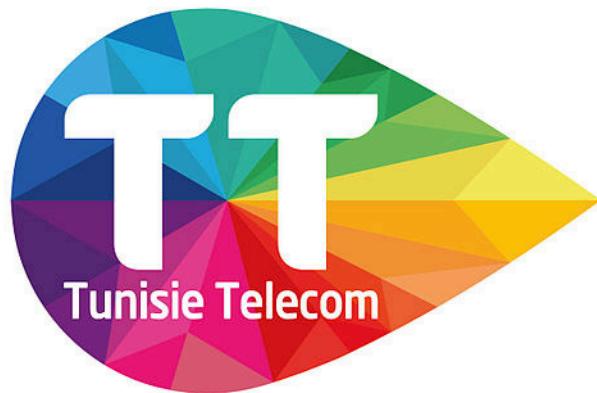




Rapport de Stage

Première Entreprise de Télécommunications en Tunisie



La vie est émotions

Période : 1 Septembre - 7 Octobre 2023

Superviseur : M. Hbib Jbir

Par : Yassin Sbaai

Table des matières

1. Remerciements
2. Introduction
3. Aperçu du stage
4. Tâches et responsabilités
 - 4.1 Activités hebdomadaires
 - 4.2 Projets clés
5. Compétences acquises
6. Défis et solutions
7. Points clés
8. Conclusion
9. Projets et flux de travail
 - 9.1 Projet d'Implémentation active directory
 - 9.2 Scripts d'automatisation
 - 9.3 Cybersecurité recherche
10. Glossaire des termes et outils

Remerciements

Je tiens à exprimer ma profonde gratitude au département IT de Tunisie Telecom, particulièrement à mon mentor **M. Hbib Jbir**, pour leurs conseils et leur soutien tout au long de ce stage. Leur expertise et leurs encouragements ont été déterminants dans mon parcours d'apprentissage.

Je souhaite également remercier mon institut I.P.S.E.T de formation pour m'avoir offert cette précieuse opportunité de stage, qui m'a permis de mettre en pratique mes connaissances théoriques et d'acquérir une expérience professionnelle enrichissante.

Introduction

Durant mon stage chez Tunisie Telecom, la première entreprise de télécommunications en Tunisie sous la tutelle du Ministère des Communications, j'ai eu l'opportunité de travailler aux côtés d'un administrateur système, M. Hbib Jbir, en tant que mentor. Cette expérience m'a permis d'acquérir des connaissances et une expérience pratique dans des domaines tels que l'Active Directory, la cybersécurité, l'architecture réseau et l'automatisation.

Aperçu du Stage

Entreprise : Tunisie Telecom

Adresse : Parc Technologique EL GHAZALA
Ariana

Département : IT

Superviseur : Mr Hbib Jbir

Durée : 5 semaines

1 Septembre 2023 - 7 Octobre 2023t

Objectifs

Comprendre les cadres opérationnels de l'administration système et du réseau dans un environnement professionnel et évaluer leurs différences entre le secteur public et privé.

Acquérir une expérience pratique avec Active Directory dans un environnement virtuel, en s'assurant que les connaissances pratiques s'alignent avec les exigences organisationnelles.

Mener des recherches et des simulations en cybersécurité et réseaux, en abordant les défis spécifiques aux opérations du secteur public.

Explorer les concepts d'automatisation de base, en mettant l'accent sur l'efficacité des tâches administratives.

Tâches et Responsabilités

Activités hebdomadaires :

Semaine 1 :

- Abordé les concepts généraux en systèmes et sécurité.
- Exploré les bonnes pratiques pour sécuriser les infrastructures IT.
- Étudié les principes fondamentaux de l'administration système

Semaine 2 :

- Concentré sur les recherches en Active Directory
- Étudié les fonctionnalités et les cas d'utilisation

Semaine 3:

- Installé Windows Server sur une machine virtuelle en utilisant VirtualBox.
- Expérimenté avec Active Directory, y compris :
 - Gestion des utilisateurs de base
 - Politiques de groupe
 - Scripts pour les tâches administratives

Semaine 4:

- Recherché les technologies VPN et leur implémentation.
- Appris à comprendre les protocoles de communication sécurisée sur le réseau

Semaine 5:

- Explorer les besoins d'automatisation en Python et les concepts.
- Engagé dans des discussions de base sur la sécurité et l'architecture système

Projets Clés :

1. Simulation Active Directory

Description : Simulé un environnement Active Directory de base en utilisant VirtualBox

Défis :

- Configuration de l'environnement virtuel
- Problèmes de compatibilité avec VirtualBox
- Configuration des rôles de Windows Server
- Gestion des politiques utilisateur et de groupe

Solutions : Résolu les problèmes de configuration grâce aux forums en ligne et aux conseils du mentor Développé une approche systématique pour la configuration des politiques

Résultat : Crée et géré correctement la simulation AD

Tools/Technologies : VirtualBox, Active Directory, Windows Server

2. Recherche en Cybersécurité :

Description : Investigation des types courants de malwares et menaces de cybersécurité

