70-685 Study Guide

to be used as an internal resource only

Introduction

This *free* study guide is for Microsoft's 70-685 exam, 70-685 TS Windows 7, Enterprise Desktop Support Technician. This guide is intended to be supplemental to your books and other study materials. If you find any corrections or would like to suggest additions, please contact me at MrNetTek2000@yahoo.com.

Skills Measured:

Pro: Windows 7, Enterprise Desktop Support Technician

Recommended Reading:

MS Press 70-685

Cram Flash Cards

Quizlet

Study Stack Flash Cards

eBook found online: Labs Online

Windows 7 Desktop Support and Administration: Real World Skills for MCITP Certification and Beyond (Exams 70-685 and 70-686) -Darril Gibson

Windows 7: Troubleshooting and Support

Skills Measured

Identifying Cause of and Resolving Desktop Application Issues (20%)

Applocker

- Windows 7 AppLocker Executive Overview
- Download details: Windows 7 Walkthrough: AppLocker

Compatibility Tools

- Enterprise Application Compatibility
- TechNet Virtual Lab: Application Compatibility Toolkit 5.0
- TechNet Virtual Lab: Mitigating Application Issues Using Shims

- Microsoft Application Compatibility Toolkit (ACT) Version 5.5
- Download details: Windows 7 Walkthrough: Enterprise Application Compatibility
- Microsoft Virtual PC
- Windows XP Mode

Identifying Cause of and Resolving Networking Issues (23%)

Windows Network Diagnostics

Troubleshooting Windows 7 Network problems

Network Troubleshooting Tools

- Ping
- Pathping
- Portqry
- Nslookup

Netsh command for IPv4 and IPv6

Netsh command for WLAN

Setting up a wireless connection with Windows 7

Managing and Maintaining Systems that run Windows 7 client (21%)

Action Center

Device Manager

Reliability Monitor

Performance Monitor

Performance Monitor - Technet

Performance Reliability Monitoring Step-by-Step Guide

Event Viewer

System Recovery Options

Windows Memory Diagnostics

Chkdsk

Disk Defragmenter

Windows 7 Boot Process

Supporting Mobile Users (18%)

Wireless

Troubleshooting Wireless problems

VPN Connections

Virtual Private Networks

Types of VPN Tunneling Protocols

- SSTP
- IKEv2
- L2TP
- PPTP

Direct Access

- DirectAccess | VPN & Corporate Networking | Windows 7
- DirectAccess Early Adopter's Guide
- DirectAccess Technical Overview for Windows 7 and Windows Server 2008 R2
- DirectAccess
- Download details: DirectAccess Early Adopter's Guide

Identify and resolve Windows Internet Explorer security issues (18%)

Credential Manager

UAC

70-685 Study Guide

to be used as an internal resource only

Internet Explorer Add-Ons

Internet Explorer - Protected Mode

Internet Explorer - Certificates

Encrypting File System

BitLocker

- Windows 7 BitLocker Executive Overview
- Changes in BitLocker Drive Encryption
- Download details: Windows 7 Walkthrough: BitLocker and BitLocker to Go

Windows Defender

WSUS

Windows Update

Baseline Security Analyzer

- ✓ The action center is a good place to begin troubleshooting.
- ✓ Win 7 includes many built-in troubleshooters that are part of the extensible Windows troubleshooting platform
- ✓ Reliability monitor enables you to learn about the relative stability of a system in recent history
- ✓ Use startup repair, in the Recovery options in Windows recovery environment
- ✓ Use memory diagnostic to check for physical memory errors.
- ✓ Use Check disk to check for physical disk errors
- ✓ Use disk defrag to check/defrag HDD
- ✓ There are 23 troubleshooters; all are available in control panel, except devices and printers.
- ✓ Begin troubleshooting computer failures by trying to determine whether the problem is related to hardware or software.
- ✓ It helps to know the boot sequence when troubleshooting hardware/software failures.
- ✓ Steps for troubleshooting components are specific to each component.
- ✓ EFI (Extensible firmware interface) is an advanced replacement for BIOS.
- ✓ Windows network diagnostics can identify many common network problems automatically. This utility can be started from many places and it will prompt the user to run it when a network problem is detected.
- ✓ Use PING to test connectivity to a remote host, but many routers and PC's drop ICMP requests, so this utility is becoming less useful. PathPing functions similarly but also lists the routers

between you & the remote host. Use PortQry to Telnet to determine whether a remote server is listening for connections on a specific port. Use nslookup to troubleshoot DNS name resolution problems.

