
| Performance Monitor | Performance Monitor displays statistics that tell you about the operation of your computer.* A *counter* identifies a specific statistic, such as % Processor Time or % Disk Free Space.
* You can add or remove counters to customize the statistics you can see.
* Real-time data are displayed in a graph.
* Performance Monitor by itself does not save any data. To save statistics over time, use a data collector set.
 |
| Reliability Monitor | Reliability Monitor maintains historical data that describe the operating system's stability.* Overall system stability is given a stability index that ranges from 1 to 10 (10 being the most stable). The stability rating is affected by application, hardware, Windows, and other failures.
* Reliability Monitor shows an historical chart that identifies when software installs/uninstalls and failures have occurred. By clicking on a day, you can view the changes to the system that have affected its stability.
 |
| System Information (Msinfo32) | Use Msinfo32 to view hardware and configuration information for your computer. While much of this information is available through other tools, Msinfo32 provides a single location for viewing information such as:* Operating system version
* Computer manufacturer, processor type, available memory
* Installed devices and drivers used
* Running tasks
* Applications that run at system startup

You can only view, not modify, configuration settings in Msinfo32. |
| System Configuration Utility (MSCONFIG) | Use the System Configuration Utility to configure your system to enable optimal troubleshooting and diagnosis of technical issues. Use the System Configuration Utility to:* Configure startup preferences
* Customize bootup configuration
* Turn services on or off
 |
| DirectX Diagnostic Tool (DxDiag) | DxDiag is a tool that shows information related to DirectX operation. DirectX is a set of programming interfaces for multimedia (video and audio). DxDiag displays information such as:* Operating system version
* Processor and memory information
* DirectX version
* Settings and drivers used by display devices
* Audio drivers
* Input devices (mouse, keyboard, USB)
 |
| Microsoft Register Server (REGSRV32) | *REGSRV32* is a command-line tool that registers .dll files as command components in the registry. |
| Command Prompt | Use the Command Prompt to execute command-line commands. To open a command prompt,* On Windows 7, click **Start** and type **cmd** in the Search box.
* On Windows 8/10, right-click the Start menu and select **Command Prompt**.

Some commands launched from the command line require elevated privileges to run. If this is the case, run Command Prompt as Administrator. |
| Regedit | **Regedit.exe** is a tool for modifying entries in the Windows registry. The registry is a database that holds hardware, software, and user configuration settings.* Whenever a change is made to preferences, software, hardware, and user-settings, those changes are stored and reflected in the registry.
* The preferred method of modifying the registry is to use the applications or management tools that write to the registry. For example, many Control Panel applets make changes to registry settings.
* There will be some advanced settings that can only be made by directly editing the registry.
 |
| Data Sources | You use the ODBC Data Source Administrator to create and manage ODBC data sources. To open the ODBC Data Source Administrator in Windows 7, do the following:1. On the Start menu, click Control Panel.
2. In Control Panel, click Administrative Tools.
3. In Administrative Tools, click Data Sources (ODBC).
 |
| Windows Memory Diagnostics | The Windows Memory Diagnostic tests the Random Access Memory (RAM) on your computer for errors. This utility is not included with Windows and must be downloaded from Microsoft's Online Crash Analysis web site. |
| Advanced Security | Everyday configuration tasks for the Windows Firewall are completed using the Windows Firewall applet in Control Panel. However, advanced firewall configuration tasks can be performed using an MMC snap-in called *Windows Firewall with Advanced Security*.Windows Firewall with Advanced Security supports a more granular firewall configuration than can be created using the Windows Firewall applet in Control Panel. For example, it can filter traffic based on parameters such as:* Source IP address
* Destination IP address
* Port number
* ICMP protocol
 |

9.1.9 System Command Facts

The following table describes the various system commands that can be used in the Windows command prompt:

|  |  |
| --- | --- |
| **Command** | **Description** |
| expand | The **expand** command is used to expand compressed .cab files.* **expand -d *[source\_file]*** displays the contents of the specified .cab file.
* **expand *[source\_file]* *[destination]*** expands all the files in the specified .cab file to the chosen destination.
* **expand *[source\_file]* f:*[filename]* *[destination]*** extracts a single file from the specified .cab file to the chosen destination.
 |
| tasklist | The **tasklist** command displays a list of the processes that are currently running on the system. The output of the**tasklist** command includes a process ID (PID) that can be used to end the process. |
| taskkill | The **taskkill** command is used to end running processes.* **taskkill /in *[image\_name]*** kills the specified process by using its image name (e.g., mspaint.exe).
* **taskkill /PID *[pid\_number]*** kills the specified process by using its PID (e.g., 3572).