Rôle : Préparation d'un rapport complet sur l'identification et l'atténuation des menaces

Outils/Technologies : Outils de documentation et recherche en ligne

3. Simulation Réseau :

Description : Simulation d'une architecture réseau à petite échelle utilisant Cisco Packet Tracer

Rôle : Conception de la disposition du réseau et configuration du routage et de la commutation de base

Outils/Technologies : Cisco Packet Tracer

4. Recherche VPN :

Description : Recherche sur les fonctionnalités VPN et l'intégration réseau

Rôle : Documentation des résultats et configurations théoriques

5. Automatisation simple :

Description : Apprentissage des scripts Python de base pour les tâches routinières

Rôle : Pratique de l'écriture de scripts d'automatisation

Outils/Technologies : Python, PowerShell

Compétences Acquises

Compétences Techniques

Administration Système :

- Gestion de Active Directory
 - Configuration des politiques de groupe
- Scripting PowerShell

Cybersécurité :

- Compréhension des malwares et des menaces
- Stratégies de mitigation

Réseau :

- Simulation de base du réseau
 - Concepts VPN
- Résolution des problèmes en utilisant Cisco Packet Tracer

Automatisation :

- Scripting avancé en Python et PowerShell
- Surveillance des ressources système
- Test de connectivité réseau
- Gestion des comptes utilisateurs
- Surveillance de la santé du système
- Gestion des fichiers journaux et de l'espace disque

Compétences Transversales

- Amélioration des capacités de résolution des problèmes
- Renforcement de la collaboration et de la communication
- Renforcement des compétences en recherche et documentation

Défis et Solutions

Apprendre les Systèmes Complexes

Défi : Adapter à Active Directory et aux concepts de réseau

Solution : Auto-éducation avec des tutoriels et des conseils du mentor

Simuler des Scénarios Réels

Défi : Relier la connaissance théorique et l'application pratique

Solution : Utilisé VirtualBox et Cisco Packet Tracer pour la pratique

Explorer l'Automatisation

Défi : Comprendre l'automatisation en Python et PowerShell

Solution : Pratiqué avec des scripts simples et exploré des ressources en ligne

Points Clés

- Expérience pratique en administration système
- Renforcement de la compréhension de la cybersécurité
- Niveau de base en concepts de réseau
- Introduction à l'automatisation en utilisant PowerShell et Python
- Expérience en création de solutions d'automatisation réutilisables

