Nom : MOSAAD
Prénom : Chehab
Classe : 1A STRI

TP N°1 (2023) :

Mise en place d'un Active Directory :

Objectif : Concevoir et réaliser son environnement Windows en réseau pour déployer les services numériques de base. Réfléchir d'où se fait l'administration et comment sécuriser cette infrastructure.

Compétences :
- Concevoir et réaliser un environnement Active Directory.
- Exécuter des commandes PowerShell et en faire des scripts.
- Mettre en œuvre les services DNS, DHCP.
- Débuter dans la sécurisation d'un environnement Windows.

Sujet :
Un active directory sert à gérer un parc de machines (postes et serveurs) ainsi qu'un ensemble d'utilisateurs faisant partie du Systèmes d'informations. On parle d'authentification Kerberos ou LDAP.
Soit un parc de 30 postes, 7 serveurs dont 1 active directory et 20 utilisateurs dont 2 administrateurs. Pour les questions, tous les éléments de votre infrastructure n'ont pas besoin d'être allumés ensemble.

1. Conception du schéma de votre infrastructure :
Présentez à travers un schéma l'organisation de votre réseau. Vous expliquerez les raisons de cette organisation.

2. PowerShell :
Ecrivez un script PowerShell qui installe et configure l'active directory. Quel est l'intérêt d'un script plutôt que d'exécuter simplement la commande ?

3. Installation de l'architecture :
Mettez en place 1 serveur Active Directory. Créez une redondance à votre serveur. Expliquez l'importance de cette redondance. Comment l'organiseriez-vous sur votre infrastructure de virtualisation et pourquoi ? Eteignez votre serveur principal et testez la résolution de nom de votre domaine. Qu'en déduisez-vous ?

4. Convaincre :

Le directeur demande être administrateur du serveur Active Directory. Que vous acceptiez ou non, quelles sont les étapes de votre démarche ?

5. Adressage automatique :

En PowerShell, installez un serveur DHCP. Puis utilisez l'interface graphique pour configurer les étendues. Installez un poste et montrez qu'il récupère une adresse de ce serveur. Joignez-le au domaine. Ce sera votre poste d'administration.

6. Un peu d'imagination :

Que mettez-vous en place (Réseau, protocole d'accès, Comptes, etc..) pour sécuriser les accès à vos serveurs AD ?

Sommaire :

Introduction :

L'Active Directory est un service d'annuaire qui permet de gérer les ressources d'un réseau Windows, comme les machines, les utilisateurs, les groupes, les politiques de sécurité, etc. Il repose sur des protocoles standardisés comme LDAP pour assurer l'authentification et l'autorisation des accès. Également, l'Active Directory est organisée en domaines, qui sont des unités logiques de gestion du réseau. Chaque domaine dispose d'au moins un contrôleur de domaine, qui est un serveur chargé de stocker et de répliquer les données de l'annuaire. Mais aussi, un domaine peut être subdivisé en unités d'organisation, qui sont des conteneurs hiérarchiques permettant de classer les objets du réseau.

Apprendre à concevoir et à mettre en œuvre un environnement Active Directory est une compétence essentielle pour tout professionnel de l'informatique qui souhaite gérer un réseau Windows de manière efficace et sécurisée. L'Active Directory offre de nombreux avantages, comme l'administration centralisée, la scalabilité, la flexibilité et l'interopérabilité. Mais il pose aussi de nombreux défis, comme la complexité, la fiabilité, la disponibilité,

Dans ce contexte, tout d'abord, l'objectif de ce TP est de concevoir et de réaliser un environnement Windows en réseau pour déployer les services numériques de base. Ensuite, nous allons réfléchir à la façon

dont se fait l'administration et comment sécuriser cette infrastructure. Enfin, nous allons mettre en œuvre les compétences suivantes :

1. Concevoir et réaliser un environnement Active Directory.
2. Exécuter des commandes PowerShell et en faire des scripts.
3. Mettre en œuvre les services DNS et DHCP.
4. Débuter dans la sécurisation d'un environnement Windows.

Pour répondre aux questions, nous allons réaliser les étapes suivantes :

- Question 1 : Conception du schéma de notre infrastructure : Nous allons dessiner un schéma qui représente l'organisation logique et physique de notre réseau.
- Question 2 : PowerShell : Nous allons écrire un script PowerShell qui installe et configure l'active directory sur un serveur. Nous allons expliquer l'intérêt d'utiliser un script plutôt qu'une commande simple.
- Question 3 : Installation de l'architecture : Nous allons mettre en place un serveur Active Directory principal et un serveur Active Directory secondaire pour assurer la redondance du service. Nous allons expliquer pourquoi cette redondance est importante et comment l'organiser sur notre infrastructure de virtualisation. Nous allons tester la résolution de nom de notre domaine en éteignant le serveur principal.
- Question 4 : Convaincre : Nous allons répondre à la demande du directeur qui veut être administrateur du serveur Active Directory. Nous allons accepter ou refuser sa demande, en justifiant notre choix avec des arguments techniques et éthiques.
- Question 5 : Adressage automatique : Nous allons installer et configurer un serveur DHCP en PowerShell, puis en interface graphique. Nous allons créer des étendues pour définir les plages d'adresses IP à attribuer aux machines du réseau. Nous allons installer un poste et vérifier qu'il reçoit une adresse IP du serveur DHCP. Nous allons joindre ce poste au domaine et l'utiliser comme poste d'administration.
- Question 6 : Un peu d'imagination : Nous allons proposer des solutions pour sécuriser les accès à nos serveurs AD, en tenant compte des aspects réseau et protocole.

Réponse à la question 1 :

Le schéma ci-dessous, réalisé par Cisco Packet Tracer, représente une infrastructure réseau composée de trois zones : la zone DMZ, la zone des serveurs internes et la zone des postes. La zone DMZ contient deux serveurs qui offrent des services externes, comme le web ou le mail, à travers l'internet. La zone des serveurs internes contient cinq serveurs qui stockent des bases de données internes, comme les données clients ou les données comptables. La zone des postes contient trente postes ou PC qui sont utilisés par les employés du réseau. Chaque switch peut connecter seize PC au maximum, donc la zone des postes est divisée en deux parties de quinze postes chacune. Toutes les zones sont reliées à un pare-feu qui assure la sécurité du réseau et qui régule les échanges de données entre les zones.

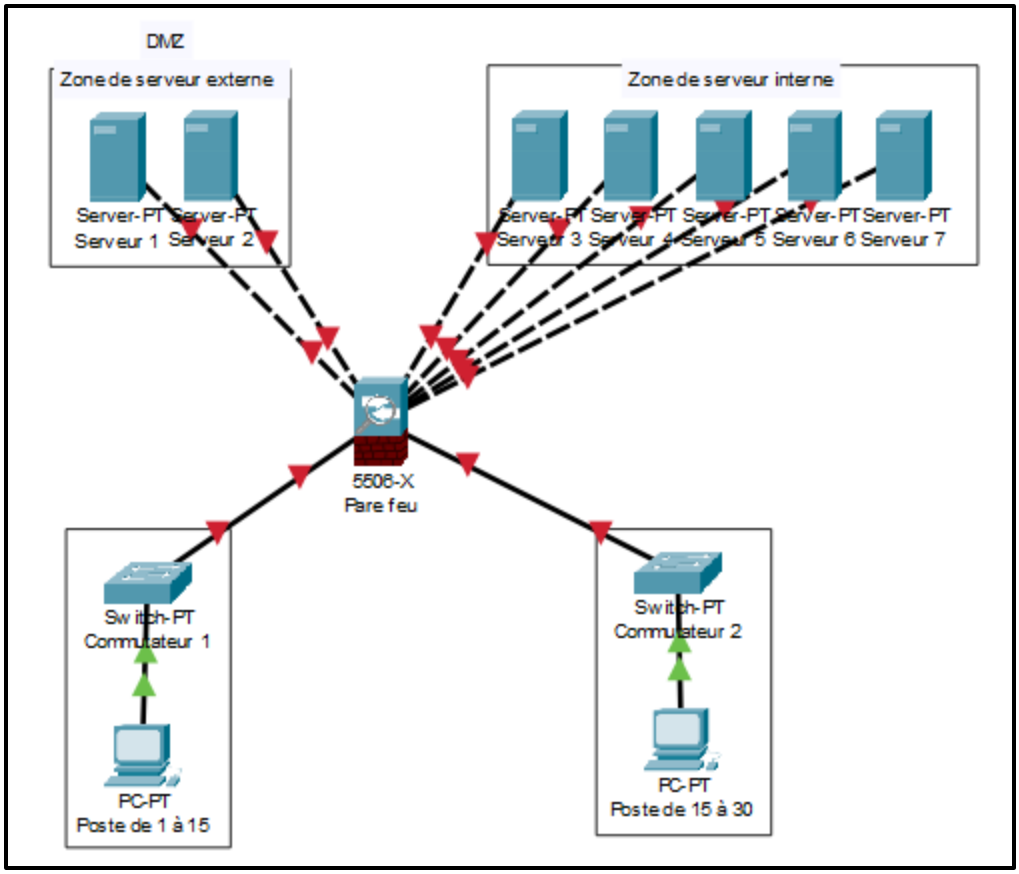


Figure 1 : Schéma de l'infrastructure de notre réseau.

