

	مكتب التكوين المهني وإنعاش الشغل	
	Office de la Formation Professionnelle et de la Promotion du Travail	
	Direction de la Recherche et de l'Ingénierie de la Formation Division Conception des Examens	

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 Systèmes et Réseaux		
Variante	2	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.

N° Des Dossiers	Travaux à réaliser	Barème
Partie Théorique		
Dossier 1	Infrastructure Réseaux et Sécurité Informatique	/ 30 pts
Dossier 2	Administration Système et Cloud	/ 10 pts
Total Partie Théorique		/40 points
Partie Pratique		
Dossier 3	Réseaux et Sécurité Informatique	/ 20 pts
Dossier 4	Administration d'un système Linux	/ 20 pts
Dossier 5	Administration d'un système Windows Server	/ 20 pts
Total Partie Pratique		/60 points
Total Général		/100 points

Filière	IDOSR	Variante	2	Page 1 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

Détail du Barème :

Question	Barème	Question	Barème	Question	Barème
THEORIE	/40	Q14.4	1	Q28	Voir détail de notations
Dossier 1	/30	Q15.1	2	Q29	2
Q1	2	Q15.2	2	Q30	2
Q2	2	PRATIQUE	/60	Q31	3
Q3	2	Dossier 3	/20	Q32	2
Q4.1	2	16.1	1	Dossier 5	/20
Q4.2	1,5	16.2	1	Q33	3
Q4.3	1	16.3	1	Q34	3
Q5	2	17	1	Q35	2
Q6.1	1,5	18.1	1	Q36.1	2
Q6.2	1	18.2	1	Q36.2	2
Q6.3	1	19	1	Q37	2
Q7	2	20	2	Q38	2
Q8	2	21	2	Q39	2
Q9	2	22	2	Q40	2
Q10	1,5	23.1	2		
Q11	1	23.2	2		
Q12	1,5	24.1	1		
Q13.1	2	24.2	1		
Q13.2	2	24.3	1		
Dossier 2	/10	Dossier 4	/20		
Q14.1	1	Q25	2		
Q14.2	2	Q26	2		
Q14.3	2	Q27	2		

Partie théorique (/40pts)

Vous travaillez désormais au sein de l'entreprise «TechOrbit.com», une organisation qui a récemment renforcé son infrastructure réseau en intégrant de nouveaux sites distants. Afin d'assurer une communication fluide entre ses différentes implantations et de garantir une connexion Internet sécurisée, l'entreprise a besoin d'une infrastructure réseau fiable et évolutive, capable de s'adapter aux exigences futures. En tant que technicien réseau, votre mission principale consiste à assumer diverses responsabilités liées à cette évolution technologique.

Dossier 1 : Infrastructure Réseaux et Sécurité Informatique (/30 points)

1. À quelle couche du modèle **OSI** se rapporte une adresse **MAC** ?

Une adresse MAC se rapporte à la **couche 2** du modèle **OSI**, appelée liaison de données.

2. Qu'est-ce qu'une **Route statique récapitulative** ?

Une route statique récapitulative est une route qui **regroupe plusieurs sous-réseaux ou préfixes IP** en une seule entrée de routage, simplifiant ainsi la table de routage et améliorant l'efficacité du réseau.

3. Quelle est la **particularité** d'un **commutateur de couche 3** ?

Un commutateur de couche 3 **combine les fonctionnalités d'un commutateur de couche 2**, comme le filtrage et la commutation de trames Ethernet, **avec celles d'un routeur**, permettant la gestion du trafic entre différents sous-réseaux grâce à son aptitude à réaliser du routage IP

4. La société, dans l'une de ses filiales, utilise une topologie **OSPF à accès multiple**. Vous avez été chargé de déterminer le routeur qui sera élu comme routeur **DR** dans cette architecture. Celle-ci peut être simplifiée comme suit :

4.1. Expliquez le processus de sélection du **DR** dans un réseau **OSPF à accès multiple**.

- Une priorité de 0 signifie non-participation à l'élection du DR. (option)
- Le routeur avec la priorité la plus élevée est préféré pour devenir DR.
- En cas d'égalité de priorité, le routeur avec la valeur '**router-id**' la plus élevée est choisi.

