7.1.12 Lesson Review

Date: 11/30/2025, 1:39:06 PM

Time Spent: 15:39

Score: 91%

Passing Score: 80%

Question 1

✕ Incorrect

A network administrator configures an authentication, authorization, and accounting (AAA) server.

Which component in the AAA server setup does not store authentication credentials but acts as a transit to forward data between devices?

● RADIUS ✕ Incorrect

○ NAP ✓ Correct

○ Supplicant

○ AAA

Explanation

The network access point (NAP) or network access server (NAS) are appliances, such as switches, access points, and VPN gateways. These do not store authentication credentials but simply act as a transit to forward this data between the AAA server and the supplicant.

The supplicant is a component of the authentication, authorization, and accounting server and is the device requesting access, such as a user's PC or laptop.

Remote Authentication Dial-in User Service (RADIUS) is a protocol that manages remote and wireless authentication infrastructures and implements AAA.

In an authentication, authorization, and accounting (AAA) configuration, the AAA server is the authentication server positioned within the local network.

Related Content

7.1.8 Directory and Authentication Servers

resources\questions\q_directory_and_authentication_servers_01.question.xml

Question 2 ✓ Correct

Which of the following is a primary function of a mail server?

○ Hosting websites and web applications

○ Providing remote terminal access to network resources

● Facilitating the sending and receiving of email messages ✓ Correct

○ Storing and managing large amounts of structured data

Explanation

Mail servers are specifically designed to handle the sending, receiving, and storage of email messages. They manage email traffic and ensure that emails are delivered to the correct recipients. This is the primary function of mail servers.

Hosting websites and web applications is the primary function of web servers, not mail servers. Web servers use HTTP or HTTPS to serve web pages and applications to clients. This function is unrelated to the operations of mail servers.

Storing and managing large amounts of structured data is associated with database servers, which are used to store, organize, and manage data for easy retrieval and manipulation. Mail servers do not primarily focus on data storage in the same way database servers do.

Providing remote terminal access to network resources is typically associated with remote terminal access servers, which allow users to access network resources from remote locations. Mail servers do not provide this type of access, as their main role is to handle email communications.

Related Content

- 7.1.5 Mail Servers
- 7.1.6 Mailbox Servers

resources\questions\q_mail_servers_01.question.xml

Question 3 ✓ Correct

A network technician securely connects to a remote server on port 3389. What protocol does the technician use?

○ SSH

○ Telnet

○ LDAP

● RDP ✓ Correct

Explanation

Remote Desktop Protocol (RDP) is Microsoft's protocol for operating remote graphical user interface (GUI) connections to a Windows machine. RDP uses port TCP/3389.

The Lightweight Directory Access Protocol (LDAP) is a TCP/IP protocol used to query and update an X.500 directory, and current directory products widely support it.

Secure Shell (SSH) is the principal means of obtaining secure remote access to UNIX and Linux servers and most types of network appliances (switches, routers, and firewalls).

Telnet is both a protocol and a terminal emulation software tool that transmits shell commands and output between a client and the remote host.

Related Content

- 6.3.6 Well-Known Ports
- 7.1.1 File/Print Servers
- 7.1.9 Remote Terminal Access Servers
- 14.2.1 Remote Desktop Tools

resources\questions\q_remote_terminal_access_servers_01.question.xml

Question 4 ✓ Correct

Which of the following statements about Server Message Block (SMB) accurately describes its current security status and implementation in modern networks?

○ SMB1 is the most secure version of the Server Message Block protocol and is enabled by default on all current Windows versions.

● SMB3 is the current version of the Server Message Block protocol and is considered secure, while SMB1 has serious security vulnerabilities and is disabled by default on current Windows versions. ✓ Correct

○ SMB2 is the latest version of the Server Message Block protocol and is primarily used for file sharing on UNIX-based systems.

○ SMB is only used for printer sharing on Windows networks and does not support file sharing functionalities.

Explanation

SMB3 is the current version and is secure, whereas SMB1 has vulnerabilities and is disabled by default on modern Windows systems.

SMB1 is not the most secure version; it has serious security vulnerabilities and is disabled by default on current Windows versions.

SMB2 is not the latest version; SMB3 is. Additionally, SMB is primarily used for file and printer sharing on Windows networks, not specifically on UNIX-based systems.

SMB is used for both file and printer sharing on Windows networks, not exclusively for printer sharing.

Related Content

- 7.1.1 File/Print Servers
- 10.1.13 Scanner Configuration

resources\questions\q_file_print_servers_02.question.xml

Question 5 ✓ Correct

Which of the following statements BEST describes the primary security concern associated with Telnet?

