INSTALLING, UPGRADING & MIGRATING TO WINDOWS 7 (14 PERCENT)

Perform a Clean Installation

Windows 7 Minimum Hardware Requirements

- Processor
  - 1 GHz (32 bit/x86) or 2 GHz (64 bit/x64)
- RAM
  - 1 GB (32 bit) or 2 GB (64 bit)
- Hard Disk
  - 16 GB (32 bit) or 20GB (64 bit)
- Direct X9 graphics w/ 128MB of video RAM (For Aero Theme)
- DVD/R-W
- Network Interface Card

Attended Installation

- Someone is required to interact with computer while installing
- Need computer that meets minimum hardware requirements
- Windows 7 drivers for anything not in Windows Logo Program
- Windows 7 DVD or installation files across a network
- Basic Input Output System (BIOS) that meets Windows 7 compatibility

Installation Methods

- DVD

- USB Flash Drive
  - Configure with diskpart to hold installation files
    - select volume
    - format fs=fat32
    - mark as active
  - Copy installation files from DVD to root partition of USB Drive

- Network Share
  - Boot to Windows PE and connect to network share

- Windows Deployment Server (WDS)
  - Install W7 on computers at a remote location across wide area network (WAN)
  - Support for Windows Image Format (WIM) and Pre-installation Environment (PE)
  - Computer with Preboot eXecution Environment (PXE), connects to WDS, which then installs the OS
  - Provides images of OS with specific settings and applications required by policy
  - Creates images that enable the automated installation of Windows 7
  - Requirements:
    - Dynamic Host Configuration Protocol (DHCP)
    - Domain Name System (DNS)
    - Active Directory Domain Services (AD DS)
    - Windows Deployment Services on Server

- Windows Automated Installation Kit (WAIK)
- F12 to use PXE for booting from network share and accessing DHCP server

Clean Installation

- Startup installation from one of the installation methods
  - Install Now
    - Upgrade
      - Only available when upgrading from inside OS
    - Custom (advanced)
  - Select partition to install Windows
    - Drive Options to perform disk maintenance
    - Shift + F10 to access command prompt from this point
  - Set Up Windows Options
    - Username and Computer Name (becomes admin)
    - User password
    - Product Key
    - Windows Updates settings
    - Set Time Zone and Date

Dual Booting

- Allows one computer to boot to many operating systems
- Requires reboot to change operating systems
- Not as common due to virtual machines
- Requires separate hard disk or partition

- Tools
  - Bootcfg.exe
    - Edit boot.ini in XP or older
  - Bcdedit.exe
    - Edit boot configuration in Vista/7
  - Winload.exe
    - OS loader
    - Loads kernel, hardware abstraction layer (HAL) and drivers on startup
  - Winresume.exe
    - Resumes the OS from hibernation

- Logging Files
  - Boot Logging → *ntbtlog.txt*
  - Action Log → *setupact.log*
  - Error Log → *setuperr.log*
  - Network/Domain Errors Log → *netsetup.log*

Upgrade to Windows 7 from previous versions of Windows

Upgrading Older Systems to Windows 7

- Run Windows 7 Upgrade Advisor
  - Address any issues

- Direct Upgrades
  - Editions
    - Vista Home Basic → Windows 7 Home Basic, Home Premium or Ultimate
    - Vista Home Premium → Windows 7 Home Premium or Ultimate
    - Vista Business → Windows 7 Professional, Enterprise or Ultimate
    - Vista Enterprise → Windows 7 Enterprise
    - Vista Ultimate → Windows 7 Ultimate

  - Insert DVD while in operating system
    - Go online to get the latest updates for installation(recommended)
    - Upgrade

- Non-Direct Upgrades
  - 9x/Me, NT 4.0, 2000, XP Professional → Cannot be upgraded, perform clean installation
  - Non-Windows OS → Cannot be upgraded, perform clean installation

Upgrade Checklist

- Check for BIOS upgrades
- Scan and eliminate viruses; remove/disable anti-virus program; remove malware
- Install any upgrade packs required for older software applications
- Install the latest service pack plus any other updated Microsoft has published

Upgrading Windows 7 Editions

- Home Basic/Starter → Home Premium, Professional, Ultimate
- Home Premium → Professional, Ultimate
- Professional → Windows 7 Ultimate
- Ultimate/Enterprise → No further upgrades
- **Use Windows Anytime Upgrade**

Migrating To Windows 7

Types of Migration

- **Side by Side Migration ("Replace")**
  - Move data from **old computer** to new **computer**

- **Wipe and Load Migration ("Refresh")**
  - Collecting data from **one computer**
  - Perform a clean installation
  - Settings reloaded onto new installation

Tools for Migration

- Windows Easy Transfer
  - Migrates user profiles, settings and data
  - Easy Transfer Wizard
    - How to Transfer
      - Easy Transfer Cable
      - Network Connection
      - CD, DVD or removable device
    - What to Transfer
      - All user accounts, files and settings
      - My user account, files and settings only
      - Advanced
        - Select specific locations, files and folders

- User State Migration Tool (USMT)
  - Migrating large number of users in corporate environment
  - Migrates local user accounts, personalized settings, personal files, operating system and applications settings
  - Supports uncompressed, compressed & hard-link migration stores
    - Compressed
      - Information is encrypted
      - Reduces HD disk space
    - Hard-Link
      - Store is maintained on local PC during Wipe & Load

  - Migration Rules
    - Migapp.xml – rules for migrating application settings
    - MigDocs.xml – rules that locate user documents automatically
    - MigUser.xml – rules for migrating user profiles and user data

  - Scanstate
    - Run on source computer
    - **scanstate store /i:[path\filename] /config: [path\filename] /hardlink /nocompress /o /p:file /vsc**

- store — Specifies a path to store
- /i:[path\filename] — Identifies a migration .xml file
- /config: [path\filename] — Specifies a config.xml file
- /hardlink — Enables creation of hard link migration store
- /nocompress — Disables data compression
- /o — Overwrites exisiting data in the store
- /p:file — Creates a size estimate in the path specified
- /vsc — Creates a size estimate in the path specified

- Creates Easy Transfer file compatible with Easy Transfer Wizard

- Loadstate
  - Run on destination computer
  - **Loadstate store /i:[path\filename] /hardlink /nocompress**

    - store — Specifies a path to store
    - /i:[path\filename] — Identifies a migration.xml file
    - /hardlink — Enables creation of hard link store
    - /nocompress — Disables data compression

Migrating Users from previous versions of Windows

- Select custom from Windows 7 setup screen
- Choose not to format partition, files and folders are preserved
- Operating system files and folders plus user settings are stored in Windows.old folder
- Application settings are preserved in Windows.old\Program Files folder
- Must reinstall all applications after Windows 7 upgrade is complete

DEPLOYING WINDOWS 7 (13 PERCENT)

***Windows System Image Manager (Windows SIM)* -** Helps create answer files

***Answer File* -** XML script that provides answers to questions during setup wizard; normal Unattend.xml

***Windows Image* -** Compressed file in .wim format that contains files and folders to duplicate Windows Installation; can include multiple Windows images

***Windows Automated Installation Kit (Windows AIK)* -** Tools and documentation that facilitates customization and deployment of computers running Windows 7 and Server 2008 R2

***Windows Preinstallation Environment (Windows PE)* -** Minimal operating system that assists you in preparing computer for installation

***Windows Deployment Services (WDS)* -** Server based deployment that helps you set up remote client computers without physically sitting at computer

***ImageX* -** Command line tool that captures and applies Windows images (.wim files)

***Sysprep* -** Removes system-specific information so you can capture and deploy the Windows Image

Windows Recovery Environment (Windows RE) - Diagnostic and recovery tool with Windows PE; can use to build a custom recovery solution

Windows PE (3.0) Commands

- BCDBoot
  - Initializes boot configuration data store to copy boot environment files to new computer
- Bootsect
  - Configure boot sectors
- DiskPart
  - Creates and configures disk partitions and volumes
- Deployment Image Servicing and Management (DISM)
  - Enumerates, installs, uninstalls, configures and updates system images
- Drvload
  - Installs and manages drivers
- ImageX
  - Captures and applies Windows images
- Net
  - Enables network communication and manages users and services
- Netcfg
  - Configures network access
- Wpeinit
  - Initializes Windows PE at boot time
- Oscdimg
  - Creates ISO file with image

Customizing Windows 7

Build an Answer File

- *Steps*
    - Copy install.wim from Windows 7 Product DVD to local computer
    - Use Windows SIM to open file and create catalog file
    - Open sample answer file from Windows AIK directory
    - Add customization to Configuration Passes
        - WindowsPE
        - offlineServicing
        - Generalize
        - Specialize
        - Audit System
        - Audit User
        - Oobe System (out-of-box experience)

    - Validate file and save as autounattend.xml/unattend.xml
        - Place on USB drive or in root directory of DVD
        - Windows will automatically search for file during setup

Capture a system image

Audit Mode

- Press Shift + Ctrl + F3
- Reboots and logs in with default administrator account so you can make changes to installation and prepare for imaging

Sysprep

- Run on reference computer at c:\Windows\System32\sysprep

- System Cleanup Action
    - Enter Out-of Box Experience
        - Generalize (removes unique settings)
    - Enter System Audit Mode

- Shutdown Options
    - Quit
    - Reboot
    - Shutdown

- Command Line
    - /audit
        - Runs in audit mode; enables you to add drivers and applications
    - /quiet
        - runs without user interaction
    - /generalize
        - removes system specific information (SSID) and product activation

- /oobe
    - runs Windows Welcome; out of box experience
- /reboot
    - force computer to reboot after completion of disk image
- /unattend: [file_name]
    - specifies the name of answer file
- /shutdown
    - forces computer to shut down after sysprep completes

Image Capture

- Use ImageX to capture contents of installation for deployment
    - ImageX /capture *image_path image_file "name" "description"* /boot /check /compress [type] /config /flags "*Edition ID"* /norpfix /scroll /verify