Sometimes a process will not respond the **taskkill** command. If this is the case, use the **/f** option with the command, which forces the process to close. |
| mstsc | The **mstsc** command is used to establish a remote desktop session with another computer. To run the **mstsc**command, use the following syntax:* **mstsc /v:*[server\_ip]***
 |
| gpupdate | The **gpupdate** command refreshes local and Active Directory-based Group Policy settings, including security settings.* **/target: { computer | user }** processes only the computer settings or the current user settings. By default, both the computer settings and the user settings are processed.
* **/force** ignores all processing optimizations and reapplies all settings.
* **/wait: *value*** identifies the number of seconds that policy processing waits to finish. The default is 600 seconds. 0 means "no wait"; -1 means "wait indefinitely."
* **/logoff** logs off after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the user logs on, such as user software installation and folder redirection. This option has no effect if there are no extensions called that require the user to log off.
* **/boot** restarts the computer after the refresh has completed. This is required for those Group Policy client-side extensions that do not process on a background refresh cycle but that do process when the computer starts up, such as computer software installation. This option has no effect if there are no extensions called that require the computer to be restarted.
* **/?** displays help at the command prompt.

To run the **gpupdate** command, use the following syntax:* **gpupdate [/target:{computer|user}] [/force] [/wait:value] [/logoff] [/boot]**
 |
| gpresult | The **gpresult** command displays Group Policy settings and Resultant Set of Policy (RSOP) for a user or a computer.* **/s *computer*** specifies the name or IP address of a remote computer. (Do not use backslashes.) The default is the local computer.
* **/u *domain* \ *user*** runs the command with the account permissions of the user that is specified by user or domain\user. The default is the permissions of the current logged-on user on the computer that issues the command.
* **/p *password*** specifies the password of the user account that is specified in the /u parameter.
* **/user *target\_user name*** specifies the user name of the user whose RSOP data is to be displayed.
* **/scope { user | computer }** displays either user or computer results. Valid values for the /scope parameter are user or computer. If you omit the /scope parameter, gpresult displays both user and computer settings.
* **/v** specifies that the output display verbose policy information.
* **/z** specifies that the output display all available information about Group Policy. Because this parameter produces more information than the /v parameter, redirect output to a text file when you use this parameter (for example, gpresult /z >policy.txt).
* **/?** displays help at the command prompt.

To run the **gpresult** command, use the following syntax:* **gpresult [/s *computer* [/u *domain*\*user* /p *password*]] [/user *target\_user name*] [/scope {user|computer}] [/v] [/z]**
 |
| shutdown | The **shutdown** command is used to shutdown local and remote systems. The following options can be used with the **shutdown** command:* **/i** opens the Remote Shutdown Dialog graphical interface window.
* **/l** logs off the current user from the local system.
* **/r** shuts down and restarts the local computer.
* **/h** causes the computer to hibernate.
* **/t *[xx]*** sets a delay time (in seconds) before the computer shuts down.
 |
| exit | The **exit** command ends the current command prompt session and closes the Command Prompt window. |

If you need further help with a particular command, type ***[command\_name]* /?** to display information about the specified command (typing **help *[command\_name]*** will also display help information).

9.2 Preferences and Settings

9.2.4 Preferences Facts

The following table describes settings that can be used to customize the appearance and function of the Windows graphical user interface.

|  |  |
| --- | --- |
| **Configuration Setting** | **Description** |
| Theme | A *theme* is used to customize the way the Windows desktop appears. Themes can be selected in the Control Panel under Appearance and Personalization > Personalization. A theme is composed of:* One or more desktop backgrounds
* Window colors
* System sounds