○ Telnet uses a secure tunneling protocol to protect data integrity and confidentiality during transmission.

● Telnet transmits data, including passwords, in plaintext. ✓ Correct

○ Telnet requires multi-factor authentication, providing an additional layer of security against unauthorized access.

○ Telnet encrypts all data transmissions, ensuring secure communication between client and server.

Explanation

Because Telnet transmits data in plaintext, it is vulnerable to eavesdropping and interception by malicious actors, which can lead to unauthorized access and data breaches.

Telnet does not encrypt data transmissions. This is a common misconception. The lack of encryption is a significant security flaw, as it allows data to be intercepted in plaintext.

Telnet does not use any secure tunneling protocol. This statement is false because Telnet lacks built-in security features to protect data integrity and confidentiality.

Telnet does not inherently require multi-factor authentication. This statement is misleading, as Telnet's standard implementation does not include advanced authentication mechanisms, making it less secure compared to modern alternatives like SSH.

Related Content

7.1.9 Remote Terminal Access Servers

14.2.1 Remote Desktop Tools

resources\questions\q_remote_terminal_access_servers_02.question.xml

Question 6 ✓ Correct

Which of the following statements correctly describes the primary function of database servers?

○ Database servers are primarily used to facilitate file sharing and printing services across a network.

○ Database servers are designed to provide secure email communication and manage email storage for users.

● Database servers are mainly used to store, organize, and manage large amounts of structured and unstructured data. ✓ Correct

○ Database servers primarily serve as a platform for hosting web applications and static web pages.

Explanation

Database servers are designed to handle large volumes of data, enabling efficient data retrieval, storage, and manipulation, which is essential for generating reports and making business decisions.

Web servers handle HTTP requests and serve web content, whereas database servers focus on data storage and management.

Providing secure email communication and managing email storage for users pertains to mail servers, which handle email communication and storage. Database servers, on the other hand, focus on data management and storage.

File/print servers manage shared access to disk and print resources, while database servers manage data storage and retrieval.

Related Content

7.1.2 Database Servers

resources\questions\q_database_servers_01.question.xml

Question 7 ✓ Correct

Which of the following BEST describes the primary function of a Time Server in a networked environment?

○ A Time Server facilitates the transfer of files between a client and a server using encrypted protocols.

○ A Time Server is responsible for managing and storing large amounts of structured and unstructured data.

● A Time Server synchronizes the clocks of computers and devices within a network. ✓ Correct

○ A Time Server provides secure access to web applications and encrypts data transmitted over the network.

Explanation

The primary function of a Time Server is to synchronize the time across all devices in a network, ensuring that all systems operate on the same time reference, which is crucial for time-sensitive operations and logging.

Being responsible for managing and storing large amounts of structured and unstructured data pertains to a Database Server, which is designed to store, organize, and manage data, allowing users to retrieve and manipulate it as needed.

Providing secure access to web applications and encrypting data transmitted over the network is related to Web Servers using HTTPS, which secure web communications through encryption, ensuring data privacy and integrity.

Facilitating the transfer of files between a client and a server using encrypted protocols is associated with File Transfer Protocols (FTP, SFTP), which are used for transferring files over a network, often with encryption for security.

Related Content

🗎 7.1.10 Time Servers

resources\questions\q_time_servers_01.question.xml

Question 8 — Partial

A web developer plans out a new website, including uniform resource locators (URLs) for each page. What are parts of the URL that the web developer will need to consider? (Select three.)

☑ FQDN ✓ Correct

□ Protocol ✓ Correct

☑ File server ✗ Incorrect

☑ File path ✓ Correct

Explanation

The developer will need to consider the fully qualified domain name (FQDN), which is not case-sensitive. The host location can also be an IP address; an IPv6 address must be in square brackets.

The developer will need to consider the protocol that describes the access method, which will likely be HyperText Transfer Protocol (HTTP) or HyperText Transfer Protocol Secure (HTTPS).

The developer will need to consider the file path, which specifies the directory and file name location of the resource (if required). The file path may or may not be case-sensitive.

In file server-based networks, a central machine provides dedicated file and print services to workstations. The benefits of server-based networks include ease of administration through centralization.

Related Content

7.1.3 Web Servers

resources\questions\q_web_servers_01.question.xml

Question 9 ✓ Correct

Your organization has been experiencing intermittent email delivery failures, and you have been tasked with analyzing the issue.

Upon investigation, you discover that the mail server is frequently reaching its maximum capacity for concurrent connections.

