Chapter 1 Lesson 1

Reliability Monitor tracks the following five events:

- Application Failures
- Windows Failures
- Miscellaneous Failures
- Warnings
- Information

Reliability Monitor collects information about software failures

Startup Repair runs the following tests:

- Check for updates
- System Disk test
- Disk failure diagnosis
- Disk metadata test
- Target OS test
- Volume content test
- Boot manager diagnosis
- System boot log diagnosis
- Event log diagnosis
- Internal state check
- Boot status test

Windows Memory Diagnostic

- Includes 3 types of tests:
    - Basic – Performs only 3 types of tests
    - Standard – Default Level – Performs 8 types of tests
    - Extended - Performs 17 types of tests
- All tests are performed twice by default
- You can also choose to test the Cache or not test the cache
- Mdsched
- Can be started from Windows Boot Manager by repeatedly tapping the space bar at startup

Chkdsk

- /f –Fixes errors on the disk
- /V – Displays the full path and name of every file on Fat/Fat32 volumes
- /R – Locates bad sectors and recovers readable information (implies /f)
- /L:size – Changes the log file size to the specified number in kilobytes
- /X – Forces the volume to dismount first if necessary
- /I – NTFS only. Performs a less vigorous check of index entries.
- /C – NTFS only. Skips checking of cycles within the folder structure.
- /B – NTFS only. Re-evaluates bad clusters on the volume (implies /R)

Disk Defragmenter:

- Runs automatically every Wednesday at 1 a.m. by default.
- If the amount of fragmented files is above 10%, you should defragment the disk.

Chapter 1 Lesson 2

The Windows Boot Process:

- Power on: The power supply feeds power to components
- Perform instructions contained in BIOS: Once the CPU has power, it starts executing instructions in the BIOS. The instructions in the BIOS consist of 2 steps:
    - POST – Check hardware (Beep codes)
    - Read instructions on the boot device
- Operating System loads from Boot device

Chapter 2 Lesson 1

IPConfig:

- Ipconfig /release – Ipconfig /renew
- Ipconfig /release6 – Ipconfig /renew6

Ping

- If latency is > 1 second, network communications probably seem slow

PathPing

- A routing loop is when traffic crosses the same router more than once
- Lists every router between you and the destination
- Like tracert, but better
- Routers handle ICMP requests at lower priority than other packets, so a high latency isn't always indicative of a problem when pinging
- Using the "-d" option prevents pathping from resolving names of each router

PortQry

- Tests whether a specific network service is running on a computer and the state of the port
- Basic syntax is as follows:
    - Portqry –n "destination" –e "portnumber"
- You can also use the telnet client to test a remote service on a TCP host

NSLookup

- Some names resolve to multiple IP addresses, this is normal. Your browser is smart enough to connect to a different IP address if the first address isn't working properly.

Chapter 2 Lesson 2

Name Resolution

- IPconfig /displaydns
    - The ttl is the time that the record will remain valid
- IPconfig /flushdns deletes all entries from the DNS cache
- To disable the DNS cache, stop the DNS client service form the Services app or run the following command from an admin command prompt: net stop dnscache
    - Stopping and restarting the dns client also clears the DNS cache

Chapter 2 Lesson 3

The WLAN Autoconfig service must be started for wireless networks to be available.

Turning off SSID broadcasting is actually dangerous, because the client is constantly sending out beacons looking for the WAP. These beacons can be intercepted by malicious parties.

Connecting to Wireless networks using Group Policy

- You should have Windows Server 2003 with SP1 or later installed on your domain controllers.
    - You need to extend the AD DS schema for servers prior to Windows Server 2008 using the 802.11Schema.ldf file. To extend the schema, follow these steps:
        - Copy the 802.11Schema.ldf file to a folder on a DC.
        - Log on to the DC as a domain admin
        - Select the folder containing the 802.11Schema.ldf file, and run the following command:
            - ldifde -i -v -k -f 802.11Schema.ldf -c DC=X *Dist_Name_of_AD_Domain*
        - Restart the DC
- You can configure a wireless network policy from Computer Configuration/Policies/Windows Settings/Security Settings/802.11

Before you can connect to a wireless network using NETSH, you must have a profile saved for that network.

- Use this command to view wireless networks:
    - Netsh wlan show networks
- Use this command to export a wireless profile
    - Netsh wlan export profile name=" "
- Use this command to create a wireless profile
    - Netsh wlan add profile filename="C:\profiles\exampleprofile.xml"
- To connect to a wireless network, use this command:
    - Netsh wlan connect "wireless profile name"
        - You can also specify the interface at the end of this command
- Use this command to disconnect from a wireless network:
    - Netsh wlan disconnect
- Use this command to allow access to a wireless network:
    - Netsh wlan add filter permission=allow ssid=" "
- Use this command to block access to a wireless network:
    - Netsh wlan add filter permission=block ssid=" "

Using Event Viewer to analyze wireless connection problems

- Open Event Viewer and go to Applications and Services\Microsoft\Windows\WLAN-Autoconfig. Then select operational.
- Event ID 11006 Indicates an authentication failure

Chapter 3 Lesson 1

- Monitoring Printer Events
    - Applications and Services Logs\Microsoft\Windows\PrintService\Admin
        - Common Events:
            - Changing the default printer
            - Errors related to initializing a new printer or driver
            - Errors occurring when attempting to connect to a network printer
            - Errors occurring when attempting to share a printer
- Group Policy Settings for Troubleshooting
    - Computer Configuration\Administrative Templates\Printers

        - Execute Print Drivers in Isolated Processes – By default, the print spooler keeps print drivers in a separate process. This enables the print spooler to continue to function even if the print driver fails. The default settings is best for troubleshooting, but if you find that the print spooler is failing, you should verify that this settings has not been disabled
        - Override Print Driver Execution Compatibility Setting Reported by Print Driver – Print Drivers provide a driver isolation compatibility flag that indicates whether the print driver should be run in a separate process from the print spooler. If you enable this setting, the print spooler runs all print drivers in a separate process.
        - Allow Print Spooler to Accept Client Connections – This setting prevents a computer from acting as a print server.
- Troubleshooting Server Problems –
    - Requirements for a print server
        - Server Service
        - Print Spooler Service
    - Requirements for a network print client
        - Workstation Service
        - Print Spooler Service
- You can clear documents that are stuck in the print queue by restarting the print spooler
- Troubleshooting Driver Problems
    - You can install print drivers by right clicking on the printer in Devices and Printers, selecting Printer Properties, Selecting the Advanced Tab, and clicking on "New Driver".
    - How to add drivers for Shared Printer Clients
        - When connecting to a new printer, clients can automatically install drivers that are stored on the print server.
        - By default, the print server has only the drivers required for the print server to print
        - To add drivers for additional operating systems, do the following:
            - Open Devices and Printers, right click the printer and select printer properties, go to the sharing tab and select additional drivers. In the additional drivers dialog box, select the processor architectures for which you want to store drivers.
            - Follow the wizard.
    - The ability to install printer drivers automatically is called point and print. You can actually connect to a printer via UNC path and double click on it to install. You can then right click on it when you are finished and click disconnect.
-