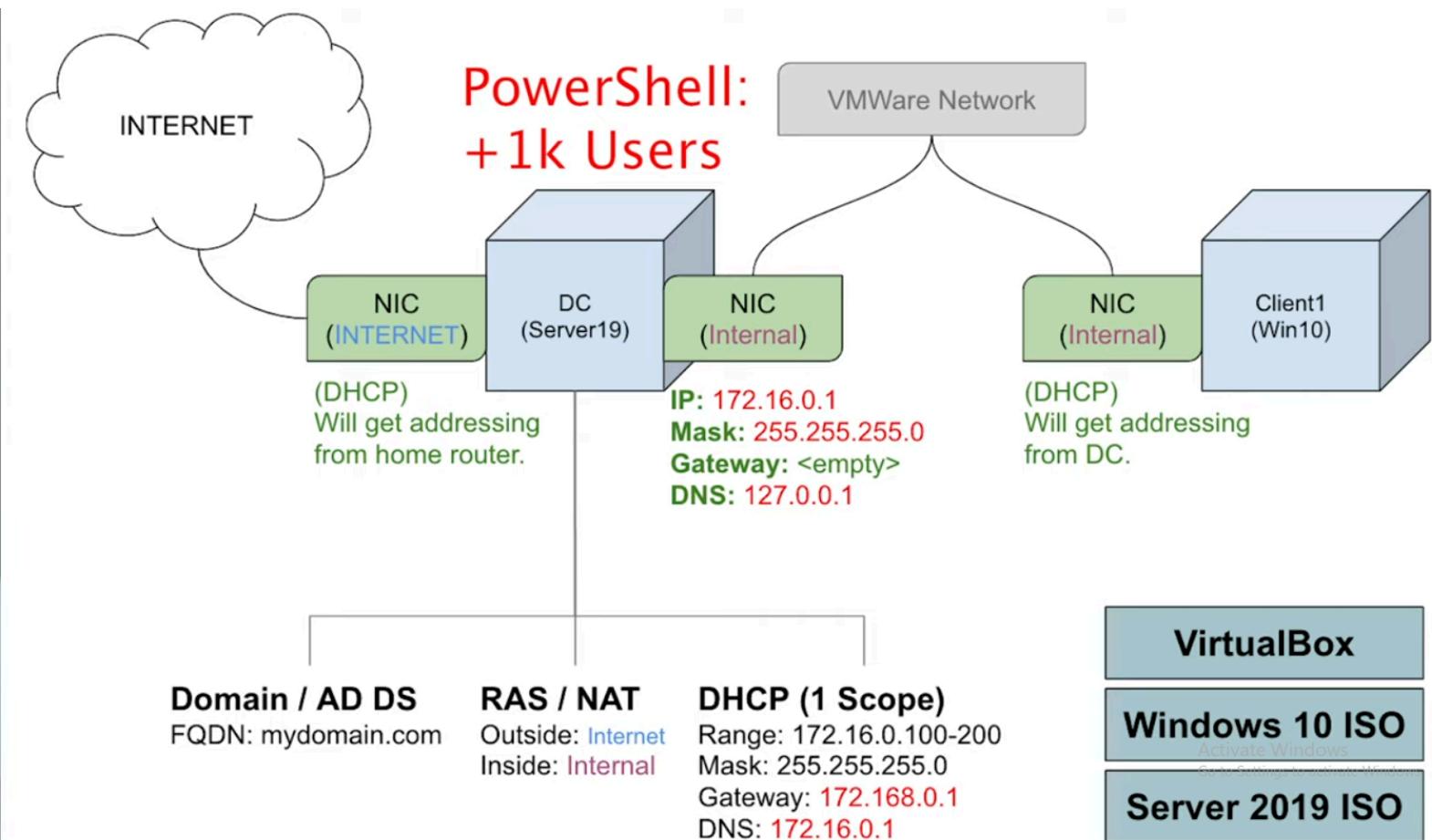
Conclusion

- Ce stage chez Tunisie Telecom a fourni une expérience précieuse dans les opérations de télécommunications gouvernementales.
- L'expérience a mis l'accent sur la conformité réglementaire, la gestion des ressources et les approches structurées pour la résolution des problèmes.
- Le développement de scripts d'automatisation pratiques a démontré la capacité de traduire la connaissance théorique en solutions concrètes.
- Le mentorat de M. Hbib Jbir et la pratique pratique ont enrichi considérablement mon expérience d'apprentissage, en me préparant pour les futurs défis dans la gestion des systèmes IT.

Projets et Flux de Travail

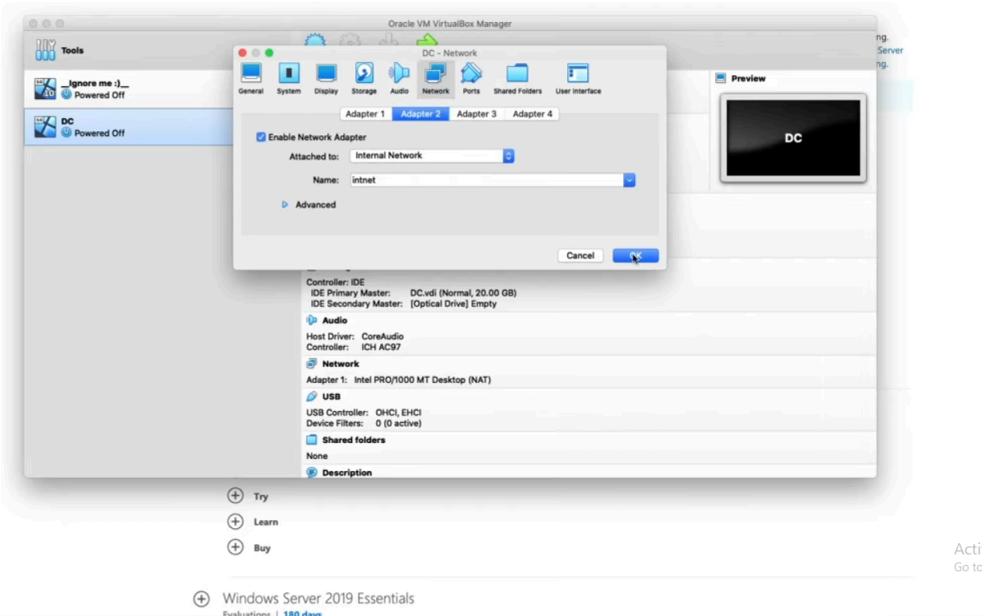
Projet d'Implémentation Active Directory

