DCOM 224
Advanced Linux Administration
4 Credits

Community College of Baltimore County
Common Course Outline

Description

DCOM 224 – Advanced Linux Administration: provides advanced knowledge of the Linux operating system, installation, configuration, and troubleshooting. Students install the Linux operating system and configure the hardware, software, and manage storage in a Linux environment. Students develop skills needed to automate and schedule jobs, apply security best practices, and configure firewalls and logging services. Students analyze, troubleshoot, and diagnose system properties and optimize system performance. This course is the culminating course for the CompTIA Linux+ certification.

Pre-requisites: DCOM 142

Overall Course Objectives

Upon completion of this course, students will be able to:

1. demonstrate knowledge of the Linux boot sequence from Basic Input/Output System (BIOS)/Unified Extensible Firmware Interface (UEFI);
2. install and configure a boot loader such as Grand Unified Bootloader (GRUB) or GRUB2;
3. create Linux partitions and manage Linux file systems such as third extended file systems (ext3), fourth extended file systems (ext4), network file systems (nfs), and X file systems (xfs);
4. summarize cloud virtualization concepts and technologies;
5. compare system manager and service manager such as SysVinit and Systemd;
6. demonstrate the ability to automate and schedule jobs;
7. apply the appropriate user and/or group permission and ownership;
8. configure appropriate access and authentication methods;
9. propose security best practices in a Linux environment;
10. configure Linux firewalls;
11. analyze system properties and remediate accordingly; and
12. implement logging services.

Major Topics

I.   Hardware and system configuration
II.   Manage storage in a Linux environment
III. System operation and maintenance
IV.   Manage services
V.   Automate and schedule jobs

The Common Course Outline (CCO) determines the essential nature of each course.
For more information, see your professor's syllabus.

VI.   Access and authentication methods
VII.   User and/or group permission and ownership
VIII.   Security best practices in a Linux environment
IX.   Logging services
X.   Linux firewalls
XI.   Optimize system performance
XII.   Troubleshoot user issues

Course Requirements

Grading will be determined by the individual faculty member, but shall include the following, at minimum:

- 6 laboratory assignments
- 2 exams

Other Course Information

This course is a program requirement for the following programs: Network Technology A.A.S. Degree with Cisco Concentration, Network Technology A.A.S. Degree with Information Technology Support Concentration, Network Technology A.A.S. Degree with General Networking Concentration, Cyber Security A.A.S. Degree, Digital Forensics A.A.S. Degree, Network Technology General Networking Certificate, Network Technology Information Technology Support Certificate, and Cyber Security Certificate. This course is a second course in a two-course sequence. This course is taught in a computerized environment.

Date Revised: 2/4/2020