4.2. Indiquez l'ID des routeurs **OSPF R1, R2 et R3**.

- Si le **router-id** est explicitement configuré sur le routeur, cette valeur est retenue comme router ID.
- Si aucun router-id n'est configuré, l'adresse IPv4 la plus élevée parmi les interfaces **Loopback** actives est sélectionnée comme router ID.
- Si le routeur n'a pas d'interface **Loopback**, l'adresse IP la plus élevée parmi toutes les autres interfaces actives est utilisée comme router ID.

En résumé :

- **Router ID de R1** : 10.10.0.2
- **Router ID de R2** : 2.2.2.2
- **Router ID de R3** : 192.168.30.1

4.3. Déterminez quel routeur sera élu comme routeur **DR**.

R3 sera le DR

L'entreprise dispose de plusieurs serveurs qui sont configuré avec des adresses IPv6 Globale.

5. Expliquez brièvement comment un hôte peut être attribué dynamiquement à une adresse **IPv6 GUA** en utilisant des services **avec état (Statefull)**.

Un hôte peut se voir attribuer dynamiquement une adresse IPv6 Global Unicast Address (GUA) en utilisant des services avec état, tels que DHCPv6,

Filière	IDOSR	Variante	2	Page 3 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

6. L'entreprise dispose d'un réseau **Wi-Fi** déployé à travers différentes topologies. La majorité des points d'accès utilisés sont de type « **double bande** ».
L'interface graphique de la configuration des paramètres Wi-Fi de l'un des points d'accès est présentée dans la figure suivante (annexe 2) :

6.1. Expliquez le rôle des paramètres 2, 3 et 6.

- **Masquer le SSID** - Cette option, lorsqu'elle est activée, empêche le nom du réseau (SSID) de s'afficher dans la liste des réseaux Wi-Fi disponibles.
- **Sécurité (WPA/WPA2-Enterprise)** - Ce paramètre définit le type de sécurité utilisé pour protéger le réseau Wi-Fi.
- **Puissance de transmission** - Ce paramètre permet de régler la puissance du signal émis par le point d'accès Wi-Fi.

6.2. Citez un avantage de l'utilisation d'un serveur **RADIUS** ?

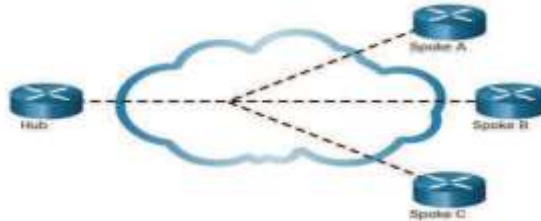
- **Centralisation de l'authentification.**
- **Produits open source et libre**

6.3. Donnez une raison pour laquelle l'élément 6 a été configuré avec la valeur '**Faible**' ?

- **Réduire les interférences** avec d'autres dispositifs ou réseaux sans fil à proximité.
- **Limiter la portée du signal** pour minimiser l'exposition au réseau à des utilisateurs non autorisés ou à des attaques potentielles, renforçant ainsi la sécurité du réseau.
- **Gestion de l'énergie** afin de réduire la consommation d'énergie.

La société possède des agences sur plusieurs villes du royaume. Ils sont reliés avec le siège via des liaisons **WAN** privées et publique (Internet).

7. Présentez, à l'aide d'un schéma simple, la topologie WAN **en étoile**.



8. Définissez le rôle de l'élément **DCE** dans une architecture WAN.

Un DCE, **fourni par le fournisseur de services**, a pour rôle de fournir l'interface physique nécessaire pour **assurer l'accès d'une entreprise à son réseau**.

La société a décidé d'introduire l'architecture **SDN**.

