PassQueen
a.k.a dumpsqueen.com

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

LPI 202-450

Version Demo

Total Demo Questions: 17

Total Premium Questions: 178

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Capacity Planning	1
Topic 2, Network Configuration	12
Topic 3, Domain Name Server	23
Topic 4, Web Services	32
Topic 5, File Sharing	29
Topic 6, Network Client Management	23
Topic 7, E-Mail Services	26
Topic 8, System Security	31
Topic 9, Mix Questions	1
Total	178

QUESTION NO: 1

Which OpenLDAP utility is used to create an LDIF representation of entries stored in a running LDAP database?

A. ldapsearch

B. slapcat

C. slapadd

D. ldapmodify

E. ldifdump

ANSWER: B

Explanation:

`slapcat` reads entries directly from an OpenLDAP database and writes them in LDAP Data Interchange Format (LDIF). It is commonly used for backups, database inspection, and migration tasks. Because it accesses the database files directly rather than using the LDAP protocol, it is normally run while `slapd` is stopped, unless the selected backend and operational procedure specifically permit safe concurrent access.

The resulting LDIF can be loaded into a database using tools such as `slapadd`, or it can be processed as text for administrative purposes. See the slapcat manual page.

QUESTION NO: 2

Which of the following settings can be used in an Apache HTTPD virtual host to configure a server certificate and its corresponding private key? (Choose two.)

A. SSLCertificateFile

B. SSLCertificateKeyFile

C. SSLPrivateKeyFile

D. SSLCertificateAuthorityFile

E. TLSCertificateFile

ANSWER: A B

Explanation:

`SSLCertificateFile` specifies the PEM-encoded server certificate file used by an SSL/TLS-enabled Apache virtual host. On supported current Apache versions, the same file can also include intermediate CA certificates after the leaf certificate, allowing Apache to provide a suitable certificate chain to clients.

`SSLCertificateKeyFile` specifies the file containing the corresponding private key. The private key must match the public key in the server certificate and must be protected from disclosure. Both directives are provided by `mod_ssl` and are used with `SSLEngine on` in a TLS virtual host. See the Apache SSLCertificateFile documentation and the Apache SSLCertificateKeyFile documentation.

QUESTION NO: 3 - (SIMULATION)

Which doveadm sub-command displays a list of connections of Dovecot in the following format? (Specify ONLY the command without any parameters.)

ANSWER: See the explanation for the answer

Explanation:

```
doveadm who
```

The `who` sub-command lists Dovecot's currently connected users and their connections/sessions.

QUESTION NO: 4

The following Apache HTTPD configuration has been set up to create a virtual host available at www.example.com and www2.example.com:

```
<VirtualHost *:80>
        ServerName www.example.com
        ServerName www2.example.com
        ServerAdmin webmaster@example.com
        DocumentRoot /var/www/
        <Directory /srv/www/>
                Require all granted
        </Directory>
</VirtualHost>
```

Even though Apache HTTPD correctly processed the configuration file, requests to both names are not handled correctly. What should be changed in order to ensure correct operations?

A. The configuration must be split into two VirtualHost sections since each virtual host may only have one name.

B. The port mentioned in opening VirtualHost tag has to be appended to the ServerName declaration's values.

C. Both virtual host names have to be placed as comma separated values in one ServerName declaration.

D. Both virtual host names have to be mentioned in the opening VirtualHost tag.

E. Only one Server name declaration may exist, but additional names can be declared in ServerAlias options.

ANSWER: E

Explanation:

Only one Server name declaration may exist, but additional names can be declared in ServerAlias options. Within a name-based Apache virtual host, `ServerName` establishes the single primary, or canonical, hostname for that host. It is not a list directive and should not be repeated to add another name. To make the same virtual host respond to both requested hostnames, retain one `ServerName` value, such as `www.example.com`, and add the other name using `ServerAlias www2.example.com`. Apache then uses the HTTP `Host` header to match either the canonical name or an alias to this same virtual-host configuration. This allows both DNS names to serve the same document root and settings while retaining an unambiguous primary identity for the virtual host. Apache's virtual-host documentation explicitly describes `ServerAlias` as the directive for alternate names that should match a virtual host, while the directive reference defines `ServerName` as the hostname and port used to identify the server. See the Apache name-based virtual host documentation and the ServerAlias directive reference.

