

Examen National de Fin De Formation
Session de Juin 2025

Examen de Fin de Formation (Epreuve Synthèse)

Eléments de correction

| | | | |
|------------------|---|-----------------|------------------------------|
| Secteur : | Digital et Intelligence Artificielle | Niveau : | Technicien Spécialisé |
| Filière : | Infrastructure digitale - Option : Cloud Computing | | |
| Variante | 1 | Durée : | 4h00 |
| | | Barème | /100 |

Consignes et Précisions aux correcteurs :

Veuillez respecter impérativement les consignes suivantes :

- Les éléments de correction sont élaborés à titre indicatif,
- Eviter de sanctionner doublement le stagiaire sur les questions liées,
- Pour toutes les questions de synthèse et de compréhension le correcteur s'attachera à évaluer la crédibilité et la pertinence de la réponse du stagiaire. Et à apprécier toute réponse cohérente du stagiaire,
- Le stagiaire n'est pas tenu de fournir des réponses aussi détaillées que celles mentionnées dans le corrigé,
- En cas de suspicion d'erreur au niveau du corrigé, prière de contacter la Division de Conception des Examens.

Détail du Barème :

| N° Des Dossiers | Travaux à réaliser | Barème |
|----------------------------------|---|-------------------|
| Partie 1 : Théorie | | |
| Dossier 1 | Comprendre et Exploiter une architecture Cloud | 06 Points |
| Dossier 2 | Cloud privé openstack | 09 Points |
| Dossier 3 | Administration Cloud propriétaire Azure | 15 Points |
| Dossier 4 | Gouvernance et Sécurité des données en Cloud | 10 Points |
| Total Partie 1 : Théorie | | /40points |
| Partie 2 : Pratique | | |
| Dossier 1 | Administration d'un environnement cloud propriétaire | 35 Points |
| Dossier 2 | Administration d'un Environnement Cloud avec une solution Libre | 25 Points |
| Total Partie 2 : Pratique | | /60points |
| Total Général | | /100points |

Dossier 1 : Comprendre et Exploiter une architecture Cloud (6 Points)

1- Quelle est la différence entre les modèles "multicloud" et "cloud hybride" ? (1 Point)

- **Multicloud** : Utilisation de plusieurs fournisseurs de cloud publics (ex : AWS + Azure) pour éviter la dépendance à un seul fournisseur.
- **Cloud Hybride** : Combinaison d'un cloud privé et d'un cloud public pour maximiser la flexibilité et la sécurité.

2- En quoi les solutions "serverless" diffèrent-elles des modèles traditionnels ? (1 Point)

- Pas besoin de gérer les serveurs ou d'assurer leur maintenance.
- Paiement uniquement pour le temps d'exécution du code ou des fonctions.
- Convient aux charges de travail dynamiques ou irrégulières.
- Exemples : AWS Lambda, Azure Functions, Google Cloud Functions.

3- Quels sont les critères à considérer pour choisir un fournisseur de cloud ? (1 Point)

- Coût et modèle de facturation.
- Disponibilité géographique des datacenters.
- Sécurité et conformité aux réglementations.
- Outils et services spécifiques proposés.
- Support technique et documentation.

4- Donnez une description et exemples par rapport aux dépenses OpEx (1 Point)

Dépenses opérationnelles quotidiennes effectuées par l'entreprise

5- Expliquez le principe de Availability Zones (1 Point)

Les Availability Zones sont des zones physiques distinctes au sein d'une région Azure. Chaque zone dispose de sa propre alimentation, de son réseau et de son refroidissement, offrant une isolation contre les pannes régionales.