Chapter 4 Lesson 1

Credential Manager

- Can roam stored user names and passwords between multiple Windows computers in an AD DS domain. Windows stores these credentials in the users' AD profile.
- Windows automatically adds credentials used to connect to shared folders to the credential manager.
- Credential Manager can be accessed from the User Accounts app in Control Panel. Select "Manager Your Credentials" in the left pane.
- The only web sites that Credential Manager can authenticate to automatically are those that use HTTP authentication. This type of authentication is when a prompt pops up asking for credentials.

Use the Resultant Set of Policy tool (RSOP) to identify a computer's effective Group Policy settings.

- The details pane shows only policy settings that have been applied.

You can identify locked out accounts by examining logon audit failures in the domain controllers Security event log with Event ID 4625.

Windows 7 provides 2 separate authentication auditing policies:

- Audit Logon Events
    - Audits authentication attempts for local resources such as a user logging on locally, elevating privileges with a UAC prompt, or connecting over the network.
- Audit Account Logon events
    - This policy audits domain authentication. These events appear only to the domain controller that handled the authentication request.
    - This can be enabled from within Group Policy or the Local Security Policy
    - Successful logon event have Event ID 4624, unsuccessful are 4625

When you are authentication to a network resource, authentication failures are always logged on the server, not on the client.

Network authentication can be a problem if Group Policy settings are used to distribute certificates required for network authentication because the client computer must first connect to the network to get the certificate. If this is ever a problem, just connect the client to the wired network and update Group Policy.

You can configure a CA trust by using Group Policy, rather than importing the Root CA's certificate into the clients store manually.

How to Troubleshoot Untrusted Computer Accounts:

- Domain Controllers automatically create and change passwords for domain computer accounts
- When computer accounts become untrusted, the computer's SID or password does not match those that are stored in AD DS. This can occur when either of the following occurs:
    - Multiple computers have the same SID. This can happen when a computer is deployed using an image and SysPrep was not used on the image prior to deployment. The image contains the SID of the computer it was captured from.
    - The computer account is corrupt in AD DS.
- You cannot reset the password on computer accounts. The easiest way to resolve this problem is to rejoin the computer to the domain.
    - Join the computer to a workgroup and then restart it; open ADUC and right click the computer account, and then click "Reset Account"; then rejoin the computer to the domain. Finally, restart the computer.

Chapter 4 Lesson 2

You can permanently delete ActiveX controls

To start IE without add-ons, type iexplore –extoff

Configuring Add-ons:

- Navigate to User Configuration\Policies\Administrative Templates\Windows Components\Internet Explorer\Security Features\Add-on Management
    - Typically, you need to use 2 settings in this group to block all unapproved add-ons:

        - Add-on list: Enable this settings, and then specify the approved add-ons. To specify an add-on, type in its CLSID as the "Value Name" in the Add-On list. You can find the CLSID for an add-on by reading the <object> tag from the HTML of a web page that references the add-on. To specify that the add-on should be denied, specify a value of 0. To all an add-on, specify a value of 1. To both allow an add-on and permit users to manager the add-on, specify a value of 2.
        - Deny all Add-ons unless specifically allow in the add-on list:
            - After specifying the allowed add-ons in the Add-on list, enable this policy to block installation of all other add-ons.
        - 2 other GP settings related to add-on management are located within both user and computer configuration under Administrative Templates\Windows Components\Internet Explorer:
            - Turn off crash detection: By default, IE detects add-ons that crash and disable them at the next startup of IE, this policy prevents that.
            - Do not allow Users to enable or disable add-ons: Users can disable and enable add-ons by default. This prevents that.
- Managing ActiveX add-ons:
    - ActiveX opt-in is enabled by default for the Internet and Restricted Sites zones. This can be altered by opening Internet Options, selecting the Security tab, selecting the zone you want to configure, and then clicking the "Custom Level" button. This settings can be found in the list under "ActiveX Controls and Plugins".
    - Enabling ActiveX opt-in causes IE NOT to install ActiveX plugins, instead requiring the user to explicitly choose to configure the add-on.
    - Opt-in applies to most ActiveX controls, however, it does not apply to those on the preapproved list. The preapproved list is in the registry at HKLM\Software\Windows\CurrentVersion\Ext\PreApproved.
    - You can use the ActiveX installer service to enable standard users to install specific ActiveX controls. To configure the preapproved list of sites that are able to install controls, go to:
        - Computer Configuration\Administrative Templates\Windows Components\ActiveX Installer Service
            - Double click the "Approved Installation Sites for ActiveX Controls" setting. Enable it.
            - Click "Show" to specify host URL's that are allowed to install ActiveX controls.

X64 version of IE can't use x32 components

Protected Mode:

- One of the features of Windows 7 that enables Protected Mode is Mandatory Integrity Control (MIC). MIC labels processes, folders, files, and registry keys using one of four integrity access levels (ILs). IE runs with a low IL, which means it can access only other low IL resources without the users permission.
    - IL Levels:
        - System: Unlimited access to the computer
        - High: Administrative
        - Medium: User
        - Low: Untrusted

How to Troubleshoot Certificate Problems:

- Certificate Purposes:
    - Encrypting Traffic
    - Authenticating the server
    - Authentication the client

Chapter 4 Lesson 3

Encrypting File System (EFS)

- Supported only on NTFS
- Windows 7 Starter, Home Basic, and Home Premium do not support EFS
- Encrypted folders are green in color
- You cannot encrypt any file marked with the System attribute
- EFS files are not indexed and will not be returned with search results. This can be changed by opening the Indexing Options, clicking Advanced, and then selecting the Index Encrypted Files check box.
- How to create and backup EFS certificates:
    - The EFS certificate backup utility can be found in the User Accounts app of Control Panel. Select "Manage Your File Encryption Certificates" in the left pane. Run through the wizard.
- To restore an EFS certificate just double click on it and run through the wizard.
- You cannot share encrypted folders with multiple users, only individual files. In fact, you cannot even share multiple files in a single action, you must do them individually. However, you can use the cipher command to automate the process.
- How to recover using a Data Recovery Agent
    - EFS grants DRA's permission to decrypt files so that an administrator can restore an encrypted file if the user loses his or her EFS key.
    - By default, workgroup computers configure the local admin account as the DRA.
    - Domain admins are default DRA for a domain

