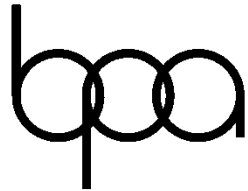


Contestant ID: \_\_\_\_\_

Time: \_\_\_\_\_

Rank: \_\_\_\_\_



**BUSINESS  
PROFESSIONALS  
of AMERICA**  
Giving Purpose to Potential

# **SERVER ADMINISTRATION USING MICROSOFT (310)**

## **REGIONAL 2026**

**CONCEPT KNOWLEDGE:**

Multiple Choice (50 @ 2 points each)

\_\_\_\_\_ (100 points)

**Test Time: 60 minutes**

**GENERAL GUIDELINES.**

Failure to follow any of these rules may result in disqualification:

1. **Submission Requirements:** Contestants must submit this test booklet along with any printouts.
2. **Permitted Items:** Only the equipment, supplies, and materials specified for this event are allowed in the testing area. Previous BPA tests and sample tests (whether handwritten, photocopied, or typed) are not permitted.
3. **Electronic Devices:** Electronic devices will be monitored according to ACT standards.

### Multiple Choice Questions

**Directions:** Identify the letter of the choice that best completes the statement or answers the question.

1. A user reports frequent system crashes after installing new hardware. What is the first step to troubleshoot this hardware device issue?
  - A. Check event logs
  - B. Replace the hardware
  - C. Update BIOS
  - D. Reinstall Windows OS
2. You need to restrict access to a specific website for all users on a Windows Server. Which feature should you configure?
  - A. Content filtering
  - B. Firewall rules
  - C. Proxy server settings
  - D. VPN configuration
3. A user experiences display issues after updating graphics drivers. What is the recommended troubleshooting step?
  - A. Roll back the driver update
  - B. Update the OS
  - C. Replace the graphics card
  - D. Reinstall the display drivers
4. What is the primary purpose of monitoring website access on a Windows Server?
  - A. Ensure security compliance
  - B. Improve server performance
  - C. Enhance user experience
  - D. Reduce network latency
5. An external webcam is not working on a Windows system. What should you check first to troubleshoot this hardware device issue?
  - A. Device Manager
  - B. Check webcam cable connections
  - C. Update the operating system
  - D. Restart the computer
6. What is the primary purpose of setting NTFS permissions on a folder?
  - A. To encrypt the folder
  - B. To manage access control
  - C. To compress the folder
  - D. To create a shortcut to the folder

7. You suspect a website is infected with malware. What tool can you use to scan and remove malware on a Windows Server?
  - A. Windows Defender
  - B. Task Manager
  - C. Disk Cleanup
  - D. Event Viewer
8. A user reports slow internet speeds. What should you check first to troubleshoot the Windows network connection issue?
  - A. Network adapter settings
  - B. System BIOS settings
  - C. Browser cache
  - D. Screen resolution settings
9. What is the purpose of configuring hardware devices and drivers on a Windows Server?
  - A. Ensure optimal device performance
  - B. Enhance server security
  - C. Improve network speed
  - D. Reduce system memory usage
10. A new mouse is not responding when connected to a Windows system. What should you do first to troubleshoot this hardware device issue?
  - A. Device manager
  - B. Update the mouse driver
  - C. Replace the mouse
  - D. Restart the system
11. You need to troubleshoot a network connection issue where multiple devices are unable to connect to the internet. What should you check?
  - A. Router settings
  - B. Wi-Fi signal strength
  - C. Network adapter status
  - D. DNS server configuration
12. A user reports that a printer is printing blank pages. What is the likely cause of this issue related to hardware devices and drivers?
  - A. Outdated printer driver
  - B. Faulty printer cable
  - C. Low printer toner level
  - D. Printer spooler service not running