9. Dans le contexte des réseaux **SDN**, expliquez la notion d'une **API privées**.

Une API privée est **développée par des entités privées** pour un **usage spécifique** à leur réseau, offrant des fonctionnalités de gestion et de personnalisation qui ne sont pas accessibles au public général.

10. Copiez sur votre feuille de réponse et complétez le tableau ci-dessous en classant les éléments suivants selon leur appartenance aux trois plans de l'architecture SDN (plan de données, plan de contrôle, plan d'application): , ,

plan de données	plan de contrôle	plan d'application
Routeurs	Ryu	Python

11. Définissez le concept de **Southbound Interface'** (SBI) dans une architecture **SDN**.

L'interface Southbound (SBI) désigne le canal de communication entre le contrôleur SDN et les dispositifs de réseau,

Filière	IDOSR	Variante	2	Page 4 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

La sécurité informatique représente une priorité majeure pour l'entreprise, en raison de l'évolution constante des menaces. Cela rend indispensable la mise en place d'une protection à la fois efficace et conforme à la législation pour assurer une gestion sécurisée des systèmes d'information.

12. Copiez sur votre feuille de réponse et complétez le tableau ci-dessous en identifiant l'emplacement des attaques suivantes en fonction des trois principes fondamentaux : la confidentialité, l'intégrité et la disponibilité :

la confidentialité	l'intégrité	la disponibilité
Analyse de trafic (traffic analysis)	Modification d'une valeur dans une base de données	Attaque Ransomware

13. Un utilisateur, ayant l'adresse IP 172.16.1.100/24, signale une impossibilité d'utiliser le serveur de noms via le protocole standard DNS. En examinant les règles du pare-feu, vous êtes chargé de modifier la configuration du pare-feu afin de rétablir la connectivité pour cet utilisateur au serveur DNS.

Tableau des règles du pare-feu :

IP Source	Port Source	IP Destination	Port Destination	Protocole	Accès
172.16.1.0/24	*	*	80	TCP	Autorisé
172.16.1.0/24	*	*	53	TCP	Autorisé
172.16.1.0/24	*	*	443	TCP	Autorisé
172.16.1.100/32	*	*	22	TCP	Refusé
172.16.1.0/24	*	*	*	ICMP	Refusé
*	*	*	*	*	Refusé

13.1. Identifiez la règle du pare-feu qui empêche l'accès de cet utilisateur au serveur DNS.

Le DNS utilise le protocole UDP pour ses requêtes, ce qui n'est pas couvert par les règles existantes.

13.2. Proposez une nouvelle règle pour résoudre ce problème.

172.16.1.0/24	*	*	53	UDP	Autorisé
---------------	---	---	----	-----	----------

Dossier 2 : Administration Système et Cloud(/10 points)

La société administre une variété de serveurs. Parmi ceux-ci se trouve un serveur DNS fonctionnant sous Windows Server 2019. Pour vérifier le statut de ce serveur, le gestionnaire DNS a été lancé. La figure ci-dessous montre l'état actuel de ce service.

14. En analysant la figure ci-dessus, répondez aux questions suivantes :

14.1. Indiquez le type de zone de recherche DNS est utilisé pour afficher ces informations.

Le type de zone de recherche DNS utilisé dans l'image est une "Zone de recherche directe".

14.2. Expliquez le rôle de l'enregistrement NS du serveur DNS.

Le rôle de l'enregistrement NS (Name Server) dans le DNS est de spécifier les serveurs DNS qui sont autoritatifs pour une zone DNS particulière.

14.3. Identifiez le nom et l'adresse IP du serveur DNS principale.

Le nom du serveur DNS principal (ou 'Hôte (A)') pour la zone "techorbit.com" est "srvcdp.techorbit.com" avec l'adresse IP 192.168.1.40.

