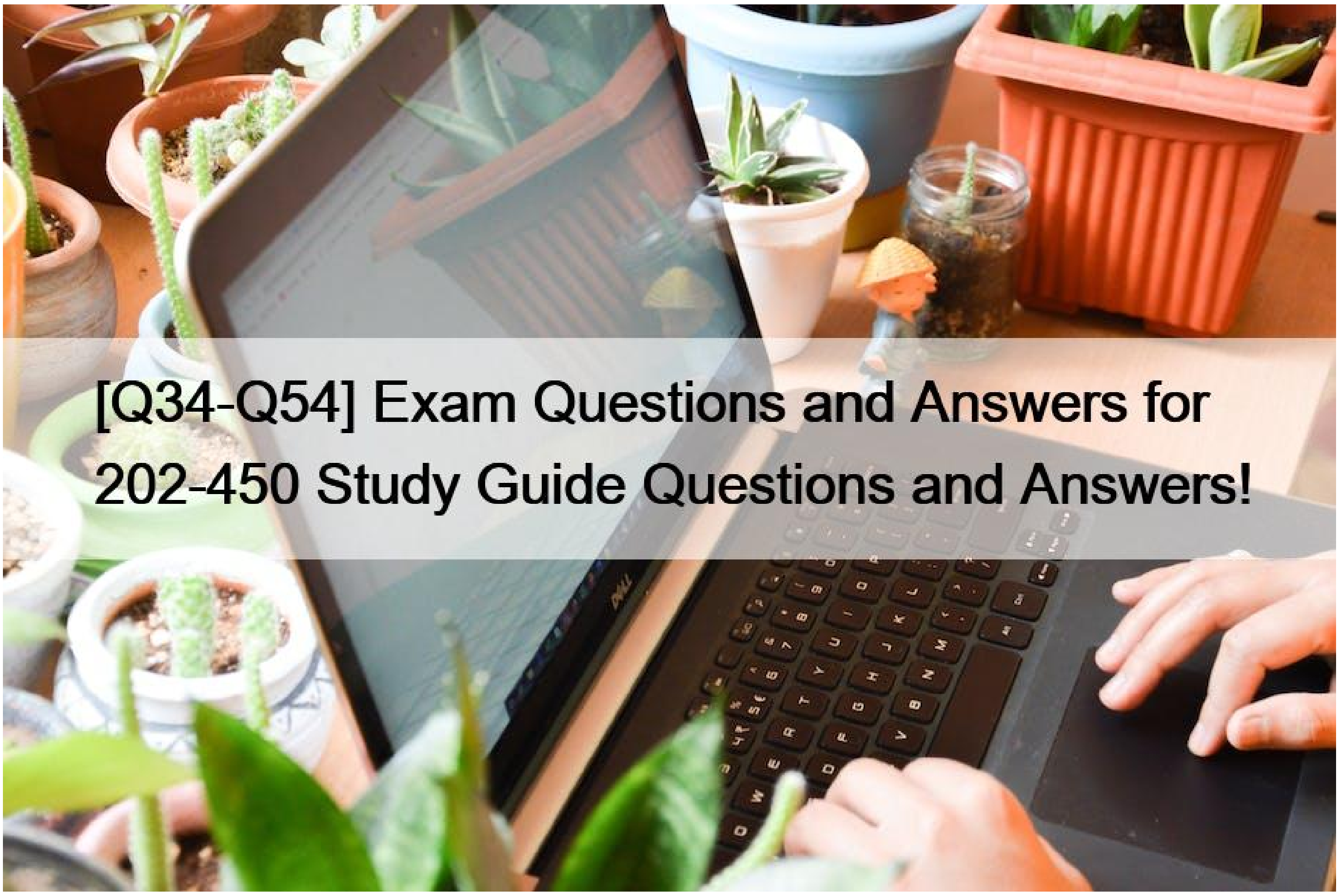
[Q34-Q54 Exam Questions and Answers for 202-450 Study Guide Questions and Answers!



