edify digital

# NOS FORMATIONS EN ADMINISTRATION RESEAU & SYSTEME

*L'expertise à portée de Clic*

# Les cursus métiers

Comme son nom l'indique, un cursus-métier est un ensemble de formations qui, une fois accompli, donne une qualification-métier à l'apprenant.

En suivant un cursus de formations, vous pourrez apprendre un nouveau métier ou développer de nouvelles compétences professionnelles dans des délais relativement réduits.

Les cursus EdLearn ont été créés sur la base de nos partenariats avec les plus grands éditeurs mondiaux de solutions tels que Cisco ou encore Microsoft, etc. De quoi voir son avenir professionnel avec confiance et enthousiasme !

Comme une bonne nouvelle n'arrive jamais seule, en vous inscrivant à un cursus métier d'Edlearn, bénéficiez d'une réduction pouvant aller jusqu' à -25% sur le coût total de chaque formations du cursus achetées individuellement

## ADMINISTRATEUR RESEAU CISCO

| CODE | FORMATIONS/CERTIFICATIONS | DURÉE |
|---|---|---|
| HD01 | ITE (COMPTIA A+) | 40 h |
| NT01 | CCNA 1 | 24h |
| NT02 | CCNA2 | 24h |
| MS02 | WINDOWS SERVER | 24h |
| LP02 | LINUX1 (LPIC-1 101) | 24h |
| NT03 | CCNA3 | 24h |
| MS01 | AZURE AZ 900 | 24h |
| NT05 | PANORAMA DES SOLUTIONS CISCO | 30h |

## ADMINISTRATEUR RESEAU ARUBA

| CODE | FORMATIONS/CERTIFICATIONS | DURÉE |
|---|---|---|
| HD01 | ITE (COMPTIA A+) | 40 h |
| NT01 | CCNA 1 | 24h |
| MS02 | WINDOWS SERVER | 24h |
| LP02 | LINUX(LPIC-1 101) | 24h |
| MS01 | AZURE AZ 900 | 24h |
| AR01 | ARUBA CERTIFIED CAMPUS ASSOCIATE (ACA) | 40h |
| AR02 | ARUBA CERTIFIED PREFESSIONAL (ACP) | 40h |
| GOV01 | ISO 27001 | |

## ADMINISTRATEUR SYSTEME

| CODE | FORMATIONS/CERTIFICATIONS | DURÉE |
|---|---|---|
| LP01 | LPIC1 | 40h |
| MS02 | WINDOWS SERVER AVANCE | 40h |
| MS03 | POWERHELL | 36h |
| VM04FR | VMware Certified Associate (VCA) | 24h |
| MS01 | AZURE 900 | 24h |
| MS04 | MICROSOFT 365 FUNDAMENTALS MS 900 | 24h |
| CL01 | AWS CLOUD PRACTIONNER | 24h |
| CL02 | AWS SYS OS | |

# Les cursus métiers

## ADMINISTRATEUR SYSTEME NIVEAU 2

| CODE | FORMATIONS/CERTIFICATIONS | DURÉE |
|---|---|---|
| MS05 | AZURE 104 | 40h |
| VM02 | VMware Certified PROFESSIONNAL (VCP) | 40h |
| LP02 | LPIC2 | 36h |
| MS06 | AZURE 800 | 24h |
| MS07 | MICROSOFT 365 SECURITY ADMINISTRATOR MS 500 | 24h |
| LP03 | RHCSA | 24h |
| CL01 | AWS SYS OS | 24h |

## ADMINISTRATEUR RESEAU HYBRIDE

| CODE | FORMATIONS/CERTIFICATIONS | DURÉE |
|---|---|---|
| NT05 | CCNP ENCOR | 40h |
| NT06 | CCNP ENARSI | 40h |
| SEC03 | NETWORK SECURITY | 36h |
| MS05 | AZURE 104 | 24h |
| CL02 | AWS CLOUD PRACTIONNER | 24h |
| CL03 | DOCKER DCA | 24h |
| CL04 | KUBERNETE KCNA | 24h |
| CL05 | KUBERNETE CKA | |

## ADMINISTRATEUR CLOUD

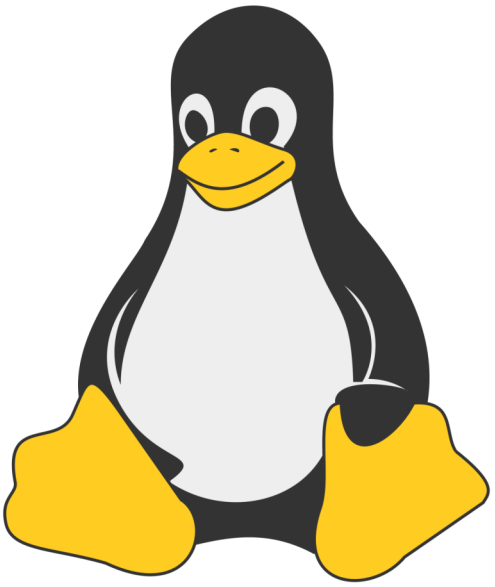
| CODE | FORMATIONS/CERTIFICATIONS | DURÉE |
|---|---|---|
| HD01 | ITE (COMPTIA A+) | 40 h |
| HD02 | NETWORK+ | 24h |
| MS02 | WINDOWS SERVER | 24h |
| LP01 | LINUX1 (LPIC-1 101) | 24h |
| CL03 | DOCKER DCA | 24h |
| CL04 | KUBERNETE KCNA | 24h |
| MS05 | AZURE 104 | 24h |
| CL01 | AWS CLOUD PRACTIONNER | 30h |

## L'importance d'un cursus métier

Les nouvelles technologies, l'évolution des méthodes de travail et de management font évoluer nos métiers. Suivre les cursus métiers d'Edify, c'est se maintenir formé et informé pour assurer sa performance et sa réussite. Nos formations spécifiques à chaque métiers vous permettent de valider et de renforcer vos compétences afin d'être plus efficace. De courtes durées, nos cursus professionnels sont conçus pour répondre de façon concrète à vos besoins professionnels immédiats. Ils sont enrichis et mis à jour de manière constante.

edify digital

# Nos formations LINUX



24H CODE : LPO2

# Programme LINUX1 (LPIC-1 101)

## Objectifs

- Installer et configurer un système Linux.
- Utiliser efficacement la ligne de commande Linux.
- Gérer les fichiers, les répertoires et les permissions.
- Comprendre l'architecture d'un système Linux.
- Gérer les paquets logiciels.
- Dépanner les problèmes courants d'un système Linux.
- Se préparer à l'examen LPIC-1 101.

## Débouchées

- Administrateur système Linux débutant.
- Technicien support informatique.
- Opérateur système
- Développeur web
- Ingénieur DevOps

## Prérequis

Connaissances de base en informatique
Familiarité avec l'utilisation d'un ordinateur
La pratique de l'anglais technique est recommandée

Introduction

Présentation de Linux: Historique, philosophie, avantages, domaines d'utilisation.
Les distributions Linux: Principales distributions (Debian, Ubuntu, Red Hat, CentOS, Fedora), différences et choix selon les besoins.
Interface en ligne de commande: Importance, fonctionnement de base, notions de shell (bash).

Module 1 : Installation et Configuration de Base

Installation de Linux: Choix d'une distribution, préparation du support d'installation, processus d'installation, personnalisation du système.
Configuration du système: Gestion des utilisateurs et groupes, configuration du réseau, configuration du système de fichiers, services de base (SSH, NTP).
Gestion des paquets: Utilisation des gestionnaires de paquets (apt, yum), installation, mise à jour, suppression de logiciels.

Module 2 : Administration Système

Le système de fichiers: Structure, permissions, opérations sur les fichiers et répertoires.
Gestion des disques et partitions: Création, formatage, montage, gestion des quotas.
Gestion des processus: Affichage, contrôle, gestion des priorités, mise en arrière-plan.
Gestion des services: Démarrage, arrêt, redémarrage, configuration des services système.

Module 3 : Réseau

Notions de réseau: Protocoles TCP/IP, adresses IP, masque de sous-réseau, routage.
Configuration réseau: Interfaces réseau, configuration de la carte réseau, routage statique et dynamique.
Serveur SSH: Installation, configuration, utilisation sécurisée.
Serveur web (Apache): Installation, configuration de base, création de sites web simples.

Module 4 : Sécurité

Sécurité de base: Mots de passe, droits d'accès, pare-feu.
Sécurisation du système: Configuration du pare-feu, durcissement du système, gestion des vulnérabilités.
Sauvegardes: Stratégies de sauvegarde, outils de sauvegarde.

Module 5 : Scripting

Introduction au scripting: Pourquoi utiliser des scripts, les différents langages de script (bash, Python).
Scripting Bash: Variables, conditions, boucles, fonctions.
Automatisation de tâches: Création de scripts pour automatiser des tâches administratives.

Module 6 : Outils et Utilitaires

Éditeurs de texte: Vi, nano, Emacs.
Outils de recherche: grep, find, locate.
Compression et archivage: tar, gzip, bzip2.
Autres outils: Cron, sed, awk.
Méthodologie Pédagogique
Cours théoriques: Présentations, échanges, questions-réponses.
**Travaux pratiques: Exercices en laboratoire, projets.**

40H CODE : LPO2

# Programme LINUX2 (LPIC-2 201)

## Objectifs

- Configurer et compiler un noyau Linux.
- Gérer les périphériques et le stockage de manière avancée.
- Maîtriser le processus de démarrage du système.
- Configurer les services réseau essentiels.
- Dépanner les problèmes complexes d'un système Linux.
- Se préparer à l'examen LPIC-2 201.

## Débouchées

- Administrateur système Linux
- Ingénieur système
- Architecte infrastructure
- Spécialiste en sécurité informatique.
- Ingénieur DevOps

## Prérequis

- La certification LPIC-1

### Module 1 : Fondamentaux et Planification des Ressources

Introduction à Linux : Historique, philosophie, distributions populaires
Structure du système Linux : Noyau, système de fichiers, processus
Commandes de base : Navigation, gestion des fichiers, manipulation des textes
Planification des ressources :
Mesure de l'utilisation du CPU, de la mémoire, du disque et du réseau
Outils d'analyse de performance
Dimensionnement des ressources pour différentes charges de travail

### Module 2 : Le Noyau Linux

Fonctionnement du noyau : Tâches principales, gestion des processus, gestion de la mémoire
Compilation du noyau : Configuration, compilation, installation
Modules du noyau : Chargement, déchargement, création de modules personnalisés

### Module 3 : Démarrage du Système

Processus de démarrage : BIOS/UEFI, chargeur de boot, init
Fichiers de configuration : /etc/fstab, /etc/inittab, fichiers de service
Personnalisation du démarrage : Initialisation de services, scripts de démarrage

### Module 4 : Système de Fichiers et Périphériques

Systèmes de fichiers : Ext4, XFS, Btrfs, comparaison et choix
Gestion des partitions : fdisk, parted, LVM
Gestion des périphériques : Disques durs, partitions, périphériques spéciaux
Systèmes de fichiers réseau : NFS, SMB

### Module 5 : Administration Avancée des Périphériques de Stockage

RAID : Concepts, niveaux de RAID, configuration et gestion
Outils de sauvegarde : rsync, tar, outils de sauvegarde incrémentale
Restauration de données : Procédures, tests de restauration

### Module 6 : Configuration Réseau

Interface réseau : Configuration, routage statique, DHCP
Services réseau : SSH, FTP, TFTP, DNS
Firewall : iptables, firewalld

### Module 7 : Maintenance du Système

Tâches de maintenance courante : Sauvegardes, mises à jour, nettoyage
Gestion des utilisateurs et des groupes : Création, modification, suppression
Sécurité du système : Permissions, mots de passe, audit

40H CODE : LPO3

## Objectifs

- Installer, configurer et maintenir un système RHEL
- Gérer les utilisateurs, les groupes et les permissions
- Configurer le réseau et les services système
- Utiliser les outils de gestion de paquets
- Mettre en œuvre des solutions de stockage
- Assurer la sécurité du système

## Débouchées

- Administrateurs système Linux débutants ou souhaitant se spécialiser sur RHEL
- Ingénieurs DevOps
- Toute personne souhaitant approfondir ses connaissances en administration système

## Prérequis

- Connaissances de base en informatique
- Expérience en utilisation d'un système d'exploitation Unix/Linux

# Programme RHCE

Module 1 : Introduction à Red Hat Enterprise Linux

Histoire et philosophie de RHEL
Architecture du système d'exploitation
Interface en ligne de commande (CLI)
Gestion des fichiers et des répertoires

Module 2 : Gestion des Utilisateurs et des Groupes

Création et gestion des utilisateurs et des groupes
Gestion des permissions
Contrôle d'accès basé sur les rôles (RBAC)

Module 3 : Gestion des Paquets

Utilisation de yum
Installation, mise à jour et suppression de logiciels
Création de référentiels personnalisés

Module 4 : Configuration du Réseau

Interfaces réseau
Configuration IP
Routage
Services réseau (SSH, FTP, HTTP)
Pare-feu

Module 5 : Gestion des Services Système

Démarrage et arrêt des services
Configuration des services
Gestion des processus
Module 6 : Stockage
Systèmes de fichiers
Gestion des partitions
Gestion des volumes logiques
Montages réseau

Module 7 : Sécurité

Gestion des utilisateurs à distance
Configuration du pare-feu
Cryptage
Sauvegardes et restaurations

Module 8 : Automatisation

Scripting shell
Ansible (introduction)

40H CODE : LPO4

## Objectifs

- Concevoir des architectures Linux robustes et évolutives
- Mettre en œuvre des solutions de virtualisation et de conteneurisation
- Gérer des environnements Linux complexes
- Automatiser les tâches administratives
- Sécuriser les systèmes Linux

## Débouchées

- Administrateur système Linux
- Ingénieur système
- Architecte infrastructure
- Spécialiste en sécurité informatique.
- Ingénieur DevOps

## Prérequis

- La certification RHCE ou notions équivalentes

# Programme RHCA

Module 1 : Fondamentaux de Red Hat Enterprise Linux
Revue des concepts clés de RHEL
Administration avancée des utilisateurs et des groupes
Gestion des systèmes de fichiers et des quotas
Configuration du réseau : interfaces, routage, firewall
Gestion des services systemd
Résolution de problèmes

Module 2 : Virtualisation
KVM : installation, configuration, gestion des machines virtuelles
Migration de machines virtuelles
Haute disponibilité avec KVM
Introduction à Libvirt

Module 3 : Conteneurisation
Docker : concepts de base, création d'images, gestion des conteneurs
Orchestration de conteneurs avec Kubernetes
Intégration de Kubernetes avec d'autres outils

Module 4 : Stockage
Gestion des volumes logiques
Systèmes de fichiers distribués (GlusterFS, Ceph)
Stockage réseau (NFS, iSCSI)

Module 5 : Réseau
Routage avancé (BGP, OSPF)
Équilibre de charge
VPN (IPsec, OpenVPN)
Réseau défini par logiciel (SDN)

Module 6 : Sécurité
Gestion des identités et des accès (IAM)
Chiffrement des données
Audit et conformité
Réponse aux incidents

Module 7 : Automatisation
Ansible : inventaire, modules, playbooks
Puppet : modules, manifests
Chef : recettes, cookbooks

Module 8 : Cloud Computing
Déploiement sur AWS, Azure, GCP
Infrastructure as Code (IaC)
Gestion des coûts

Module 9 : Architecture d'Entreprise
Conception d'architectures hautement disponibles
Dimensionnement des systèmes
Choix des technologies adaptées

edify digital

# Nos formations

aruba

40H CODE : ARO1

## Objectifs

- Comprendre les concepts fondamentaux des réseaux.
- Décrire l'architecture des solutions Aruba pour les campus.
- Configurer et gérer les points d'accès Aruba.
- Configurer et gérer les commutateurs Aruba.
- Mettre en œuvre des mesures de sécurité de base sur les réseaux Aruba.
- Utiliser les outils de gestion et de surveillance Aruba.
- Préparer l'examen de certification ACA.

