Linux Fundamentals

Exam Information

Exam number
890

Items
41

Points
70

Prerequisites
Introduction to Information Technology

Recommended course length
One semester

National Career Cluster
Information Technology

Performance standards
N/A

Certificate available
Yes

Description

The Linux Fundamentals industry certification exam assesses the competencies required for a junior-level Linux administrator. Learners demonstrate their knowledge of how to work at the Linux command line, perform maintenance tasks such as assisting users, adding users to a system, executing backup and restore, and managing system shutdowns and reboots. Learners also show their understanding of installing and configuring a workstation, including X, and connecting it to a LAN or standalone PC via modem to the Internet.

Exam Blueprint

Standard	Percentage of exam
1. System architecture	27%
2. Linux installation & package management	32%
3. GNU & Unix commands	20%
4. Devices, Linux Filesystems, Filesystem Hierarchy Standard	22%

Standard 1

Introduction to the Linux operating system

Objective 1 Linux Char Linux Characteristics

1. Be familiar with the history of Linux.
2. Understand the difference between free, open-source, and Free and Open Source (FOSS) software
3. Distribution Types
    a. Commercial (e.g. RedHat Enterprise, Linux SUSE)
    b. Home (e.g. Ubuntu, Fedora, Linux Mint)
    c. Security (e.g. Kali, Alpine)
    d. Live (e.g. Manjaro, Antegros)
4. Distribution Base
    a. RedHat-based (e.g. Redhat, Fedora, CentoS)
    b. Debian-based (e.g. Debian, Ubuntu)
    c. Security-based (e.g. Kali, LinuxSE)
5. Differentiate between Command Line Interface (CLI) and Graphical user Interface (GUI).
6. Perform basic commands using the CLI.
7. Use and modify the shell environment, including defining, referencing and exporting environment variables.
8. Use the history command to view the history of commands that have been typed.

Objective 2 Linux File S d 2: Linux File System Hier em Hierarch

1. Understand the Linux Filesystem Hierarchy (FHS).
2. Understand how directories work.
3. Understand how permissions affect the file system
4. Understand that the Linux Filesystem Hierarchy is a definition of what files and directories are placed based on their contents.
5. Identify and understand important folders and what types of files they contain including:
    a. Root: symbolized with a single slash, /, indicating the top-level directory.
    b. Boot: files relating to the booting/starting the system.
    c. Bin: critical binary executables.
    d. Etc: configuration files.
    e. Home: user home directory
    f. Usr: libraries, binaries, and documentation for installed software applications.
6. Know how to show and hide hidden files in a directory.

Objective 3 W d 3: Working with the CLI

1. Understand that a shell is a program that is used to type and issue commands to the system. Examples of a shell include Bash, Z Shell (zsh), and Kornshell (ksh).
2. Use basic and common shell commands, including:
    a. cat
    b. cd
    c. less
    d. ls
    e. pwd
    f. touch
    g. tree
    h. shutdown

i. whoami
3. Use simple and advanced wildcard specifications in commands.
4. Using built-in man pages, help command, and Linux manual to get the description and usage of Linux commands.
5. Use streams, pipes and redirects in a command.
6. Redirect standard input, standard output, and standard error.
7. Pipe the output of one command to the input of another command.
8. Use the output of one command as arguments to another command.
9. Send output to both stdout and file.

Standard 2

User and file management

Objective 1 Manage Users

1. Identify where user account data is stored.
   a. /etc/passwd file contains the user information settings.
   b. /etc/shadow file stores the password information for the user account.
2. Identify permissions of a standard user.
3. Identify and understand the superuser or root account.
4. Escalate privileges with su and sudo commands.
5. Use commands to create and modify users
   a. useradd or adduser as appropriate
   b. usermod
   c. userdel
   d. passwd
   e. chage

Objective 2 Manage Groups

1. Understand that group data is contained inside the /etc/group files.
2. Use the following commands to create and modify groups:
   a. groupadd
   b. groupmod
   c. groupdel
3. Add and modify group membership using the *useradd* command.

