Exam Report: 12.11.8 Practice Questions

Date: 4/10/2020 9:59:05 pm
Time Spent: 6:33

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 29%

Passing Score: 80%

View results by: ○ Objective Analysis ● Individual Responses

Individual Responses

Question 1: Correct

You work as the IT administrator for a small startup company. Lily's computer has two internal hard drives and runs Windows 10. She is concerned that she may accidently delete a file or that her primary hard disk may fail at some future time. She has come to you for suggestions about how to protect her files. Due to the size and revenue of this startup company, resources are somewhat limited.

Which of the following would BEST protect Lily's files?

○ Purchase a third-party backup software.

➡ ● Back up her files using File History.

○ Create a network share to which Lily can copy her files.

○ Configure scheduled disk maintenance.

Explanation

Windows 10 includes the ability to back up files to another drive. This service is known as Back up using File History and can be found under Settings > Update & Security > Backup. This drive could include such things as a second drive in a computer, a USB-connected drive, or a network drive. Lily could use this feature to back up her files from her primary drive to her second drive, or you could purchase her an inexpensive USB drive she could automatically back files to.

With the limited funds available, buying a third-party backup software probably isn't feasible at this time. Having Lily copy her files to a network share would work for files she creates, but counting on her to back these up on a regular basis is risky. Scheduled disk maintenance allows the system to diagnose and repair disk errors. It does not back up files.

References

TestOut PC Pro - 12.11 System Backup
[e_sysback_pp6.exam.xml Q_RECOVERY_01]

Question 2: Incorrect

You need to protect the user data on a Windows 10 system.

Which tools could you use to do this?

□ Work Folders

➡ ☑ File History

➡ □ Windows 7 (Backup and Restore)

□ Previous Versions

□ Storage Spaces

Explanation

You can protect user data on a Windows 10 system using the following tools:

- File History can be used to protect user data. All user profile files (such as documents, music, and videos) are automatically backed up at a regular interval to a second storage device in the system.
- Windows 7 (Backup and Restore) can be used to back up user data to backup media on a specified schedule.

Previous Versions was used on Windows 7 to provide a similar function to File History on Windows 8.1 and later. Storage Spaces are used to aggregate storage space from multiple storage devices in the system. Work Folders are used to make files available on other devices, even when the main system is offline.

References

TestOut PC Pro - 12.11 System Backup

[e_sysback_pp6.exam.xml Q_RECOVERY_02]

Question 3: Correct

Why should backup media be stored offsite?

○ It is required by government regulations in the USA.

➡ ● To prevent the same disaster from affecting both the system and its associated backup media.

○ To reduce the possibility of theft.

○ It improves the efficiency of the restoration process.

Explanation

Backup media should be stored offsite to prevent the same disaster from affecting both the system itself as well as its associated backup media. For example, if your primary facility is destroyed by flood or fire, then your data remains protected at an offsite location.

Offsite storage does not significantly reduce the possibility of media theft because it can be stolen while in transit and while at the remote storage location. Offsite storage is not mandated by government regulation. Offsite storage does not improve the efficiency of the restoration process because additional time will be spent maintaining the backup media at the remote location.

References

TestOut PC Pro - 12.11 System Backup
[e_sysback_pp6.exam.xml Q_RECOVERY_03]

Question 4: Incorrect

You need to back up user data on a Windows 10 system. The computer has a single SSD storage device installed that contains both the Windows operating system (in C:\Windows) and user profile data (in C:\Users). You plan to do the following:

- Use Backup and Restore to backup user data.
- Run the backup automatically every night at 11:00 p.m.
- Store the backups in the C:\Backups folder.
- Include a system image in each backup.

Will this configuration work?

○ No. Windows 10 does not include the Backup and Restore utility. File History must be used instead.

○ No. System image backups can't be scheduled with Backup and Restore. They must be run manually.

➡ ○ No. Backups created with Backup and Restore can't be stored on the drive that contains the information being backed up.

● ~~Yes. All of the requirements for using Backup and Restore have been met.~~

Explanation

The configuration in the scenario will not work because backups created with the Backup and Restore utility can't be stored on the same drive containing the information being backed up. To fix this issue, a second hard disk or an external storage device needs to be added to the system.

Windows 10 includes both File History and Backup and Restore utilities. System image backups can be included within a scheduled file backup.