- ✓ You can troubleshoot problems connecting to shared folders from either the client or the server. Most often the problem is related to insufficient privileges. However, the server might be offline, windows firewall might be blocking, or network firewall might be filtering traffic.
- ✓ APIPA addresses are in the range 169.254.0.0 – 169.254.254.255. If a computer is assigned one of these addresses, it means the computer is set to receive an address from DHCP, but the server is unavailable.
- ✓ Connectivity problems can be caused by either the network or application. Network connectivity problems prevent any traffic from being sent. App connectivity problems block just the app's specific traffic. Typically, app connectivity problems occur because windows firewall exception was not created on the server or a network firewall is blocking the app's communications.
- ✓ Name resolution problems occur when both the client and server are online but the client can't determine the server's IP address. Causes can be incorrect client configuration, offline DNS server, or DNS server with incorrect IP address.
- ✓ Use ipconfig /flushdns to clear the dns cache, if changes are made.
- ✓ Wireless networks allow PC's to be connected using radio signals rather than an Ethernet cable. Wireless networks are more complex than wired networks because there are multiple security standards and wireless signal strength can vary.
- ✓ W7 includes a new user interface for connecting to wireless networks. With W7, users click the networking icon in the system tray and then click an available network.
- ✓ If network settings change, you can use the manage wireless networks tool in control panel to update them and change the priority of wireless networks.

- ✓ W7 supports several different types of network security: open – 1) which uses no security. 2) WEP, WPA-PSK, and WPA2-PSK – which use static key for authentication and encryption. 3) WPA-EAP and WPA2-EAP – which uses a RADIUS server for authentication. Additionally, you can configure wireless clients running W7 to use open security with 802.1X network authentication.

- ✓ The most common wireless network problem is turning off a mobile computer's wireless radio; this is solved by turning on the wireless radio back on. Other common problems include weak signal strength, poor network performance, incompatibilities, and wireless network settings that have changed since the network was first configured.

- ✓ You can use apps and services log\Microsoft\windows\WLAN-Autoconfig\Operational to determine which networks a user has connected to and view any problems that occurred.

- ✓ WEP uses 64 or 128 bit encryption.

- ✓ WPA is successor to WEP.

- ✓ WPA-PSK is also known as WPA-Personal, intended for home environments. Users are required to enter an 8-63 character passphrase into every wireless client. WPA converts the passphrase to a 256-bit key.

- ✓ WPA-EAP is also known as WPA-Enterprise, relies on a RADIUS server for authentication, which then authenticates the user to AD-DS or by verifying the certificate.
- ✓ WPA2 is an updated version of WPA, adding improved security.
- ✓ Open with 802.1X is network authentication used for wired networks.
- ✓ Use the printer troubleshooter to diagnose and solve common problems.
- ✓ Use the apps and services logs\Microsoft\Windows\PrintService\Admin event log to determine any printer-related events.
- ✓ You can configure GP settings to help with printer troubleshooting, especially with driver issues.
- ✓ Print servers must have both the print spooler and server services running to share printers. The most common print server problems are when the print queue stops processing print jobs; fix this restart the print spooler service.
- ✓ Troubleshoot problems connecting across the network to a shared printer by verifying that the client can resolve the name of the server, that no firewall is blocking file and printer sharing connection to the server.
- ✓ Both the print server and client must have a printer driver installed. You can update drivers from the printer properties. Reinstall any print drivers that don't install correctly.
- ✓ Using a print server offers several advantages: you can integrate with windows security, with AD DS, set up automatic installation of printer drivers, and integrate with enterprise management tools.
- ✓ Authentication is the process of identifying a user and proving the user's identity.
- ✓ Credential manager stores user's credentials to provide automatic authentication during future attempts to access resources. You can add credentials manually using the stored user names and passwords tool in control panel.
- ✓ When troubleshooting user authentication issues, you should enable failure logon auditing, reproduce the authentication problem, and examine the security event log for details of the authentication failure. When troubleshooting network authentication issues, verify that GP settings have been updated and work with network administrators to resolve the problem. If you are working with an untrusted CA, then import the CA's cert into the trusted root CA's store.
- ✓ Credential manager can store roaming user accounts passwords between computers. If you check the "remember my password" box, Cred. Manager will retrieve the password if you log onto another computer.