When a theme is selected in the Control Panel, all three of these elements are changed at the same time. Windows installs several default themes during installation. Additional themes can be downloaded and installed by selecting **Get more themes online**.On Windows 7 and Windows 8, individual theme components can be customized in Control Panel. However, on Windows 10, this functionality has been moved to the Settings app. The Settings app provides additional theme configuration options that are not found in most earlier versions of Windows, including:* Automatically pick an accent color from my background
* Show color on Start, taskbar, and action center
* Make Start, taskbar, and action center transparent
* Lock screen settings
 |
| Screen Saver | A *screen saver* is designed to prevent "burn-in" damage to the monitor by displaying constantly changing output on the screen after the system has been idle for a specified amount of time. A screen saver can be selected under Appearance and Personalization > Personalization > Change Screen Saver in Control Panel. The following can be configured:* Which screen saver to use
* How long to wait before activating the screen saver
* Whether authentication is required after deactivating the screen saver
 |
| Mouse | Mouse properties can be set in Control Panel by going to Hardware and Sound > Mouse. The mouse properties are configured using the following tabs:* **Buttons**: Configures the button configuration, double-click speed, and ClickLock settings.
* **Pointers**: Configures the pointer scheme.
* **Pointer Options**: Configures the pointer speed, snap-to, and visibility settings.
* **Wheel**: Configures vertical and horizontal scrolling settings.
 |
| Sounds | System sounds can be set in Control Panel by going to Hardware and Sound > Change System Sounds. A sound scheme can be selected and customized on the Sounds tab. |
| Indexing | Windows includes a quick search tool. The search tool is used in the Start menu, File Explorer, and Control Panel.* Searches execute quickly because the search tool does not search the entire hard drive. Instead, it searches through a pre-built database.
* By default, Windows indexes selected file types on local hard disks as well as offline files.
* Use the **Indexing Options** in Control Panel to customize what information is included in the index. You can:
	+ Modify the list of locations to include or exclude specific drives, folders, or other locations.
	+ Modify the list of file types to include or exclude files from being indexed based on the file extension.
	+ Index files based on filename, properties, or file contents.
* In File Explorer, use the **Search** settings in **Folder Options** to customize how searches are executed.
 |
| Region and Language Settings | Use the Region and Language options in Control Panel to manage language capabilities for the system.* Region settings control how times, dates, numbers, and currency are formatted and displayed. For example, dates are displayed differently in different parts of the world and for different languages. For example:
	+ Canada (French) displays dates in the format: yyyy-MM-dd (2002-11-02)
	+ Canada (English) displays dates in the format: dd/MM/yyyy (02/11/2002)
	+ United States (English) displays dates in the format: M/d/yyyy (11/2/2002)
	+ Australia (English) displays dates in the format: d/MM/yyyy (2/11/2002)
* The Change Location setting identifies the area of the world where the computer is connected. Some software services use the location to modify the content based on the location.
* An input language identifies the language, font, and keyboard layouts that can be used on the system. When you add an input language, the language toolbar is made available. Using the language toolbar, you can quickly change the current input language within an application.
 |

9.3 Performance Monitoring

9.3.3 Performance Monitoring Facts

A *bottleneck* occurs when a component is unable to keep up with demand and subsequently slows down other processes or functions. When a system seems to respond slowly, it's important to be able to accurately identify the component(s) that are causing the problem so you can take the proper actions to improve performance.

Common components to examine in order to improve performance are:

* Processor (CPU)
* Hard disk
* Memory
* Network

One way to identify components that are causing a bottleneck is to monitor system performance statistics. These statistics give you a measure of the activity of a certain aspect of the system. By recognizing abnormal statistics, you can identify the component that is overloaded or not responding appropriately. Windows identifies system performance statistics using the following terms:

* A *counter* is a specific statistic you can monitor (such as the amount of free memory or the number of bytes sent on a network card).
* An *object* is a statistic group, often corresponding to a specific type of hardware device or software process (such as the processor or memory).

Use Task Manager, System Monitor, Resource Monitor, and Performance Monitor to track statistics. You should be familiar with the meaning and use of the following counters:

|  |  |
| --- | --- |
| **Counter** | **Description** |
| % Processor Time (processor utilization) | *Processor utilization* is the amount (percentage) of time the processor spends doing non-idle tasks.* Processor utilization should be relatively low, up to 40% on average.
* Processor utilization will spike (85 - 90% or higher) when a major task is launched or a significant task is performed.
* Utilization is reported for each processor in a multi-processor or multi-core system. A CPU that supports Hyper-Threading will show two utilization graphs for each processor.
* If the processor utilization is consistently high (over 90%), then the CPU is likely the bottleneck.
	+ Check the running processes to see the CPU use of each process. If possible, delay or pause non-critical processes or run them during off hours.
	+ A process that has hung could show 100% CPU use. If the process does not complete after a period of time and does not respond, end the process to return CPU use to normal.
	+ A computer with a virus might show an unknown process consuming most of the processor time. Use the Internet to identify the function of unknown processes.
	+ Configure the processor *affinity* to specify that a specific process use a certain processor in a multi-processor system.
	+ Upgrade to a faster CPU or add more cores to the system.
 |
| % Disk Time (highest active time) | The % Disk Time statistic identifies the percentage of time that the disk subsystem is busy reading from and writing to disk. If this value is consistently over 90%, check the following other statistics to identify the source of the high disk activity:* Average Disk Queue Length
* Memory statistics
 |
| Average Disk Queue Length | The disk *queue* holds read and write requests that are waiting to be processed by the disk controller. The average disk queue length tells you the number of read and write requests that are typically waiting to be processed.* A high number indicates that the system has requested data from the hard disk, or has tried to save data to the hard disk, but that request could not be fulfilled immediately (i.e. it has to wait).
* This number should be below 2 times the number of disk spindles. Most physical hard disks have a single spindle (although some newer drives have 2 or 3). RAID arrays will have at least one spindle per physical disk.