Objective 3 Con d 3: Configure Permissions

1. Understand the use of Linux standard permissions.
   a. Access Levels: read, write, and execute (rwx).
   b. Access Identity: user (owner), group, and others.
2. Understand that other permission types exist aside from the standard permissions, such as special permissions and Access Control Lists (ACLs).
3. Display and identify existing permissions using the ls -l command.
4. Interpret permission strings of files and directories.
5. Modify permissions using umask and chmod command.
   a. use absolute and symbolic modes with the *chmod* command.
6. Understand the concept of ownership in Linux in relation to permissions.
   a. Use the *chown* and *chgrp* to modify the user or group own of a file or a directory.

Objective 4 File Manag File Management

1. Perform basic file management, such as display, copy, move, and delete files and directories individually and recursively.
2. Display file metadata using the stat and file commands.
3. Use proper Linux file naming conventions.
4. Compare the differences between absolute and relative file paths.
5. Navigate the linux file system.
    a. Use of *cd* command to navigate to and from a directory.
    b. Use the ~ command to indicate the root directory.
    c. Use the *pwd* command to display the current working directory.
    d. Use *grep* and *find* commands to find files and search the content of a file.

Objective 5 Text File Editing

1. Open a text file using vi, vim, nano, or gedit.
2. Insert, edit, delete, copy and find text within a text file.

Standard 3

Implementing Shell scripts

Objective 1 Script Basics

1. Understand why scripts are used when managing a Linux system.
2. Know how to read a script, such as a Bash script.
3. Know how to execute and schedule a script to run.
4. Describe the syntax of a script.

Objective 2 Use Scrip Use Scripts

1. Identify results of a script.
2. Understand errors returned by an executed script.
3. Run scripts written by others.

Objective 3 W d 3: riting Scrip riting Scripts

1. Use comments to explain functionality of a snippet of a script to promote readability.
2. Use and understand variables.
3. Use and understand loops.
4. Use and understand operators.
5. Use scripts in a script and shell parameter expansion.

Standard 4

Installation and security

Objective 1 Linux Ins d 1: Linux Installation

1. Install Linux on either a physical or virtual device.
2. Install drivers for a standard device.
3. Identify and mount different storage devices.
4. Understand the boot process of a linux system.
5. Install and configure a boot loader, such as GRUB / GRUB2.

Objective 2 Security d 2: Security

1. Understand that the goals of security are Confidentiality, Integrity, and Availability, commonly known as the CIA Triad.
2. Understand authentication methods and Identity and Access Management (IAM).
3. Locate and display log files.
4. Understand the role of a firewall and iptables.
5. Understand the concept of intrusion detection.
6. Select, sort, monitor, and kill processes.

Objective 3 Manage Software Soare

1. Find packages containing specific files or libraries which may or may not be installed.
2. Obtain package information like version, content, dependencies, package integrity and installation status (whether or not the package is installed) and included files.
3. Install, upgrade, and uninstall using various installation tools such as apt and npm.

Performance Skills

Students will have the content knowledge to use and manage a Linux system effectively.

Workplace Skills

The following workplace skills should be discussed, taught, and re-enforced in the course:

1. Communication
2. Teamwork
3. Critical and creative thinking
4. Problem Solving
5. Dependability
6. Legal requirements / expectations

Vocabulary and Key Terms

Standard 1 - Introduction to the Linux Operating System

Term	Description
Free and Open Source (FOSS)	Software license that grants the right to use, modify, and distribute the software, modified or not, to everyone free of charge.
Distro	Short for distribution, a Linux operating system packaged with specific components.
Kernel	The heart of an operating system, a software that provides essential services and manages system resources.
Command Line Interface (CLI)	A text-based interface between the user and the operating system that accepts input in the form of commands.