QUESTION NO: 5

The Samba configuration file contains the following lines:

```
host allow = 192.168.1.100 192.168.2.0/255.255.255.0  local host
host deny = 192.168.2.31
interfaces = 192.168.1.0/255.255.255.0192.168.2.0/255.255.255.0
```

A workstation is on the wired network with an IP address of 192.168.1.177 but is unable to access the Samba server. A wireless laptop with an IP address 192.168.2.93 can access the Samba server. Additional trouble shooting shows that almost every machine on the wired network is unable to access the Samba server.

Which alternate host allow declaration will permit wired workstations to connect to the Samba server without denying access to anyone else?

A. host allow = 192.168.1.1-255

B. host allow = 192.168.1.100192.168.2.200localhost

C. host deny = 192.168.1.100/255.255.255.0192.168.2.31localhost

D. host deny = 192.168.2.200/255.255.255.0192.168.2.31localhost

E. hosts allow = 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0 localhost

F. hosts allow = 192.168.1.0/24 192.168.2.0/24 localhost

ANSWER: E F

Explanation:

The declarations `hosts allow = 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0 localhost` and `hosts allow = 192.168.1.0/24 192.168.2.0/24 localhost` are equivalent valid Samba configurations. Each explicitly permits the complete wired IPv4 subnet, 192.168.1.0 through 192.168.1.255, so the workstation at 192.168.1.177 is included. They also retain access for every host on the wireless 192.168.2.0/24 subnet, including 192.168.2.93, and permit connections originating from the Samba server itself through `localhost`. This meets the requirement to extend access to the wired network without reducing access for users who can already connect.

Samba evaluates the `hosts allow` parameter as a space-separated access list. A network may be represented using either an address plus a dotted-decimal netmask or CIDR prefix notation. A /24 mask, equivalent to 255.255.255.0, identifies all addresses sharing the first three octets. The Samba `smb.conf` manual documents the `hosts allow` parameter and accepted address/netmask forms: Samba smb.conf manual. Additional Samba configuration documentation is available at Samba Documentation.

QUESTION NO: 6

Which command can be used to test the syntax of an Nginx configuration file without starting or reloading Nginx?

A. nginx -t

B. nginx -c

C. nginx --verify

D. nginx -s check

E. nginxctl test

ANSWER: A

Explanation:

`nginx -t` tests the Nginx configuration syntax and attempts to open files referenced by the configuration. It reports whether the configuration file syntax is valid and whether the configuration test was successful. This makes it appropriate before reloading Nginx after changing a virtual host, TLS setting, upstream definition, or other configuration directive.

The command does not itself replace the running configuration. After a successful test, an administrator can reload the service using the distribution's service-management mechanism or an appropriate Nginx signal. See the Nginx command-line parameter documentation.

QUESTION NO: 7

Which of the following sshd configuration should be set to no in order to fully disable password based logins? (Choose two.)

A. PAMAuthentication

B. ChallengeResponseAuthentication

C. PermitPlaintextLogin

D. UsePasswords

E. PasswordAuthentication

ANSWER: B E

Explanation:

Set `PasswordAuthentication no` to disable SSH's direct password-authentication method, in which the client submits the account password to the SSH server. Set `ChallengeResponseAuthentication no` as well to disable challenge-response (keyboard-interactive) authentication, which can otherwise present a password prompt through PAM or another authentication backend. Disabling both settings prevents users from reaching a password-based SSH login path while allowing non-password methods, such as public-key authentication, to remain available when configured.

In current OpenSSH releases, `ChallengeResponseAuthentication` is a deprecated alias for `KbdInteractiveAuthentication`. Therefore, on newer systems, administrators should also verify that the effective `KbdInteractiveAuthentication` setting is `no`, particularly when configuration files include directives from multiple sources. The OpenSSH server configuration manual documents `PasswordAuthentication` and the keyboard-interactive/challenge-response setting and their relationship. See the OpenSSH sshd_config manual and the OpenSSH manual pages.