Exam Questions and Answers for 202-450 Study Guide Questions and Answers! LPIC-2 - Exam 202 (part 2 of 2), version 4.5 Certification Sample Questions and Practice Exam QUESTION 34

Which rdnc sub command can be used in conjunction with the name of a zone in order to make BIND reread the content of the specific zone file without reloading other zones as well?
* lookup
* reload
* fileupdate
* reread
* zoneupdate
Explanation

The rndc sub command that can be used in conjunction with the name of a zone in order to make BIND reread the content of the specific zone file without reloading other zones as well is reload. The reload sub command instructs the BIND server to reload the specified zone or all zones if no zone is specified. The reload sub command is useful for applying changes made to the zone files without restarting the BIND service or affecting other zones. The syntax of the reload sub command is as follows:

rndc reload [zone [class [view]]]

For example, to reload the zone example.com in the IN class and the default view, use the following command:

rndc reload example.com IN

References:

rndc &#8211; man pages section 8: System Administration Commands, sub command &#8220;reload&#8221;

17.2.3. Using the rndc Utility &#8211; Red Hat Customer Portal, section &#8220;Reloading the Configuration and Zones&#8221;

QUESTION 35

Which configuration parameter on a Postfix server modifies only the sender address and not the recipient address?
* alias_maps
* alias_rewrite_maps
* sender_canonical_maps
* sender_rewrite_maps

QUESTION 36

In a BIND zone file, what does the @ character indicate?
* It&#8217;s the fully qualified host name of the DNS server
* It&#8217;s an alias for the e-mail address of the zone master
* It&#8217;s the name of the zone as defined in the zone statement in named.conf
* It&#8217;s used to create an alias between two CNAME entries

QUESTION 37

It has been discovered that the company mail server is configured as an open relay. Which of the following actions would help prevent the mail server from being used as an open relay while maintaining the possibility to receive company mails? (Choose two.)
* Restrict Postfix to only accept e-mail for domains hosted on this server
* Configure Dovecot to support IMAP connectivity
* Configure netfilter to not permit port 25 traffic on the public network
* Restrict Postfix to only relay outbound SMTP from the internal network
* Upgrade the mailbox format from mbox to maildir
Explanation

An open relay is a mail server that allows anyone to send e-mail through it without authentication or authorization. This can expose the mail server to spam, abuse, and blacklisting. To prevent the mail server from being used as an open relay, while maintaining the possibility to receive company mails, the following actions would help:

Restrict Postfix to only accept e-mail for domains hosted on this server. This can be done by setting the mydestination parameter in the /etc/postfix/main.cf file to include the company domains, and the smtpd_recipient_restrictions parameter to reject_unauth_destination. This will ensure that Postfix will only accept mail for the domains that it is responsible for, and reject mail for other domains unless the sender is authenticated or authorized. For example:

mydestination = example.com, example.net, localhost smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination Restrict Postfix to only relay outbound SMTP from the internal network. This can be done by setting the mynetworks parameter in the /etc/postfix/main.cf file to include the IP addresses or networks of the internal hosts that are allowed to relay mail through Postfix, and the smtpd_relay_restrictions parameter to permit_mynetworks. This will ensure that Postfix will only relay mail from the trusted internal hosts, and reject mail from external hosts unless the sender is authenticated or authorized. For example:

mynetworks = 192.168.0.0/24, 127.0.0.0/8 smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, defer_unauth_destination The other actions would not help prevent the mail server from being used as an open relay, or they would affect the functionality of the mail server. Configuring Dovecot to support IMAP connectivity would not affect the SMTP relay, but it would allow users to access their mailboxes remotely. Configuring netfilter to not permit port 25 traffic on the public network would prevent the mail server from receiving any mail from the outside world, which would defeat the purpose of having a mail server. Upgrading the mailbox format from mbox to maildir would not affect the SMTP relay, but it would change the way the mail messages are stored on the disk.

