

Version : **2024.01**

Dernière mise-à-jour : 2024/11/06 10:55

UX006 : Linux - Linux Administration Avancée

Présentation

Type d'Action (Article L. 6313-1) : Action d'acquisition, d'entretien ou de perfectionnement des connaissances.

Objectif : Maîtriser l'administration système avancé de RHEL/CentOS 8 Linux.

Public : Administrateurs Linux.

Pré requis : Avoir suivi la formation UX005 - Administration Système ou posséder les compétences équivalentes.

Méthode d'apprentissage : Alternance entre un scénario pédagogique clair et précis et des travaux pratiques basés sur des cas et exemples concrets.

Validation des acquis : Évaluation payante à l'aide d'un test auto-correctif.

Durée : 5 jours (35h)

Prérequis

- Un poste (MacOS, Linux, Windows™ ou Solaris™),
- Clavier AZERTY FR,
- Un casque ou des écouteurs,
- Un micro (optionnel),
- Chrome version 72+ ou Microsoft Edge version 79+ ou Firefox version 65+,
- Un accès à Internet rapide (4G minimum) SANS passer par un proxy,
- Accès débloqué aux ports 80 et 443 à : <https://www.ittraining.team> ainsi que ses sous-domaines.

Programme

- **LDF504 - Gestion des Disques, des Systèmes de Fichiers et du Swap**

- Contenu du Module
- Périphériques de stockage
- Partitions
- Partitionnement
 - LAB #1 - Partitionnement de votre Disque avec fdisk
- Logical Volume Manager (LVM)
 - LAB #2 - Volumes Logiques Linéaires
 - LAB #3 - Étendre un Volume Logique à Chaud
 - LAB #4 - Snapshots
 - LAB #5 - Suppression des Volumes
 - LAB #6 - Volumes Logiques en Miroir
 - LAB #7 - Modifier les Attributs LVM
 - LAB #8 - Volumes Logiques en Bandes
 - LAB #9 - Gérer les Métadonnées
- Systèmes de Fichiers Journalisés
 - Présentation
 - Ext3
 - Gestion d'Ext3
 - LAB #10 - Convertir un Système de Fichiers Ext3 en Ext2
 - LAB #11 - Convertir un Système de Fichiers Ext2 en Ext3
 - LAB #12 - Placer le Journal sur un autre Partition
 - LAB #13 - Modifier la Fréquence de Vérification du Système de Fichiers Ext3
 - Ext4
 - LAB #14 - Créer un Système de Fichiers Ext4
 - LAB #15 - Ajouter une Étiquette au Système de Fichiers Ext4
 - LAB #16 - Convertir un Système de Fichiers Ext3 en Ext4
 - XFS
 - LAB #17 - Créer un Système de Fichiers XFS
 - LAB #18 - Ajouter une Étiquette au Système de Fichiers XFS
 - ReiserFS

- LAB #19 - Créer un Système de Fichiers ReiserFS
- LAB #20 - Ajouter une Étiquette au Système de Fichiers ReiserFS
- JFS
 - LAB #21 - Créer un Système de Fichiers JFS
 - LAB #22 - Ajouter une Étiquette au Système de Fichiers JFS
- Btrfs
 - LAB #23 - Créer un Système de Fichiers Btrfs
 - LAB #24 - Convertir un Système de Fichiers Ext4 en Btrfs
 - LAB #25 - Créer un Snapshot
 - LAB #26 - Ajouter une Étiquette au Système de Fichiers Btrfs
- Comparaison des Commandes par Système de Fichiers
- Systèmes de Fichiers Chiffrés
 - LAB #27 - Créer un Système de Fichiers Chiffré avec encryptfs
 - LAB #28 - Créer un Système de Fichiers Chiffré avec LUKS
- Raid Logiciel
 - LAB #29 - Mise en Place du RAID 5 Logiciel
 - 29.1 - Préparer le disque
 - 29.2 - Créer une Unité RAID
 - 29.3 - Remplacer une Unité Défaillante
- Le Swap
 - Taille du swap
 - Partitions de swap
 - La Commande swapon
 - La Commande swapoff
 - LAB #30 - Créer un Fichier de Swap

• LDF508 - Gestion de la Journalisation

- Contenu du Module
- Présentation
- La Commande dmesg
- LAB #1 - Surveillance Sécuritaire
 - 1.1 - La Commande last
 - 1.2 - La Commande lastlog
 - 1.3 - La Commande lastb

