

Version : **2020.01**

Dernière mise-à-jour : 2020/12/07 14:45

Linux avancé - Validation de la Formation

Contenu du Module

- **LCF308 - Validation de la Formation**
 - Contenu du Module
 - Pour Aller Plus Loin
 - Support de Cours
 - L'Infrastructure Hors Formation
 - Matériel
 - Logiciels
 - Machine Virtuelle
 - Rappel du Programme de la Formation
 - Jour #1
 - Jour #2
 - Jour #3
 - Jour #4
 - Remettre en Etat l'Infrastructure
 - Évaluation de la Formation
 - Remerciements

Pour Aller Plus Loin

Support de Cours

L'accès au supports de cours ainsi que les LABS et les validations des acquis se fait grâce à un abonnement annuel par stagiaire à une plateforme de cours sur Internet.

L'utilisation de cette plateforme permet :

- de mesurer le niveau du stagiaire avant la formation et celui atteint en fin de formation grâce aux tests de validations des acquis,
- de suivre du travail de chaque participant en termes de temps passé dans chaque module grâce à un reporting détaillé.

L'abonnement permet aux stagiaires :

- de télécharger des supports de cours et des LABS au format PDF le dernier jour de la formation,
- de refaire les LABS en mode autonome en cas de missions décalées en relation avec le contenu de la formation initiale,
- de rester en contact avec le formateur en cas de problèmes en production liés au contenu du cours,
- de consulter les mises à jour du contenu des supports de cours pendant la période de l'abonnement,
- d'échanger avec les autres participants de la session ainsi qu'avec les anciens stagiaires.

L'Infrastructure Hors Formation

Matériel

- Un poste 64 bits (MacOS, Linux, Windows™ ou Solaris™),
- Dans le cas de Windows™, **seulement** la version 7 ou 10 avec Hyper-V **désinstallé**,
- Le mot de passe du compte administrateur du système,
- Clavier AZERTY FR ou QWERTY US,
- 8 Go de RAM minimum,
- Processeur 4 cœurs minimum,
- 8 Go d'espace disque disponible.

Logiciels

- Oracle VirtualBox v 6.0 ou plus (MacOS, Linux, Windows™ ou Solaris™),
- Si Windows™ - Putty et WinSCP,

- Navigateur Web Chrome ou Firefox.

Machine Virtuelle

A télécharger : [CentOs_7](#).

Rappel du Programme de la Formation

Jour #1 - 7 heures

- **Linux avancé** - 1 heure.
 - Pré-requis
 - Matériel
 - Logiciels
 - Internet
 - Utilisation de l'Infrastructure
 - Connexion au Serveur Cloud
 - Linux, MacOS et Windows 10 muni du client ssh
 - Windows 7 et Windows 10 sans client ssh
 - Démarrage de la Machine Virtuelle
 - Connexion à la Machine Virtuelle
 - Programme de la Formation
 - Évaluation des Compétences
- **LCF203 - Gestion des Droits** - 1 heure.
 - Les Droits Unix Étendus
 - SUID/SGID bit
 - Inheritance Flag
 - Sticky bit
 - Les Droits Unix Avancés
 - Les ACL

- Les Attributs Étendus

- **LCF204 - Gestion des Disques, des Systèmes de Fichiers et du Swap** - 5 heures.

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

- LAB #19 - Ajouter une Étiquette au Système de Fichiers XFS
- Autres Systèmes de Fichiers
 - ReiserFS
 - JFS
 - Btrfs
- Comparaison des Commandes par Système de Fichiers
- LAB #20 - Créer un Système de Fichiers ISO
 - La Commande mkisofs
- Systèmes de Fichiers Chiffrés
 - LAB #21 - Créer un Système de Fichiers Chiffré avec encryptfs sous RHEL/CentOS 6
 - LAB #22 - Créer un Système de Fichiers Chiffré avec LUKS sous RHEL/CentOS 7
 - Présentation
 - Mise en Place
 - Ajouter une deuxième Passphrase
 - Supprimer une Passphrase
- Le Swap
 - Taille du swap
 - Partitions de swap
 - La Commande swapon
 - La Commande swapoff
 - LAB #23 - Créer un Fichier de Swap

Jour #2 - 7 heures

- **LCF301 - Gestion des Paramètres et les Ressources du Matériel** - 3 heures.
 - Fichiers Spéciaux
 - Commandes
 - La Commande lspci
 - La Commande lsusb
 - La Commande dmidecode
 - Répertoire /proc
 - Répertoires
 - ide/scsi

- acpi
- bus
- net
- sys
 - La commande sysctl
 - Options de la commande
- 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
- Interprétation des informations dans /proc
 - Commandes
 - free
 - uptime ou w
 - iostat
 - vmstat
 - mpstat
 - sar
 - Utilisation des commandes en production
 - Identifier un système limité par le processeur
 - Identifier un système ayant un problème de mémoire
 - Identifier un système ayant un problème d'E/S
 - Modules usb
 - udev
 - La commande udevadm

- Les options de la commande
 - Système de fichiers /sys
 - Limiter les Ressources
 - ulimit
 - Groupes de Contrôle
 - LAB #1 - Travailler avec les cgroups sous RHEL/CentOS 7

- **LCF303 - Gestion du Noyau et des Quotas** - 4 heures.