Réponse à la question 2 :

Tout d'abord, nous avons utilisé le logiciel VirtualBox pour créer des machines virtuelles sur lesquelles nous avons installé Windows Server avec l'interface graphique. Nous avons créé trois machines virtuelles : ChehabDomain qui est le contrôleur de domaine principal, ChehabBackup qui est le contrôleur de domaine secondaire et ChehabClient1 qui est un domaine avec une machine cliente. ChehabDomain est responsable de la création et de la gestion du domaine Active Directory, des utilisateurs, des groupes, des objets, des stratégies, etc. Il est aussi le serveur DNS principal, qui permet de résoudre les noms de domaine en adresses IP. ChehabBackup est une copie du contrôleur de domaine principal, qui assure la redondance et la disponibilité du service Active Directory en cas de panne ou de déconnexion du contrôleur principal. Il est aussi le serveur DNS secondaire, qui prend le relais du serveur DNS principal si besoin. ChehabClient1 représente un ordinateur d'un utilisateur qui appartient au domaine Active Directory et elle peut se connecter au domaine avec un compte utilisateur et bénéficier des services et des ressources du réseau. Elle peut aussi communiquer avec les autres machines du domaine grâce au service DNS.

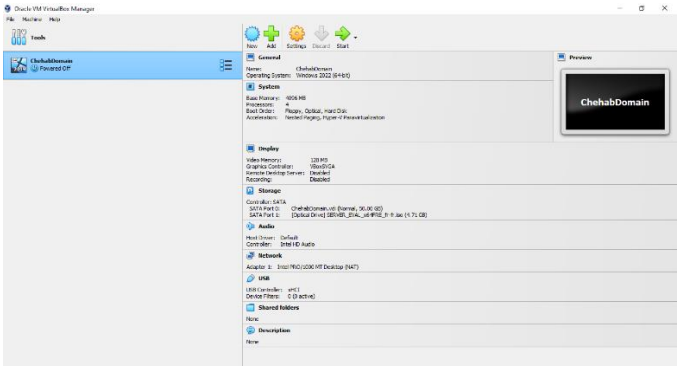


Figure 2 : Création de la machine virtuelle ChehabDomain sur le logiciel VirtualBox.

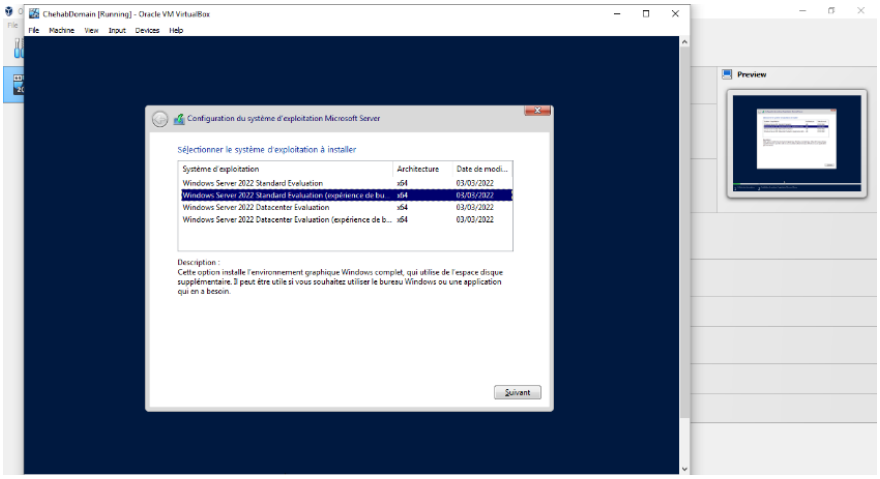


Figure 3 : Choisissons d'installer Windows Server avec l'interface graphique.

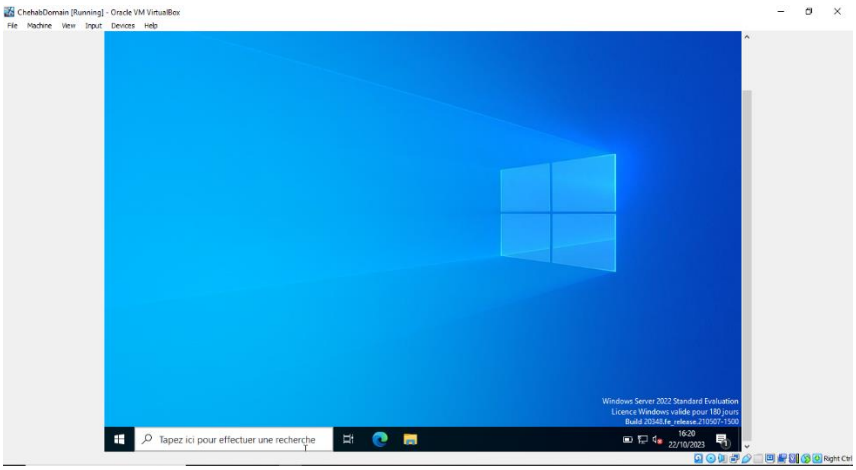


Figure 4 : Page d'accueil de la machine virtuelle ChehabDomain après l'installation de Windows.

Après avoir créé les trois machines virtuelles sur VirtualBox, nous avons décidé de les copier au format VHD pour pouvoir les importer sur Hyper-V. Hyper-V est une solution de virtualisation intégrée à Windows 10 Pro qui offre plus de performances et de fonctionnalités que VirtualBox.

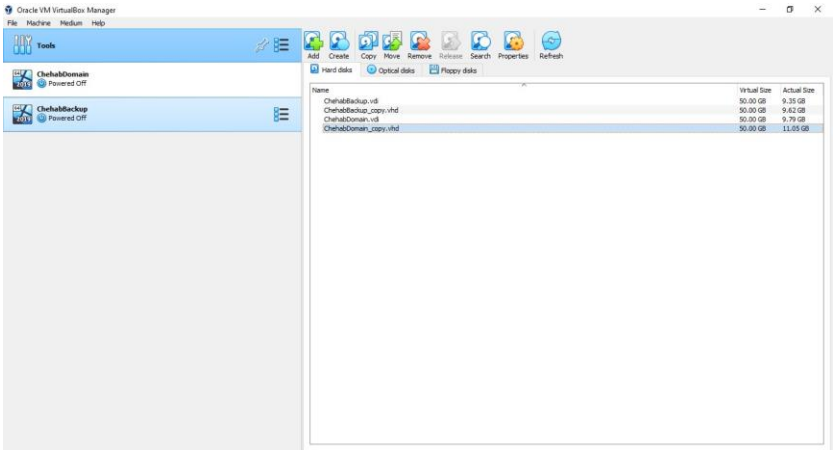


Figure 5 : Conversion des machines virtuelles au format VHD.

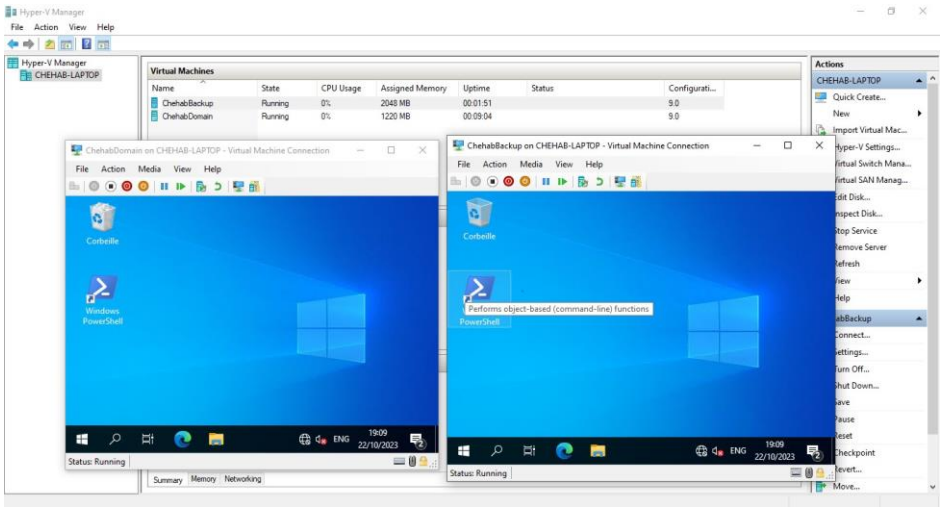


Figure 6 : L'importation des machines virtuelles en Hyper-V avec succès.

Avant d'installer l'active directory sur ChehabDomain, nous avons dû modifier le nom du PC en DC pour indiquer qu'il s'agit d'un contrôleur de domaine. Ensuite, nous avons dû changer l'adresse IP du PC et ne pas laisser le système choisir une adresse automatique. Pour connaître l'adresse de la passerelle par défaut, nous avons utilisé la commande PowerShell ipconfig, qui affiche les informations sur la configuration réseau. Puis, nous avons ouvert l'interface graphique des paramètres Ethernet et nous avons modifié l'adresse IP et le serveur DNS en fonction de la passerelle. Ces étapes sont nécessaires pour configurer correctement le réseau et le service DNS. Puis nous avons redémarré la machine ChehabDomain pour appliquer les modifications.