14.4. Quelle est la signification de la mention 'statique' affichée dans le champ 'Horodateur' d'un enregistrement DNS ?

La mention 'statique' dans le champ 'Horodateur' d'un enregistrement DNS signifie que l'enregistrement a été créé manuellement et ne sera pas supprimé automatiquement

15. Lors de la création d'une machine virtuelle (VM) sur Azure Cloud, la société a opté pour la région '(US) West US 2.

15.1. Expliquez ce qu'est une zone de disponibilité (Availability Zone) dans le contexte d'Azure.

Filière	IDOSR	Variante	2	Page 5 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

Une zone de disponibilité dans Azure **est une zone géographiquement isolée** au sein d'une région, contenant un ou plusieurs datacenters **équipés de leur propre alimentation, refroidissement, et réseautage**, conçue pour garantir que les services restent opérationnels même si un autre datacenter dans la région tombe en panne.

15.2. Expliquez le rôle de l'option '**Zone autosélectionnée**' dans ce contexte.

L'option 'Zone autosélectionnée' dans Azure permet de déployer automatiquement les ressources dans plusieurs zones de disponibilité, offrant ainsi une haute disponibilité sans nécessiter une sélection manuelle spécifique de la zone par l'utilisateur.

Filière	IDOSR	Variante	2	Page 6 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

Partie pratique (/60pts)

Dossier 3 : Réseaux et Sécurité Informatique (/20 points)

16. Pour optimiser la gestion de trafic, vous devez créer des vlan sur le commutateur **de couche 3 S4**, de l'entreprise ainsi de configurer le routage inter-vlan. Le tableau suivant présente la liste des vlan ainsi que les ports attribués à chaque vlan :

16.1. Créez les vlan sur le commutateur **S4**.

Pour chaque VLAN (30, 40, 50), utilisez la commande suivante pour le créer :

```
S4(config) vlan 30
```

```
S4(config-vlan) name Utilisateurs
```

16.2. Affectez les ports du commutateur **S4** aux vlan appropriés.

```
S4(config) interface range fastEthernet 0/10 – 15
```

```
S4(config-if) switchport mode access
```

```
S4(config-if) switchport access vlan 30
```

```
S4(config) interface range fastEthernet 0/16 – 24
```

```
S4(config-if) switchport mode access
```

```
S4(config-if) switchport access vlan 40
```

```
S4(config) interface range fastEthernet 0/25 – 30
```

```
S4(config-if) switchport mode access
```

```
S4(config-if) switchport access vlan 50
```

16.3. Configurez les ports **Trunk** sur le commutateur **S4**.

```
S4(config) interface range fastEthernet 0/1
```

```
S4(config-if) switchport mode trunk
```

17. Configurez les interfaces **SVI** du commutateur **S4** conformément aux adresses fournies dans le tableau d'adressage.

```
S4(config) interface vlan 30
```

```
S4(config-if) ip address 172.16.30.1 255.255.255.0
```

```
S4(config-if) no shutdown
```

```
S4(config) interface vlan 40
```

```
S4(config-if) ip address 172.16.40.1 255.255.255.0
```

```
S4(config-if) no shutdown
```

```
S4(config) interface vlan 50
```

```
S4(config-if) ip address 172.16.50.4 255.255.255.0
```

```
S4(config-if) no shutdown
```

18. Afin de gérer d'une façon efficace votre réseau redondant qui utilise plusieurs chemins physiques, vous êtes chargé d'implémenter le protocole **STP** qui permet d'éliminer les boucles.

18.1. Configurez le protocole **STP** pour utiliser la version **PVST+**

```
S4(config) spanning-tree mode pvst
```

18.2. Configurez le commutateur **S4** en tant que **pont secondaire** pour les **trois Vlan**.

```
S4(config) spanning-tree vlan 30,40, 50 root secondary
```

19. Configurez l'agrégation de liaisons entre les commutateurs **S3** et **S4** en utilisant le protocole **LACP**. Utilisez les ports et les paramètres spécifiés dans le tableau ci-dessous :

Commutateur	Ports
S3	Fa0/4, Fa0/5
S4	Fa0/4, Fa0/5

```
S3(config) interface range fa0/4 - fa0/5
```

Filière	IDOSR	Variante	2	Page 7 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

```
S3(config-if) channel-protocol lacp
S3(config-if) channel-group 1 mode active
```

20. Pour assurer la redondance des passerelles sans configuration supplémentaire des périphériques finaux, vous êtes chargé de configurer le protocole **HSRP**.

