LPI

202-450

LPIC-2 - Exam 202 (part 2 of 2), version 4.5

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**



Latest Version: 6.0

Question: 1

Which of the following Samba services handles the membership of a file server in an Active Directory domain?

A. winbindd
B. nmbd
C. msadd
D. admemb
E. samba

Answer: A

Explanation:
The Samba service that handles the membership of a file server in an Active Directory domain is winbindd. Winbindd is a daemon that provides a number of services to the Name Service Switch (NSS) capability of the system, such as resolving user and group information from a Windows NT server and authentication. Winbindd can also be used to join a Samba file server to an Active Directory domain and authenticate domain users to access the file shares 1 2
Reference:
Chapter 4. Using Samba for Active Directory Integration Red Hat Enterprise Linux 7 - Red Hat Customer Portal
Winbind: Use of Domain Accounts - SambaWiki

Question: 2

What is the purpose of DANE?

A. Verify the integrity of name information retrieved via DNS.
B. Allow secure dynamic DNS updates.
C. Invalidate name information stored on caching name servers to speed up DNS updates.
D. Discover which servers within a DNS domain offer a specific service.
E. Provide a way to verify the association of X 509 certificates to DNS host names.

Answer: E

Explanation:
DANE stands for DNS-based Authentication of Named Entities. It is a protocol that provides a way to verify the association of X 509 certificates to DNS host names. X 509 certificates are digital documents that contain the public key and identity information of an entity, such as a web server or an email server. They are used to establish secure connections and authenticate the identity of the entity. However, the traditional way of obtaining and validating X 509 certificates relies on a hierarchical system of trusted third parties, called certificate authorities (CAs), which can be vulnerable to attacks or compromise. DANE aims to enhance the security and trust of X 509 certificates by using DNSSEC, which is a set of extensions to DNS that provide cryptographic signatures and validation for DNS records. DANE allows the owner of a domain name to publish the X 509 certificate or its fingerprint in a DNS record, called a TLSA record, which can be verified by the DNSSEC chain of trust. This way, the client can check the authenticity of the certificate directly from the DNS, without relying on external CAs. DANE can also be used to specify which CAs are authorized to issue certificates for a domain name, or to indicate that no CA is needed at all. DANE can be applied to various protocols that use X 509 certificates, such as HTTPS, SMTP, IMAP, POP3, etc.
Reference:
DANE - Wikipedia
DNS-Based Authentication of Named Entities (DANE) - Internet Society
DANE: Taking TLS Authentication to the Next Level Using DNSSEC

Question: 3

Which of the following lines is valid in a configuration file in /etc/pam.d/?

A. authrequired pam_unix.sotry_first_pass nullok
B. authtry_first_pass nullok, require pam_unix.so
C. authrequired:pam_unix.so(try_first_pass nullok)
D. authpam_unix.so(required try_first_pass nullok)

Answer: A

Explanation:
The line A is valid in a configuration file in /etc/pam.d/ because it follows the correct syntax and semantics of a PAM configuration file. The syntax of a PAM configuration file is:
module_interface control_flag module_name module_arguments
The module_interface specifies the type of authentication action that the module can perform. There are four types of module interface: auth, account, password, and session. The control_flag specifies how important the success or failure of the module is to the overall authentication process. There are four types of control flag: required, requisite, sufficient, and optional. The module_name specifies the name of the library that contains the module. The module_arguments are optional parameters that can modify the behavior of the module.

The line A has the following components:
module_interface: auth, which means the module is used for user authentication.
control_flag: required, which means the module must succeed for authentication to continue. If the module fails, the failure is recorded and the rest of the modules are executed.
module_name: pam_unix.so, which means the module is the standard Unix authentication module that verifies the user's password against the /etc/passwd and /etc/shadow files.
module_arguments: try_first_pass nullok, which means the module tries to use the password that was previously entered by the user (if any), and allows users with empty passwords to log in.
The line B is invalid because it has the wrong order of the fields. The control_flag should come before the module_name, not after. The line C is invalid because it uses parentheses and colons instead of spaces to separate the fields. The line D is invalid because it has the wrong syntax for the control_flag. The control_flag should be a single word, not a word in parentheses.

Question: 4

Which Apache HTTPD configuration directive specifies the RSA private key that was used in the generation of the SSL certificate for the server?

A. SSLCertificateKeyFile
B. SSLKeyFile
C. SSLPrivateKeyFile
D. SSLRSAKeyFile

Answer: A

Explanation:
The Apache HTTPD configuration directive that specifies the RSA private key that was used in the generation of the SSL certificate for the server is SSLCertificateKeyFile 1 . This directive sets the file path and name of the file containing the server private key 2 . The private key is used to decrypt the data that is encrypted with the public key contained in the certificate 1 . The private key must match the certificate, otherwise an error will occur when starting the server 2 . The other options are not valid directives for Apache HTTPD.
Reference:
mod_ssl - Apache HTTP Server Version 2.4
Why is SSLCertificateKeyFile needed for Apache? - Stack Overflow

Question: 5

Which of the following information has to be submitted to a certification authority in order to request a web server certificate?

A. The web server's private key.
B. The IP address of the web server.
C. The list of ciphers supported by the web server.
D. The web server's SSL configuration file.
E. The certificate signing request.