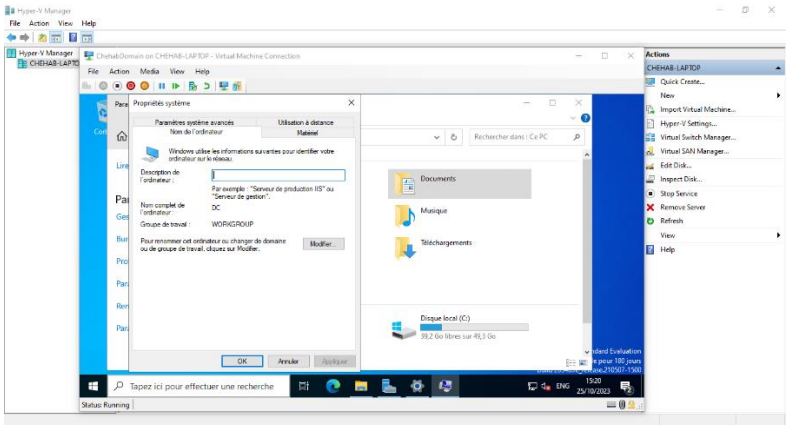


Figure 7 : Changement du nom du PC.

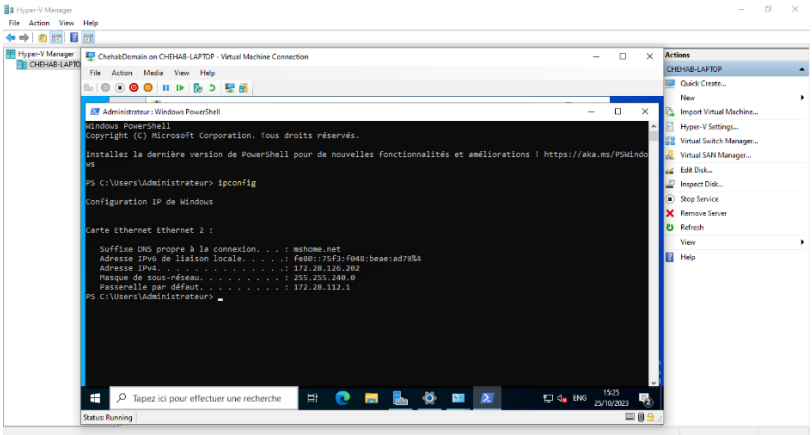


Figure 8 : La commande PowerShell ipconfig qui affiche les informations sur la configuration réseau.

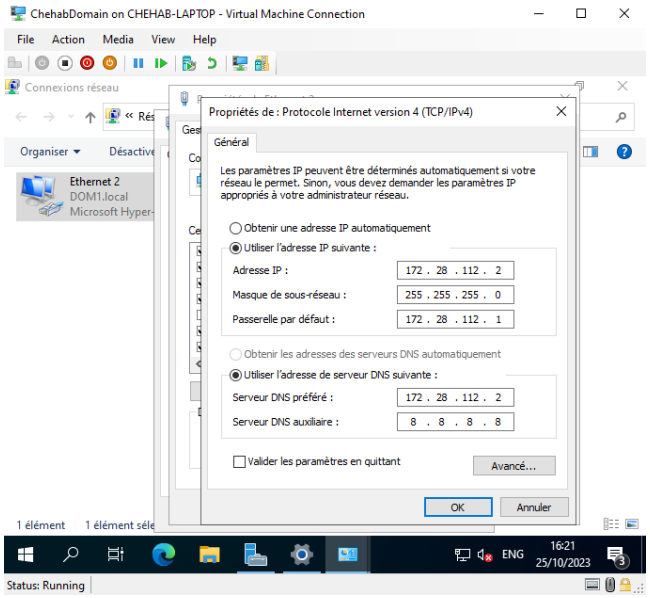


Figure 9 : Modification de l'adresse IP et du serveur DNS en fonction de la passerelle.

Nous avons ensuite créé un script à l'aide du PowerShell ISE, qui est un environnement graphique pour écrire et exécuter des scripts PowerShell1. Mon script contient deux commandes, la première commande est « Add-windowsfeature AD-domain-services » qui permet d'installer le rôle Active Directory Domain Services, qui est nécessaire pour créer un contrôleur de domaine. La deuxième commande est « Install-ADDSForest -DomainName "DOM1.local" -DomainNetBiosName "DOM1" -InstallDns:$true -NoRebootOnCompletion:$true » qui permet de créer une nouvelle forêt et un nouveau domaine Active Directory avec les noms spécifiés, d'installer le service DNS (Domain Name System) et de ne pas redémarrer le serveur à la fin de l'installation. Nous avons exécuté ce script en cliquant sur le bouton Exécuter le script dans la barre d'outils du PowerShell ISE. Ces deux commandes permettent de pouvoir automatiser la création d'un contrôleur de domaine avec les paramètres souhaités, sans avoir à passer par l'interface graphique du Gestionnaire de serveur.

L'intérêt d'un script plutôt que d'exécuter simplement la commande est de pouvoir automatiser l'installation et la configuration de l'active directory, sans avoir à saisir manuellement les paramètres à chaque fois. Un script permet également de documenter les étapes effectuées et de les reproduire facilement sur d'autres serveurs. En plus, un script peut être intégré à des outils d'automatisation comme PowerShell DSC ou Ansible pour déployer des contrôleurs de domaine de manière cohérente et standardisée.

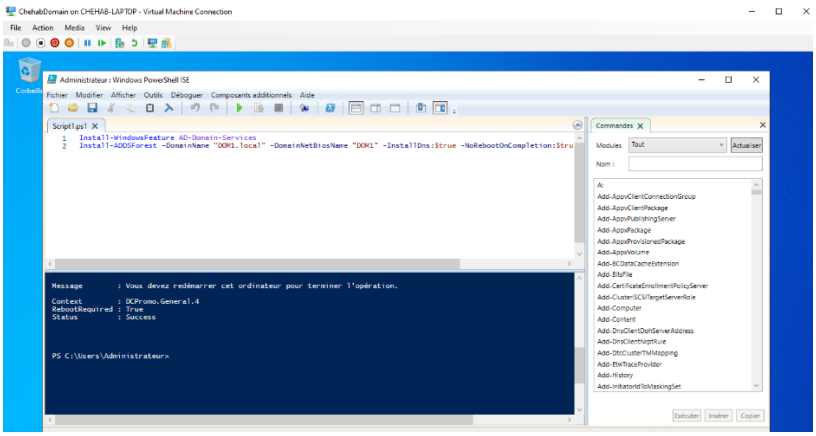


Figure 10 : Le script est exécuté avec succès.

Réponse à la question 3 :

Tout d'abord, dans la machine virtuelle ChehabBackup, nous avons dû modifier le nom du PC en ADC et nous avons modifié l'adresse IP et le serveur DNS en fonction de la passerelle et de l'adresse IP du serveur principal ChehabDomain.

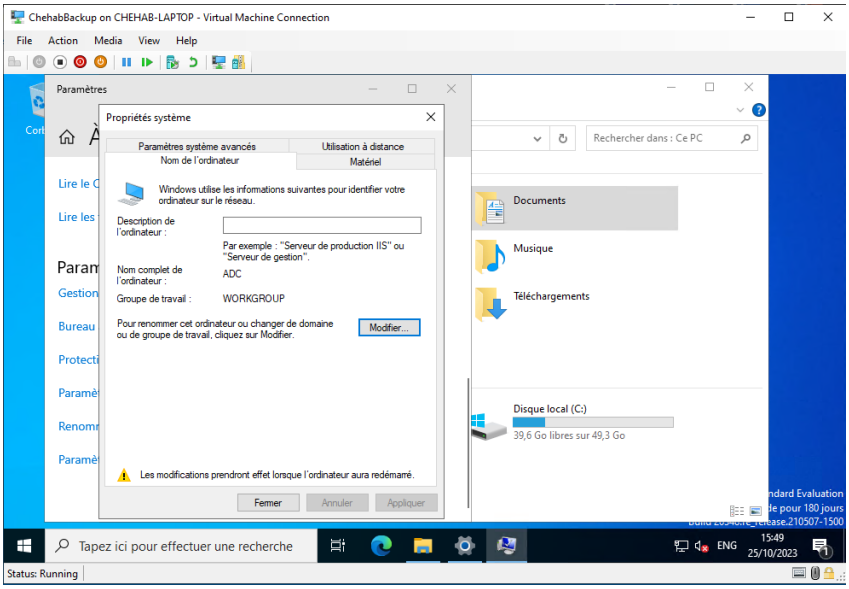


Figure 11 : Changement du nom du PC.