If this statistic shows consistently waiting read/write requests, you might need to upgrade your disks.* Choose a faster disk (higher RPM and faster access time).
* Use a RAID-0 configuration to improve disk access.
 |
| Available, used, and free physical memory | You can use Task Manager to quickly identify the use of physical memory in your system.* The total installed memory value reflects the amount of memory available to the operating system. On a 32-bit system, this value will be less than 4 GB, even if you have 4 GB of memory installed. This value could also be slightly less than the amount of installed physical RAM if the video adapter shares the system memory. The amount of memory used for this purpose is displayed under hardware reserved.
* The cached value identifies memory that is being used for a disk cache to improve read/write operations from the hard disk.
* The available value identifies how much memory is unassigned.

If the amount of memory in use is close to the amount of RAM installed, you might need to add RAM or quit some running programs to free up memory. |
| Memory committed bytes (commit charge) | When a process runs, the operating system assigns memory to the process. The amount of committed memory identifies how much memory has been assigned to running processes. Be aware of the following conditions indicated by this statistic:* If the value exceeds the amount of physical RAM, then the page file is being used instead of physical RAM. At some point, this will start to cause a bottleneck.
* To temporarily make more memory available, quit running programs or increase the page file size. However, the only permanent solution is to add more physical memory.
 |
| Page file usage | The page file usage identifies the amount or percentage of the page file that is being used.* A common recommendation is for the page file to be 1.5 to 2 times larger than the physical memory. In most cases, you will let the system manage the page file size.
* It is normal for the page file to show some use, even when the system has sufficient physical memory.
* When the page file use percentage is near 100%, you can increase the page file size as a temporary measure. Adding more memory is the best permanent solution.
 |
| Memory pages per second | The operating system allocates memory to processes in 4,096 KB blocks called *pages*.* Instead of assigning physical memory addresses, the operating system assigns *virtual memory* addresses to shield the process from the details of the physical memory storage system.
* The *paging supervisor* is a process that maintains a table that correlates virtual memory addresses with the actual physical memory locations.

When physical memory is low, data in RAM that is currently not being used by the CPU can be moved to the hard disk in order to free up memory for other processes.* The area on the hard disk used for storing the contents of RAM is called the *page file*.
* When the CPU needs to access data in RAM, a *page fault* (also called a *hard fault*) occurs when that data does not exist in RAM but is instead in the page file.
* *Paging* is the process of moving data from RAM to disk and back. Before the CPU can work with data required by a process, that data must be placed into RAM.

The memory pages per second statistic identifies the number of hard faults that occur each second. A high number for this statistic accompanied by high disk activity (% Disk Time or the disk activity light constantly flashing) could indicate a condition known as *thrashing*.* With thrashing, the demand for memory and the low amount of physical RAM means that the system must be constantly moving data from RAM, to disk, and back.
* The negative effects associated with paging increases as the amount of memory increases past the amount of physical RAM. While some paging is normal, as the demands on memory increase, the amount of paging will at some point reach a point where thrashing occurs and the effect on performance is noticeable--even to the point of making the system unusable.
* As a temporary solution, you can quit some running programs in order to decrease the demand for RAM. The only long-term solution is to add more physical RAM.
* Increasing the page file size will have no effect unless you are also experiencing out of memory errors. The problem is not that there isn't sufficient combined memory, but that the amount of physical memory is insufficient.
 |
| Network Utilization | Network utilization identifies the amount of traffic sent and received by a network connection.* Utilization is listed as a percentage of the total available theoretical bandwidth (such as 100 Mbps for a Fast Ethernet connection).
* Poor performance that has low CPU, disk, and memory statistics but high network utilization could indicate a bottleneck at the network adapter.
 |

9.4 Users and Groups

9.4.3 Users and Group Facts

The ability to use a computer is controlled through a *user account*.