QUESTION NO: 8

CORRECT TEXT

What command creates a SSH key pair? (Specify ONLY the command without any path or parameters)

A. ssh-keygen

ANSWER: A

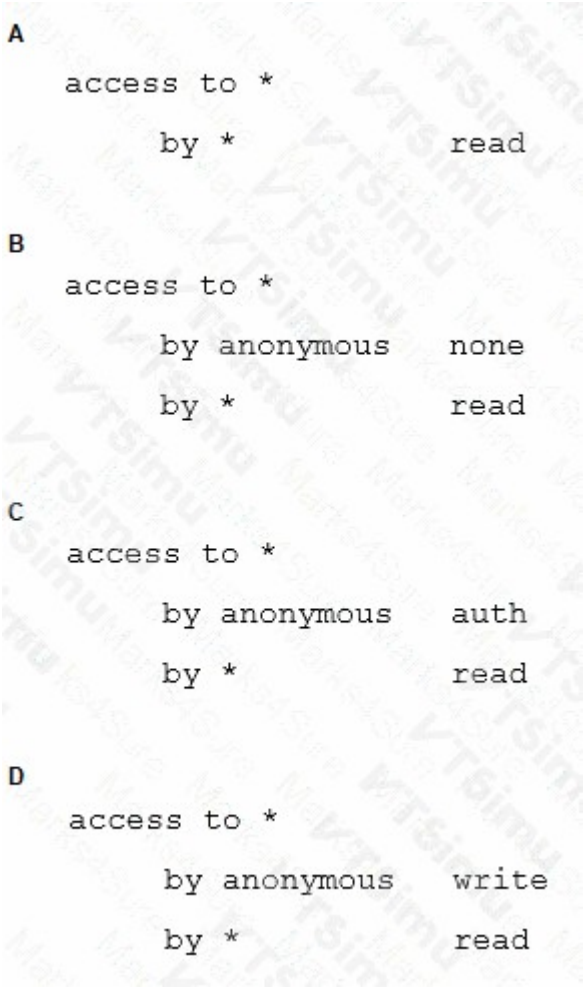
Explanation:

The correct command is `ssh-keygen`. It is the standard OpenSSH utility for generating public/private key pairs used for SSH public-key authentication. When run without parameters, `ssh-keygen` interactively prompts for the key file location, the key type and size or algorithm defaults, and an optional passphrase to protect the private key. By default, current OpenSSH implementations generate an Ed25519 key pair when supported, storing the private key in the user's `~/.ssh` directory and writing the matching public key with a `.pub` suffix. The public key can then be installed on a remote host, commonly in the

target account's `~/.ssh/authorized_keys` file, while the private key must remain confidential. This command is part of the OpenSSH suite and is the appropriate command to know for SSH key management in LPIC-2 objectives. The OpenBSD manual documents `ssh-keygen` as the program that "generates, manages and converts authentication keys for ssh." See the ssh-keygen manual page and the OpenSSH manual pages for supported key-generation and key-management operations.

QUESTION NO: 9

If there is no access directive, what is the default setting for OpenLDAP?



A. access to * by * write

B. access to * by * none

C. access to * by * read

D. access to * by dn.exact="cn=Manager,dc=example,dc=com" write by * none

ANSWER: C

Explanation:

The default OpenLDAP access-control policy is `access to * by * read`. When no `access` directives are configured, the server applies this implicit rule to the entire directory tree. The target selector `to *` covers every entry and attribute, while the access clause `by * read` grants every client read-level access. Read access permits clients to search for and retrieve directory information according to normal LDAP operation, but it does not grant permission to alter entries or attributes. This default is important when deploying a new LDAP server: administrators who need to restrict anonymous or authenticated directory searches must define explicit access-control rules rather than relying on an unspecified policy. OpenLDAP also treats the configured database root identity specially; it has unrestricted administrative access

independently of ordinary ACL evaluation. The OpenLDAP Administrator's Guide explicitly states that, in the absence of access directives, `access to * by * read` is used as the default policy. See the OpenLDAP Administrator's Guide: Access Control and the slapd.access(5) manual page.

