Lesson 4: Managing Applications, Services, and Disks

**Multiple Choice**

1. Which of the following gives you a quick glance at performance and provides information about programs and processes running on your computer?

a) EFS

c) Task Manager

d) Performance Monitor

d) None of the above

Answer: b

Difficulty: Medium

Section Reference: Managing Processes and Applications with Task Manager

Explanation: Task Manager gives you a quick glance at performance and provides information about programs and processes running on your computer.

2. Which of the following is a collection of settings stored in Active Directory on a Windows network?

a) Certificate store

b) Library

c) Group Policy

d) EFS

Answer: c

Difficulty: Medium

Section Reference: Understanding Group Policy and Network Application Installation

Explanation: Group Policy is a collection of settings (policies) stored in Active Directory on a Windows network. Group Policy affects users and computers contained in sites, domains, and organizational units.

3. Which of the following handles requests for print spooling, file indexing, task scheduling, and the Windows Firewall?

a) Dependencies

b) Services

c) Encryption keys

d) NTFS

Answer: b

Difficulty: Easy

Section Reference: Understanding Services

Explanation: Services run in the background, essentially helping the operating system work with other programs. Although services do not usually have user interfaces, you can manage services through the Microsoft Management Console (MMC) Services snap-in.

4. Which of the following can you perform using Group Policy? (Choose all that apply.)

a) Update an application

b) Install applications from a network location

c) Restrict user access to an application

d) Encrypt a user’s files

Answer: a, b, c

Difficulty: Hard

Section Reference: Understanding Group Policy and Network Application Installation

Explanation: In a Windows network in a domain environment, administrators can use Group Policy to ease the burden of administering and managing many users and client computers. Group Policy enables you to control who may install software, and on which computers, and helps you push software updates and security configurations across the network. In addition, Group Policy enables you to restrict user access to an application. You do not use Group Policy to encrypt a user’s files.

5. Which tab in System Configuration enables you to launch Performance Monitor?

a) Services

b) Tools

c) Startup

d) General

Answer: b

Difficulty: Hard

Section Reference: Using MSCONFIG

Explanation: The Tools tab in the System Configuration utility lists many programs you can start for reporting and diagnostic purposes. Some of the tools are Change UAC Settings, Event Viewer, Performance Monitor, and Task Manager.

6. What is the maximum disk size NTFS can handle?

a) 256 GB

b) 256 TB

c) 32 GB

d) 32 TB

Answer: b

Difficulty: Easy

Section Reference: Understanding File Systems

Explanation: Most Windows 10 users use NTFS because it supports larger disks than FAT32 or FAT, and NTFS-formatted files and folders provide better security. An NTFS file system supports a maximum disk size of 256 terabytes.

7. What is the primary use of Programs and Features in Control Panel?

a) Compress application files

b) Encrypt application files

c) Uninstall applications

d) Install applications

Answer: c

Difficulty: Easy

Section Reference: Configuring Windows Features

Explanation: A user or administrator might need to remove, or uninstall, a local application for a variety of reasons. Windows 7 provides Programs and Features in Control Panel for this purpose.

8. Which of the following default accounts can run services in the background but has limited access to resources and objects, which helps protect the system when individual services are compromised?

a) Local Service

b) Network Service

c) Administrator

d) Network Operator

Answer: b

Difficulty: Hard

Section Reference: Understanding Service Startup Types

Explanation: The Local Service account is a built-in account (it’s already created in the operating system). It can run services in the background but has limited access to resources and objects, which helps protect the system if individual services are compromised. The Network Service is similar to the Local Service account but is geared for networking services. The Administrator account has full access to resources and objects. Windows does not have a default Network Operator account.

9. Which of the following was a standard developed in the mid-1990s that defines cable connectors and protocols used to connect external devices to a computer?

a) eSATA

b) FireWire

c) IEEE 1394

d) Universal serial bus (USB)

Answer: d

Difficulty: Medium

Section Reference: Understanding Storage Device Types

Explanation: Universal serial bus (USB) was a standard developed in the mid-1990s that defines cable connectors and protocols used to connect external devices to a computer.

10. Which of the following statements are true of volumes?

a) A spanned volume uses free space available on a single disk.

b) A simple volume spans across multiple disks, up to a maximum of 32.

c) A mirrored volume duplicates data from one disk to a second disk for redundancy and fault tolerance.

d) All of the above.

Answer: c

Difficulty: Hard

Section Reference: Understanding Disks and Drive Types

Explanation: A mirrored volume duplicates data from one disk to a second disk for redundancy and fault tolerance.

