

Windows Server Security And Maintenance

1. Which Windows Server feature allows administrators to control user permissions and security policies across the network?

- A. Task Scheduler
- B. Group Policy
- C. Device Manager
- D. File Explorer

Answer: B. Group Policy

2. What is the purpose of BitLocker in Windows Server?

- A. File sharing
- B. Disk encryption
- C. Firewall configuration
- D. User account creation

Answer: B. Disk encryption

3. Which tool is used to monitor security-related events such as login attempts?

- A. Task Manager
- B. Event Viewer
- C. Disk Cleanup
- D. Control Panel

Answer: B. Event Viewer

4. What is the use of Windows Update in server maintenance?

Answer:

Windows Update installs the latest security patches, bug fixes, and improvements, helping to keep the server secure and stable.

5. Why is user account management important for server security?

Answer:

Proper user account management prevents unauthorized access by assigning appropriate permissions and enforcing password policies.

6. What is the purpose of a firewall on a Windows Server?

Answer:

A firewall monitors and controls incoming and outgoing network traffic to block malicious connections and unauthorized access.

7. Mention one reason to review the Security log in Event Viewer.

Answer:

To detect suspicious login attempts or unauthorized access to the server.

8. Explain three important best practices to secure a Windows Server.

Answer:

1. Regular Updates – Keep the server updated with the latest patches to fix security vulnerabilities.
2. Strong Password Policies – Enforce complex passwords and enable account lockout to prevent brute-force attacks.
3. Use Firewalls and Antivirus – Protect against malware and unauthorized access using Windows Defender Firewall and Antivirus.

9. What is the role of Group Policy in Windows Server security?

Answer:

Group Policy allows administrators to enforce security settings across all computers in a network. It can restrict user actions, enforce password rules, disable USB ports, block software installations, and more — ensuring consistent and controlled security throughout the domain.

10. Describe the importance of regular server maintenance and monitoring.

Answer:

Regular maintenance ensures that the server remains secure, efficient, and reliable. Monitoring tools help detect hardware failures, performance issues, and potential security threats early. Tasks such as patching, checking disk health, reviewing logs, and backing up data are essential to avoid downtime and data loss.