References:

LPIC-2 Exam 202 Objectives, Objective 205.3: Managing a postfix server

Postfix Basic Configuration, Postfix Documentation

Postfix SMTP relay and access control, Postfix Documentation

How to disable open relay on Postfix? &#8211; Howtoforge, Forum

Postfix SMTP relay without authentication | Guide &#8211; Bobcares, Blog

QUESTION 38

Which of the following values can be used in the OpenLDAP attribute olcBackend for any object of the class olcBackendConfig to specify a backend? (Choose three.)
* xml
* bdb
* passwd
* ldap
* text

QUESTION 39

Which of the following PAM modules allows the system administrator to use an arbitrary file containing a list of user and group names with restrictions on the system resources available to them?
* pam_filter
* pam_limits
* pam_listfile
* pam_unix

QUESTION 40

When the default policy for the netfilter INPUT chain is set to DROP, why should a rule allowing traffic to localhost exist?
* All traffic to localhost must always be allowed
* It doesn&#8217;t matter; netfilter never affects packets addressed to localhost
* Some applications use the localhost interface to communicate with other applications

* syslogd receives messages on localhost
* The iptables command communicates with the netfilter management daemon netfilterd on localhost to create and change packet filter rules

Explanation

The localhost interface, also known as the loopback interface, is a virtual network interface that allows a host to communicate with itself. It has the IP address 127.0.0.1 for IPv4 and ::1 for IPv6. Some applications use the localhost interface to communicate with other applications running on the same host, such as database servers, web servers, or inter-process communication. Therefore, when the default policy for the netfilter INPUT chain is set to DROP, which means that all incoming packets that do not match any rule are dropped, a rule allowing traffic to localhost should exist to avoid breaking these applications. The rule can be something like this:

```
iptables -A INPUT -i lo -j ACCEPT
```

This rule appends a new rule to the INPUT chain that accepts any packet that comes from the loopback interface (lo). The other options are incorrect for the following reasons:

A). All traffic to localhost must always be allowed. This is false because there may be situations where traffic to localhost should be restricted or filtered, such as for security or performance reasons. For example, some malware may try to exploit vulnerabilities in applications listening on localhost, or some applications may generate excessive traffic on localhost that affects the system resources. Therefore, allowing all traffic to localhost is not always necessary or desirable.

B). It doesn&#8217;t matter; netfilter never affects packets addressed to localhost. This is false because netfilter does affect packets addressed to localhost, unless they are explicitly allowed by a rule or the default policy. Netfilter processes all packets that enter or leave the network stack, regardless of their source or destination address. Therefore, packets addressed to localhost are subject to the same rules and policies as packets addressed to any other host.

D). syslogd receives messages on localhost. This is false because syslogd does not necessarily receive messages on localhost. Syslogd is a daemon that handles system logging, and it can receive messages from various sources, such as local processes, files, pipes, or remote hosts. Syslogd can be configured to listen on a network socket, such as UDP port 514, but it does not have to listen on localhost. Therefore, allowing traffic to localhost is not required for syslogd to function properly.

E). The iptables command communicates with the netfilter management daemon netfilterd on localhost to create and change packet filter rules. This is false because there is no such daemon as netfilterd, and the iptables command does not communicate with any daemon on localhost to create and change packet filter rules. The iptables command is a user-space tool that interacts directly with the netfilter kernel module through the netlink socket. Therefore, allowing traffic to localhost is not needed for the iptables command to work.

References: LPIC-2 202 exam objectives, LPIC-2 202-450 Exam Prep: Network Configuration, Netfilter &#8211; Wikipedia, Iptables Essentials: Common Firewall Rules and Commands

QUESTION 41

Which rdncsub command can be used in conjunction with the name of a zone in order to make BIND reread the content of the specific zone file without reloading other zones as well?

* lookup
* reload
* fileupdate
* reread
* zoneupdate

QUESTION 42

FILL BLANK

Which directive in a Nginx server configuration block defines the TCP ports on which the virtual host will be available, and which protocols it will use? (Specify ONLY the option name without any values.)
listen

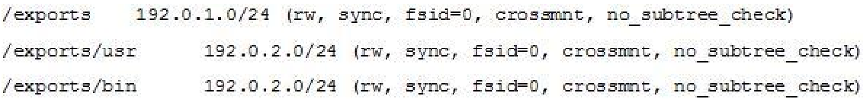
QUESTION 43

Which command is used to administer IPv6 netfilter rules?
* iptables
* iptablesv6
* iptables6
* ip6tables
* ipv6tables
Explanation/Reference: https://www.centos.org/docs/5/html/5.1/Deployment_Guide/s1-ip6tables.html

QUESTION 44

In order to export /usr and /bin via NFSv4, /exports was created and contains working bind mounts to /usr and /bin.