Sur le routeur **R4** configurez le protocole de redondance au premier saut **HSRP** pour le **Vlan 50** en appliquant les paramètres suivants :

```
R3(config)# interface Gi0/0
R3(config-if)# standby 10 ip 172.16.50.1
R3(config-if)# standby 10 priority 120
R3(config-if)# standby 10 preempt
```

21. Configurez **une route par défaut** sur le commutateur **S4** pour diriger le trafic vers l'adresse IP **172.16.50.1**.

```
S4(config)#ip route 0.0.0.0 0.0.0.0 172.16.50.1
```

22. Configurez **des routes statiques** sur le routeur **R3** pour diriger le trafic vers les réseaux des **VLANs 30 et 40**.

```
R3(config)#ip route 172.16.30.0 255.255.255.0 172.16.50.4
```

```
R3(config)#ip route 172.16.40.0 255.255.255.0 172.16.50.4
```

23. L'accès au site de serveurs de l'entreprise est basé sur des listes de contrôles d'accès.

- 23.1. Créez une liste de contrôle d'accès (ACL) nommée « **ACL-2025** » sur le routeur R4 afin de:

- Permettre à tous les utilisateurs d'accéder au serveur **DNS**, **qui utilise le protocole UDP**, à l'adresse IP **172.16.10.10**
- Autorisez le poste administratif ayant pour adresse IP **172.16.40.3** à utiliser le service **FTP** (protocole **TCP**) sur le serveur situé à l'adresse IP **172.16.10.30**.
- Interdisez tout autre trafic non spécifié dans cette ACL.

```
R4(config)#ip access-list extended ACL-2025
R4(config-ACL)#permit udp any host 172.16.10.10 eq 53
R4(config-ACL)#permit tcp host 172.16.40.3 host 172.16.10.30 eq 21
R4(config-ACL)#deny ip any any
```

- 23.2. Indiquez la commande pour appliquer la liste d'accès « **ACL-2025** » sur l'interface appropriée.

```
R4 (config)#int G0/0
R4(config)#ip access-group ACL-2025 in.
```

24. En raison des besoins d'évolutivité, la société envisage de migrer certaines de ses services vers le protocole IPv6.

- 24.1. Configurez l'interface **G0/0** de routeur **R4** avec l'adresse **IPv6 link local** suivante **Fe80::1**

```
R4(config)# ipv6 unicast-routing
R4(config)# interface G0/0
R4(config-if)# ipv6 address fe80::1 link-local
```

- 24.2. Configurez l'interface **S0/0** du routeur **R4** avec l'adresse **IPv6** globale suivante : **2002:abcd::1234:1/64**.

```
R4(config)# interface S0/0
R4(config-if)# ipv6 address 2002:abcd::5678:1/64
```

- 24.3. Configurez la liaison **VPN** de type **GRE** entre les deux routeurs **R2** et **R4** en en appliquant les paramètres suivants :

- L'adresse IPv6 de **R2** est **2002:abcd::5678:2/64**
- Le nom du tunnel est **tunnel0**
- L'adresse privé à utiliser est **Fe80::1**

```
R4(config)# interface Tunnel0
R4(config-if)# tunnel source S0/0
R4(config-if)# tunnel destination 2002:abcd::5678:2
R4(config-if)# ipv6 address fe80::1/64 link-local
```

Dossier 4 : Administration d'un système Linux (/20 points)

Filière	IDOSR	Variante	2	Page 8 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

La correction fournie a été effectuée sur la distribution **Linux CentOS**. Il est important de noter que la solution **peut varier** en fonction de la distribution Linux utilisée par le stagiaire.

