

Exam Report: 1.1.5 Practice Questions

Date: 2/18/2020 4:54:02 pm
Time Spent: 9:32

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 87%



View results by: ☐ Objective Analysis ☒ Individual Responses

Individual Responses

▼ Question 1: Correct

Linux can be implemented in many different ways.

Drag the implementation type to the definition that matches it BEST.

Running Linux and Windows on the same physical computer.

✓ Linux virtualization

Infrastructure as a Service (IaaS).

✓ Linux and Cloud Computing

Used by Google on many of the physical products it sells.

✓ Linux on mobile devices

Manages intelligent devices, such as automation and control equipment.

✓ Embedded Linux

Explanation

Linux on mobile devices:

Linux has nearly taken over the mobile device market in the form of the Android operating system. The current Android operating system is a specialized Linux distribution created by Google. It was designed primarily for touch screen mobile devices, such as smart phones, and tablet computers.

Linux Virtualization:

Virtualization is the ability to install and run multiple operating systems concurrently on a single physical machine. The Linux operating system can be virtualized.

Embedded Linux:

Embedded Linux is the process of embedding Linux within intelligent devices, such as automation and control equipment, smart TVs, smart phones, and tablets. To accomplish this, the operating system is reworked and customized in such a way that it provides only the functions required by that particular device and all the remaining unnecessary elements of the Linux kernel are removed. Once that's done, the kernel itself is embedded in flash memory chips on the given device.

Linux and Cloud Computing:

In cloud computing, the hardware, software, and/or network resources that have historically been implemented onsite are moved offsite. When a new Linux system is required, you can use an internet cloud provider to deploy the new Linux virtual machine using a hypervisor at their site. You then pay that provider a fee to access this virtual machine through your organization's network connection. This process is referred to as Infrastructure as a Service (IaaS).

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_LINUX_INTRO_LP5_02]

▼ Question 2: Correct

Users are complaining that the clocks for their operating systems do not match the current time for the location in which they live.

Which of the following server roles is BEST for correcting this issue?

- ☐ SSH
- ☐ DHCP
- ☐ Proxy
- ➡ ☒ NTP

Explanation

The Network Time Protocol (NTP) is used to synchronize the time on your Linux system with a centralized NTP server. A local NTP server on the network can be synchronized with an external timing source to keep all the servers in your organization in sync with an accurate time. NTP uses a hierarchy of clocks and computers for synchronizing the current time.

SSH (Secure Shell or Secure Socket Shell) is a protocol used to securely log onto remote systems using encryption.

The Dynamic Host Configuration Protocol (DHCP) centralizes IP address assignment management by allowing a server (such as a Linux server) to dynamically assign IP addresses to clients.

A Proxy server is used to access the internet using a shared connection on a LAN and cache internet content. A proxy server provides internet access control among other features.

References

Linux Pro - 1.1 Linux Introduction

[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_01]

▼ Question 3: Correct

Users are complaining that they are unable to connect to any servers or the internet. Based on the symptoms they describe, you suspect that the users are not being assigned the correct IP addresses.

Which of the following server roles would be the BEST role to work with to correct this issue?

- ☐ Proxy
- ➡ ☒ DHCP
- ☐ SNMP
- ☐ VPN

Explanation

The Dynamic Host Configuration Protocol (DHCP) centralizes IP address assignment management by allowing a server (such as a Linux server) to dynamically assign IP addresses to clients. DHCP also allows users who move from network to network to easily obtain an IP address appropriate for the subnet they are connected to. Since the users are not able to connect to each other as well as to the internet, the most likely cause is an issue with the DHCP server.

A proxy is a computer that provides indirect internet access to the computers in your network. In most cases, a proxy server is installed on the same computer as the firewall. Although the proxy could be part of the problem, since the users are not able to communicate with each other, it would not be the only or main issue.

The Simple Network Management Protocol (SNMP) is a protocol designed for managing complex networks and is used to communicate with and monitor network devices, servers, and other devices through the IP protocol. SNMP lets network hosts exchange configuration and status information.

A VPN (Virtual Private Network) can be installed on a Linux host and is a type of network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. Although the VPN could be part of the problem, since the users are not able to communicate with each other, it would not be the only or main issue.

References

Linux Pro - 1.1 Linux Introduction

[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_02]

▼ Question 4: Correct

Drag the server role to its proper description.

A protocol used to communicate with and monitor network devices and servers.

✓ SNMP

A protocol used to securely log on to remote systems using encryption.

✓ SSH

Resolves (or maps) the fully qualified domain names (FQDNs) to IP Addresses.

