

# Chapter 10 data defense



## 10. 1. 10 Practice exam

Which form of alternate site is the cheapest but may not allow an organization to recover before reaching their maximum tolerable downtime?

Reciprocal agreement

Which of the following network strategies connects multiple servers together such that if one server fails, the others immediately take over its tasks, preventing a disruption in service? Clustering

Which of the following drive configurations is fault tolerant? RAID 5

You have been asked to deploy a network solution that requires an alternate location where operational recovery is provided within minutes of a disaster.

Which of the following strategies would you choose? Hot site

Daily backups are done at the ABD company location and only a weekly backup is maintained at another network location. Which of the following disaster recovery strategies is ABD using? Warm site

You manage a Web site for your company. The Web site uses three servers configured in a cluster. Incoming requests are distributed automatically between the three servers. All servers use a shared storage device that holds the website contents. Each server has a single network connection and a single power supply. Considering the availability of your website, which components represent a single point of failure? Website storage

You manage the website for your company. The web1 server hosts the website. This server has the following configuration: Dual core processorDual

power supplies RAID 5 volume One RAID controller Two 1000 Mbps network adapters Which component is a single point of failure for the website? Disk controller

You have been asked to implement a RAID 5 solution for your network. What is the minimum number of hard disks that can be used to configure RAID 5?

3

What is an advantage of RAID 5 over RAID 1? RAID 5 improves performance over RAID 1

You manage the website for your company. The website uses a cluster of two servers with a single shared storage device. The shared storage device uses a RAID 1 configuration. Each server has a single connection to the shared storage, and a single connection to your ISP. You want to provide redundancy such that a failure in a single component does not cause the website to be unavailable. What should you add to your configuration to accomplish this? Connect one server through a different ISP to the Internet

When should a hardware device be replaced in order to minimize downtime?

Just before its MTBF is reached

You have a Web server on your network that hosts the public Web site for your company. You want to make sure that the Web site will continue to be available even if a NIC, hard drive, or other problem prevents the server from responding. Which solution should you implement? Load balancing

Which of the following is a recovery site that may have electricity connected, but there are no servers installed and no high-speed data lines present? Cold site

Which of the following terms describes the actual time required to successfully recover operations in the event of an incident? Recovery Time Objective (RTO)

Match the recovery term on the right with the appropriate definition on the left  
MTTF- Measures the average time to failure of a system or component

MTD- Identifies the length of time an organization can survive with a specific service, asset, or process down

MTTR- Identifies the average amount time to repair a failed component or to restore an operation

MTFB- Identifies the average lifetime of a system or component

10. 2. 10 practice exam

Even if you perform regular backups, what must be done to ensure that you protected against data loss? Regularly test restoration procedures

Why should backup media be stored offsite? To prevent the same disaster from affecting both the network and the backup media

A system failure has occurred. Which of the following restoration processes would result in the fastest restoration of all data to its most current state?

Restore the full backup and the last differential backup

Which of the following are backed up during a differential backup? Only files that have changed since the last full backup.

To increase your ability to recover from a disaster, where should you store backup tapes? In a safety deposit box at a bank

Which backup strategy backs up all files from a computer's file system regardless of whether the file's archive bit is set or not marks them as having been backed up? Full

Which backup strategy backs up only files which have the archive bit set, but does not mark them as having been backed up? Differential

Your organization uses the following tape rotation strategy for its backup tapes: The first set of tapes is used for daily backups.

At the end of each week, the latest daily backup tape is promoted to be the weekly backup tape.

At the end of the each month, one of the weekly backup tapes is promoted to be the monthly backup tape.

What kind of backup tape rotation strategy is being used?

Grandfather

The disaster recovery plan calls for having tape backups stored at a different location. The location is safe deposit box at the local bank. Because of this, the disaster recovery plan specifies to choose a method that uses the fewest tapes, but is also quick to back up and restore files. Which backup strategy

would best meet the disaster recovery plan for tape backups? Perform a full back up once a week with a differential back up the other days of the week.

What does an incremental backup do during the backup? Backs up all files with the archive bit set; resets the archive bit.

What does a differential backup do during the backup? Backs up all files with the archive bit set; does not reset the archive bit.