- Planification et Initialisation du Projet

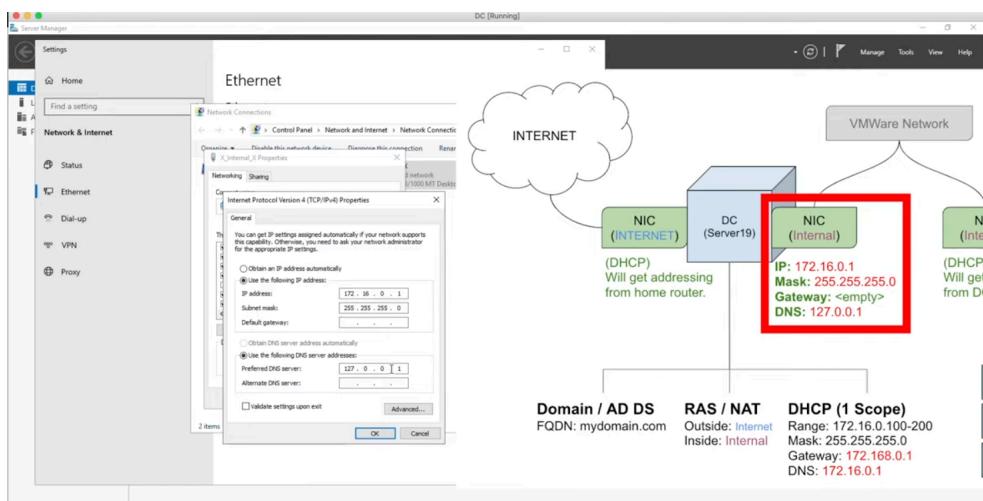


- Configuration du Réseau

VM cartes

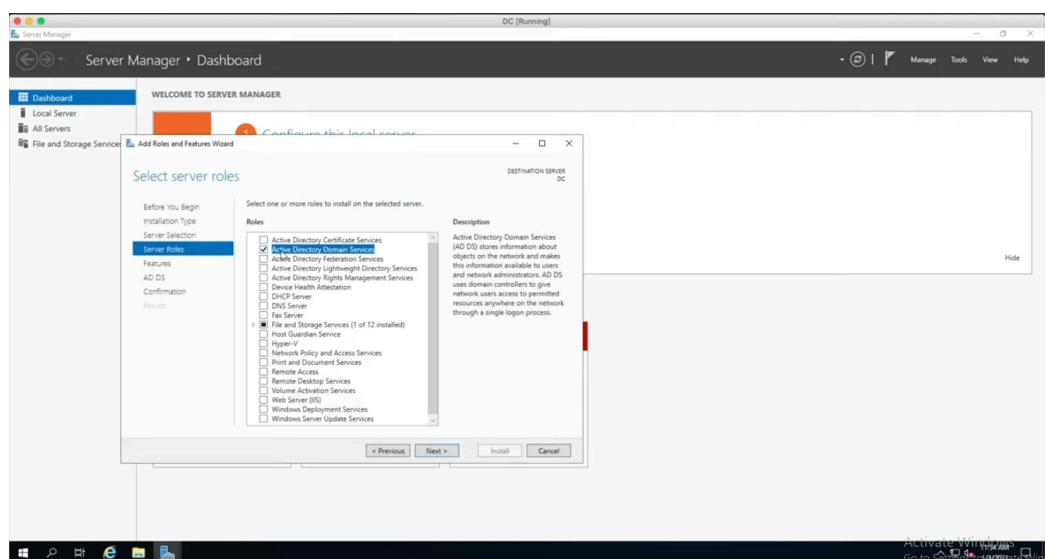


Attribution d'adresse IP interne de la carte réseau

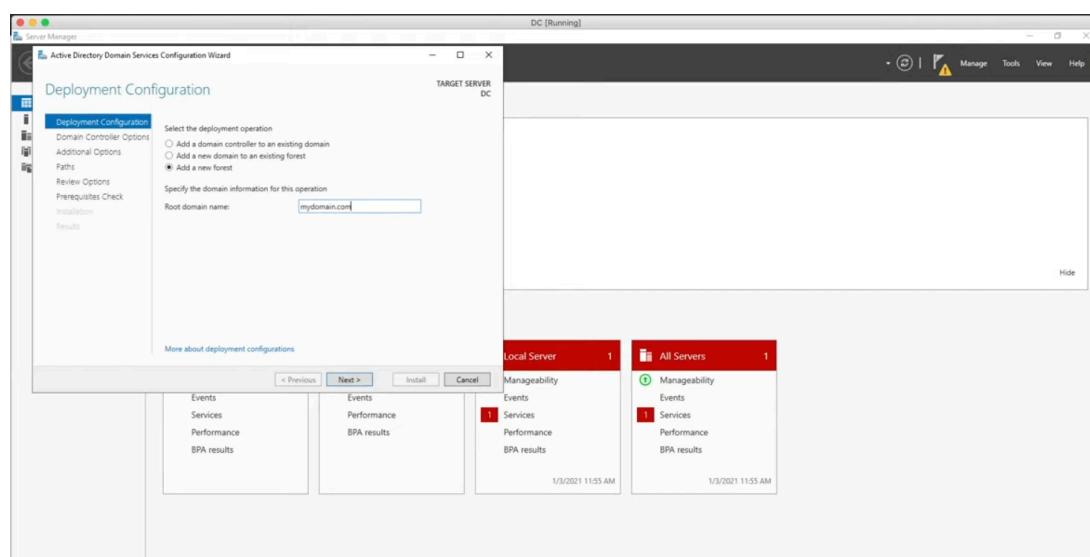


- Configuration de Windows Server

Installation des services de domaine AD