## Débouchées

- Technicien réseau
- Administrateur réseau junior
- Technicien support informatique
- Intégrateur de solutions réseau

## Prérequis

Des connaissances de base en informatique
Une familiarité avec l'utilisation d'un ordinateur
familiarité avec les concepts de réseau

# Programme ACA

Module1:Concepts de base des réseaux :

Modèle OSI et TCP/IP.

Adresses IP et sous-réseaux.

Protocoles de routage de base.

Concepts de base des réseaux sans fil (Wi-Fi).

Module2: Solutions Aruba pour les campus

Présentation de l'architecture des solutions Aruba pour les campus. Types de déploiements (centralisé, distribué).

Présentation des différents produits Aruba (points d'accès, contrôleurs, commutateurs).

Module3:Configuration des points d'accès Aruba (AP)

Découverte et configuration des AP. Configuration des SSID (Service Set Identifier).

Paramètres de sécurité sans fil (WPA2/3).

Gestion des canaux et de la puissance.

Module4:Configuration des commutateurs Aruba

Configuration des VLAN (Virtual LAN).

Spanning Tree Protocol (STP).

Agrégation de liens (Link Aggregation).

Qualité de service (QoS).

Module5:Sécurité des réseaux Aruba

Concepts de base de la sécurité des réseaux.

Pare-feu.

Systèmes de détection d'intrusion (IDS).

Authentification (802.1X, RADIUS). Intégration avec Aruba ClearPass (introduction).

Module6:Gestion et surveillance des réseaux Aruba

Utilisation d'Aruba Central pour la gestion centralisée.

Outils de surveillance et de dépannage.

Génération de rapports.

40H CODE : ARO2

## Objectifs

- Comprendre et mettre en œuvre une architecture Zero Trust.
- Identifier et atténuer les menaces et vulnérabilités réseau avancées.
- Sécuriser les infrastructures réseau Aruba.
- Configurer et gérer Aruba ClearPass pour l'authentification et le contrôle d'accès.
- Déployer des solutions de sécurité Aruba pour protéger les réseaux contre les menaces.
- Intégrer les solutions de sécurité Aruba avec d'autres systèmes de sécurité.

## Débouchées

- Administrateur réseau
- Ingénieur réseau
- Spécialiste en sécurité réseau
- Consultant réseau

## Prérequis

- La certification Aruba Certified Associate (ACA)
- Une expérience pratique significative en administration réseau
- Une bonne connaissance des technologies sans fil (Wi-Fi )

## Programme ACP (Campus Access)

Module 1 : Architecture et conception des réseaux Aruba

Conception de réseaux pour les campus et les succursales.
Haute disponibilité et redondance.
Planification de la capacité.

Module 2 : Configuration avancée des commutateurs Aruba

Protocoles de routage avancés (OSPF, VRRP).
Sécurité avancée des ports (802.1X, MAC Authentication). Qualité de service (QoS) avancée.
Virtual Switching Framework (VSF) et Virtual Switching Extension (VSX).

Module 3 : Configuration avancée des points d'accès Aruba

Gestion du spectre radio.
Mobilité et itinérance.
Gestion des clients.
Mesh Wi-Fi.

Module 4 : Sécurité avancée des réseaux Aruba

Intégration avec Aruba ClearPass pour l'authentification et le contrôle d'accès.
Firewalling avancé.
Signatures numériques
Segmentation dynamique.

Module 4 : Gestion et surveillance avancées des réseaux Aruba

Utilisation d'Aruba Central pour la gestion centralisée et l'automatisation.
Outils de dépannage avancés.
API et intégration.


40H CODE : ARO2

## Objectifs

- Comprendre et mettre en œuvre une architecture Zero Trust.
- Identifier et atténuer les menaces et vulnérabilités réseau avancées.
- Sécuriser les infrastructures réseau Aruba.
- Configurer et gérer Aruba ClearPass pour l'authentification et le contrôle d'accès.
- Déployer des solutions de sécurité Aruba pour protéger les réseaux contre les menaces.
- Intégrer les solutions de sécurité Aruba avec d'autres systèmes de sécurité.

## Débouchées

- Ingénieur en sécurité réseau
- Analyste en sécurité
- Consultant en sécurité
- Administrateur de sécurité

## Prérequis

- Une expérience pratique significative en administration réseau
- Des connaissances de base en sécurité réseau
- La certification Aruba Certified Associate - Network Security (ACA)

## Programme ACP *(Network Security)*

Module 1 : Concepts de sécurité avancés

Architecture Zero Trust.

Menaces et vulnérabilités réseau avancées (ex : attaques DDoS, APT, etc.).

Principes de la cryptographie et des VPN.

Module 2 : Sécurité des infrastructures Aruba

Sécurisation des commutateurs Aruba (ex : port security, dynamic segmentation).

Sécurisation des points d'accès Aruba (ex : WPA3, AirWave).

Configuration des pare-feu Aruba (ex : Policy Enforcement Firewall).

Module 3 : Aruba ClearPass Policy Manager

Gestion du spectre radio.

Authentification, autorisation et comptabilité (AAA).

Profilage des périphériques.

Contrôle d'accès réseau (NAC).

Gestion des certificats.

Intégration avec d'autres systèmes de sécurité.

Module 4 : Solutions de sécurité Aruba

Aruba IntroSpect (analyse du comportement des utilisateurs et des entités).

VPN et sécurité d'accès à distance.

Intégration avec des solutions tierces de sécurité.


40H CODE : ARO2

# Programme ACP (Data Center)

## Objectifs

- Concevoir et mettre en œuvre une architecture de réseau de centre de données Aruba.
- Configurer et gérer les commutateurs Aruba CX dans un environnement de centre de données.
- Mettre en œuvre des solutions de sécurité pour les centres de données.
- Automatiser et orchestrer les tâches de gestion du réseau du centre de données.
- Utiliser les outils de gestion et de surveillance pour optimiser les performances et

## Débouchées

- Administrateur réseau
- Ingénieur réseau
- Spécialiste en sécurité réseau
- Consultant réseau

## Prérequis

- La certification Aruba Certified Associate (ACA)
- Une expérience pratique significative en administration réseau
- Une bonne connaissance des technologies sans fil (Wi-Fi )

<u>Module 1 : Architecture et conception des réseaux de centres de données</u>

Principes de conception des centres de données (ToR, EoR, Spine-Leaf).

Haute disponibilité et redondance dans les centres de données.

Virtualisation des fonctions réseau (NFV).

Automatisation et orchestration des réseaux.

<u>Module 2 : Commutateurs Aruba pour les centres de données</u>

Configuration avancée des commutateurs Aruba CX pour les centres de données.

Protocoles de routage pour les centres de données (BGP, EVPN).

Virtual Switching Framework (VSF) et Virtual Switching Extension (VSX) pour les centres de données.

Qualité de service (QoS) dans les centres de données.

Fabric Composer.

<u>Module 3 : Sécurité dans les centres de données</u>

Microsegmentation.

Sécurité des API.

Intégration avec les solutions de sécurité tierces.

<u>Module 4 : Automatisation et orchestration</u>

Utilisation d'API REST.

Intégration avec des outils d'automatisation (Ansible, Puppet, Chef).

SDN (Software-Defined Networking) et orchestration.

<u>Module 5 : Gestion et surveillance des réseaux de centres de données</u>

Outils de surveillance et d'analyse du trafic.

Dépannage avancé.

edify digital

# Nos formations

Microsoft


36H CODE : MSO1

## Objectifs

- Comprendre les concepts fondamentaux du cloud computing.
- Connaître les principaux services Azure et leurs cas d'utilisation.
- Utiliser les outils de gestion Azure de base.
- Comprendre les aspects de sécurité, de confidentialité et de conformité sur Azure.
- Connaître les bases de la gestion des coûts et des SLA Azure.

## Débouchées

- Vendeur de solutions cloud.
- Chef de projet cloud.
- Consultant en transformation digitale.
- Administrateur cloud junior.
- Technicien support cloud.
- Développeur cloud débutant.

## Prérequis

- Une compréhension de base des concepts informatiques
- Une familiarité avec l'utilisation d'ordinateurs et d'internet.

# Programme AZURE AZ 900

Module 1 : Décrire les concepts du cloud

Concepts de base du cloud computing (IaaS, PaaS, SaaS).
Avantages du cloud (évolutivité, élasticité, agilité, etc.).
Concepts de base de la facturation et des tarifs Azure.

Module 2 : Décrire les services Azure de base

Calcul (machines virtuelles, conteneurs, fonctions serverless).
Stockage (stockage d'objets, stockage de fichiers, bases de données).
Réseau (réseaux virtuels, VPN, équilibrage de charge).

Module 3 : Décrire les solutions et les outils de gestion sur Azure

Outils de gestion Azure (portail Azure, Azure CLI, PowerShell).
Surveillance et journalisation (Azure Monitor).
Déploiement et gestion des ressources (Azure Resource Manager).

Module 4 : Décrire les fonctionnalités de sécurité, de confidentialité et de conformité générales

Concepts de sécurité Azure (identité, accès, sécurité des données).
Confidentialité et conformité (RGPD, ISO 27001).

Module 5 : Décrire la gestion des coûts et les contrats de niveau de service Azure

Outils de gestion des coûts Azure.
Contrats de niveau de service (SLA).


24H CODE : MSO2

## Objectifs

- Être capable d'installer, de configurer et d'administrer un serveur Windows.
- Maîtriser la gestion des utilisateurs, des groupes et des ressources.
- Utiliser PowerShell pour automatiser les tâches.
- Diagnostiquer et résoudre les problèmes courants.

## Débouchées

- Administrateur système Windows.
- Technicien support informatique.
- Opérateur système.

## Prérequis

- Connaissances de base en informatique (systèmes d'exploitation, réseaux).
- Familiarité avec l'environnement Windows.

# Programme WINDOWS SERVER

Module 1 : Installation et configuration de Windows Server

Choix du type d'installation (Server Core, Desktop Experience).

Gestion des rôles et des fonctionnalités.

Configuration du stockage (disques, partitions, systèmes de fichiers).

Module 2 : Gestion des utilisateurs et des groupes

Active Directory (création d'utilisateurs, de groupes, gestion des GPO).

Module 3 : Gestion des services

Démarrage, arrêt et configuration des services.

Surveillance des performances.

Module 4 : Gestion du stockage

Gestion des disques, des volumes et des partages.

Gestion des quotas.

Module 5 : Automatisation avec PowerShell

Introduction à PowerShell et aux cmdlets.

Scripts pour automatiser les tâches d'administration.

Module 6 : Maintenance et dépannage

Gestion des mises à jour.

Résolution des problèmes courants.


36H CODE : MSO3

## Objectifs

- Comprendre les concepts de base de PowerShell.
- Être capable d'utiliser les cmdlets de base pour naviguer dans le système de fichiers et gérer les objets.
- Écrire des scripts simples pour automatiser des tâches courantes.

## Débouchées

- Support technique de premier niveau.
- Technicien d'assistance informatique.
- Premières tâches d'automatisation pour les administrateurs systèmes

## Prérequis

- Connaissances de base en informatique et en utilisation de Windows.
- Familiarité avec l'invite de commandes (CMD)

# Programme POWERSHELL *(Niveau Débutant)*

Module 1 : Introduction à PowerShell

L'environnement PowerShell (console, ISE, VS Code).

Les cmdlets (prononcés "command-lets") : verbes-noms (Get-Process, Stop-Service).

L'aide PowerShell : Get-Help, exemples.

Module 2 : Navigation et manipulation du système de fichiers

Cmdlets de navigation (Get-Location, Set-Location, Get-ChildItem).

Création, suppression et modification de fichiers et de répertoires.

Module 3 : Gestion des objets

Le pipeline PowerShell (|) : passage d'objets d'une cmdlet à une autre.

Filtrage et sélection d'objets (Where-Object, Select-Object).

Mise en forme de la sortie (Format-List, Format-Table).

Module 4 : Variables et opérateurs

Création et utilisation de variables.

Opérateurs arithmétiques, de comparaison et logiques.

Module 5 : Introduction aux scripts

Création et exécution de scripts simples (.ps1).

Commentaires dans les scripts.


36H CODE : MSO3

## Objectifs

- Maîtriser les structures de contrôle et les fonctions pour écrire des scripts plus complexes.
- Être capable de gérer les erreurs et de manipuler des données.
- Comprendre l'interaction avec WMI et CIM.

## Débouchées

- Administrateur système.
- Ingénieur système.
- Spécialiste en automatisation.

## Prérequis

- Connaissances acquises au niveau 1.
- Notions de programmation

# Programme POWERSHELL (Intermédiaire)

### Module 1 : Structures de contrôle

Instructions conditionnelles (if, elseif, else).
Boucles (for, foreach, while, do).
Switch.

### Module 2 : Fonctions et modules

Création et utilisation de fonctions.
Portée des variables.
Utilisation de modules PowerShell.

### Module 3 : Gestion des erreurs

Blocs try-catch-finally.
Gestion des exceptions.

### Module 4 : Manipulation de chaînes de caractères

Opérateurs de chaînes.
Expressions régulières (Regex - introduction).

### Module 5 : Gestion des données

Importation et exportation de données (CSV, XML, JSON).
Manipulation d'objets complexes.

### Module 6 : WMI et CIM

Interaction avec WMI (Windows Management Instrumentation) et CIM (Common Information Model).


24H CODE : MSO3

## Objectifs

- Être capable d'administrer des environnements complexes avec PowerShell.
- Maîtriser l'automatisation des tâches d'administration système et cloud.
- Comprendre l'intégration de PowerShell dans les pratiques DevOps.

## Débouchées

- Ingénieur DevOps.
- Architecte infrastructure.
- Spécialiste en automatisation et orchestration.
- Consultant en infrastructure.

## Prérequis

- Connaissances acquises au niveau 2.
- Expérience en administration système.
- Notions de DevOps sont un plus.

## Programme POWERSHELL (Niveau Avancé)

Module 1 : Administration Active Directory avec PowerShell

Gestion des utilisateurs, des groupes, des ordinateurs et des GPO.
Automatisation des tâches d'administration Active Directory.

Module 2 : Gestion des serveurs avec PowerShell

Gestion des services, des processus, des événements et du stockage.
Configuration et déploiement de rôles et de fonctionnalités serveur.

Module 3 : PowerShell et le Cloud (Azure, AWS)

Utilisation des modules Azure PowerShell et AWS Tools for PowerShell.
Automatisation du déploiement et de la gestion des ressources cloud.

Module 4 : PowerShell et la configuration d'état souhaité (DSC)

Définition et application de configurations souhaitées.
Automatisation du déploiement et de la configuration des serveurs.

Module 5 : PowerShell et DevOps

Intégration de PowerShell dans les pipelines CI/CD.
Utilisation de PowerShell pour l'infrastructure as code.