Bitlocker:

- Bitlocker encrypts entire volumes, including system files. EFS cannot encrypt system files or entire volumes.
- To allow you to initialize TPM chips manually and turn them on or off at the operating system level, Windows 7 includes the TPM Management snap-in.
- Bitlocker has 4 main modes on computers with TPM hardware:
    - TPM Only
    - TPM with External Key
    - TPM with PIN
    - TPM with Pin and External Key
- In its default configuration, Bitlocker tells the TPM to measure the MBR, the active boot partition, the boot sector, the Windows Boot Manager, and the Bitlocker storage root key. It hashes all of this information and then compares it each time the computer boots.
- If TPM hardware is not available, Bitlocker can store decryption keys on a USB flash drive.
- If the computer does not have a TPM, you must select "Allow Bitlocker without compatible a TPM" within Group Policy.
- You can use manage-bde to manager Bitlocker on a remote computer
- If the drive is locked, you can boot only to recovery mode, where the recovery key must be entered.
- As a last resort, you can use the Bitlocker repair tool (repair-bde) to help recover data from an encrypted volume. You can use this tool to decrypt a volume (if you have the recovery key), and then copy the files to a different volume. You can also attempt to repair a volume without copying any data.
- You can dual boot a computer after enabling Bitlocker

Chapter 5 Lesson 1

Types of malware:

- Virus – A self-replicating program that can install itself on a target computer.

- Worm – Self-replicating programs that can spread automatically over a network without any help from a user or a program such as an email client or web browser.
- Trojan – A program that is presented to users as a desirable application but that is intentionally written to harm a system.
- Spyware – A type of privacy invasive software that secretly records information about user behavior, of for the purposes of market research.
- Adware – Displays unsolicited advertisements to the user in the form of pop-up windows or web browser alterations.
- Backdoor – Used for unauthorized remote access.
- Rootkit –

Understanding UAC:

- The UAC notification that normally appears for admins is called the consent prompt. And it appears on the secure desktop.
- Whenever standard users attempt to make changes to a system, a credential prompt appears on the secure desktop.
- Configuring UAC through the Control Panel
    - Can be found under System and Security\Action Center\Change User Account Control Settings
    - Notification Levels:
        - Always Notify – will notify any time changes that require admin privileges are attempted on the system. This is the default setting for standard users.
        - Notify me only when programs try to make changes to my computer – Default for admins and is not available for standard users. Administrators are not notified when they make changes that require admin privileges. However, users are notified through a consent prompt when a program tries to make a change.
        - Always Notify me (Do not dim desktop) – Not available for administrators. Same as the default level for standard users, except UAC does not prompt on the secure desktop.
        - Never Notify – Disables UAC notifications.
- Configuring UAC through Group Policy:
    - Can be found at Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options
        - Admin Approval Mode for the Built in administrator account – Applies only to the built in admin account. When this is enabled, the built in admin account see's UAC notifications just as other admins do. When you disable this, the built in admin account does not experience UAC.
        - Allow UIAccess Applications to prompt for elevation without using the secure desktop –
        - Behavior of the elevation prompt for administrators in admin approval mode: - Controls the behavior of the elevation prompt for administrators
            - Elevate without prompting – admins never see elevation prompts
            - Prompt for credentials on the secure desktop – admins see credential prompts on a secure desktop
            - Prompt for consent on the secure desktop – Admins see a consent prompt on the secure desktop
            - Prompt for credentials
            - Prompt for consent
            - Prompt for consent for non-windows binaries – causes a consent prompt to appear any time an application requests elevation.
        - Behavior of the elevation prompt for standard users: - Controls the behavior of the elevation prompt for standard users.
            - Automatically deny elevation requests
            - Prompt for credentials on the secure desktop

        - Prompt for credentials
    - Detect application installations and prompt for elevation – This settings makes UAC prompt for admin credentials when the user attempts to install an application that makes changes to protected aspects of the system.
    - Only Elevate executables that are signed and validated – When this is enabled, Windows 7 refuses to run any executables that aren't signed with a trusted certificate.
    - Only elevate UIAccess applications that are installed in secure locations – This policy only allows user interface access programs that are installed in Program Files and subfolders to run.
    - Run all administrators in admin approval mode – Causes all admin accounts except for the built in admin account to see consent prompts
    - Switch to the secure desktop when prompting for elevation – This policy controls whether or not the secure desktop appears with UAC prompts.
    - Virtualize File and Registry write failures to per-user locations – Improves compatibility for applications not developed by UAC by redirecting requests for protected resources.

Windows Defender:

- Configured by default to download new definitions and then do a quick scan at 2 am daily.
- 3 types of scans:
    - Quick scan
    - Full scan
    - Custom scan
- 4 options for detected malware:
    - Ignore
    - Quarantine
    - Remove
    - Always allow
- Configuring Windows Defender with Group Policy
    - Can be found at Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender
    - Turn on definition updates through both WSUS and Windows Update –
    - Turn on definition updates through both wsus and the Microsoft Malware Protection Center
    - Check for new signatures before scheduled scans
    - Turn off Windows Defender
    - Turn off Real Time Monitoring
    - Turn Off Routinely Taking Action
    - Configure Microsoft Spynet Reporting

Chapter 6 Lesson 1

- Direct Access is built exclusively on IPv6 and has not fallback to IPv4
- 2 Types of VPN's: Site to Site and Remote Access
- VPN tunneling protocols can validate data in 2 ways
    - Data Integrity checking
    - Data Origin Authentication
- Requirements for A VPN infrastructure
    - VPN client
    - VPN server running RRAS
    - DNS Server
- Typically a VPN infrastructure also includes a DC, certificate server, and a DCHP server. A NPS server might also be used.
- VPN clients can be any of the following types:

    - Windows 7 VPN client
    - Connection Manager Client (CM)
    - Third part client
- The Connection Manager Administration Toolkit (CMAK) can be used to create client connection profiles and then distributed to clients as CM clients. This is very scalable compared to creating
- For authentication, RRAS can be configured to forward request to a RADIUS (NPS) server or use Windows authentication. When configured to use Windows authentication, the RRAS server passes requests to an available DC.
- Remote access authentication precedes domain logon authentication.
- VPN clients that connect to a network must be configured with the address of a DNS server on that network, so that it can resolve names on that network.
- NPS is the Microsoft implementation of a RADIUS server and proxy.
- Windows 7 supports 4 tunneling protocols.
    - IKEv2
        - New in Windows 7 and Server 2008 R2
        - Uses IPSec for encryption
        - Only protocol that supports VPN reconnect (also called mobility)
        - Clients do not need to provide authentication through a machine certificate or a preshared key. The same goes for SSTP and PPTP.
        - IKEv2 VPN's require a PKI. The server must present a server authentication certificate to the client, and the client needs to be able to validate the certificate. To perform this validation, the root certificate for the CA that issued the server authentication certificate must be in the Trusted Root Certification store on the client computer.
    - SSTP
        - Can be used by clients running Vista SP1 or later
        - Based on HTTPS (uses only port 443 for communication, most firewalls leave this port open)
        - Does not require client computer authentication by default, though this can be configured.
        - The SSTP VPN server must present a computer certificate to the connecting client at the beginning of the connection process. The client must validate this certificate. The issuing root CA of the certificate must be in the Trusted Root Certificate Authorities store on the client.
        - User authentication via PPP
    - L2TP
        - Security provided by IPsec
        - Besides requiring user authentication as all VPN protocols do, L2TP requires client computer authentication also. Because of this, all VPN client computers from which a user might connect must be configured either with a computer certificate or a preshared key specific to the vpn server. Therefore, L2TP prevents a user from establishing a connection from a public computer or from any computer not specially configured for the VPN.
        - To configure the client to use a certificate or a preshared key, open the properties box of the connection, click the security tab, and then click advanced settings.
    - PPTP
        - Easiest protocol to implement, but also least secure
        - Does not require any certificates or preshared keys on either the client or server.
        - Can be used with older Operating Systems
        - Does not ensure data integrity or data origin authentication
        - User authentication via PPP
- Remote Access Connectivity Process:
    - VPN client contacts the VPN server

        - Client must be configured with proper IP address of VPN server. VPN server needs to be publicly available.
    - VPN tunnel is negotiated
        - Client requests a tunnel type in the following order: Ikev2, SSTP, L2TP, PPTP
        - Authentication protocol is also negotiated. For IKEv2, the EAP-MSCHAPv2 protocol is used. For other VPN's, MSCHAPv2 is preferred. Otherwise Chap is requested.
        - Encryption is also negotiated during this phase.
    - VPN tunnel is created
        - If the tunnel type, authentication type, and encryption type can be agreed upon, the tunnel Is created. After this point, all exchanges are encrypted.
    - Remote Access Authentication is Performed
        - User account properties are check to make sure the user is authorized for remote access
        - List of network policies on the VPN server or NPS server is checked.
    - The VPN connected is established
        - Domain logon occurs.

Chapter 6 Lesson 2 – Direct access

Supported on Windows 7 Ultimate, Enterprise, and Windows Server 2008 R2.

VPN client machines are typically not subject to Group Policy

Benefits of Direct Access

- Always on connectivity
- Seamless connectivity
- Bidirectional access
- Enhanced security

Direct Access is built on IPsec and IPv6

- IPsec is used to authenticate both user and computer

IPv6 Transition Technologies

- ISATAP (Intra-site Automatic Tunnel Addressing Protocol)
    - Allows an IPv6 network to communicate with an IPv4 network through an ISATAP router.
    - ISATAP allows IPv4 and IPv6 hosts to communicate by performing a type of address translation
    - All ISATAP clients receive an address for an ISATAP interface.
    - ISATAP is intended for use within a private network.
- 6to4
    - Tunnels IPv6 traffic over IPv4 traffic through 6to4 routers.
    - 6to4 clients have their router's IPv4 address embedded in their IPv6 address and do not require an IPv4 address.
    - 6to4 is intended for use on the internet
- Teredo
    - A tunneling protocol that allows clients located behind an IPv4 NAT device to use IPv6 over the internet.
    - Teredo is used only when no other transition technology is available.
    - Teredo relies on an infrastructure of teredo clients, teredo servers, teredo relays, and teredo host specific relays.

            - Teredo client – A computer that is enabled with IPv4 and IPv6 and is located behind and IPv4 NAT device. The client creates a Teredo tunneling interface and configures a routable IPv6 address with the help of a Teredo server.
            - Teredo Server
            - Teredo Relay
            - Teredo Host-specific relay
    - IP-HTTPS
        - Developed by Microsoft for Windows 7 and Windows Server 2008 R2.
        - Enables hosts located behind a web proxy server or firewall to establish connectivity by tunneling IPv6 packets inside an IPv4 based HTTPS session.
        - This is considered a fallback technology for when no other transition technology will work.
        - IPv6/IPv4 NAT
            - Deprecated

Direct Access Infrastructure Features

- PKI, Domain controllers, IPv6 transition technologies, and DNS servers, Direct access clients, Direct Access servers, and a network location server, CRL Distribution Points
- Direct Access server
    - Must be Windows Server 2008 R2 and joined to the domain
    - Sits on perimeter of network and also acts as a IPv6 relay and IPsec gateway
    - Accepts connections from Direct Access clients
    - Needs 2 physical network adapters
    - Also needs 2 consecutive publicly addressable IPv4 addresses
- Direct Access client
    - Must be domain joined and running Windows 7 Enterprise or Ultimate
    - Add the to a group, and then specify this group when you run the DA setup wizard on the DA server
    - The Name Resolution Policy Table (NRPT) allows clients to separate internet traffic from intranet traffic. This can be applied to clients through Group Policy. Located at Computer Configuration\Policies\Windows Settings\name Resolution Policy
- Network Location Server
    - A web server accessed by DA clients to determine whether or not they are on the local intranet or the internet.
- IPv6 capable network
    - The order of connection methods attempted by DA clients is as follows:
        - Native IPv6
        - 6to4
        - Teredo
        - IP-HTTPS
    - For remote client computers to reach computers on the internal network, internal computers must be fully IPv6 compatible.
- IPsec
    - Provides end-to-end security for remote client computers accessing resources on the internal network. Used for authentication and encryption of all DA connections.
- PKI
    - Required to issue computer certificates for client and server authentication and also for issuing health certificates when NAP has been implemented.
-
- CRL Distribution Points (CDP's)
    - Servers that provide access to the CRL published by the CA issuing certificates for DA.