* The user account identifies a specific user.
* *Logon* is the process of authenticating to the computer by supplying a user account name and the password associated with that user account.
* On Windows systems, the ability to perform actions on a computer, such as modifying system settings or installing hardware, are called *rights*.
* Access to files, folders, and printers is controlled through *permissions*. Permissions identify what the user can do with the associated object.
* Windows includes two built-in users.
	+ The Administrator account has all rights and permissions on the computer.
	+ The Guest account has very limited capabilities, usually restricted to logging on, viewing files, and running some programs. As a security measure, Windows XP and later automatically disable the Guest account in order to prevent logging on to the system.
* Rights and permissions can be assigned to multiple users by using *groups*. Privileges assigned to the group are granted to all group members.
* On a Windows system, users and groups are stored in one of three locations:
	+ Local accounts are stored on each computer and control access to resources on that computer.
	+ Domain accounts are stored in a central database called Active Directory. A domain controller is a special server that stores user accounts, groups, and the rights and permissions assigned to them.
	+ Online accounts are stored online by Microsoft.

Windows systems have default groups that are created automatically. These groups have pre-assigned rights, permissions, and group memberships. These groups can be renamed, but not deleted. In most cases, you should not modify the membership or privileges of these groups without understanding how they are used. Additionally, many Windows features or 3rd party applications installed on the system may create additional groups.

The following table lists some of the default groups used on Windows systems:

|  |  |
| --- | --- |
| **Group Name** | **Capabilities** |
| Administrators | Members of the Administrators group have complete and unrestricted access to the computer, including every system right. The Administrator user account and any other account designated as a "computer administrator" is a member of this group. |
| Backup Operators | Members of the Backup Operators group can back up and restore files (regardless of permissions), log on locally, and shut down the system. Members of this group cannot change security settings. |
| Power Users | Modern versions of Windows no longer use the Power Users group, although it still exists for backwards compatibility. This group was originally used in Windows XP and earlier. Its members could:* Create user accounts
* Modify or delete accounts they created
* Create local groups
* Modify group membership for groups they created
* Modify group membership for the Power Users, Users, and Guests groups
* Change the system date and time
* Install applications

Power Users were not allowed to:* Change membership of the Administrators or Backup Operators groups
* Take ownership of files
* Back up or restore files
* Load or unload device drivers
* Manage security and auditing logs

In modern versions of Windows, you should avoid assigning users to be members of the Power Users group unless an application or service specifically requires it. |
| Users | Members of the Users group can use the computer but cannot perform system administration tasks and might not be able to run some legacy applications.* Members cannot share folders.
* Members cannot install printers if the driver isn't already installed on the system.
* Members cannot view or modify system files.
* Any user created with Local Users and Groups is automatically a member of this group.
* User accounts designated as "standard" or "limited use" accounts are members of this group.
* A user account created as a "computer administrator" is made a member of this group (in addition to being a member of the Administrators group).
 |
| Guests | Members of the Guests group have limited rights (similar to members of the Users group). Members can shut down the system. |
| Cryptographic Operators | Members of the Cryptographic Operators group are allowed to perform cryptographic operations. |
| Event Log Readers | Members of the Event Log Readers group are allowed to use Event Viewer to read the system's event logs. |
| Network Configuration Operators | Members of the Network Configuration Operators group have limited administrative privileges to allow them to manage the system's network configuration. |
| Remote Desktop Users | Members of the Remote Desktop Users group are allowed to access the system remotely using the Remote Desktop Client. |
| Performance Monitor Users | Members of the Performance Monitor Users group can access performance counter data on the system. |
| Performance Log Users | Members of the Performance Log Users group are allowed to schedule logging of performance counters, enable trace providers, and collect event traces on the system. |
| Hyper-V Administrators | Members of the Hyper-V Administrators group are allowed to use Hyper-V on the system to create and manage virtual machines. |

9.4.5 Online Authentication Facts

If a Windows 8 or later system has Internet access, online Microsoft accounts can be used as well as local user accounts to authenticate. A local account is stored on the local system and all profile information associated with the account stays on the computer.

If an online Microsoft account is used to authenticate to the Windows system, Microsoft's online service is used to authenticate the user to the local system as well as to back up some user profile information to Microsoft's cloud.