13. How can you control access to specific websites for a group of users on a Windows Server?
  - A. Set up group policies
  - B. Update system BIOS
  - C. Configure DHCP settings
  - D. Change firewall settings
14. You are unable to connect to a shared network drive on a Windows system. What should you check first to troubleshoot this network issue?
  - A. Network permissions
  - B. Monitor CPU usage
  - C. Check browser history
  - D. Clear DNS cache
15. What is the primary benefit of configuring and troubleshooting Windows network connections on a Windows Server?
  - A. Enhance network security
  - B. Improve device compatibility
  - C. Optimize server performance
  - D. Reduce server storage usage
16. A user reports they are unable to connect remotely to the server. Which of the following steps should you take first to troubleshoot the issue?
  - A. Check firewall settings
  - B. Restart the server
  - C. Check network cables
  - D. Update the server software
17. You need to allow remote desktop connections to a Windows Server. Which port is commonly used for Remote Desktop Protocol (RDP) connections?
  - A. 22
  - B. 3389
  - C. 80
  - D. 443
18. To implement auditing on a Windows Server, which feature should you enable to track successful and failed login attempts?
  - A. Windows Defender Firewall
  - B. Windows Defender Antivirus
  - C. Account Logon Auditing
  - D. BitLocker Drive Encryption

19. Which tool can you use to manage local security policies on a Windows Server?
- A. Task Manager
  - B. Local Security Policy
  - C. Device Manager
  - D. Control Panel
20. A user is having issues connecting to the server remotely. Which of the following commands can you use to check the status of remote desktop services?
- A. netstat
  - B. ipconfig
  - C. ping
  - D. qwinsta
21. When configuring inbound connections on a Windows Server, which protocol is commonly used for secure remote access?
- A. FTP
  - B. HTTP
  - C. SSH
  - D. RDP
22. Which of the following should you configure to restrict access to a specific resource on a Windows Server based on user permissions?
- A. Group Policy
  - B. Network Address Translation (NAT)
  - C. Windows Firewall
  - D. Access Control Lists (ACLs)
23. To troubleshoot a remote access issue, which Windows feature allows you to track failed login attempts and security events?
- A. Task Scheduler
  - B. Event Viewer
  - C. Windows Defender
  - D. Resource Monitor
24. Which of the following policies should be configured to enforce complex password requirements on a Windows Server?
- A. Account Lockout Policy
  - B. Password Policy
  - C. Security Policy
  - D. Audit Policy

25. You need to allow remote access to a specific application on the server. Which feature should you configure to allow this?
- A. Windows Defender Firewall
  - B. Remote Desktop Services
  - C. Windows Update
  - D. Windows Defender Antivirus
26. In a Windows environment, what should you configure to specify which users or groups can access specific files and folders on the server?
- A. File Explorer
  - B. Task Manager
  - C. Local Security Policy
  - D. Access Control Lists (ACLs)
27. When troubleshooting remote access issues, which tool can you use to check the status of network connections to the server?
- A. netstat
  - B. ipconfig
  - C. ping
  - D. tracert
28. Which setting should be configured to enable Network Level Authentication (NLA) for remote desktop connections on a Windows Server?
- A. Advanced Security Settings
  - B. Remote Desktop Connection settings
  - C. Local Security Policy
  - D. Windows Defender Firewall settings
29. To enhance security on a Windows Server, which of the following should you configure to restrict access based on IP addresses?
- A. Windows Defender Firewall rules
  - B. Network Address Translation (NAT) rules
  - C. Remote Desktop Gateway settings
  - D. Access Control Lists (ACLs)
30. Which policy should be configured to specify the maximum number of failed login attempts before an account is locked out on a Windows Server?
- A. Account Lockout Policy
  - B. Password Policy
  - C. Security Policy
  - D. Audit Policy