- ✓ Windows automatically adds credentials used to connect to shared folders to the CM. You can manually add credentials.
- ✓ Most UAC issues are authorization, rather than authentication related.
- ✓ Web application developers often use IE add-ons to extend the web browser's capabilities. Some add-ons can cause system instability or reliability issues.IE provides ways to disable add-ons and delete ActiveX controls.
- ✓ IE restricts what web sites on the public internet can do to help protect the user's security. If you access a web site that isn't working right, you can add the site to the trusted sites list.
- ✓ Protected mode is one of the most important security features of IE8, but you need vista, W7 to use it. It runs IE8 with low privileges, which reduces the access to system resources.
- ✓ Many add-ons use certs to authenticate the web server and to provide encrypted communications. Issues with certs include non-matching server host name, fix this by providing the host name on the cert. with an intranet, the client computers must trust the internal CA.
- ✓ GP gives administrators detailed control over IE features. If a user has a problem with a feature, check the configurations settings. Use RSOP and check IE nodes for any conflicts.
- ✓ Enabling ActiveX opt in causes IE to not install ActiveX controls by default, instead requiring the user to explicitly choose to configure the add-ons. It doesn't apply to pre-approved add-ons.
- ✓ Use EFS to encrypt individual files and folders. These files are unavailable if the user loses their key. Backup the keys and certs for each user.
- ✓ Use bitlocker to encrypt the entire system volume. If there is TPM available, BL makes use of it to seal the encryption key. It works with TPM hardware during computer startup to verify the integrity of the computer and operating system. If TPM hardware is unavailable, you can optionally require the user to insert a USB flash drive with special key or type a password to gain access. BL is disabled by default on computers w\o TPM hardware, but you can enable BL by using GP settings.
- ✓ EFS files are not indexed and won't be returned by a search.
- ✓ EFS encrypts files with the FEK (File encryption key), then it encrypts the FEK with the user's personal EFS key. Decryption will then require 2 separate keys. The FEK key can be encrypted multiple times for different user and each user can access their own encrypted copy of the FEK key to decrypt files.
- ✓ EFS can't encrypt system files.

- ✓ BL provides computer-specific encryption, not user-specific, so you need EFS to protect files from other valid users.
- ✓ TPM only mode: transparent to user, TPM validates the integrity of the computer and OS, if there is a change, it enters recovery mode.
- ✓ TPM with external key: same checks as TPM only mode, but the user is required to provide an external key-usually a USB flash drive.
- ✓ TMP w/PIN: user must enter a PIN to start the computer.
- ✓ TPM w/PIN and external key: the most secure mode.
- ✓ If your PC doesn't have TPM, you can manually configure by going through GP and enabling the require additional security at startup.
- ✓ UAC helps prevent malware from secretly installing itself on your computer by notifying users that a request has been made to write to protected areas of the OS.
- ✓ You can configure the behavior of UAC notifications. By default, admins see consent prompts on a secure desktop when a program requests elevation. Standard users by default see credential prompts on a secure desktop whenever they or a program request elevation.
- ✓ Malware includes viruses, worms, Trojans, spyware, adware, backdoor programs and rootkits.
- ✓ User education is essential when working with UAC.
- ✓ In a domain environment, UAC should be configured and controlled by GP. In workgroups, UAC can be configured in control panel.
- ✓ UAC has 5 notification levels: 1. **always notify**- the default for standard users. Users are notified whenever a program tries to make changes to the computer.
    - 2. **Notify me only when programs try to make changes to my computer**. This is the default for admins and is not available for standard users. Admins are not notified when they make changes that require admin privileges; however users are notified through consent prompt when a program requests elevation.
    - 3. **Always notify me (and do not dim my desktop)** this level is not available for admins. Secure desktop is never displayed. This setting reduces protection, but improves user experience.
    - 4. **Notify when only when programs try to make changes to my computer (do not dim the desktop)** this setting is available for both admins and standard users.
    - 5. **Never notify**. This level disables the UAC.

- ✓ You can configure UAC via GP: computer configuration\policies\windows settings\security settings\local policies\security options.
- ✓ Windows defender is best suited for small organizations or home users. It has 2 types of protection: 1) Automatic scanning which downloads updates from windows updates, and then performs a quick scan. 2) Real-time protection in which WD constantly monitors computer usage in areas such as startup folder, run keys in registry, windows add-ons.
- ✓ WD will prompt uses to deny (block) or permit (allow) changes.

- ✓ WD has 3 scan types: 1) **Quick scan** which scans only areas of the computer most likely to be infected with malware, areas include memory, registry settings that link to startup apps. This scan will detect most spyware. 2) **Full scan** scans every file in the computer, including archives and apps already loaded in memory. This scan can take hours. Run this scan after a quick scan if you suspect more malware present. 3) **Custom scan** begins with quick scan and then detailed scans on selected areas.

- ✓ There are 4 options for dealing with malware: 1) **ignore**: this option allows the detected spyware to remain untouched on your computer and is detectable by WD on the next scan. This option might be useful if you are researching software. 2) **Quarantine**: isolates the detected software to another location on the computer, preventing it from running until decision is made to restore or remove from the computer. This option is most often used when detected software can't be removed successfully. 3) **Remove:** deletes the detected software from your computer. 4) **Always allow:** adds the detected software to the WD allowed list, and WD stops alerting you to actions taken by the program. Choose this option if you trust the software.