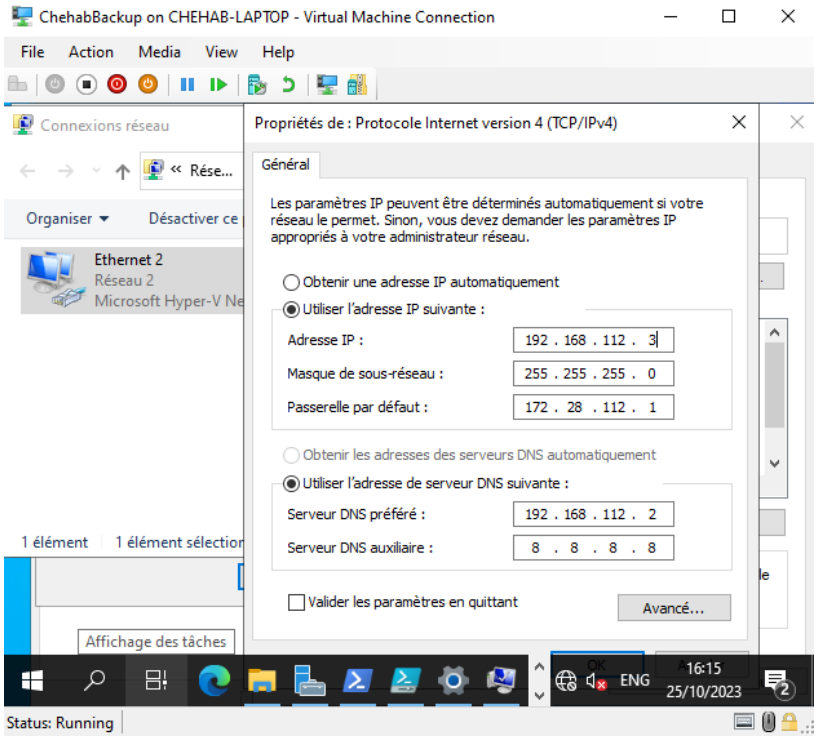


Figure 12 : Modification de l'adresse IP et du serveur DNS.

Nous avons créé ensuite un script sur la machine ChehabBackup avec le PowerShell ISE. Mon script contient deux commandes : La première commande est « Add-windowsfeature AD-domain-services » permet d'installer le rôle Active Directory Domain Services, qui est requis pour devenir un contrôleur de domaine. Et la deuxième commande est « Install-ADDSDomainController -DomainName "DOM1.local" -Credential (Get-Credential

"DOM1\administrateur") » qui permet d'ajouter la machine ChehabBackup comme un contrôleur de domaine secondaire du domaine DOM1.local, en utilisant les identifiants de l'administrateur du domaine.
L'intérêt de ces deux commandes est de pouvoir configurer la machine ChehabBackup comme une redondance du serveur principal ChehabDomain.

L'importance de cette redondance est de garantir la disponibilité et la fiabilité des services Active Directory, qui sont essentiels pour l'authentification, l'autorisation et la gestion des objets du réseau. En ayant deux contrôleurs de domaine, nous évitons le risque de perdre les données du domaine en cas de défaillance du serveur principal, et nous permettons aux utilisateurs et aux machines de se connecter au domaine même si le serveur principal est hors ligne.

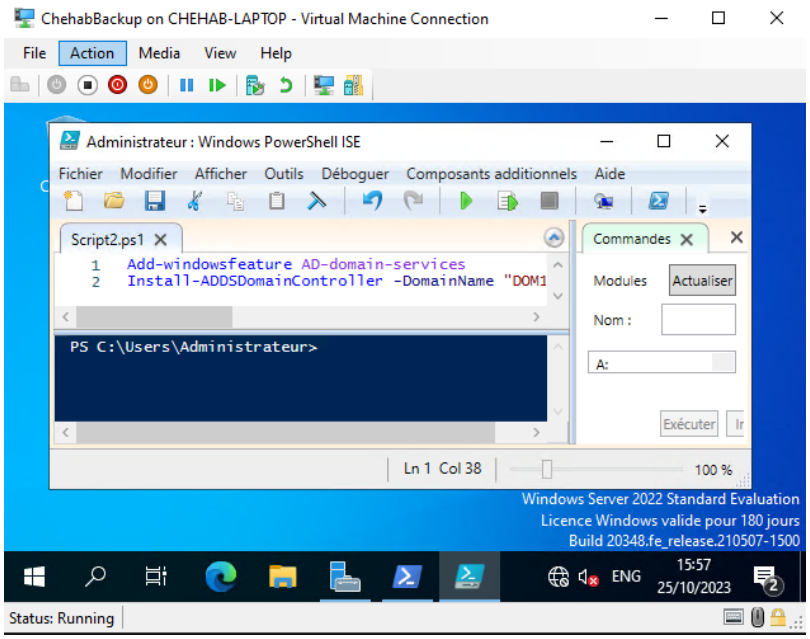


Figure 13 : Le script qui configure la machine ChehabBackup comme une redondance du serveur principal.

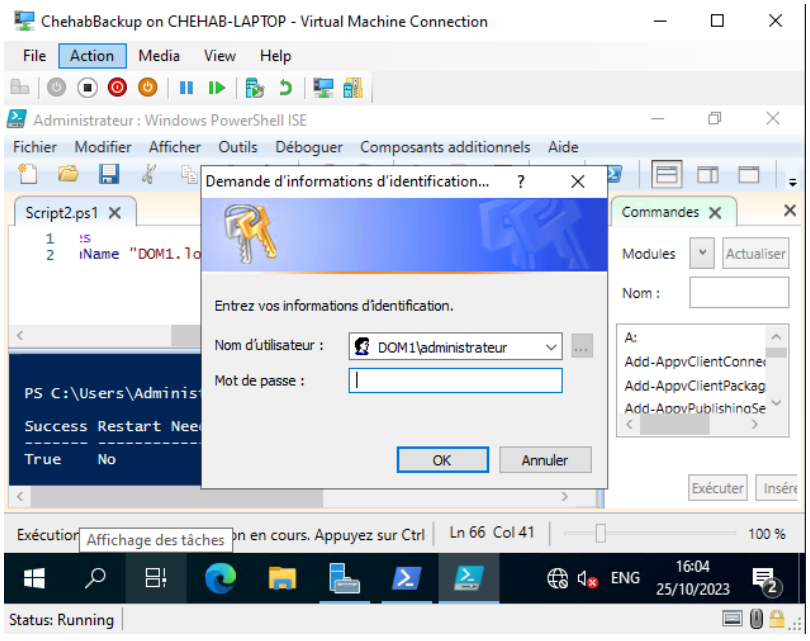


Figure 14 : Demande d'identification du serveur principal pour être un contrôleur secondaire de domaine.

Pour organiser notre infrastructure de virtualisation, nous avons utilisé la technologie Hyper-V qui est intégrée à Windows Server 2022. Hyper-V nous permet de créer et de gérer des machines virtuelles sur lesquelles nous pouvons installer nos contrôleurs de domaine. Nous pouvons également créer un cluster Hyper-V qui regroupe plusieurs serveurs physiques en une seule entité logique. Un cluster Hyper-V nous permet de bénéficier d'une haute disponibilité, d'une répartition de charge et d'une tolérance aux pannes pour nos machines virtuelles.

Si nous éteignons notre serveur principal, nous devrions pouvoir tester la résolution de nom de notre domaine en utilisant le serveur secondaire comme serveur DNS. En effet, les contrôleurs de domaine sont également des serveurs DNS qui hébergent les zones du domaine Active Directory. Ces zones sont répliquées entre les contrôleurs de domaine du même domaine, ce qui assure la cohérence des données DNS. Nous pouvons utiliser la commande « nslookup » pour vérifier la résolution de nom de notre domaine.

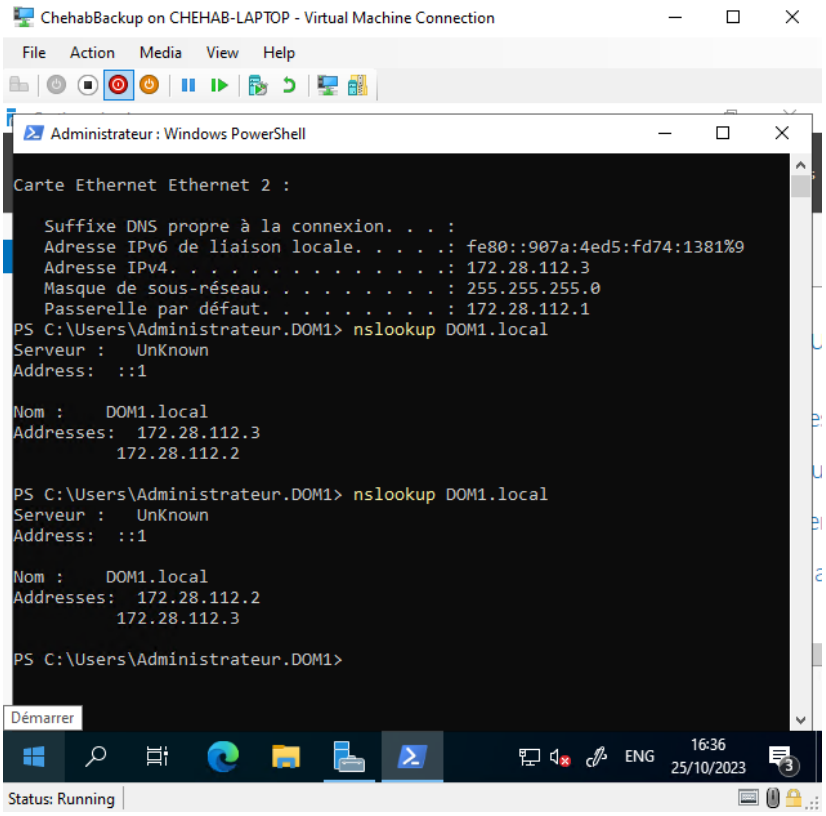


Figure 15 : La commande nslookup qui vérifie le fonctionnement du service DNS et de la redondance.

