Designing and Implementing Cloud Connectivity (ENCC)

ID ENCC **Prix** CHF 4 500,– (Hors Taxe) **Durée** 4 jours

A qui s'adresse cette formation

- Architectes Cloud
- Administrateurs Cloud
- Ingénieurs Cloud
- Ingénieurs réseau Cloud
- Ingénieurs en automatisation Cloud
- Ingénieurs systèmes Cloud
- Analystes en sécurité
- Gestionnaires de sécurité Cloud
- Consultants Cloud
- Développeurs d'applications Cloud
- Ingénieurs systèmes
- Architectes de solutions techniques

Cette formation prépare à la/aux certifications

Cisco Certified Network Professional Enterprise (CCNP ENTERPRISE)

Pré-requis

Les connaissances et compétences que vous devez avoir avant de suivre cette formation sont :

- Compréhension de base du routage d'entreprise
- Compréhension de base des réseaux WAN
- Compréhension de base de la technologie VPN
- Compréhension de base de Cisco Catalyst SD-WAN
- Compréhension de base des services Cloud publics

Ces compétences peuvent être acquises en suivant ces formations Cisco :

- Implementing and Administering Cisco Solutions (CCNA)
- Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
- Cisco SDWAN Fundamentals (SDWFND)
- Implementing Cisco SD-WAN Security and Cloud Solutions (SDWSCS)

Objectifs

- Décrire les composants et concepts fondamentaux de l'informatique en cloud, y compris les modèles de déploiement, les services cloud et les fournisseurs cloud, afin de fournir aux apprenants une vue d'ensemble complète du sujet
- Décrire les options disponibles pour établir la connectivité aux services cloud publics, y compris les VPN IPsec point à point et diverses options de déploiement Cisco Catalyst SD-WAN Cloud OnRamp
- Expliquer les similitudes et les différences de l'architecture de connectivité aux services cloud publics entre différents fournisseurs de services cloud et explorer les options de connectivité disponibles vers le cloud public à partir d'un environnement Cisco Catalyst SD-WAN
- Décrire les options de connectivité privée à l'infrastructure des fournisseurs de cloud publics
- Décrire les connexions directes aux différents fournisseurs de cloud publics pour l'appairage privé
- Décrire les solutions de connectivité telles que la colocation, l'échange de cloud et les fournisseurs d'interconnexion de cloud définie par logiciel pour la connexion à l'infrastructure de cloud public
- Décrire les options disponibles pour la connectivité aux applications SaaS à partir des locaux d'une organisation géographiquement distribuée
- Expliquer l'émergence du DIA pour optimiser les performances des applications cloud et l'expérience utilisateur
- Décrire les prérequis commerciaux et techniques essentiels pour atteindre une haute disponibilité, résilience et évolutivité au sein d'une solution de réseau de connectivité cloud d'entreprise
- Décrire la sécurité native d'AWS, Azure et GCP
- Décrire les exigences de conformité PCI DSS, FedRAMP et HIPAA et leur rôle dans l'intégration du cloud public
- Mettre en œuvre la connectivité sous-jacente (basée sur Internet) pour se connecter au cloud public
- Configurer des tunnels superposés sur le transport public vers une passerelle native du cloud dans AWS, Azure et GCP et vers un routeur Cisco IOS XE hébergé dans le cloud
- Déployer une instance de routeur basée sur Cisco IOS XE hébergée dans le cloud et personnaliser la configuration réseau cloud
- Configurer le routage OSPF et BGP pour un réseau d'entreprise typique
- Explorer Cisco Umbrella SIG
- Introduire l'architecture de la politique Cisco vManage et

les politiques de données centralisées
- Expliquer les composants et la mise en œuvre de la politique AAR
- Comprendre les catégories de trafic et les zones de service de Microsoft 365
- Décrire la fonctionnalité AppQoE
- Décrire les considérations de déploiement de DRE
- Décrire comment diagnostiquer et dépanner les problèmes courants de connectivité aux environnements cloud publics utilisant la connectivité basée sur Internet
- Introduire le protocole de routage BGP utilisé pour établir la connectivité entre les appareils sur site et les appareils cloud publics via différentes options de connexion
- Discuter des problèmes d'appairage et de connectivité BGP avec Microsoft Azure et explorer divers outils et techniques de dépannage et de test
- Discuter de certains problèmes courants de configuration, de mise en réseau et de routage rencontrés sur les appareils de périphérie des clients lors de la connexion à Microsoft Azure ExpressRoute

