Microsoft

Exam 70-680

TS: Windows 7, Configuring

Version: 36.0

[Total Questions: 564]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	99
Topic 4: Volume D	100
Topic 5: Volume E	100
Topic 6: Volume F	65

Topic 1, Volume A

Question No : 1 - (Topic 1)

Your company has an Active Directory domain. All computers are members of the domain.

Your network contains an internal Web site that uses Integrated Windows Authentication.

From a computer that runs Windows 7, you attempt to connect to the Web site and are prompted for authentication.

You verify that your user account has permission to access the Web site.

You need to ensure that you are automatically authenticated when you connect to the Web site.

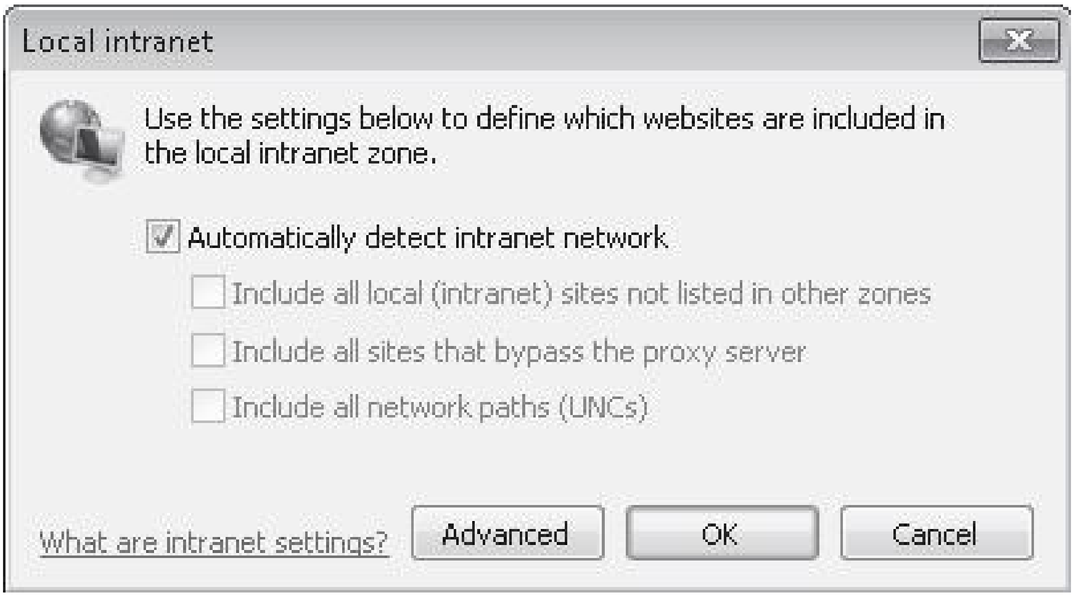
What should you do?

A. Create a complex password for your user account.
B. Open Credential Manager and modify your credentials.
C. Add the URL of the Web site to the Trusted sites zone.
D. Add the URL of the Web site to the Local intranet zone.

Answer: D

Explanation:

Local Intranet Sites in the Local Intranet zone are computers on your organizational intranet. Internet Explorer can be configured to detect intranet sites automatically. It is also possible to add Web sites to this zone by clicking the Advanced button on the Local Intranet sites dialog box, as shown in the figure. The default security level of this zone is Medium-Low. Protected Mode is not enabled by default for sites in this zone.



Local intranet

Use the settings below to define which websites are included in the local intranet zone.

☑ Automatically detect intranet network

□ Include all local (intranet) sites not listed in other zones

□ Include all sites that bypass the proxy server

□ Include all network paths (UNCs)

Security settings are configured primarily by assigning sites to zones. Sites that require elevated privileges should be assigned to the Trusted Sites zone. Sites that are on the intranet are automatically assigned to the Local Intranet zone, though this may require manual configuration in some circumstances. All other sites are assigned to the Internet zone. The Restricted Sites zone is used only for Web sites that may present security risks but must be visited.

Question No : 2 - (Topic 1)

You have a computer that runs Windows 7.

You need to configure the computer to download updates from a local Windows Server Update Services (WSUS) server. What should you do?

A. From Windows Update, modify the Windows Update settings.
B. From the local Group Policy, modify the Windows Update settings.
C. From the System settings, modify the System Protection settings.
D. From the local Group Policy, modify the Location and Sensors settings.

Answer: B

Question No : 3 - (Topic 1)

You have a computer that runs Windows Vista Service Pack 2 (SP2).

You need to upgrade the computer to Windows 7.

What should you do?

A. Start the computer from the Windows 7 installation media and select the Upgrade option.
B. Start the computer from the Windows 7 installation media and select the Custom (advanced) option.
C. From Windows Vista, run Setup.exe from the Windows 7 installation media and select the Upgrade option.
D. From Windows Vista, run Setup.exe from the Windows 7 installation media and select the Custom (advanced) option.

