

# Lead2Passed



Lead2Passed

HOME

ALL VENDORS

★ GUARANTEE

? FAQ

TESTIMONIALS

Login / Register My Shopcart (1)

Input your exam code ...



## Try before you buy

Download a free sample of any of our exam questions and answers

- ✓ Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.
- ✓ PDF format: Easy to read and print learning materials, our products are available in PDF file format.
- ✓ Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.



### Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.



### 365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



### Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.



### Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

<http://www.lead2passed.com>

Valid Certification Exam Dumps Materials and Study Guide -  
Lead2Passed

**Exam** : **202-450-JPN**

**Title** : LPIC-2 Exam 202, Part 2 of 2, version 4.5 (202-450日本語版)

**Vendor** : Cisco

**Version** : DEMO

### QUESTION NO: 1

サンバツール命令をすることは、Samba構成に関して、確認します？

- A. 構成は、うまくロードします。
- B. サービスは、予想通りに営業します。
- C. システムが起動するとき、Sambaサービスは自動的に始まります。

D.

Sambaサーバーのnetfilter構成は、構成で定められるサービスのいかなる利用も妨害しません。

- E. すべての経営Sambaプロセスは、ごく最近の構成版を使います。

**Answer: A**

Explanation

The samba-tool testparm command is a simple test program to check a Samba configuration file for internal correctness. It verifies that the file can be parsed and loaded by Samba without errors or warnings. If the command reports no problems, it means that the configuration file is valid and can be used by Samba.

However, this does not guarantee that the services defined in the configuration file will operate as expected, or that the Samba services are running or enabled on the system. The command also does not check the firewall or netfilter rules on the Samba server, or the version of the configuration file used by the running Samba processes. Therefore, the only correct answer is A.

### QUESTION NO: 2

PAMモジュールはどのように編成され、保管されていますか？

- A. プレーンテキストファイルとして / etc / security /にある
- B. tc/pam.d/bin/に静的にリンクされたバイナリ
- C. / lib / modules /の各サブディレクトリ内のLinuxカーネルモジュールとして
- D. / lib /ディレクトリ階層内の共有オブジェクトファイルとして
- E. / usr / lib / pam / sbin /にある動的にリンクされたバイナリとして

**Answer: D**

Explanation

PAM modules are organized and stored as shared object files within the /lib/ directory hierarchy. A shared object file is a file that contains executable code and data that can be loaded into memory and used by one or more programs. This allows PAM modules to be dynamically loaded and unloaded by the PAM library as needed, without requiring recompilation or relinking of the programs that use them. The /lib/ directory hierarchy contains subdirectories for different architectures and operating systems, such as /lib/x86\_64-linux-gnu/ or /lib64/. The PAM modules are usually located in a subdirectory named security, such as /lib/x86\_64-linux-gnu/security/ or /lib64/security/. The PAM modules have names that start with pam\_ and end with .so, such as pam\_unix.so or pam\_cracklib.so12.

References:

PAM Modules: A section from the Linux-PAM System Administrators' Guide that explains what PAM modules are, how they are named, and where they are located.

An introduction to Pluggable Authentication Modules (PAM) in Linux: An article from Red Hat

that introduces the concept and usage of PAM in Linux, which includes a description of PAM modules and their location.

### QUESTION NO: 3

Nginxサーバー構成ブロックのどの指令がバーチャル・ホストが利用できるTCPポートを定めて、そして、それはどのプロトコルを使う？

( 何のないオプション名でも評価するONLYを指定してください。 )

#### Answer:

listen

Explanation:

The listen 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. The listen directive takes one or more parameters, such as the port number, the IP address, and the protocol name. For example, the following directive tells Nginx to listen for HTTP requests on port 80 on all network interfaces:

```
listen 80;
```

The following directive tells Nginx to listen for HTTPS requests on port 443 on the 192.0.2.1 IP address:

```
listen 192.0.2.1:443 ssl;
```

The following directive tells Nginx to listen for both TCP and UDP traffic on port 53 on the 192.0.2.2 IP address:

```
listen 192.0.2.2:53 udp tcp;
```

The listen directive can also take some options, such as `default_server`, which specifies that the server block should act as the default server for the given port, or `backlog`, which sets the maximum number of pending connections for the socket.

References:

Server Block Examples | NGINX

NGINX Docs | Configuring HTTP Servers

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?