- Rôle du noyau
- Compilation et installation du noyau et des modules
 - Déplacer /home
 - Créer un Nouveau Noyau
 - Préparer l'Arborescence Source du Noyau
 - Paramétrage du noyau
 - Compiler le Noyau
 - Installer le Nouveau Noyau
- Gestion des Quotas
 - La Commande quotacheck
 - La Commande edquota
 - La Commande quotaon
 - La Commande repquota
 - La Commande quota
 - La Commande warnquota

Jour #3 - 7 heures

- **LCF403 - Authentification** - 3 heures.

- Le Problématique
 - LAB #1 - Installer John the Ripper
- Surveillance Sécuritaire
 - La commande last
 - La commande lastlog
 - La Commande lastb
 - /var/log/secure

- Les Contre-Mesures
 - LAB #2 - Renforcer la sécurité des comptes
- LAB #3 - PAM sous RHEL/CentOS 7
 - Bloquer un Compte après N Echecs de Connexion
 - Configuration
- 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

- **LRF404 - Balayage des Ports** - 4 heures.

- Le Problématique
 - LAB #1 - Utilisation de nmap et de netcat
 - nmap
 - Installation
 - Utilisation
 - Fichiers de Configuration
 - Scripts
 - netcat
 - Utilisation
- Les Contre-Mesures
 - LAB #2 - Mise en place du Système de Détection d'Intrusion Snort
 - Installation
 - Configuration de Snort
 - Editer le fichier /etc/snort/snort.conf
 - Utilisation de snort en mode "packet sniffer"
 - Utilisation de snort en mode "packet logger"

- Journalisation
- LAB #3 - Mise en place du Système de Détection et de Prévention d'Intrusion Portsentry
 - Installation
 - Configuration
 - Utilisation

Jour #4 - 7 heures

- **LCF407 - System Hardening** - 3 heures.

- System Hardening Manuel
 - Les compilateurs
 - Les paquets
 - Les démons et services
 - Les fichiers .rhosts
 - Les fichiers et les répertoires sans propriétaire
 - Interdire les connexions de root via le réseau
 - Limiter le délai d'inactivité d'une session shell
 - Renforcer la sécurité d'init
 - Les Distributions SysVInit
 - Les Distributions Upstart
 - Renforcer la sécurité du Noyau
 - La commande sysctl
- LAB #1 - System Hardening à l'aide de l'outil Bastille
 - Présentation
 - Installation
 - Utilisation
- LAB #2 - 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 #3 - 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
- **LCF408 - Sécurité Applicative** - 3 heures.
 - Le Problématique
 - Préparation
 - Les Outils
 - LAB #1 - Netwox
 - Installation
 - Utilisation
 - Avertissement important
 - LAB #2 - OpenVAS
 - Présentation
 - Préparation
 - Installation

- Configuration
- Utilisation
- Analyse des Résultats
- Les Contres-Mesures
 - LAB #3 - La commande chroot
 - LAB #4 - Sécuriser Apache
 - Installation
 - Testez le serveur apache
 - Avec un navigateur
 - Avec Telnet
 - Préparation
 - Gestion de serveurs virtuels
 - Hôte virtuel par nom
 - Hôte virtuel par adresse IP
 - mod_auth_basic
 - Configuration de la sécurité avec .htaccess
 - Mise en place d'un fichier de mots de passe
 - mod_auth_mysql
 - Installation
 - Configuration de MariaDB
 - Configuration d'Apache
 - mod_authnz_ldap
 - mod_ssl
 - Présentation de SSL
 - Fonctionnement de SSL
 - Installation de ssl
 - Configuration de SSL
 - Mise en place des paramètres de sécurité SSL
 - Tester Votre Configuration

- **Linux avancé - Validation de la Formation** 1 heure.

- Pour Aller Plus Loin
 - Support de Cours
 - L'Infrastructure Hors Formation

- Matériel
- Logiciels
- Machine Virtuelle
- Rappel du Programme de la Formation
 - Jour #1
 - Jour #2
 - Jour #3
 - Jour #4
- Remettre en Etat l'Infrastructure
- Évaluation de la Formation
- Remerciements

Remettre en Etat l'Infrastructure

Utilisez la commande suivante pour arrêter la machine virtuelle :

```
desktop@serverXX:~$ VBoxManage controlvm CentOS_7 poweroff
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

Ensuite restaurez l'état d'origine de la machine virtuelle :

```
desktop@serverXX:~$ VBoxManage snapshot CentOS_7 restore snapshot1
Restoring snapshot 'snapshot1' (22df4e22-876a-4e94-88a8-8422a3a6b158)
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
```

Évaluation de la Formation

Afin de valider votre formation, veuillez compléter l'Évaluation de la Formation et passer la Validation des Acquis.

Remerciements

Nous vous remercions de votre confiance et nous vous souhaitons une excellente continuation.

<html> <DIV ALIGN="CENTER"> Copyright © 2020 Hugh Norris

 Document non-contractuel. Le programme peut être modifié sans préavis.
</div> </html>

From:

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

Permanent link:

https://ittraining.team/doku.php?id=sparks:linux_avance_eval

Last update: **2020/12/07 14:45**