6- Donnez des exemples de services de stockage proposés par Azure (1 Point)

- **Azure Blob Storage** : Stockage d'objets pour les fichiers volumineux (images, vidéos, etc.).
- **Azure Disk Storage** : Disques gérés pour les machines virtuelles.
- **Azure File Storage** : Partages de fichiers accessibles via SMB.
- **Azure Queue Storage** : Gestion des messages pour la communication entre applications.
- **Azure Data Lake Storage** : Stockage optimisé pour les grandes quantités de données

Dossier 2 : Cloud privé openstack (9 Points)

7- Complétez le tableau suivant avec les éléments manquants (4 Points)

| Composant | Description |
|-----------------|--|
| Nova | Service de calcul qui gère la création, l'exécution et la gestion des machines virtuelles. |
| Neutron | Service de réseau qui fournit la gestion des réseaux virtuels, des sous-réseaux et des routeurs. |
| Cinder | Service de stockage en bloc qui permet de créer, gérer et attacher des volumes persistants. |
| Swift | Service de stockage objet distribué et redondant pour stocker des données non structurées. |
| Keystone | Service d'authentification et de gestion des identités, des utilisateurs et des permissions. |
| Glance | Service de gestion des images qui permet de stocker et gérer des images de machines virtuelles. |
| Horizon | Interface web graphique pour administrer et utiliser les différents services OpenStack. |
| Heat | Service d'orchestration pour déployer et gérer les applications via des modèles (templates). |
| Trove | Service de gestion de bases de données en tant que service (DBaaS). |

8- Vous configurez une image dans Glance. Quel format est compatible ? (1 Point)

QCOW2

9- Quel outil est utilisé pour automatiser le déploiement d'OpenStack ? (1 Point)

DevStack

10- Que représente une "Floating IP" dans OpenStack ? (1 Point)

Une adresse IP publique associée à une instance pour se connecter à internet

11- Citez d'autres solutions pour mettre en place un Cloud Privé (2 Points)

Microcloud
Red Hat OpenShift
OpenNebula

Dossier 3 : Administration Cloud propriétaire Azure (15 Points)

| | | | | | |
|---------|-------------------------|----------|-----------|------|---------------|
| Filière | IDOCC | Variante | 1 | Page | Page 3 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

12- Quel outil est recommandé pour planifier les coûts d'Azure ? (1 Point)

Azure Calculator de prix

13- Quelle fonctionnalité Azure assure la haute disponibilité des applications ? (2 Points)

Application Gateway
Traffic Manager

14- Comment limiter l'accès réseau à une machine virtuelle Azure ? (2 Points)

Créer une règle NSG (Network Security Group)

15- Classez par ordre la hiérarchie d'organisation et de gestion des ressources dans Azure (2 Points)

Management Groupes
Abonnements
Groupe de ressources
Ressources

16- Quelles options sont disponibles pour connecter 3 Virtual Networks (VNETs) dans Azure ? (3 Points)

Peering VNet-to-VNet
Hub-and-Spoke Architecture

17- Pour utiliser Azure Site Recovery (ASR), vous avez besoin d'un compte de stockage de cache pour la réplication, il doit être située dans la région source ou cible ? (2 Points)

La région Source

18- Quelles solutions sont disponibles dans Azure pour connecter des ressources Azure avec un datacenter local (on-premises) ? (3 Points)

VPN Gateway
Point-to-Site VPN.
Azure Virtual WAN
Azure ExpressRoute
Azure Private Link

Dossier 4 : Gouvernance et Sécurité des données en Cloud (10 Points)

| | | | | | |
|---------|-------------------------|----------|-----------|------|---------------|
| Filière | IDOCC | Variante | 1 | Page | Page 4 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

19- Comment s'appelle le service permettant de gérer les autorisations dans Azure où les permissions sont appliquées à un niveau supérieur sont héritées par les niveaux inférieurs ? (2 Points)

Azure RBAC

20- Qu'est-ce qu'Azure Blueprints ? (2 Points)

Azure Blueprints est un service de gouvernance qui permet de définir et d'appliquer des modèles préconfigurés pour déployer rapidement et de manière cohérente des environnements cloud Azure conformes aux standards de sécurité et aux meilleures pratiques.

21- Quelle fonctionnalité qui permet d'ajouter des métadonnées aux ressources afin de faciliter leur identification, leur gestion et leur analyse des coûts. (2 Points)

Les Tags dans Azure

22- Une entreprise a récemment migré ses services dans Azure. Les ressources principales comprennent :

- Applications Web (hébergées dans Azure App Service).
- Bases de données SQL Azure contenant des données sensibles des clients.
- Une infrastructure hybride reliant les bureaux locaux de l'entreprise au cloud via un VPN Site-to-Site.
- Plusieurs machines virtuelles (VM) pour exécuter des workloads critiques.