        - /capture — Captures system
        - image_path — Name & location of image
        - image_file — Name and location of new .wim file
        - "name" — Name of the new .wim file
        - "description" — Optional description
        - /boot — Marks volume image as bootable
        - /check — Checks the integrity of .wim file
        - /compress[type] — Type of compression during capture
        - /config — Name and location of configuration file (.ini)
        - /flags "*Edition ID*" — Specifies version of Windows to be captured
        - norpfix — Disables reparse point tag fixup
        - /scroll — Scrolls output for redirection
        - /verify — Checks file resources for errors and duplicates
        - /split — Splits an image

- Once sysprep runs and is computer is restarted, boot into Windows PE mode
    - Net use network share
        - Net use z: \\r2d2\Windows Installations

    - Go to z:

    - Use ImageX to capture image
        - Imagex /capture c: c:\image1.wim "Windows 7 Ultimate" /compress fast /verify

Prepare a system image for deployment

Deployment Image Servicing and Management (DISM)

- Command line utility enabling you to configure Windows images before deploying them
- Install, configure, enumerate, update and uninstall applications, drivers, Windows features and international settings
- Does not enable you to capture new Windows images

- dism /image: *image_path* /online {dism_options} {servicing_command} [servicing_argument]
    - /image: *image_path*
        - Specifies the path of windows image being worked on
    - /online
        - Specifies servicing a running computer
    - {dism_options}
        - Specifies optional parameters
    - {servicing_command} [servicing_argument]
        - Specifies action to be taken along with any arguments

- /Mount-Wim
    - ***dism /mount-wim /wimfile:w7ultimate.wim /index:1 /mountdir:c:\mount***

- /Commit-Wim
    - ***dism /commit-wim /mountdir: c:\mount***

- /Unmount-Wim
    - ***dism /unmount-wim /mountdir: c:\mount /commit***

- /Remount-Wim
    - **dism /remount-wim /mountdir:c:\mount**

- /Cleanup-Wim
    - ***dism /cleanup-wim*** (use while WIM is mounted)

- /Get-MountedWimInfo
    - ***dism /get-mountedwiminfo*** (use while WIM is mounted)

- /Get-Wim Info
    - ***dism /get-wiminfo /wimfile:w7ultimate.wim /index:1*** (use when WIM is unmounted)

Inserting an application into an image

- dism /image:*image_path* /Add-Package /PackagePath: [path_to_.cab_file]
- dism /image:*image_path* /Remove-Package /PackagePath: [path_to_.cab_file]

Inserting a driver into system images

- /Get Drivers
  - ***dism /image:c:\mount /get-drivers /all***
    - displays basic information about all driver packages, no /all tag shows 3rd party drivers only

- /Get-Driver Info
  - ***dism /image:c:\mount /get-driverinfo /driver:[path to the inf.file]***
    - displays detailed information about a specific driver package

- /Add-Driver
  - ***dism /image:c:\mount /add-driver /driver:[path to the .inf file]***
    - Adds third-party driver packages

- /Remove-Driver
  - ***dism /image:c:\mount /remove-driver /driver:[path to the .inf file]***
    - Removes third party driver packages

Inserting Updates into system images

- /Get-Current Edition
  - ***dism /image:c:\mount /Get-CurrentEdition***
    - Displays the edition of specified image

- /Get-TargetEditions
  - ***dism /image:c:\mount /Get-TargetEditions***
    - Lists the Windows editions that the image can be upgraded to

- /Set-Edition:<target_edition_ID>
  - ***dism /image:c:\mount /Set-Edition:Ultimate***
    - Upgrades the image to higher edition

- /Set-ProductKey:<productKey>
  - ***dism /image:c:\mount /Set-ProductKey:<product key>***
    - Enters the product key for the current edition

Configuring Tasks To Run After Deployment

- Windows Optional Component Setup Tool (OCSetup.exe)
  - ocsetup.exe *component* log:file /norestart /passive /quiet /unattendfile:filename /uninstall /x:parameter

Deploy a system image

- Boot To Windows PE
  - Create two Volumes
    - System Reserved
      - Diskpart
        - select disk 0
        - clean
        - create partition primary size=100
        - select partition 1
        - format fs=ntfs quick label=system
        - active
    - OS Installation
      - Diskpart
        - create partition primary
        - select partition 2
        - format fs=ntfs quick label=windows
        - assign letter=g

  - net use z: \\r2d2\WindowsInstallations
  - Go to z:
  - ImageX to apply image
    - Imagex /apply image1.wim 1 g:
  - Run BCDBoot
    - g:\windows\system32\bcdboot g:\windows

Types of Automated Deployments

- **High Touch with Retail Media**
  - Installing Windows 7 on each client computer with the DVD, followed by manual configuration of each computer
  - You can automate with answer file

- **High Touch with Standard Image**
  - Manual installation of Windows using volume-licensed media and answer files, plus manual installation of applications and configuration of computers
  - Windows AIK with reference computer

- **Lite-Touch, High-Volume Deployment**
  - Utilizes *Microsoft Deployment Toolkit 2010(MDT)* to deploy to networks
    - Use **Deployment Workbench** to work on your image
  - Makes use of USMT, ACT, Windows AIK
  - Need media or server configured with WDS as well as file server and distribution share
  - Requires some amount of user intervention

- **Zero-Touch, High-Volume Deployment**
    - Same as Lite Touch but also utilizes Configuration Manager 2007 R2, a server based tool providing comprehensive deployment strategy for OS, software, updates and remote administration and systems inventory
    - No user intervention required

- **Windows Deployment Services (WDS)**
    - Enables you to install Windows 7 on computers at a remote location using Wide Area Network (WAN)
    - Support for Windows PE and WIM file format
    - Reduces complexity; simplifies management of installation server; simplifies recovery procedures
    - **Transport Service Mode**
        - **Allows you to install Windows 7 without AD DS domain or DNS server**

    - Setting Up WDS
        - Requirements
            - DHCP (Dynamic Host Configuration Protocol)
            - DNS (Domain Name System)
            - AD DS (Active Directory Domain Services)

    - Using WDS to Automate Deployment of Windows 7
        - Computers need Network Interface Card (NIC) that supports PXE Boot Environment or create a discover image if no PXE card available

        - F12 for Network Boot
            - Must enable for all client computers by accessing boot tab of servers properties dialog box in WDS Management Console
        - Notes
            - Computer security is retained when you restart computer
            - There is a MMC snap-in for WDS on server
            - User selects boot image to be applied
            - Copy unattend.xml to WDS server to automate answers

<u>Configure a VHD</u>

- Single file with files and folders on HD Partition
- Available in Windows 7 Enterprise & Ultimate and Server 2008 R2

Types of VHD
- Fixed - Describes VHD with a fixed size
- Dynamic - The VHD is only as large as the data contained in it; You can specify maximum size
- Differencing
    - "Child VHD"
    - Contains only modified disk block of parent VHD
    - Parent VHD can be any type of the three. Multiple differencing VHD's is called *differencing chain*
- Use Hyper-V to run Windows 7 Virtual Machines on Windows Server 2008 R2

Tools used with VHD

- Disk Management
  - MMC snap-in to manage VHD's
- DiskPart
  - Perform VHD Management; similar to Disk Management
- Bcdedit
  - Manage boot configuration data (BCD) stores
- Bcdboot
  - Manage and create new BCD stores and BCD entries;
- DISM
  - Apply udates, applications, drivers to VHD
- Sysprep
  - Enables you to prepare system for imaging and deployment
- ImageX
  - Create, modify and apply Windows Images

Creating VHD's

- Use Disk Management
  - Create VHD
    - Save File
    - Specify Size
    - Initialize Disk
    - Create New Simple Volume
      - Format Volume
    - Detach VHD

- Use DiskPart
  - Run command prompt as administrator
  - Diskpart
    - create vdisk file="c:\vhd\windows_7.vhd" maximum=20000 type=fixed/expandable
    - select vdisk file="c:\vhd\windows_7.vhd"
    - attach vdisk
    - create partition primary
    - format fs=ntfs quick label=Windows 7 VHD
    - assign letter=j

Mounting VHD's

- Disk Management
  - Attach VHD
- DiskPart
  - select vdisk file="path"
  - attach vdisk

Deploying VHD's

- Treat Windows 7 VHD files similarly to .wim files
- Known as "VHD Boot"
- Process:
  1) Install Windows
  2) Customize installation
  3) Use Sysprep to generalize image
  4) Use ImageX to capture image
  5) Deploy image to VHD file and initialize the VHD boot environment
     - Open command prompt
     - Navigate to Windows AIK → Tools →Architecture
     - Use ImageX to locate index number for image you want to deploy
     - Apply to drive letter assigned to VHD
       - imagex /apply c:\Windows_Install \install.wim \check 1 p:

Booting VHD's

- Configure with bcdedit
  - bcdedit /copy {current} /d "Windows 7 VHD"
  - bcdedit /set {GUID} device vhd=c:\vhd\windows_7.vhd
  - bcdedit /set {GUID} osdevice vhd=c:\vhd\windows_7.vhd
  - bcdedit /set {GUID} detecthal=on

Updating VHD's

- Offline servicing – modification or updating a Windows image offline without first booting it
  - dism
    - /Add-Driver
    - /Remove-Driver
    - /Add-Package
    - /Remove-Package
    - /Get-Package
    - /Get-Features
    - /Get-FeatureInfo
    - /Enable-Feature
    - /Disable-Feature
    - /Set-Edition

- Microsoft System Center Virtual Machine Manager (MSCVMM)
  - Integrates with System Center Configuration Manager (SSCM) and Windows Server Update Services (WSUS)

CONFIGURING HARDWARE AND APPLICATIONS (14 PERCENT)

Configure devices

Updating Drivers

- Windows Update
  - Compares hardware ID's of installed devices with drivers made available on Microsoft website. Only if exact match is found is update installed.