- Perimeter Firewall Exceptions
    - The following ports must be open:
        - UDP port 3544 to enable inbound teredo traffic
        - IPv4 protocol 41 to enable inbound 6to4 traffic
        - TCP port 443 to enable inbound IP-HTTPS traffic

Client configuration

- Clients are normally configured when you run the DA setup wizard, however you can do it manually.
    -

PURPOSE	COMMAND	GROUP POLICY SETTING
Configure the Teredo client as an enterprise client and configure the IPv4 address of the Teredo server (the DirectAccess server).	*netsh interface teredo set state type=enterpriseclient servername=*FirstPublicIPv4AddressOfDirectAccessServer	Computer Configuration\Policies\Administrative Templates\Network\TCPIP Settings\IPv6 Transition Technologies\Teredo State=Enterprise Client and Computer Configuration\Policies\Administrative Templates\Network\TCPIP Settings\Ipv6 transition Technologies\Teredo Server Name=*FirstPublicIPv4AddressOfDirectAccessServer*
Configure the public IPv4 address of the 6to4 relay (the DirectAccess server).	*netsh interface 6to4 set relay name=*FirstPublicIPv4AddressOfDirectAccessServer	Computer Configuration\Policies\Administrative Templates\Network\TCPIP Settings\Ipv6 transition Technologies\6to4 Relay Name=*FirstPublicIPv4AddressOfDirectAccessServer*
Enable the IP-HTTPS client and configure the IP-HTTPS Uniform Resource Locator (URL).	*netsh interface httpstunnel add interface client https://*FQDNofDirectAccessServer*/IPHTTPS*	Computer Configuration\Policies\Administrative Templates\Network\TCPIP Settings\Ipv6 transition Technologies\IP-HTTPS State set to Enabled and the IP-HTTPS URL of *https://*SubjectOfIP-HPPTSCertificate:*443/IPHTTPS*

The DA connection process

- The DA client detects that it is connected to a network
- The DA client attempts to contact the network location server. If the NLS is available, the client determines it is already connected to the intranet and the DA process stops. If the NLS is not available, the DA client determines that it is connected to the internet and the DA connection process continues.
- The DA client computer connects to the DA server using IPv6 over IPsec. If a native IPv6 connection isn't available, the client establishes an IPv6 over IPv4 tunnel using 6to4 or Teredo.
- If a firewall or proxy server prevents the user of 6to4 or Teredo, the client attempts to use IP-HTTPS.
- The DA client and server authenticate each other using computer certificates for authentication.
- The server authorizes the client by checking the DA group membership.
- If NAP is enabled, the DA client attempts to obtain a health certificate from an HRA located on the LAN.
- The DA server begins forwarding traffic from the DA client to intranet resources.

Troubleshooting DA

- The following must be configured correctly for DA to work:
    - The DA client must have a global IPv6 address. Global IPv6 addresses start with a 2 or 3

Chapter 7 Lesson 1

- Methods of updating
  - Windows Update
  - WSUS
  - SCCM
- To deploy updates to Windows 7 using you must have WSUS 3.0 SP2 or later
- Types of updates:
  - Critical Updates:
  - Service Packs
  - Optional Updates
- Windows Update GP settings
  - Located at Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update
  - Configure Automatic Updates – Specifies whether client computers will receive security updates and other important downloads through the Windows Update service.
  - Specify Intranet Microsoft Update Service Location
  - Automatic Updates detection Frequency.
  - All non-administrators to receive update notifications
  - Allow Automatic updates immediate installation
  - Turn on recommended updates via automatic updates
  - No auto restart with logged on users for scheduled automatic updates installations
  - Reprompt for restart with scheduled installations
  - Delay restart for scheduled installations
  - Enable client-side targeting – specifies which group the computer is a member of
  - Enabling windows update power management to automatically wake up the system to install scheduled upates
- Additional GP settings found under "User Configuration" but not "Computer Configuration"
  - Do not display "install updates and shut down" option in Shutdown Windows dialog box
  - Do not adjust default option to install updates and shut down in shut down windows dialog box
  - Remove access to all windows update features
- How to script updates
  - Updates are opened with the WUSA and have the .msu extension.
  - WUSA
    - /uninstall
    - /quiet
    - /norestart
    - /warnrestart
    - /promptrestart
    - /forcerestart
- You can use the MBSA to check computers for missing updates
- Troubleshooting update installation problems
  - Check the Windows update log at %Windir%\WIndowsUpdate.log
  - If using WSUS, verify that the client can connect to the WSUS server by opening up a web browser and going to http://<WSUSSERVERNAME>/iuident.cab. If all is working properly, you will be prompted to download a file.
  - If using GP to update clients, use the RSOP to verify the configuration.
  - If changes the Windows Update configuration, restart the Windows Update service (wuauserv)
- Troubleshooting Restart Manager
  - Restart Manager is a feature of Windows Installer that strives to reduce the requirement by closing and restarting programs and services that have files in use.

    - To diagnose a problem with Restart Manager, open Event Viewer and go to Windows Logs\Application and Applications and Services logs\Microsoft\Windows\RestartManager\Operationl
- You can remove updates from the Programs and Features applet
- You can also use WUSA to uninstall updates

Chapter 8 lesson 1

- Event Forwarding
    - Uses HTTP or HTTPS to send events from a forwarding computer to a collecting computer.
    - Even though HTTP is unencrypted, event forwarding sends events encrypted with Microsoft Negotiate Security Support Provider in workgroup environment or Kerberos in Domain environments.
    - HTTPS uses an SSL certificate which you will have to generate to provide an additional layer of encryption.
    - Configuring forwarding in domains:
        - Both the forwarding and collecting computers must have 2 services running:
            - Windows Event Collector
            - Windows Remote Management
        - In addition, the forwarding computer must have a firewall exception for HTTP.
        - To configure a computer to forward events, follow these steps:
            - Open an admin cmd prompt and type in "winrm quickconfig"
                - WInrm configures the computer to accept WS-Management requests from other computers
                - Starts the Windows Remote Management service (WS-Management) to Automatic (Delayed Start)
                - Configures a Windows Remote Management HTTP listener.
                - Creates a Windows Firewall exception to allow incoming connections to the Windows Remote Management service using HTTP.
            - Next you add the computer account of the collecting computer to the Event Log Readers group on the forwarding computer.
        - To configure a computer to collect events:
            - Windows 7 supports 2 types of event collection:
                - Collector-initiated
                - Source-computer initiated
                    - Source initiated are the only type available in workgroups
                - Windows 7 will prompt you to configure the collecting computer when you create a subscription.
                - Type in the following command at an admin cmd prompt:
                    - Wecutil qc
                - If you plan to use source computer initiated subscriptions, you need to also run winrm quickconfig on the collecting computer.
        - After setting up the computer, you create a subscription from the Event Viewer console
        - 3 types of subscriptions:
            - Normal – Ensures delivery of events and does not attempt to conserve bandwidth
            - Minimize Bandwidth – Uses push delivery mode, where the forwarding computer contacts the collecting computer.
            - Minimize Latency – Ensures events are delivered with minimal delay. Uses push delivery mode.
    - By default, normal subscriptions check for events every 15 minutes
        - To adjust the event subscription delay, run these commands:

