Google Cloud Platform - Réseau

Découvrez les options d'infrastructure et de mise en réseau disponibles dans Google Cloud Platform

A distance

21 h | Prix inter : 2.650,00 € HT | Réf.: CC411

Cette formation de trois jours offre aux participants une vue approfondie des différentes options de mise en réseau disponibles sur Google Cloud Platform. Grâce à des présentations, des démonstrations et des travaux pratiques, les participants explorent et déploient les technologies de mise en réseau de Google Cloud.Ces technologies comprennent : les réseaux, sous-réseaux et pare-feu de cloud privé virtuel (VPC) ; l'interconnexion entre réseaux ; l'équilibrage de charge ; le DNS cloud ; le CDN cloud ; le NAT cloud. Le cours couvre également les modèles de conception de réseau courants.
Cette formation prépare aux certifications Google Professional Cloud Security Engineer et Google Professional Cloud Network Engineer.

A qui s'adresse cette formation ?

Pour qui

- Ingénieurs et administrateurs réseau qui utilisent Google Cloud Platform ou envisagent de le faire
- Toute personne intéressée par les solutions de mise en réseau définies par logiciel dans le cloud

Prérequis

- Avoir suivi la formation "Architecture Google Compute Engine - Infrastructure" (CC400) ou disposer des compétences équivalentes
- Connaissance et expérience pratique de GCP et du cloud computing
- Connaissance du modèle OSI à 7 couches, de l'adressage et du routage IPv4

Programme

1 - Principes de base de la mise en réseau VPC Google Cloud

- Créer une machine virtuelle Compute Engine avec plusieurs interfaces réseau
- Utiliser le niveau standard pour réduire les coûts de mise en réseau cloud
- Utiliser le niveau premium pour offrir une latence plus faible et un accès plus rapide aux ressources Google Cloud.

2 - Partage de réseaux VPC

- Décrire les différentes manières de partager des réseaux VPC disponibles dans Google Cloud
- Identifier quand utiliser un VPC partagé et quand utiliser l'appairage de réseaux VPC
- Configurer l'appairage entre des réseaux VPC non liés.

3 - Surveillance et journalisation du réseau

- Configurer des contrôles de disponibilité, des stratégies d'alerte et des graphiques pour vos services réseau
- Surveiller les ressources réseau de Google Cloud
- Utiliser VPC Flow Logs pour consigner et analyser le comportement du trafic réseau.

4 - Routage et adressage réseau dans Google Cloud

- Définir les principaux concepts de routage et d'adressage pertinents pour Google Cloud, notamment les adresses IP, les sous-réseaux, les tables de routage, les pare-feu, BYOIP et les NAT
- Décrire les options de configuration et de gestion pour Google Cloud DNS, y compris les zones privées et gérées
- Configurer et gérer les tables de routage pour contrôler le flux de trafic, résoudre efficacement les noms de domaine et utiliser les règles NAT pour un accès sécurisé.

5 - Options de connexion privée

- Définir et différencier différentes options de connexion privée (par exemple, Private Google Access, Private Services Access, Private Service Connect)
- Explorer les cas d'utilisation de Private Service Connect, Private Service Access et Private Google Access
- Mettre en oeuvre Private Google Access avec Cloud NAT.

6 - Introduction à l'architecture réseau

- Décrire les composants fournis par Google Cloud qui créent une bonne architecture réseau, tels que Cloud Interconnect, VPC Network Peering, Shared VPC et Network Tiers
- Résumer les considérations clés pour la conception du réseau.

7 - Topologies de réseau

- Expliquer quand utiliser chaque topologie de réseau en fonction d'exigences spécifiques
- Identifier les goulots d'étranglement potentiels ou les vulnérabilités de sécurité dans les topologies de réseau.
- Implémenter une topologie maillée pour une architecture réseau résiliente et évolutive.