Your network uses the following backup strategy: o Full backups every Sunday night o Incremental backups Monday through Saturday nights Thursday morning the storage system fails. How many restore operations will you need to perform to recover all of the data? 4

Your network uses the following backup strategy: Full backups every Sunday night Differential backups Monday through Saturday nights Thursday morning the storage system fails. How many restore operations will you need to perform to recover all of the data? 2

Your network performs a full back up every night. Each Sunday, the previous night's backup tape is archived. Wednesday morning the storage system fails. How may restore operations will you need to perform to recover all of the data? 1

### 10. 3. 10 practice exam

You would like to implement BitLocker to encrypt data on a hard disk even if it moved to another system. You want the system to boot automatically

without proving a startup key on an external USB device. What should you do? Enable TPM in the BIOS

You want to protect data on hard drives for users with laptops. You want the drive to be encrypted, and you want to prevent the laptops from booting unless a special USB drive is inserted. In addition, the system not boot if a change is detected in any of the boot files. What should you do? Implement BitLocker with a TPM

Which of the following are backed up during an incremental backup? Only files that have changed since the last full or incremental backup.

You want a security solution that protects the entire hard drive, preventing access even when it is moved to another system. Which solution would you choose? BitLocker

Which of the following security solutions would prevent a user from reading a file which she did not create? EFS

You've used Bitlocker to implement full volume encryption on a notebook system. The notebook motherboard does not have a TMP chip, so you've used an external USB flash drive to store the Bitlocker startup key. Which system components are encrypted in this scenario? select two Master boot record

C: volume

You've used Bitlocker to implement full volume encryption on a notebook system. The notebook motherboard does not have a TMP chip, so you've

used an external USB flash drive to store the Bitlocker startup key. You use EFS to encrypt the C: secret folder and its contents. Which of the following is true in this scenario? select two. Only the user who encrypted the C: secrets file will be able to open it by default.

If the C: secrets file is copied to an external USB flash drive, it will be saved in an unencrypted state.

You create a new document and save it to a hard drive on a file server on your company's network. Then, you employ an encryption tool to encrypt the file using AES. This activity is an example of accomplishing what security goal? Confidentiality.

#### 10. 4. 9 Practice exam

You are purchasing a hard disk over the Internet from an online retailer. What does your browser use to ensure that others cannot see your credit card number on the Internet? SSL.

IPSec is implemented through two separate protocols. What are these protocols called? (Select two.) AH, ESP.

Which of the following security measures encrypts the entire contents of a hard drive? DriveLock.

Which of the following protocols can be used to securely manage a network device from a remote connection? SSH.

Which of the following protocols are often added to other protocols to provide secure transmission of data? (Select two.) TLS, SSL.



What is the primary function of the IKE policy used with IPSec? Create a security association between communicating partners.

Which of the following protocols can TLS use for key exchange? (Select two.)RSADiffie-Hellman

SFTP uses which mechanism to provide security for authentication and data transfer? SSH

Which of the following is a secure alternative to FTP that uses SSL for encryption? FTPS

Which protocol does HTTPS use to offer security in Web transactions? SSL

As network administrator you are asked to recommend a secure method of transferring data between hosts on a network. Which of the following protocols would you recommend? (Select two.)SCPSFTP

Telnet is inherently insecure because its communications is in plain text and easily intercepted. Which of the following is an acceptable alternative to TelnetSSH

What is the default encryption algorithm used by SSH (Secure Shell) to protect data traffic between a client and the controlled server? IDEA

SSL (Secure Socket Layer) operates at which layer of the OSI model? Session

When using SSL authentication, what does the client verify first when checking a server's identity? The current date and time must fall within the server's certificate validity period.

## 10. 5. 4 Practice exam

Which of the following cloud computing solutions will deliver software applications to a client either over the Internet or on a local area network?

SaaS

Which of the following best describes the Platform as a Service (PaaS) cloud computing service model? PaaS delivers everything a developer needs to build an application onto the cloud infrastructure.

Which of the following is not true regarding cloud computing? Cloud computer requires end-user knowledge of the physical location and configuration of the system that delivers the services.

Which of the following are true concerning the Virtual Desktop Infrastructure (VDI)? select two User desktop environments are centrally hosted on servers instead of on individual desktop systems. In the event of a widespread malware infection, the administrator can quickly reimage all user desktops on a few central servers.

Match each description on the left with the appropriate cloud technology on the right  
Public cloud- Provides cloud services to just about anyone

Private cloud- Provides cloud services to a single organization

Community cloud- Allows cloud services to be shared by several organizations

Hybrid cloud- Integrates one cloud service with other cloud services

Which of the following network layer protocols provides authentication and encryption services for IP based network traffic? IPSec