Comment améliorer la sécurité des connexions utilisateur aux machines virtuelles ? (4 Points)

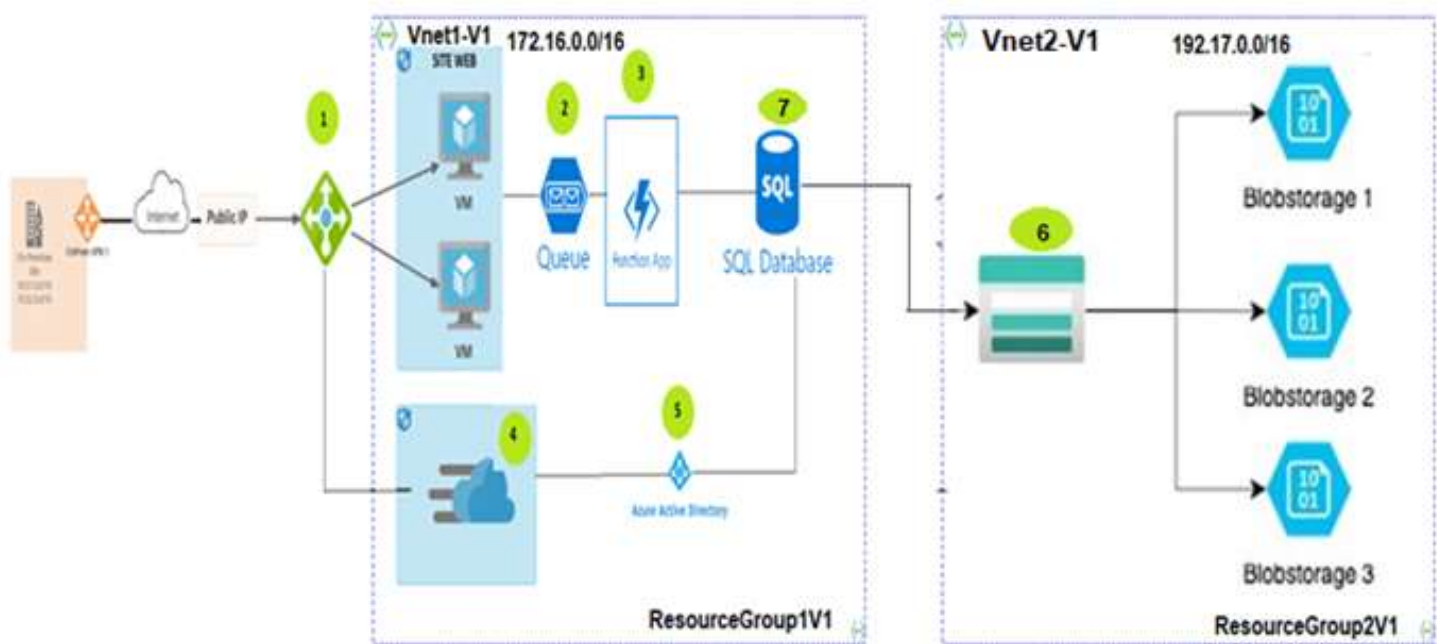
- Activer Azure Bastion pour fournir un accès sécurisé aux machines virtuelles via le portail Azure, sans exposer d'IP publique.
- Mettre en œuvre l'authentification multi-facteur (MFA) pour toutes les connexions administratives.
- Utiliser des identités managées pour limiter l'utilisation de mots de passe et centraliser la gestion des permissions.
- Implémenter des politiques d'expiration de mot de passe et forcer l'utilisation de mots de passe complexes.