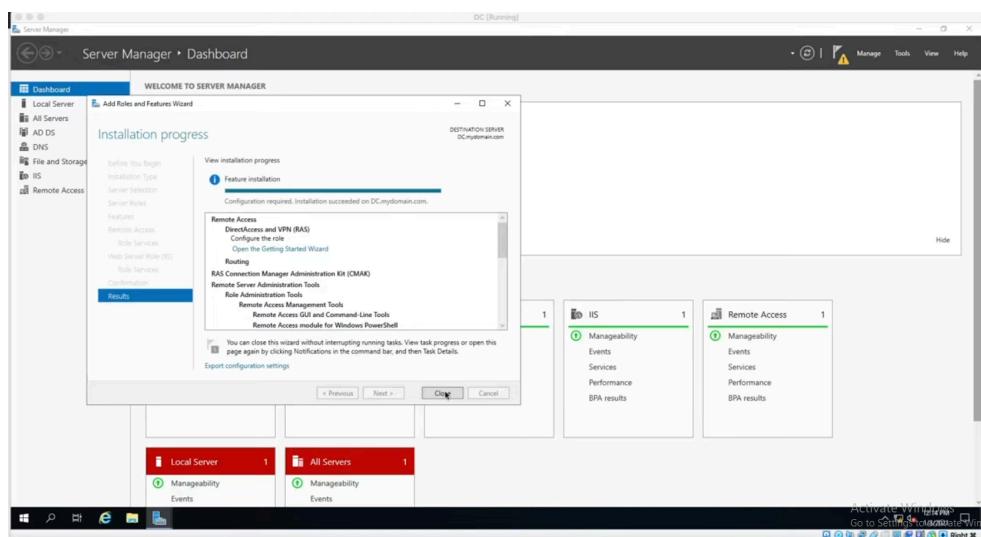


Promoter l'ordinateur vers un domaine

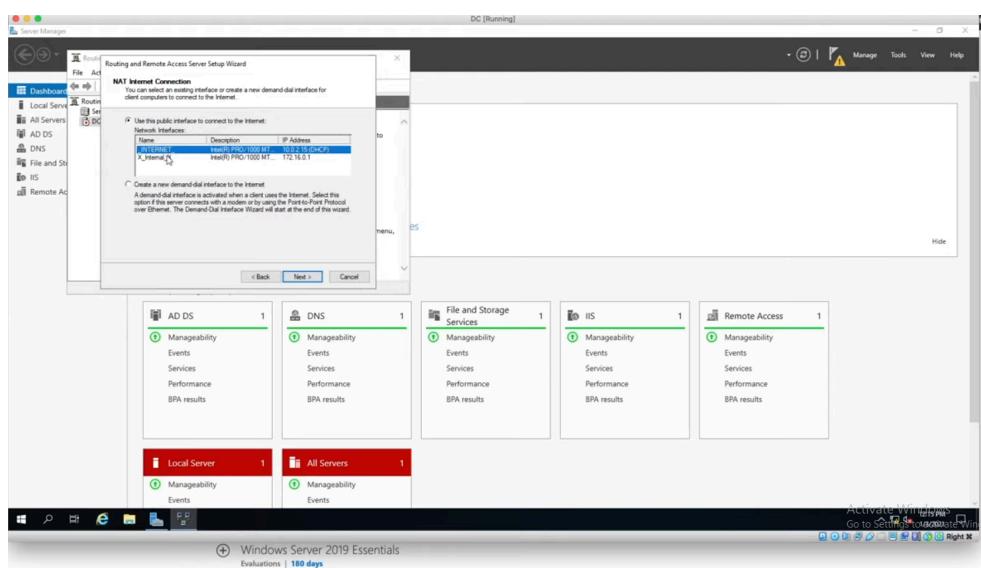


- Configuration Active Directory

Installation du rôle RAS des services d'accès à distance

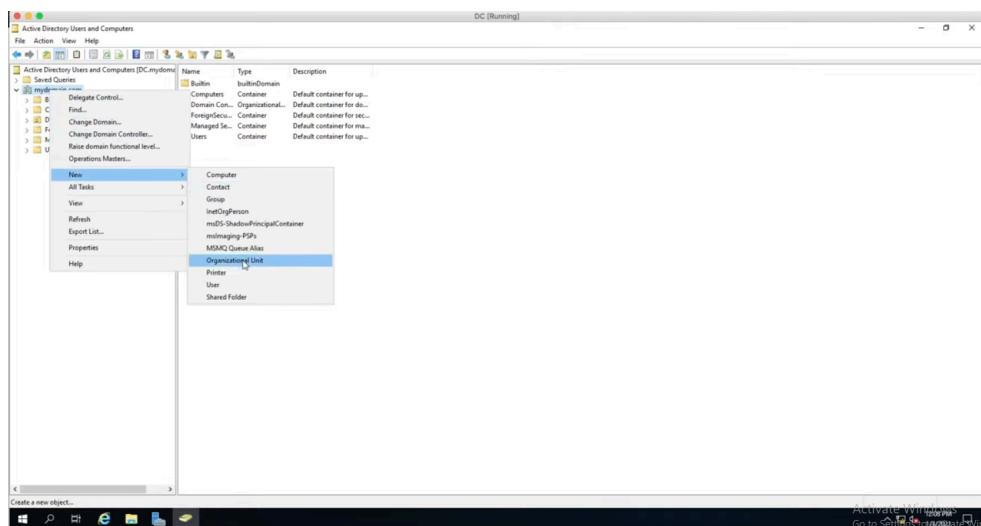


Terminer l'installation de RAS en choisissant la carte réseau utilisée pour se connecter à Internet