Toute réponse permettant d'atteindre le résultat attendu est acceptable. Cela peut inclure :

- **Une ou plusieurs commandes.**
- **Un script.**
- **La modification d'un fichier de configuration**

25. Quelle commande utilise-t-on pour vérifier si le package **Apache** est correctement installé ?

`yum list installed httpd`

26. Configurez les paramètres réseau du serveur **web-srv** en utilisant les valeurs fournies dans le tableau.

`nmcli mod con ens33 ipv4.method manual ipv4.address 172.16. 10.10/24 ipv4.gateway 172.16.10.1`

27. Quelle directive Apache permet de configurer le serveur pour écouter les demandes des clients sur le port TCP 8800 et depuis n'importe quelle adresse IP.

`Listen * :8800`

28. Utilisez le format général d'un fichier de configuration Apache ci-dessous pour configurer un **VirtualHost** pour le site web **www.techorbit.com**. Complétez les champs pointillés en utilisant les spécifications fournies.

DocumentRoot	<code>/var/www/techorbit/html</code>
Nom de domaine	<code>techorbit.com</code>
Fichier de log d'erreurs	<code>/var/log/httpd/techorbit_error.log</code>
Fichier de log d'accès	<code>/var/log/httpd/techorbit_access.log</code>
Ecouter sur le port	<code>8800</code>

<code><VirtualHost *:8800></code>	0.5pt
<code>ServerName techorbit.com</code>	1pt
<code>ServerAlias www.techorbit.com</code>	1pt
<code>DocumentRoot /var/www/techorbit/html</code>	1pt
<code><Directory /var/www/techorbit/html</code>	0.5pt
<code> AllowOverride none</code>	
<code> Require all granted</code>	
<code></Directory></code>	
<code>ErrorLog /var/log/httpd/techorbit_error.log</code>	0.5pt
<code>CustomLog /var/log/httpd/techorbit_access.log combined</code>	0.5pt
<code></VirtualHost></code>	

29. Indiquez le chemin du dossier contenant tous les fichiers de configuration d'**Apache**.

`/etc/httpd/`

30. Un utilisateur rapporte ne pas pouvoir accéder à un fichier sur le site web. Les journaux (logs) d'Apache indiquent l'erreur suivante :

```
[Wed Jan 29 12:34:56.123456] [authz_core:error] [pid 1234] [client 175.50.1.47:54321]
AH01630: client denied by server configuration: /var/www/techorbit/html/restricted/file.txt
```

Identifiez la cause du problème mentionné et proposez une solution appropriée.

Le fichier ou le répertoire ne dispose pas des permissions appropriées pour être accessible aux clients d'Apache. Il est nécessaire de modifier la configuration d'Apache concernant les permissions d'accès.

31. Configurez le service **Apache** pour qu'il démarre **automatiquement** lors du démarrage du serveur

`systemctl enable httpd`

Filière	IDOSR	Variante	2	Page 9 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

32. Affichez la **liste** des règles actuellement appliquées au **pare-feu**

```
firewall-cmd --list-all
```

Dossier 5 : Administration d'un système Windows Server (/20 points)

Consignes de Notation pour le Partie de PowerShell :

- **Commande Correcte (100% de la note) :**
Si la commande PowerShell, y compris toutes ses options, est correcte, la totalité de la note sera attribuée au stagiaire.
- **Commande Incorrecte (Notation Partielle) :**
 - **Commande Principale Correcte (50% de la note) :**
 - Si la commande principale (applet de commande) est correcte, la moitié de la note totale sera attribuée.
 - **Options de la Commande :**
 - **Options pour une Commande Acceptant Deux Options :**
 - Si la commande principale accepte deux options, 0,5 point sera déduit pour chaque option incorrecte.
 - **Options pour une Commande Acceptant Plus de Deux Options :**
 - Si la commande principale accepte plus de deux options, 0,25 point sera déduit pour chaque option incorrecte.
 - Il va sans dire que lorsque toutes les options sont fausses, la note zéro sera attribuée.