- 1.4 - Le fichier /var/log/auth.log
- 1.5 - Gestion des évènements audit
 - Le fichier /var/log/audit/audit.log
 - auditd
 - auditctl
 - audispd
 - La consultation des événements audit
 - La Commande aureport
 - La Commande ausearch
- Le fichier /var/log/messages
- Applications
- LAB #2 - rsyslog
 - 2.1 - Priorités
 - 2.2 - Sous-systèmes applicatifs
 - 2.3 - /etc/rsyslog.conf
 - Modules
 - Directives Globales
 - Règles
 - Sous-système applicatif.Priorité
 - Sous-système applicatif!Priorité
 - Sous-système applicatif=Priorité
 - L'utilisation du caractère spécial *
 - n Sous-systèmes avec la même priorité
 - n Sélecteurs avec la même Action
- LAB #3 - La Commande logger
- LAB #4 - La Commande logrotate
- LAB #5 - La Journalisation avec journald
 - 5.1 - Consultation des Journaux
 - 5.2 - Consultation des Journaux d'une Application Spécifique
 - 5.3 - Consultation des Journaux depuis le Dernier Démarrage
 - 5.4 - Consultation des Journaux d'une Priorité Spécifique
 - 5.5 - Consultation des Journaux d'une Plage de Dates ou d'Heures
 - 5.6 - Consultation des Journaux en Live

• LDF510 - Gestion du Démarrage et de l'Arrêt du Système

- Contenu du Module
- Présentation
- BIOS, EFI et OpenFirmware
 - Systèmes à base du BIOS
 - Charger de Démarrage
 - Systèmes à base de l'EFI
 - Autres Systèmes
- Gestionnaire d'amorçage
 - LILO
 - La Commande LILO
 - Codes Erreur de LILO
 - GRUB 2
 - Le fichier /boot/grub2/device.map
 - Le fichier /etc/default/grub
 - Les fichiers du répertoire /etc/grub.d
 - Modifier la Configuration de GRUB 2 en Ligne de Commande
 - Gestionnaires de Démarrages Alternatifs
 - Systemd-boot
 - U-boot
 - Le Projet Syslinux
 - SYSLINUX
 - EXTLINUX
 - ISOLINUX
 - PXELINUX
 - Isodhpx
- Initramfs
 - LAB #1 - Travailler avec Initramfs
 - 1.1 - Examiner l'image existante
 - 1.2 - La Commande mkinitramfs
- Processus de Démarrage du Noyau Linux
- systemd
 - LAB #2 - La Commande systemctl
 - LAB #3 - Fichiers de Configuration

- 3.1 - Fichiers de Configuration par Défaut
- 3.2 - Surchargement des Fichiers par Défaut
- 3.3 - Les Fichiers d'Unités
- LAB #4 - La Commande systemd-analyze
- LAB #5 - Les Cibles
 - 5.1 - Contrôler les dépendances d'une Cible
 - 5.2 - La Cible par Défaut
- LAB #6 - Gestion des Services
 - 6.1 - Gestion des Instances Uniques
 - 6.2 - Gestion d'Instances Multiples
 - 6.3 - Interdire la Modification du Statut d'un Service
- Arrêt Système du Système
 - La Commande shutdown
 - La Commande reboot
 - La Commande halt
 - La Commande poweroff

• LDF511 - Gestion des Paramètres et les Ressources du Matériel

- Contenu du Module
- Présentation des Fichiers Spéciaux
- LAB #1 - Commandes
 - 1.1 - La Commande lspci
 - 1.2 - La Commande lsusb
 - 1.3 - La Commande lsblk
 - 1.4 - La Commande lsscsi
 - 1.5 - La Commande lscpu
 - 1.6 - La Commande lshw
 - 1.7 - La Commande dmidecode
 - 1.8 - La Commande smartctl
 - 1.9 - Les Commandes accton et dump-acct
 - 1.10 - La Commande lastcomm
 - 1.11 - La Commande sa
 - 1.12 - La Commande ac
- LAB #2 - La Commande sysctl