Partie 2 : Pratique / 60 PTS

| | | | | | |
|---------|-------------------------|----------|-----------|------|---------------|
| Filière | IDOCC | Variante | 1 | Page | Page 5 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

Dossier 1 : Administration d'un environnement cloud propriétaire (35 Points)

La société CLOUD1 dispose d'un abonnement Microsoft Azure nommé CLOUD1Sub1
La société héberge 70% de son infrastructure sur Microsoft azure et elle garde juste trois serveurs et une baie de stockage comme ressource locale (on-premise) comme il le montre le schéma ci-dessous



1- Identifier les services azure 1 et 3 dans le schéma ? (1Pt)

- 1 : c'est un load balancer
- 3 : function app ou Azure Serverless

2- Expliquer le rôle des services 4 et 5 ? (1Pt)

4 : est un Azure CDN (Content Delivery Network) est un service proposé par Microsoft Azure qui permet de distribuer du contenu web de manière rapide, fiable et sécurisée à des utilisateurs

5 : Azure Active Directory (Azure AD) est un service d'annuaire cloud et une solution de gestion des identités proposé par Microsoft. Son rôle est de sécuriser et de gérer les identités des utilisateurs, des groupes, et des applications dans des environnements cloud

3- Donner deux avantages de l'administration de votre infrastructure avec azure powershell par rapport à l'interface graphique sur azure portal ? (1Pt)

- Automatisation des tâches répétitives
- Gestion à grande échelle et cohérence
- Rapidité

Gérer un Groupe de ressource en utilisant les commandes powershell :

| | | | | | |
|---------|-------------------------|----------|-----------|------|---------------|
| Filière | IDOCC | Variante | 1 | Page | Page 6 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

- 4- Expliquer le rôle d'un Groupe de ressource dans l'architecture Microsoft azure ? (1Pt)

Un **groupe de ressources** dans Azure est une unité logique qui permet d'organiser, gérer et administrer les ressources Azure associées à une application ou à un projet spécifique.

- 5- Donner la commande PowerShell pour Se connecter à votre abonnement Azure ?(1Pt)

Connect-AzAccount

- 6- Créer une nouvelle ressource groupe nommée ResourceGroup1V1 en utilisant 'EastUS' comme location. (1Pt)

New-AzResourceGroup -Name 'ResourceGroup1V1-Location 'EastUS''

- 7- Afficher la liste des groupes de ressources(1Pt)

Get-AzResourceGroup

- 8- Pour empêcher les utilisateurs de votre organisation de supprimer accidentellement votre ressource ResourceGroup1V1 créer un verrou Nommé LockResourceGroup1V1? (1Pt)

New-AzResourceLock -ResourceGroupName "test1" -LockLevel CanNotDelete

Gérer et sécuriser un réseau virtuel avec azure CLI :

- 9- Créer un sous-réseau de Vnet1V1. Nommé « Sub1Vnet1V1 » (adresse : 172.16.1.0/24, Location 'EastUS') ? (2pts)

az network vnet subnet create --name Sub1Vnet1V1 --vnet-name Vnet1V1--resource-group ResourceGroup1V1 --address-prefix 172.16.1.0/24

- 10- Créer le réseau virtuel « Vnet1V1 » dans ResourceGroup1V1 (adresse : 172.16.0.0/16, Location 'EastUS' et sous-réseau Sub1Vnet1V1). (2pts)

az network vnet create --name Vnet1V1 --resource-group ResourceGroup1V1 --location EastUs --address-prefixes 172.16.0.0/16 --subnet-name Subnet1-v1

- 11- Créer une adresse IP publique **PublicIPV1** (Sku Standard , Location 'EastUS' et ResourceGroup1V1) pour voter site web (2pts)

az network public-ip create --name PublicIPV1 --resource-group ResourceGroup1V1--Location EastUS --allocation-method Static --sku Standard

- 12- Sur quelle ressource azure peut-on associer un groupe de sécurité NSG ? (2pts)

| | | | | | |
|---------|-------------------------|----------|-----------|------|---------------|
| Filière | IDOCC | Variante | 1 | Page | Page 7 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

- Interface réseau (NIC)

- Sous-réseau

13- Créer le groupe de sécurité réseau **NSG-v1** (Location ' EastUS ' et ResourceGroup1V1 et l'associer au Sub1Vnet1V1 ? (2pts)

az network nsg create --name NSG-v1 --resource-group ResourceGroup1V1 --location EastUS

az network vnet subnet update --resource-group ResourceGroup1V1 --vnet-name Vnet1V1--name Sub1Vnet1V1 --network-security-group NSG-v1

14- Quel service azure doit-on ajouter pour interconnecter les réseaux **Vnet1V1** et **Vnet2V1** ? (1Pt)