- ✓ In an AD DS environment, you can configure clients using GP. Navigate to Computer configuration\Policies\Administrative Templates\Windows Components\Windows Defender

- ✓ There are 7 policies for WD to configure:

- ✓ Turn on definition updates through both WSUS and windows update
- ✓ Turn on definition updates through both WSUS and Microsoft Malware Protection center
- ✓ Check for new signatures before scheduled exams
- ✓ Turn off Windows Defender
- ✓ Turn off Real-time monitoring
- ✓ Turn off Routinely taking action
- ✓ Configure Microsoft spinet reporting

- ✓ You can use a bootable A/V CD if the computer runs so slowly you can't run the programs normally.
- ✓ Windows firewall blocks all incoming connection requests by default. You need to create exceptions for programs.
- ✓ In a windows network, a VPN infrastructure includes at least a VPN client, a VPN server running RRAS, and a DNS server. Additional elements would include a DC, CA, DHCP, and NPS servers.
- ✓ 4 VPN tunneling protocols are available in W7. They are negotiated in this order: IKEv2, SSTP, L2TP, PPTP

- ✓ IKEv2 is a new tunneling protocol that requires W7 and server 2k8 R2. An advantage of IKEv2 is the VPN reconnect, it allows for improved client mobility and automatic reconnection.
- ✓ To attempt a VPN connection, a VPN client first contacts the VPN server with a request for tunneling protocol, which is negotiated, tunnel created, and remote access authentication of the user and (sometimes the computer) follows. Once authorization is complete, the VPN connection is established.
- ✓ Only IKEv2 supports VPN reconnect
- ✓ SSTP can be used by clients running Vista SP1 or later. Based on the same HTTP over SSL protocol used for secure web sites. It only uses port 443, which is left open by most firewalls. It also allows for access through NAT devices, firewalls, and web proxies. Does not require client computer configuration by default, but it can be set.
- ✓ L2TP/IPSec requires client computer configuration. You can use a certificate or pre-shared key.
- ✓ PPTP is the easiest to configure. Doesn't require certificates, not as secure as other VPNs.
- ✓ Direct Access is a new technology that replaces a traditional VPN. It enables remote clients running W7 Enterprise or Ultimate to establish and always-on, IPSec, IPv6 connection.
- ✓ Computers rely on Teredo, 6to4, ISATAP, and IP-HTTPS if IPv4 is being used.
- ✓ Direct Access infrastructure includes a DA server, client, DCs, network location server, and PKI.
- ✓ To establish a DA connection, a client first determines its location by attempting to contact the network location server. If the client determines it's on the internet, it attempts to contact the DA server over IPv6 (using a transition technology if necessary). It creates an IPSec tunnel, validates the client, and establishes the connection.
- ✓ VPN client machines are typically not subject to GP.
- ✓ Internet performance is slowed if both internet and intranet traffic is going through the VPN connection.
- ✓ Benefits of DA include always on technology, seamless connectivity, bidirectional access, enhanced security.
- ✓ ISATAP is a tunneling protocol that allows an IPv6 network to communicate with an IPv4 network through an ISATAP router. IPv4 and IPv6 hosts can communicate with each other.
- ✓ 6to4 is a protocol that tunnels Ipv6 traffic over IPv4 through 6to4 routers. 6to4 clients have their routers IPv4 address embedded in their IPv6 address. Intended for use on the internet.
- ✓ Teredo is a tunneling protocol that allows clients located behind an IPv4 device to use IPv6 over the internet. Teredo is used only when no other IPv6 transition technology is available.
- ✓ IP-HTTPS enables hosts located behind web proxy server or firewall to establish connectivity by tunneling IPv6 packets inside an HTTPS session.
- ✓ Network location server is a web server accessed by DA client to determine whether the client is located on the intranet or internet. DA server can act as NLS, but it's better to have them separate.
- ✓ Perimeter firewall exceptions. Open the following ports to support DA: UDP 3544 to enable inbound teredo traffic, IPv4 protocol 41 to enable inbound 6to4 traffic, TCP port 443 to allow inbound IP-HTTPS traffic.
- ✓ If clients have native IPv6 addresses, the following exceptions are needed: ICMPv6, IPv4 protocol 50
- ✓ Microsoft provides 3 ways for distributing updates: 1) the windows update client, 2) WSUS, 3) configuration manager for enterprises.
- ✓ Test all updates in a test lab before deploying to production network