Which of the following analyses would BEST help you determine the root cause of this problem?

○ Evaluate the file/print server's resource allocation to determine if it is affecting the mail server's performance.

○ Review the database server's query performance to check for any delays in data retrieval impacting email processing.

○ Examine the web server's bandwidth usage to identify any potential network bottlenecks affecting email delivery.

● Analyze the mail server's configuration settings to ensure they are optimized for handling the current volume of email traffic. ✓ Correct

Explanation

Analyzing the mail server's configuration settings is crucial in understanding why it might be reaching its maximum capacity for concurrent connections. By ensuring that the server is configured to handle the expected volume of email traffic, you can identify if the issue is due to misconfiguration or if the server needs to be upgraded to accommodate higher demand.

While network bottlenecks can affect email delivery, examining the web server's bandwidth usage is not directly related to the mail server's capacity issues. The focus should be on the mail server itself, as it is the component experiencing the problem.

Database server performance is not directly related to the mail server's ability to handle concurrent connections. While slow data retrieval can affect applications, it is unlikely to be the root cause of the mail server's capacity issues.

The file/print server's resource allocation is not relevant to the mail server's capacity for handling email connections. The analysis should focus on the mail server's settings and performance, as it is the system directly involved in email delivery.

Related Content

- 7.1.5 Mail Servers
- 7.1.6 Mailbox Servers

resources\questions\q_mail_servers_03.question.xml

Question 10 ✓ Correct

Which of the following BEST evaluates the role of a mailbox server in a modern network environment?

○ A mailbox server is used to host websites and web applications, providing HTTP and HTTPS access to users.

○ A mailbox server primarily manages the authentication and authorization of users attempting to access network resources.

○ A mailbox server is responsible for filtering spam and malicious emails before they reach the user's inbox, thereby protecting the network from potential threats.

● A mailbox server primarily functions to store and manage email messages. ✓ Correct

Explanation

Mailbox servers are integral to email systems, as they store and manage email messages, handle the delivery process, and provide access to users through various email clients. This aligns with the core functions of mailbox servers.

While spam filtering is an important aspect of email security, it is typically handled by a separate component known as a mail filter or gateway, not the mailbox server itself. The mailbox server's primary role is not focused on filtering but on storing and managing emails.

Web servers are responsible for hosting websites and web applications, whereas mailbox servers are dedicated to managing email communications.

Primarily managing the authentication and authorization of users attempting to access network resources pertains to the role of directory and authentication servers, which handle user authentication and authorization. Mailbox servers do not primarily manage these functions; instead, they focus on email storage and management.

Related Content

7.1.5 Mail Servers

7.1.6 Mailbox Servers

resources\questions\q_mailbox_servers_02.question.xml

Question 11 ✓ Correct

A network technician is configuring an email connection that will have a permanent connection to the mail server. What kind of email connection is the technician configuring?

○ POP3

○ SMTP

○ HTML

● IMAP ✓ Correct

Explanation

The Internet Message Access Protocol (IMAP) is a mail retrieval protocol that supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously.

In Simple Mail Transfer Protocol (SMTP), the SMTP server of the sender discovers the IP address of the recipient SMTP server by using the domain name part of the recipient's email address.

HyperText Markup Language (HTML) web pages are plain text files with coded tags describing how to format the document.

The Post Office Protocol (POP) is an early example of a mailbox access protocol. POP is generally known as POP3 because the active version of the protocol is version 3.

Related Content

7.1.5 Mail Servers

7.1.6 Mailbox Servers

resources\questions\q_mailbox_servers_01.question.xml

Question 12 ✓ Correct

You are a network administrator tasked with securing your company's website to ensure that all data exchanged between your clients and the server is encrypted.

You need to implement a protocol that will provide this security by encrypting the data and verifying the server's identity.

Which of the following actions should you take to achieve this goal?

○ Set up the website to use FTP for data transmission and ensure that it operates over port 21.

○ Enable NetBIOS over TCP/IP on the web server to allow secure data transmission.

○ Configure the website to use HTTP and ensure all data is transmitted over port 80.

● Install a digital certificate from a trusted Certificate Authority (CA) on the web server and configure the website to use HTTPS. ✓ Correct

Explanation

By installing a digital certificate and configuring the website to use HTTPS, you ensure that data is encrypted and the server's identity is verified, providing the necessary security for data exchange.

HTTP does not encrypt data, leaving it vulnerable to interception. Port 80 is used for HTTP, which does not provide the security features required in the scenario.