Dans l'image ci-dessus, nous avons exécuté la commande nslookup deux fois sur la machine ChehabBackup.
La première fois, le serveur DNS utilisé est 172.28.112.2, qui est l'adresse de ChehabDomain. Cela signifie que le serveur DNS fonctionne correctement et qu'il connaît le nom du contrôleur de domaine principal.
La deuxième fois, le serveur DNS utilisé est 172.28.112.3, qui est l'adresse locale de ChehabBackup. Cela signifie que le serveur DNS ne peut pas résoudre le nom du contrôleur de domaine principal, parce qu'il est éteint.

En déduisant, nous pouvons constater que la redondance des contrôleurs de domaine nous permet de maintenir le fonctionnement des services Active Directory et DNS même si le serveur principal est éteint. Cela montre l'intérêt d'avoir au moins deux contrôleurs de domaine dans un domaine Active Directory.

Réponse à la question 4 :

En effet, nous allons refuser la demande du directeur et les étapes de notre démarche sont les suivantes :

- Nous devons justifier notre refus en invoquant des raisons objectives et fondées, comme la politique de sécurité de l'entreprise, la séparation des rôles et des responsabilités, ou la complexité et la sensibilité du serveur Active Directory. Nous devons lui expliquer les risques et les conséquences d'une mauvaise administration du serveur Active Directory, qui peuvent affecter la disponibilité, la performance et l'intégrité du réseau et des données.
- Nous devons proposer au directeur des alternatives pour répondre à ses besoins, sans lui accorder le rôle d'administrateur. Par exemple, nous pouvons lui créer un compte d'utilisateur avec des droits et des autorisations limités à certaines ressources ou tâches spécifiques. Nous pouvons également lui déléguer certaines fonctions administratives à travers des outils ou des interfaces adaptés. Nous pouvons aussi lui offrir un accès en lecture seule au serveur Active Directory, pour qu'il puisse consulter les informations sans pouvoir les modifier.
- Nous devons négocier avec le directeur un compromis acceptable pour les deux parties, en tenant compte de ses attentes et de nos contraintes. Nous devons établir un dialogue constructif et respectueux, basé sur la confiance et la transparence. Nous devons également nous engager à assurer un service de qualité et à répondre à ses demandes dans les meilleurs délais.

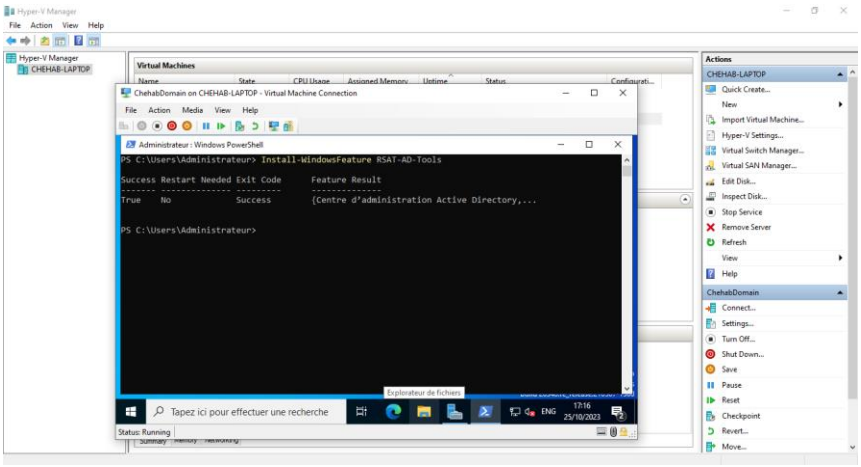
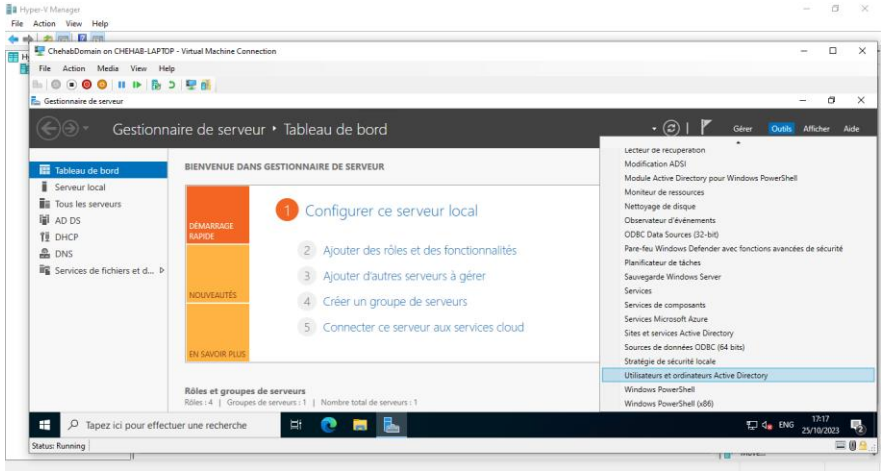


Figure 16 : Installation des outils d'active directory sur PowerShell pour créer des utilisateurs.



:

Figure 17 : Utilisons le gestionnaire de reseau pour créer un nouveau utilisateur pour le directeur.

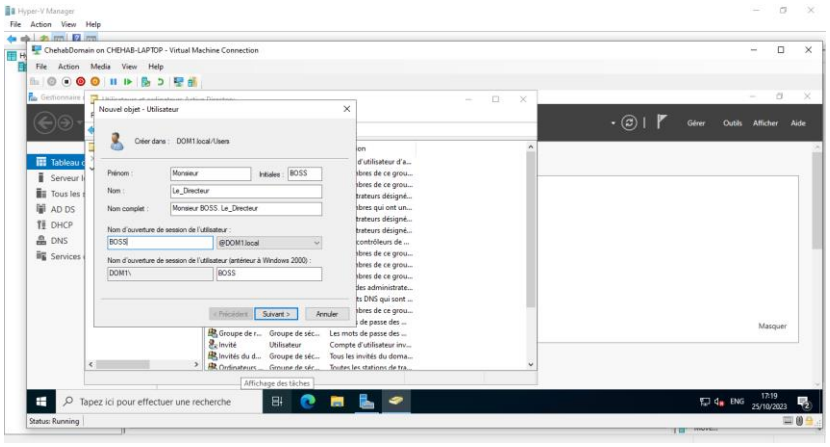


Figure 18 : Créons-le nouvel utilisateur.

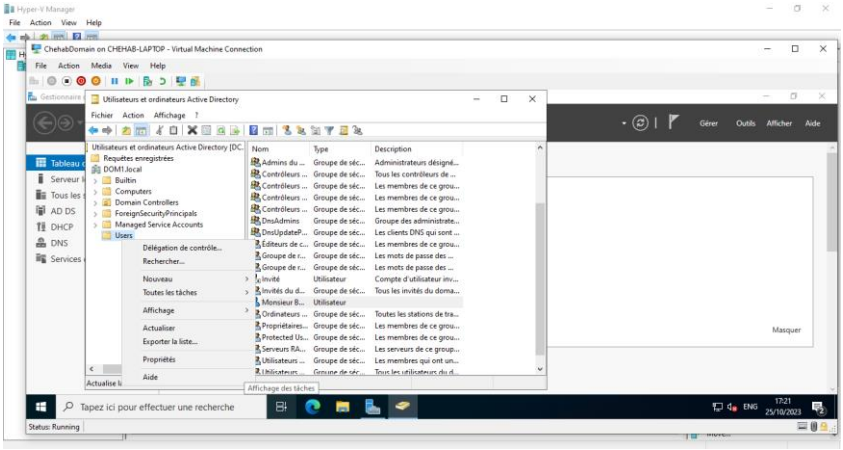


Figure 19 : Choisissons « Délégation de contrôle » pour privilégier le directeur.

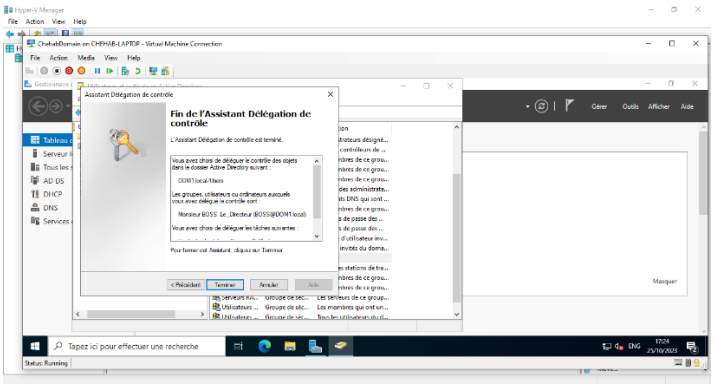


Figure 20 : Le directeur maintenant possède certaines autorisations.

Alors que si le directeur fournit les documents nécessaires pour approuver sa demande, il faut être conscient des risques et des responsabilités liés à ce rôle, qui implique un accès privilégié à l'ensemble du domaine et à ses objets. Alors les étapes de notre démarche sont les suivantes :

- Nous devons informer le directeur des implications de son rôle d'administrateur, notamment en termes de sécurité, de conformité et de bonnes pratiques. Nous devons lui expliquer les tâches qu'il peut effectuer avec ce rôle, mais aussi les précautions qu'il doit prendre pour éviter de compromettre le serveur Active Directory ou de causer des dommages involontaires aux objets du domaine.