Answer: C

Explanation:

Upgrading Windows Vista to Windows 7 instructionsAccess the Windows 7 installation source and double-click Setup.exe. When prompted by User Account Control, click Allow. This loads the Install Windows page. Click Install Now.Other NotesYou can upgrade computers running Windows Vista to Windows 7. When you upgrade from Windows Vista to Windows 7, all documents, settings, applications, and user accounts that existed on the computer running Windows Vista are available when the upgrade is finished. The advantage to an upgrade is that it allows you to keep the current application configuration. When you perform a migration, you need to reinstall the user’s applications on the new computer. As mentioned previously, this can be problematic in organizations that are not careful about keeping track of which specific set of applications are installed on each user’s computer. Prior to attempting to perform the upgrade from Windows Vista to Windows 7, you should run the Windows 7 Upgrade Advisor. The Windows 7 Upgrade Advisor is an application that you can download from Microsoft’s Web site that will inform you if Windows 7 supports a computer running the current hardware and software configuration of Windows Vista. Prior to running the Windows 7 Upgrade Advisor, you should ensure that all hardware that you want to use with Windows 7, such as printers, scanners, and cameras, are connected to the computer. The Upgrade Advisor generates a report that informs you of which applications and devices are known to have problems with Windows 7. A similar compatibility report is generated during the upgrade process, but the version created by the Windows 7 Upgrade Advisor is more likely to be up to date.

Question No : 4 - (Topic 1)

In which of the following scenarios must you perform a migration rather than an upgrade? Choose three.

A. Windows XP Professional (x64) to Windows 7 Professional (x64)
B. Windows Vista Business (x86) to Windows 7 Professional (x64)
C. Windows Vista Enterprise (x64) to Windows 7 Enterprise (x64)
D. Windows Vista Home Premium (x64) to Windows 7 Home Premium (x86)

Answer: A,B,D

Question No : 5 - (Topic 1)

You have a computer that runs Windows 7.

You need to prevent Internet Explorer from saving any data during a browsing session.

What should you do?

A. Disable the BranchCache service.
B. Modify the InPrivate Blocking list.
C. Open an InPrivate Browsing session.
D. Modify the security settings for the Internet zone.

Answer: C

Explanation:

InPrivate Mode consists of two technologies: InPrivate Filtering and InPrivate Browsing. Both InPrivate Filtering and InPrivate Browsing are privacy technologies that restrict the amount of information available about a user’s browsing session. InPrivate Browsing restricts what data is recorded by the browser, and InPrivate Filtering is used to restrict what information about a browsing session can be tracked by external third parties.

Question No : 6 - (Topic 1)

You want to prohibit read, write, and execute access to all types of external storage devices.

What computer policy setting do you enable?

A. All Removable Storage: Allow Direct Access In Remote Sessions
B. All Removable Storage Classes: Deny All Access
C. Removable Disks: Deny Read Access
D. Removable Disks: Deny Write Access

Answer: B

Question No : 7 - (Topic 1)

You have a computer that runs Windows 7.

You need to view the processes that currently generate network activity.

What should you do?