### QUESTION NO: 4

Apache

HTTPDでHTTPSを処理するための証明書署名要求 ( CSR ) を作成するツールはどれですか？

- A. apachect1
- B. certgen
- C. cartool
- D. httpsgen
- E. openssl

Answer: E

Explanation

OpenSSL is a software library that provides cryptographic functions and tools for creating and managing SSL/TLS certificates. One of the tools included in OpenSSL is the command-line utility `openssl`, which can be used to generate various types of cryptographic objects,

such as private keys, public keys, certificate signing requests (CSRs), and certificates. A CSR is a file that contains the information needed by a certificate authority (CA) to issue a digital certificate for a web server. A CSR includes the public key of the web server, the domain name or names that the certificate will cover, and some identifying information about the organization or individual requesting the certificate. To generate a CSR for serving HTTPS with Apache HTTPD, the openssl command can be used with the req option, which stands for request. The req option takes several parameters, such as -new, -newkey, -nodes, -keyout, and -out, to specify the details of the CSR generation process. For example, the following command will generate a new private key and a new CSR for the domain example.com, using a 2048-bit RSA algorithm, and saving the files as example.key and example.csr respectively:

```
openssl req -new -newkey rsa:2048 -nodes -keyout example.key -out example.csr
```

The command will also prompt the user to enter some information for the CSR, such as the country code, state or province name, locality name, organization name, organizational unit name, common name, and email address. The common name is the most important field, as it should match the domain name or names that the certificate will cover. For example, if the certificate is for example.com, the common name should be example.com. If the certificate is for multiple domains, such as example.com and www.example.com, the common name should be one of them, and the rest should be specified as subject alternative names (SANs) in a configuration file. After the CSR is generated, it can be sent to a CA for signing and obtaining a certificate, which can then be installed and configured on the Apache HTTPD server to enable HTTPS.

References:

OpenSSL: The official website of the OpenSSL project, which provides documentation, downloads, and support for the OpenSSL software.

Apache: CSR & SSL Installation (OpenSSL) - DigiCert: A guide from DigiCert on how to create a CSR and install an SSL certificate on an Apache server using OpenSSL.

How to Generate a Certificate Signing Request (CSR) for Apache Web Server Using

OpenSSL - The SSL Store™: A tutorial from The SSL Store on how to generate a CSR for an Apache web server using OpenSSL.

GoDaddy - Apache: Generate CSR (Certificate Signing Request): A step-by-step instruction from GoDaddy on how to generate a CSR for Apache 2.x using OpenSSL.

### QUESTION NO: 5

LDAPエントリに変更を指定するために、どんなキーワードが、以下のLDIFファイル抜粋からなくなっていますか？

```
dn: cn=Some Person, dc=example, dc=com
```

```
changetype: _____
```

```
...
```

キーワードだけおよび他の情報を全然指定してはならない。

**Answer:**

modify

Explanation

In the context of LDAP, when alterations need to be specified to an entry, the "changetype:

modify" keyword is used in the LDIF file. This keyword indicates that modifications are to be made to the existing LDAP entry.

The modify operation can be used to add, replace, or delete attributes and their values. The syntax of the modify operation is as follows:

```
changetype: modify add: attribute attribute: valuereplace: attribute attribute: valuedelete: attribute attribute: value
```

Each modify operation is separated by a hyphen (-) and a blank line separates different entries. The attribute;binary subtype can be used to indicate that the attribute values are binary data. The LDIF syntax for reading a binary value from a file is:

```
attribute;binary:< file:///path/to/file
```

References:

LPIC-2 Exam 202 Objectives, Objective 207.3: LDAP Operations

How To Use LDIF Files to Make Changes to an OpenLDAP System, DigitalOcean Modifying Entries Using ldapmodify, Oracle ldap - ldapadd/ldapmodify: clarifications needed about these commands, Server Fault Modify Attribute type definition on LDAP server, Stack Overflow

## QUESTION NO: 6

ISC

DHCPD構成の次のステートメントのどれを使用して、構成内の対応するホストセクションを持つノードがアドレスプールを使用できるかどうかを指定しますか？

- A. identified-nodes
- B. unconfigured-hosts
- C. missing-peers
- D. unmatched-hwaddr
- E. unknown-clients

**Answer:** E

Explanation

The unknown-clients statement in the ISC DHCPD configuration is used to specify whether or not an address pool can be used by nodes which have a corresponding host section in the configuration. A host section is a declaration that defines a static IP address for a specific client based on its MAC address or other identifier.

An unknown client is a client that does not have a host section. The unknown-clients statement can be either allow, deny, or ignore, and it can be applied to a pool, a subnet, or a shared-network. For example, the following configuration allows unknown clients to use the pool of addresses from 192.168.1.100 to

192.168.1.200, but denies them from using the pool of addresses from 192.168.1.201 to 192.168.1.254:

```
subnet 192.168.1.0 netmask 255.255.255.0 { pool { range 192.168.1.100 192.168.1.200; allow unknown-clients; } pool { range 192.168.1.201 192.168.1.254; deny unknown-clients; } }
```

References:

ISC DHCP 4.4 Manual Pages - dhcpd.conf: The official documentation of ISC DHCPD on how to configure the dhcpd.conf file, which includes the description of the unknown-clients statement and examples.

How To Configure a DHCP Server on Ubuntu 20.04 | DigitalOcean: A tutorial from

DigitalOcean on how to configure a DHCP server on Ubuntu 20.04, which includes the use of the unknown-clients statement and host sections.