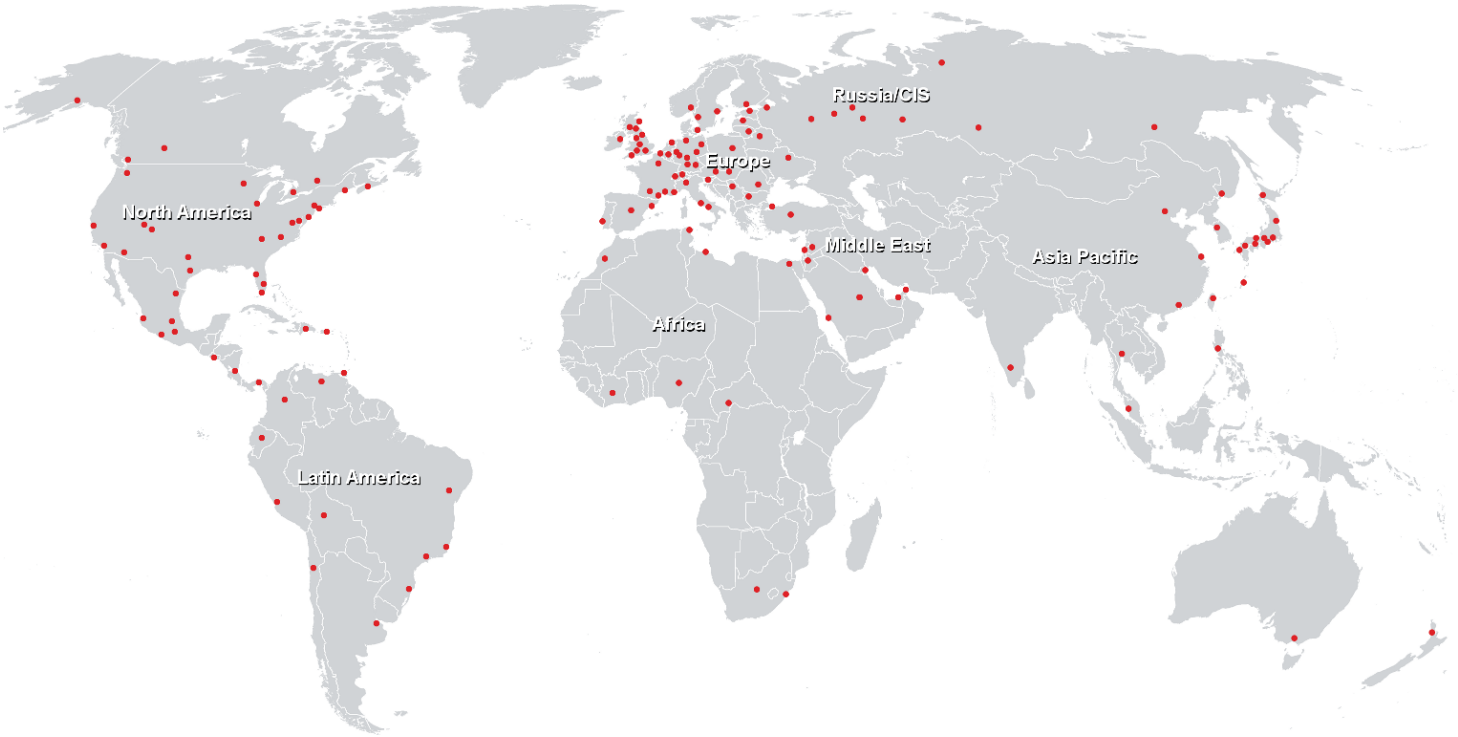
Contenu

- Fondamentaux du cloud public
- Connectivité basée sur Internet vers le cloud public
- Connectivité privée vers le cloud public
- Connectivité SaaS
- Connectivité cloud public résiliente et évolutive
- Politiques de sécurité natives du cloud
- Exigences de conformité réglementaire
- Connectivité cloud public basée sur Internet
- Déploiement du routage superposé
- Connectivité cloud basée sur Internet avec Cisco SD-WAN
- Sécurité du cloud Cisco SD-WAN
- Cloud OnRamp pour SaaS
- Politiques Cisco SD-WAN
- Qualité d'expérience des applications
- Diagnostics de connectivité cloud public basée sur Internet
- Diagnostics du routage superposé
- Diagnostics de la connectivité cloud public avec Cisco SD-WAN

Labs

- Exploration initiale du réseau de laboratoire
- Mettre en œuvre la connectivité IPsec vers les passerelles de cloud public
- Mettre en œuvre la connectivité IPsec vers les routeurs Cisco IOS-XE hébergés dans le cloud
- Mettre en œuvre le routage superposé
- Déployer Cloud OnRamp pour Multicloud
- Déployer la sécurité cloud Umbrella
- Mettre en œuvre Cloud OnRamp pour SaaS
- Dépanner la connectivité sous-jacente
- Dépanner le routage superposé
- Diagnostiquer Cloud OnRamp pour Multicloud

Centres de formation dans le monde entier





Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, https://www.flane.ch