                - Wecutil ss <subscription name> /cm:custom
                - Wecutil ss <subscription name> /hi:<milliseconds delay>
            - If you need to check the interval, run the following command:
                - Wecutil gs <subscription name>
    - Configure Event Forwarding to use HTTPS
        - You must perform these addition tasks on the forwarding computer
            - Configure the computer with a computer certificate.
            - Create a firewall exception for port 443.
            - Run the following command at an elevated command prompt:
                - Winrm quickconfig –transport:https
        - On the collecting computer, you must modify the subscription properties to use https.
        - In addition, the collecting computer must trust the CA that issues the computer certificate for the forwarding computer.
    - Configuring forwarding in workgroups
        - The process is very similar to creating a subscription in a domain, with the following exceptions:
            - You must add a Windows Firewall exception for Remote Event Log Management on each forwarding computer
            - You must add an account with admin privileged to the Event Log Readers local group on each forwarding computer.
            - On each collecting computer, run the following command to allow the forwarding computers to use NTLM authentication: winrm set winrm/config/client@{TrustedHosts="<forwarding_comptuer>"}

Chapter 8 Lesson 2

- Task Manager
    - Task Manager has 6 tabs
        - Applications
        - Processes
        - Services
        - Performance
        - Networking
        - Users
    - Processes run within threads.
    - A Processor can only run 1 thread at a time
- Performance Monitor
    - Graphically displays real time data
    - Change the interval to show a more smooth and less jagged graph
        - This can be done by clicking action > properties > General tab. Then change the graph elements section.
    - You can select from the following chart types:
        - Line
        - Histogram
        - Report
    - Data Collector Sets and Reports
        - Will log performance counter data, allowing you to view it later
        - Event Trace Data shows detailed debugging information
        - Built in Data Collector Sets
            - System Performance
                - Logs Processor, disk, memory, and network performance counters and kernel tracing.

        - System Diagnostics
            - Logs all information included in the System Performance data collector set, plus more detailed info.
    - To use a data collector set, right click it and then click start. The system performance DCS stop automatically after a minute. The system diagnostics DCS stops after10 minutes. You can also manually stop it by right clicking and then clicking stop.
    - After running a DCS, you can view a summary of the data gathered in the reports node.
    - Creating a DCS from a Standard Template
        - Basic
        - System Diagnostic
        - System Performance
- Troubleshooting Disk Performance Problems
    - To reduce fragmentation, increase the amount of free disc space
    - Use disk cleanup to cleanup the hard drive
    - Disk defragmenter
    - Virtual Memory
        - Maximize performance by storing virtual memory on a different physical disk from other files.
- Configuring Power settings
    - Advanced power settings
        - Turn off hard disk after
        - Wireless adapter settings
        - Sleep
        - USB settings
        - Power Buttons and Lid
        - PCI Express
        - Processor Power Management
        - Multimedia Settings
        - Battery
- System Configuration
    - MSConfig

Chapter 9 Lesson 1

- To install software, you must have local admin privileges
- When you install a program, Windows 7 checks for a certificate and digital signature to authenticate the publisher of the program.
    - To verify this digital signature properly, the local computer must trust the root CA for the publisher certificate.
- Applocker
    - Blocks all programs that are not specifically allowed.
    - Assign rules to specific users or groups. In Software restriction policies, you can only assign rules to everyone.
    - Create exception to rules
    - Audit only mode
    - The ability to import and export rules to and from computers
    - Applocker rules are enforced only on computers running Windows 7 Ultimate and Enterprise, and windows server 2008 R2.
    - Applocker always overrules Software Restriction Policies
    - Permissions:
        - Allow or Deny
    - Conditions:
        - Publisher, Path, or File Hash

Chapter 9 Lesson 2

- Windows Resource Protection
    - Also called File and Registry Virtualization
    - A feature in Windows Vista and Windows 7 that intercepts any application requests to write to protected system areas and redirects them to safe and temporary locations. Some applications cannot handle this redirection process.
- Program Compatibility Assistant
    - A tool that automatically appears when Windows 7 detects known compatibility issues in older programs.
- Program Compatibility Troubleshooter
    - A control Panel program that you can use to configure the compatibility settings for an older program if you notice that the program is not running smoothly.
- Compatibility Tab of a program
    - Manually configure what the Program Compatibility Troubleshooter would do.
- Windows XP mode
    - Requires special virtualization hardware
    - Can run on Windows 7 Professional, Enterprise, or Ultimate
- Understanding the ACT
    - Application Compatibility Manager
        - Collect and analyze data so that you can identify any issues prior to deploying a new operating system or deploying a Windows update.
    - Application Compatibility Toolkit Data Collector
        - This tool is distributed to each computer. It then performs scans by using compatibility evaluators. Data is collected and stored in a database.
    - Setup Analysis Tool
        - Automates the running of application installations while monitoring the actions taken by each application's installer.
    - Standard User Analyzer
        - Determines the possible issues for applications running as a standard user in Windows 7.
- Configuring Application Compatibility Diagnostics through Group Policy
    - Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Application Compatibility Diagnostics
        - Notify Blocked Drivers – Determines whether the PCA will notify a user if drivers are blocked. This is the default behavior in Windows 7.
        - Detect Application Failures Caused by deprecated Windows COM objects- Determines whether the PCA will notify a user when a DLL load failure is detected in an application.
        - Detect Application Install Failures – Configures the PCA to notify the user when an application installation has failed.
        - Detect application installers that need to be run as administrator – determines whether the PCA will notify the user when application installations have failed because they need to be run as an administrator.
        - Detect applications unable to launch installers under UAC – Configures the PCA to notify the user when UAC is preventing an application from launching an installer.

