

LFCS Domains and Competencies V 2.16

Checklist

November 2015

A Linux Foundation Training Publication

training.linuxfoundation.org

 **LINUX FOUNDATION**

TRAINING

Starting February 2, 2016, the LFCS Certification Exam will test on Domains and Competencies V2.16 as listed in this pdf. For more details, go [here](#).

LFCS Domains and Competencies V2.16

Essential Commands - 25%

- Identify the component of the Linux distribution that a file belongs to
- Install Linux Distribution to physical media
- Install Linux Distribution over a network
- Install Linux Distribution into a virtual disk image
- Log into graphical and text mode consoles
- Search for files
- Evaluate and compare the basic file system features and options
- Compare text files
- Compare binary files
- Identify different types of files
- Create and edit text files
- Use input-output redirection (e.g. >, >>, |, 2>)
- Analyze text using basic regular expressions
- Access remote systems securely using CLI
- Archive, compress, unpack, and uncompress files
- Create, delete, copy, and move files and directories
- Create hard and soft links
- List, set, and change standard file permissions
- Read, and use system documentation
- Manipulate file content programmatically
- Transfer files securely via the network
- Manage access to the root account
- Perform disk image management
- Use version control tools
- Run commands on many systems simultaneously

Operation of Running Systems - 20%

- Boot, reboot, and shut down a system safely
- Boot systems into different runlevels manually
- Install, configure and troubleshoot the bootloader
- Manage shared libraries
- Change the priority of a process
- Identify resource utilization by process
- Locate and analyze system log files
- Schedule tasks to run at a set date and time
- Verify completion of scheduled jobs
- Manipulate Linux system during the boot process
- Manipulate Linux system during the recovery process
- Support incident management for outages/trouble
- Identify and resolve system performance bottlenecks and platform instability
- Update hardware to provide required functionality and security
- Update operating systems to provide required functionality and security
- Update software to provide required functionality and security
- Update the kernel and ensure the system is bootable
- Verify the integrity and availability of hardware
- Verify the integrity and availability of resources
- Verify the integrity and availability of key processes
- Change kernel runtime parameters, persistent and non-persistent
- Use scripting to automate system maintenance tasks
- Manage the startup process and services
- List and identify SELinux/AppArmor file and process contexts
- Produce and deliver reports on system use (processor, memory, disk, and network), outages, and user requests
- Update packages from the network, a remote repository, or from the local file system
- Configure and modify SELinux/AppArmor policies
- Monitor security and conduct audits
- Script automation tools to make work faster and more accurate
- Develop and test disaster recovery plans
- Maintain systems via configuration management tools
- Train team members on new technology or changes to existing systems
- Develop system disaster recovery tests
- Install software from source

User and Group Management - 15%

- Create, delete, and modify local user accounts
- Create, delete, and modify local groups and group memberships
- Manage system-wide environment profiles
- Configure a client to use LDAP for user and group information
- Configure a system to authenticate using Kerberos
- Configure set-GID directories for collaboration
- Manage template user environment
- Configure user resource limits
- Manage user processes
- Configure PAM

Networking - 15%

- Configure networking and hostname resolution statically or dynamically
- Configure network services to start automatically at boot
- Implement packet filtering
- Configure firewall settings
- Configure a system to perform Network Address Translation
- Start, stop, and check the status of network services
- Monitor network performance
- Statically route IP traffic
- Dynamically route IP traffic
- Synchronize time using other network peers
- Configure network traffic tunneling

Service Configuration - 10%

- Configure a basic DNS server
- Maintain a DNS zone
- Configure a caching-only name server
- Configure a caching-only name server to forward DNS queries
- Configure an FTP server
- Configure anonymous-only download on FTP servers
- Provide/configure network shares via NFS
- Provide/configure network shares via CIFS
- Configure an smtp service
- Restrict access to an smtp server
- Configure a mail transfer agent (MTA) to accept inbound email from other systems
- Configure an MTA to forward (relay) email through a smart host
- Configure email aliases
- Configure SSH servers and clients
- Configure SSH-based remote access using public/private key pairs
- Configure a DHCP server
- Configure the HTTP proxy server
- Restrict access to the HTTP proxy server
- Configure an HTTP client to automatically use a proxy server
- Configure an IMAP and IMAPS service
- Configure host-based and user-based security for a service
- Query and modify the behavior of system services at various run levels
- Configure direct-attach and network printers
- Configure an HTTP server
- Configure HTTP server log files
- Configure SSL with HTTP server
- Set up name-based virtual web hosts
- Deploy a basic web application
- Restrict access to a web page
- Configure time synchronization server
- Synchronize time using other time synchronization peers
- Configure a system to log to a remote system
- Configure a PXE Boot server
- Configure an LDAP server and schema
- Configure a system to accept logging from a remote system
- Diagnose routine SELinux/AppArmor policy violations
- Configure SELinux/AppArmor to support a service
- Configure database server
- Configure SELinux/AppArmor to confine a service

Virtualization - 5%

- Configure a hypervisor to host virtual guests
- Install Linux systems as virtual guests
- Start, stop, modify the status of virtual machines
- Access a VM console
- Migrate a VM between two hosts
- Configure systems to launch virtual machines at boot
- Evaluate memory usage of virtual machines
- Create light-weight virtualized guests via namespaces
- Resize RAM or storage of VMs
- Cloning and replicating VMs using images or snapshots

Storage Management - 10%

- List, create, delete, and modify storage partitions
- Create, migrate, and remove Physical Volumes
- Assign Physical Volumes to Volume Groups
- Create, modify and delete Logical Volumes
- Extend existing Logical Volumes and filesystems
- Create and configure encrypted partitions
- Configure systems to mount file systems at or during boot
- Configure and manage swap space
- Add new partitions, and logical volumes
- Create, mount, and unmount standard Linux file systems
- Assemble partitions as RAID devices
- Identify storage devices using block device attributes
- Configure systems to mount standard, encrypted, and network file systems on demand
- Create and manage filesystem Access Control Lists (ACLs)
- Diagnose and correct file permission problems
- Setup user and group disk quotas for filesystems
- Restore default SELinux file contexts
- Manage Linux file system features and flags
- Configure remote block storage devices
- Design and test backup/recovery strategies
- Deploy, configure, and maintain high availability/clustering/replication

LINUX FOUNDATION

The Linux Foundation promotes, protects and standardizes Linux by providing unified resources and services needed for open source to successfully compete with closed platforms.

To learn more about our Linux Training program, please visit us at training.linuxfoundation.org.