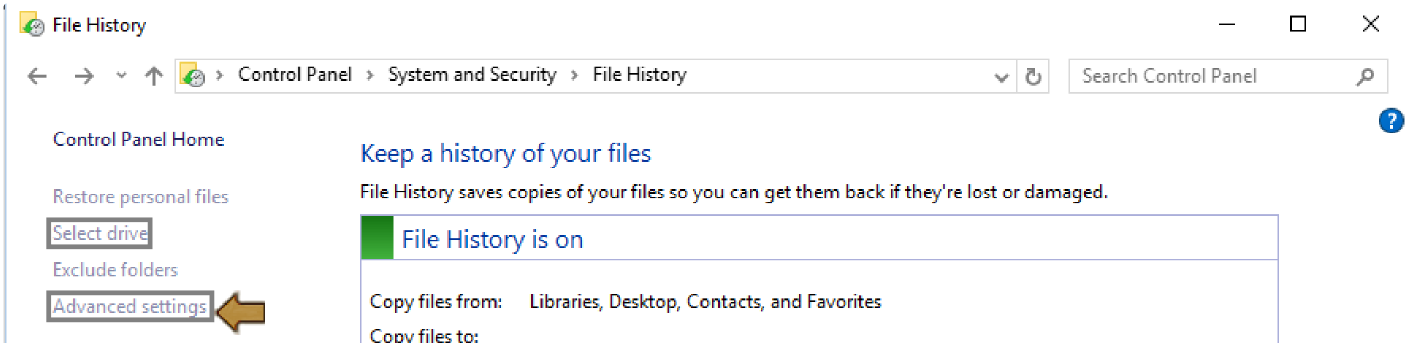
References

TestOut PC Pro - 12.11 System Backup
[e_sysback_pp6.exam.xml Q_RECOVERY_04]

Question 5: Incorrect

You need to configure File History to automatically delete any stored snapshots that are older than one month.

Click the Control Panel option you would use to do this.



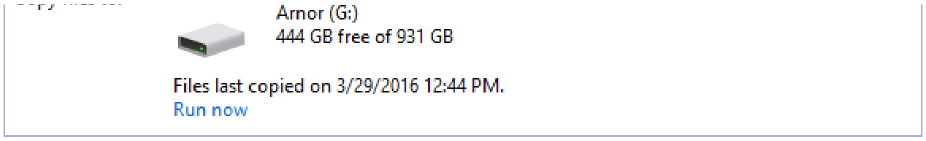
Keep a history of your files

File History saves copies of your files so you can get them back if they're lost or damaged.

File History is on

Copy files from: Libraries, Desktop, Contacts, and Favorites

Copy files to:



Arnor (G:)
444 GB free of 931 GB

Files last copied on 3/29/2016 12:44 PM.

Explanation

To clean up old versions, select the Advanced Settingsoption. Then select the appropriate cleanup interval from the Keep Saved Versions drop-down list.

The Exclude Folders option is used to prevent certain folders from being protected by File History. The Select Drive option is used to specify which hard disk is used to store File History data. The Restore Personal Files option is used to retrieve previous versions of files protected by File History.

References

TestOut PC Pro - 12.11 System Backup
[e_sysback_pp6.exam.xml Q_RECOVERY_05]

Question 6: Incorrect

You have configured your Windows systems to automatically back up user data every night at midnight. You also take a system image backup once per month.

What else should you do to ensure that you are protected from data loss? (Select TWO.)

➡ □ Regularly test restoration procedures.

□ Restrict restoration privileges to system administrators.

□ Configure System Maintenance to automatically defragment system hard drives every night.

➡ ☑ Store a copy of all backups off-site.

☑ ~~Write-protect all backup media.~~

Explanation

The only way to ensure that you are protected from data loss is to regularly test your restoration procedures. This activity will reveal whether or not your backup process is functioning properly and whether or not your restoration procedures will actually work. You should also store a redundant copy of your backups at an offsite location. The chance that a disaster at your main sight will also affect backups stored offsite is very small.

Restoration privileges should be restricted to trusted staff to prevent confidentiality violations. However, this is a security issue and is not related to the issue of data restoration in this scenario. Write-protecting backup media will provide little protection for the stored data because it can be easily removed.

References

TestOut PC Pro - 12.11 System Backup
[e_sysback_pp6.exam.xml Q_RECOVERY_06]

Question 7: Incorrect

An administrator configures the Time Machine application on Mac OS computers and develops scripts that use the **tar** command on Linux computers.

Which of the following best practices is the administrator following?

➡ ○ Scheduled backups

● ~~Scheduled disk maintenance~~

○ Driver/firmware updates

○ Patch management

Explanation

The Time Machine application on Mac OS computers and the **tar** command in Linux are used for backups.

While Time Machine and tar can be used to restore disk files, scheduled disk maintenance is usually performed to maintain disk and filesystem integrity. Patch management involves updating operating systems and applications, not performing backups. Driver/firmware updates involves updating the middleware that interfaces with internal and external devices, not performing backups.

References

TestOut PC Pro - 12.11 System Backup
[e_sysback_pp6.exam.xml Q_RECOVERY_07]