- ✓ You can verify that an update is installed on a single computer by viewing the update history. If you use WSUS in your organization, you can view the reports that WSUS provides to identify which computers have installed an update. If you need to audit computers, use the MBSA tool.
- ✓ You can install updates interactively using the windows update tool in control panel, but this takes forever. Use GP instead.
- ✓ If you have a problem installing an update, you can diagnose the problem by viewing the windows update history by analyzing the %Windir%\WindowsUpdate.log file.
- ✓ You can rename updates manually or via WSUS.
- ✓ Install updates immediately on new computers to protect them.
- ✓ Event forwarding uses HTTP by default, allowing it to pass through most firewalls and the communication is encrypted.
- ✓ To configure event forwarding in a domain, run the winrm quickconfig command at the forwarding computer and run the wecutil qc command on the collecting computer. Then add the collecting computers account to the forwarding computer's event log reader's group.
- ✓ Allow enough time for event forwarding, subscriptions are active, check windows remote management configuration on the forwarding and collecting computers.
- ✓ Event forwarding sends communications encrypted with the Microsoft negotiate security support (SSP) in workgroups, or Microsoft Kerberos SSP in domains.
- ✓ For the exam remember that event forwarding uses encryption even if you choose the HTTP protocol.
- ✓ Event forwarding needs the windows remote management and windows event collector services running.
- ✓ For the exam remember that you must configure the TrustedHosts parameter on the collecting computer, not the forwarding computer.
- ✓ Task manager provides a quick way to examine a computer's performance and solve some performance problems. With TM, you can identify which processes are consuming the most resources and either lower the priority of those processes or end them
- ✓ You can use performance monitor to analyze system statistics in real time or you can use to analyze data logged using a data collector set.
- ✓ Data collector sets and reports gather performance and configuration data about a computer and enable you to analyze that info easily using reports or performance monitor.
- ✓ Disk performance problems are most often caused by low disk space and fragmentation. W7 automatically defragments disks that need it.
- ✓ If a startup program is causing performance problems, you can use the msconfig.exe tool to prevent it from starting. You can easily re-enable apps later if necessary.
- ✓ Task manager has 6 tabs: **Applications, processes, services, performance, networking, users**.
- ✓ You can create data collector sets (DCS) to log the following information: Performance counters and alerts, event trace data, and registry settings.
- ✓ There are several built-in DCS under system performance and system diagnostics.
- ✓ If an app malfunctions after is has been working correctly, the problem is usually a result of a configuration error or system change. Strategies to fix include system restore, backups, repairing or reinstalling the app, reviewing event logs.
- ✓ Each new release of windows introduces features that affect the functionality of programs written for earlier OS. With W7, the features likely to affect app compatibility include UAC, Windows resource protection, and new system APIs.

- ✓ W7 includes tools that help detect and mitigate compatibility problems for older apps. The PCA automatically appears when W7 detects known compatibility issues. The program compatibility troubleshooter is a wizard that enables you to run an older program with settings used in a previous version of windows. You can configure these same compatibility settings on the compatibility tab of the program.
- ✓ If you need to support and app that is not compatible with W7, you can run the program in a compatible OS within a virtual machine.
- ✓ W7 includes several GP settings that allow you to determine how the PCA will diagnose and troubleshoot app compatibility problems.
- ✓ Windows firewall is a host firewall built into W7.
- ✓ You can configure WF by accessing control panel. You can access WFAS by clicking advanced settings on firewall page.
- ✓ WF inspects all incoming packets and compares them against this list of allowed traffic. If a packet matches an entry in the exception list, WF passes the ticket to the TCP/IP protocol stack, if not then vice versa.
- ✓ By default, WF allows all outbound connections from the local computer, but you can deny connections you need to.
- ✓ There are 4 network locations: Domain, work, home, public.
- ✓ Network discovery is a multicast protocol, and is disabled public and domain network locations
- ✓ Network locations can be set automatically or manually.
- ✓ Windows firewall logging is not enabled by default.
- ✓ You can use event viewer to monitor issues. There are 4 event logs you can look at: ConnectionSecurity, ConnectionSecurityVerbose, Firewall, FirewallVerbose
- ✓ Offline files allow you to keep local copies of files stored on a network share.
- ✓ Offline files improve the availability, reliability, and performance of network shares.
- ✓ If you are working online, your local copy of the file synchronizes with the newest version when you open the file.
- ✓ You should synchronize your files manually before going offline if you plan to work with files that have been modified by other users.
- ✓ When you make a shared file or folder available offline, windows automatically creates a copy of that file/folder on your computer. W7 then automatically synchronizes the 2 versions of the file/folder in the following instances: 1) if you are working online and save changes to the file, 2) working online and open the file, 3) if you start the computer when disconnected from network, edit the files, and later reconnect to the network folder containing those files, 4) if while connected to the network, you choose the option to work offline and later choose the option to work online again – synchronization will not be immediate in this case. 5) If the connection is abruptly broken and reset.
- ✓ You can use the sync center to manage and setup synchronization. You can choose to synchronize at a scheduled time or when an event occurs. Both of these options have additional options available.
- ✓ You can manage disk space for offline files, click change limits
- ✓ Offline files can be configured through GP. There are 28 settings available in the computer configuration and 15 for user configuration.
- ✓ Most of these settings are reserved for use in OS versions before Vista.
- ✓ There are 10 GP settings that affect offline files in W7.
  1. Administratively assigned offline files: allows you to enforce specific network shares.
  2. Configure background sync: allows for custom synchronization over slow-links.