In this configuration, the email address and password associated with the Microsoft account is used to log on to the system. If the same Microsoft account is used to log on to another Windows 8 or later system, the account's profile information is automatically synchronized to the other computer, including password, desktop configuration, and apps. Files associated with the user profile are not synchronized. However, the account's associated OneDrive account can be used to make user files available on other systems.

Once the online account has been created, you can associate a local user account with an online user account by opening the Settings app and going to **Accounts** > **Your Account** > **Sign In with a My Microsoft Account Instead**.

Online account settings can be managed by opening the Settings app and going to **Accounts** > **Your Account** > **Manage My Microsoft Account**. The following information can be managed:

* Name
* The account email address (which is the account name)
* Personal info
* The account password
* The account security information

You can also close the account and delete all data associated with it.

9.4.8 UAC Facts

User Account Control (UAC) helps minimize the dangers of unwanted actions or unintended software installations. UAC prompts for permission before allowing changes that can affect your computer's security or performance. How UAC works depends on the user account type:

* A standard user account is an account that has the least amount of user rights and privileges required to perform most basic tasks. An administrator account can perform any action on the system.
* Regardless of the user account type, the system first attempts to perform any action using standard user privileges. If standard user rights are not sufficient to perform a task, UAC requests privilege *elevation*:
	+ The standard user is prompted to provide administrator user credentials (username and password). This process is referred to as *Prompt for credentials*.
	+ The administrator user is asked whether the requested task should be allowed. Because the administrator has already logged on with an administrator username and password, this is a simple **Continue** or **Cancel** question. This process is referred to as *Prompt for consent*.
* Actions that require elevated credentials are typically indicated in the interface with a shield icon.
* Prompting for credentials or consent activates the Secure Desktop. With the Secure Desktop, the desktop and all active applications are darkened, and the prompt appears over the shaded desktop. You must respond to the prompt before you can continue with the requested operation or return to the desktop.
* If you disable the Secure Desktop, the prompt is still shown, but the desktop is not dimmed (or locked), allowing you to work with the desktop without responding to the prompt.
* To manage UAC settings, go to **User Accounts** in the Control Panel. You can use the slider displayed to select one of the following UAC configurations:

|  |  |
| --- | --- |
| **Setting** | **Description** |
| Always notify | When configured to always notify:* + Notification occurs when programs make changes
	+ Notification occurs when you make changes
	+ The desktop is dimmed (Secure Desktop is enabled)
 |
| Notify me only when programs try to make changes to my computer | When configured to notify for program changes:* + Notification occurs when programs make changes
	+ Notification does not occur when you make changes
	+ The desktop is dimmed (Secure Desktop is enabled)

This is the default setting. |
| Notify me only when programs try to make changes to my computer (do not dim my desktop) | When configured to notify for program changes without dimming the desktop:* + Notification occurs when programs make changes
	+ Notification does not occur when you make changes
	+ The desktop is not dimmed (Secure Desktop is disabled)

This setting is recommended only if it takes a long time to dim the desktop. |
| Never notify | When configured to never notify, UAC is disabled. No notification occurs and the Secure Desktop is disabled. |

* Additional control over how UAC functions is provided using Local Security policies (located under Local Policies > Security Options). You can configure the following policies:
	+ Use Admin Approval Mode for the built-in Administrator account
	+ Allow UIAccess applications to prompt for elevation without using the secure desktop
	+ Behavior of the elevation prompt for administrators in Admin Approval Mode
	+ Behavior of the elevation prompt for standard users
	+ Detect application installations and prompt for elevation
	+ Only elevate executable files that are signed and validated
	+ Only elevate UIAccess applications that are installed in secure locations
	+ Run all administrators in Admin Approval Mode
	+ Switch to the secure desktop when prompting for elevation
* If you disable UAC (or configure UAC to **Never notify**), the system no longer prompts when you or a program makes changes that require administrative privileges. This is not a secure configuration, and could expose your computer to attacks. If you disable the UAC prompts, you should be careful about programs that you run because they'll have the same access to your computer as you do.
* After enabling or disabling UAC, you must restart the computer to apply the changes. Other changes (such as changing the prompt behavior) can be applied without restarting.

9.5 Remote Services

9.5.3 Remote Desktop Facts

Remote Desktop lets you access your computer from a remote location over a network connection. With Remote Desktop:

* The remote host (called the server) is left running in a state ready to accept a connection.
* The remote client (running on a different computer) establishes the connection and logs on to the remote host.
* The client computer can then run programs, make configuration changes, or access data on the host computer.