L'entreprise souhaite mettre en place un réseau basé sur **Windows Server 2019** pour gérer ses ressources informatiques. Elle dispose d'un contrôleur de domaine unique appelé **DC1**. techorbit.com et d'un serveur DHCP nommé **DHCP_Srv1**. techorbit.com:

Vous êtes chargé d'effectuer certaines tâches d'administration système à l'aide des commandes PowerShell.

33. Configurez le serveur **DC1** avec une adresse IP statique de **172.16.10.9** avec un masque de sous-réseau **255.255.255.0** et une passerelle par défaut **172.16.10.1** sur le serveur **DC1**, en utilisant l'interface nommée **Ethernet**.

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 172.16.10.9 -PrefixLength 24 -DefaultGateway 172.16.10.1
```

34. Configurez le serveur DC1 comme contrôleur de domaine principal en respectant les spécifications suivantes :

- Nom de domaine : **techorbit.com**
- Installation de DNS : **Oui**
- Autres options : **Paramètres par défaut.**

```
Install-ADDSForest -DomainName "techorbit.com" -InstallDns
```

35. Créez une unité organisationnelle appelée **Finance_users** au sein de l'unité organisationnelle existante **OU= Finance_Team, DC= techorbit, DC= com**.

```
New-ADOrganizationalUnit -Name "Finance_users" -Path "OU=Finance_Team, DC= techorbit, DC= com "
```

Filière	IDOSR	Variante	2	Page 10 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	

36. L'administrateur a ajouté un utilisateur au domaine techorbit.com à l'aide de PowerShell, puis a exécuté la commande suivante :

```
PS C:\> Get-ADUser -Identity abc.user1

DistinguishedName : CN=user1,CN=Users,DC= techorbit, DC=com
Enabled           : True
Name              : user1
SamAccountName    : abc.user1
UserPrincipalName : abc.user1@ techorbit.com
```

- 36.1. Quel est le **chemin d'annuaire complet** de l'utilisateur **user1** dans **Active Directory**?

CN=user1,CN=Users,DC= techorbit, DC=com

- 36.2. Déplacez l'utilisateur **user1** vers l'unité organisationnelle **Finance_Computers**.

Move-ADObject -Identity "CN=user1,CN=Users,DC= techorbit, DC=com" -TargetPath " OU= Finance_users ,OU=Finance_Team, DC= techorbit, DC=com"

37. Autorisez dans Active Directory le serveur **DHCP_Srv1** ayant l'adresse IP 172.16.10.3.

Add-DhcpServerInDC -DnsName "DHCP_Srv1. techorbit.com" -IPAddress "172.16.10.3"

38. Créez une étendue sur le serveur **DHCP_Srv1**, avec les paramètres suivants :

- Nom : **LAN 1**
- Plage d'adresses IP : **172.16.10.8-172.16.10.254**
- Masque de sous-réseau : **255.255.255.0**

Add-DhcpServerV4Scope -Name "LAN 1" -StartRange 172.16.10.8 -EndRange 172.16.10.254 -SubnetMask 255.255.255.0

39. Configurez sur le serveur **DHCP_Srv1** l'option suivante pour la plage :

- Passerelle par défaut (Option 003) : **172.16.10.1**

Set-DhcpServerV4OptionValue -ScopeId 172.16.0.0 -OptionId 6 -Value 172.16.10.1

40. Configurez également l'adresse IP du contrôleur de domaine **DC1** pour qu'elle **soit exclue** de l'attribution aux clients.

Add-DhcpServerV4ExclusionRange -ScopeId 172.16.10.0 -StartRange 172.16.10.9 -EndRange 172.16.10.9

Filière	IDOSR	Variante	2	Page 11 sur 11
CORRIGE	Examen Fin de Formation	Session	Juin 2025	