Azure Peering

15- Donner la commande azure CLI pour créer une connexion depuis le **Vnet1V1** vers **Vnet2V1** ?(2pts)

**az network vnet peering create **
**--name Vnet1V1-to-Vnet2V1 **
**--resource-group ResourceGroup1V1 **
**--vnet-name Vnet1V1 **
--remote-vnet /subscriptions/<subscription-id>/resourceGroups/
**ResourceGroup1V1 /providers/Microsoft.Network/virtualNetworks/Vnet2V1 **
--allow-vnet-access

16- Proposer deux solutions pour interconnecter votre réseau local « on-premise » avec votre datacenter sur Microsoft Azure ? (1Pt)

Vpn site-to-site
azure express route

Gérer une machine virtuelle et conteneur en utilisant les commandes powershell :

17- En quoi l'architecture d'une machine virtuelle diffère-t-elle de celle d'un conteneur en termes d'utilisation du système d'exploitation et des ressources système ? (1Pt)

| Aspect | Machine Virtuelle (VM) | Conteneur |
|-----------------------------|-----------------------------------|--------------------------------------|
| Niveau de virtualisation | Matériel (via hyperviseur) | Système d'exploitation |
| Système d'exploitation | Chaque VM a son propre OS invité | Partage le kernel de l'OS hôte |
| Isolation | Complète (niveau matériel et OS) | Partielle (via namespaces et groups) |
| Consommation des ressources | Plus lourde (OS complet par VM) | Très légère (partage du kernel) |

18- Créer un compte de stockage StorageAccountV1 de type Standard general (Location 'EastUS' , sku Standard ZRS et ResourceGroup2V1) (2pts)

```
New-AzStorageAccount ` -ResourceGroupName "ResourceGroup2V1" ` -Name "StorageAccountV1" ` -Location "EastUS" ` -SkuName "Standard_ZRS" ` -Kind "StorageV2"
```

19- Déployer une nouvelle machine virtuelle Azure nommée VM1V1 (ResourceGroup1V1 ,Location 'EastUS' , Image: AdminV1LTS , Size: Standard_B2ms) et qui utilise le réseau virtuel Vnet1V1 et l'adresse IP public PublicIPV1 ? (2pts)

```
New-AzVM -ResourceGroupName " ResourceGroup1V1" -Name VM1V1 - Location "EastUs" - -VirtualNetworkName " Sub1Vnet1V1" -PublicIpAddress 'PublicIPV1' -Image " AdminV1LTS " -Size " Standard_B2ms "
```

20- Afficher la liste des machines virtuelles. ?(2pts)

```
Get-AzVM -ResourceGroupName "ResourceGroup1V1"
```

Sécurité et Surveillance sur le cloud :

21- Quels sont les principaux cas d'utilisation d'Azure Key Vault pour le stockage sécurisé des secrets ? (1Pt)

- Gestion des Secrets d'Applications
- Gestion des Clés de Chiffrement
- Gestion des Certificats

22- Quels sont les avantages d'utiliser Azure Bastion pour se connecter à des machines virtuelles, comparé à une connexion classique avec un client RDP ou SSH ? (1Pt)

- Accès à des VM sans adresse IP publique
- Surveillance et journalisation
- Aucun port ouvert (via HTTPS 443 uniquement)
- Intégration facile avec Azure Monitor et Log Analytics

23- Comment peut-on Renforcer la sécurité des VM proposer trois solutions ? (2pts)

Gestion des mises à jour et des correctifs

Désactivation de l'accès RDP/SSH

Utiliser une connexion bastion

24- Expliquer c'est quoi Chiffrement des données au repos et en transit et citer quelque exemple d'utilisation ? (1Pt)

| | | | | | |
|---------|-------------------------|----------|-----------|------|---------------|
| Filière | IDOCC | Variante | 1 | Page | Page 9 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

- Chiffrement des données au repos

Le chiffrement des données **au repos** consiste à protéger les données stockées sur un support, tel qu'un disque dur, une base de données, un compte de stockage ou un système de fichiers. Exemple : **Azure Disk Encryption (ADE)**