- Device Manager
  - Icons
    - Device disabled – black downward pointing arrow (⬇)
    - Red 'X' – device not functioning (drivers are not installed) (✖)
    - Yellow question mark – device is functioning but experiencing problems (**?**)
    - Blue "i" – device has forced resource configurations (i)

  - Tabs (change depending on type of driver):
    - General
    - Advanced
    - Driver
      - Driver Details
      - Update Driver
      - Roll Back Driver
      - Disable
      - Uninstall
    - Details (GUID#)
    - Resources
    - Power Management (turn on/off)

Driver Signing

- Administrators can only install drivers (both signed and unsigned)
  - Run **device installation** to manage for individual desktops
  - Change with group policy
- Microsoft validation for 3rd party manufacturers
- Microsoft signs the driver files digitally (electronic signature)
- Troubleshooting Tools
  - sigverif
    - Verifies drivers throughout entire system
  - driverquery
    - Command prompt to check which unsigned drivers have been installed
      - Switches
        - /si Signed only
        - /v Verbose
        - /fo File Output (table/list/csv)
  - dxdiag
  - verifier
    - Need to configure first and then restart computer

        - System Information (msinfo32)
            - Hardware Resources → Conflicts/Sharing
            - Software Environment → System Drivers

- Staging Driver Packages
    - Ensuring drivers are digitally signed by Windows or trusted publisher, add certificates to trusted certificate store; *Only way for users to update drivers without administrative rights*
    - *C:\windows\system32\driverstore\file repository*

Configure application compatibility

Configuring Application Compatibility

- **Run this program in compatibility mode for:**
    - Select Windows Version
- **Run in 256 colors**
    - Limited colors to run program
- **Run in 640x480 screen resolution**
    - Run program in smaller window
- **Disable visual themes**
    - Disables themes
- **Disable desktop composition**
    - Shuts off advanced display features (Aero Theme)
- **Disable display scaling on high DPI settings**
    - Shuts off automatic font resizing
- **Run this program as administrator**
    - Requires administrative mode
- **Change settings for all users**
    - Choose settings that apply to all users

Application Compatibility Toolkit (ACT)

- Identifies compatibility with Vista & Windows 7
- Which applications need additional testing or use of shims
- Test web applications and websites

- Implementing Shims
    - Minor compatibility fix to assist applications originally written for older operating systems to match with newer OS
    - Create own shims with **Compatibility Administrator** from the Application Compatibility Toolkit
    - Redirects application API to shim
        - .sdb extension

- Internet Explorer Compatibility Test Tool
    - Collects issues with company's websites and web-based applications in IE 7 & 8.
    - Uploads data to ACT Log Processing Service and displays results in real time

Windows XP Mode

- Uses Virtual PC as runtime engine
- Available in Professional, Ultimate & Enterprise
- Requirements are 2GB RAM, 15GB hard disk space
- Processor needs hardware virtualization
- BIOS needs to support virtualization

Configure application restrictions

Application Restrictions

- Create separate rules for Windows installer files, executable files and script files
- AppLocker enables you to restrict applications according to publisher rules (applications digital signature) and version

Software Restriction Policies

- Can be implemented on Windows XP, Vista & Windows 7
- Set with local group policy or with group policy management on domain
    - Computer Configuration\Windows Settings\Security Settings\Software Restriction Policies
        - Global Settings
            - Enforcement
            - Designated File Types
            - Trusted Publishers
        - Security Levels
            - Disallowed
                - Does not allow software to run regardless of user's access rights
            - Basic User
                - Enables the user to run applications as normal user only
            - Unrestricted
                - Allows software to run according to user's access rights; default
        - Additional Rules (in order of effectiveness)
            - (1)Hash Rule
                - Fixed length series of bytes that uniquely identify application or file
                - Control very specific applications (even by version number)
            - (2)Certificate Rule
                - Identifies software according to its publisher
                - Cryptographic signature
                - Application must be signed
                - Resource intensive
            - (3)Path Rule
                - Identifies software according to its Universal Naming Convention (UNC) file path

        - Based on files or folders
        - Can be circumvented by moving file

    - (4)Network Zone Rule
        - Identifies software according to an Internet Explorer network zone (Internet, Trusted Sites, etc.) downloaded from
        - Only applies to .msi and not .exe files

    - (5)Default Rule
        - Security Levels

AppLocker

- Only available in Windows 7 Enterprise, Ultimate, Server 2008 R2
- Specifies type of applications that users can run
- Define rules according to file attributes in digital signature
- Prevent execution of unlicensed, unapproved, unauthorized applications

- Configure from Group Policy
    - **Application Identity Service (needs to be running for AppLocker to work)**
        - Set at *Computer Configuration**Policies**Windows Settings**Security Settings**System Services on domain*

    - Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker
        - Rules
            - Executable Rules
                - .exe and .com files
                - Default Rules
                    - Everyone – All files in Program Files folder
                    - Everyone – All files in Windows folder
                    - BUILTIN/Administrators – All Files

            - Windows Installer Rules
                - .msi and .msp files (do not need to be downloaded from Internet)
                - Default Rules
                    - Everyone – All digitally signed Windows Installer files
                    - Everyone – All Windows Installer files in c:\Windows\Installer
                    - BUILTIN/Administrators – All Windows Installer files

            - Script Rules
                - .bat, .cmd, .js, .ps1, .vbs
                - Default Rules
                    - Everyone – All scripts located in the Program Files folder
                    - Everyone – All scripts located in the Windows folder
                    - BUILTIN/Administrators – All scripts

- Create New Rule
  - Action
    - Allow or Deny
  - User or Group
  - Type of Condition
    - Publisher
      - Select file to pull publisher information
      - Needs to be digitally signed
    - Path
      - Browse for file path
      - Needs to be digitally signed
    - File Hash
      - Add/remove files
      - Use when applications are not digitally signed
    - Exceptions
      - Add, edit or remove exceptions
      - Can be a combination of publisher, path or file hash

<u>Configure Internet Explorer</u>

Compatibility Mode

- Runs Internet Explorer as an "older" version

- Tools → Compatibility View or Compatibility View Button
  - Change current website into compatibility view

- Tools → Compatibility View Settings
  - Add a specific website to always be displayed in compatibility view
    - Include updated websites from Microsoft
    - Display intranet sites in compatibility view
    - Display all websites in compatibility view

- Group Policy settings
  - Administrative Templates\Windows Components\Internet Explorer\Compatibility View
    - Turn on Internet Explorer 7 Standards Mode
    - Turn off Compatibility View
    - Turn on Internet Explorer Standards Mode for Local Intranet
    - Turn off Compatibility View button
    - Include updated websites from Microsoft
    - Use Policy List of Internet Explorer 7 Sites
      - Add sites that must be viewed in IE7 Compatibility View

- Use Policy List of Quirks Mode sites

Configuring Internet Explorer Settings

- Tools → Internet Options
  - General Tab
    - Set Home page
    - Browsing History
      - Delete
      - Settings
    - Search
      - Settings
    - Tabs
      - Settings
    - Appearance
      - Colors
      - Languages
      - Fonts
      - Accessibility
  - Security Tab
    - Security Zones
      - Internet
        - All websites are included in the Internet zone
        - Custom Level
      - Local intranet
        - Sites Button
          - Automatically detect intranet zone
        - Custom Level
      - Trusted Sites
        - Sites Button
          - Add sites to zone
        - Custom Level
      - Restricted Sites
        - Sites Button
          - Add sites to zone
        - Custom Level
      - Protected Mode
        - Provides enhanced levels of security and protection from malware
        - User needs to provide consent to run malware
        - Enabled by default on all zones except Trusted Zones
        - Runs by default on IE8

- Privacy Tab
  - Select a preset level for handling cookies
    - High
    - Medium High
    - Medium
    - Low
    - Accept All Cookies
  - Sites Button
    - Block or allow cookies to be exchanged with specific websites
  - Advanced Button
    - To establish a different method for handling cookies in Internet zone
  - Pop-up Blocker
    - Settings
      - Add sites to allow
      - Change default handling of Pop-ups
        - High: Block all pop-ups
        - Medium: Block most automatic pop-ups
        - Low: Allow pop-ups from secure sites
- Content Tab
  - Parental Controls
    - Enables you to control types of content children are permitted to access
  - Content Advisor
    - Control Internet content that users can view on computer
  - Certificates
  - Auto Complete
  - Feeds and Web Slices
- Advanced Tab
  - Set additional options

- SmartScreen Filter
  - Checks websites against a list of reported phishing sites; also checks software downloads against a list of reported malware sites
  - Sends addresses/sites to Microsoft

- Configuring Providers
  - Change default search providers
  - Find more search providers… (link)

- Managing Add-ons
  - Additional features that you can install to IE that provide additional functionality

  - Tools → Manage Add-ons
    - Show:
      - All add-ons
      - Currently loaded add-ons
      - Run without permission (preapproved by Microsoft, manufacturer, ISP)
      - Download controls

    - Cannot uninstall add-ons from Manage Add-ons location; must do it from Control Panel, Programs and Features

- InPrivate Browsing
  - Information that is discarded in this mode
    - Cookies and temporary Internet files
    - Website browsing history
    - Information on form pages including passwords
    - AutoComplete and address bar information
    - Automatic Crash Restore information

- InPrivate Filtering
  - Blocks providers of additional website information from being sent to these providers
    - Perform selective blocking of content providers
    - Disable In Private Filtering
    - Manage your add-ons
    - Modify the number of providers displayed

- Certificates For Websites
  - Provides secure identification and verification ; protects and encrypts user information
  - HTTPS with SSL
  - Gold lock icon
    - Click to view information about websites certificate

  - Content Tab
    - Certificates
      - Clear SSL state
        - ➢ Remove personal information
      - Publishers
        - ➢ View information on trusted and untrusted publishers
      - Certificates
        - ➢ View certificates issued to yourself or others on computer

CONFIGURING NETWORK CONNECTIVITY (14 PERCENT)

Transmission Control Protocol (TCP) – connection orientated, reliable communication between two hosts; large amounts of data

User Datagram Protocol (UDP) – fast, nonconnection-orientated communication; short bursts of data

Internet Protocol (IP) – handles, addresses and routes packets between hosts on a network

Internet Control Messaging Protocol (ICMP) – enables hosts on TCP/IP network to share status and error information

Address Resolution Protocol (ARP) – used to resolve IP address of destination computer to the physical or Media Access Control (MAC) address