- 2.1 - Répertoire /proc
 - Fichiers
 - Processeur
 - Interruptions système
 - Canaux DMA
 - Plages d'entrée/sortie
 - Périphériques
 - Modules
 - Statistiques de l'utilisation des disques
 - Partitions
 - Espaces de pagination
 - Statistiques d'utilisation du processeur
 - Statistiques d'utilisation de la mémoire
 - Version du noyau
 - Répertoires
 - ide/scsi
 - acpi
 - bus
 - net
 - sys
- 2.2 - Utilisation de la Commande sysctl
- LAB #3 - Interprétation des informations dans /proc
 - 3.1 - free
 - 3.2 - uptime ou w
 - 3.3 - iostat
 - 3.4 - hdparm
 - 3.5 - vmstat
 - 3.6 - mpstat
 - 3.7 - sar
- Modules usb
- udev
 - La Commande udevadm
- Système de fichiers /sys
- Limiter les Ressources

- LAB #4 - ulimit
- LAB #5 - cgroups v2
 - 5.1 - Préparation
 - 5.2 - Présentation
 - 5.3 - Limitation de la CPU
 - 5.4 - La Commande systemctl set-property

- **LCF513 - Gestion du Réseau**

- Contenu du Module
- Comprendre les Réseaux
 - Présentation des Réseaux
 - Classification des Réseaux
 - Classification par Mode de Transmission
 - Classification par Topologie
 - Classification par Étendue
 - Les Types de LAN
 - Le Modèle Client/Serveur
 - Modèles de Communication
 - Le modèle OSI
 - Spécification NDIS et le Modèle ODI
 - Le modèle TCP/IP
 - Les Raccordements
 - Les Modes de Transmission
 - Les Câbles
 - Les Réseaux sans Fils
 - Le Courant Porteur en Ligne
 - Technologies
 - Ethernet
 - Token-Ring
 - Périphériques Réseaux Spéciaux
 - Les Concentrateurs
 - Les Répéteurs
 - Les Ponts
 - Les Commutateurs

- Les Routeurs
 - Les Passerelles
- Comprendre le Chiffrement
 - Introduction à la cryptologie
 - Définitions
 - La Cryptographie
 - Le Chiffrement par Substitution
 - Algorithmes à clé secrète
 - Le Chiffrement Symétrique
 - Algorithmes à clef publique
 - Le Chiffrement Asymétrique
 - La Clef de Session
 - Fonctions de Hachage
 - Signature Numérique
 - Utilisation de GnuPG
 - Présentation
 - Installation
 - Configuration
 - Signer un message
 - Chiffrer un message
 - PKI
 - Certificats X509
- Comprendre IPv4
 - En-tête TCP
 - En-tête UDP
 - Fragmentation et Ré-encapsulation
 - Adressage
 - Masques de sous-réseaux
 - VLSM
 - Ports et sockets
 - /etc/services
 - Résolution d'adresses Ethernet
- Comprendre IPv6
 - Présentation

- Adresses IPv6
- Masque de Sous-réseau
- Adresses IPv6 Réservées
- L'Adresse Link-local
- DHCPv6
- Configuration
 - La Commande nmcli
- LAB #1 - Configuration du Réseau
 - 1.1 - Connexions et Profils
 - 1.2 - Résolution des Noms
 - 1.3 - Ajouter une Deuxième Adresse IP à un Profil
 - 1.4 - La Commande hostname
 - 1.5 - La Commande ip
 - 1.6 - Activer/Désactiver une Interface Manuellement
 - 1.7 - Routage Statique
 - La commande ip
 - Activer/désactiver le routage sur le serveur
- LAB #2 - Diagnostic du Réseau
 - 2.1 - ping
 - 2.2 - netstat -i
 - 2.3 - traceroute
- LAB #3 - Connexions à Distance
 - 3.1 - Telnet
 - 3.2 - wget
 - 3.3 - ftp
 - 3.4 - SSH
 - Présentation
 - SSH-1
 - SSH-2
 - Authentification par mot de passe
 - Authentification par clef asymétrique
 - Configuration du Serveur
 - Configuration du Client
 - Tunnels SSH

- 3.5 - SCP
 - Présentation
 - Utilisation
- 3.6 - Mise en Place des Clefs Asymétriques
- **LCF606 - Gestion de la Sécurité**
 - Contenu du Module
 - Le Pare-feu Netfilter/iptables
 - LAB #1 - La Configuration par firewalld
 - La Configuration de Base de firewalld
 - La Commande firewall-cmd
 - La Configuration Avancée de firewalld
 - Le mode Panic de firewalld
 - System Hardening
 - Les compilateurs
 - Les paquets
 - Les démons et services
 - Les fichiers .rhosts
 - Les fichiers et les repertoires sans propriétaire
 - Limiter le delai d'inactivite d'une session shell
 - Renforcer la securite d'init
 - Les Distributions SysVinit
 - Les Distributions Upstart
 - Renforcer la sécurité du Noyau
 - La commande sysctl
 - Mise en place de SELinux pour sécuriser le serveur
 - Introduction
 - Définitions
 - Security Context
 - Domains et Types
 - Roles
 - Politiques de Sécurité
 - Langage de Politiques
 - allow