# MICROSOFT 365 FUNDAMENTALS MS 900

40H CODE : MSO4

## Objectifs

- Comprendre les concepts fondamentaux du cloud computing et les différents modèles de service cloud.
- Décrire les principaux services Microsoft 365 et leurs cas d'utilisation, en mettant l'accent sur la productivité et la collaboration.
- Comprendre les aspects de sécurité, de conformité, de confidentialité et de confiance dans Microsoft 365.
- Connaître les options de tarification, de support et les SLA de Microsoft 365.

## Débouchées

- Chef de projet Microsoft 365.
- Formateur Microsoft 365 pour les utilisateurs finaux.
- Consultant en transformation digitale axé sur Microsoft 365.
- Administrateur Microsoft 365.
- Technicien support Microsoft 365.

## Prérequis

Aucun

### Module 1 : Décrire les concepts du cloud

Concepts de base du cloud computing (IaaS, PaaS, SaaS, Public, Privé, Hybride).
Avantages et considérations de l'utilisation des services cloud (par exemple, haute disponibilité, évolutivité, fiabilité, prévisibilité des coûts, sécurité, gouvernance).

### Module 2 : Décrire les services et les concepts de base de Microsoft 365

Services de base de Microsoft 365 et leurs cas d'utilisation (Exchange Online, SharePoint Online, Teams, OneDrive, etc.).
Concepts de productivité et de collaboration dans Microsoft 365.
Licences et abonnements Microsoft 365.
Cycle de vie des services Microsoft 365.

### Module 3 : Décrire la sécurité, la conformité, la confidentialité et la confiance dans Microsoft 365

Concepts de sécurité dans Microsoft 365 (identité, accès, protection contre les menaces, gestion des informations).
Concepts de conformité dans Microsoft 365 (par exemple, RGPD, conformité réglementaire).
Concepts de confidentialité et de confiance dans Microsoft 365.

### Module 4 : Décrire les prix et le support Microsoft 365

Modèles de tarification Microsoft 365.
Options de support Microsoft 365.
Contrats de niveau de service (SLA).


24H CODE : MSO5

## Objectifs

- Gérer les identités et les accès dans Azure.
- Implémenter et gérer des solutions de stockage Azure.
- Déployer et gérer des machines virtuelles, des conteneurs et des solutions sans serveur.
- Configurer et gérer les réseaux virtuels Azure et la connectivité.
- Surveiller et sauvegarder les ressources Azure.
- Automatiser les tâches d'administration Azure à l'aide d'Azure CLI, de PowerShell et d'ARM Template.

## Débouchées

- Administrateur Azure.
- Ingénieur Cloud.
- Architecte Cloud (en combinaison avec d'autres certifications).
- Ingénieur DevOps (en combinaison avec d'autres compétences).
- Consultant Cloud.

## Prérequis

- Une expérience pratique en administration de systèmes d'exploitation (Windows Server ou Linux).
- Une compréhension des concepts de réseau (TCP/IP, DNS, VPN).Une familiarité avec les concepts de virtualisation.

## Programme AZURE 104

Module 1 : Gérer les identités et la gouvernance Azure

Gestion des utilisateurs et des groupes dans Azure Active Directory (Azure AD).

Mise en œuvre du contrôle d'accès basé sur les rôles (RBAC).

Gestion des abonnements et des ressources Azure.

Mise en œuvre de la gouvernance (Azure Policy, Blueprints).

Module 2 : Implémenter et gérer le stockage

Gestion des comptes de stockage (Stockage Blob, Stockage de fichiers, Stockage de files d'attente, Stockage de tables).

Configuration du stockage Azure (niveaux d'accès, réplication, sécurité).

Gestion des disques Azure.

Module 3 : Déployer et gérer les ressources de calcul Azure

Déploiement et configuration des machines virtuelles (VM).

Gestion des ensembles de machines virtuelles identiques.

Implémentation des solutions de calcul sans serveur (Azure Functions, Azure Logic Apps).

Gestion des conteneurs (Azure Kubernetes Service - AKS, Azure Container Instances).

Module 4 : Configurer et gérer les réseaux virtuels

Planification et implémentation des réseaux virtuels.

Configuration des sous-réseaux, des adresses IP et des tables de routage.

Implémentation de la connectivité entre les réseaux virtuels (appairage de réseaux virtuels, VPN Gateway).

Configuration d'Azure DNS.

Configuration de l'équilibrage de charge (Azure Load Balancer, Application Gateway).

Module 5 : Surveiller et sauvegarder les ressources Azure

Configuration de la sauvegarde des machines virtuelles.

Implémentation d'Azure Monitor (métriques, journaux, alertes).

Configuration de Log Analytics.

Utilisation de Network Watcher.


24H CODE : MSO6

## Objectifs

- Déployer et gérer AD DS dans des environnements hybrides.
- Gérer des serveurs Windows et des charges de travail dans Azure.
- Gérer des machines virtuelles et des conteneurs dans un contexte hybride.
- Configurer et gérer une infrastructure réseau hybride.
- Gérer les services de stockage et de fichiers dans un environnement hybride.
- Utiliser les outils et les services Azure pour gérer les environnements hybrides.

## Débouchées

- Administrateur système hybride.
- Ingénieur cloud hybride.
- Spécialiste en infrastructure hybride.
- Consultant en migration vers le cloud hybride.

## Prérequis

Notions en informatique et en réseau

## Programme AZURE 800

Module 1 : Déployer et gérer Active Directory Domain Services (AD DS) dans des environnements locaux et cloud

Installation et configuration des contrôleurs de domaine AD DS.
Gestion des objets AD DS (utilisateurs, groupes, GPO).
Implémentation de l'intégration hybride avec Azure AD (Azure AD Connect, synchronisation du hachage de mot de passe, authentification directe).
Gestion des identités hybrides (authentification unique, authentification multifacteur).
Résolution des problèmes d'AD DS.

Module 2 : Gérer les serveurs et les charges de travail Windows Server dans un environnement hybride

Gestion des serveurs Windows Server sur site et dans Azure (machines virtuelles Azure).
Implémentation et gestion de Windows Admin Center.
Gestion des mises à jour des serveurs.
Migration des charges de travail vers Azure.

Module 3 : Gérer les machines virtuelles et les conteneurs

Déploiement et gestion des machines virtuelles Azure.
Configuration du stockage et du réseau pour les machines virtuelles.
Gestion des conteneurs avec Azure Kubernetes Service (AKS) et Azure Container Instances (ACI).
Implémentation de solutions de conteneurisation hybrides.

Module 4 : Implémenter et gérer une infrastructure réseau locale et hybride

Configuration des réseaux virtuels Azure et de la connectivité hybride (VPN, ExpressRoute).
Gestion de la résolution de noms (DNS) dans un environnement hybride.
Implémentation et gestion des services de routage et d'équilibrage de charge.
Configuration des pare-feu et de la sécurité réseau.

Module 4 : Gérer les services de stockage et de fichiers

Implémentation et gestion du stockage Azure (Stockage Blob, Stockage de fichiers, Stockage de files d'attente).
Implémentation et gestion de la synchronisation de fichiers Azure (Azure File Sync).
Gestion des partages de fichiers et des permissions.
Implémentation de solutions de sauvegarde et de récupération.


24H CODE : MS07

## Objectifs

- Mettre en œuvre et gérer les solutions d'identité et d'accès dans Microsoft 365.
- Déployer et gérer les solutions de protection contre les menaces de Microsoft 365.
- Implémenter et gérer la protection des informations dans Microsoft 365.
- Gérer la gouvernance et la conformité des données dans Microsoft 365.
- Utiliser les outils d'administration et de surveillance de la sécurité de Microsoft 365.

## Débouchées

- Administrateur de la sécurité Microsoft 365.
- Ingénieur en sécurité cloud.
- Analyste en sécurité.
- Consultant en sécurité Microsoft 365.

## Prérequis

- Une expérience pratique en administration de Microsoft 365.
- Une compréhension des concepts de sécurité réseau et des principes de sécurité informatique.
- Une familiarité avec les outils d'administration Microsoft, tels que PowerShell et le centre d'administration Microsoft 365.
- Avoir suivi le cours MS-900 (Microsoft 365 Fundamentals)

## Programme SECURITY ADMINISTRATOR MS 500

Module 1 : Implémenter et gérer l'identité et l'accès

Planifier et mettre en œuvre l'authentification et l'autorisation modernes (par exemple, Azure AD, authentification multifacteur, accès conditionnel).

Gérer les identités et les rôles dans Azure AD.

Mettre en œuvre et gérer la gouvernance des identités (par exemple, gestion du cycle de vie des identités, gestion des accès privilégiés).

Module 2 : Implémenter et gérer la protection contre les menaces

Planifier, mettre en œuvre et gérer Microsoft Defender pour Office 365 (protection contre les menaces par e-mail et collaboration).

Planifier, mettre en œuvre et gérer Microsoft Defender pour Identity (protection des identités sur site).

Planifier, mettre en œuvre et gérer Microsoft Defender pour point de terminaison (protection des appareils).

Gérer les alertes et les incidents de sécurité.

Module 3 : Implémenter et gérer la protection des informations

Planifier et mettre en œuvre la classification et l'étiquetage des données.

Mettre en œuvre et gérer la prévention de la perte de données (DLP).

Mettre en œuvre et gérer le chiffrement des données (par exemple, Azure Information Protection, chiffrement des messages Office 365).

Module 4 : Gérer la gouvernance et la conformité dans Microsoft 365

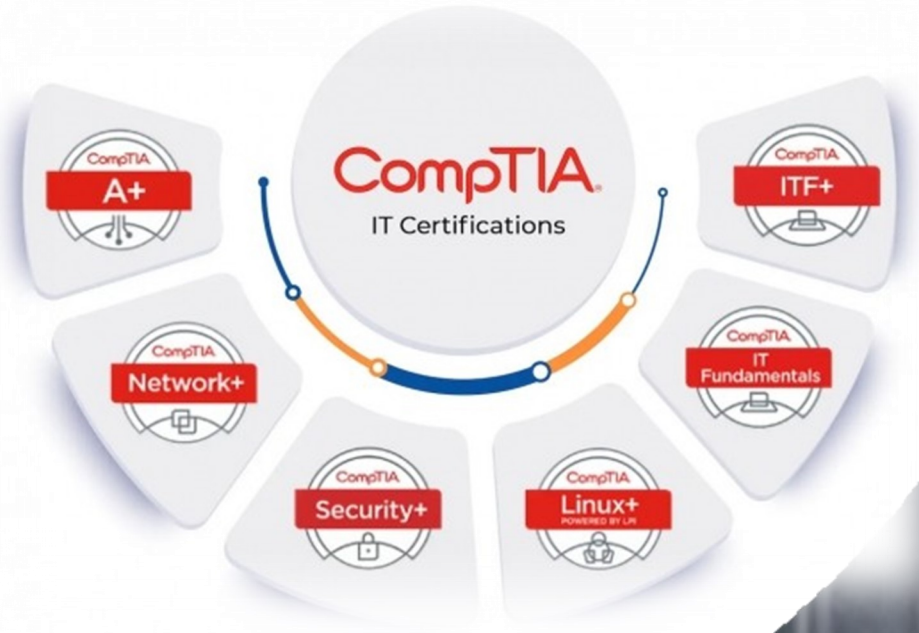
Planifier et mettre en œuvre la gouvernance des informations (par exemple, rétention, suppression, eDiscovery).

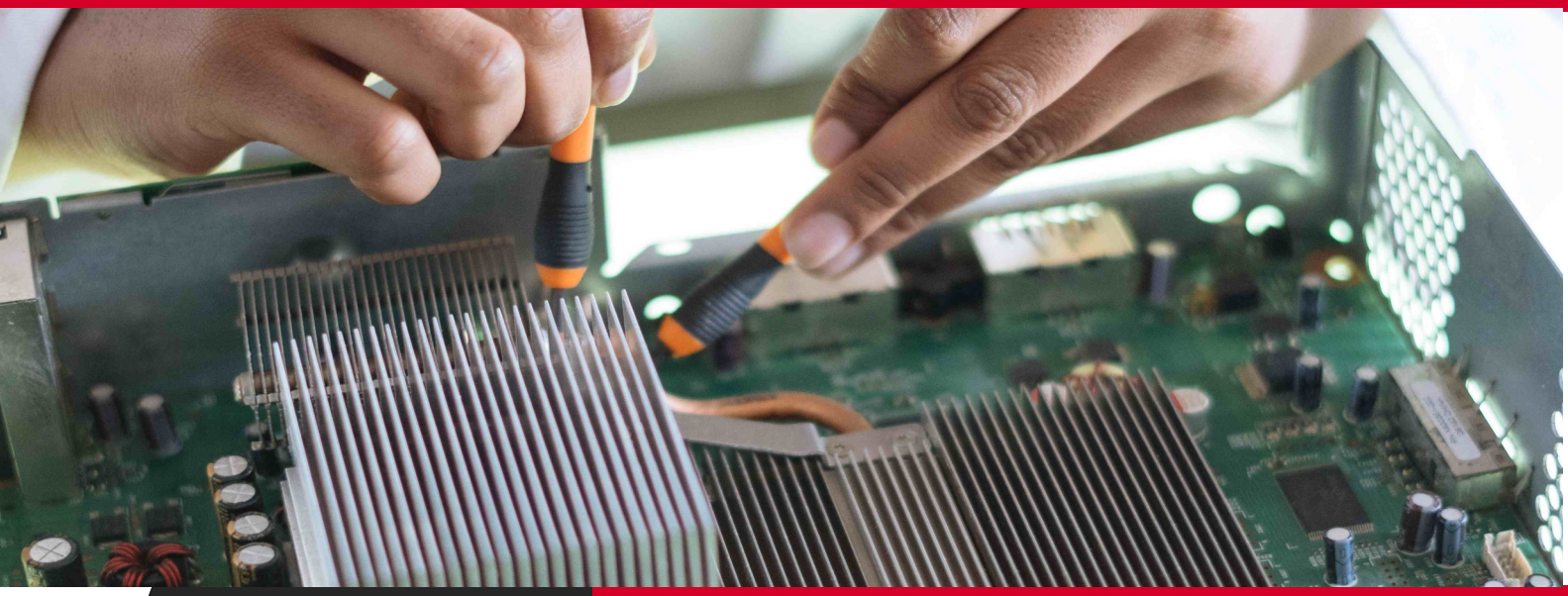
Gérer les audits et les rapports de conformité.

Comprendre les réglementations et les normes de conformité pertinentes.

edify digital

# Nos formations





70H CODE : HDO1

## Objectifs

- Choisir les composants informatiques appropriés pour assembler, réparer ou mettre à niveau des ordinateurs personnels.
- utiliser correctement les outils et travailler en toute sécurité dans un atelier.
- Installer des composants pour assembler, réparer ou mettre à niveau des ordinateurs personnels.
- Installer, assurer la gestion et la maintenance des systèmes d'exploitation Windows.
- Configurer les ordinateurs afin qu'ils communiquent sur un réseau.
- Configurer des périphériques pour qu'ils se connectent à Internet et aux services cloud.
- Décrire les procédures de configuration, de sécurisation et de dépannage des systèmes d'exploitation mobiles, macOS et Linux.
- Mettre en œuvre la sécurité de base du réseau, et des données

## Débouchées

- Spécialiste du support informatique.
- Technicien de helpdesk.
- Technicien sur le terrain.
- Spécialiste du support de niveau I.
- Spécialiste du support de bureau Technicien de support système.
- Administrateur système junior.