Configure IPv4 network settings

IP Address

- Unique, logical address that identifies computer (host or node) and the subnet on which it is located
- Dotted decimal (each decimal is octet of 1 and 0's)
- 8 bits = 1 byte = 1 octet, therefore 192.168.56.1 is equal to 32 bits or 4 octets

Subnet Mask

- Applied to an IP address to determine the subnetwork address and the host address on that subnet
- All hosts on the same subnet must have the same subnet mask for them to be applied

Default Gateway

- Location on the local subnet to which the local computer will send all data meant for other subnets; IP address for router capable of transmitting data to other networks

DHCP (Dynamic Host Configuration Protocol)

- Provided to computer when it needs to be connected to network
- Automatically assigns IP addresses, subnet mask, default gateway, etc.
- Uses DHCP server
    - Leased for a specific period of time
    - When lease is up, IP address is placed back in pool and can be delivered to another computer

DNS server address

- Place where names of IP hosts are sent so that the DNS server will respond with an IP Address; *name resolution*
- Distributed database of records that maps names to IP addresses and vice versa

Windows Internet Naming Service (WINS)

- Server address is location where network computers send requests to resolve NetBIOS names to IP addresses.
- Used on older system where NetBIOS is running

Network Address Translation (NAT)

- converts private addresses into public addresses for communication over the Internet
- Lives inside router or firewall

IPv4 Addressing

- Static IP address is one that is permanently assigned to a computer on the network
- Routers and servers require static; client computers assigned dynamic because they are more likely to be moved around

- Address Classes
  - Class A 1.0.0.0 – 126.255.255.255 [Large Networks/ISP's]
    - Network 1, Host .0.0.0
  - Class B 128.0.0.0 – 191.255.255.255 [Large or midsize ISP's]
    - Network 128.0, Host .0.0
  - Class C 192.0.0.0 – 223.255.255.255 [Small networks]
    - Network 192.0.0, Host .0
  - Class D 224.0.0.0 – 239.255.255.255 [Multicasting]
  - Class E 240.0.0.0 – 254.255.255.255 [Reserved for future use]
  - Loopback 127.0.0.1 – 127.255.255.255 [Loopback testing]
    - Ping 127.0.0.1 to test

- Private IPv4 Networks
  - Class A 10.0.0.0 – 10.255.255.255 1 Network 16,777,214 hosts/ntwk
  - Class B 172.16.0.0 – 172.16.255.255 1 Network 65,534 hosts/ntwk
  - Class C 192.168.0.0 – 192.168.255.255 254 Networks 254 hosts/ntwk

Configuring Addresses

- Network & Sharing Center
  - Change adapter settings, right click adapter → Properties
  - Set IP address, subnet address, default gateway and DNS server addresses

- Command Line
  - netsh interface ipv4 show interfaces
  - netsh interface ipv4 show ipaddresseses
  - netsh interface ipv4 set "local area connection" static 192.168.56.3 255.255.255.0 192.168.56.1

Automatic Private Internet Protocol Addressing (APIPA)

- Provides alternative configuration to DHCP for automatic IP addressing in small networks
  - 169.254.0.1 - 169.254.255.254
- Useful on small LAN or backup to DHCP
- Only communicates with other APIPA-enabled computers (not routable on Internet)

Configure IPv6 network settings

IPv6 Addressing

- 16 bit blocks (128 bits) with 4 digit hexadecimal number and each block is separated by a colon
- "Zero compression" – removing leading zeros; double colon indicates all zeros.
- Does not employ subnet masks
- Types
  - Unicast
    - Communication from device to device (host to host)
      - Global
        - 2000:: /3 (Equivalent to public IPv4 addresses)
      - Link-Local
        - fe80:: /64 (Equivalent to APIPA IPv4 addresses)
      - Unique Local
        - fc00:: /10 (Equivalent to private IPv4 addresses)
      - Loopback address
        - :1 (Equivalent to 127.0.0.1)
  - Multicast (one to many)
    - Represents one packet delivered to multiple devices
    - Begins with ff
  - Anycast (one to many)
    - Represents packets that are delivered to the nearest interface identified by the address
    - Utilized as a destination address assigned to routers
- Teredo Address
  - Tunneling communication enabling IPv6 connectivity between IPv4 nodes across NAT interfaces
  - 2001:: /32
- 6 to 4 Addresses
  - Two nodes running both IPv4 and IPv6 addresses across IPv4 routing infrastructure
  - 2002:

Configuring Addresses

- Network and Sharing Center
  - Change Adapter settings, right click adapter → Properties
  - Set IPv6 settings

        - IPv6 address, Default Gateway & DNS

    - Command Line
        - netsh interface ipv6 set address "local area connection" ::192.168.56.3
        - netsh interface ipv6 show addresses
        - netsh interface ipv6 show neighbors

Link-local Multicast Name Resolution (LLMNR)

- Capability of computers running IPv6 on local subnet to resolve each other's names without the need for a DNS server

Resolving connectivity issues (IPv4 & IPv6)

- Windows 7 Network Diagnostics
    - Network and Sharing Center → Troubleshoot problems
    - Local Area Connection Status dialog box

- TCP/IP utilities
    - Address Resolution Protocol
        - Resolves IP address to MAC addresses by creating an Address Resolution table in each host that transmits data on the network segment

    - FTP/TFTP
        - Not tools, used to see if data can move from one network segment to another

    - ipconfig
        - ipconfig /all
            - Comprehensive set of IPv4 and IPv6 data for all network adapters

        - ipconfig /release   /release6
            - Releases current DHCP lease on client computer

        - ipconfig /renew   /renew6
            - Renews current DHCP lease on client computer

        - ipconfig /displaydns
            - Displays content of DNS cache

        - ipconfig /flushdns
            - Flushes the content of DNS cache

        - ipconfig /registerdns
            - ***Renews all adapters DHCP leases*** and refreshes DNS configuration

        - ipconfig /showclassid *adapter*
            - Shows the DHCP class ID; use * for all adapters

        - ipconfig /setclassid *adapter*
            - Change the DHCP class I; use * for all adapters
    - nbtstat
        - Used on networks with NetBIOS over TCP/IP

    - netstat
        - Check the current status of computer's IP connection; look for services that are listening for incoming connections

    - nslookup
        - Name Server Lookup
        - Communicates with DNS server

    - ping
        - Packet InterNet Groper
        - Used for determining problem with connectivity
        - Echos →return acknowledgment

    - tracert
        - Trace Route
        - Used when you have a problem communicating with a particular host
        - Higher level of information than ping command

    - pathping
        - combines ping and tracert utilities into single command
        - tests connectivity to remote host and maps the route taken by packets

Suggested response to connectivity problem

- Verify hardware functioning
- Ipconfig /all to validate IP address, subnet mask, default gateway & DNS server, DHCP lease
- Ping 127.0.0.1 or ::1 (loopback) to validate TCP/IP is working
- Ping computers own IP address to eliminate duplicate
- Ping default gateway
- Ping a host that is not on network segment

<u>Configure networking settings</u>

Network Devices and Locations

- Control Panel → Network & Sharing Center
- Click active network icon to change type of network

Setup New Network Connection

- Network & Sharing Center
    - Change your networking settings
        - Set up a new connection or network
            - Connect to the Internet (ISP username and password)
            - Setup a new network (search for wireless router or access point)

        - Connect to a workplace (VPN)
        - Set up a dial-up connection

Connecting to Wireless Networks

- Wireless Local Area Network (WLAN)
- Wireless Access Point (WAP)
- Wired Equivalent Privacy (WEP)
- WiFi Protected Access (WPA/WPA2)

- Wireless Network Protocols
    - 802.11b
        - 2.4 GHz; used by many appliances
    - 802.11a
        - 5 GHz; reduces interference from appliances, has short signal range
    - 802.11g
        - 2.4 GHz; backward compatibility with 802.11b; better than 802.11b but suffers from same interference from appliances
    - 802.11n
        - 2.4 or 5 GHz; best signal range and most resistant to interference

Setup Wireless Network Connection

- Network & Sharing Center → Set up a new connection or network → Set up a new network
    - Network Name (SSID)
    - Security Type
        - None
        - WEP (Wired Equivalent Privacy)
        - WPA-Personal
            - Preshared passphrase or key
            - **TKIP is default encryption**
        - WPA2-Personal
            - Version 2 of WPA
            - Preshared passphrase or key
            - **AES is default encryption**
        - WPA-Enterprise
            - WPA using 802.1x authentication
            - **TKIP is default encryption**
        - WPA2-Enterprise
            - Version 2 of WPA
            - Highest level of security
            - **AES is default encryption**
        - 802.1x (authentication using WEP)

        - Encryption type
            - TKIP or AES
        - Security Key
            - Key required by security type
        - Start this connection automatically
        - Connect even when the network is not broadcasting

Internet Connection Sharing

- Begins simplified DHCP service with DNS forwarding and NAT service to rest of computers

Location Aware Printing

- Automatically print to a printer on a network your computer is connected to

- Devices and Printers → Manage default printers
    - Change my default printer when I change networks
        - Select Network and then select printer

Configure Windows Firewall

Basic Configuration

- No scope in settings, cannot set connection security rules

- Control Panel → Windows Firewall
    - Allow a program or feature through Windows Firewall
        - Select programs allowed/not allowed to communicate through firewall

    - Change notification settings
        - Change settings for Firewall profiles (Home/Work/Domain)
            - Block all incoming connections, including those in list of allowed programs
            - Notify me when Windows Firewall blocks a new program
            - Turn off Windows Firewall (not recommended)

    - Turn Windows Firewall on or off
        - Same screen as Change notification settings

    - Restore Defaults

    - Advanced Settings
        - Takes you to Windows Firewall with Advanced Security

Windows Firewall w/Advanced Security

- Can customize rules by program, port, pre-defined rules, protocols, scope, actions, profile
- Types of rules
    - Inbound Rules
    - Outbound Rules
    - Connection Security Rules
        - Connections between computers/secure tunnels