- Chiffrement des données en transit

Le chiffrement des données **en transit** protège les données lorsqu'elles circulent entre deux points, comme entre un client et un serveur ou entre deux services. Exemple : **azure vpn**

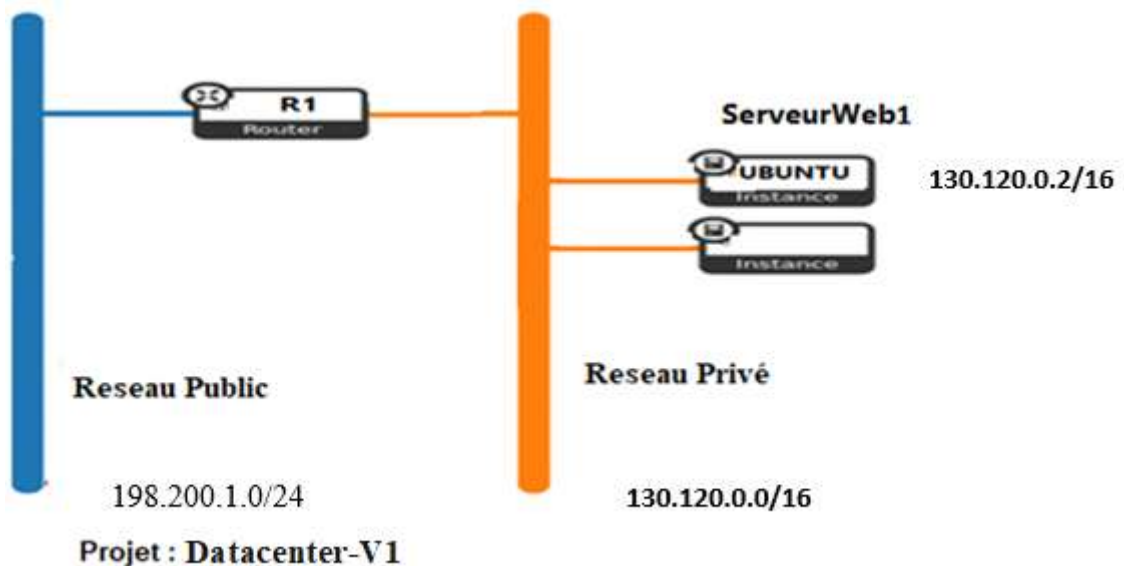
25- Sur quelle infrastructure est basé Microsoft Sentinel pour rechercher les menaces de sécurité de façon proactive? (1Pt)

Miter attack

Dossier 2 : Administration d'un Environnement Cloud avec une solution Libre (25 Points)

HIGH-CLOUD a décidé de faire une migration vers une plateforme Cloud Open Source comme openstack au lieu de Microsoft azure.

L'illustration suivante représente l'architecture principale de HIGH-CLOUD :



Créer le projet Datacenter-V1

| | | | | | |
|---------|-------------------------|----------|-----------|------|----------------|
| Filière | IDOCC | Variante | 1 | Page | Page 10 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

26- Expliquer les avantages de l'utilisation d'une plateforme Open Source comme solution de cloud computing ? (1Pt)

OpenStack est une solution open source permettant de déployer une infrastructure de cloud
Privée et sécurisé

On considère l'architecture ci-dessus donner les commandes permettant de réaliser les tâches suivantes :

27- Afficher la liste des services ? (1Pt)

`$Openstack service list`

28- Créer un nouveau projet nommé **Datacenter-V1** dans le domaine par défaut « default » ? (1Pt)

`$ openstack project create --domain default Datacenter-V1`

29- Créer un utilisateur « **AdminV1** » dans le projet **Datacenter-V1** avec « AdminV1@2025 » comme mot de passe et Email : AdminV1@HIGHCLOUD1.ma ? (1Pt)

`$ openstack user create --project Datacenter-V1 --password AdminV1@2025 --email AdminV1@ HIGHCLOUD1.ma AdminV1`

30- Attribuer le rôle « admin » à l'utilisateur **AdminV1** sur le projet **Datacenter-V1**? (1Pt)

`$ openstack role add --project Datacenter-V1 --user - AdminV1 admin`

Créer le réseau privé P1-Network

31- Créer le réseau privé « P1-Network » dans votre projet **Datacenter-V1** ? (1Pt)