## Prérequis

Aucune connaissance particulière n'est requise pour cette formation

## Programme A+

<u>Présentation de l'ordinateur personnel :</u>

Expliquer l'interaction des différents composants d'un ordinateur personnel.

Expliquer les caractéristiques et les fonctions des composants.

Démonter un ordinateur.

<u>Installer des composants pour assembler, réparer ou mettre à niveau des ordinateurs personnels.</u>

Construire un ordinateur.

Matériel informatique, notions avancées :

<u>Installer et configurer les composants pour mettre à niveau un ordinateur</u>.

Expliquer la procédure de vérification des paramètres du BIOS et de l'UEFI.

Expliquer l'alimentation électrique.

Expliquer le fonctionnement de l'ordinateur.

Sélectionner les composants pour mettre à niveau un ordinateur afin de répondre à la configuration requise.

Expliquer les procédures nécessaires pour protéger l'environnement.

<u>Maintenance préventive et dépannage :</u>

Explication de l'importance de la maintenance préventive sur les ordinateurs personnels.

Résoudre les problèmes liés à l'ordinateur et aux périphériques.

<u>Concepts et configuration réseaux : .</u>

Expliquer les composants et les types de réseaux informatiques.

Expliquer les protocoles, les normes et les services réseau.

Expliquer les rôles des appareils sur un réseau.

Fabriquer un câble réseau.

Configurer les appareils pour les réseaux filaires et sans fil.

Résoudre les problèmes liés aux réseaux.

<u>Ordinateurs portables et terminaux mobiles</u>

Expliquer les procédures de dépannage des ordinateurs portables et des terminaux mobiles.

Expliquer les caractéristiques et les fonctionnalités des ordinateurs portables et des autres terminaux mobiles.

Expliquer les procédures de configuration des paramètres sans fil et d'alimentation d'un ordinateur portable.

Ordinateurs portables et terminaux mobiles (suite)

Explication des procédures de retrait et d'installation des composants d'un ordinateur portable.

Expliquer la finalité et les caractéristiques des terminaux mobiles.

Description des procédures de configuration de la connectivité réseau et de la messagerie électronique sur des appareils mobiles.

Utiliser les techniques de maintenance préventive courantes pour les ordinateurs portables et les terminaux mobiles.

Expliquer les procédures de dépannage des ordinateurs portables et des terminaux mobiles.

Installer une imprimante en répondant aux exigences définies.

Expliquer la fonction et les caractéristiques des différents types d'imprimantes.

Comparer les différents types d'imprimantes.

Installer une imprimante.

Configuration du partage d'imprimante.

Décrire les méthodes visant à améliorer la disponibilité des imprimantes.

Virtualisation et cloud computing.

Expliquer le cloud et la virtualisation.

Comparer et différencier les concepts du cloud computing

Installer des systèmes d'exploitation Windows.

Expliquer les exigences en matière de système d'exploitation.

Créer une partition dans Windows à l'aide de l'utilitaire de gestion des disques.

Objectifs

Installer un système d'exploitation Windows.

Assurer la gestion et la maintenance des systèmes d'exploitation Windows.

Configurer le bureau Windows et l'Explorateur de fichiers

Configurer Windows à l'aide des panneaux de configuration.

Configurer Windows à l'aide des panneaux de configuration.

Utiliser les outils et utilitaires Windows pour gérer le système Windows.

Utiliser les outils en ligne de commande de Microsoft Windows.

Configurer un ordinateur Windows pour utiliser un réseau

Utiliser les outils de maintenance préventive courants sur un ordinateur à l'aide des outils Microsoft Windows.

Expliquer les procédures de dépannage du système d'exploitation Microsoft Windows.

Systèmes d'exploitation mobiles, Linux et macOS

Expliquer la finalité et les caractéristiques des systèmes d'exploitation pour appareils mobiles.

Décrire les méthodes de protection des appareils mobiles.

Expliquer la finalité et les caractéristiques des systèmes d'exploitation macOS et Linux.

Explication des procédures de dépannage d'autres systèmes d'exploitation

Mettre en œuvre la sécurité de base du réseau, de l'hôte et des données.

Présenter les menaces pour la sécurité.

Expliquer les procédures de sécurité.

Configurer les paramètres et politiques de sécurité de base pour les terminaux.

Configurer la sécurité sans fil.

Expliquer les six étapes du processus de dépannage pour la sécurité.

Rôles et les responsabilités du professionnel de l'IT.

Présentation des raisons pour lesquelles de bonnes compétences en communication sont essentielles au travail du professionnel de l'IT.

Expliquer comment gérer les changements et interruptions imprévus dans une entreprise.

Explication du comportement à adopter face à des problèmes d'ordre éthique et juridique dans le secteur de l'IT.

Description de l'environnement d'un centre d'appels et des responsabilités des techniciens.


24H CODE : HDO2

# Objectifs

- Acquérir les connaissances théoriques et pratiques nécessaires pour installer, configurer et gérer des réseaux informatiques.
- Maîtriser les concepts fondamentaux des protocoles réseau, des topologies et des dispositifs de réseau.
- Développer les compétences de dépannage et de résolution de problèmes liés aux réseaux.

# Débouchées

- Spécialiste du soutien technique,
- spécialiste des opérations réseau,
- Spécialiste du support réseau de niveau 1
- Administrateur système junior.

# Prérequis

- Comptia A+ ou notions équivalentes

# Programme N+

## Module 1 : Fondamentaux des Réseaux

Modèle OSI et TCP/IP : Comprendre les différents modèles, les couches et les protocoles associés.

Topologies de réseau : Étudier les topologies physiques et logiques (étoile, bus, maillage, etc.).

Médias de transmission : Connaître les différents types de câbles et leurs caractéristiques.

Adresses IP : Comprendre les classes d'adresses, le sous-réseautage et le NAT.

## Module 2 : Dispositifs de Réseau

Hubs, switches et routeurs : Fonctionnement, configuration et différences.

Pare-feu : Types de pare-feu, règles de filtrage et configuration.

VPN : Concepts de base, types de VPN et configuration.

Wi-Fi : Standards, sécurité et configuration des points d'accès.

## Module 3 : Services Réseau

DHCP : Attribution dynamique d'adresses IP.

DNS : Système de noms de domaine.

SNMP : Protocole de gestion de réseau.

NTP : Synchronisation de l'heure.

## Module 4 : Sécurité des Réseaux

Menaces et vulnérabilités : Identifier les principales menaces et vulnérabilités.

Mesures de sécurité : Mise en œuvre de mesures de sécurité (mot de passe, chiffrement, etc.).

Gestion des risques : Évaluer et gérer les risques liés à la sécurité.

## Module 5 : Dépannage et Résolution de Problèmes

Outils de diagnostic : Utiliser des outils tels que ping, traceroute, Wireshark.

Méthodologie de dépannage : Suivre une démarche structurée pour résoudre les problèmes.

Analyse des journaux : Interpréter les journaux système pour identifier les causes des problèmes.


40H CODE : SECO1

## Objectifs

- Maîtriser les concepts fondamentaux de la sécurité informatique.
- Acquérir les compétences nécessaires pour mettre en œuvre et gérer des systèmes de sécurité efficaces

## Débouchées

- Technicien en sécurité informatique
- Analyste de la sécurité
- Spécialiste de la réponse aux incidents
- sécurité et restauration des systèmes.
- Consultant en sécurité

## Prérequis

- CCNA ou notions équivalentes

## Programme S+

Module 1 : Les fondamentaux de la sécurité

Définition de la sécurité informatique
Types de menaces (malware, phishing, etc.)
Vulnérabilités courantes
Les principes de la sécurité (CIA : confidentialité, intégrité, disponibilité)
Risques et gestion des risques:
Analyse des risques
Plans de continuité d'activité
Gestion des incidents
Législation et conformité:
Réglementations en matière de sécurité des données (RGPD, etc.)
Audits de sécurité

Module 2 : Architecture et conception des systèmes sécurisés

Protocoles sécurisés (HTTPS, VPN, etc.)
Firewalls–IDS/IPS
Segmentation de réseau
**Sécurité des systèmes d'exploitation:**
Configuration sécurisée de Windows et Linux
Gestion des privilèges
Patch management
Sécurité des applications:
Développement sécurisé
Tests d'intrusion
Protection contre les injections SQL et XSS

Module 3 : Cryptographie et gestion des identités

Algorithmes de chiffrement
Gestion des clés
Signatures numériques
Gestion des identités et des accès (IAM):
Authentification (mot de passe, biométrie)
Autorisation
Contrôle d'accès basé sur les rôles (RBAC)

Module 4 : Sécurité des systèmes d'information cloud et mobiles

Modèles de déploiement cloud (IaaS, PaaS, SaaS)
Sécurité des données dans le cloud
Sécurité des appareils mobiles:
Gestion des appareils mobiles (MDM)
Sécurité des applications mobiles

Module 5 : Réponse aux incidents et analyse numérique

Identification-Confinement-Éradication-Récupération
**Analyse numérique:**
Collecte d'évidences
Analyse des logs
Investigation d'incidents

# CISCO l'expertise mondiale

## en réseaux, sécurité et Internet !

Cisco, le leader mondial dans les domaines des réseaux, de la sécurité et de l'internet a mis en place ces dernières années une offre de certifications (Cisco Career Certifications) devenue aujourd'hui une référence incontournable sur le marché du travail. Cette importante offre de certification est hiérarchisée et classée selon 4 niveaux de qualification : Entry, Associate, Professionnal, et Expert. Connue de tous et recherchée par les professionnels des IT, la certification « Entry » est le niveau initial des certifications CCENT.

À noter que depuis le mois de février 2020, CISCO a changé la classification de ses certifications. Elles se présentent désormais en 4 niveaux de compétences (CCNA, Specialist, CCNP et CCIE) pour 6 domaines de spécialités techniques (Enterprise, Security, Service Provider, Collaboration, Data Center et DevNet) au lieu de 7.

Le parcours de certification Cisco sera ainsi plus rapide, plus lisible, plus spécialisé mais aussi plus facile à maintenir dans une carrière.

Rendez-vous sur notre site pour découvrir toutes les nouveautés CISCO.

# NOUVEAUX PARCOURS DE CERTIFICATION CISCO

| | Enterprise | | Security | Service Provider | Collaboration | Data Center | DevNet |
|---|---|---|---|---|---|---|---|
| CCIE | CCIE Enterprise Infrastructure 300-401 ENCOR + Infrastructure Lab v1.0 | CCIE Enterprise Wireless CCIE 300-401 ENCOR + Wireless Lab v1.0 | CCIE Security 300-701 SCOR + Lab | CCIE Service Provider 300-501 SPCOR + Lab | CCIE Collaboration 300-801 CLCOR + Lab | CCIE Data Center 300-601 DCCOR + Lab | CCIE DevNet |
| CCNP | CCNP Enterprise 300-401 ENCOR | | CCNP Security 300-701 SCOR + concentration | CCNP Service Provider 300-501 SPCOR + concentration exam | CCNP Collaboration 300-801 CLCOR + concentration exam | CCNP Data Center 300-601 DCCOR + concentration exam | Cisco Certified DevNet Professional 300-901 DEVCOR + concentration exam |
| SPECIALIST | Pass any CORE Exam | | | | | | DevNet Specialist Pass any concentration exam |
| CCNA | CCNA 200-301 | | | | | | DevNet Associate DEVASC 200-901 |

edify digital

72H CODES : NTO1 NTO2 NTO3

## Objectifs

Maitriser l'installation, la configuration et la maintenance d'un réseau de petite et moyenne taille

- Maitriser les connaissances théoriques fondamentales des réseaux et de la mise en place de réseaux locaux simples
- Comprendre les fondamentaux de la sécurité, de la mise en réseau et de l'automatisation
- Savoir sécuriser un réseau informatique et ses périphériques
- Passer et réussir l'examen de certification CCNA 200-301

## Débouchées

- Ingénieur réseaux
- Administrateur réseaux
- Technicien réseaux
- Technicien support

## Prérequis

Bonnes connaissances en informatique
Compétences en matière d'utilisation Internet

# Programme CCNA

### Approche fondamentale du réseau

Exploration des fonctions réseaux
Modèle de communication d'hôte à hôte
Fonctionnalités du logiciel Cisco IOS
Présentation des réseaux locaux LAN
Explication de la couche de liaison TCP/IP
Fonctionnement d'un commutateur
Explication de la couche Internet TCP/IP, de l'adressage IPv4 et des sous-réseaux
Couche de transport TCP/IP et les applications
Présentation des fonctions de routage

### Les accès au réseau

Configuration d'un routeur Cisco
Fonctionnalités du processus de livraison de paquets
Dépannage d'un réseau

### La connectivité IP

Explication de l'IPv6
Configuration d'un routage statique
Mise en place des VLANs et des trunks
Explication du routage entre VLANs

### Les services IP

Présentation du protocole de routage dynamique d'OSPF
Création d'un réseau commuté avec des liens redondants
Améliorer la structure commutée redondantes avec EtherChannel

Configuration de la redondance de la couche 3 avec le protocole HSRP
Exploration des technologies WAN
Explication des accès ACL
Activation de la connectivité Internet
Présentation de la qualité de service informatique (QoS)
Principes de base des réseaux sans fil
Présentation des architectures informatiques et la virtualisation
Explication de l'évolution des réseaux intelligents

### Les fondamentaux de la sécurité

Explication sur le monitoring du système

Gestion des périphériques Cisco

Identifier les menaces pour la sécurité du réseau
Présentation des technologies de défense contre les menaces
Sécurisation de l'accès administratif
Mise en place des dispositifs de renforcement

### Virtualisation du réseau

Cloud computing
Virtualisation .
Infrastructure de réseau virtuelle virtualisation des services et des périphériques réseau.
Réseaux SDN
Contrôleurs

### Automatisation du réseau

Décrire l'automatisation.
Formats de données Comparer les formats de données JSON, YAML et XML.
API & REST
Gestion de la configuration(Puppet, Chef, Ansible et SaltStack)
IBN et Cisco DNA Center

Take this course to level up your Network Security skills and get ready for in-demand security job roles. You'll get lots of practice, with 45 hands-on labs. Build your skills in implementing security measures, detecting vulnerabilities, and responding to incidents while ensuring network integrity. This comprehensive course helps you develop a deep understanding of Network Security and build expertise in designing, implementing, and supporting secure networks and data protection.