- Monitoring
    - Firewall
    - Active Connection Security Rules
    - Security Associations
        - Main mode
        - Quirks mode

- Configuring Multiple Firewall Profiles
    - Group of firewall rules that apply affected computers dependent on where the computer is connected
        - Domain profile
            - Connected to AD DS domain
        - Private profile
            - Home/Work
        - Public profile
            - Insecure public network, WiFi access point

- Create New Input or Outbound Rule (Wizard)
        - Program
        - Port
        - Predefined
            - List of predefined rules already in Windows Firewall
        - Custom

    - New Connection Security Rule Wizard
        - Isolation
            - Limit connection according to criteria you define
        - Authentication exemption
            - Enables specific computers to be exempt from authentication
        - Server-to-server
            - Secured connection between computers in two endpoints according to IP address ranges
        - Tunnel
            - Secure communication between 2 computers using IPSec tunnel mode
        - Custom

Configure remote management

Remote Management Methods

- Remote Assistance
  - Enables end-user to request assistance online and enables expert to offer assistance remotely.
  - Configure Windows Firewall to enable Remote Assistance or Remote Desktop
  - Control Panel → System → Remote Settings

  - Offering Remote Assistance
    - Invite someone you trust to help you
      - Save invitation as file
      - Use e-mail to send invitation (email with invitation attachment)
      - Use Easy Connect (password)

    - Help someone who has invited you
      - Use an invitation file
      - Use Easy Connect

- Remote Desktop
  - Uses Remote Desktop Protocol (RDP)
  - Any version of Windows can be a client, however only Professional, Enterprise or Ultimate can be a remote host (server)

  - Start → All Programs → Accessories → Remote Desktop Connection
    - Type computer/server name and connect
    - Configure options

  - Configuring Server Side (computer you are connection to)
    - Control Panel → System → Remote Tab
      - Don't allow connections to this computer
      - All connections to this computer running any version of Remote Desktop(less secure)
      - All connection only from computers running Remote Desktop with Network Level Authentication (more secure)
        - Select Users allowed to Access

- Windows Remote Management Service (WinRM)
  - Command line tools
  - Can configure with group policy
  - PowerShell
    - 240 cmdlets (command-lets)
      - Form of *verb-object* (e.g. Get-Process)
        - Get: retrieves data
        - Set: modifies output data
        - Format: formats data
        - Select: selects properties of an object or set of objects
        - Out: outputs data to location
      - Remote Command
        - icm computer-name {cmdlet}
          - icm server2 {get-process}

  - winrm quickconfig
    - Enables Windows Remote Management Service on computer to which you are making connection and configures firewall

  - winrs
    - Command line to run scripts/commands to remote computer
      - winrs –r:http://deathstar:5985 –u:star.wars/admin_bgroff "dir c:\"

CONFIGURING ACCESS TO RESOURCES (13 PERCENT)

<u>Configure shared resources</u>

Sharing

- Making resources available on the network
  - Public Folder Sharing (enable or disable public folders)
  - Standard Folder Sharing (use permissions to determine user access)

- Control Panel →Network & Sharing Center → Change advanced sharing settings
  - Network Discovery
  - File and Printer Sharing
  - Public Folder Sharing
  - Media Streaming
  - File Sharing Connections
  - Password Protected Sharing
  - HomeGroup Connections

Sharing Folders

- Basic Sharing
  - Right click folder → Share with…

- Advanced Sharing
  - Right click Folder → Properties
    - Sharing Tab → Advanced Sharing
      - Share This Folder (click to share)
      - Share Name
      - User Limit
      - Comment
      - Permissions (Shared Folder)
        - Add users or groups
          - Read
            - Users are allowed to view but not modify files
          - Change
            - Users are allowed to view and modify files but not change the attributes of the folder itself
          - Full Control
            - Users are allowed to perform any task on the folder or its constituent files, including modifying attributes and permissions
      - Caching

- Share via command line
    - net share
        - netshare downloads=c:\Users\Enterprise\Downloads /grant:admin_bgroff, full

- Central Share Management
    - Control Panel → Administrative Tools → Computer Management → Shared Folders → Shares

Folder Virtualization

- **Library**
    - Set of virtual folders that is shared by default with other users of the computer
        - Documents
        - Pictures
        - Music
        - Videos

    - Right click on Virtual Folder properties → Include a folder…

Sharing Printers

- Start → Devices and Printers → Printer Properties
    - Sharing Tab
        - Share This Printer

    - Security Tab
        - Set permissions for shared printers for users and groups
            - Print
                - Users can connect to printer and print documents and control print jobs for their documents only

            - Manage this printer
                - Users can assign forms to paper trays and set a separator page; change the print order of documents in queue; pause, resume and purge the printer; change printer properties; change printer permissions; can also do tasks for Manage Documents

            - Manage Documents
                - Users can pause, resume, restart and cancel all documents

            - Special Permissions
                - Enables assignment of granular permissions, read, change, take ownership
                - Advanced Button

HomeGroup

- Use for home or small office network
- Run on any edition, must have Home Premium, Professional or Ultimate to create a HomeGroup

- Control Panel → HomeGroup → Create a HomeGroup
    - Provides password for other computers to join HomeGroup

- Join Homegroup
    - Control Panel → HomeGroup → Join Now
        - Change advanced sharing settings to change sharing profile settings (file and printer sharing, public folder sharing, etc.)

Configure files and folder access

New Technology File System (NTFS) Permissions
- Secure and manage access to resources on both network and local level
- Applies to files and folders, shared or not shared
- Not available on FAT32 file systems

File and Folder Permissions
- Types of Permissions
    - **Read**
        - Display filenames, subfolder names, owner permissions and file attributes
        - Display data, file attributes, owner and permissions
    - **Read & Execute**
        - Runs files and display file attributes, owner and permissions
        - Run application files and display file attributes, owner & permissions
    - **Write**
        - Create new folders and files, change folder's attributes display owner and permissions
        - Write changes to file, change its attributes and display owner and permissions
        - Cannot delete files
    - **Modify**
        - Delete folders, grant read permission and list folder contents
        - Modify file's contents, delete files, perform actions allowed by Write and Read & Execute
    - **Full Control**
        - Change permissions, take ownership and delete subfolders and files
- Security Tab
    - Properties → Security
        - Edit Button
            - Add (add a user or group)
            - Remove (remove a user or group)

        - Set Permissions (allow or deny)

- NTFS Permissions Inheritance
    - All permissions are inherited, pass down through the folder hierarchy from parent to child
    - **Explicit denial of permission overrides any allowed permissions**

- Effective Permission Rules
    - If a user receives permission by virtue of membership in one or more **groups,** the *least restrictive* permission is the effective permission
        - If **Read** permission in user account and **Full Control** in a group/membership → **Full control is the effective permission**

        - If user is accessing **shared folder over network** and has shared folder and NTFS permissions applied, the *most restrictive* permission is the effective permission
            - If user has **Full Control** permission on a folder but accesses it across the network where he/she has **Read** permission → **Read is the effective permission**

        - If user is accessing shared folder on computer where it exists, shared permissions do not apply

        - **If user has denial of permission at shared folder or NTFS level, they are denied access to object regardless of any other permissions they have**

- Copying/Moving Permissions
    - Copying
        - When you copy a file or folder, it *inherits* the parent object/folder's permissions

    - Moving
        - **When you move a file or folder on same partition it retains its permissions**
        - When you move a file or folder from one partition to another, it *inherits* the destination's permissions

    - Moving or copying to FAT32, files or folders lose all their permissions

Data Encryption

- Encrypting File System (EFS)
    - *You can't compress and encrypt a file or folder at the same time*

    - Encrypt Files
        - File properties → General Tab → Advanced
            - Encrypt contents to secure data
                - File color changes to green

        - Certificate gets automatically generated

- Command Line
    - Cipher
        - /e - Specifies files and folders should be encrypted
        - /d - Specifies files and folders should be decrypted
        - /s:dir - Specifies that subfolders of target should also be encrypted
        - /I - Ignore errors
        - /h - Files with hidden attributes are omitted from display
        - /k - Creates new certificate file and certificate key
        - /r - Generates a recovery agent key and certificate
        - /x - Used to back up EFS certificate and key into specified filename

- EFS Recovery Agents
    - Create key for recovery agent with cipher
        - cipher /r:filename
            - .cer file (Certificate)
            - .pfx file (Private Key)

    - Default Recovery Agents
        - Local administration account
        - First domain administrator account
        - Can use group policy to assign specific agents

Configure User Account Control (UAC)

Administrator Token

- Only used when administrative privileges are required

Standard User Token

- Used for all actions that do not require administrative privileges

Tasks and Program Levels

- Low Integrity
    - Task or application less likely to compromise OS
- High Integrity
    - Action that performs tasks that have a higher potential for compromising the system

Elevated Privileges

- Shield icon next to tasks
- Receive a UAC prompt to continue
- Application Prompts
    - High-risk blocked program
        - Message box with red title bar and red shield, *"This program has been blocked for your protection"*

- Program Signed by Windows
  - Blue title bar and yellow shield

- Unsigned program from verified publisher
  - Includes name and publisher; legitimate digital signature

- Unsigned program from non-verified publisher
  - No digital signature, yellow title bar and yellow shield

Run program as administrator

- Right click program and select run as administrator

Configuring User Account Control

- Control Panel → System & Security → Change User Account Control Settings
- Control Panel → User Accounts → Change User Account Control Settings
  - Always notify me
  - Notify me only when programs try to make changes to my computer (Default)
  - Notify me when programs try to make changes to my computer (do not dim my desktop)
  - Never notify me

User Account Control Policies

- Group policy provides polices to govern UAC behavior
  - Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
  - Control Panel → Administrative Tools →Local Security Policy → Security Options
    - Admin Approval Mode for the Built-in Administrator Account
    - Allow UIAccess applications to prompt for elevation without using secure desktop (dimmed)
    - Behavior of 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 executables that are signed and validated
    - Only elevate UIAccess applications that are installed in secure locations
    - Run all administrators in Admin Approval Mode
    - Switch to secure desktop when prompting for elevation
    - Virtualize file and registry write failures to per user locations