The following lines are added to /etc/exports on the NFC server:



```
/exports     192.0.1.0/24 (rw, sync, fsid=0, crossmnt, no_subtree_check)
/exports/usr      192.0.2.0/24 (rw, sync, fsid=0, crossmnt, no_subtree_check)
/exports/bin      192.0.2.0/24 (rw, sync, fsid=0, crossmnt, no_subtree_check)
```

After running mount-tnfsv4 server://mnt of an NFC-Client, it is observed that /mnt contains the content of the server&#8217;s /usr directory instead of the content of the NFSv4 foot folder.

Which option in /etc/exports has to be changed or removed in order to make the NFSv4 root folder appear when mounting the highest level of the server?

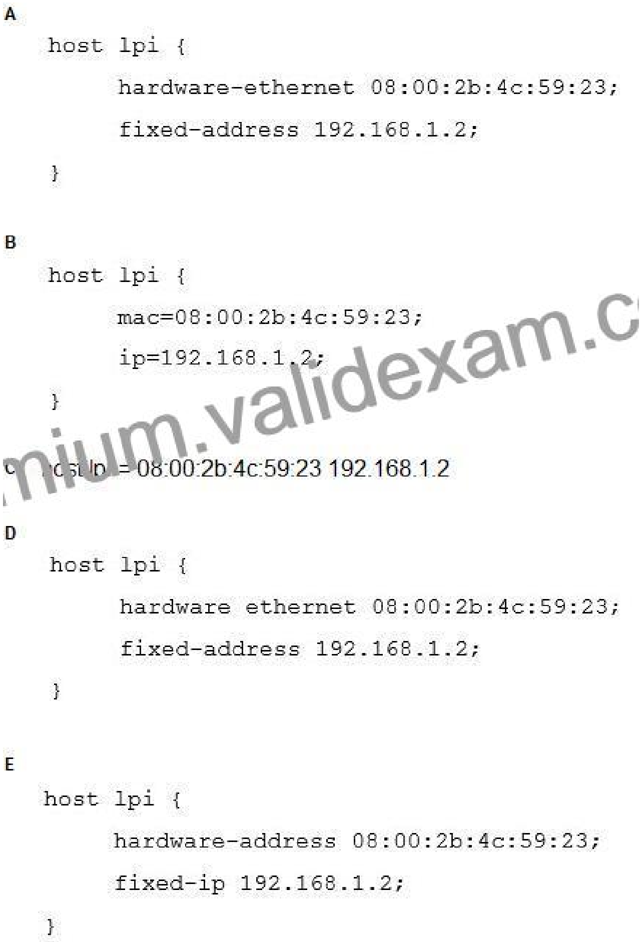
(Specify ONLY the option name without any values or parameters.)
mount

QUESTION 45

A host, called lpi, with the MAC address 08:00:2b:4c:59:23 should always be given the IP address of

192.168.1.2 by a DHCP server running ISC DHCPD.

Which of the following configurations will achieve this?



A

```
host lpi {
      hardware-ethernet 08:00:2b:4c:59:23;
      fixed-address 192.168.1.2;
}
```

B

```
host lpi {
      mac=08:00:2b:4c:59:23;
      ip=192.168.1.2;
}
```

C

```
hostip = 08:00:2b:4c:59:23 192.168.1.2
```

D

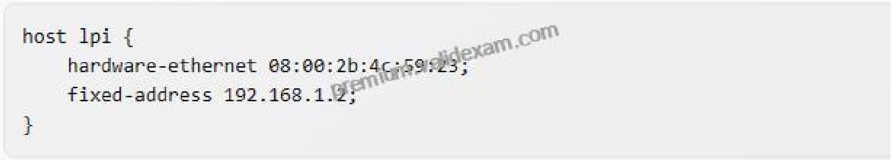
```
host lpi {
      hardware ethernet 08:00:2b:4c:59:23;
      fixed-address 192.168.1.2;
}
```

E

```
host lpi {
      hardware-address 08:00:2b:4c:59:23;
      fixed-ip 192.168.1.2;
}
```

* Option A
* Option B
* Option C
* Option D
* Option E
Explanation

In the ISC DHCPD server configuration, to always assign the IP address 192.168.1.2 to a host with the MAC address 08:00:2b:4c:59:23, you need to create a host declaration within your dhcpd.conf file. Option A provides the correct syntax for this configuration:



```
host lpi {
    hardware-ethernet 08:00:2b:4c:59:23;
    fixed-address 192.168.1.2;
}
```

This configuration ensures that whenever a DHCP request is received from the MAC address specified, the ISC DHCPD server will always assign it the IP address 192.168.1.2.