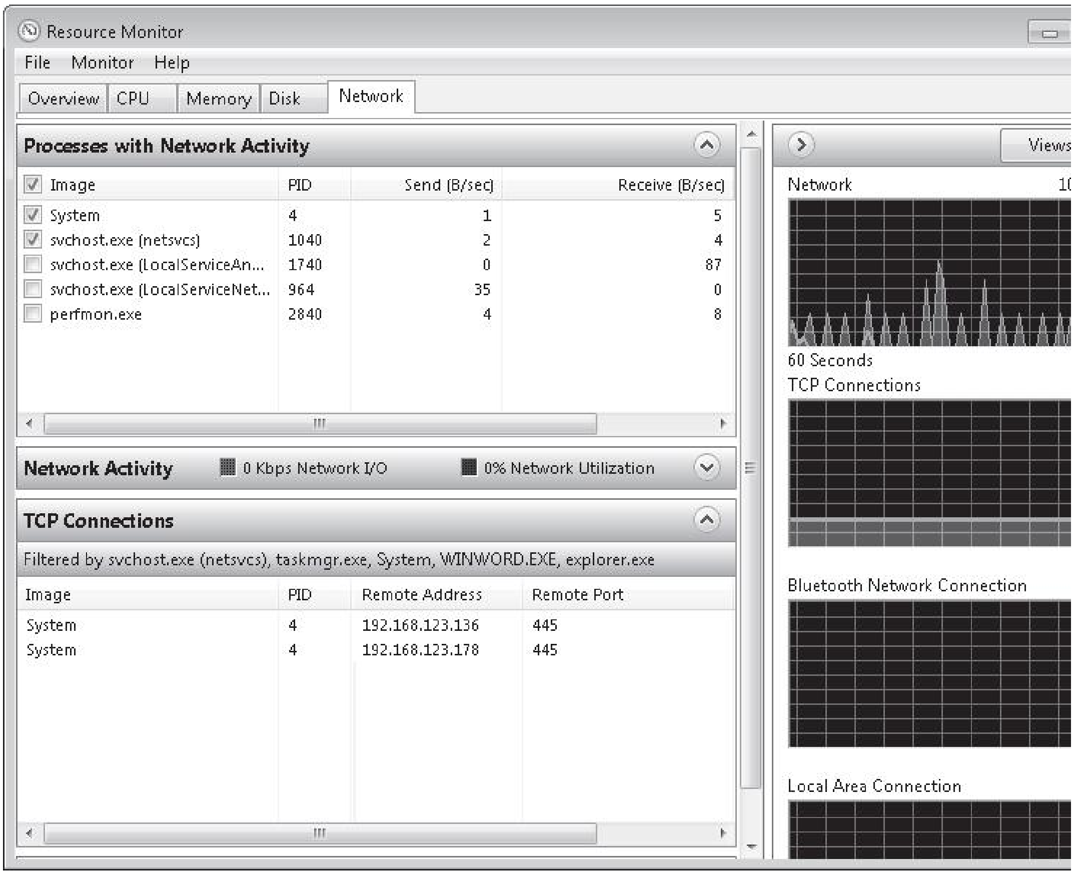
A. Open Resource Monitor and click the Network tab.
B. Open Windows Task Manager and click the Networking tab.
C. Open Event Viewer and examine the NetworkProfile Operational log.
D. Open Performance Monitor and add all the counters for network interface.

Answer: A

Explanation:

Resource Monitor

Windows 7 offers an enhanced version of the Resource Monitor tool. Windows 7 Resource Monitor allows you to view information about hardware and software resource use in real time. You can filter the results according to the processes or services that you want to monitor. You can also use Resource Monitor to start, stop, suspend, and resume processes and services, and to troubleshoot unresponsive applications. You can start Resource Monitor from the Processes tab of Task Manager or by entering resmon in the Search box on the Start menu. To identify the network address that a process is connected to, click the Network tab and then click the title bar of TCP Connections to expand the table. Locate the process whose network connection you want to identify. You can then determine the Remote Address and Remote Port columns to see which network address and port the process is connected to.



Processes with Network Activity

☑ Image	PID	Send (B/sec)	Receive (B/sec)
☑ System	4	1	5
☑ svchost.exe (netsvcs)	1040	2	4
□ svchost.exe (LocalServiceAn...	1740	0	87
□ svchost.exe (LocalServiceNet...	964	35	0
□ perfmon.exe	2840	4	8

Network Activity ■ 0 Kbps Network I/O ■ 0% Network Utilization

TCP Connections

Filtered by svchost.exe (netsvcs), taskmgr.exe, System, WINWORD.EXE, explorer.exe

Image	PID	Remote Address	Remote Port
System	4	192.168.123.136	445
System	4	192.168.123.178	445

Question No : 8 - (Topic 1)

You have a wireless access point that is configured to use Advanced Encryption Standard (AES) security. A pre-shared key is not configured on the wireless access point.

You need to connect a computer that runs Windows 7 to the wireless access point.

Which security setting should you select for the wireless connection?

A. 802.1x
B. WPA-Personal
C. WPA2-Enterprise
D. WPA2-Personal

Answer: C

Explanation:

WPA and WPA2 indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. WPA2 enhances WPA, which in turn addresses weaknesses in the previous system, WEP. WPA was intended as an intermediate measure to take the place of WEP while an IEEE 802.11i standard was prepared. 802.1X provides port-based authentication, which involves communications between a supplicant (a client computer), an authenticator (a wired Ethernet switch or WAP), and an authentication server (typically a Remote Authentication Dial In User Service, or RADIUS, server).

WPA2-Enterprise

WPA-Enterprise and WPA2-Enterprise authenticate through the Extensible Authentication Protocol (EAP) and require computer security certificates rather than PSKs. The following EAP types are included in the certification program:

- EAP-TLS
- EAP-TTLS/MSCHAPv2
- PEAPv0/EAP-MSCHAPv2
- PEAPv1/EAP-GTC
- EAP-SIM

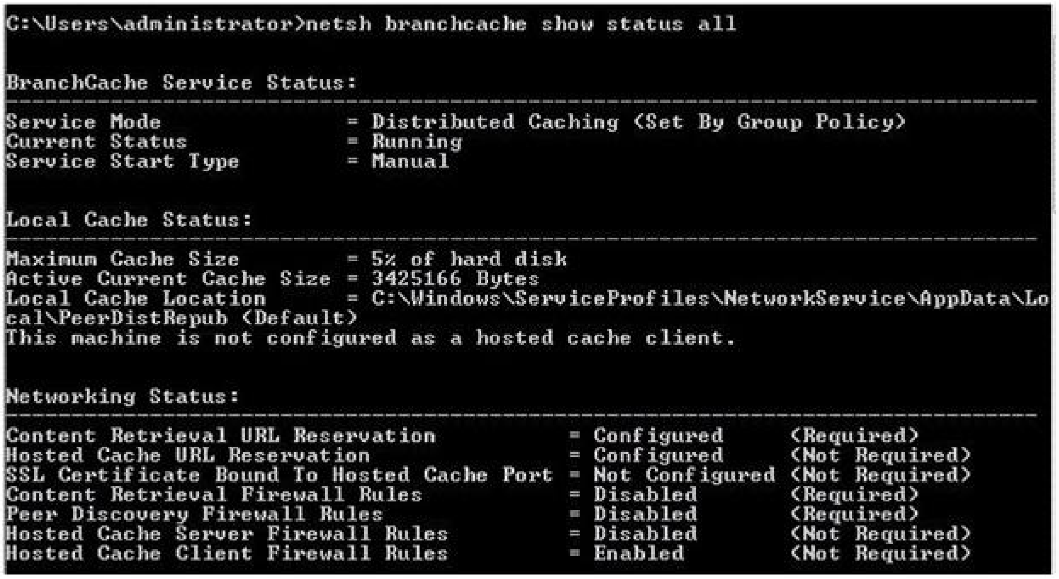
If you want to use AES and to use computer certificates rather than a PSK, you would choose WPA2- Enterprise.WPA2-PersonalIf you have a small network that is not in a domain and cannot access a CA server, but you install a modernWAP that supports AES, you would use WPA2-Personal (with a PSK).WPA-Personal

If you have a small network that is not in a domain and cannot access a CA server and your WAP does not support AES, you would use WPA-Personal.802.1x

If you have a RADIUS server on your network to act as an authentication server and you want the highest possible level of security, you would choose 802.1X.

Question No : 9 - (Topic 1)

Your network has a main office and a branch office. The branch office has computers that run Windows 7. A network administrator enables BranchCache in the main office. You run Netsh on your computer as shown in the exhibit. (Click the Exhibit button.)



```
C:\Users\administrator>netsh branchcache show status all

BranchCache Service Status:
----------------------------------------------------------------------------
Service Mode                = Distributed Caching (Set By Group Policy)
Current Status              = Running
Service Start Type          = Manual

Local Cache Status:
----------------------------------------------------------------------------
Maximum Cache Size          = 5% of hard disk
Active Current Cache Size = 3425166 Bytes
Local Cache Location        = C:\Windows\ServiceProfiles\NetworkService\AppData\Lo
cal\PeerDistRepub (Default)
This machine is not configured as a hosted cache client.

Networking Status:
----------------------------------------------------------------------------
Content Retrieval URL Reservation          = Configured     (Required)
Hosted Cache URL Reservation               = Configured     (Not Required)
SSL Certificate Bound To Hosted Cache Port = Not Configured (Not Required)
Content Retrieval Firewall Rules           = Disabled       (Required)
Peer Discovery Firewall Rules              = Disabled       (Required)
Hosted Cache Server Firewall Rules         = Disabled       (Not Required)
Hosted Cache Client Firewall Rules         = Enabled        (Not Required)
```

You need to ensure that other computers in the branch office can access the cached content on your computer.

What should you do?

A. Turn on Internet Information Services (IIS).
B. Configure the computer as a hosted cache client.
C. Configure the BranchCache service to start automatically.
D. Modify the Windows Firewall with Advanced Security rules.

Answer: D

Explanation:

Distributed Cache Mode

Distributed Cache mode uses peer caching to host the branch office cache among clients running Windows 7 on the branch office network. This means that each Distributed Cache mode client hosts part of the cache, but no single client hosts all the cache. When a client running Windows 7 retrieves content over the WAN, it places that content into its own cache. If another BranchCache client running Windows 7 attempts to access the same content, it is able to access that content directly from the first client rather than having to retrieve it over the WAN link. When it accesses the file from its peer, it also copies that file into its own cache. When you configure BranchCache in distributed cache mode, BranchCache client computers use the Hypertext Transfer Protocol (HTTP) for data transfer with other client computers. BranchCache client computers also use the Web Services Dynamic Discovery (WS-Discovery) protocol when they attempt to discover content on client cache servers. You can use this procedure to configure client firewall exceptions to allow incoming HTTP and WS-Discovery traffic on client computers that are configured for distributed cache mode. You must select Allow the connection for the