✓ Name server

A program responsible for accepting HTTP (Hypertext Transfer Protocol) requests from clients.

✓ Web server

Explanation

SSH (Secure Shell or Secure Socket Shell) is a protocol used to securely log onto remote systems using encryption. SSH is the most common way to access a remote Linux system. OpenSSH is an open-source implementation of the Secure Shell (SSH) protocol and is implemented on most Linux distributions by default.

A web server is the program responsible for accepting HTTP (Hypertext Transfer Protocol) requests from web browsers or clients and, in turn, sending the clients the files that form webpages. For example, webpages often consist of HTML (Hypertext Markup Language) documents and linked objects, such as images. A machine that has been dedicated to perform this role is also called a web server.

A name server resolves (or maps) the fully qualified domain names (FQDNs), such as *www.TestOut.com*, to their respective IP addresses and IP addresses to their respective FQDNs. This would let a user access the TestOut site from her web browser by entering *https://www.TestOut.com* instead of something like *https://104/16/32/53*.

The Simple Network Management Protocol (SNMP) is a protocol designed for managing complex networks and is used to communicate with and monitor network devices, servers, and other devices through the IP protocol. SNMP lets network hosts exchange configuration and status information. For example, SNMP can be used to remotely retrieve the operational statistics of a router or a firewall. On a Linux machine, SNMP runs as a daemon.

References

Linux Pro - 1.1 Linux Introduction

[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_03]

▼ Question 5: Correct

Drag the server role to its proper description.

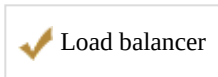
Capturing a timeline of events that have taken place on the computer in the form of a file.

✓ Logging

A type of network that uses encryption to allow IP traffic to travel securely over the TCP/IP network.

✓ VPN

Increases response time to back-end servers by distributing the workload across the available servers.



A computer that provides indirect internet access to the computers in your network.



Explanation

Proxy: A proxy is a computer that provides indirect internet access to the computers in your network. In most cases, a proxy server is installed on the same computer as the firewall. Proxy servers provide increased performance and security by blocking direct access between two networks, such as the corporate network and the internet. Proxy can be configured in a variety of ways, such as using SSH tunneling or installing an app on a system that has been configured as a Web server.

Logging: An important Linux role is the ability to capture a timeline of events that have taken place on the computer in the form of a file, referred to as a log file. The process of creating these logs is known as logging. Logging is enabled by default and logs are often captured for such things as services, the Linux operating system, and applications. Logging is useful for such things as troubleshooting, security, and for evaluating server performance. If desired, you can configure a centralized logging server making it easier to evaluate and use the logs created on many systems. Although log files can be stored in a variety of places, most logs are stored in the /var/log directory or a subdirectory thereof.

VPN: A VPN (Virtual Private Network) can be installed on a Linux host and is a type of network that uses encryption to allow IP traffic to travel securely over the TCP/IP network. A VPN is used primarily to support secure communications over an untrusted network. For example, connecting two remote site by means of the internet.

Load balancer: When a company has back-end servers that receive a significant amount of traffic (such as Netflix, Hulu and Airbnb), response time to these servers can be increased through load balancers by distributing the workload across the available servers. Although load balancers can be purchased as a hardware appliance, software can be installed on a Linux server, making it a load balancer. Three common Linux load balancers include Linux Virtual Server (a free and open-source project), Nginx, and HAProxy, all of which run on top of Linux. Some of the load balancer software is free and some are for pay.

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_04]

▼ Question 6: Correct

Your company develops applications to run on Linux systems. You currently have four teams working on a different aspect of the same application.

Which of the following server roles would give you the BEST method for testing all team members' code without effecting your part of the project or your operating system and personal files?

- ☐ Monitoring
- ☐ Database
- ☐ Load balancer
- ☒ Containers
- ☐ Clustering

Explanation

Linux containers give you the ability to run an application (with all of the necessary libraries, dependencies, and files) in an isolated environment known as an image or container. Due to this isolation, multiple containers can run on the same host without affecting each other or the main operating system. All containers utilize and share the same operating system kernel of the host machine, making them very lightweight and fast.

Containers are highly portable. When you move or copy a container from one host to another, all of the files and changes necessary to run the applications within the container are moved or copied with it. Moving a container to a new host does not impact the host operating system. Although Linux containers are extremely portable, they must be compatible with the underlying system. For example, x86 Linux systems will run x86 containers while ARM Linux systems only run ARM Linux containers. However, an x86 Linux system cannot run an ARM Linux container.

With clustering, two or more servers are grouped together to make them work like one. Clustering is often used to create a failover system, a load balance system, or a parallel processing unit.