Keep in mind the following details when working with Remote Desktop:

* The Remote Desktop service is only supported on Professional, Business, Enterprise, and Ultimate editions of Windows.
* The Remote Desktop client software is available on all editions of Windows.
* A default installation does not enable the Remote Desktop feature. Edit the System properties to enable Remote Desktop.
* By default, Administrators have the ability to log on remotely. You can also allow other users to connect to the system by making them members of the Remote Desktop Users group.
* The user account that is used to authenticate through the Remote Desktop connection must have a password assigned. If one is not set, the connection cannot be established.
* Firewalls must be configured to allow Remote Desktop traffic through them. This is done by opening TCP port 3389 (by default). This port is opened automatically on the Remote Desktop host when remote connections are enabled.
* As you make the connection, you can configure the connection to redirect devices on the host device to the client device. For example, Remote Desktop can:
	+ Play sound from the remote computer through the local computer's speakers
	+ Connect a printer on the local computer to the remote computer. When printing from an application on the remote computer, the print job is redirected through the Remote Desktop connection to the local printer.
	+ Map local drives to the remote computer. This allows access to local drives from the remote computer. It also makes it easy to share files between the remote and local computers.

In addition to Remote Desktop, you can use the following protocols for remote access administration:

* Telnet opens a plain-text, unsecured, remote console connection. Telnet uses TCP port 23.
* Secure Shell (SSH) provides the same capabilities as Telnet, but encrypts the data being transferred. SSH uses TCP port 22.

These protocols are typically used to manage Linux and Macintosh computer systems. While they can also be configured on Windows, Remote Desktop is the preferred solution.

9.5.5 Remote Assistance Facts

Remote Assistance allows a person needing help with their computer to request help from another user, such as a help desk technician or workstation support professional. The person offering assistance can view the desktop of the requester and, with permission, perform actions remotely.

* Remote Assistance uses the Remote Desktop Protocol (RDP) for sending desktop information to a remote computer.
* Remote Assistance must be enabled on the target computer. Use the **Remote** tab in System Properties to enable Remote Assistance and to specify whether remote control is allowed.
* Firewalls must be configured to allow Remote Assistance connections. This is done by opening TCP port 3389 (by default).
* A Remote Assistance session is initiated by sending an assistance invitation. The invitation includes information that allows the remote user and computer to make the connection, exchange messages, and take control if necessary.
* To initiate a remote assistance session, select **Launch Remote Assistance** under System and Security in Control Panel. The requester has three options for sending an invitation:
	+ Save the invitation as a file. If this option is selected, the invitation file must be manually attached to an email message and sent to the person providing assistance.
	+ Use email to send the invitation. If this option is selected, the user's default email program is launched and the invitation automatically attached to a new message.
	+ Use Easy Connect. This allows an invitation to be delivered directly to the person providing assistance through a network connection. However, this option requires that both the requester and the helper have access to Microsoft's global peer-to-peer network. Many (if not most) organizational firewalls block access to this network by default. If this is the case, use one of the above options instead.
* By default, the requester must initiate the invitation. However, in a corporate environment Active Directory can be configured to allow the expert to initiate a Remote Assistance connection.
* Invitations require a password and have an expiration date. Expired invitations cannot be answered.
* With permission, the helper can take control of the user's computer. The user can regain control of the computer at any time by pressing the Esc key, Ctrl + C, or clicking **Stop Control**.
* The helper cannot copy files from a user's computer. The user must explicitly send any files the helper may need.

9.5.9 Screen Sharing Facts

Screen Sharing allows you to share the screen of your Mac OS system. If enabled, it can also allow a remote user to control the system. Use Screen Sharing to:

* Remotely access your own system
* Help troubleshoot an issue on a client's system
* Give a presentation or collaborate on a project with others

Keep in mind the following information regarding Screen Sharing:

* Screen Sharing is disabled by default. To enable Screen Sharing, complete the following steps:
	1. Click **Apple** menu > **System Preferences**.
	2. Click **Sharing**.
	3. Select the **Screen Sharing** checkbox.
* You can specify which users are able to connect to the system in the Screen Sharing settings dialog (e.g., all registered users, specific users only, or anyone who requests access).
* To allow non-Mac systems to use Screen Sharing (i.e., Windows and Linux systems), you need to enable the VNC viewer setting and specify a VNC password.
* Systems on the network that have Screen Sharing enabled will appear in the Shared category in the Finder window.
* Mac OS uses the Screen Sharing app to connect to systems that have Screen Sharing enabled.
* Screen Sharing has two different sharing modes:
	1. Control mode allows you to control the system as if you were physically at the computer.
	2. Observe mode places control of the system in the hands of the user and is typically used when giving a presentation.
* With the Shared Clipboard setting enabled, text can be copied between the remote system and the local system, and vice versa.
* Display and quality settings can be customized in order to match the remote system's settings and connection speed.