3. Limit disk space used by offline files.
4. Allow / disallow use of offline files feature
5. Encrypt the offline files cache: in the client side cache
6. Exclude files from being cached: you can specify file types you don't want to make offline
7. Remove "make available offline": this removes the make available option from shortcut menus.
8. Enable transparent caching: used to force clients to cache temporarily any network file opened over a slow link. Improves response times and decreases bandwidth usage.
9. Turn on economical application of administrative assigned offline files:
10. Configure slow-link mode: allows you to determine when clients use slow-link mode. Enabled by default when latencies reach 80 milliseconds.

- ✓ Previous versions allow you to restore earlier versions of files worked on.
- ✓ You have the option of copy and replace, don't copy, or copy, but keep both files.
- ✓ Windows makes available only files/folders saved from restore points and backups.
- ✓ Restore points are created by the system protection feature, which is enabled on system volumes by default.
- ✓ When you restore a previous version, it can't be undone.
- ✓ User profiles are stored in the C:\Users folder by default
- ✓ There have been some changes in the file structure since XP.
  1. Root of profile namespace has changed from %systemdrive%\Documents and Settings to %systemdrive%\Users
  2. My prefix has been dropped from some folders.
  3. My music, pictures, videos are no longer subfolders of my documents.
  4. New subfolders have been added under the root profile folder to organize. They are contacts, downloads, searches, links, saved games.
  5. There is a hidden folder named AppData that stores per user settings and binaries
  6. All users folder has been renamed to Public
  7. Default user is now default

- ✓ Background registry roaming is disabled by default in W7. You can turn it on in GP. Go to computer configuration\policies\administrative Templates\System\user profiles\background upload of a user profile's registry while user is logged on.

- ✓ Folder redirection allows you to change the target location of user profile folders in a way that is transparent to the user. Folder redirection offers some advantages over roaming profiles:

  1. Compatibility between W7 and earlier versions of windows
  2. Faster logons
  3. Real-time data synchronization
  4. Network problems do not disperse data
  5. Folder redirection can be automated through GP

- ✓ There are several settings for folder redirection:
  1. Not configured,

2) Basic: redirects the selected folder to the same share for all users.

3) Advanced: redirects selected folders to different locations for different security groups. For example you would move sales folders to the sales file server.

- ✓ Follow the documents folder allows the music, pictures, and videos to follow the documents folder.
- ✓ There are 4 options for target folder locations:
  1. Create a folder for each user under the root path
  2. Redirect to the following location
  3. Redirect to the local user profile location
  4. Redirect to the user's home directory
- ✓ A roaming profile is a profile stored centrally on a network share. It is configured in the properties of the user account in AD DS.
- ✓ Setup automatically installs the Windows Recovery Environment (WRE) which includes the startup repair tool.
- ✓ Ntldr has been replaced with the windows boot manager and boot loader.
- ✓ Boot.ini has been replaced with the boot configuration data (BCD) registry file.
- ✓ Ntdetect.com has been merged into the kernel.
- ✓ Hardware profiles are no longer required.
- ✓ The recovery console is replaced by the graphical WinRE.
- ✓ The BCD is stored in a data file that uses the same format as the registry and is located on the EFI system partition or on system volume.
- ✓ You can modify the BCD in the following ways:
  1. Startup and recovery
  2. Msconfig.exe
  3. BCD windows management instrumentation provider
  4. BCDEdit.exe
  5. Non-microsoft tools
- ✓ Startup recovery tools include startup repair, system restore, system image recovery, windows memory diagnostic, command prompt tools.
- ✓ W7 startup sequence is as follows:
  1. POST
  2. Initial startup phase
  3. Windows boot manager phase
  4. Windows boot loader phase
  5. Kernel loading phase
  6. Logon phase
- ✓ Initial startup for EFI computers differs from BIOS computers. EFI have a built-in boot manager that enables the computer's hardware to choose from multiple OS based on user input.
- ✓ Some of the important startup files include: BootMgr, WinLoad, BCD, Ntoskrnl.exe, Hal.dll, Smss.exe, Csrss.exe, Winlogon.exe,Services.exe, Lsass.exe, System registry, device drivers.
- ✓ Msconfig has the following tabs: general, boot, services, startup and tools.
- ✓ Last known good configuration registry key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet

- ✓ Startup problems can be divided into 3 categories:
  1. Problems that occur before the starting windows logo appears.