- Nous devons lui fournir une documentation sur l'utilisation et la gestion du serveur Active Directory, ainsi que sur les outils et les commandes disponibles. Nous devons également lui indiquer les sources d'information et de support auxquelles il peut se référer en cas de besoin.
- Nous devons lui créer un compte d'utilisateur dans le domaine, avec un nom distinct du compte Administrateur intégré. Nous devons lui attribuer un mot de passe complexe et sécurisé, et lui demander de le changer régulièrement. Nous devons également lui imposer l'utilisation d'une carte à puce pour ouvrir une session interactive sur le serveur Active Directory, afin de renforcer l'authentification et de limiter les risques de vol ou de perte des informations d'identification.
- Nous devons ajouter son compte d'utilisateur au groupe Administrateurs du domaine, qui lui confère les droits et les autorisations nécessaires pour administrer le serveur Active Directory. Nous devons également vérifier que son compte n'est pas membre d'autres groupes qui pourraient entrer en conflit ou réduire ses privilèges.
- Nous devons auditer régulièrement les actions du directeur sur le serveur Active Directory, en utilisant les journaux d'événements, les rapports d'activité ou les outils de surveillance. Nous devons également lui demander de nous informer de toute modification ou anomalie qu'il constate ou qu'il effectue sur le serveur Active Directory.

Réponse à la question 5 :

Dans cette partie, nous avons allons installer et configurer un serveur DHCP (Dynamic Host Configuration Protocol) avec PowerShell et l'interface graphique. Le serveur DHCP permet d'attribuer automatiquement des adresses IP et des options DHCP aux clients DHCP connectés au réseau. Nous avons utilisé le serveur principal ChehabDomain comme serveur DHCP et le poste ChehabClient1 comme client DHCP pour tester le fonctionnement du service. Nous avons également rejoint le domaine DOM1.local avec le poste ChehabClient1.

Pour installer le serveur DHCP avec PowerShell sur le serveur ChehabDomain, nous avons ouvert une fenêtre PowerShell en tant qu'administrateur et nous avons exécuté la commande « Install-WindowsFeature DHCP -IncludeManagementTools » pour installer le rôle Serveur DHCP et les outils de gestion. Puis pour configurer les étendues DHCP avec l'interface graphique sur le serveur ChehabDomain, nous avons ouvert le Gestionnaire de réseau, qui est l'outil graphique pour gérer le service DHCP. Nous avons cliqué avec le bouton droit sur IPv4 et nous avons choisi Nouvelle étendue. Ensuite, nous avons suivi l'Assistant Nouvelle étendue pour créer une étendue nommée Client1, avec une plage d'adresses IP allant de 172.28.112.5 à 172.28.112.100, un masque de sous-réseau de 255.255.255.0, une durée de bail de 1 journée, une passerelle par défaut de 172.28.112.1 et un serveur DNS de 172.28.112.2 et nous avons activé l'étendue à la fin de l'assistant.

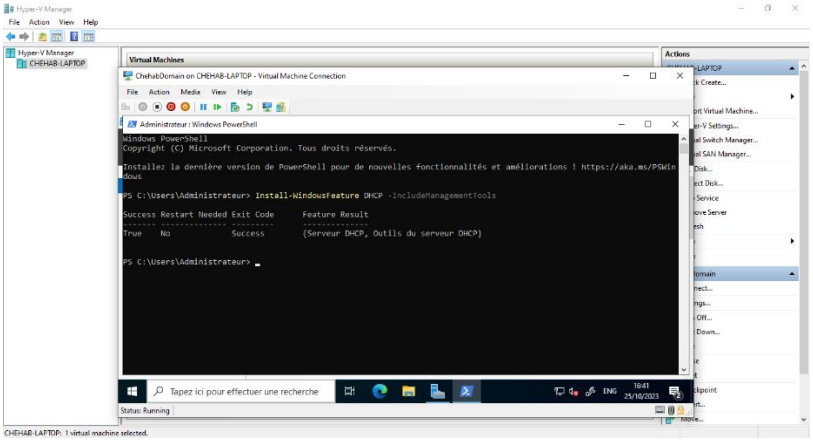


Figure 21 : Installation du rôle Serveur DHCP.

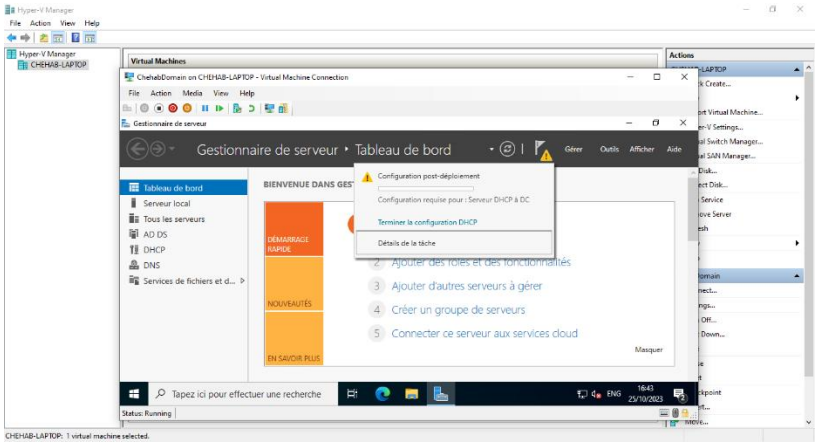


Figure 22 : Terminaison de la configuration DHCP sur le Gestionnaire de réseau.

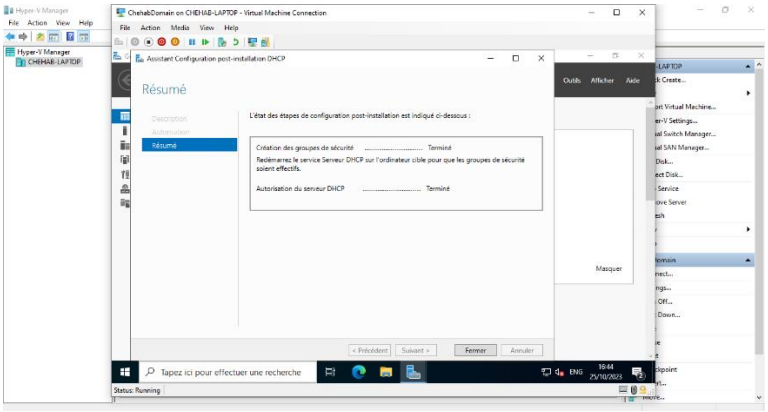


Figure 23 : Configuration DHCP terminé avec succès.

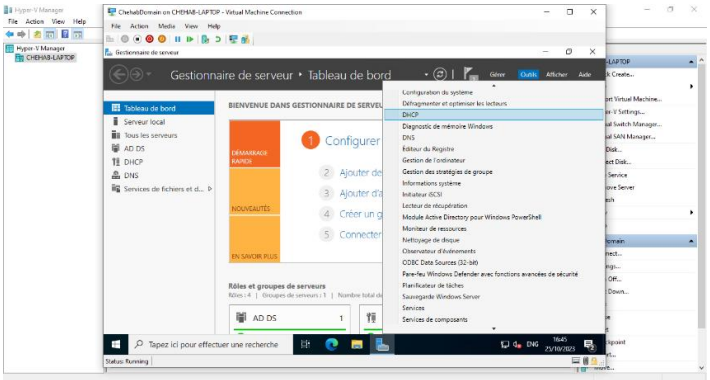


Figure 24 : Choisissons DHCP d'après les outils pour créer l'étendue.

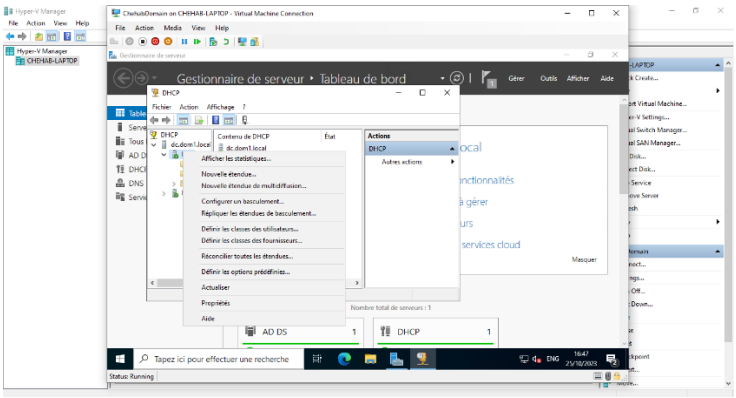


Figure 25 : Cliquons avec le bouton droit sur IPv4 et nous avons choisi Nouvelle étendue

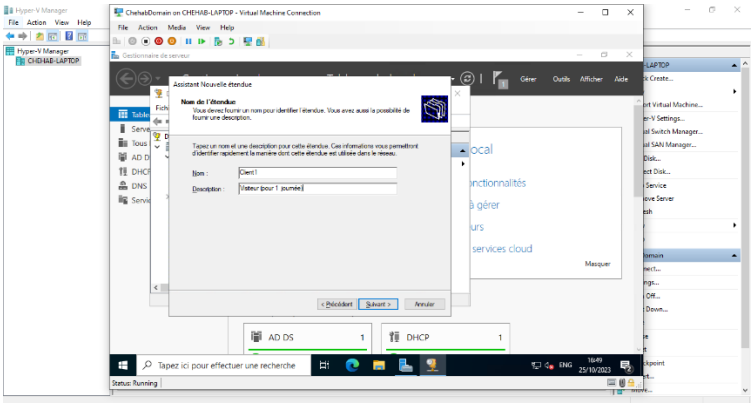


Figure 26 : Créons une étendue nommée Client1.