**QUESTION NO: 7**

リモートのTCPネットワークサービスと接続し、対話するために、以下のコマンドのうちのどれが使用できるか？

( 2つを選択してください )

- A. nettalk
- B. nc
- C. telnet
- D. cat
- E. netmap

**Answer:** B C

Explanation

The commands nc and telnet can be used to connect and interact with remote TCP network services. nc stands for netcat, a utility that can read and write data across network connections using TCP or UDP protocols.

telnet is a client-server protocol that allows a user to communicate with a remote host using a virtual terminal.

Both commands can be used to test the connectivity and functionality of network services such as web servers, mail servers, FTP servers, etc. by specifying the host name or IP address and the port number of the service.

References:

LPIC-2 exam 201 topics, section 205.1, "Use and configure network monitoring tools".

LPIC-2 exam 202 topics, section 208.1, "Implementing a web server".

Linux Essentials 010 exam objectives, section 4.3, "Basic network configuration and troubleshooting".

**QUESTION NO: 8**

netfilter

INPUTチェーンのデフォルトポリシーがDROPに設定されている場合、なぜローカルホストへのトラフィックを許可するルールが存在するのでしょうか？

- A. localhostへのすべてのトラフィックは、常に許可する必要があります
- B. それは問題ではありません; netfilterはローカルホスト宛のパケットには影響しません
- C. 一部のアプリケーションでは、localhostインターフェイスを使用して他のアプリケーションと通信します
- D. syslogdはlocalhostでメッセージを受信します
- E. iptablesコマンドは、localhost上のnetfilter管理デーモンnetfilterdと通信して、パケットフィルタルールを作成および変更します

**Answer:** C

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'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 - Wikipedia, Iptables Essentials: Common Firewall Rules and Commands

### QUESTION NO: 9

標準のポートは何でOpenVPNにより使われるか？

- A. 1723
- B. 4500
- C. 500
- D. 1194

**Answer:** D

## Explanation

The standard port used by OpenVPN is 1194. OpenVPN is a VPN daemon that supports SSL/TLS security, ethernet bridging, TCP or UDP tunnel transport, and other features. OpenVPN can be configured to listen on any port, but the default port is 1194, which is registered with the IANA for OpenVPN. The port number can be specified in the OpenVPN configuration file using the port directive. For example:

```
port 1194
```

This will instruct OpenVPN to listen on port 1194. The port number must match on both the server and the client sides of the connection. The port number can also be specified as an argument to the `openvpn` command.

For example:

```
openvpn --port 1194
```

This will run OpenVPN with port 1194 as the default port.

References:

Reference Manual For OpenVPN 2.6 | OpenVPN

Reference Manual For OpenVPN 2.0 | OpenVPN

Which ports to open for VPN PPTP, L2TP, IPsec, OpenVPN and ... - ITIGIC

## QUESTION NO: 10

サンバコンフィギュレーションファイルは以下のラインを含んでいる :

```
host allow = 192.168.1.100 192.168.2.0/255.255.255.0 local host
```

```
host deny = 192.168.2.31
```

```
interfaces = 192.168.1.0/255.255.255.0 192.168.2.0/255.255.255.0
```

ワークステーションは、192.168.1.177のIPアドレスを持つつながっているネットワークにあるけれども、サンバサーバーにアクセスすることができない。IPアドレス192.168.2.93を持つワイアレスのラップトップは、サンバサーバーにアクセスできる。追加の故障発見修理は、つながっているネットワークのほとんどすべてのマシンがサンバサーバーにアクセスすることができないことを示す

どの交替のホストが、宣言が、アクセスを他の誰かに拒まずに、つながっているワークステーションがサンバサーバーと接続することを許すと認めるか？

A. host allow = 192.168.1.1-255

B. host allow = 192.168.1.100 192.168.2.200 localhost

C. host deny = 192.168.1.100/255.255.255.0 192.168.2.31 localhost

D. host deny = 192.168.2.200/255.255.255.0 192.168.2.31 localhost

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

**Answer: E**

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 NO: 11**

次のnamed.confファイルの抜粋には、どのような単語が行方不明であるか？

```
_____ friends {  
    10.10.0.0/24; 192.168.1.0/24;  
};  
  
options {  
    allow-query { friends; };  
};
```

- A. networks
- B. net
- C. list
- D. acl
- E. group

**Answer:** D

Explanation

The word missing from the excerpt of a named.conf file is "acl". This is because the excerpt is defining an access control list (ACL) for the DNS server. The ACL is used to restrict access to the DNS server and is defined in the named.conf file. The syntax for defining an ACL is:

```
acl name { address_match_list; };
```

where name is the name of the ACL, and address\_match\_list is a list of IP addresses,

networks, or keywords that match the clients that are allowed or denied access. References:

LPIC-2 Overview

LPIC-2 202-450

BIND 9 Administrator Reference Manual

**QUESTION NO: 12**

既定でDNSサーバー上の再帰的クエリを無効にするグローバルオプションには、BINDのどのオプションが必要ですか？

- 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<sup>123</sup>

References:

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