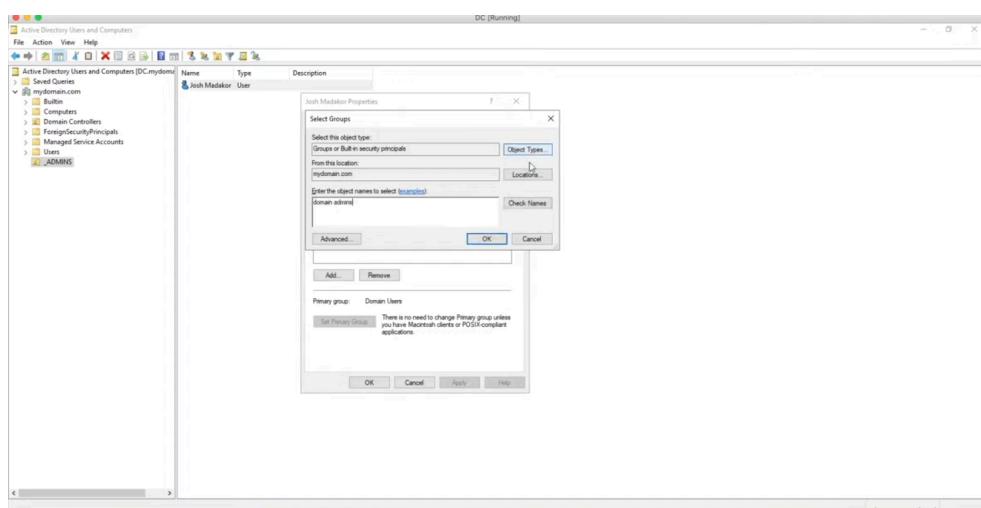


- Configuration Administrative

Ajouter une unité organisationnelle pour le compte administrateur dédié

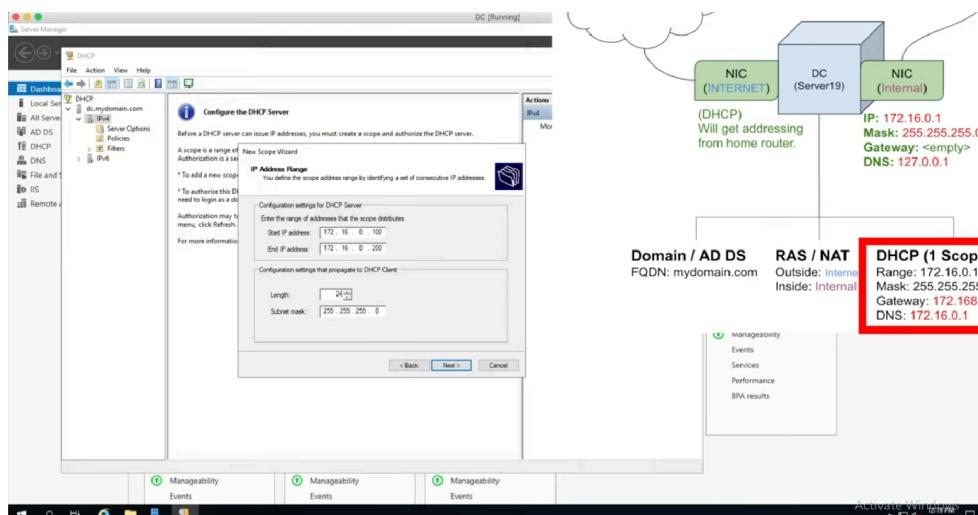


Faire du nouvel utilisateur un administrateur et l'ajouter au groupe des administrateurs