**40H CODE : SECO3**

## Objectifs

Comprendre et prévenir les menaces et attaques réseau.
Mettre en œuvre des mesures de sécurité robustes pour protéger les réseaux.
Configurer et gérer des dispositifs de sécurité réseau (firewalls, VPN, etc.).
Développer des compétences pratiques en matière de sécurité réseau

## Débouchées

- Technicien en sécurité informatique
- Analyste de la sécurité
- Spécialiste de la réponse aux incidents
- sécurité et restauration des systèmes.
- Consultant en sécurité

## Prérequis

- CCNA ou notions équivalentes

## NETWORK SECURITY

Module 1 : Introduction à la sécurité réseau
Concepts fondamentaux de la sécurité réseau (CIA : confidentialité, intégrité, disponibilité)
Types de menaces et attaques (malware, attaques DDoS, phishing, etc.)
Vulnérabilités communes (erreurs de configuration, failles logicielles, etc.)
Principes de défense en profondeur

Module 2 : Sécurité des périphériques réseau
Gestion et surveillance sécurisée des périphériques réseau (SNMP, syslog)
Configuration des niveaux de privilège et des commandes CLI basées sur les rôles
Mise en œuvre de l'authentification, de l'autorisation et de la comptabilité (AAA) (RADIUS, TACACS+)

Module 3 : Filtrage de trafic et pare-feu
Listes de contrôle d'accès (ACL) : configuration et utilisation
Pare-feu basés sur les zones (ZBF) : configuration et utilisation
Comparaison des différents types de pare-feu (stateless, stateful)

Module 4 : Systèmes de prévention des intrusions (IPS)
Principes de fonctionnement des IPS
Types d'IPS (NIPS, HIPS)
Configuration et gestion des IPS

Module 5 : Sécurité des points d'extrémité
Vulnérabilités des points d'extrémité (ordinateurs, appareils mobiles)
Méthodes de protection des points d'extrémité (antivirus, anti-malware, firewalls logiciels)
Gestion des correctifs et des mises à jour

Module 6 : Sécurité de la couche 2
Semaine 6 :
Attaques de la couche 2 (attaques ARP, attaques de diffusion)
Méthodes de mitigation des attaques de la couche 2 (VLAN, STP)

Module 7 : Cryptographie
Concepts de base de la cryptographie (chiffrement, hachage, signatures numériques)
Algorithmes de chiffrement symétrique et asymétrique
Infrastructure à clé publique (PKI)

Module 8 : VPN
Protocoles VPN (IPsec, SSL/TLS)
Configuration d'un VPN IPsec site-à-site
Utilisation des VPN pour l'accès à distance

Module 9 : Cisco ASA
Présentation du Cisco ASA
Configuration du pare-feu ASA à l'aide de la CLI et de l'ASDM
Fonctionnalités avancées du Cisco ASA

Module 10 : Tests de sécurité
Méthodes de test de sécurité (tests d'intrusion, analyse des vulnérabilités)
Outils de test de sécurité (nmap, Wireshark)
Analyse des résultats des tests de sécurité


40H CODE : SECO4

## Objectifs

- Identifier et analyser les menaces cybernétiques: Détecter les incidents de sécurité, comprendre les techniques d'attaque et évaluer les risques.
- Mettre en œuvre des mesures de sécurité: Configurer et gérer les systèmes de sécurité réseau, tels que les IDS/IPS, les firewalls et les systèmes de prévention des intrusions.
- Réagir aux incidents de sécurité: Suivre les procédures d'incident, mener des investigations et mettre en œuvre des mesures correctives.
- Collaborer au sein d'une équipe de sécurité: Communiquer efficacement avec les autres membres de l'équipe et contribuer à l'amélioration continue des processus de sécurité.

## Débouchées

- Analyste de la sécurité: Surveillance des événements de sécurité, détection des incidents.
- Ingénieur de la sécurité
- Responsable de la sécurité:
- Consultant en sécurité:

## Prérequis

- Connaissances de base en réseau: TCP/IP, routage, commutation.
- Expérience avec les systèmes d'exploitation: Windows, Linux

## CYBER OPS 200-201

Module 1 : Fondamentaux de la Sécurité Cybernétique

Cycle de vie d'un incident de sécurité: Détection, analyse, réponse, récupération.

Menaces courantes: Malware, attaques par déni de service, piratage, ingénierie sociale.

Vulnérabilités: Failles logicielles, erreurs de configuration.

Contrôles de sécurité: Authentification, autorisation, chiffrement.

Module 2 : Technologies de Sécurité Réseau

IDS/IPS: Fonctionnement, signature, anomalies.

Firewalls: Stateful, NGFW, WAF.

VPN: IPsec, SSL.

EDR: Endpoint Detection and Response.

SIEM: Security Information and Event Management.

Module 3 : Analyse des Menaces et Incidents

Techniques d'attaque: Exploitation de vulnérabilités, attaques par force brute, phishing.

Outils d'analyse: Wireshark, Snort, SIEM.

Investigation d'incidents: Collecte d'évidences, analyse forensique.

Module 4 : Réponse aux Incidents

Plans de réponse aux incidents: Élaboration et mise en œuvre.

Gestion de crise: Communication, escalade, coordination.

Restauration des systèmes: Sauvegardes, récupération.

Module 5 : Automatisation et Orchestration

SOAR: Security Orchestration, Automation and Response.

Intégration des outils de sécurité: API, scripts.

Module 6 : Pratiques Meilleurs et Tendances

Frameworks de sécurité: NIST CSF, CIS Controls.

Sécurité cloud: IaaS, PaaS, SaaS.

Sécurité IoT: Vulnérabilités et défis

40H CODE : SECO3

# CCNP SCNF 300-710

## Objectifs

Maîtriser le Cisco Firepower: Acquérir une connaissance approfondie des fonctionnalités avancées du Cisco Firepower en tant que pare-feu nouvelle génération.
Mettre en œuvre des politiques de sécurité: Configurer des règles de sécurité complexes, des contrôles d'accès et des politiques de VPN.
Gérer les menaces: Identifier, analyser et répondre aux menaces en utilisant les fonctionnalités IPS et Threat Intelligence.
Optimiser les performances: Configurer et ajuster le Cisco Firepower pour garantir des performances optimales dans différents environnements.
Intégrer le Cisco Firepower dans une architecture de sécurité globale: Comprendre comment le Cisco Firepower s'intègre avec d'autres produits Cisco et tiers

## Débouchées

- Ingénieur sécurité réseau: Conception, mise en œuvre et maintenance de solutions de sécurité réseau
- Administrateurs réseaux
- Architectes réseau: Pour concevoir des architectures de sécurité robustes et évolutives.
- Consultants en sécurité

## Prérequis

- CCNP SECURITY CORE ou notions équivalentes

<u>Module 1 : Introduction au Cisco Firepower</u>

Architecture du Cisco Firepower: Composants, fonctionnement.

Fonctionnalités clés: Pare-feu, IPS, VPN, WAF.

Intégration avec d'autres produits Cisco: ISE, Prime Infrastructure.

<u>Module 2 : Configuration de Base</u>

Interface utilisateur: FMC (Firepower Management Center)

Objets de sécurité: Groupes d'accès, réseaux, services.

Politiques de sécurité: Règles d'accès, NAT, VPN.

<u>Module 3 : Système de Prévention des Intrusions (IPS)</u>

Signatures IPS: Types de signatures, mise à jour.

Configuration des règles IPS: Adaptation aux besoins spécifiques.

Gestion des fausses alertes.

<u>Module 4 : Sécurité des Applications Web (WAF)</u>

Protection contre les attaques web: XSS, SQL injection, etc.

Configuration des règles WAF: Protection des applications web.

<u>Module 5 : VPN</u>

IPsec VPN: Configuration de tunnels site-à-site et de télétravail.

SSL VPN: Accès distant sécurisé.

<u>Module 6 : Gestion des Menaces</u>

Threat Intelligence: Sources d'information, intégration dans le Cisco Firepower.

Analyse des événements: Corrélation des événements, investigation des incidents.

Automatisation des réponses: Playbooks, orchestration.

<u>Module 7 : Optimisation des Performances</u>

Dimensionnement du Cisco Firepower: Calcul des capacités.

Optimisation des règles: Éviter les goulots d'étranglement.

Dépannage: Outils et techniques.

<u>Module 8 : Intégration Avancée</u>

Intégration avec SIEM: Corrélation des événements de sécurité.

Automatisation: Ansible, Python.


Cette formation certifiante est la porte d'entrée de la filière sécurité de Cisco. Elle compose l'un des deux prérequis pour devenir CCNP Security. En la suivant, vous apprendrez à maîtriser les compétences et les technologies nécessaires pour implémenter les principales solutions de sécurité Cisco afin d'assurer une protection avancée contre les attaques de cyber sécurité. Durant la formation vous développerez vos connaissances dans la mise en œuvre et l'exploitation des technologies de sécurité de base, notamment la sécurité des réseaux, la sécurité dans les cloud, la sécurité du contenu, la protection et la détection des points d'extrémité, l'accès sécurisé aux réseaux, la visibilité et l'application. Cette formation vous prépare également à réussir l'examen de certification SCOR (350 -701)

**40H CODE : SECO4**

## Objectifs

- Connaitre les concepts et les stratégies de sécurité de l'information au sein du réseau
- Comprendre les attaques TCP/IP courantes, les applications réseau et les points d'extrémité
- Savoir décrire comment les différentes technologies de sécurité des réseaux fonctionnent ensemble pour se protéger contre les attaques
- Savoir mettre en place un contrôle d'accès sur les équipements Cisco ASA et le pare-feu Cisco Firepower
- Connaitre et mettre en œuvre les caractéristiques et les fonctions de sécurité du contenu web fournies par le Cisco Web Security Appliance
- Maitriser les capacités de sécurité de Cisco Umbrella, les modèles de déploiement, la gestion des politiques et la console Investigate
- Connaitre les VPN et savoir décrire les solutions et les algorithmes de cryptographie
- Savoir mettre en œuvre les solutions de connectivité d'accès à distance sécurisé Cisco et savoir décrire comment configurer l'authentification 802.1X et EAP, etc.

## Débouchées

- Technicien en sécurité informatique
- Analyste de la sécurité
- Spécialiste de la réponse aux incidents
- sécurité et restauration des systèmes.
- Consultant en sécurité

## Prérequis

- CCNA + Network security ou notions équivalentes

## CCNP SCOR 350-701

**Module 1 : Fondamentaux de la Sécurité Réseau**

Concepts de base: Définition de la sécurité réseau, menaces courantes, bonnes pratiques.

Protocoles de sécurité: TCP/IP, SSL/TLS, VPN, IPSec.

Architecture de sécurité: DMZ, pare-feu, systèmes de prévention d'intrusion.

**Module 2 : Technologies de Sécurité Cisco**

Cisco Firepower: Configuration et gestion, règles de sécurité, fonctionnalités avancées.

Cisco Identity Services Engine (ISE): Authentification, autorisation, comptabilité (AAA), gestion des politiques.

Cisco Secure Email: Protection contre les menaces par e-mail, filtrage du contenu.

**Module 3 : Sécurité du Cloud et des Centres de Données**

Sécurité dans les environnements cloud: AWS, Azure, GCP.

Sécurité des conteneurs: Docker, Kubernetes.

Sécurité des données au repos et en transit.

**Module 4 : Gestion des Événements de Sécurité**

Systèmes de détection d'intrusion (IDS/IPS): Configuration et analyse des alertes.

Gestion des logs: Collecte, analyse, corrélation.

Incident response: Plans d'urgence, procédures d'investigation.

**Module 5 : Automatisation et Orchestration**

Ansible: Automatisation des tâches de configuration et de maintenance.

Intégration avec d'autres outils: SIEM, SOAR.

70H CODE : SECO6

# INTRO TO CLOUD SECURITY

## Objectifs

- Comprendre les concepts fondamentaux du cloud computing et ses modèles de service (IaaS, PaaS, SaaS).
- Identifier les menaces et les vulnérabilités spécifiques au cloud.
- Connaître les principaux domaines de la sécurité du cloud : sécurité des données, sécurité des identités et des accès, sécurité des infrastructures, conformité et gouvernance.
- Comprendre le modèle de responsabilité partagée dans le

## Débouchées

Chefs de projet

Responsables métiers

Professionnels des achats et des contrats

Toute personne souhaitant évoluer

## Prérequis

Connaissances de base en informatique

Notions élémentaires de sécurité informatique

Toute personne souhaitant évo-

Module 1 : Introduction au Cloud Computing

Qu'est-ce que le cloud computing ? Définition, avantages, inconvénients.

Les modèles de service cloud : IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service).

Les modèles de déploiement cloud : public, privé, hybride.

Concepts clés : virtualisation, élasticité, scalabilité, haute disponibilité.

Module 2 : Menaces et Vulnérabilités dans le Cloud

Menaces spécifiques au cloud : accès non autorisés, violations de données, attaques DDoS, vulnérabilités des API, etc.

Les risques liés à la virtualisation et à la multi-location.

Les défis de la sécurité dans un environnement partagé.

Module 3 : Le Modèle de Responsabilité Partagée

Explication détaillée du modèle de responsabilité partagée entre le fournisseur de services cloud et le client.

Clarification des responsabilités de chacun en matière de sécurité pour les différents modèles de service (IaaS, PaaS, SaaS).

Importance de la configuration et de la gestion de la sécurité côté client.

Module 4 :Sécurité des Données dans le Cloud

Chiffrement des données au repos et en transit.

Gestion des clés de chiffrement.

Contrôle d'accès aux données.

Protection contre la perte et la corruption de données

Module 5 :Sécurité des Identités et des Accès

Gestion des identités et des accès (IAM).

Authentification multi-facteurs (MFA).

Contrôle d'accès basé sur les rôles (RBAC).

Gestion des identités fédérées.

Module 6 :Sécurité de l'Infrastructure Cloud

Sécurité des réseaux virtuels (VPC).

Groupes de sécurité et pare-feu.

Sécurité des instances virtuelles.

Module 7:Conformité et Gouvernance dans le Cloud

Normes et certifications de sécurité du cloud (ISO 27001, SOC 2, etc.).

Exigences réglementaires et juridiques.

Audit et conformité dans le cloud.

Module 8 : Bonnes Pratiques et Outils de Sécurité du Cloud

Principes de sécurité Zero Trust.

Sécurité par conception (Security by Design).

Outils de sécurité cloud natifs et tiers.

Automatisation de la sécurité.

70H CODE : NTO4

# CCNP ENTERPRISE CORE

## Objectifs

Le CCNP ENCOR vise à vous doter des compétences nécessaires pour :
Installer, configurer et vérifier les technologies de routage et de commutation Cisco.
Mettre en œuvre des solutions de réseau d'entreprise.
Dépanner les problèmes de réseau.
Assurer la sécurité des réseaux d'entreprise.
Automatiser les tâches de configuration réseau.

## Débouchées

Ingénieur réseau senior: Conception, implémentation et maintenance de réseaux d'entreprise complexes.
Architecte réseau: Conception de solutions réseau à grande échelle.
Spécialiste de la sécurité réseau: Mise en œuvre de mesures de sécurité pour protéger les réseaux.
Consultant réseau: Fourniture de conseils et d'expertise aux entreprises.

## Prérequis

CCNA ou notions équivalentes

### Module 1 : Fondamentaux des Réseaux

Modèle OSI et TCP/IP: Révision des concepts de base.
Technologie Ethernet: Trames Ethernet, commutation, VLAN.
Routage IP: Protocoles de routage (RIP, OSPF, EIGRP), concepts de routage.

### Module 2 : Technologies de Commutation

Spanning Tree Protocol (STP): Prévention des boucles, modes de fonctionnement.
STP topology with root bridge
VLANs: Segmentation de réseaux, inter-VLAN routing.
VTP: Gestion centralisée des VLANs.
EtherChannel: Agrégation de liens.

### Module 3 : Technologies de Routage Avancé

OSPF: Configuration détaillée, areas, LSA.
EIGRP: Configuration détaillée, métriques, auto-summarisation.
BGP: Routage inter-domaine, attributs BGP.

### Module 4 : Services IP

DHCP: Configuration de serveurs DHCP.
NAT: Traduction d'adresses réseau.
QoS: Classification, marquage, gestion de la congestion.