31. You are configuring remote access to a Windows Server. Which feature should you enable to encrypt data transmitted between the server and clients?
- A. BitLocker Drive encryption
  - B. Windows Defender Firewall encryption
  - C. Remote Desktop Services encryption
  - D. Windows Update encryption
32. Which tool is commonly used to view and manage event logs related to security, application, and system events on a Windows Server?
- A. Task Scheduler
  - B. Event Viewer
  - C. Windows Defender
  - D. Resource Monitor
33. To restrict access to specific websites on a Windows Server, which feature should you configure to control internet access?
- A. Windows Defender Firewall settings
  - B. Internet Explorer settings
  - C. Remote Desktop Services settings
  - D. Windows Update settings
34. When implementing auditing on a Windows Server, which feature should you enable to track changes made to files and folders?
- A. Account Management Auditing
  - B. Object Access Auditing
  - C. Logon/Logoff Auditing
  - D. Policy Change Auditing
35. Which security setting should be configured to prevent unauthorized access to specific services on a Windows Server?
- A. Windows Defender Firewall rules
  - B. Service Control Manager settings
  - C. Remote Desktop Gateway settings
  - D. BitLocker Drive Encryption settings
36. A user is experiencing slow remote access to the server. Which tool can you use to identify network latency issues affecting the connection?
- A. netstat
  - B. ipconfig
  - C. ping
  - D. tracert



37. Which policy should be configured to enforce password expiration requirements on a Windows Server?
- A. Account Lockout Policy
  - B. Password Policy
  - C. Security Policy
  - D. Audit Policy
38. You need to allow secure file transfers over the network to the server. Which protocol should you typically use for encrypted file transfers?
- A. FTP
  - B. HTTP
  - C. SSH
  - D. SFTP
39. When configuring auditing on a Windows Server, which feature should you enable to track changes made to user accounts?
- A. Account Management Auditing
  - B. Object Access Auditing
  - C. Logon/Logoff Auditing
  - D. Policy Change Auditing
40. Which tool can you use to view and manage installed certificates on a Windows Server for secure communication?
- A. Certificate Manager
  - B. Device Manager
  - C. Control Panel
  - D. Event Viewer
41. To restrict remote access to specific users on a Windows Server, which feature should you configure to authenticate users before connection?
- A. Windows Defender Firewall rules
  - B. Remote Desktop Services settings
  - C. Network Policy Server settings
  - D. Access Control Lists (ACLs)
42. Which policy should be configured to specify the level of encryption required for secure network communications on a Windows Server?
- A. Encryption Policy
  - B. Password Policy
  - C. Security Policy
  - D. Audit Policy

43. You need to monitor remote access connections to the server in real-time. Which tool should you use to view active sessions and users?
- A. Task Manager
  - B. Event Viewer
  - C. Remote Desktop Services Manager
  - D. Resource Monitor
44. What is the first step in troubleshooting an OS installation?
- A. Installing drivers
  - B. Checking the system logs for error messages
  - C. Configuring network settings
  - D. Running updates
45. Which security setting should be configured to prevent unauthorized software installations on a Windows Server?
- A. Windows Defender Firewall rules
  - B. AppLocker settings
  - C. Remote Desktop Gateway settings
  - D. BitLocker Drive Encryption settings
46. A user is unable to connect remotely to the server. Which command can you use to check if the Remote Desktop service is running?
- A. netstat
  - B. ipconfig
  - C. ping
  - D. qwinsta
47. To enhance security on a Windows Server, which of the following should you configure to monitor and manage security events?
- A. Windows Defender Firewall
  - B. Security and Maintenance
  - C. Windows Defender
  - D. Windows Security Event Logs
48. When configuring inbound connections on a Windows Server, which protocol is commonly used for secure file transfers over the network?
- A. FTP
  - B. HTTP
  - C. SSH
  - D. SFTP

49. Which policy should be configured to specify the minimum password length required for user accounts on a Windows Server?
- A. Account Lockout Policy
  - B. Password Policy
  - C. Security Policy
  - D. Audit Policy
50. You need to allow remote access to a specific database application on the server. Which feature should you configure to enable this access?
- A. Task Scheduler
  - B. Remote Desktop Services
  - C. SQL Server Management Studio
  - D. Windows Defender Antivirus