Load balancers distribute workload across available servers, which increases response time.

Monitoring refers to the process of monitoring the essential Linux services, including operating system metrics, process state, logs, service state, and file system usage. It also refers to monitoring servers' availability.

A database is a structured set of data held in a computer, especially one that is accessible in various ways. In simpler terms, a database is an organized collection of various forms of data.

References

Linux Pro - 1.1 Linux Introduction

[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_05]

▼ Question 7: Correct

Tim, a system administrator, wants to simplify the provisioning and disabling of user accounts.

Which of the following server roles should Tim install and configure?

☐ Proxy

➡ ☒ Authentication server

☐ Containers

☐ Load balancer

Explanation

Linux centralized authentication using an authentication server makes provisioning and disabling user accounts easier.

A proxy is a computer that provides indirect internet access to the computers in your network.

Linux containers give you the ability to run an application (with all of the necessary libraries, dependencies, and files) in an isolated environment known as an image or container.

When a company has back-end servers that receive a significant amount of traffic (such as Netflix, Hulu, or Airbnb), response time to these servers can be increased through load balancers by distributing the workload across the available servers.

References

Linux Pro - 1.1 Linux Introduction

[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_AUTH_SERVER]

▼ Question 8: Correct

Your company recently setup a VPN and wants to use a digital certificate for authentication instead of a pre-shared key.

Which of the following server roles would allow the company to provide this functionality internally instead of using an external provider?

☐ SNMP

➡ ☒ Certificate Authority

☐ SSH

☐ Name server

Explanation

At times, you may find that using digital certificates within your own organization can be beneficial. For example, when using VPNs, you could use a digital certificate for authentication instead of a pre-shared key. Digital certificates could also be useful for such things as your development and staging systems. Rather than paying a public certificate authority for digital certificates for your internal needs, you can configure a Linux system to be a certification authority. One method for doing this is to use OpenSSL, a free open-source library.

A name server resolves (or maps) fully qualified domain names (FQDNs), such as `www.testout.com`, to their respective IP addresses, and IP addresses to their respective FQDNs.

The Simple Network Management Protocol (SNMP) is a protocol designed for managing complex networks and is used to communicate with and monitor network devices, servers, and more by means of the IP protocol.

SSH (Secure Shell or Secure Socket Shell) is a protocol used to securely log onto remote systems using encryption. SSH is the most common way to access a remote Linux system.

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_CERT_AUTH]

▼ Question 9: Correct

Your company is running a critical business application. The executive team wants to ensure the server is available at all times, even in the event of a server failure.

Which of the following server roles would be used to provide a failover server in the event of a system failure?

☐ Proxy

☐ SNMP

➡ ☒ Clustering

☐ Load balancer

Explanation

Clustering is often used to create a failover system, a load balance system, or a parallel processing unit. A failover cluster means that if one system fails, the other servers will take over the load, giving end-users uninterrupted access to the desired data. There are many options for building a Linux cluster, including using free open-source software (such as OpenHPC) or purchasing a commercial product. .

When a company has back-end servers that receive a significant amount of traffic (such as Netflix, Hulu, or Airbnb), response time to these servers can be increased through load balancers by distributing the workload across the available servers.

A proxy is a computer that provides indirect internet access to the computers in your network. In most cases, a proxy server is installed on the same computer as the firewall.

The Simple Network Management Protocol (SNMP) is a protocol designed for managing complex networks and is used to communicate with and monitor network devices, servers, and more by means of the IP protocol.

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_CLUSTERING]

▼ Question 10: Correct

Alex, a webmaster, is implementing an order processing system on the company's website.

Which of the following server roles should Alex implement with the order processing application?

- ☐ Clustering
- ☐ VPN
- ☐ Monitoring

➡ ☒ Database

Explanation

A database server should be implemented with the order processing application to store the data gathered by the application.

Monitoring refers to the process of monitoring the essential Linux services, including such things as operating system metrics, process state, logs, service state, and file system usage.

Clustering is often used to create a failover system, a load balance system, or a parallel processing unit. A failover cluster means that if one system fails, the other servers will take over the load, giving end users uninterrupted access to the desired data.

A VPN (Virtual Private Network) is a type of network that uses encryption to allow IP traffic to travel securely over the TCP/IP network.

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_DATABASE]

▼ Question 11: Correct

Your company uses both Linux desktops and Windows desktops.

Which of the following server roles should be used to provide a central location for users of both operating systems to share files?