### Module 5 : Sécurité Réseau

ACLs: Listes de contrôle d'accès.
Firewalls: Fonctionnement et configuration.
VPN: Tunnels IPsec, DMVPN.
Module 6 : Virtualisation et SDN

VXLAN: Encapsulation VXLAN, VTEP.
SDN: Concepts de base, SDN controllers.

### Module 7 : Automatisation et Programmation

Ansible: Automatisation de tâches de configuration.
Python: Programmation réseau avec Python.

### Module 8 : Dépannage

Méthodologie de dépannage.
Utilisation des commandes show.
Analyse de captures de paquets.

70H CODE : NT05

# CCNP ENTERPRISE ADVANCED ROUTING

## Objectifs

Le cours CCNP ENARSI vise à doter les professionnels de la réseau des compétences nécessaires pour :

- Configurer, optimiser et dépanner des réseaux d'entreprise complexes.
- Mettre en œuvre des technologies de routage avancées.
- Assurer la haute disponibilité et la performance des réseaux.
- Sécuriser les réseaux d'entreprise.
- Automatiser des tâches de configuration et de gestion de réseau.

Compétences clés à acquérir :

- Routage avancé: EIGRP, OSPF, BGP, ISIS
- VPN: IPsec, DMVPN, GRE
- Services de qualité de service (QoS): Classification, marquage, gestion de la congestion
- Protocoles de routage multicast: PIM, DVMRP
- Technologies de virtualisation: VXLAN, NVGRE
- Automatisation: Ansible, Python
- Sécurité: ACL, IPS, Firewall

## Débouchées

- Ingénieur réseau senior: Conception, implémentation et maintenance de réseaux d'entreprise complexes.
- Architecte réseau: Conception de solutions réseau à grande échelle.
- Spécialiste de la sécurité réseau: Mise en œuvre de mesures de sécurité pour protéger les réseaux.
- Consultant réseau: Fourniture de conseils et d'expertise aux entreprises.

Module 1 : Fondamentaux du Routage Avancé

EIGRP: Concepts de base, métriques, auto-summarisation

Configuration avancée (stub areas, route summarization)

OSPF: Types d'areas, LSA, SPF

Configuration avancée (virtual links, OSPFv3)

BGP: Attributs BGP, AS path, route reflectors

Configuration de routage inter-domaine

Module 2 : VPN et Services de Tunnel

IPsec: Encapsulation, modes de transport et tunnel

Configuration de VPN site-à-site

DMVPN: Hub and spoke, full mesh

Configuration et gestion de DMVPN

GRE: Encapsulation générique

Utilisation de GRE pour les tunnels VPN

Module 3 : QoS et Multicast

QoS: Classification, marquage, gestion de la congestion

Configuration de QoS sur les routeurs et commutateurs

Multicast: PIM, DVMRP :Configuration de routage multicast

Module 4 : Technologies de Virtualisation

VXLAN: Encapsulation VXLAN, VTEP

Intégration avec les réseaux physiques

NVGRE: Comparaison avec VXLAN

Cas d'utilisation spécifiques

Module 5 : Automatisation et Programmation Réseau

Ansible: Playbooks, modules

Automatisation de tâches de configuration

Python: Programmation réseau avec Python

Intégration avec les API des équipements réseau

Module 6 : Sécurité Réseau

ACL: Configuration d'ACL étendues et standard

IPS: Déploiement et configuration d'un système de prévention des intrusions

Firewall: Configuration de règles de pare-feu

Module 7 : Haute Disponibilité et Redondance

HSRP, VRRP : Protocoles de routage de secours

CARP: Protocole de clustering pour les commutateurs

Clustering de routeurs: Configuration de clusters de routeurs

Module 8 : Dépannage Avancé

Outils de dépannage:

Debug, show commands

Méthodologie de dépannage

Analyse de traces

Module 9 : Labos Pratiques

Configuration de scénarios réseau complexes

Résolution de problèmes réels

70H CODE : SECO6

# PANORAMA DU TOP 5 DES EDITEURS DE SECURITE

## Objectifs

Comprendre les fondamentaux de la sécurité réseau
Comparer et contraster les solutions de sécurité réseau proposées par Cisco, Palo Alto, Fortinet, Checkpoint et F5. Analyser les forces et les faiblesses de chaque solution en fonction des besoins spécifiques d'une organisation.
Évaluer les exigences de sécurité, les contraintes budgétaires et les caractéristiques techniques.
Configurer les fonctionnalités clés, surveiller la performance et répondre aux incidents.
S'adapter aux évolutions technologiques en matière de sécurité réseau: Rester informé des dernières tendances et des nouvelles menaces

## Débouchées

Ingénieur sécurité réseau: Conception, mise en œuvre et maintenance de solutions de sécurité réseau
Administrateurs réseaux: Pour enrichir leurs compétences et choisir les meilleures solutions pour sécuriser leurs infrastructures.
Architectes réseau: Pour concevoir des architectures de sécurité robustes et évolutives.
Consultants en sécurité: Pour conseiller leurs clients sur les solutions de sécurité les plus adaptées.

## Prérequis

CCNA ou notions équivalentes

<u>Module 1 : Fondamentaux de la Sécurité Réseau</u>
Les enjeux de la sécurité dans un environnement numérique en constante évolution
Principes de défense en profondeur:
Normes et certifications:
ISO 27001, NIST Cybersecurity Framework
Certifications professionnelles (CISSP, CCSP)

<u>Module 2 : Présentation des Principaux Éditeurs</u>
Cisco:
Cisco ASA, FTD, Firepower
IPS, VPN, NGFW
Intégration avec d'autres produits Cisco
Palo Alto:
Pare-feu nouvelle génération
Prévention des intrusions
Analyse des menaces
Fortinet:
FortiGate
FortiClient
FortiAnalyzer
Checkpoint:
Pare-feu nouvelle génération
Threat Prevention
SandBlast
F5:
BIG-IP
Load balancing, WAF, DDoS protection

<u>Module 3 : Comparaison des Solutions</u>
Tableau comparatif des fonctionnalités:
NGFW, IPS, VPN, WAF, Sandboxing
Gestion unifiée des menaces
Intégration avec d'autres solutions de sécurité

Cas d'utilisation:
Protection des réseaux d'entreprise
Sécurité des datacenters
Sécurité du cloud

Critères de sélection:
Taille de l'entreprise
Budget
Exigences réglementaires
Compétences internes

<u>Module 4 : Mise en œuvre et Gestion Configuration de base</u>:
Création de zones de sécurité
Définition de règles de pare-feu
Configuration de VPN

Gestion des événements de sécurité:
Systèmes de détection d'intrusion (IDS/IPS)
Gestion des logs
Réponse aux incidents

Intégration avec d'autres systèmes:
SIEM, SOAR
Orchestration de la sécurité

<u>Module 5 : Tendances et Perspectives</u>
Sécurité cloud:
Sécurité des applications cloud
Sécurité des données dans le cloud

Sécurité IoT:
Protection des appareils connectés

IA et machine learning en sécurité:
Détection des menaces avancées
Automatisation de la réponse aux incidents

70H CODE : NTO5

# CCNP ENTERPRISE ADVANCED ROUTING

## Objectifs

Le cours CCNP ENARSI vise à doter les professionnels de la réseau des compétences nécessaires pour :

- Configurer, optimiser et dépanner des réseaux d'entreprise complexes.
- Mettre en œuvre des technologies de routage avancées.
- Assurer la haute disponibilité et la performance des réseaux.
- Sécuriser les réseaux d'entreprise.
- Automatiser des tâches de configuration et de gestion de réseau.

Compétences clés à acquérir :

- Routage avancé: EIGRP, OSPF, BGP, ISIS
- VPN: IPsec, DMVPN, GRE
- Services de qualité de service (QoS): Classification, marquage, gestion de la congestion
- Protocoles de routage multicast: PIM, DVMRP
- Technologies de virtualisation: VXLAN, NVGRE
- Automatisation: Ansible, Python
- Sécurité: ACL, IPS, Firewall

## Débouchées

- Ingénieur réseau senior: Conception, implémentation et maintenance de réseaux d'entreprise complexes.
- Architecte réseau: Conception de solutions réseau à grande échelle.
- Spécialiste de la sécurité réseau: Mise en œuvre de mesures de sécurité pour protéger les réseaux.
- Consultant réseau: Fourniture de conseils et d'expertise aux entreprises.

### Module 1 : Fondamentaux du Routage Avancé

**EIGRP**: Concepts de base, métriques, auto-summarisation
Configuration avancée (stub areas, route summarization)
**OSPF**: Types d'areas, LSA, SPF
Configuration avancée (virtual links, OSPFv3)
**BGP**: Attributs BGP, AS path, route reflectors
Configuration de routage inter-domaine

### Module 2 : VPN et Services de Tunnel

**IPsec**: Encapsulation, modes de transport et tunnel
Configuration de VPN site-à-site
**DMVPN**: Hub and spoke, full mesh
Configuration et gestion de DMVPN
**GRE**: Encapsulation générique
Utilisation de GRE pour les tunnels VPN

### Module 3 : QoS et Multicast

**QoS**: Classification, marquage, gestion de la congestion
Configuration de QoS sur les routeurs et commutateurs
**Multicast**: PIM, DVMRP :Configuration de routage multicast

### Module 4 : Technologies de Virtualisation

**VXLAN**: Encapsulation VXLAN, VTEP
Intégration avec les réseaux physiques
**NVGRE**: Comparaison avec VXLAN
Cas d'utilisation spécifiques

### Module 5 : Automatisation et Programmation Réseau

**Ansible**: Playbooks, modules
Automatisation de tâches de configuration
**Python**: Programmation réseau avec Python
Intégration avec les API des équipements réseau

### Module 6 : Sécurité Réseau

**ACL**: Configuration d'ACL étendues et standard
**IPS**: Déploiement et configuration d'un système de prévention des intrusions
**Firewall**: Configuration de règles de pare-feu

### Module 7 : Haute Disponibilité et Redondance

HSRP, VRRP : Protocoles de routage de secours
CARP: Protocole de clustering pour les commutateurs
Clustering de routeurs: Configuration de clusters de routeurs

### Module 8 : Dépannage Avancé

Outils de dépannage:
Debug, show commands
Méthodologie de dépannage
Analyse de traces

### Module 9 : Labos Pratiques

Configuration de scénarios réseau complexes
Résolution de problèmes réels

# CISSP (Certified Information Systems Security Professional)

40H CODE : SECO3

## Certified Information Systems Security Professional)

## Objectifs

- Maîtriser les huit domaines du CBK du CISSP :
- Comprendre les concepts, les principes et les meilleures pratiques de la sécurité de l'information.
- Développer une approche holistique de la sécurité des systèmes d'information.
- Préparer efficacement l'examen de certification CISSP.

## Débouchées

- Directeur de la sécurité des systèmes d'information (DSSI/CISO).
- Responsable de la sécurité de l'information.
- Architecte de sécurité.
- Consultant en sécurité.

## Prérequis

- Expérience professionnelle significative dans le domaine de la sécurité de l'information (comme mentionné ci-dessus).
- Connaissances générales en informatique et en réseaux.

Module 1 : Sécurité et gestion des risques (Security and Risk Management)

Concepts de base de la sécurité de l'information.

Gestion des risques : identification, analyse, évaluation, traitement et surveillance.

Cadres de gestion des risques (NIST, ISO 31000).

Politiques, normes, procédures et directives de sécurité.

Lois, réglementations et conformité (RGPD, HIPAA, etc.).

Éthique professionnelle.

BCP/DRP (Business Continuity Planning/Disaster Recovery Planning).

Module 2 : Sécurité des actifs (Asset Security)

Classification des informations.

Propriété des données.

Protection de la vie privée.

Gestion du cycle de vie des informations.

Module 3 :Ingénierie de sécurité (Security Architecture and Engineering)

Principes de conception sécurisée.

Modèles de sécurité.

Architecture des systèmes de sécurité.

Sécurité des systèmes embarqués et des systèmes de contrôle industriel (ICS).

Cryptographie : concepts, algorithmes, implémentations.

Module 4 :Sécurité des communications et des réseaux (Communication and Network Security)

Modèles de réseau (OSI, TCP/IP).

Protocoles réseau et sécurité des protocoles.

Conception et implémentation de réseaux sécurisés (pare-feu, VPN, IDS/IPS).

Sécurité des réseaux sans fil.

Module 5 : Gestion des identités et des accès

Identification et authentification.

Autorisation.

Gestion du cycle de vie des identités.

Types de contrôles d'accès.

Module 6 : Évaluation et tests de sécurité (Security Assessment and Testing)

Types de tests de sécurité (tests de pénétration, analyses de vulnérabilités).

Méthodologies de test.

Outils de test de sécurité.

Audit de sécurité.

Module 7 :Opérations de sécurité (Security Operations)

Gestion des incidents de sécurité.

Gestion des changements.

Gestion des vulnérabilités.

Surveillance et journalisation de la sécurité.

Sécurité physique.

Sensibilisation et formation à la sécurité.

40H CODE : SECO3

# AWS Certified Security – Specialty

## Objectifs

- Maîtriser les concepts et les services AWS liés à la sécurité.
- Être capable de concevoir et de mettre en œuvre des solutions de sécurité robustes sur AWS.
- Comprendre les meilleures pratiques en matière de sécurité, de conformité et de gestion des risques sur AWS.
- Savoir automatiser les tâches de sécurité et répondre aux incidents de sécurité.

## Débouchées

- Ingénieur sécurité cloud.
- Architecte sécurité cloud.
- Consultant en sécurité AWS.
- Spécialiste en réponse aux incidents sur

## Prérequis

- Expérience pratique avec les services AWS (au moins 2 ans).
- Connaissances solides en sécurité informatique (réseaux, systèmes d'exploitation, cryptographie).
- Certification AWS Certified Cloud Practitioner ou AWS Certified Solu-

Module 1 : Réponse aux incidents

Planification de la réponse aux incidents.

Détection et analyse des incidents de sécurité.

Confinement, éradication et reprise après incident.

Utilisation des services AWS pour la réponse aux incidents (AWS Security Hub, Amazon GuardDuty, AWS Config, AWS CloudTrail, Amazon CloudWatch).

Automatisation de la réponse aux incidents avec AWS Lambda et AWS Systems Manager.

Module 2 :Surveillance et journalisation

Collecte et analyse des journaux (AWS CloudTrail, Amazon CloudWatch Logs, VPC Flow Logs, AWS Config).

Surveillance des métriques de sécurité (Amazon CloudWatch Metrics).

Utilisation des services de sécurité pour la surveillance (Amazon GuardDuty, AWS Security Hub, Amazon Inspector).

Création d'alertes et de tableaux de bord de sécurité.

Centralisation de la gestion des journaux avec Amazon S3 et Amazon Athena.

Module 3 :Sécurité de l'infrastructure

Sécurité des réseaux : VPC, sous-réseaux, groupes de sécurité, Network ACLs, AWS Network Firewall, AWS Transit Gateway.Sécurité des instances EC2 : durcissement des instances, gestion des accès, utilisation d'AMIs sécurisées.

Sécurité des conteneurs : ECS, EKS, Fargate, sécurité des images Docker.

Sécurité du serverless : AWS Lambda, API Gateway.

Sécurité du stockage : S3, EBS, EFS, Glacier, chiffrement des données au repos et en transit.

Module 4 : Gestion des identités et des accès (IAM)

IAM : utilisateurs, groupes, rôles, politiques, identités fédérées.