`$openstack network create P1-Network`

32- Créer un sous-réseau « Sub-P1-Network » avec la configuration suivante : ? (2pts)

- **Network : 130.120.0.0/16**
- **Passerelle : 130.120.1**
- **DNS : 8.8.8.8**
- **Réseau : P1-Network**

`$openstack subnet create --network P1-Network --subnet-range 130.120.0.0/16 --dns-nameserver 8.8.8.8 --gateway 130.120.1 Sub-P1-Network`

33- Afficher la liste des réseaux disponibles ? (1Pt)

`$openstack network list`

34- Créer le routeur « R1 » pour interconnecter le réseau privé « P1-Network » avec le réseau public ? (1Pt)

| | | | | | |
|---------|-------------------------|----------|-----------|------|----------------|
| Filière | IDOCC | Variante | 1 | Page | Page 11 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

```
$openstack router create R1
```

35- Ajouter le sous-réseau « **Sub-P1-Network** » en tant qu'interface sur le routeur R1 (2pts)

```
Openstack router add subnet R1 Sub-P1-Network
```

36- Définir une passerelle sur le réseau Public pour le routeur R1 ?(1Pt)

```
Openstack router set R1 --external-gateway Public
```

37- Créer un port avec IP fixe **130.120.0.2/16** nommé « Port-AdminV1 » à partir du réseau P1-Network ? (1Pt)

```
$openstack port create --network P1-Network --fixed-ip subnet= Sub-P1-Network ,ip-address=130.120.0.2 Port-AdminV1
```

38- Pour accéder à votre instance via SSH créer un groupe de sécurité « **SSH-GRP** » qui autorise la connexion SSH vers votre instance AdminV1 ? (1Pt)

```
$openstack security group create SSH-GRP
```

```
$openstack security group rule create --protocol tcp --dst-port 22 SSH-GRP
```

39- Créer une paire de clé nomme **Key-shhV1** avec la clé ssh « `./ssh/id-rsa.pub` » (1Pt)

```
Openstack keypair create --public-key ./ssh/id_rsa.pub Key-shhV1
```

Créer l'instance ServeurWeb1

40- Créer une image openstack « **Ubuntu** » pour l'instance de votre serveur web en utilisant le fichier image « `bionic-server-cloudimg-amd64.img` » et `qcow2` comme format de disque ? (2pts)

```
openstack image create " Ubuntu " --file bionic-server-cloudimg-amd64.img --disk-format qcow2 --public
```

41- Afficher la liste des images disponibles ? (1Pt)

```
Openstack image list
```

42- Créer un volume vide avec les spécifications suivantes : taille=10Go, nom = disque-v1. ? (1Pt)

```
openstack volume create --size 10 --name disque-v1
```

43- Créer une machine virtuelle « **ServeurWeb1** » avec la configuration suivante : ? (2pts)

| | | | | | |
|---------|-------------------------|----------|-----------|------|----------------|
| Filière | IDOCC | Variante | 1 | Page | Page 12 sur 13 |
| CORRIGE | Examen Fin de Formation | Session | Juin 2025 | | |

- **Image : Ubuntu**
- **Flavor : m1.small**
- **Security-group : SSH-GRP**
- **Port: Port-AdminV1**
- **Key-ssh : Key-shhV1**

```
$openstack server create --image Ubuntu --flavor m1.small --security-group SSH-GRP --
nic port-id= Port-AdminV1 -key-name Key-shhV1 ServeurWeb1
```

44- Attacher le volume **disque-v1** à l'instance **ServeurWeb1** ?(1Pt)

```
Openstack server add volume ServeurWeb1 disque-v1
```

Configurer l'accès à distance pour votre ServeurWeb1

45- Allouer une adresse IP flottante sur le réseau public « Public1-IPv4 » (pour un accès public sur le serveur web) Associer IP flottante à votre instance «ServeurWeb1 » ? (1Pt)

```
openstack floating ip create Public1-IPv4
openstack server add floating ip ServeurWeb1 <floating-ip-address>
```

46- Afficher la liste des instances avec leurs IP flottante (1Pt)

```
openstack server list --floating-ip
```