Appendix A

- Understanding Windows Firewall
    - To control inbound traffic based on its associated program, you can use the Windows Firewall Page in Control Panel.
        - Found under System and Security

    - If you want to control outbound traffic, or be more granular with the control of inbound traffic, use the Windows Firewall with Advanced Security. To open this, click advanced settings on the Windows Firewall page in Control Panel.
    - By default, Windows Firewall allows all outbound connections
- Understanding Network Locations
    - Four network Locations are available, every connection is assigned to ONE of these locations:
        - Home
        - Work
        - Public
    - Network Discovery is disabled by default in the Domain and Public network locations.
    - HomeGroups are only available In the Home Network Location
- Understanding Firewall Profiles
    - Domain Profile – Defines rules assigned to the domain network location
    - Private Profile – Defines rules assigned to either the home or work network location
    - Public Profile - defines the rules assigned to the public network location

Appendix B

- Managing Offline Files
    - Sync Center
    - GP settings for Offline Files
- Managing Data for Roaming Users
    - In all versions of Windows prior to Windows 7, any changes made to a RUP are copied back to the share when the person logs off. In Windows 7 and Server 2008 R2, changes to user settings can be synced periodically with a remote network share.
    - The AppData folder is used for storing application settings and binaries. The following 3 subfolders under AppData:
        - Local – contains computer specific application information that should not roam
        - Roaming – Stores information that should roam with the user profile
        - LocalLow – Allows low integrity processes to have write access to it
    - Background Registry roaming
        - Allows user settings to be synced back to the server while they are logged on.
- Understanding Windows 7 Folder Redirection

Appendix C

Setup automatically installs WinRE

NTLDR has been replaced by the Windows Boot Manager

Boot.ini has been replaced by the BCD

NTDETECT.COM has been merged into the kernel

- Boot Configuration Data
    - Tracks operating system locations
    - Stored in a data file that uses the same format as the registry
    - You cannot use Bootcfg to modify the BCD, you must use BCDEdit
    - A BCD store normally has at least 2 BCD objects:
        - A Windows Boot Manager Object
        - At least one Windows Boot Loader Object
- System Recovery
    - Provides access to the following tools
        - Startup Repair

        - System Restore
        - System Image Manager
        - Windows Memory Diagnostics
        - Command Prompt
- Windows Boot Performance Diagnostics
    - Use GP to manager Windows boot performance diagnostics
        - Computer configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Windows Boot Performance Diagnostics
            - Edit the Configure Scenario Execution Level Policy and choose from the following 2 settings:
                - Detection and troubleshooting only
                - Detection, troubleshooting, and resolution
    - For Windows Boot performance Diagnostics to run, the Diagnostic Policy Service must be running.
- Understanding the startup process
    - The normal startup process for Windows 7 is:
        - POST
            - Test Hardware
        - Initial startup phase
            - Choose the startup device
            - BIOS: IF booting from a hard disk, the computer reads the boot code instructions located in the MBR. The MBR is the first sector of data on the startup hard disk. The MBR contains boot code and the partition table. The BIOS reads the MBR into memory and transfers control to the MBR. The computer then searches for an active partition
        - Windows Boot Manager Phase
            - "Choose an Operating System"
        - Windows Boot Loader Phase
            - Starts the Windows Boot Loader
            - Loads the Kernel and HAL.DLL. Loads the page file. Passes control to the Kernel.
        - Kernel Loading Phase
            - Initialize a group of software features called the "Windows Executive"
        - Logon Phase
- Using Msconfig
    - Tabs: General, Boot, Services, Startup, Tools
        - General – Used to change the startup selection
        - Boot – Used to edit BCD, change the default OS, etc
        - Services – Used to configure services that run at startup
        - Startup – Used to configure programs that run at startup
        - Tools – Launch various tools
- Using BCDEdit
    - You must use admin creds to run BCDEdit
    - Before making changes to the BCD store, export the current settings so you have a backup.
        - BCDEDIT /export "backupbcd.bcd"
- Startup Repair log files are located in %windir%\system32\logfiles\srt\srttrail.txt
- Bootrec.exe
    - /fixmbr – writes a new MBR
    - /scanos – Scans for Windows Installations and displays entries not currently listed in BCD
    - /fixboot – Writes a new boot sector
    - /rebuildbcd – rebuilds the bcd with all windows entries
- How to analyze boot logs
    - Boot logging lists the successfully and unsuccessfully loaded during startup

    - Enable boot logging, and then compare the list of drivers loaded in normal mode to those loaded in safe mode.
- By holding down the shift key during startup, you prevent the operating system from loading any startup programs
- You can configure programs that run at startup by using GP
    - Computer Configuration or User configuration\Policies\Administrative Templates\System\Logon
        - Run these programs at user logon

Appendix D

- Windows Troubleshooting Platform
    - Running Troubleshooting Packs Remotely
        - Import-Module TroubleshootingPack
          $aero = Get-TroubleshootingPack $env:SystemRoot\Diagnostics\System\Aero
          Invoke-TroubleshootingPack -Pack $aero -Result C:\DiagResult –unattend
- Resource Monitor
    - "Advanced Task Manager"
    - You can search online for information about a process
- Windows Memory Diagnostics
- Disk Failure Diagnostics
    - Windows queries for SMART status on an hourly basis
    - You can configure Disk Diagnostics using 2 GP settings:
        - Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Disk Diagnostics
            - Disk Diagnostics: Configure Execution Level
                - Use this to enable or disable disk diagnostics
            - Disk Diagnostics: Configure Custom Alert Text
                - Define Custom Alert Text up to 512 characters
        - For Disk diagnostics to work, the Diagnostic Policy Service must be running
- Self Healing NTFS
    - Included in Windows Vista and Windows 7
    - Detect and repair corruption while the OS is running
- Improved Driver Reliability
    - Windows 7 includes Driver Verifier to help developers create more stable drivers.
- Reliability Monitor
    - The chart provides a day-by-day report of any problems or significant changes.
    - Types of alerts
        - Application Failures, Windows Failures, Miscellaneous Failures, Warnings, and Information
- Data Collector Sets
    - Viewed from Performance Monitor
    - You must "start" Data Collector Sets
- Driver Verifier (verifier.exe) can be used to identify potentially problematic drivers
- File signature verification (sigverif.exe) detects signed files and unsigned files.
    - Signed drivers are those that pass the WHQL
    - Using signed drivers results in a more stable system
- Troubleshooting Tools:
    - DiskView
        - Shows how files are physically laid out on your disk and allows you to view where specific files are stored.
    - Handle
        - Allows you to determine which process has a file or folder open

    - Process Monitor
        - Monitors File and registry accesses by an application