References:

ISC DHCP 4.1 Manual Pages &#8211; dhcpd.conf: The official documentation of ISC DHCPD on how to configure the dhcpd.conf file, which includes the host declaration syntax and examples.

isc-dhcp-server: Using option dhcp-client-identifier in host declaration to identify a client: A question and answer from Server Fault on how to use the option dhcp-client-identifier in a host declaration, which also shows the use of the hardware-ethernet and fixed-address parameters.

QUESTION 46

Which of the following commands displays an overview of the Postfix queue content to help identify remote sites that are causing excessive mail traffic?
* mailtraf
* queuequery
* qshape
* postmap
* poststats

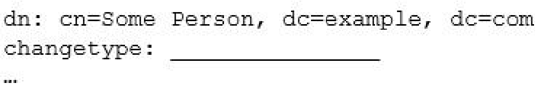
Explanation/Reference: https://easyengine.io/tutorials/mail/postfix-queue/

QUESTION 47

Which option within the ISC DHCPD configuration file defines the IPv4 DNS server address(es) to be sent to the DHCP clients?
* domain-name-servers
* domain-server
* name-server
* servers

QUESTION 48

In order to specify alterations to an LDAP entry, what keyword is missing from the following LDIF file excerpt?



```
dn: cn=Some Person, dc=example, dc=com
changetype: ______________
…
```

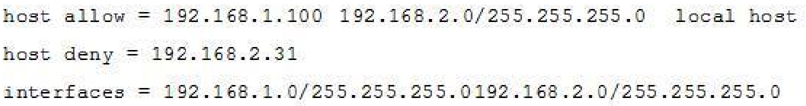
Specify the keyword only and no other information.
add

QUESTION 49

Which command is used to administer IPv6 netfilter rules?
* iptables
* iptablesv6
* iptables6
* ip6tables
* ipv6tables

QUESTION 50

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?
* host allow = 192.168.1.1-255
* host allow = 192.168.1.100192.168.2.200localhost
* host deny = 192.168.1.100/255.255.255.0192.168.2.31localhost
* host deny = 192.168.2.200/255.255.255.0192.168.2.31localhost
* host allow = 192.168.1.0/255.255.255.0192.168.2.0/255.255.255.0 localhost
Explanation

The host allow option in the smb.conf file specifies the hosts or networks that are allowed to access the Samba server. The hosts can be specified by name, IP address, or network address with a netmask. The host allow option can also include the special name localhost, which refers to the local machine. The host allow option can be overridden by the host deny option, which specifies the hosts or networks that are denied access to the Samba server. The host deny option has a higher priority than the host allow option.

In this question, the host allow option is set to 192.168.1.100 192.168.2.0/24 localhost, which means that only the host with the IP address 192.168.1.100, the hosts on the network 192.168.2.0/24 (from 192.168.2.1 to

192.168.2.254), and the local machine can access the Samba server. This explains why a wireless laptop with an IP address 192.168.2.93 can access the Samba server, but a workstation on the wired network with an IP address 192.168.1.177 cannot. Almost every machine on the wired network is unable to access the Samba server because they are not included in the host allow option.

To fix this problem, the host allow option should be changed to include the entire wired network, which is assumed to be 192.168.1.0/24 (from 192.168.1.1 to 192.168.1.254). This can be done by using the network address and the netmask, or by using a range of IP addresses. The host allow option should also keep the wireless network and the localhost in the list, so that the existing access is not denied. Therefore, the correct answer is E. host allow = 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0 localhost. This will allow any host on either network, or the local machine, to access the Samba server, without denying access to anyone else.

