Cisco CCNP : maîtrisez les réseaux d'entreprise Cisco (ENCOR 350-401)

Date et durée

Code formation : ENCOR
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec préparation à la certification

CCNP Enterprise®

Description

Cette formation de préparation constitue le socle commun du programme de certification Cisco Enterprise. En effet, elle est l'un des **prérequis pour devenir CCNP Enterprise** ou encore CCIE Enterprise. Ainsi, vous développerez des compétences et maîtriserez les technologies réseaux Cisco nécessaires pour configurer, dépanner et gérer des réseaux dans un environnement professionnel.
Durant ces 5 jours, vous apprendrez aussi à **mettre en œuvre les principes de sécurité au sein d'un réseau d'entreprise** et à superposer la conception du réseau en utilisant des solutions telles que SD-Access et SD-WAN. L'automatisation, les protocoles réseaux, l'utilisation d'API, le dépannage et la programmabilité des réseaux d'entreprise sont également abordés.
Chaque module comprend des travaux pratiques et des supports pédagogiques en ligne. Ainsi, vous serez parfaitement **préparé pour passer l'examen de certification (ENCOR 350-401)** et devenir un Cisco Certified Specialist - Enterprise Core.

Objectifs

En suivant la **formation Cisco Enterprise ENCOR**, vous validerez les objectifs de compétence suivants :

- connaître et appliquer les procédures de configuration des réseaux filaires et sans fil d'une entreprise ;
- diagnostiquer et résoudre tout problème lié à la connexion d'un réseau câblé ou sans fil ;
- assimiler et mettre en œuvre les bonnes pratiques de sécurité au sein d'un réseau d'entreprise ;
- être bien préparé à l'examen Cisco 350-401 ENCOR afin d'obtenir la certification Cisco CCNP Enterprise.

Points forts

Un formateur expert et certifié Cisco, des support de cours officiel avec des labs et une préparation à l'examen Cisco ENCOR 350-401.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre la **formation Cisco Enterprise ENCOR** nécessite les prérequis suivants :

- savoir implémenter des réseaux locaux d’entreprise ;
- connaitre les bases de la programmation Python ;
- maîtriser les bases du routage et de la connectivité en entreprise.

Public

Cette formation s'adresse aux publics suivants :

- les ingénieurs réseau de niveau intermédiaire, les administrateurs de réseau, les techniciens support réseau ou les agents chargés de l'assistance technique (help desk).

Cette formation s'adresse aux profils suivants

Administrateur réseaux - télécoms
Ingénieur réseaux - télécoms
Technicien Support / HelpDesk

Programme

Domaine 1 : l'architecture réseau Cisco

- Les méthodes de conception utilisés pour un réseau d'entreprise :
  - conception du réseau d'entreprise (planification de la capacité des couches 2 et 3 et du maillage) ;
  - mise en place des techniques de haute disponibilité (redondance, FHRP, SSO, etc.).
- Les modèles de conception pour le déploiement d'un réseau local sans fil (WLAN) :
  - mise en place de modèles de déploiement sans fil (centralisé, distribué, sans contrôleur, basé sur un contrôleur, dans le cloud et dans une installation distante) ;
  - utilisation des services de localisation dans la conception d'un WLAN.
- Comparaison entre le déploiement d'une infrastructure sur site et le déploiement d'une infrastructure dans le cloud.
- Les principes de fonctionnement du SD-WAN de Cisco :
  - élaboration des éléments de contrôle et des plans de données du SD-WAN ;
  - comparaison entre les solutions WAN traditionnelles et les solutions SD-WAN.
- Les principes de fonctionnement du SD-Access de Cisco :
  - élaboration des éléments de contrôle et des plans de données de SD-Access ;
  - interopération des réseaux de distribution traditionnels avec SD-Access.
- Les concepts de qualité de service (QoS) pour les réseaux câblés et sans fil :
  - revue des composants de la qualité de service ;
  - mise en place d'une politique de qualité de service.
- Les mécanismes de commutateurs matériels et logiciels :
  - compréhension des processus et de la fonction CEC ;
  - compréhension des tables d'adresses MAC et TCAM ;
  - comparaison entre le FIB et le RIB.