Appendix E

- Arp
    - Useful for diagnosing communications on a LAN when it doesn't travel through a router
- Event Viewer
    - Administrators can use Wireless Diagnostics Tracing to capture and analyze diagnostic information by using graphical tools.
    - You can find network diagnostic information in 2 logs within Event Viewer
        - Windows Logs\System
        - Applications and Services Logs\Microsoft\Windows\Diagnostics-Networking\Operational
- IPConfig
- NBLookup
    - Used for diagnosing WINS name resolution problems
- Nbtstat
    - Used for troubleshooting NetBIOS name resolution problems.
- Net
    - Net can be used to change network configuration settings, start and stop services, and view shared resources.
    - Use the "net share" command to view shared resources on a local computer
    - Use the "net view <computer name>" to view shared resources on a remote computer. You can identify the computer by using the name or IP address. If you receive an access is denied error while trying to view remote shares, establish a NetBIOS connection to the remote computer by doing the following:
        - Run the 'net use \\PC1 /user:<username>
        - You should then be able to run the 'net view' command
- NetStat
    - Can be used to view network services and the ports they listen on.
    - You can also view the process ID that an open connection is related to, and then view this process within task manager. This would be helpful in troubleshooting malware infections.
- Network Monitor
    - Only available if download
    - Sniffer
- NSLookup
- PathPing
    - Can identify routing loops
    - Can also be used to identify network performance problems (RTT and packet count lost/received)
- Performance Monitor
    - Can be used to view thousands of real time counters related to networking
    - Can be used on a local or remote computer
- Data Collector Sets
- Resource Monitor
- Ping
- PortQry
- Route
- Task Manager
- TCPView
- Telnet Client
- Test TCP (ttcp.exe)

- Troubleshooting network Problems
    - Troubleshooting Performance Problems and Intermittent Connectivity Issues
        - Network utilization on wired networks should not exceed 60-70%, on wireless 50%. This can be checked in Task Manager from on the networking tab.
    - How to troubleshoot joining or logging on to a domain
        - Always view error information when troubleshooting domain logon or join problems
        - If the error does not reveal the problem, view the %windir%\debug\netsetup.log file. This log details the process of joining a domain as well as the details of any problems encountered.
        - To reproduce the problem, or check to see if it is resolved, run the following command:
            - Net use \\servername\ipc$ /u:<account> <password>
        - Requirements for joining a domain:
            - The client computer must be able to resolve the ip address for a DC
            - The client computer must be able to exchange traffic with the DC on several different TCP and UDP ports:
                - TCP port 135 for RPC traffic
                - TCP Port 389 and UDP port 389 for LDAP traffic
                - TCP port 636 for LDAP over SSL traffic
                - TCP port 3268 for LDAP Global Catalog traffic
                - TCP port 3269 for LDAP GC SSL traffic
                - TCP port 53 and UDP port 53 for DNS traffic
                - TCP port 88 and UDP port 88 for Kerberos traffic
                - TCP port 445 for SMB
            - The administrator must have privileges to add a computer to a domain
                - Must have the 'Add Workstations to Domain' user right
            - The computer must be running Windows 7 Pro, Ultimate, or Enterprise.
    - How to troubleshoot Network Discovery
        - Network Discovery turned off by default on Public network types
        - On a domain, Network Discovery is controlled with GP, but is disabled by default
        - To troubleshoot Network Discovery:
            - Verify that the Function Discovery Provider Host service is running
            - Very that Windows Firewall has exceptions for Network Discovery
            - Change the type of network from Public to Private.
    - How to troubleshoot file and printer sharing
        -

Appendix F

- Identify the following information about the stop error to begin troubleshooting
    - Stop Error Number -
    - Stop Error Parameters
    - Driver Information
- Memory Dump Files
    - Windows writes the information to the pagefile on the %SystemRoot% drive by default.
    - Types of dump files:
        - Small Dump file
            - Also known as minidumps, contain the least amount of info possible.
            - These are stored in the %SystemRoot%\MiniDump director, rather than at the root of the drive.
            - A small dump file is always created, even if a Kernel or Complete Dump file are created. These can be used for WER or Debuggers
            - A small Memory Dump file includes the following:

        - Stop Error information – error number and additional parameters
        - A list of running drivers – identifies the modules in memory when the stop error occurred.
        - Processor context info for the process that has stopped – includes the proc and hardware state, performance counters, multiprocessor packet information, deferred procedure call information, and interrupts.
        - Kernel context information for the process that has stopped – include offset of the directory table and the page frame number database, which describes the state of every physical page in memory.
        - Kernel context information for the thread that has stopped – identifies registers and IRQLs and includes pointers to OS data structures.
        - Kernel mode call stack info for the thread that stopped – Consists of a series of memory locations and includes a pointer to the initial location. Developers might be able to use this information to track the source of the error.
      - A small dump file requires a paging file of at least 2 MB on the boot volume.
    - Kernel Dump File
      - Record the contents of kernel memory
      - These are the type of dump file created by default.
      - Records only kernel memory and can occupy several megabytes of disk space.
      - Contains more information than a small memory dump file
    - Complete Dump file
      - Record the complete contents of physical memory. The size of this file will be slightly larger than the amount of physical RAM installed.
      - Sometimes referred to as a full dump file
  - Using dump files to analyze stop errors
    - You can use WER to upload dump files to Microsoft, or you can view them using the Microsoft Kernel Debugger (kd.exe), or Microsoft WinDbg Debugger (WinDbg.exe)
    - You can also view information about the stop error in the System Log of Event Viewer.
  - Using Windows Error Reporting
    - After a stop error occurs, Windows displays the "Windows has recovered from an unexpected shutdown" dialog box. To view the stop error code, operating system information, and dump file locations, click "View Problem Details".
    - You can also select "Check for Solution" to submit the dump file to Microsoft.
- Being prepared for stop errors
  - Prevent System restarts after a stop error
    - Can be done from the Advanced System Settings
  - Record and Save stop message information
  - Check Software Disk Space Requirements
  - Install a Kernel Debugger and Symbol Files

Miscellaneous

- Security Log in Event Viewer
  - Shows login failures connecting to local computer (Audit Events)
  - Audit Object Access Events logs when users try to access folders without sufficient privileges
- **wevtutil (Windows Events Command Line Utility)** enables you retrieve information about event logs and publishers, install and uninstall event manifests, run queries, and export, archive, and clear logs
- Group Policy

- **"Audit Process Tracking" & "Audit Privilege Use"** are enabled to track UAC elevation in Event Viewer
- **"Disk Diagnostic: Configure Execution Level"** Displays error messages to the users
- **"Configure Corrupted File Recovery Behavior"** controls how Windows recovers files
- **"Require Trusted Path for Credential Entry"** requires users to hit CTRL-ALT-DEL to open UAC elevation prompt
- **"Active X installation for sites in Trusted Zones"** can be Enabled for automatic installation of Active X for Trusted Sites, if Disabled user will be prompt. Options: (0 - not installed; 1 - prompt for install; 2 - installed silently)

- **Security**
  - **Security Configuration and Analyzer Tool** is used to compare settings in a security template to your computer's current configuration
- VPN Troubleshooting
  - **Error 13801 (Client side error, IKE authentication credentials are unacceptable)**
  - **Error 13806 (Server side, IKE failed to find valid machine certificate)**
  -