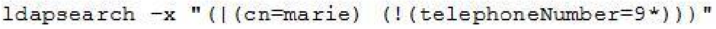
QUESTION 51

When using mod_authz_core, which of the following strings can be used as an argument to Require in an Apache HTTPD configuration file to specify the authentication provider? (Choose three.)
* method
* all
* regex
* header

- expr

QUESTION 52

Which of these sets of entries does the following command return?



```
ldapsearch -x "(|(cn=marie) (!(telephoneNumber=9*)))"
```

- Entries that don&#8217;t have a cn of marie or don&#8217;t have a telephoneNumber that begins with 9.
- Entries that have a cn of marie or don&#8217;t have a telephoneNumber beginning with 9.
- Entries that have a cn of marie and a telephoneNumber that ending with 9.
- Entries that don&#8217;t have a cn of marie and don&#8217;t have a telephoneNumber beginning with 9.
- Entries that have a cn of marie or have a telephoneNumber beginning with 9.

Explanation

The command in the question is using the ldapsearch tool to query an LDAP directory. The filter expression is (|(cn=marie)(!(telephoneNumber=9*))), which means to match entries that satisfy either one of the two conditions inside the parentheses. The first condition is (cn=marie), which means the common name attribute (cn) of the entry is equal to marie. The second condition is (!(telephoneNumber=9*)), which means the telephone number attribute (telephoneNumber) of the entry is not equal to 9 followed by any number of characters. The ! operator means logical negation, and the * operator means wildcard matching. Therefore, the command will return entries that have a cn of marie or don&#8217;t have a telephoneNumber beginning with 9.

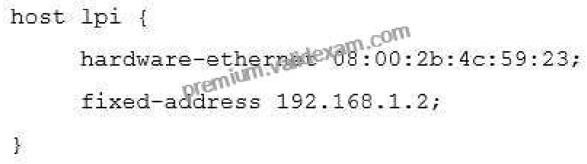
References: LPIC-2 202 exam objectives, LDAP Search Filters

QUESTION 53

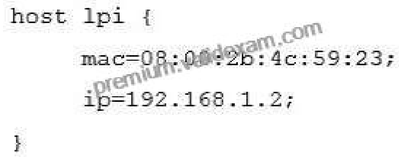
A host, called lpi, with the MAC address 08:00:2b:4c:59:23 should always be given the IP address of

192.168.1.2 by a DHCP server running ISC DHCPD.

Which of the following configurations will achieve this?

- 

```
host lpi {
       hardware-ethernet 08:00:2b:4c:59:23;
       fixed-address 192.168.1.2;
  }
```

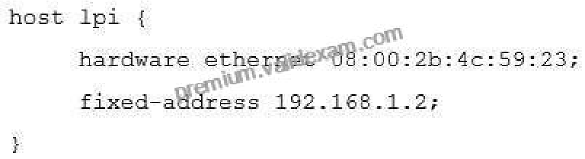
- 

```
host lpi {
       mac=08:00:2b:4c:59:23;
       ip=192.168.1.2;
  }
```

host lpi = 08:00:2b:4c:59:23 192.168.1.2

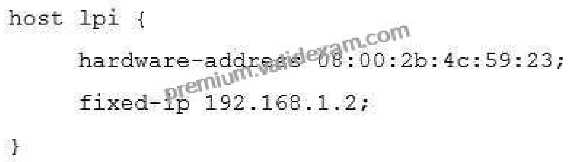
*

*



```
host lpi {
       hardware ethernet 08:00:2b:4c:59:23;
       fixed-address 192.168.1.2;
  }
```

*



```
host lpi {
       hardware-address 08:00:2b:4c:59:23;
       fixed-ip 192.168.1.2;
  }
```

QUESTION 54

Which tool creates a Certificate Signing Request (CSR) for serving HTTPS with Apache HTTPD?
* apachect1
* certgen
* cartool
* httpsgen
* openssl

The LPI 202-450 is the standard exam that requires the individual to know about the networking related areas within the IT field. If you are passionate to pursue your career in the IT sector, this can be a lifetime opportunity for you. You can get the LPIC-2 certification if you pass 201-450 and 202-450 tests. So, now let's get to know more about the second validation.

202-450 certification dumps - LPIC-2 Certified Linux Engineer 202-450 guides - 100% valid:
https://www.validexam.com/202-450-latest-dumps.html]