9.6 Windows Application Management

9.6.3 Desktop Application Management Facts

Be aware of the following facts about managing applications.

* Application installation involves more than just copying the executable files to the computer. Installation typically modifies the registry, creates shortcuts, and configures other settings required by the application.
* Installation of an application usually creates a tile on the Start menu and may also create a shortcut on the desktop. A *shortcut* is a pointer file that identifies the location of the executable file that runs the application.
	+ Shortcuts that point to removable drives (such as CD/DVD drives) or network drives could become unavailable if the referenced drive is disconnected.
	+ During install, you can often choose to add shortcuts for only the current user or all users.
	+ The shortcut also identifies a directory that the application uses or references when it first starts. You can modify the directory by changing the **Start in** property for the shortcut or executable file.
* A 64-bit operating system can run both 32-bit and 64-bit applications. However, a 32-bit operating system can only run 32-bit applications.
* By default, applications are installed into the **Program Files** directory on the root of the system drive.
	+ During installation, you can typically specify an alternate install location.
	+ 64-bit operating system versions include an additional folder named **Program Files (x86)**. 32-bit applications are installed into this folder.
* Users must have the correct permissions or rights to install applications. The ability to install applications depends on the user's group membership and the operating system:

|  |  |
| --- | --- |
| **Group** | **Permissions** |
| Users | Users who are members of only the Users group are not able to install applications. |
| Power Users | On legacy versions of Windows (XP and earlier), users who are members of the Power Users group can install applications that do not make modifications to system files.On modern versions of Windows, Power Users cannot install applications. |
| Administrators | Users who are members of the Administrators group can install applications. |

* In some cases, users require special privileges or rights to run applications. For example, legacy applications that access the system in certain ways may require running the application run as an administrator.
* Copying an application's shortcut to the C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup folder will cause that application to be automatically launched every time the system is booted. You can also use Task Scheduler to configure an application to run automatically based upon event triggers that you define.
* Many applications as they run create data files (such as documents or video files), and might also require creating temporary files. The user must have sufficient permissions to the directories where the data and temporary files are created.

9.6.5 Application Compatibility Facts

Some older applications may not run properly when you try to use them on new versions of Windows. There are several options for fixing the issue:

* Buy a newer version of the application.
* Use Compatibility Mode settings.
* Use XP Mode (Windows 7 only).
* Use Client Hyper-V to create a virtual machine running an older version of Windows.

Application vendors may provide upgrades to their current applications to resolve application compatibility issues. This is the best long-term application compatibility solution.

Compatibility Mode can be used to run an older program using settings from a previous version of Windows. The Program Compatibility Assistant (PCA) runs in the background and monitors applications for known compatibility issues when they are run. When a potential issue with an application is detected, the PCA will prompt the user and provide links to recommended solutions. The following options are available:

* Use the Compatibility Troubleshooter to automatically determine the settings for the application to run on the current version of Windows. When using the Program Compatibility Troubleshooter:
	+ You start the utility by right-clicking on the executable file or the executable file shortcut and then selecting **Run compatibility troubleshooter** on the Compatibility tab.
	+ If a solution is found, the settings are stored and the application will be launched using the modified environment.
* Manually specify predefined compatibility mode.
	+ The predefined mode replicates the environment of a previous version of a Windows operating system.
	+ To manually specify settings, mark **Run this program in compatibility mode for** on the Compatibility tab, then select the version of Windows the application was written for. You may have to try more than one to get the application to run correctly.
	+ The service pack level is an important consideration when selecting a previous version.
* Manually set compatibility settings without selecting a specific version of Windows. The options that can be configured include:
	+ **Reduced color mode** allows applications with a limited color pallet to display correctly. Select one of the following:
		- **8-bit (256) color**
		- **16-bit (65536) color**
	+ **Run in 640 x 480 screen resolution** allows low resolution applications to display properly.
	+ **Disable display scaling on high DPI settings** turns off automatic resizing of applications when large-scale fonts are being used.
	+ **Run this program as administrator** configures the application to run with administrator-level privileges. Old applications that ran on legacy versions of Windows may require elevated access to run correctly.
* END Week 2 Class 3