8 - Protection contre les attaques par déni de service distribué (DDoS)

- Identifier les quatre couches d'atténuation des attaques DDoS.
- Identifier les méthodes utilisées par Google Cloud pour atténuer le risque d'attaque DDoS pour ses clients.
- Utiliser Google Cloud Armor pour bloquer une adresse IP et restreindre l'accès à un équilibreur de charge d'application externe global.

9 - Contrôle de l'accès aux réseaux VPC

- Décrire comment les stratégies IAM affectent l'accès au réseau VPC.
- Identifier les avantages de l'utilisation des stratégies hiérarchiques de Cloud Firewall à différents niveaux de la hiérarchie de l'infrastructure cloud.
- Appliquer des stratégies de pare-feu réseau globales et régionales à l'aide de Cloud Firewall.
- Expliquer le rôle de Cloud IDS dans la protection des réseaux VPC contre les activités malveillantes.
- Déployer Cloud IDS et configurer ses paramètres en fonction des besoins de sécurité spécifiques.
- Décrire le rôle de Secure Web Proxy dans l'amélioration de la résilience et de la disponibilité du réseau.
- Décrire les meilleures pratiques en matière de sécurité du réseau cloud.

10 - Advanced Security Monitoring and Analysis

- Définir Packet Mirroring et expliquer son objectif dans la surveillance et la sécurité du réseau.
- Apprendre les meilleures pratiques en matière de sécurité réseau

11 - Équilibrage de charge hybride et gestion du trafic

- Décrire les avantages de l'équilibrage de charge hybride
- Configurer la gestion du trafic dans un équilibrage de charge

12 - Mise en cache et optimisation de l'équilibrage de charge

- Décrire comment configurer un équilibreur de charge réseau interne en tant que saut suivant.
- Utiliser la configuration Cloud CDN pour optimiser les performances de diffusion de contenu.
- Créer une politique de sécurité périphérique Google Cloud Armor pour protéger le contenu.

13 - Options de connectivité

- Décrire les différentes options de connectivité proposées par Google Cloud pour les environnements hybrides et multicloud, notamment Network Connectivity Center, Cloud VPN, Cloud Interconnect et Cloud CDN.
- Définir et différencier les différentes options d'interconnexion cloud disponibles dans Google Cloud, notamment l'interconnexion dédiée, l'interconnexion partenaire et l'interconnexion cross-cloud.

14 - Cloud VPN

- Mettre en oeuvre un VPN haute disponibilité (VPN HA) pour la redondance et le basculement
- Identifier les avantages et les cas d'utilisation du VPN HA dans le cloud

Les objectifs de la formation

- Configurer les réseaux, sous-réseaux et routeurs VPC
- Contrôler l’accès administratif aux objets VPC
- Contrôler l’accès réseau aux points de terminaison dans les VPC
- Interconnecter les réseaux entre les projets Google Cloud
- Mettre en oeuvre la connectivité réseau entre les projets Google Cloud
- Mettre en oeuvre l’équilibrage de charge
- Configurer la gestion du trafic entre les services back-end d’équilibrage de charge
- Utiliser Cloud CDN pour réduire la latence
- Optimiser les dépenses réseau à l’aide des niveaux de service réseau
- Configurer les options de connexion privée pour fournir l’accès aux ressources et services externes à partir des réseaux internes.

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- Cette formation de 2 jours offre aux participants une vue approfondie des différentes options de mise en réseau disponibles sur Google Cloud Platform.
- Une formation complète durant laquelle s'alternent les phases d'apports théoriques et d'échanges.
- Les consultants spécialistes de la technologie apportent leurs conseils et leur expérience.
- Une formation animée par un formateur certifié Google Cloud Platform.
- La qualité d'une formation officielle Google (support de cours en anglais).

Dates 2026 - Référence CC411

Dernières places disponibles Session garantie

du 11 févr. au 13 févr.	du 17 juin au 19 juin	du 14 oct. au 16 oct.
du 15 avr. au 17 avr.	du 12 août au 14 août	du 9 déc. au 11 déc.