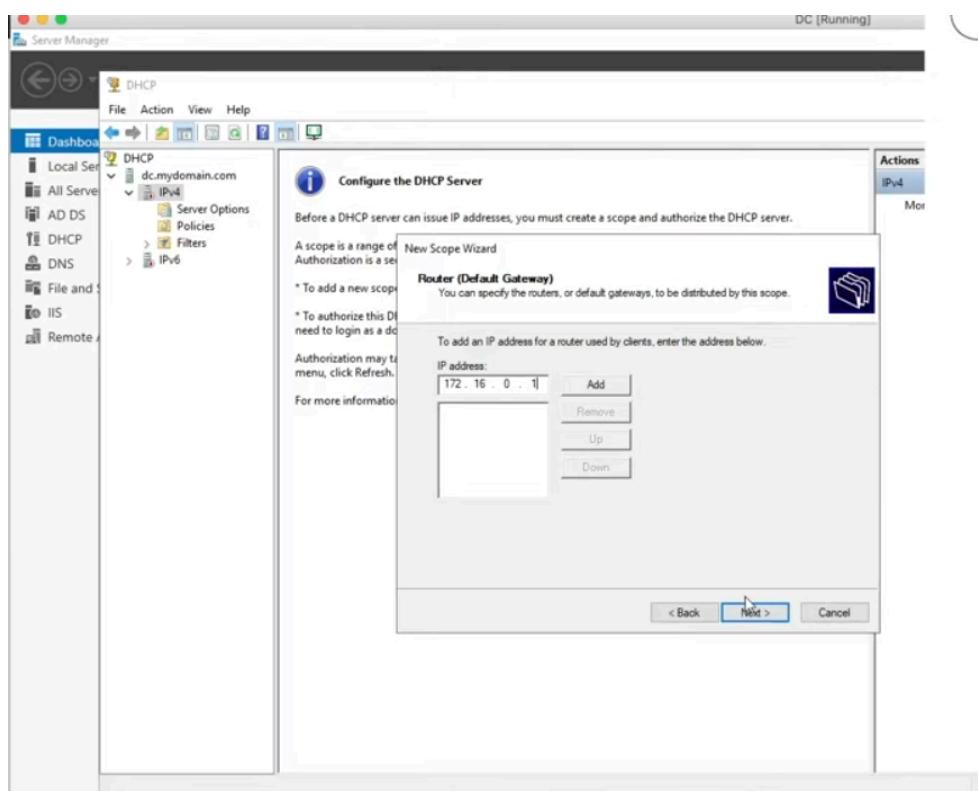


- Configuration des Services Réseau (DHCP)

Configuration de la portée DHCP après l'avoir installée



Sélection du contrôleur de domaine comme passerelle par défaut



- Implémentation de l'Automatisation

Configuration de la politique d'exécution PowerShell sur UNRESTRICTED avant d'exécuter le script de création d'utilisateur

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
DC [Running]
T:\CREATE_USERS.ps1 X
1 # ----- Edit these Variables for your own Use Case ----- #
2 $PASSWORD_FOR_USERS = "Password1"
3 $USER_FIRST_LAST_LIST = Get-Content .\names.txt
4 #
5
6 $password = ConvertTo-SecureString $PASSWORD_FOR_USERS -AsPlainText -Force
7 New-ADOrganizationalUnit -Name _USERS -ProtectedFromAccidentalDeletion $false
8
9 foreach ($n in $USER_FIRST_LAST_LIST) {
10     $first = $n.Split(" ")[0].ToLower()
11     $last = $n.Split(" ")[1].ToLower()
12     $username = "$($first.Substring(0,1))$($last)".ToLower()
13     Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
14
15     New-ADUser -AccountPassword $password
16         -GivenName $first
17         -Surname $last
18
19
20
on the current system. For more information about running scripts and setting execution policy, see
about_Execution_Policies at https://go.microsoft.com/fwlink/?LinkId=135170.
+ CategoryInfo          : SecurityError: (:) [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : UnauthorizedAccess
PS C:\Windows\system32> Set-ExecutionPolicy Unrestricted
```

Exécuter le script de création d'utilisateur PowerShell

```
$first = $n.Split(" ")[0].ToLower()
$last = $n.Split(" ")[1].ToLower()
$username = "$($first.Substring(0,1))$($last)".ToLower()
Write-Host "Creating user: $($username)" -BackgroundColor Black -ForegroundColor Cyan
New-ADUser -AccountPassword $password
    -GivenName $first
    -Surname $last
    -DisplayName $username
    -Name $username
    -EmployeeID $username

Creating user: pruane
Creating user: jtourville
Creating user: pluck
Creating user: ahitch
Creating user: jgatson
Creating user: bsuber
Creating user: yeasler
Creating user: afleitas
Creating user: fschreiber
Creating user: sahlquist
Creating user: tnewbury
Creating user: dresendes
Creating user: cplia
Creating user: ebuton
Creating user: dkim
```

Scripts d'Automatisation

Scripts d'Automatisation Python

1. Collecteur d'Informations Système

Ce script collecte les informations système essentielles, telles que le système d'exploitation, les cœurs CPU, et la mémoire.

```
import platform
import psutil

def get_system_info():
    """
    Collecte et affiche les informations système de base
    incluant l'OS, CPU, et mémoire.

    """
    print(f"OS: {platform.system()} {platform.release()}")
    print(f"CPU Cores: {psutil.cpu_count()}")
    print(f"Total Memory: {psutil.virtual_memory().total / (1024**3):.2f} GB")
```

2. Vérificateur de Taille des Fichiers Journaux

Ce script surveille la taille des fichiers journaux dans un répertoire et génère une alerte pour ceux dépassant 100 Mo.

```
import os
```

```
def check_log_file_sizes(directory):
```

```
    """
```

Surveille la taille des fichiers journaux et alerte si
>100MB.

```
    """
```

```
    for filename in os.listdir(directory):
```

```
        if filename.endswith('.log'):
```

```
            filepath = os.path.join(directory, filename)
```

```
            size = os.path.getsize(filepath) / (1024 * 1024)
```

```
            if size > 100:
```

```
                print(f"Fichier journal volumineux : {filename} -
```

```
{size:.2f} MB")
```

3. Vérificateur d'Expiration des Comptes Utilisateurs

Ce script alerte sur les comptes utilisateurs expirant dans les 30 jours.

```
import datetime
```

```
def check_account_expiration(users):
```

```
    """
```

Vérifie les dates d'expiration des comptes et alerte si <30 jours restants.