2. Problems that occur after the starting windows logo appears, but before the logon prompt is displayed.
3. Problems that occur after logon

- ✓ Use device manager to roll back/update drivers.
- ✓ Use sigverif to verify if drivers are signed, unsigned, or view certs of signed files.
- ✓ Use msconfig to temporarily disable a service while troubleshooting
- ✓ You can manually repair the boot sector by typing bootsect /NT60 ALL. If you have earlier versions of windows on your computer, you will need to add entries to the BCD registry file.
- ✓ Windows troubleshooting platform acts as wizard to help users resolve issues.
- ✓ It has built-in troubleshooting packs to correlate to the top 10 categories of MS support calls.
- ✓ The troubleshooting packs are as follows:
  1. Aero
  2. Playing audio
  3. Recording audio
  4. Printer
  5. Performance
  6. System maintenance
  7. Power
  8. Home group
  9. Hardware and devices
  10. IE performance
  11. IE safety
  12. Windows media player library
  13. Windows media player settings
  14. Media player DVD
  15. Connect to workplace with Direct Access
  16. Shared folders
  17. Incoming connections
  18. Network adapters
  19. Internet connections
  20. Program compatibility
  21. Search and indexing
  22. Windows update

- ✓ You can use powershell to remotely run these troubleshooting packs. Example for aero

```
Import-Module TroubleshootingPack
$aero = Get-TroubleshootingPack $env:SystemRoot\Diagnostics\System\Aero
Invoke-TroubleshootingPack –Pack $aero –Result C:\DiagResult –unattend
```

- ✓ Use resource monitor to view processes, networking data, services, handles, registry keys, files accessed.
- ✓ W7 has self-healing NTFS which can detect and fix file system corruption while the OS is running. It is similar to check disk, but doesn't lock up the volume. Enabled by default.
- ✓ If self-healing fails, the volume is marked as "dirty" and windows will run chkdsk on the next startup.

- ✓ Windows memory diagnostic has 3 levels: Basic, standard, and extended. You can schedule the diagnostic to run on the next startup. You can configure 0-99 passes for each test.
- ✓ Driver verifier or verifier.exe can help isolate a driver causing issues.
- ✓ USB issues include insufficient power, cables too long, too many devices, low bandwidth.
- ✓ If using performance monitor to troubleshoot USB, add these counters: iso Packet Errors/sec, Transfer errors/sec, bulk bytes/sec, avg. bytes/sec.
- ✓ Enhanced = USB 2.0
- ✓ DiskView shows how files are 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/folder open. You can use this to delete or update a file/folder when access is denied, because the object is in use.
- ✓ Process Monitor will monitor file and registry accesses by application.
- ✓ **Some clients can't connect to a server**: Arp, ipconfig, nbtstat, netstat, network monitor, nslookup, pathping, PortQry, Telnet Client, Windows network diagnostics
- ✓ **No clients can't connect to a server**: ipconfig, network monitor, PortQry, telnet client, windows network diagnostics.
- ✓ **Clients can't connect to shared resources**: ipconfig, nbtstat, net, nslookup, network monitor, PortQry, Telnet client, windows network diagnostics.
- ✓ **Clients can't connect to the network**: ipconfig, windows network diagnostics
- ✓ **Network performance is poor or unpredictable**: network monitor, performance monitor, pathping, resource monitor, task manager.
- ✓ **Arp**: command line tool.
- ✓ **Event viewer**: look in the windows logs\system and applications and services logs\Microsoft\Windows\Diagnostics-Networking\Operational
- ✓ **Ipconfig**: command line tool that shows detailed information about network configurations.
- ✓ **Nblookup**: tool for diagnosing WINS name resolution problems.
- ✓ **Nbtstat:** tool for troubleshooting NetBIOS name resolution issues, session layer protocol. Applications identify services on the network by using the 16-character NetBIOS names.
- ✓ **Net**: command-line tool that is useful for changing network configuration settings, starting and stopping services and viewing shared resources and their names.
- ✓ **Net share** command to view shared resources located on local computer.
- ✓ **Net view** command will show shared resources located on another computer.
- ✓ **Netstat**: for identifying network services and the ports they listen on, good for verifying the network service is using the expected port.
- ✓ **Netstat** will display a list of listening ports as well as outgoing connections and the process Identifiers associated with each listener or connection.
- ✓ **Network monitor**: a free download for analyzing network communications. It's a protocol analyzer or sniffer that can capture bytes transferred to or from a computer running W7.
- ✓ Network monitor can troubleshoot network performance problems, TCP connections, IP protocol stack, network filtering issues, application layer issues.
- ✓ **Nslookup**: primary tool for isolating DNS name resolution problems. Performs DNS lookups and provides a report on the results, showing the DNS server used to resolve the request.
- ✓ The Hosts file might contain static entries that could override DNS lookups for most applications. Nslookup ignores this file. %Windir%\System32\Drivers\Etc is location.
- ✓ Use nslookup *host*name or nslookup ip address
- ✓ **PathPing:** useful tool for isolating connectivity problems from the client. Can diagnose problems with name resolution, network connectivity, routing, and network performance.