Domaine 2 : la virtualisation

- Les technologies de virtualisation des périphériques :
  - utilisation des hyperviseurs de type 1 et 2 ;
  - utilisation des machines virtuelles ;
  - utilisation des commutateurs virtuels.
- Paramétrage et contrôle des technologies de virtualisation pour les chemins de données (DRV, tunnels GRE et IPsec).
- Les éléments de virtualisation du réseau :

- utilisation du protocole LISP ;
- utilisation du protocole de tunnelisation VXLAN.

Domaine 3 : les infrastructures

- La couche 2 :
  - résolution des problèmes liés aux protocoles 802.1 statiques et dynamiques ;
  - résolution des problèmes liés aux canaux Ethernet statiques et dynamiques ;
  - configuration et vérification des protocoles Spanning Tree communs (RSTP et MST).
- La couche 3 :
  - comparaison des systèmes de routage EIGRP et OSPF (vecteur de distance avancé vs. état lié, équilibrage de charge, sélection de chemin, opérations de chemin et mesures) ;
  - configuration et vérification d'environnements OSPF simples, y compris les zones standards multiples, le résumé et le filtrage ;
  - configuration et vérification de l'eBGP entre voisins directement connectés (algorithme de sélection du meilleur chemin et relations de voisinage).
- La transmission sans fil :
  - description des concepts de la couche 1, y compris la puissance RF, RSSI, SNR, le bruit d'interférence, la bande et les canaux, ainsi que les capacités des dispositifs clients sans fil ;
  - description des modes AP et des types d'antennes ;
  - description de la découverte des points d'accès et du processus de jonction (algorithmes de découverte et processus de sélection du WLC) ;
  - description des principes fondamentaux et des cas d'utilisation de l'itinérance des couches 2 et 3 ;
  - résolution des problèmes de configuration du réseau local sans fil et de connectivité des clients sans fil.
- Les services IP :
  - description du protocole NTP (Network Time Protocol) ;
  - configuration et vérification de NAT/PAT ;
  - configuration des protocoles de redondance de premier saut, tels que HSRP et VRRP ;
  - description des protocoles de multidiffusion, tels que PIM et IGMP v2/v3.

Domaine 4 : l'assurance réseau

- Détection des problèmes de réseau à l'aide d'outils comme les débogages, le traçage de route, le ping, le SNMP et le protocole syslog.
- Configuration et vérification de la surveillance des périphériques avec syslog pour la journalisation à distance.
- Configuration et vérification de NetFlow et Flexible NetFlow.
- Configuration et vérification de SPAN/RSPAN/ERSPAN.
- Configuration et vérification de la fonction IPSLA.
- Description des flux de travail du Centre DNA de Cisco pour mettre en œuvre la configuration, la surveillance et la gestion du réseau.
- Configuration et vérification de NETCONF et RESTCONF.

Domaine 5 : la sécurité

- Le contrôle d'accès des périphériques :
  - protection des lignes et des mots de passe ;
  - authentification et autorisation à l'aide de la méthode AAA.
- Les fonctions de sécurité de l'infrastructure :
  - configuration des listes de contrôle d'accès (ACL) ;
  - utilisation du protocole CoPP.
- Description de la sécurité de l'API REST.
- Les fonctions de sécurité sans fil ;

    - configuration du protocole EAP ;
    - configuration du protocole WebAuth ;
    - configuration de authentification par mot de passe (PSK).
- Les composants nécessaires à la conception de la sécurité du réseau :
    - mise en place d'une protection contre les menaces ;
    - mise en place de la sécurité des points d'extrémité ;
    - mise en place du pare-feu de nouvelle génération ;
    - mise en place des architectures TrustSec et MACsec ;
    - vérification du contrôle d'accès au réseau avec 802.1X, MAB et WebAuth.

Domaine 6 : l'automatisation

- Exécution de composants et de scripts Python standard.
- Création d'un fichier JSON conforme aux exigences de la norme.
- Description des principes de haut niveau et des avantages d'un langage de modélisation des données, comme le langage YANG.
- Description des API pour Cisco DNA Center et vManage.
- Interprétation des codes de réponse de l'API REST et des résultats dans la charge utile à l'aide du Cisco DNA Center et de RESTCONF.
- Création d'une Applet EEM pour automatiser la configuration, le dépannage ou la collecte de données
- Comparaison des outils de gestion des agents et des outils de gestion sans agent, tels que Chef, Puppet, Ansible et SaltStack.