Exam Report: 15.2.8 Practice Questions

Date: 12/6/2019 4:58:42 pm
Time Spent: 1:23

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 75%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

Which of the following statements is true?

A system image backup:

- Does not include user profile settings.
- Can be saved to a Bitlocker-enabled volume.
- ~~Is the only type of backup supported by the backup and restore console.~~
- Is saved as a .vhd file.

Explanation

A system image backup consists of an entire volume backed up to a .vhd file. It contains everything on the system, including the operating system, installed programs, drivers, and user data files.

References

LabSim for Network Pro, Section 15.2.
[netpro18v5_all_questions_en.exm *NP15_DATA_PROTECTION_01]

Question 2: Correct

Which of the following media types can you save backup files on? (Select two.)

- [ ] The system disk
- [x] External hard drives
- [x] Network attached storage (NAS)
- [ ] Tape drives

Explanation

Backups can be saved to:

- Secondary internal hard drives
- External hard drives
- Optical drives
- USB flash drives
- Network shares
- .vhd files
- Network attached storage (NAS) or storage area network (SAN).

Backup files cannot be saved to:

- The same disk being backed up
- A system disk
- A Bitlocker-enabled

- A tape drive

References

LabSim for Network Pro, Section 15.2.
[netpro18v5_all_questions_en.exm *NP15_DATA_PROTECTION_02]

Question 3: Correct

In addition to performing regular backups, what must you do to protect your system from data loss?

- Write-protect all backup media.
- Store the backup media in an on-site fireproof vault.
- Regularly test restoration procedures.
- Restrict restoration privileges to system administrators.

Explanation

The only way to ensure that you have protection against data loss is to regularly test your restoration procedures. This activity reveals whether or not your backup process functions properly and your restoration and recovery procedures are accurate.

It's a good idea to store backup media in a fireproof vault, but it is a better idea to store it off site. Restoration privileges should be restricted to trusted staff to prevent confidentiality violations (but this does not address the issue of data loss protection). Write-protecting backup media provides little real security for the stored data because anyone can flip the switch on the media to remove the protection.

References

LabSim for Network Pro, Section 15.2.
[netpro18v5_all_questions_en.exm CISSP-1016 SP [7]]

Question 4: Correct

Why should you store backup media off site?

- To reduce the possibility of theft.
- To comply with government regulations.
- To make the restoration process more efficient.
- To prevent the same disaster from affecting both the network and the backup media.

Explanation

Backup media should be stored off site to prevent the same disaster from affecting the network and the backup media. If your primary facility is destroyed by fire, your only hope of recovery is off site data storage.

Off site storage does not significantly reduce the possibility of media theft because it can be stolen while in transit or at your storage location. Off site storage is not a government regulation. Off site storage does not make the restoration process more efficient because additional time is spent retrieving backup media from its off site storage location.

References

LabSim for Network Pro, Section 15.2.
[netpro18v5_all_questions_en.exm CISSP-1016 SP [15]]