Answer: E

Explanation:
A certificate signing request (CSR) is a message sent from an applicant to a certificate authority (CA) in order to apply for a digital identity certificate. The CSR contains information about the applicant's identity, such as domain name, organization, location, etc., as well as the applicant's public key. The CSR is digitally signed by the applicant using their private key, which proves that they own the corresponding public key. The CA will verify the CSR and issue a certificate if the applicant meets the requirements. The certificate will contain the applicant's public key and identity information, as well as the CA's digital signature, which validates the certificate. Reference: LPIC-2 Exam 202 Objectives , What is a Certificate Signing Request (CSR)? Do I need one?

Question: 6

What option for BIND is required in the global options to disable recursive queries on the DNS server by default?

A. allow-recursive-query (none;);
B. allow-recursive-query off;
C. recursion {disabled; };
D. recursion {none; };
E. recursion no;

Answer: E

Explanation:
The option for BIND that is required in the global options to disable recursive queries on the DNS server by default is recursion no;. This option tells the server not to provide recursive query behavior to any client, unless overridden by a view or a zone statement. Recursive queries are queries that the server will try to resolve by contacting other servers if it does not have the answer in its cache or zones. Disabling recursive queries can improve the security and performance of the server, especially if it is only meant to serve authoritative zones 1 2 3
Reference:

BIND: Stop Recursion DNS Under Linux / UNIX - nixCraft
How to Disable External DNS Recursion in BIND? | DeviceTests
bind - How to Disable External DNS recursion? - Ask Ubuntu

Question: 7

What information can be found in the file specified by the status parameter in an OpenVPN server configuration file? (Choose two.)

A. Errors and warnings generated by the openvpn daemon
B. Routing information
C. Statistical information regarding the currently running openvpn daemon
D. A list of currently connected clients
E. A history of all clients who have connected at some point

Answer: B, D

Explanation:
The status parameter in an OpenVPN server configuration file specifies the name of a file where OpenVPN writes information about the current status of the VPN tunnel, such as the time, bytes sent and received, and the IP address and port of each connected client. This file can be used to monitor the VPN activity and troubleshoot any issues. The file does not contain any information about errors and warnings generated by the openvpn daemon, as those are written to the log file specified by the log or log-append parameter. The file also does not contain any historical information about the clients who have connected at some point, as it only shows the current state of the VPN tunnel.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/
https://openvpn-status.readthedocs.io/en/latest/api.html

Question: 8

In order to prevent all anonymous FTP users from listing uploaded file names, what security precaution can be taken when creating an upload directory?

A. The directory must not have the execute permission set.
B. The directory must not have the read permission set.
C. The directory must not have the read or execute permission set.
D. The directory must not have the write permission set.
E. The directory must not contain other directories.

Answer: C

Explanation:
To prevent anonymous FTP users from listing uploaded file names, the upload directory must not have the read or execute permission set for the anonymous user or group. The read permission allows the user to view the contents of a file or directory, while the execute permission allows the user to enter or search a directory. Therefore, removing both permissions will prevent the user from accessing or listing the files in the upload directory. However, the write permission can be left on, as it allows the user to create or modify files in the directory, which is the purpose of an upload directory.
Reference:
LPIC-2 Exam 202-450 Objectives , Topic 211: File Sharing, Objective 211.2: Manage FTP Service, Weight: 3
LPIC-2 Linux Professional Institute Certification Study Guide: Exam 201 and Exam 202 , Chapter 9: File Sharing, FTP, p. 353-354
Linux File Permissions Explained , Read, Write, and Execute Permissions, p. 2-4

Question: 9

A company is transitioning to a new DNS domain name and wants to accept e-mail for both domains for all of its users on a Postfix server.
Which configuration option should be updated to accomplish this?

A. mydomain
B. mylocations
C. mydestination
D. myhosts
E. mydomains

Answer: C

Explanation:
The mydestination parameter in the Postfix main.cf configuration file specifies the list of domains that are delivered via the $local_transport mail delivery transport. This means that Postfix will accept mail for those domains and deliver it to local mailboxes. To accept mail for both the old and new domain names, the mydestination parameter should include both domains, separated by commas. For example:
mydestination = olddomain.com, newdomain.com, localhost
This will allow Postfix to accept mail for user@olddomain.com and user@newdomain.com and deliver it to the same local user mailbox.
Reference:
LPIC-2 Exam 202 Objectives , Objective 205.3: Managing a postfix server
Postfix Basic Configuration , Postfix Documentation

Postfix Configuration Parameters: mydestination , Postfix Documentation
How to configure Postfix to receive mail for multiple domains , Server Fault

Question: 10

Which of the following services belongs to NFSv4 and does not exist in NFSv3?

A. rpc.idmapd
B. rpc.statd
C. nfsd
D. rpc.mountd

Answer: A

Explanation:
The rpc.idmapd service is a new component of NFSv4 that does not exist in NFSv3. It is responsible for mapping user and group IDs between the NFS client and server, using string names instead of numeric values. This allows for better security and compatibility across different systems. The rpc.idmapd service runs on both the NFS client and server and communicates with each other using the NFSv4 protocol. The other services, rpc.statd, nfsd, and rpc.mountd, are common to both NFSv3 and NFSv4, although they have some differences in functionality and behavior. References: 1 , 2 , 3

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/