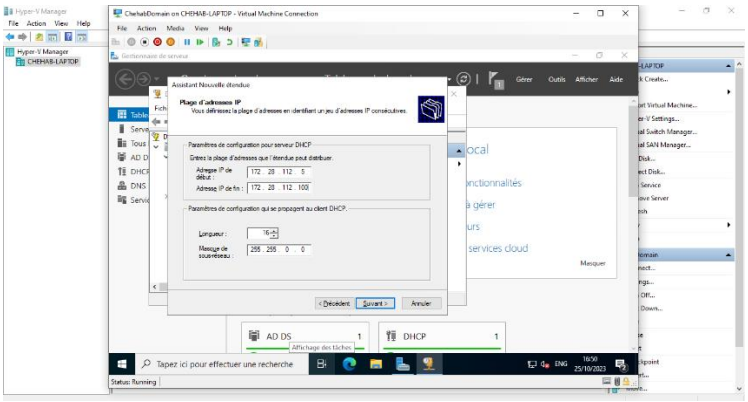


Figure 27 : Choisissons une plage d'adresses IP allant de 172.28.112.5 à 172.28.112.100.

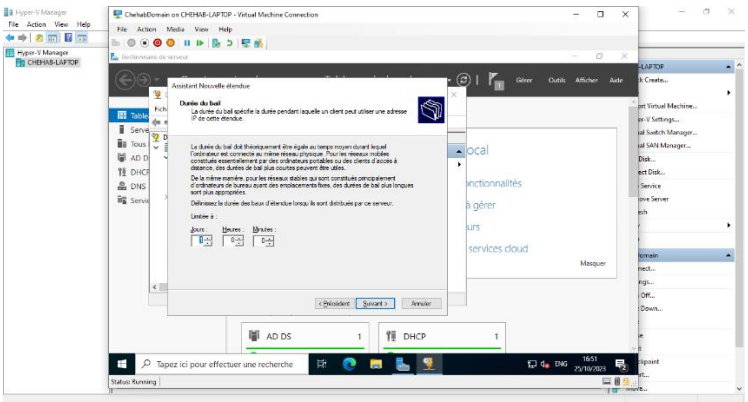


Figure 28 : Choisissons la durée de bail de 1 journée.

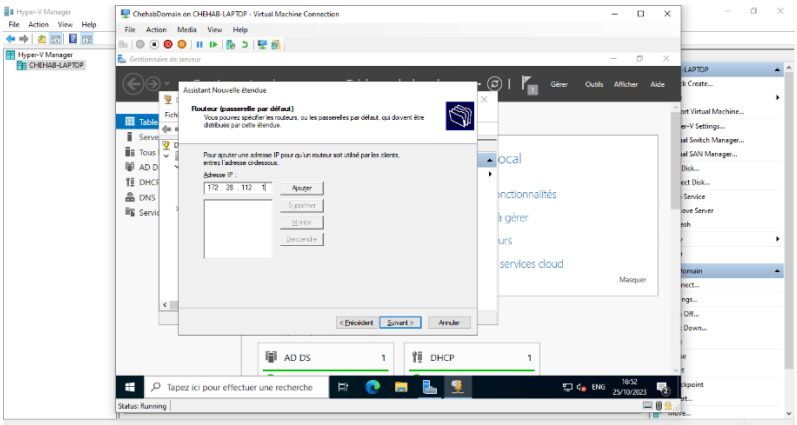


Figure 29 : Choisissons la passerelle par défaut de 172.28.112.1.

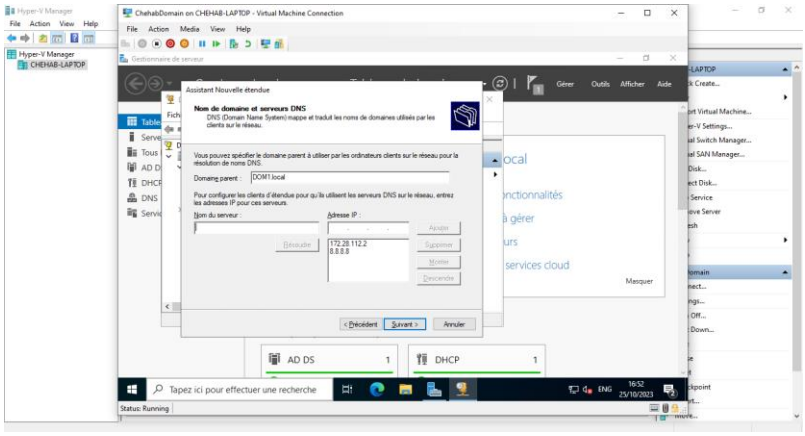


Figure 30 : Choisissons le serveur DNS principal de la machine ChehabDomain.

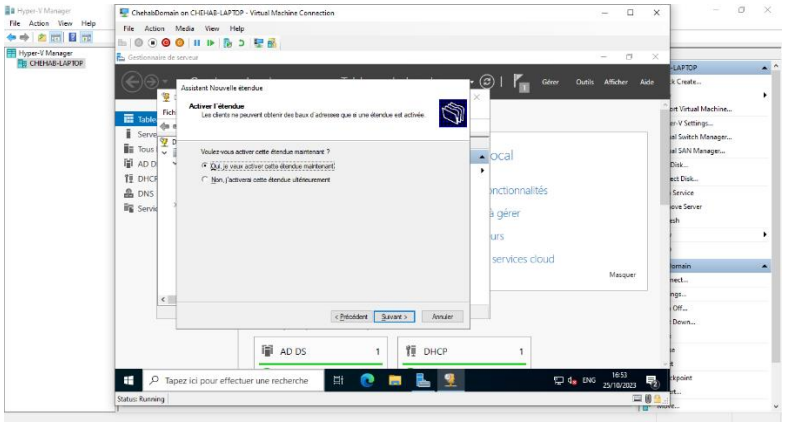


Figure 31 : Activation de l'étendue maintenant.

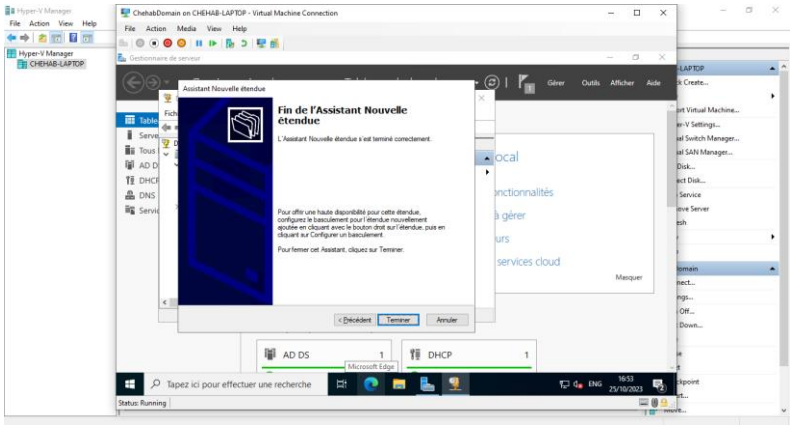


Figure 32 : Création de l'étendue avec succès.

Pour tester le serveur DHCP avec un poste client sur le poste ChehabClient1, nous avons ouvert les paramètres Ethernet et nous avons modifié le serveur DNS préféré et nous avons mis l'adresse IP du serveur principal ChehabDomain. Nous avons ensuite rejoint le domaine DOM1.local à partir des paramètres avancés. Puis nous avons redémarré le poste ChehabClient1 pour appliquer les modifications. Sur le poste ChehabClient1, nous avons ouvert une fenêtre PowerShell et nous avons exécuté la commande « ipconfig » pour vérifier les informations de configuration réseau. Nous avons constaté que le poste avait reçu une adresse IP de la plage du serveur DHCP ChehabDomain, il a reçu l'adresse 172.28.112.5.

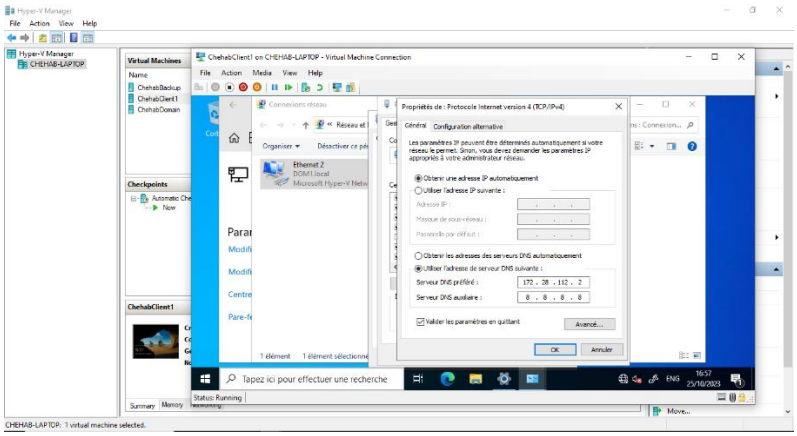


Figure 33 : Modification du serveur DNS préféré sur la machine ChehabClient1.