<u>Configure authentication and authorization</u>

Authentication

- Process of user or computer proving its identity

- Types
  - Kerberos version 5

        - NTLM (NT Lan Manager)
            - Challenge question and response
        - Certificates
            - Public and private keys

        - Smart Cards
            - Multifactor identification
        - Biometric
            - Finger/eye scanners

Authorization

- Process of the system giving appropriate resource access to user who has been authenticated by using permissions, policies and rights

- Built In Groups
    - Administrators
    - Backup Operators
    - Event Log Readers
    - Network Configuration Operators
    - Remote Desktop Users
    - Power User
    - Users
    - Guests

    - When a user logs in locally, they are part of the following groups:
        - Users
        - Authenticated Users
        - Everyone
        - Interactive

User rights

- Control the use of the operation system for users
    - Configure with Group Policy
        - Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignments

Managing Credentials

- Control Panel → Credential Manager
        - Stores in electronic Windows Vault
        - Add, backup and restore credentials

Managing Certificates

- Personal store of Certificate Manager
    - Smart Cards & EFS creates certificates that are stored in personal store
    - Access by typing certmgr.msc
        - Double click to view certificate details
        - Right click properties for more details

Smart Cards

- Supports multi-factor identification
    - Smartcard
    - Pin/Password
    - Biometric

- Smartcards with PIV (personal identification verification)

- Use Group Policy to configure smart card policies
    - Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
        - Interactive logon: Require smart card
        - Interactive logon: Smart card removal behavior

Password Policies

- Enforce password history
    - Number of passwords remembered for each user

- Maximum password age
    - Number of days a user can use a password before being required to change; 42 days default

- Minimum password age
    - Minimum number of days password must be used before it can be changed; at least one day, less than maximum password age

- Minimum password length
    - Minimum number of characters that can make up a password

- Password must meet complexity requirements
    - Cannot contain user account name or full parts of the name that exceeds two consecutive characters, 3 of 4: lowercase, uppercase, numerals, non-alphanumeric

- Store passwords using reverse encryption
    - Level of encryption for storing passwords
    - Least secure method

Resolving Authentication Issues

- Resetting passwords
    - Local Users and Groups → Users → Set Password
        - User must change password at next logon

- Create Password Reset Disk
    - Control Panel → User Accounts → Create Password Reset Disk

Configure BranchCache

Hosted Mode

- Server located at every remote location
- Each server hosts files cached from main office server

- Infrastructure requirements
  - Windows Server 2008 R2
  - SSL Certificates
    - Import certificates under local computer accounts so client computers can trust server

Distributed Mode

- Each user's Windows 7 desktop computer hosts files cached from main office server
- Only 1 server in this mode
- Single subnet with no more than 50 computers
- Infrastructure requirements same as Hosted Mode

Enabling BranchCache

- Turn on with Group Policy
  - Computer Configuration\Administrative Templates\Network\BranchCache
    - Turn on BranchCache
    - Set BranchCache Distributed Cache Mode
    - Set BranchCache Hosted Cache Mode
    - Configure BranchCache for network files
    - Set percentage of disk space used for client computer cache

- Need to have PeerDistSvc running

Configure Firewall

- Both modes require TCP Port 80 (inbound and outbound)
- Distributed Mode
  - UDP Port 3702 (inbound and outbound)
- Hosted Mode
  - Port 43 (outbound)

Network Requirements

- Infrastructure requirements are significantly reduced when BranchCache is enabled.
  - BranchCache server sends requested file in 64KB blocks with metadata

  - When client computer requests file, BranchCache resends metadata and the client computer compares the two sets of metadata to determine whether the contents of the requested file have changed. The server resends the file only if changes have occurred.

  - Metadata is 2,000 times smaller than file size, bandwidth requirements are reduced by a factor of 2,000 when BranchCache is enabled.

CONFIGURE MOBILE COMPUTING (10 PERCENT)

Configure BitLocker and BitLocker To Go

BitLocker Drive Encryption

- Uses Trusted Platform Module (TPM) to provide secure protection of encryption keys and checking of key components when Windows is booting. TPM is a microchip inside computer used to store cryptographic information (keys)

- Requirements
  - Windows 7 Enterprise or Ultimate
  - 100MB System Partition
  - TPM 1.2 or higher

BitLocker Modes

- TPM only
- TPM and PIN
- TPM and USB startup key
- Without TPM (USB Key)
- TPM with USB and PIN (most secure)

Enabling BitLocker

- Control Panel → BitLocker Drive Encryption
  - Turn On BitLocker
    - Use BitLocker without additional keys
    - Require PIN at every startup
    - Require a startup key at every startup
    - Save to USB, file or print recovery key
  - Turn Off BitLocker
  - Suspend Protection
  - Manage BitLocker
    - Resave or print the recovery key
  - TPM Administration

BitLocker To Go

- Extends volume encryption to USB and Portable hard drives regardless of format
- Does not require TPM
- Need Windows 7 Enterprise or Ultimate and can be read on any edition of Windows 7
- Access data by using password or smartcard

- Control Panel → BitLocker Drive Encryption
  - BitLocker To Go
    - Turn on BitLocker
      - Password or Smartcard
      - Recovery Key

BitLocker Group Policies

- Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption
    - Store BitLocker recovery information in Active Directory Domain Services
    - Chose default folder for recovery password
    - Choose how users can recover BitLocker protected drives
    - Choose drive encryption method and cipher strength
    - Provide the unique identifiers for your organization

- Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives
    - Require additional authentication at startup
    - Require additional authentication at startup (Server 2008 and Vista)
    - Allow enhanced PIN's for startup
    - Configure minimum PIN length for startup
    - Chose how BitLocker protected operating system drive can be recovered
        - Allow data recovery agent
        - 48 digit recovery password
        - 256 Bit recovery key
        - Omit recovery options from BitLocker setup wizard
        - Save BitLocker recovery information to AD DS for operating system drives
        - Configure storage of BitLocker recovery information to AD DS
        - Do not enable BitLocker until recovery of information is stored to AD DS for operating system drives

- Data Recovery Agents
    - Computer Configuration\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption
        - Add Data Recovery Agent
            - Locate/Import DRA certificate

<u>Configure Direct Access</u>

Direct Access

- Directly connect to corporate networks from any internet connection
- Uses IPv6 with IPSec (with our without VPN)
- Requires Windows 7 Enterprise or Ultimate

Network Infrastructure Requirements

- Windows Server 2008 R2 (Must be a domain member server)
    - Also needs at least one domain controller and DNS Server running 2008 SP2 or 2008 R2
- 2 Network Interface Cards
    - One connected to the network and one to the Internet
    - Network adapter connected to Internet needs two consecutive IPv4 public addresses

- Windows Certificate Authority Server
    - Client computers need certificates in order to trust

Connection Options

- Type of IP Address
    - **Globally Routable IPv6 address**
        - Connects with Globally Routable IPv6 address
    - **Public IPv4 address**
        - Connect with 6-to-4
    - **Private (NAT) IPv4 address**
        - Connects with Teredo
    - **Unable to connect using above methods**
        - Connects with IP-HTTPS

Configuring Clients

- Computers must be joined to AD DS domain and belong to security group that has access to DirectAccess server

- Group Policy Settings
    - Computer Configuration\Windows Settings\Name Resolution Policy
        - DNS Settings for Direct Access
            - Use IPSec to communicate between DNS client and DNS server

- Authentication
    - DirectAccess authenticates computer before user logs on with the aid of client computer and server certificates. Provides access to DNS servers and domain controllers so the user can logon with their username and password and authenticate to AD DS
    - 2 Factor authentication – smart card with username and password

<u>Configure mobility options</u>

Offline Files

- Enables user to access and work with files and folders stored on network shares when the user is disconnected from that share
- Stored in local cache
- Need to configure both client and server

- Configuration
    - Right click file/folder and select 'Always available offline'

- Control Panel → Sync Center
    - View sync partnerships
    - View sync conflicts
    - View sync results
    - Manage offline files
        - General
            - Disable offline files
            - Open Sync Center
            - View your offline files
        - Disk Usage
            - Change Limits
            - Delete Temporary Files
        - Encryption
            - Encrypt (EFS)
        - Network
            - How often to check for slow link
            - Default is 5 minutes

- Group Policies
    - Computer Configuration\Administrative Templates\Network\Offline Files
        - Administratively assigned offline files (Universal Naming Convention path)
        - Configure Background Sync
        - Limit disk space used by offline files
        - Allow or Disallow use of the Offline Files feature
        - Encrypt the Offline Files cache
        - Exclude files from being cached
        - Enable Transparent Caching
            - Enables client computer to temporarily cache files obtained across a slow WAN link more aggressively, reducing the number of times client might have to retrieve file
            - Set latency value
        - Configure slow-link mode
            - Latency
        - Configure slow link speed
            - Set a value when slow link mode will be used

Power Options

- Modes
    - Sleep Mode
        - Hard disk, monitor, CPU shutdown
        - RAM, mouse and keyboard still powered

    - Hybrid Sleep
        - RAM saved to hard disk
        - Enters sleep mode

    - Hibernate
        - RAM saved to hard disk
        - Computer shutdown, no power consumption

- Power Plans
    - Balanced
        - Battery – display 5 minutes, sleep 15 minutes, display dims
        - AC Outlet – display 20 minutes, sleep 1 hour, display full brightness

    - Power Saver
        - Battery – display 3 minutes, sleep 15 minutes, display dims
        - AC Outlet – display 20 minutes, sleep 1 hour, full brightness

    - High Performance
        - Battery – display 20 minutes, sleep 1 hour, full brightness
        - AC Outlet – display 20 minutes, no sleep, full brightness

- Advanced Power Settings
    - Change advanced power settings
        - Hard disk
        - Desktop background settings
        - Wireless adapter settings
        - Sleep
        - USB Settings
        - Power buttons and lid
        - PCI Express
        - Processor power management
        - Display
        - Multimedia settings
        - Battery

- Other Options
    - Choose what the power buttons does

- Command Line
    - powercfg

- Group Policies
    - Computer Configuration\Administrative Templates\System\Power Management