11. Where are EFS certificates stored?

a) Windows Certificate database

b) EFS Certificate database

c) Documents library

d) Certificate library

Answer: a

Difficulty: Hard

Section Reference: Understanding Encrypting File System (EFS)

Explanation: When you mark a file for encryption, Windows generates a large, random number—a unique encryption key. The key is used to scramble the contents of the file. This encryption key is also encrypted with a personal file encryption certificate, which is stored in the Windows Certificate database. The file’s encryption key is stored along with the file.

12. Which of the following statements are true of file systems?

a) The three primary types of file systems for Windows are FAT, FAT32, and NTFS.

b) It’s best to use NTFS-formatted disks for Windows Vista through Windows 10 because NTFS handles small to very large hard disks, provides better security, and is the most reliable.

c) A FAT32 partition is limited to a maximum size of 32 gigabytes (GB).

d) All of the above.

Answer: d

Difficulty: Medium

Section Reference: Understanding File Systems

Explanation: All statements are true of file systems.

13. Which chip can be used by BitLocker to protect BitLocker encryption keys?

a) Trusted Hard Drive Module

b) Trusted Protection Module

c) Encryption Platform Module

d) Trusted Platform Module

Answer: d

Difficulty: Medium

Section Reference: Understanding BitLocker

Explanation: Some computers have a Trusted Platform Module (TPM) chip on the motherboard. If the chip is present, BitLocker uses the TPM chip to protect the BitLocker keys. When a user starts a computer with a TPM chip and with BitLocker enabled, BitLocker requests the keys from the TPM and unlocks the system.

14. Which of the following is the best choice to protect specific folders on a DVD from unauthorized access?

a) NTFS

b) BitLocker Drive Encryption

c) Encrypting File System (EFS)

d) Group Policy

Answer: c

Difficulty: Medium

Section Reference: Encrypting and Compressing Files and Folders

Explanation: Encryption protects the contents of files and folders from unauthorized access. Windows uses Encrypting File System (EFS) to allow users to encrypt information on hard disks, external flash disks, CDs, DVDs, backup tapes, and other types of physical media.

15. Where do you configure the setting to enter Safe Mode the next time the computer starts?

a) System Configuration, Boot tab

b) System Configuration, General tab

c) Services console

d) System Configuration, Startup tab

Answer: a

Difficulty: Hard

Section Reference: Understanding MSCONFIG

Explanation: The options on the Boot tab in System Configuration enable you to adjust boot options, usually for diagnostic purposes. The Boot tab options match the options in the Advanced boot configuration menu that displays when you press F8 at startup. To boot the system into Safe Mode, select the Safe bootcheck box.

**Fill in the Blank**

1. A \_\_\_\_\_ is a sequence of instructions written to perform a specified task for a computer. Today, most of these programs are installed as desktop apps or Windows Store apps.

Answer: software application or "app"

Difficulty: Easy

Section Reference: Configuring Applications

Explanation: A software program (also known as an app) is a sequence of instructions written to perform a specified task for a computer. Today, most of these programs are installed as desktop apps or Windows Store apps.

2. \_\_\_\_\_ is the process of decreasing the size of files or folders without affecting the content of the files.

Answer: Compression

Difficulty: Medium

Section Reference: Understanding Compression

Explanation: The purpose of compression is to decrease large files that would otherwise use a lot of storage space. Because files often include a lot of redundant, repeated data, compressing them replaces repeated data with pointers to the data. The pointers take up much less space than the repeated data, so the size of the file is reduced.

**Short Answer**

1. Which feature encrypts an entire drive rather than individual files and folders on a disk?

Answer: BitLocker Drive Encryption

Difficulty: Easy

Section Reference: Understanding BitLocker

Explanation: BitLocker Drive Encryption is another method of protecting data stored on a fixed drive in a Windows computer. BitLocker encrypts the entire drive, rather than individual files and folders. The complementary BitLocker To Go protects data on removable data drives, such as an external flash drive.

2. What is the difference between encryption and compression?

Answer: Encryption protects files; compression reduces file size.

Difficulty: Medium

Section Reference: Understanding Compression

Explanation: Encryption protects the contents of files and folders from unauthorized access.

Compression is the process of decreasing the size of files or folders without affecting the files’ content.

3. You want to determine whether the COM+ Event System service has any dependent services. How do you find this information?

Answer: Open the service’s Properties dialog box and click the Dependencies tab.

Difficulty: Hard

Section Reference: Understanding Service Startup Types

Explanation: Open the Services console and then double-click the COM+ Event System service to open the Properties dialog box. The Dependencies tab shows you which services depend on other services to run. A dependent service starts after the service upon which it depends starts. Stopping a service also stops any other service that depends on it. There are no options available on this tab—it’s informational only. However, before you stop or disable a service on the General tab, you should view the information on the Dependences tab to know which other services might be affected by your change.