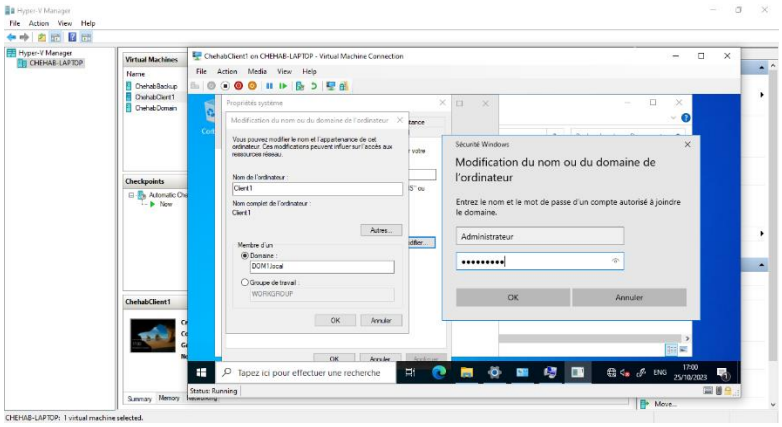


Figure 34 : Demande de l'accès au domaine DOM1.local lors du changement du domaine de la machine cliente.

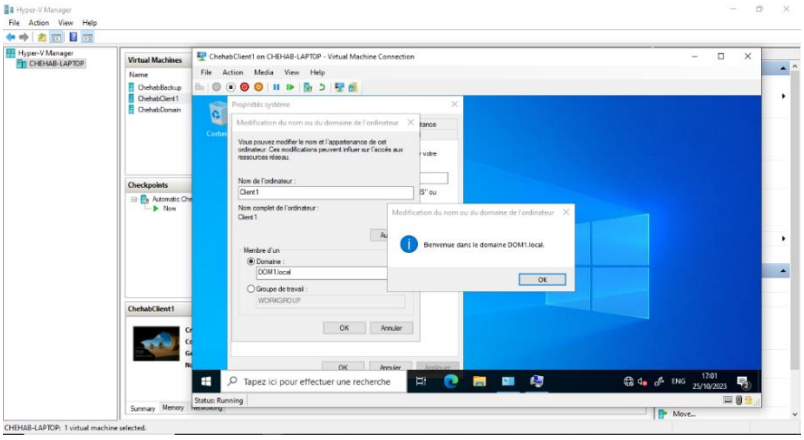


Figure 35 : Succès du changement du domaine.

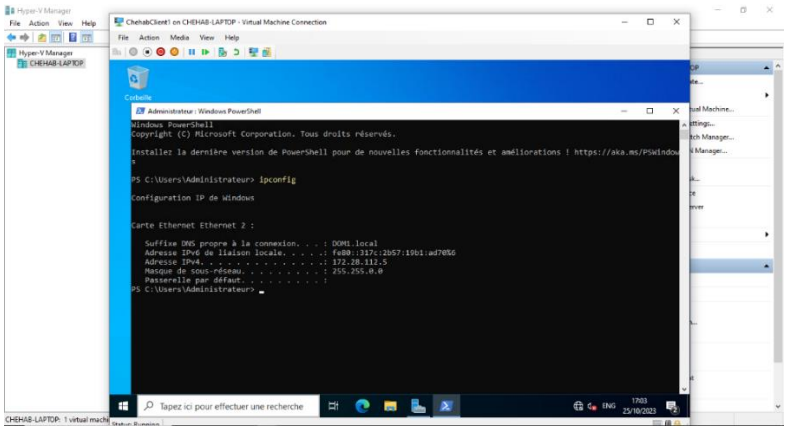


Figure 36 : Vérification de la configuration réseau et que l'adresse IP appartient à la plage correcte.

Nous avons vu comment installer et configurer un serveur DHCP avec PowerShell et l'interface graphique sur Windows Server 2022. Nous avons créé une étendue DHCP pour attribuer des adresses IP aux clients DHCP sur un sous-réseau local. Nous avons utilisé un poste client pour tester le service DHCP et pour rejoindre le domaine Active Directory.

Réponse à la question 6 :

Pour sécuriser les accès à nos serveurs Active Directory, nous pouvons mettre en place les mesures suivantes :

- Au niveau du réseau : nous pouvons utiliser un réseau dédié et isolé pour les opérations d'administration des serveurs AD, afin de limiter les risques d'interception ou d'altération des données. Nous pouvons également utiliser des technologies de chiffrement et de signature, comme IPsec ou SSL/TLS, pour protéger les communications entre les serveurs AD et les clients.
- Au niveau du protocole d'accès : nous pouvons utiliser un protocole d'accès qui assure une authentification forte et une autorisation granulaire des utilisateurs, comme Kerberos ou LDAP. Nous pouvons également activer le mode LDAP sécurisé (LDAPS) pour chiffrer les requêtes LDAP entre les serveurs AD et les clients.
- Au niveau des comptes : nous pouvons appliquer des règles de sécurité strictes sur les comptes qui ont accès aux serveurs AD, comme changer régulièrement le mot de passe, utiliser un mot de passe complexe et sécurisé, limiter le nombre de tentatives de connexion et verrouiller le compte en cas d'échec. Nous pouvons également utiliser des comptes de moindres privilèges pour les opérations courantes, et réserver les comptes privilégiés comme administrateurs du domaine pour les opérations sensibles.

Conclusion :

En conclusion, ce TP nous a permis de mettre en pratique nos connaissances sur l'Active Directory et les services associés. Nous avons appris à :

1. Concevoir un schéma logique et physique de notre réseau.
2. Utiliser PowerShell pour automatiser l'installation et la configuration de l'Active Directory.
3. Mettre en place une redondance du contrôleur de domaine pour assurer la disponibilité et la fiabilité du service.
4. Gérer les droits d'accès et les rôles des utilisateurs, notamment le directeur qui demande à être administrateur du serveur Active Directory.
5. Installer et configurer un serveur DHCP pour attribuer des adresses IP dynamiques aux machines du réseau.
6. Joindre une machine au domaine et l'utiliser comme poste d'administration.
7. Réfléchir aux mesures de sécurité à mettre en place pour protéger les accès aux serveurs AD.

Ce TP nous a également permis de développer notre méthodologie et notre esprit critique. Nous avons suivi les étapes du sujet en respectant les consignes et les bonnes pratiques. Nous avons testé le fonctionnement de notre infrastructure et vérifié la cohérence des résultats. Nous avons également identifié les limites et les axes d'amélioration possibles, tels que :

1. Optimiser la répartition des charges entre les serveurs AD.
2. Renforcer la sécurité du réseau par des mécanismes de chiffrement, de filtrage ou de surveillance.
3. Intégrer d'autres services numériques comme le partage de fichiers, l'impression ou la messagerie.

Pour conclure, nous pouvons dire que ce TP nous a été utile et intéressant. Tandis que, nous aurions pu réaliser ce TP en utilisant uniquement PowerShell, sans passer par l'interface graphique pour être plus familiariser avec les commandes PowerShell. Ces commandes sont plus rapides et plus pratiques que l'interface graphique, qui nécessite plus de clics et de saisies. De plus, nous aurions pu gagner du temps si nous avions créé les machines virtuelles directement sur Hyper-V, au lieu de les créer sur VirtualBox puis de les importer sur Hyper-V. Hyper-V est plus performant et plus intégré à Windows que VirtualBox, et il permet d'éviter les étapes de conversion et d'importation des fichiers VHD.

Bibliographie :

Afin de réaliser ce TP, nous avons effectué des recherches sur plusieurs sites web qui traitent le sujet de l'Active Directory et de ses aspects techniques. Nous avons utilisé des sites fiables et pertinents, dont les références sont les suivantes :

1) Comment installer et importer le module Active Directory pour PowerShell : https://www.varonis.com/fr/blog/powershell-active-directory-module
2) Automating the install of Windows Server 2022 Active Directory : https://github.com/sysadmintutorials/windows-server-2022-powershell-ad-install-config
3) Windows server 2019 Step-By-Step: Setup Active Directory environment : https://social.technet.microsoft.com/wiki/contents/articles/52765.windows-server-2019-step-by-step-setup-active-directory-environment-using-powershell.aspx
4) Cluster Hyper-V : installation et configuration - RDR-IT : https://rdr-it.com/cluster-hyper-v-installation-configuration/
5) Comment installer un serveur Active Directory (AD) - Tutos-Informatique : https://www.tutos-informatique.com/installer-active-directory/
6) Comptes Active Directory | Microsoft Learn : https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/manage/understand-default-user-accounts
7) (PDF) Mise en place d'un contrôleur de domain Active Directory sous Windows : https://www.academia.edu/43135942/Mise_en_place_dun_contr%C3%B4leur_de_domain_Active_Directory_sous_windows_serveur_pour_la_gestion_des_utilisateur_et_des_ressources_de_la_DPI_K_O_CC
8) Annexe D - Sécurisation des comptes d'administrateur intégrés : https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory
9) Installer et configurer un serveur DHCP sous Windows Server 2019 : https://www.it-connect.fr/installer-et-configurer-un-serveur-dhcp-sous-windows-server-2019/
10) Installer et configurer un serveur DHCP en PowerShell : https://wiki.jdelgado.fr/windows/server/powershell/dhcp_server/
11) Meilleures pratiques pour la sécurisation d'Active Directory : https://learn.microsoft.com/fr-fr/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
12) 8 bonnes pratiques de sécurité pour Active Directory (AD). https://www.flexsi.fr/2020/07/28/pratiques-securite-ad/