FTP, especially when operating over port 21, does not inherently provide encryption for data transmission. The scenario requires encrypted data exchange, which FTP does not fulfill without additional security measures like FTPS or SFTP.

NetBIOS over TCP/IP is not related to securing web data transmission. It is an outdated protocol for network communication and does not provide the encryption and server identity verification required by the scenario.

Related Content

6.3.6 Well-Known Ports

7.1.4 Hypertext Transfer Protocol Secure resources\questions\q_hypertext_transfer_protocol_secure_02.question.xml

Question 13 ✓ Correct

Your company has recently experienced issues with inconsistent timestamps on transaction logs across multiple servers, leading to difficulties in tracking and auditing activities.

As the network administrator, you need to resolve this issue to ensure all servers have synchronized time.

Which of the following actions should you take to address this problem?

○ Set up a File Transfer Protocol (FTP) server to regularly back up transaction logs for auditing purposes.

● Install and configure a centralized Time Server to synchronize the clocks of all network devices. ✓ Correct

○ Implement HTTPS on all servers to secure data transmission and improve timestamp accuracy.

○ Deploy a new Database Server to manage and store transaction logs more efficiently.

Explanation

By installing and configuring a centralized Time Server, you can ensure that all devices on the network have synchronized time, which will resolve the issue of inconsistent timestamps on transaction logs.

While a Database Server can help manage and store data, it does not address the issue of time synchronization across servers, which is the root cause of the inconsistent timestamps.

HTTPS is used to secure data transmission over the network but does not directly affect the synchronization of time across servers. It does not resolve the issue of inconsistent timestamps.

While setting up an FTP server for backups can aid in data recovery and auditing, it does not address the core issue of time synchronization, which is necessary for consistent timestamps.

Related Content

7.1.10 Time Servers

resources\questions\q_time_servers_02.question.xml

Question 14 ✓ Correct

Your organization has recently deployed a Network Monitoring Server to address frequent network outages and potential security breaches.

After a week of monitoring, you receive a report indicating a significant increase in network traffic during non-business hours, along with several failed login attempts from an unfamiliar IP address.

As the network analyst, how should you interpret these findings to enhance network security and performance?

○ Conclude that the increased traffic is due to legitimate after-hours work by employees, and no action is needed.

● Analyze the report to identify potential unauthorized access attempts and recommend implementing stricter access controls. ✓ Correct

○ Assume the network monitoring server is malfunctioning and schedule a maintenance check to resolve the issue.

○ Determine that the failed login attempts are likely due to forgotten passwords and advise users to reset their credentials.

Explanation

Analyzing the report to identify potential unauthorized access attempts and recommending the implementation of stricter access controls and monitoring demonstrates an analytical approach by considering the possibility of unauthorized access based on the report's findings.

Concluding that the increased traffic is due to legitimate after-hours work by employees and no action is needed overlooks the potential security threat posed by the unusual traffic patterns and failed login attempts. Analyzing the situation requires considering the possibility of unauthorized access rather than assuming all activity is legitimate.

While forgotten passwords can cause failed login attempts, this explanation does not account for the unusual timing and unfamiliar IP address. A deeper analysis is needed to assess potential security risks.

Assuming a malfunction without further investigation dismisses the potential security threat. Analyzing the data should focus on understanding the traffic patterns and addressing any security vulnerabilities.

Related Content

resources\questions\q_network_monitoring_servers_03.question.xml

Question 15 ✓ Correct

Which of the following best describes the primary function of Network Monitoring Servers?

○ To store, organize, and manage large amounts of structured and unstructured data

○ To enable secure communication over the internet using encryption protocols

● To monitor and analyze network traffic to ensure optimal performance and security ✓ Correct

○ To provide shared access to disk and print resources

Explanation

Network monitoring servers are tasked with observing and analyzing network traffic to maintain network performance and security.

Providing shared access to disk and print resources describes the function of File/Print Servers, which are responsible for allowing shared access to disk and print resources over a network. Network Monitoring Servers, on the other hand, focus on monitoring network traffic and performance.

Storing, organizing, and managing large amounts of structured and unstructured data pertains to Database Servers, which are designed to handle the storage and management of data. Network Monitoring Servers do not primarily deal with data storage or management but rather with monitoring network activities.

Enabling secure communication over the internet using encryption protocols. Incorrect is the function of servers that implement security protocols like HTTPS, which ensure secure communication over the internet. Network Monitoring Servers are not primarily focused on enabling secure communication but rather on monitoring network traffic and performance.

Related Content

resources\questions\q_network_monitoring_servers_01.question.xml