Configure remote connections

Authentication Protocols for Remote Access (VPN)

- **PAP** (Password Authentication Protocol)
  - Client submits a clear text(unencrypted) user identification and password to server
  - One way authentication
  - Least secure method

- **CHAP** (Challenge Handshake Authentication Protocol)
  - One way authentication
  - Client requests access, server sends a challenge to client via a MD5 hash value

- **MS-CHAP2** (Microsoft Challenge Handshake Authentication Protocol version 2)
  - Client and server must be Windows based
  - Does not work with LAN manager
  - Two-way authentication

- **EAP** (Extensible Authentication Protocol)
  - Used with MD5 hash challenge, smart cards and certificate authentication in Windows 7

- **PEAP/PEAP-TLS** (Protected Extensible Authentication Protocol with Transport Layer Security)
  - Highly secure password based authentication protocol using certificate based authentication
  - Requires computer certificate on VPN server

VPN Protocols

- Data encryption, data integrity and data authentication

- **PPP** (Point to Point Protocol)
  - Dial up protocol supporting multiple network protocols

- **PPTP** (Point to Point Tunneling Protocol)
  - Used to transmit private network data across public network securely
  - Least secure, no data integrity or authentication
  - Port 1723

- **L2TP/IPSec** (Layer 2 Tunneling Protocol with IP security)
  - Used to transmit private network data across public network
  - Supports multiple networking protocols
  - Port 1701, UDP port 500

- **SSTP** (Secure Socket Tunneling Protocol)
  - Uses Secure Hypertext Transfer Protocol (HTTPS) over TCP port 443 to transmit across firewalls and proxy servers
  - Uses Secure Sockets Layer (SSL)
  - Newest technology
  - Also used on Server 2008
  - Does not work through proxies

- **IKEv2** (Internet Key Exchange version 2)
    - Uses IPSec Tunnel mode over port 500
    - Supports strong authentication and encryption methods
        - PEAP, EAP-MSCHAPv2
        - Cannot use PAP, CHAP or MSCHAPv2

Establishing VPN connections and authentication

- VPN server sits between private network and internet
- Connect using TCP/IP
- Uses PPTP or L2TP protocols to encapsulate data
- After data is received encapsulated headers and footers are stripped off

VPN reconnect

- Uses IKEv2 to automatically re-establish VPN connection when user temporarily loses their Internet connection
- Can be used up to 8 hours after connection was lost

Network Access Protection (NAP)

- Available in Professional, Enterprise & Ultimate
- Addresses antivirus and antispyware, Windows Firewall, automatic updating, security updates, software updates

- NAP Remediation
    - Goes to Remediation Network to address issues
    - If no Remediation Network, it's up to user to configure & fix
    - Enforcement options
        - No enforcement
        - IPSec
        - 802.1x
        - Terminal Services Gateway
        - VPN
        - DHCP
        - DirectAccess

- Security Auditing
    - Audit Logon Events to see who's logging onto the network
    - Group Policy
        - Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit Logon Events

Remote Desktop Gateway Server

- Having many users connect simultaneously to remote machine
- Enable in Group Policy
    - User Configuration\Administrative Templates\Windows Components\Remote Desktop Service\RD Gateway
- Use RemoteApp to run program from a local machine

MONITORING AND MAINTAINING SYSTEMS THAT RUN WINDOWS (11 PERCENT)

Configure updates to Windows 7

Type of Updates

- Important Updates
  - Critical Security Updates - "Patch Tuesdays"

- Recommended Updates
  - OS and application updates

- Optional Updates
  - Not security related, software and driver updates, language packs, etc.

- Update roll-ups
  - Fix problems with specific Windows components or software packages
  - Service packs
    - Comprehensive OS updates that package together all updates since launch of OS

Configuring Windows Updates

- Control Panel → Windows Update → Check for updates
  - Change Settings
    - Install updates automatically (recommended)
    - Download updates but let me choose whether to install them
    - Check for updates but let me choose whether to download them and install them
    - Never check for updates (not recommended)
    - Give me recommended updates the same way I receive important updates
    - Allow all users to install updates on this computer

  - Hide Updates
    - Right click on an update and select hide
    - Standard users cannot hide updates
    - Restore Hidden Updates to view
    - Updates may be hidden if user requests Windows not to notify or install updates automatically

  - View Update History
    - See a list of all installed updates and their status

  - Uninstall an Update
    - Control Panel → Programs and Features →View Installed Updates
      - Right click, Uninstall

- WSUS Server
    - Server-based component enabling you to provide update services to computer on corporate network without the need to go on each computer and update

- Windows Update Standalone Installer
    - wusa.exe
        - Manual installation of Microsoft Update files (.msu)
        - wusa.exe d:\windows6.1-kb7564321-x64.msu /quiet /norestart

Configuring Windows Update Policies

- Group Policy
    - Computer Configuration\Administrative Templates\Windows Components\Windows Update
        - Configure Automatic Updates
            - 2-Notify for downloading any updates and notify again before installing them
            - 3-Download the updates automatically and notify when they are ready to be installed
            - 4-Automatically download updates and install them on the schedule specified below
            - 5-Allow local administrators to select the configuration mode that Automatic Updates should notify and install updates

        - Specify Intranet Microsoft Update Service Location
            - Specifies name of WSUS server from which client gets their updates

<u>Manage Disks</u>

Disk Management

- Start → Computer → Manage → Disk Management
    - Create Dynamic Disks
    - Create Volumes
    - Extend Volumes
    - Shrink Volumes
    - Display Properties of Disks and Volumes

Partition Styles

- Master Boot Record (MBR)
    - Partition table that describes location of partitions on disk
    - Supports volumes up to 2TB
    - 4 primary partitions or 3 primary and one extended partition

- GUID Partition Table (GPT)
    - Disks larger than 2TB; Max 256TB
    - No backwards compatibility with older operating systems

Types of Disks

- Basic Disk
  - MBR Partition
  - Hard disk on which you install Windows
  - Primary and extended partitions; logical drives

- Dynamic Disk
  - GPT Partition
  - Logical Disk Managment (LDM)
    - Database that is replicated to other disks
  - Create specialized volumes
    - Spanned
    - Striped (RAID-0)
    - Mirrored (RAID-1)
    - Striped with Parity (RAID-5)
  - Unlimited number of volumes

Dynamic Volume Types

- Simple
  - A single region of free space on single disk
  - No fault tolerance

- Spanned
  - Spans across 2-32 disks, enabling you to add space without new drive letter
  - No fault tolerance

- Striped (RAID-0)
  - Multiple regions of free space from 2-32 separate hard disks
  - Data is evenly interleaved across disks in stripes
  - Improvement in read/write performance
  - No fault tolerance, if one disk is lost entire volume is lost

- Mirrored (RAID-1)
  - Data on one disk is replicated on the second disk
  - Cannot be extended
  - Fault tolerance equal to maximum capacity of smallest disk
  - Used for data recovery

- Striping with Parity (RAID-5)
  - Minimum number of disks is 3
  - Data is interleaved equally across disks with parity stripe of data also interleaved across the disks. Parity stripe rotates from one disk to next as each stripe is written
  - Fault tolerance with maximum capacity of the number of disks minus 1 (five 200GB disks, volume would be 800GB, 1,000GB total – 200GB)
  - Data recovery
  - No Windows 7 support

Managing File Systems

- Disk Defragmenter
  - All Programs → Accessories → System Tools → Disk Defragmenter
  - Right click on drive → Properties → Tools
    - Schedule Defragmentation
    - Analyze Disk
    - Perform an on-demand defragmentation

  - Command Line
    - defrag
      - volume drive letter
      - /b optimize boot file
      - /c defrag all local volumes
      - /e defrag all local volumes except those specified
      - /a analyze the volume and display report; do not defrag
      - /x perform free space consolidation
      - /t track a defrag already in process
      - /h run defrag at normal priority
      - /m defrag multiple volumes simultaneously
      - /u print the defrag process on screen
      - /v verbose mode

- Caching
  - Hard Drive
    - Right click on Volume → Properties → Hardware → Select Properties → Change Settings
      - Policies Tab
        - Enable write caching on the device
  - USB
    - Right click on Volume → Properties → Hardware → Select Properties
      - Policies Tab
        - Quick removal (default)
          - Can eject without using Safely Remove Hardware
          - No caching
        - Better performance
          - Enables write cache on USB device
          - Eject with Safely Remove Hardware

- Disk Cleanup
  - Right click on Volume → Properties → Disk Cleanup
    - Select files to delete
    - Clean Up System Files to scan again and add more files (Admins only)

- Error Checking
    - Right click on Volume → Properties → Tools
    - Check for disk errors
        - If disk in use, schedule check next time computer boots up

Removable Device Policies
- Group policy or Local Group Policy Editor
    - Computer Configuration\Administrative Templates\System\Removable Storage Access

Ready Boost
- Allows flash memory devices to be used as additional memory cache
- Requirements
    - At least 256MB storage capacity
    - USB 2.0
    - Must support a throughput of 2.5MB/sec for 4K and 1.75MB/sec for 512K

ReadyDrive
- Need hybrid hard disks to use

Monitor Systems

Configuring Event Logs
- Start → Computer → Manage
- Control Panel → Administrative Tools
    - Event Viewer
        - Application
            - Logs events related to applications running on the computer
        - Security
            - Logs events related to security related actions
        - Setup
            - Logs events related to setup of applications
        - System
            - Contains events related to actions taking place on the computer in general, including hardware events
        - Forwarded events
            - Contains events logged from remote computers
        - Applications and Service logs
            - Stores events from single applications or components, as opposed to system wide events

- Create Custom View
    - Logged
    - Event Level
    - By log
    - By source
    - Task category
    - Keywords
    - User and Computer(s)
    - XML tab

Events Forwarding

- Terms
    - ***Source Computer***
        - Computer(s) configured to forward events
    - ***Collector Computer***
        - Computer configured to receive these events

- Event Log Subscriptions
    - **Collector-initiated**
        - Collector computer gathers the specified events from each of the source computers
        - Good for smaller environments