Graphical User Inter face (GUI)	An environment for passing commands to a computer by using a graphical, mouse-driven interface rather than by using text-based commands.
Shell	A program that takes commands from the keyboard and gives them to the operating system to perform.
Environment Variables	Variables that store information about the shell session and the working environment.
Root	The top-level directory of the system.
Stream	A communication channel between a program and the environment where the command was launched from.
Standard Input (stdin)	A text stream that acts as the source for command input.
Standard Output (std out)	A text stream that acts as the destination for command output.
Standard Error (stderr)	A text stream that is used as the destination for error messages.
Pipe	The | character, used to take the standard output of one process and passes it as standard input into another process.
Redirection	The process of accepting input data from and sending output data to a component that is not a default Input/Output device.

Strand 2 - User and File Management

Term	**Definition**
Group	An access control object that contains multiple users with similar security requirements.
Privilege Escalation	The practice of gaining a greater level of access than was intended for the user or application.
The su command	A command to switch the user to the root account and perform administrative tasks.
The sudo command	A command to allow users to execute specific commands with elevated privileges.

Permissions	Security settings that control access to objects including file system items and network resources.
Principle of Least Privilege	Basic principle of security stating that something should be allocated the minimum necessary rights, privileges, or information to perform its role.
Absolute Mode	A syntax for setting Linux permissions that uses numeric octal values to represent permissions values.
Symbolic Mode	Syntax for setting Linux permissions that uses characters to represent permissions values.
Ownership	The property by which a user is allowed to apply and modify the permissions of a file or directory.
The superuser account	The local administrative account on a Linux system, typically named root.
File System	Structure for file data indexing and storage created by a process of formatting a partition that allows an operating system to make use of a mass storage device, such as hard drives.
Linux FileSystem Hierarchy Standard (FHS)	A set of guidelines for the names of files and directories and their locations on Linux systems.
Path	A reference to a specific location on a file system.
Absolute Path	A reference to a specific location on a file system irrespective of the current working directory or combined paths.
Relative Path	A reference to a specific location on a file system that is relative to the current working directory.
Parent Directory	The directory that is one level above the current working directory.
Child Directory (Subdirectory)	The directory that is one level below the current working directory.

Strand 3 - Implementing Shell Scripts

Term	**Definition**

Text Editor	An application that enables you to view, create, or modify the contents of text files.
Comments	A method of annotating a part of a script so that it is easier for the others to understand.
Escape Character	A character that is used to remove the special meaning from another character so it can be interpreted literally.
Variable	A named temporary storage for a value.
Array	A collection of values, enables you to store multiple values in a single variable.
Function	A block of code that you can reuse to perform a specific task.
Exit Code	A value that a child process passes back to its parent process when the child process terminates.
Control Statement	A programming element that enables a program to execute instructions in a specified order.
Conditional Statement	A control statement that tells the program it must make a decision based on various factors.
Loop	A control statement that executes code repeatedly based on a certain condition
Shell Parameter Expansion	The process by which a shell identifies special tokens that it substitutes values for.
Command Substitution	A method of shell expansion in which the output of a command replaces the command itself.
Operators	Objects that evaluate expressions in a variety of ways.
Operands	Operands are the values being operated on.

Strand 4 - Installation and Security

Term	**Definition**

ISO Image	A disk image for operating system booting and installation.
Virtual Machine	A computer system created using software on one physical computer in order to emulate the functionality of another separate physical computer.
Firmware	A type of software that is embedded into hardware devices to control their functionality.
Boot Process	The process and sequence in which a computer system is started and the operating system is loaded.
BIOS (Basic Input/Output System)	Legacy 32-bit firmware type that initializes hardware and provides a system setup interface for configuring boot devices and other hardware settings.
UEFI (Unified Extensible Firmware Inter face)	A type of system firmware providing support for 64-bit CPU operation at boot, full GUI and mouse operation at boot, and better boot security.
Boot Loader	A small program stored in ROM that loads the kernel from a storage device and then starts the operating system.