- ☐ Proxy
- ☐ Authentication server

➡ ☒ File servers

- ☐ Database

Explanation

A Linux file server is a machine that has been set up and configured to let other machines store and retrieve files to and from a central location. In addition, using a file server can simplify backups and security. Using SMB shares and a variety of programs such as Samba or Network File System, a Linux file server can share files with other Linux systems, as well as with non-Linux systems such as Windows and Mac.

Linux centralized authentication (an authentication server) can be accomplished in many ways, depending on the Linux distribution being used.

A proxy is a computer that provides indirect internet access to the computers in your network. In most cases, a proxy server is installed on the same computer as the firewall.

A database is a structured set of data held in a computer, especially one that is accessible in various ways. In simpler terms, a database is an organized collection of various forms of data.

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_FILE_SERVERS]

▼ Question 12: Incorrect

Your company has been expanding the number of servers in the company's data center, and there is an increased need to gather metrics, watch process states, work with logs, watch services states and file system

usage.

Which of the following sever roles should be installed to provide this functionality?

- ☒ Logging
- ☐ Containers
- ☐ Database
- ➡ ☐ Monitoring

Explanation

Monitoring refers to the process of monitoring the essential Linux services, including such things as operating system metrics, process state, logs, service state, and file system usage. It also refers to monitoring servers' availability.

Depending on the Linux distribution, monitoring information can often be gathered manually using command line monitoring tools, such as top , lsof , tcdump , and vmstat . Web-based utilities (such as Monit and Nagios) can also be installed, which usually provides some type of user interface that makes seeing and analyzing the information easier.

A database is a structured set of data held in a computer, especially one that is accessible in various ways. In simpler terms, a database is an organized collection of various forms of data.

An important Linux role is the ability to capture a timeline of events that have taken place on the computer in the form of a file, which is referred to as a log file.

Linux containers give you the ability to run an application (with all of the necessary libraries, dependencies, and files) in an isolated environment known as an image or container.

References

Linux Pro - 1.1 Linux Introduction

[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_MONITORING]

▼ Question 13: Correct

Which of the following is the primary role of a mail transfer agent (MTA)?

- ☐ Control the bandwidth used by mail user agent (MUA).
- ➡ ☒ Store messages so they can be downloaded or send email to a destination MTA.
- ☐ Provide redundant online storage for the mail sever.
- ☐ Transfer mail to a print server queue.

Explanation

The mail transfer agent (MTA) has been installed. It is the MTA's responsibility to then either save the message so it can be downloaded by another local user or, using the internet, send the email to the destination MTA, where it will be stored for download by the intended user.

The MUA is the email client, such as Evolution, Mozilla Thunderbird, or Mutt.

Redundant online storage and transferring email to a print server are not performed by the MTA.

References

Linux Pro - 1.1 Linux Introduction

[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_MTA]

▼ Question 14: Correct

Which of the following server roles would you implement to provide services offered by CUPS and IPP?

- ➡ ☒ Print server
- ☐ Proxy

- ☐ SSH
- ☐ Monitoring

Explanation

When a company wants to make a printer available to multiple users over a network, this goal is typically accomplished using a print server. Print servers accept the print jobs from the users and stores them in a queue. When the appropriate printer is available, the job is sent from the queue to the printer. In addition, a print server makes printer queue and status information available to end users and network administrators. The Common UNIX Printing System, or CUPS, is the most common Linux printing system in use today. CUPS manages print jobs and queues and provides network printing using the standard Internet Printing Protocol (IPP).

A proxy is a computer that provides indirect internet access to the computers in your network. In most cases, a proxy server is installed on the same computer as the firewall.

SSH (Secure Shell or Secure Socket Shell) is a protocol used to securely log on to remote systems using encryption.

Monitoring refers to the process of monitoring the essential Linux services, including such things as operating system metrics, process state, logs, service state, and file system usage.

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_PRINT_SERVER]

▼ Question 15: Incorrect

A technician has been given a work order to install the Apache webserver on a system configured with a YUM repository. Which of the following commands will install the webserver?

- ☐ **dnf install httpd**
- ➡ ☐ **yum install httpd**
- ☒ ~~yum install apache2~~
- ☐ **rpm -ivh apache2**

Explanation

yum install httpd is used to install Apache on a system using a YUM repository.
dnf install httpd would work on systems where dnf is used instead of YUM.

yum install apache2 will return "No package apache2 available."

rpm -ivh apache2 will return "No such file or directory." The **rpm** command need the full .rpm file name.

References

Linux Pro - 1.1 Linux Introduction
[e_linux_intro_lp5.exam.xml Q_SERVER_ROLES_LP5_WEB]