Stratégies de moindre privilège.

Gestion des clés d'accès.

AWS Organizations : gestion multi-comptes et contrôle d'accès centralisé.

AWS Single Sign-On (SSO).

Intégration avec des fournisseurs d'identité externes.

Module 5 : Protection des données

Chiffrement des données : KMS, CloudHSM, chiffrement côté client et côté serveur.

Gestion des clés de chiffrement.

Protection contre la perte de données : sauvegardes, restauration, réplication.

Conformité aux réglementations sur la protection des données (RGPD, HIPAA, etc.).Classification et étiquetage des données.AWS Data Loss Prevention

40H CODE : SECO3

# Kubernetes and Cloud Native Associate

## Objectifs

- Comprendre les concepts fondamentaux de Kubernetes et de l'architecture Cloud Native.
- Connaître les composants clés de Kubernetes et leur interaction.
- Être capable de déployer et de gérer des applications conteneurisées sur Kubernetes.
- Comprendre les principes de sécurité, de stockage et de mise en réseau dans Kubernetes.
- Se familiariser avec les outils et les bonnes pratiques de l'écosystème Cloud Native.

## Débouchées

- Développeur Cloud Native.
- Administrateur Kubernetes Junior.
- Ingénieur DevOps Junior.

## Prérequis

- Connaissances de base des systèmes d'exploitation Linux ou Windows.
- Familiarité avec la ligne de commande.
- Notions de base sur la conteneuri-

Module 1 : Introduction au Cloud Native et à Kubernetes

Les principes du Cloud Native : microservices, conteneurs, orchestration dynamique.

Présentation de Kubernetes : historique, architecture, avantages.

Comparaison entre Kubernetes et d'autres solutions d'orchestration.

Installation et configuration de kubectl (l'outil en ligne de commande de Kubernetes).

Premier contact avec le cluster Kubernetes : commandes de base (kubectl get, kubectl describe).

Module 2 : Architecture de Kubernetes

Les composants du Master Node : API Server, etcd, Scheduler, Controller Manager.

Les composants du Worker Node : kubelet, kube-proxy, Container Runtime (Docker, containerd, CRI-O).

Communication entre les composants.

Module 3 :Déploiement d'applications sur Kubernetes

Les Pods : définition, cycle de vie, gestion.

Les Deployments : déploiement et mise à jour d'applications.

Les Services : exposition des applications aux clients internes et externes.

Les Namespaces : organisation des ressources dans un cluster.

Exercices pratiques de déploiement d'applications simples.

Module 4 :Gestion des ressources et configuration Analyse des risques

Évaluation des impacts : conséConfigMaps et Secrets : gestion de la configuration et des informations sensibles.

Resource Quotas et Limit Ranges : contrôle de l'utilisation des ressources.

Liveness et Readiness Probes : surveillance de l'état des applications.

Module 5 : Stockage dans Kubernetes

Volumes : persistance des données.

Persistent Volumes et Persistent Volume Claims : abstraction du stockage.

Storage Classes : provisionnement dynamique du stockage.

Module 6 : Mise en réseau dans Kubernetes

Les Services : types de services (ClusterIP, NodePort, LoadBalancer).

Ingress : exposition des applications aux clients externes avec gestion du trafic.

CNI (Container Network Interface) : interfaces réseau pour les conteneurs.

Module 7 :Sécurité dans Kubernetes

Principes de sécurité dans Kubernetes.

RBAC (Role-Based Access Control) : contrôle d'accès basé sur les rôles.

Network Policies : isolation du réseau entre les Pods.

Security Contexts : configuration de la sécurité des conteneurs.

Module 8: Écosystème Cloud Native

Présentation des projets de la CNCF (Cloud Native Computing Foundation).

40H CODE : SECO3

# Kubernetes Certified Administrator (CKA)

## Objectifs

- Maîtriser l'installation, la configuration et la gestion d'un cluster Kubernetes.
- Comprendre en profondeur l'architecture et les composants de Kubernetes.
- Être capable de déployer, de maintenir et de dépanner des applications sur Kubernetes.
- Gérer le stockage persistant, la mise en réseau et la sécurité dans Kubernetes.
- Automatiser les tâches d'administration et mettre en œuvre les

## Débouchées

- Administrateur système Docker.
- Ingénieur DevOps.
- Développeur d'applications conteneurisées.

## Prérequis

- Connaissances de base des systèmes d'exploitation Linux ou Windows.
- Familiarité avec l'utilisation de la ligne de commande.

Module 1 : Introduction à Kubernetes et son architecture

Les concepts de l'orchestration de conteneurs.

Présentation de Kubernetes et de son écosystème.

Architecture de Kubernetes : Master Node (API Server, etcd, Scheduler, Controller Manager) et Worker Nodes (kubelet, kube-proxy, Container Runtime).

Installation et configuration d'un cluster Kubernetes avec kubeadm.

Utilisation de kubectl : configuration et commandes de base.

Module 2 :Workloads et Scheduling

Les Pods : définition, cycle de vie, multi-conteneurs, init containers.

Les Deployments : déploiement déclaratif, mises à jour (rolling updates, blue/green), rollbacks.

Les ReplicaSets : gestion du nombre de réplicas.

Les DaemonSets : déploiement de pods sur chaque nœud.

Les Jobs et CronJobs : exécution de tâches ponctuelles et planifiées.

Scheduling : planification des pods sur les nœuds, affinités, anti-affinités, taints et tolerations.

Module 3 :Services et Networking

Les Services : abstraction pour accéder aux pods (ClusterIP, NodePort, LoadBalancer, ExternalName).

DNS dans Kubernetes : CoreDNS.

Ingress : exposition des services aux clients externes, gestion du trafic (routing, TLS).

CNI (Container Network Interface) : concepts et exemples d'implémentations (Calico, Flannel).

Network Policies : isolation du trafic réseau entre les pods.

Module 4 : Stockage

Volumes : types de volumes (emptyDir, hostPath, NFS, etc.).

Persistent Volumes (PV) et Persistent Volume Claims (PVC) : provisionnement dynamique du stockage.

Storage Classes : configuration des provisionneurs de stockage.

Module 5 : Configuration et Sécurité

ConfigMaps : gestion de la configuration des applications.

Secrets : gestion des informations sensibles (mots de passe, clés, certificats).

Security Contexts : configuration de la sécurité des conteneurs (capabilities, user IDs, SELinux).

RBAC (Role-Based Access Control) : contrôle d'accès basé sur les rôles, utilisateurs, groupes, service accounts.

Gestion des certificats et TLS.

Audit logging.

Module 6 : Maintenance et Dépannage

Mise à niveau du cluster Kubernetes.

Gestion des logs et monitoring avec kubectl logs et describe.

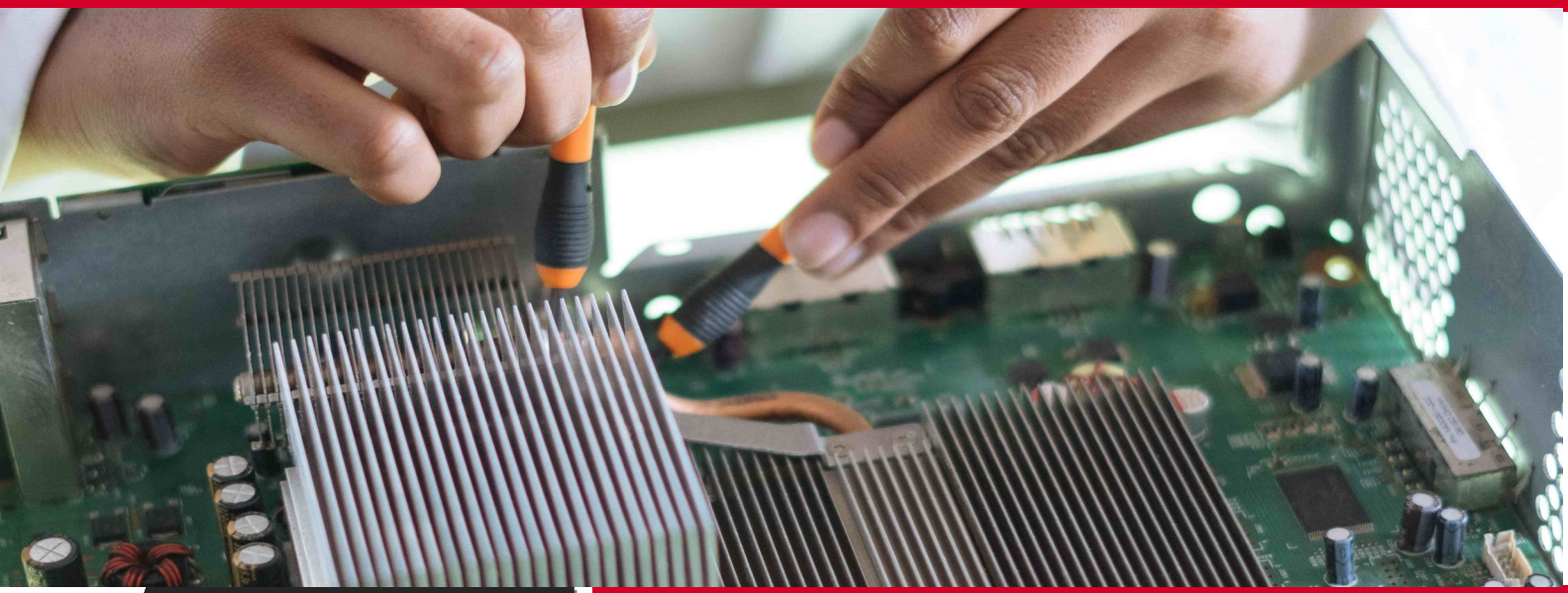
Dépannage des pods, des deployments, des services et du réseau.

Résolution des problèmes courants.

Collecte de logs et de métriques pour le débogage.

Module 7 :etcd et les opérations de cluster

Fonctionnement de etcd : base de don-



70H CODE : GOV01

# ISO 27001

## Objectifs

Comprendre les principes fondamentaux de la norme ISO 27001 et son importance pour la sécurité de l'information.

- Acquérir les connaissances nécessaires pour planifier, mettre en œuvre, maintenir et améliorer un SMSI conforme à la norme.
- Identifier et évaluer les risques liés à la sécurité de l'information.
- Mettre en place des mesures de sécurité appropriées pour protéger les informations sensibles.
- Préparer un organisme à la certification ISO

## Débouchées

- Responsable de la sécurité des systèmes d'information (RSSI) / Chief Information Security Officer (CISO)
- Auditeur interne ISO 27001
- Auditeur externe ISO 27001 (Lead Auditor)
- Consultant en sécurité de l'information

## Prérequis

Formation d'initiation (sensibilisation)

Formation d'implémentation (Lead

<u>Introduction à la sécurité de l'information et à la norme ISO 27001 :</u>

Concepts clés de la sécurité de l'information : confidentialité, intégrité, disponibilité.

Menaces et vulnérabilités des systèmes d'information.

Présentation de la norme ISO 27001 : historique, objectifs, structure.

Liens avec d'autres normes (ISO 27002, ISO 27005, ISO 22301, etc.).

Les bénéfices de la certification ISO 27001 pour une organisation.

<u>Exigences de la norme ISO 27001</u>

Analyse détaillée des exigences de la norme :

Contexte de l'organisme.

Leadership.

Planification (analyse des risques, objectifs de sécurité).

Support (ressources, compétences, sensibilisation, communication, informations documentées).

Réalisation des activités opérationnelles (maîtrise des risques).

Évaluation des performances (surveillance, mesure, analyse et évaluation, audit interne, revue de direction).

Amélioration.

Exercices pratiques d'interprétation des exigences.

<u>Analyse et traitement des risques</u>

Méthodologies d'analyse des risques (ISO 27005, EBIOS RM).

Identification des actifs informationnels.

Identification des menaces et des vulnérabilités.

Évaluation des risques (impacts et probabilités).

Options de traitement des risques : éviter, transférer, atténuer, accepter.

Mise en place des mesures de sécurité (contrôles de l'Annexe A de l'ISO 27001).

Exercices pratiques d'analyse et de traitement des risques.

<u>Mise en œuvre et maintenance d'un SMSI :</u>

Explication de l'importance de la Élaboration de la documentation du SMSI (politique de sécurité, procédures, instructions).

Mise en œuvre des mesures de sécurité.

Formation et sensibilisation du personnel.

Gestion des incidents de sécurité.

70H CODE : SECO6

# AWS CLOUD PRACTIONNER

## Objectifs

- Comprendre les concepts fondamentaux du cloud computing et son vocabulaire.
- Connaître les services AWS clés et leurs cas d'utilisation.
- Comprendre le modèle de responsabilité partagée d'AWS.
- Identifier les aspects de sécurité et de conformité dans le cloud AWS.
- Comprendre les modèles de tarification et de support AWS.
- Préparer les participants à l'examen de

## Débouchées

Chargé d'affaires cloud

Chef de projet cloud

Analyste des besoins cloud

Consultant cloud junior

## Prérequis

Une familiarité générale avec l'informatique

Module 1 : Une familiarité générale avec l'informatique

Qu'est-ce que le cloud computing ? Définition, avantages et inconvénients.

Les différents modèles de service cloud : IaaS, PaaS, SaaS.

Les modèles de déploiement cloud : public, privé, hybride.

Concepts clés : élasticité, scalabilité, haute disponibilité, tolérance aux pannes.

Introduction à AWS et son infrastructure globale.

Module 2 :Services AWS Fondamentaux

Calcul (Compute) :

Amazon EC2 (Elastic Compute Cloud) : instances, types d'instances, options d'achat.

Amazon EC2 Auto Scaling : mise à l'échelle automatique.

Elastic Load Balancing : répartition de charge.

AWS Lambda : calcul sans serveur (serverless).

Stockage (Storage) :

Amazon S3 (Simple Storage Service) : stockage d'objets.

Amazon EBS (Elastic Block Storage) : stockage de blocs pour EC2.

Amazon Glacier : stockage d'archives à faible coût.

Bases de données (Databases) :

Amazon RDS (Relational Database Service) : bases de données relationnelles.

Amazon DynamoDB : base de données NoSQL.

Réseau (Networking) :

Amazon VPC (Virtual Private Cloud) : réseau virtuel privé.

Route 53 : service DNS.

Sécurité (Security) :

AWS Identity and Access Management (IAM) : gestion des identités et des accès.

AWS Key Management Service (KMS) : gestion des clés de chiffrement.

Module 3 :Sécurité et Conformité dans AWS :

Le modèle de responsabilité partagée d'AWS.

Sécurité physique des infrastructures AWS.

Sécurité des données dans le cloud

Module 4: Tarification et Support AWS :

Les différents modèles de tarification AWS : paiement à l'utilisation, instances réservées, Savings Plans.

AWS Cost Explorer : outil d'analyse des coûts.

AWS Budgets : définition de budgets et d'alertes de coûts.

Les différents niveaux de support AWS.

AWS Marketplace : achat de logiciels et de services tiers.

Module 5 : Architecture et Conception dans le Cloud AWS

Principes d'architecture cloud : conception pour la scalabilité, la haute disponibilité et la tolérance aux pannes.

Bonnes pratiques d'architecture AWS.

Exemples d'architectures courantes.