- ✓ Use PathPing *destination*. The usefulness is degrading as pings are not always allowed through firewalls now.
- ✓ PathPing displays its output in 2 sections: the first shows a numbered list of all devices that responded. The 2nd list shows statistics.
- ✓ You can use PathPing to detect routing loops
- ✓ **Performance monitor**: shows 1000's of counters with information about the local computer or remote computer. Shows current bandwidth usage.

- ✓ Can be useful in troubleshooting issues with:
  1. .NET CLR networking
  2. BITS Net Utilization
  3. Browser
  4. ICMP and ICMPv6
  5. IPSec AuthIPv4, IPSec AuthIPv6, IPsec driver, IPSec IKEv4, IPSec IKEv6
  6. IPv4 and IPv6
  7. NBT connection
  8. Network interface
  9. Redirector
  10. Server
  11. TCP v4 and v6 and UDP v4 and v6

- ✓ Data collector sets: both the system diagnostic and system performance data collector sets. They will show the following information:
  1. Computer make and model
  2. OS version
  3. List of all services, current states, and their PIDs
  4. Network adapter driver information and networking system files and versions.
  5. Processor , disk, network, and memory utilization
  6. Total bandwidth of each network adapter
  7. Packets sent and received
  8. Active TCPv4, v6 connections.

- ✓ Resource monitor allows you to view processor, disk, network, and memory utilization.
- ✓ PING is becoming less useful as ICMP requests are dropped, you can use ping –t to continuously submit requests to check on connectivity.
- ✓ PortQry: not included with W7, but can be downloaded from M$. It's a TCP connectivity utility that helps identify the port # for services. Provides support for UDP as well.
- ✓ PortQry can test the following UDP ports:
  1. LDAP
  2. RPC's
  3. DNS
  4. NetBIOS name service
  5. SNMP
  6. ISA
  7. SQL server
  8. TFTP
  9. L2TP

- ✓ Route: used to diagnose routing problems. C:\>route print produces a routing chart.
- ✓ Task Manager: a GUI tool used to view, end processes, end applications, view networking information, log off users, view services.
- ✓ TCP View: used to view which servers a client connects to, including port #'s, or identify clients connecting to a server.
- ✓ Telnet client: can determine whether TCP-based network services are reachable from a client, including web, mail, or file transfer services.
- ✓ Test TCP: allows you to initiate and test for TCP connections and UDP.
- ✓ Windows network diagnostic: helps users diagnose and resolve network problems via a wizard.
- ✓ Networking connectivity problems include: failed network adapters, network hardware, connections, cables, misconfigured network hardware and adapters.
- ✓ You can use the Hosts file as another name resolution method. It is a text file, editable with notepad.

- ✓ Name resolution problems include:
  1. DNS servers have failed.
  2. Network connecting the client to the DNS server has failed.
  3. Host name is missing from DNS database
  4. A host name is associated with incorrect IP address. Often this happens because a host has recently changed its IP address and DNS database has not been updated.
  5. The client does not have DNS servers configured or is misconfigured.

- ✓ Use the NetSetup.log file to troubleshoot domain change problems.
- ✓ With network discovery, users can browse shared network resources. These services need to be running: Function discovery provider. Set exceptions in WF, change network type to private.
- ✓ When troubleshooting stop errors, try to get the error #, error parameters, driver information if available.
- ✓ Stop messages report information about stop errors. They will have the following information:
  1. Bugcheck information
  2. Recommended user action
  3. Technical information
  4. Driver information
  5. Debug port and dump status

- ✓ Types of stop errors include: faulty hardware, hardware issues, executive initilialization stop errors, installation errors that occur during setup.
- ✓ Memory dump files write information to the paging file (pagefile.sys)
- ✓ Small memory dumps, aka minidump files.
- ✓ Kernel memory dump files record the contents of kernel memory.
- ✓ Complete memory dump files record the entire contents of physical memory when the stop error occurred.
- ✓ You can prevent the system from restarting after an error by using msconfig.exe

Event Types Defined:

- **Application events**- These events are either classified as error, warning, or information, depending on the severity of the event. An error is a significant problem, such as loss of data. A warning is an event that is not necessarily significant, but might indicate a possible future problem. An information event describes the successful operation of a program, driver, or service.
- **Security-related events** - These events are called audits and are described as successful or failed, depending on the event, such as whether a user trying to log on to Windows was successful.
- **Setup events** - Computers that are configured as domain controllers will have additional logs displayed here.
- **System events** - System events are logged by Windows and Windows system services, and are classified as error, warning, or information.
- **Forwarded events** - These events are forwarded to this log by other computers.
- **Applications and Services Logs vary** - Applications and Services logs are a new category of event logs. They include separate logs about the programs that run on your computer, as well as more detailed logs that pertain to specific Windows services.

70-685 Study Guide

to be used as an internal resource only