QUESTION NO: 10

Which FTP names are recognized as anonymous users in vsftp when the option anonymous_enable is set to yes in the configuration files? (Choose two.)

A. anonymous

B. ftp

C. In the described configuration, any username which neither belongs to an existing user nor has another special meaning is treated as anonymous user.

D. nobody

E. guest

ANSWER: A B

Explanation:

The correct FTP login names are **anonymous** and **ftp**. In vsftpd, setting `anonymous_enable=YES` permits anonymous FTP logins, and vsftpd explicitly recognizes both of these conventional usernames as anonymous access requests. This behavior supports the long-established FTP convention in which public download sites allow users without local system accounts to connect using either `anonymous` or `ftp`. The client normally supplies an email address as the password, although the server's configuration can impose additional restrictions or password requirements.

Anonymous access is controlled separately from local-user access. Enabling it allows these recognized anonymous identities to use the permissions assigned to the configured FTP user account, commonly an account named `ftp`. Further settings, such as `anon_world_readable_only`, `write_enable`, and the various `anon_*` directives, determine what an anonymous session may read, upload, create, or modify after login. The vsftpd configuration manual specifically states that both `ftp` and `anonymous` are recognized as anonymous logins when anonymous logins are enabled. See the vsftpd.conf manual page and the vsftpd configuration reference.

QUESTION NO: 11

Which of the following actions can be performed by the fail2ban-client command? (Choose two.)

A. Display the status of configured jails.

B. Unban an IP address from a specified jail.

C. Create a new PAM authentication module.

D. Compile a firewall kernel module.

E. Generate SSH host keys.

ANSWER: A B

Explanation:

`fail2ban-client status` queries the running Fail2Ban server and displays global status information, including the currently configured jails. A jail-specific form such as `fail2ban-client status sshd` can display information about a selected jail, including currently banned addresses.

`fail2ban-client set sshd unbanip 192.0.2.25` instructs the selected jail to remove an address from its ban list. This is useful when an administrator has confirmed that a ban should be revoked before its configured expiry time. The command can also start, stop, reload, and otherwise manage the running Fail2Ban service. See the fail2ban-client(1) manual page.

QUESTION NO: 12

Which of the following Samba configuration parameters is functionally identical to the parameter read only=yes?

A. browseable=no

B. read write=no

C. writeable=no

D. write only=no

E. write access=no

ANSWER: C

Explanation:

`writeable=no` is functionally identical to `read only=yes` for a Samba share. The `read only` setting controls whether clients can create, modify, rename, or delete files through that share. When it is set to `yes`, Samba presents the share as non-writable, subject to the usual access checks and any more-specific configuration controls. Samba documents `writeable`, also commonly spelled `writable`, as an inverted synonym for `read only`. Therefore, setting `writeable=no` expresses precisely the same share-level behavior as setting `read only=yes`: write operations are disabled for clients accessing that service. This equivalence is useful when reading existing `smb.conf` files because administrators may use either spelling and either of the inverse parameter forms. The Samba manual describes the relationship directly, noting that the `read only` setting is inverted by the `writable` setting and that the alternate spelling is supported for historical reasons. See the official smb.conf manual page and the testparm documentation for validating effective Samba configuration values.

QUESTION NO: 13

Which of the following options are valid in /etc/exports? (Choose two.)

A. rw

B. ro

C. rootsquash

D. norootsquash

E. uid

ANSWER: A B

Explanation:

`rw` and `ro` are valid NFS export options in `/etc/exports`. They specify the access mode granted to clients for the exported directory and are written in the parenthesized, comma-separated option list following a client specification, such as `/srv/share client.example(rw,sync)`. The `rw` option permits clients to perform both read and write operations on the export, subject to normal filesystem permissions and any additional export controls. This is used when remote clients must create, modify, or delete files.