70H CODE : SECO6

# AWS SYS OS

## Objectifs

- Maîtriser les services AWS essentiels pour les opérations système.
- Être capable de déployer, gérer et maintenir des applications sur AWS.
- Comprendre les concepts de haute disponibilité, de tolérance aux pannes et de mise à l'échelle sur AWS.
- Savoir automatiser les tâches d'administration système sur AWS.

## Débouchées

Administrateur système AWS (Cloud SysOps Administrator)

Ingénieur DevOps

Ingénieur Cloud

Spécialiste en automatisation et

## Prérequis

Expérience pratique en administration système.

Connaissances de base en réseau.

Maîtrise des outils en ligne de commande.

<u>Module 1 : Introduction aux opérations système sur AWS</u>

Concepts clés des opérations sur AWS.

Le modèle de responsabilité partagée d'AWS.

Le framework AWS Well-Architected.

Présentation des outils de gestion AWS (AWS Management Console, AWS CLI, SDKs).

<u>Module 2 :Gestion des accès et des identités</u>

AWS Identity and Access Management (IAM) : utilisateurs, groupes, rôles, politiques.

Gestion des clés d'accès.

Bonnes pratiques de sécurité IAM.

<u>Module 3 :Déploiement et gestion des instances EC2</u>

Amazon EC2 (Elastic Compute Cloud) : types d'instances, options d'achat.

Création et configuration d'instances EC2.

Gestion des volumes EBS (Elastic Block Storage).

Utilisation des Amazon Machine Images (AMIs).

Automatisation du déploiement avec AWS CloudFormation et AWS Systems Manager.

<u>Module 4 :Mise en réseau sur AWS</u>

Amazon VPC (Virtual Private Cloud) : sous-réseaux, tables de routage, passerelles.

Groupes de sécurité et listes de contrôle d'accès réseau (ACLs).

Elastic Load Balancing (ELB) : répartition de charge.

Amazon Route 53 : service DNS.

<u>Module 5 :Stockage et bases de données</u>

Amazon S3 (Simple Storage Service) : stockage d'objets, politiques de cycle de vie.

Amazon RDS (Relational Database Service) : gestion des bases de données relationnelles.

Options de sauvegarde et de restauration.

<u>Module 6 :Surveillance et journalisation</u>

Amazon CloudWatch : surveillance

Module 7: Automatisation et gestion de la configuration :

AWS Systems Manager : automatisation des tâches d'administration, gestion des correctifs.

AWS CloudFormation : Infrastructure as Code (IaC).

AWS OpsWorks : gestion des applications et des serveurs.

Module 8 : Haute disponibilité et reprise après sinistre

Concepts de haute disponibilité et de tolérance aux pannes.

Utilisation des Availability Zones et des régions AWS.

Stratégies de sauvegarde et de restauration.

AWS Disaster Recovery.

40H CODE : SECO3

# ISO 27005

## Objectifs

- Comprendre les concepts fondamentaux de la gestion des risques de sécurité de l'information selon la norme ISO 27005.
- Maîtriser les étapes du processus de gestion des risques : contexte, identification, analyse, évaluation, traitement, acceptation et communication.
- Être capable de mettre en œuvre une méthodologie d'analyse des risques adaptée à son organisation.
- Savoir identifier et évaluer les actifs informationnels, les menaces et les vulnérabilités.
- Déterminer les mesures de sécurité appropriées pour traiter les risques identifiés.

## Débouchées

- Analyste des risques SSI
- Consultant en gestion des risques SSI
- Responsable de la sécurité des systèmes d'information (RSSI)

## Prérequis

- Connaissances de base en sécurité de l'information.
- Familiarité avec la norme ISO

Module 1 : Module 1 : Introduction à la gestion des risques et à ISO 27005

Concepts clés de la gestion des risques : risque, menace, vulnérabilité, impact, probabilité.

Présentation de la norme ISO 27005 : historique, objectifs, structure, liens avec ISO 27001.

Importance de la gestion des risques pour la sécurité de l'information.

Les bénéfices d'une approche structurée de la gestion des risques.

Module 2 : Contexte et établissement des critères

Définir le contexte de la gestion des risques : objectifs, périmètre, parties prenantes.

Établir les critères d'acceptation des risques : niveaux de risque acceptables, échelles d'impact et de probabilité.

Définir les rôles et les responsabilités dans le processus de gestion des risques.

Module 3 : Identification des risques

Identification des actifs informationnels : données, logiciels, matériels, services, personnes.

Identification des menaces : sources de danger potentielles.

Identification des vulnérabilités : faiblesses exploitables par les menaces.

Techniques d'identification des risques : brainstorming, questionnaires, analyses de vulnérabilités, revues de documents.

Exercices pratiques d'identification des actifs, des menaces et des vulnérabilités

Module 4 : Analyse des risques

Évaluation des impacts : conséquences potentielles de la réalisation d'un risque.

Évaluation des probabilités : chance qu'une menace exploite une vulnérabilité.

Méthodes d'analyse des risques : qualitative, quantitative, semi-quantitative.

Utilisation de matrices de risques.

Exercices pratiques d'analyse des risques et de calcul des niveaux de risque.

Module 5 : Traitement des risques

Options de traitement des risques : éviter, transférer, atténuer, accepter.

Sélection des mesures de sécurité appropriées : contrôles techniques, organisationnels et physiques.

Élaboration d'un plan de traitement des risques.

40H CODE : SECO3

# DOCKER DCA

## Objectifs

- Comprendre les concepts fondamentaux de Docker et de la conteneurisation.
- Maîtriser l'installation, la configuration et l'utilisation de Docker Engine.
- Savoir créer, gérer et optimiser des images Docker.
- Comprendre le fonctionnement des réseaux et du stockage avec Docker.
- Être capable de déployer et d'orchestrer des applications conteneurisées avec Docker Swarm.
- Connaître les bonnes pratiques

## Débouchées

- Administrateur système Docker.
- Ingénieur DevOps.
- Développeur d'applications conteneurisées.

## Prérequis

- Connaissances de base des systèmes d'exploitation Linux ou Windows.
- Familiarité avec l'utilisation de la ligne de commande.

<u>Module 1 : Introduction à la conteneurisation et à Docker</u>

Les concepts de la conteneurisation : avantages par rapport à la virtualisation traditionnelle.

Présentation de Docker : historique, architecture, composants clés (Docker Engine, Docker Client, Docker Registry).

Installation et configuration de Docker Engine sur Linux et Windows.

Les commandes Docker de base : docker run, docker ps, docker stop, docker rm.

Premier contact avec les images et les conteneurs.

<u>Module 2 : Contexte et établissement des critères</u>

Les Dockerfiles : structure, instructions (FROM, RUN, COPY, CMD, ENTRYPOINT, etc.).

Création d'images Docker personnalisées.

Optimisation de la taille des images (multi-stage builds, .dockerignore).

Gestion des tags et des versions d'images.

Utilisation des registres Docker : Docker Hub, registres privés.

Les commandes **docker build, docker images, docker push, docker pull, docker rmi.**

<u>Module 3 :Gestion des conteneurs</u>

<u>Cycle de vie d'un conteneur.</u>

Configuration des conteneurs : variables d'environnement, ports, volumes.

Gestion des logs et du débogage des conteneurs.

Les commandes docker exec, docker logs, docker inspect, docker stats.

Utilisation de Docker Compose pour gérer des applications multi-conteneurs

<u>Module 4 : Réseaux Docker</u>

Les différents types de réseaux Docker : bridge, host, overlay, macvlan.

Configuration des réseaux Docker.

Communication entre les conteneurs.

Publication des ports des conteneurs.

Résolution de noms avec Docker.

<u>Module 5 : Stockage avec Docker</u>

Les différents types de stockage avec Docker : volumes, bind mounts, tmpfs mounts.

Gestion des volumes Docker.

Persistance des données.

Choix de la stratégie de stockage appropriée.

<u>Module 6 : Orchestration avec Docker Swarm</u>

Introduction à l'orchestration de conteneurs.

Création et gestion d'un cluster Swarm : managers et workers.

Déploiement de services sur Swarm.

Mise à l'échelle des services.

Gestion des mises à jour des services (rolling updates).

Gestion des secrets et des configurations avec Swarm.

Les commandes docker swarm, docker service, docker stack.

<u>Module 7 :Sécurité avec Docker</u>

Bonnes pratiques de sécurité pour les images Docker.

40H CODE : SECO3

# Kubernetes and Cloud Native Associate

## Objectifs

- Comprendre les concepts fondamentaux de Kubernetes et de l'architecture Cloud Native.
- Connaître les composants clés de Kubernetes et leur interaction.
- Être capable de déployer et de gérer des applications conteneurisées sur Kubernetes.
- Comprendre les principes de sécurité, de stockage et de mise en réseau dans Kubernetes.
- Se familiariser avec les outils et les bonnes pratiques de l'écosystème Cloud Native.

## Débouchées

- Développeur Cloud Native.
- Administrateur Kubernetes Junior.
- Ingénieur DevOps Junior.

## Prérequis

- Connaissances de base des systèmes d'exploitation Linux ou Windows.
- Familiarité avec la ligne de commande.
- Notions de base sur la conteneuri-

Module 1 : Introduction au Cloud Native et à Kubernetes

Les principes du Cloud Native : microservices, conteneurs, orchestration dynamique.

Présentation de Kubernetes : historique, architecture, avantages.

Comparaison entre Kubernetes et d'autres solutions d'orchestration.

Installation et configuration de kubectl (l'outil en ligne de commande de Kubernetes).

Premier contact avec le cluster Kubernetes : commandes de base (kubectl get, kubectl describe).

Module 2 : Architecture de Kubernetes

Les composants du Master Node : API Server, etcd, Scheduler, Controller Manager.

Les composants du Worker Node : kubelet, kube-proxy, Container Runtime (Docker, containerd, CRI-O).

Communication entre les composants.

Module 3 :Déploiement d'applications sur Kubernetes

Les Pods : définition, cycle de vie, gestion.

Les Deployments : déploiement et mise à jour d'applications.

Les Services : exposition des applications aux clients internes et externes.

Les Namespaces : organisation des ressources dans un cluster.

Exercices pratiques de déploiement d'applications simples.

Module 4 :Gestion des ressources et configuration Analyse des risques

Évaluation des impacts : conséConfig-Maps et Secrets : gestion de la configuration et des informations sensibles.

Resource Quotas et Limit Ranges : contrôle de l'utilisation des ressources.

Liveness et Readiness Probes : surveillance de l'état des applications.

Module 5 : Stockage dans Kubernetes

Volumes : persistance des données.

Persistent Volumes et Persistent Volume Claims : abstraction du stockage.

Storage Classes : provisionnement dynamique du stockage.

Module 6 : Mise en réseau dans Kubernetes

Les Services : types de services (ClusterIP, NodePort, LoadBalancer).

Ingress : exposition des applications aux clients externes avec gestion du trafic.

CNI (Container Network Interface) : interfaces réseau pour les conteneurs.

Module 7 :Sécurité dans Kubernetes

Principes de sécurité dans Kubernetes.

RBAC (Role-Based Access Control) : contrôle d'accès basé sur les rôles.

Network Policies : isolation du réseau entre les Pods.

Security Contexts : configuration de la sécurité des conteneurs.

Module 8: Écosystème Cloud Native

Présentation des projets de la CNCF (Cloud Native Computing Foundation).

40H CODE : SECO3

# Kubernetes Certified Administrator (CKA)

## Objectifs

- Maîtriser l'installation, la configuration et la gestion d'un cluster Kubernetes.
- Comprendre en profondeur l'architecture et les composants de Kubernetes.
- Être capable de déployer, de maintenir et de dépanner des applications sur Kubernetes.
- Gérer le stockage persistant, la mise en réseau et la sécurité dans Kubernetes.
- Automatiser les tâches d'administration et mettre en œuvre les

## Débouchées

- Administrateur système Docker.
- Ingénieur DevOps.
- Développeur d'applications conteneurisées.

## Prérequis

- Connaissances de base des systèmes d'exploitation Linux ou Windows.
- Familiarité avec l'utilisation de la ligne de commande.

Module 1 : Introduction à Kubernetes et son architecture

Les concepts de l'orchestration de conteneurs.

Présentation de Kubernetes et de son écosystème.

Architecture de Kubernetes : Master Node (API Server, etcd, Scheduler, Controller Manager) et Worker Nodes (kubelet, kube-proxy, Container Runtime).

Installation et configuration d'un cluster Kubernetes avec kubeadm.

Utilisation de kubectl : configuration et commandes de base.

Module 2 :Workloads et Scheduling

Les Pods : définition, cycle de vie, multi-conteneurs, init containers.

Les Deployments : déploiement déclaratif, mises à jour (rolling updates, blue/green), rollbacks.

Les ReplicaSets : gestion du nombre de réplicas.

Les DaemonSets : déploiement de pods sur chaque nœud.

Les Jobs et CronJobs : exécution de tâches ponctuelles et planifiées.

Scheduling : planification des pods sur les nœuds, affinités, anti-affinités, taints et tolerations.

Module 3 :Services et Networking

Les Services : abstraction pour accéder aux pods (ClusterIP, NodePort, LoadBalancer, ExternalName).

DNS dans Kubernetes : CoreDNS.

Ingress : exposition des services aux clients externes, gestion du trafic (routing, TLS).

CNI (Container Network Interface) : concepts et exemples d'implémentations (Calico, Flannel).

Network Policies : isolation du trafic réseau entre les pods.

Module 4 : Stockage

Volumes : types de volumes (emptyDir, hostPath, NFS, etc.).

Persistent Volumes (PV) et Persistent Volume Claims (PVC) : provisionnement dynamique du stockage.

Storage Classes : configuration des provisionneurs de stockage.

Module 5 : Configuration et Sécurité

ConfigMaps : gestion de la configuration des applications.

Secrets : gestion des informations sensibles (mots de passe, clés, certificats).

Security Contexts : configuration de la sécurité des conteneurs (capabilities, user IDs, SELinux).

RBAC (Role-Based Access Control) : contrôle d'accès basé sur les rôles, utilisateurs, groupes, service accounts.

Gestion des certificats et TLS.

Audit logging.

Module 6 : Maintenance et Dépannage

Mise à niveau du cluster Kubernetes.

Gestion des logs et monitoring avec kubectl logs et describe.

Dépannage des pods, des deployments, des services et du réseau.

Résolution des problèmes courants.

Collecte de logs et de métriques pour le débogage.

Module 7 :etcd et les opérations de cluster

Fonctionnement de etcd : base de don-

# Nos partenaires technologiques

NDG

cisco

aruba

RHOPEN LABS

Microsoft

# Ils nous font confiance

neeco
LOBAL ICT SERVICE

KONICA MINOLTA

ASTON ECOLE IT BY SQLI

E.S.I.C
Ecole Supérieure d'Informatique et de Commerce

m2i Formation

MOLIGE CAMEROUN
Industrie de fabrication des Produits Agroalimentaires

# Où Nous trouver

**CAMEROUN**

Akwa 34 rue Boue lapeyrère ,
face hôtel planet

Tel : +237 670 556 187
+237 697 925 426
+237 656 019 902

**CONGO BRAZAVILLE**

Diata derrière le
stade Aphonse
Massamba Debat

Tel : +242 06 923 74 03

**CANADA**

102 Rue de Touraine, Lévis,
QC, G6J 2A8

Tel : +1 (581) 308-8186

**FRANCE**

30 Rue de Liège
75008 Paris, France
RCS Paris

Tel : +33(0) 920 303 773