1.1.4 Server Roles Facts

This lesson covers the following topic:

- Linux Server Roles

Linux Server Roles

As a result of the continued popularity, growth, and development of Linux, it can now fulfill many server roles. In most cases, a server role is an application or process installed on a Linux server. In some cases, the Linux server may be dedicated to run or fulfill a single server role, while at other times, several server roles may be functioning on the same server.

The following table summarizes and explains several of the Linux server roles.

Role	Description
NTP	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. NTP uses stepping to quickly make large adjustments to close wide time discrepancies, usually about once every 60 seconds. For example, if there's a big differential between the time provider's time and the time on your local system, NTP will adjust the time on your local system in small increments until the time eventually becomes synchronized.
SSH	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 implemented by default on most Linux distributions. Two major components of SSH include the SSH client and the SSH server. The SSH client is a program that is typically only run as needed. Once installed, the SSH server is a daemon that constantly runs in the background.
Web server	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 performing this role is also called a web server. A few examples of Linux web server implementations include: ▪ Apache server ▪ Nginx ▪ Lighttpd ▪ Apache Tomcat ▪ Monkey HTTP Daemon
Certificate authority	A digital certificate is an electronic document that can be used as proof of identification. For example, digital certificates are used between an end user and a bank to establish a trusted connection. As an end user, we trust digital certificates because we trust the entities that create the digital certificates. The entities that create these certificates are called certificate authorities (CAs). A few of the most public certificate authorities include GeoTrust, Comodo, Digicert, Thawte, Verisign and GoDaddy. These CAs require the person or company applying for a certificate (such as your bank) to provide documents and information that proves they are who they claim to be. 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 of doing this is to use OpenSSL, a free open-source library.
Name 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. For example, this lets a user access the TestOut site from their web browser by entering https://www.TestOut.com instead of something like https://104/16/32/53. In many cases, you need to download and install a name resolver software on your Linux system to enable the name server features. The Berkeley Internet Name Domain (BIND) software is an example of one of the most widely used DNS software on the internet.
DHCP	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. The DHCP server and the client use broadcasts to communicate with each other. In many cases, you need to download and install the DHCP server software. For example, for a Ubunto server, enter **$ sudo apt install isc-dhcp-server** at the command prompt.

	Configuration of the server can then be completed as needed.
SNMP	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. 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. In many cases, you need to download and install SNMP. For example, to install SNMP on a CentOS system ,enter **yum -y install net-snmp net-snmp-utils** at the command prompt.
File servers	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.
Authentication server	Most enterprise networks require centralized user authentication and access controls for all system resources. This is not only convenient for users, but also allows an administrator to monitor and audit user types and the type of access they have on each machine. It also makes provisioning and disabling user accounts easier. Linux centralized authentication (an authentication server) can be accomplished in many ways, depending on the Linux distribution being used. Some options include installing and using OpenLDAP (Lightweight Directory Access Protocol) or purchasing programs that aid in the installation and management of centralized authentication, such as FreeIPA Identity & Access Manager.
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, which is 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 troubleshooting, security, and evaluating server performance. 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.
Containers	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 be 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 on the host operating system. Although Linux containers are extremely portable, they must be compatible with the underlying system. For example, x86 Linux systems run x86 containers while ARM Linux systems only run ARM Linux containers. However, an x86 Linux system cannot run an ARM Linux container.
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 primarily used to support secure communications over an untrusted network (for example, connecting two remote site by means of the internet).
Monitoring	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.
Database	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. The information stored in a database is typically organized into rows, columns, and tables. Database information is also indexed, to make it easier to find the information required. Many open-source databases are available for Linux, which allow you to manage large chunks of data in a secure way with high performance abilities. Many versions of Linux databases can be installed on your Linux system, such as MySQL, Apache Derby, and PostgreSQL.
Print server	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).
Mail server	

	A mail server is a computer that sends, receives, and stores email for users. When a user creates an email, he or she does so using a mail user agent (MUA) (such as Evolution, Mozilla Thunderbird, or Mutt). The MUA must be configured to send and receive mail by means of a mail server or a Linux system where 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. Some Linux distribution may have a default MTA that can be configured and used. If one does not exist or you want to use a different email system, other MTAs can be downloaded and installed. A few common MTAs include Postfix and Qmail.
Load balancer	When a company has back-end servers that receive a significant amount of traffic (such as Netfilx, Hulu, or 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 must be purchased.
Clustering	With clustering, two or more servers are grouped together in a way to make them work like one. 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.