- type
 - type_transition
 - Décisions de SELinux
 - Décisions d'Accès
 - Décisions de Transition
 - Commandes SELinux
 - Les Etats de SELinux
 - Booléens
- LAB #2 - Travailler avec SELinux
 - Copier et Déplacer des Fichiers
 - Vérifier les SC des Processus
 - Visualiser la SC d'un Utilisateur
 - Vérifier la SC d'un fichier
 - Troubleshooting SELinux
 - La commande chcon
 - La commande restorecon
 - Le fichier /.autorelabel
 - La commande semanage
 - La commande audit2allow
- Mots de Passe
 - LAB #3 - John the Ripper
 - LAB #4 - Mise en place du Système de Prévention d'Intrusion Fail2Ban
 - Installation
 - Configuration
 - Le répertoire /etc/fail2ban
 - Le fichier fail2ban.conf
 - Le répertoire /etc/fail2ban/filter.d/
 - Le répertoire /etc/fail2ban/action.d/
 - Commandes
 - Activer et Démarrer le Serveur
 - Utiliser la Commande Fail2Ban-server
 - Ajouter un Prison
- Balayage des Ports
 - LAB #5 - Utilisation de nmap et de netcat

- nmap
 - Installation
 - Utilisation
 - Fichiers de Configuration
 - Scripts
- netcat
 - Utilisation
- LAB #6 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry
 - Installation
 - Configuration
 - Utilisation
- Système de Fichiers
 - LAB #7 - Mise en place du File Integrity Checker Afick
 - Présentation
 - Installation
 - Configuration
 - La Section Directives
 - La Section Alias
 - La Section File
 - Utilisation
 - Automatiser Afick
 - LAB #8 - Mise en place de rkhunter
 - Installation
 - Les options de la commande
 - Utilisation
 - Configuration
- **LCF607 - Gestion du Noyau et des Quotas**
 - Contenu du Module
 - Rôle du noyau
 - LAB #1 - Modules
 - LAB #2 - Compilation et installation du noyau et des modules
 - 2.1 - Déplacer /home
 - 2.2 - Préparer l'Environnement

- 2.3 - Préparer l'Arborescence Source du Noyau
 - Le Fichier .config
 - Le Fichier Makefile
- 2.4 - Paramétrage du noyau
- 2.5 - Compiler le Noyau
- 2.6 - Installer le Nouveau Noyau
- LAB #3 - Gestion des Quotas
 - 3.1 - La Commande quotacheck
 - 3.2 - La Commande edquota
 - 3.3 - La Commande quotaon
 - 3.4 - La Commande repquota
 - 3.5 - La Commande quota
 - 3.6 - La Commande warnquota

- **LDF607 - Gestion du Noyau et des Quotas**

- Contenu du Module
- Rôle du noyau
- LAB #1 - Compilation et installation du noyau
 - 1.1 - Déplacer /home
 - 1.2 - Télécharger le Code Source du Noyau
 - 1.3 - Configurer le Noyau
 - 1.4 - Compiler le Noyau
 - 1.5 - Installer le Nouveau Noyau
 - 1.6 - Désinstaller un Noyau
- LAB #2 - Mise à Jour du Noyau avec le Gestionnaire des Paquets
- LAB #3 - Gestion des Quotas
 - 3.1 - La Commande quotacheck
 - 3.2 - La Commande edquota
 - 3.3 - La Commande quotaon
 - 3.4 - La Commande repquota
 - 3.5 - La Commande quota
 - 3.6 - La Commande warnquota

Copyright © 2024 Hugh Norris - Document non-contractuel. Le programme peut être modifié sans préavis.

From:
<https://www.ittraining.team/> - **www.ittraining.team**

Permanent link:
<https://www.ittraining.team/doku.php?id=elearning:workgroups:gkn:ux006>

Last update: **2024/11/06 10:55**