        - Source Computer(s):
            - Run winrm quickconfig
            - Add ***collector computer*** to Event Log Readers group

        - Collector Computer:
            - Run wecutil quick-config

            - Create Subscription
                - Subscription Name
                - Destination Log
                    - Forwarded Events
                - Subscription type and source computers
                    - Collector Initiated
                        - Select Computers (source computers)
                - Events to collect
                    - Select Events → Edit
                - Advanced

    - **Source-initiated**
        - Each source computer pushes the specified events to the collector computer
        - Good for large environments

- Collector Computer:
    - Run winrm quickconfig
    - Run wecutil quick-config

    - Create Subscription
        - Subscription Name
        - Destination Log
            - Forwarded Events
        - Subscription type and source computers
            - Source computer initiated
                - Select Computer Groups
                - Add Certificates
        - Events to collect
            - Select Events → Edit
        - Advanced

- Source Computer(s):
    - Run winrm quickconfig

    - Edit Group Policy
        - Computer Configuration\Administrative Tools\Windows Components\Event Forwarding
            - Configure the server address

<u>Configure Performance Settings</u>

Reliability Monitor

- Analysis of computer's stability over time (days, weeks)
- Types of Events
    - Application Failures
    - Windows Failures
    - Miscellaneous Failures
        - Improper shutdowns, sleep failures
    - Warnings
    - Informational Events
        - Which programs have been installed
        - Hardware failures

Resource Monitor

- Provides summary of CPU, disk, network and memory performance statistics
- Includes mini graphs
- Tabs
    - CPU
        - Number of threads per application, CPU cycles used by applications
    - Memory
        - hard faults/sec and memory usage

- Disk
    - File being read/written by each application, current read write speeds (bytes/minute), total disk I/O
- Network
    - IP address of computer, amount of data(bandwith) in bytes/second

Performance Monitor

- View Performance Data real-time or from a log file

- Data Collector Sets
    - Set of performance object and counters that enables you to log computer performance over time (60 seconds is default) while performing other tasks
    - Create a performance baseline

    - Default Collector Sets
        - System Diagnostics
        - System Performance
            - Right click Data Collector Set → Start
    - Reports to view results

- Optimizing and Troubleshooting Memory
    - Memory Counters
        - Pages/sec
            - Rate at which data is read to or written to
            - Value of 20 or more indicates shortage of RAM

        - Available Bytes/Available MBytes
            - Physical memory available
            - Below 4MB indicates shortage of available memory

        - Committed Bytes
            - Virtual memory committed to physical RAM or running process
            - If exceeds RAM, might need to add more RAM

        - Pool Nonpaged
            - Amount of RAM in nonpaged pool system
            - If steady increase without increase in computer activity, check for leaks

        - Page faults/sec
            - Number of data pages that must be read from or written to page file per second
            - High value indicates lot of paging activity, add more RAM

- Optimizing Processor Utilization
    - Processor Counters
        - % Processor Time
            - Percentage of time the processor is executing meaningful actions
            - If > 85% could be bottleneck, check memory counters and RAM or consider faster processor

        - Interrupts/sec
            - Rate of service requests from I/O devices that interrupt other processor activities
            - Significant increase without increase in system activity might indicate hardware failure

Virtual Memory

- Control Panel → System → Advanced System Settings →Performance → Settings
    - Change Virtual Memory Under Advanced Tab
        - Uncheck **Automatically manage paging files for all drives**
            - Set the size of paging file on hard drive used for RAM
- Paging File
    - C:\pagefile.sys
        - Hidden & System File, uncheck both options in Folder Options to view

System Configuration Utility

- Msconfig
    - General
        - Loan system services
        - Load startup times
        - Use original boot configuration
    - Boot
        - Safe boot
        - No GUI boot
        - Boot log
        - Base video
        - OS boot information
    - Services
        - All services available on the computer
    - Startup
        - All applications configured to start automatically
    - Tools
        - Start diagnostic applications

Configuring Processor Scheduling

- Task Manager
    - Processor Affinity
        - Which processor a given process will execute
        - Distribute processes/activity evenly across more than one processor

CONFIGURING BACKUP AND RECOVERY OPTIONS (11 PERCENT)

Configure backup

Windows Backup

- Control Panel → Backup and Restore
  - Setup Backup
    - Select Location for backup
    - What do you want to backup?
      - Let Windows choose
      - Let me choose
        - Data Files
        - Computer
      - Include a system image of drives
    - Change Schedule
  - Back up now
    - Performs incremental backup of files/folders according to settings configured in Backup and Restore wizard.
    - Only backups files that have changed (incremental)
  - Manage Space
    - Summary of space used by backups
    - View backups
      - Delete older ones no longer needed
    - System Images
      - Change Settings
        - Let Windows manage the space used for backup
        - Keep only the latest system image and minimize space used by backup
  - Change settings
    - Where do you want to save your backup
    - Let Windows Choose
      - Set backup schedule with this option
    - Let Me Choose
  - Restore
    - Restore My Files
      - Browse for files to restore
    - Restore All Users Files
    - Select another backup to restore from
    - Recover system settings or your computer
      - Opens System Restore option

    - Create a system image
        - Manually run a system backup
        - Where to store the image (network, HD, DVD's)

    - Create a system repair disk
        - Contains tools to recover a Windows system that is having problems
        - Needs to be stored on an optic disk (DVD)

- When problem occurs Windows provides troubleshooting options
    - Manage backup disk space
    - Change backup settings
    - Try to run backup again

- Command prompt
    - wbadmin start backup –backuptarget: *targetdrive:* - include: *sourcedrive:*
        - Start backup
        - Stop job
        - Get versions
        - Get items
        - Get status

<u>Configure system recovery options</u>

System Restore

- Recover from problems with improper system settings, faulty drivers or incompatible applications

- Restore Point
    - Creates snapshot of the system
    - Used to restore the system state and changes to documents
    - Contains registry, system files, program files
    - Created at startup, midday or during significant OS changes
        - Driver and application installations, etc.

- Computer → Properties → System Protection
- Control Panel → System → System Protection
    - System Restore
        - Restore system files and settings from a previous restore point

    - Protection Settings
        - Configure
            - Restore system settings and previous versions of files
            - Only restore previous versions of files
            - Turn off system protection
            - Change disk space usage
            - Delete restore points
    - Create Restore Point

Advanced Recovery Methods

- Control Panel → Recovery → Advanced Recovery Methods
    - Use a system image you created to recover your computer
    - Reinstall Windows

System Repair Disk

- Also available on DVD Installation Disk → Repair My Computer Option at Welcome Screenc
- Attempts to automatically recover a computer that will not start normally
- Restore a computer using a system image

    - Recovery Tools
        - Startup Repair
        - System Restore
            - Restore system to earlier restore point
        - System Image Recovery
        - Windows Memory Diagnostic
        - Command Prompt

    - Restore your computer using a system image
        - Select a system image backup

Advanced System Startup Options

- F8 during boot process
    - Repair Your Computer

    - Safe Mode (minimal set of drivers)
        - Computer stops responding or runs slowly
        - Computer display is blank or distorted
        - Computer fails to respond after new hardware/software installed
    - Safe Mode with Networking
    - Safe Mode with Command Prompt
    - Enable Boot Logging
        - ntbtlog.txt
    - Enable Low Resolution Video (640x480)

    - **Last Known Good Configuration (advanced)**
        - Configuration is store in registry
            - HKLM\System\CurrentControlSet
        - Updates after every successful login

    - Debugging Mode
    - Disable Automatic Restart on System Failure
    - Disable Driver Signature Enforcement
    - Start Windows Normally

Configure file recovery options

Restoring Files and Folders

- Windows Backup
  - Restore
    - Restore my files
    - Choose a different date
      - Used to restore file to an earlier version
    - Restore all users' files
    - Select another backup to restore files from

- Previous Versions
  - Formerly known as Shadow Copies
  - Available in Professional, Enterprise and Ultimate
  - Created when a restore point is created
  - Must start Volume Shadow Copy
    - Default is set for manual
  - No setting for keep only last shadow copy setting

  - Revert to previous versions
    - Right click file → File Properties → Restore Previous Versions
      - Open (view file)
      - Copy (copy to a location)
      - Restore

OTHER

- Active directory takes precedence of any local policies
- Computer configuration policies take precedence over any user configurations

Steps to Deploy Windows Manually:

1) Build Answer File
    - Save and validate

2) Install Windows 7 from DVD w/Answer File
    - Add drivers, applications, etc

3) Run Sysprep to prepare installation for images
    - /generalize – removes out of box device drivers
        - To keep drivers set *PersistAllDeviceInstalls* in the Microsoft-Windows-PnpSysprep component to **True** in the answer file

4) Create Bootable Windows PE Image with ImageX

5) Boot into Windows PE on the reference computer
    - Capture image with ImageX to Network Share

6) Boot into Windows PE on destination computer
    - Format hard drive with Diskpart
    - Copy Image from Network Share
    - Apply Image with ImageX
    - Copy boot files using BCDboot.exe

Windows Deployment Services (Server 2008 R2)

- Enable role on server
- Configure WDS
- Add Windows Image & Boot Image
- Connect client computers using PXE capable network card to WDS and install

BCD Edit Commands

- /createstore	Creates a new empty boot configuration data store
- /export	Exports the content of the system store in a file
- /import	Restores the state of the system store by using file from export
- /store	Specifies the store to be used
- /copy	Makes a copy of the specified boot entry
- /set	Sets an entry option value
- /default	Specifies the default entry for boot options
- /displayorder	Specifies the display order for boot options
- /timeout	Specifies the time to wait, in seconds before default is selected

- More information
    - Complete descriptions of all commands
        - http://www.omnisecu.com/windows-2008/introduction-to-windows-2008-server/boot-configuration-data-store-editor-bcdedit-options.htm
    - How to use BCDEdit
        - http://www.sevenforums.com/tutorials/2676-bcdedit-how-use.html

IPv4 Subnet Explanation

- Great reference, easy to understand!
- http://www.pantz.org/software/tcpip/subnetchart.html