The `ro` option exports the directory as read-only, preventing NFS clients from making changes through that export. Read-only exports are appropriate for software repositories, static shared data, installation media, or any content that should be

consumed by clients without being modified remotely. Both access-mode options are defined by the NFS server export configuration and are standard entries recognized by the `exports(5)` configuration format. Administrators can combine either option with other supported controls, including synchronization, subtree checking, security-flavor, and root-mapping settings, to produce the required NFS export policy. See the exports(5) manual page and the Linux NFS configuration documentation.

QUESTION NO: 14

Which of the following statements about the Postfix aliases database are true? (Choose two.)

A. /etc/aliases can map a local recipient name to another address.

B. newaliases rebuilds the database used for local alias lookup.

C. Postfix reads /etc/aliases directly for every delivery attempt.

D. Aliases in /etc/aliases authorize SMTP clients to relay mail.

E. Changing /etc/aliases requires generating a new TLS certificate.

ANSWER: A B

Explanation:

The `/etc/aliases` file maps local recipient names to one or more destination addresses, local users, files, or commands. After modifying this source file, `newaliases` must be run to build the lookup database used by Postfix, commonly `/etc/aliases.db`. The command is equivalent to running `postalias /etc/aliases` on systems using the default database type.

Aliases are used for local delivery expansion and do not by themselves configure SMTP relay authorization or virtual-domain recipient mappings. See the aliases(5) manual page and the newaliases(1) manual page.

QUESTION NO: 15

What is the name of the Dovecot configuration variable that specifies the location of user mail?

A. mbox

B. mail_location

C. user_dir

D. maildir

E. user_mail_dir

ANSWER: B

Explanation:

`mail_location` is the Dovecot configuration setting used to define where users' mailboxes are stored and which mailbox storage format Dovecot should use. It is commonly configured in Dovecot's mail settings, such as `/etc/dovecot/conf.d/10-mail.conf`, with a value that begins with a storage driver name and can include a filesystem path. For example, `mail_location = maildir:~/Maildir` configures Maildir-format storage beneath each user's home directory, while an mbox-based configuration can specify an mbox location. This setting is fundamental because Dovecot needs both the mailbox format and location in order to find, read, and deliver users' messages correctly. The setting may also be supplied through user database attributes in installations where mailbox locations differ per user, but the Dovecot configuration variable itself remains `mail_location`. Dovecot's configuration documentation identifies `mail_location` as the mail storage configuration setting, and its Maildir documentation provides examples using this variable. See the Dovecot mail configuration reference and the Dovecot mail location documentation.

QUESTION NO: 16 - (SIMULATION)

What is the path to the global Postfix configuration file? (Specify the full name of the file, including path.)

ANSWER: See the explanation for the answer

Explanation:

The global Postfix configuration file is:

`/etc/postfix/main.cf`

This is Postfix's primary configuration file and contains global parameter settings.

QUESTION NO: 17

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:

`mydestination` is the Postfix `main.cf` parameter that specifies the domains for which the server accepts mail as the final destination and performs local delivery. To receive mail for both an old and a new company domain, both domain names should be included in this parameter, either directly or through a referenced lookup table. For example, a configuration can retain the usual local host values and add both domains: `mydestination = $myhostname, localhost.$mydomain, localhost, old.example.com, new.example.com`. When Postfix receives a message addressed to a recipient in one of these domains, it recognizes that domain as local rather than attempting to relay it elsewhere. Local recipient handling then uses the server's configured local delivery mechanism, aliases, virtual mappings, or mailbox configuration as appropriate. This setting is specifically intended for Internet domains that the Postfix instance delivers locally, including multiple names during a domain migration. After changing `main.cf`, validate the configuration with `postfix check` and reload Postfix with `postfix reload` so the updated destination-domain list is applied. The Postfix documentation describes `mydestination` as the list of domains delivered through the local transport. See the Postfix postconf(5) documentation for mydestination and the Postfix basic configuration guide.