```
    """
```

```
    for user in users:
```

```
        expiration_date = datetime.datetime(2024, 12, 31)
```

```
        days_left = (expiration_date -
```

```
datetime.datetime.now()).days
```

```
        if days_left < 30:
```

```
            print(f"Le compte utilisateur {user} expire dans  
{days_left} jours")
```

4. Moniteur d'Espace Disque

Surveille l'espace disque disponible et alerte si un seuil (par défaut 20%) est franchi.

```
import psutil
```

```
def monitor_disk_space(threshold=20):
```

```
    """
```

Surveille l'espace disque et alerte si le seuil de libre est atteint.

```
    """
```

```
    for partition in psutil.disk_partitions():
```

```
        usage = psutil.disk_usage(partition.mountpoint)
```

```
        if (usage.free / usage.total * 100) < threshold:
```

```
            print(f"Espace disque faible sur
```

```
{partition.mountpoint}: {usage.free / usage.total *  
100:.2f}% libre")
```

5. Test de Connectivité Réseau

Teste la connectivité réseau vers une liste d'hôtes sur le port 80 (HTTP).

```
import socket
```

```
def test_network_connectivity(hosts):
```

```
    """
```

Teste la connectivité réseau vers des hôtes spécifiés.

```
    """
```

```
    for host in hosts:
```

```
        try:
```

```
            socket.create_connection((host, 80), timeout=5)
```

```
            print(f"Connecté à {host}")
```

```
        except (socket.timeout, socket.error):
```

```
            print(f"Impossible de se connecter à {host}")
```

6. Scanner de Port Simple

Un scanner de ports multi-thread pour identifier rapidement les ports ouverts.

```
import socket
import threading
from queue import Queue

def port_scan(target, port, open_ports):
    """
    Analyse un port spécifique pour déterminer s'il est ouvert.
    """
    try:
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as sock:
            sock.settimeout(1)
            if sock.connect_ex((target, port)) == 0:
                open_ports.put(port)
    except:
        pass

def scan_ports(target, port_range=(1, 1024)):
    """
    Scanner de ports multi-thread pour identifier les ports ouverts.
    """
    open_ports = Queue()
    threads = [
        threading.Thread(target=port_scan, args=(target, port, open_ports))
        for port in range(port_range[0], port_range[1] + 1)
    ]
    for thread in threads:
        thread.start()
    for thread in threads:
        thread.join()

    print(f"\nPorts ouverts sur {target}:")
    while not open_ports.empty():
        print(f"Le port {open_ports.get()} est ouvert")
```

Scripts d'Administration PowerShell

1. Gestion des Comptes Utilisateurs

Une fonction pour créer des comptes utilisateurs standard dans Active Directory, en définissant un nom d'utilisateur et un département.

```
function Create-StandardUser {  
    param (  
        [string]$Username, # Nom d'utilisateur pour le  
        nouveau compte  
        [string]$Department # Département pour  
        l'organisation de l'utilisateur  
    )  
    New-ADUser -Name $Username `'  
        -Department $Department `'  
        -Enabled $true # Compte actif dès la création  
}
```

2. Script de Sauvegarde Système

Ce script permet de sauvegarder les fichiers système critiques avec un horodatage dans un dossier de sauvegarde.

```
function Backup-SystemFiles {  
    $BackupPath = "C:\Backups"  
    $Date = Get-Date -Format "yyyyMMdd"  
    Backup-Directory -Path "C:\Important" -Destination  
    "$BackupPath\Backup_$Date"  
}
```

3. Vérificateur de Santé des Services

Surveille l'état des services critiques et alerte si l'un d'eux n'est pas actif.

```
function Check-ServiceStatus {  
    $CriticalServices = @("Spooler", "MSSQLSERVER",  
    "W32Time")  
    foreach ($Service in $CriticalServices) {  
        $Status = Get-Service -Name $Service  
        if ($Status.Status -ne "Running") {  
            Write-Host "Le service $Service n'est pas en cours  
d'exécution !" -ForegroundColor Red  
        }  
    }  
}
```

4. Moniteur de Ressources Système

Ce script surveille l'utilisation des ressources système comme le CPU et la mémoire, et génère une alerte en cas de surcharge.

```
function Monitor-SystemResources {  
    $CPUUsage = (Get-WmiObject  
        Win32_Processor).LoadPercentage  
    $MemoryUsage = (Get-WmiObject  
        Win32_OperatingSystem)  
  
    if ($CPUUsage -gt 80) {  
        Write-Host "Utilisation CPU élevée : $CPUUsage%" -  
            ForegroundColor Red  
    }  
}
```

5. Vérificateur de Mises à Jour Logicielles

Vérifie les mises à jour Windows en attente et affiche le nombre de mises à jour disponibles.

```
function Check-SoftwareUpdates {  
    $UpdateSession = New-Object -ComObject  
    Microsoft.Update.Session  
    $UpdateSearcher =  
    $UpdateSession.CreateUpdateSearcher()  
    $SearchResult =  
    $UpdateSearcher.Search("IsInstalled=0")  
    Write-Host "Nombre de mises à jour disponibles :"  
    $($SearchResult.Updates.Count)  
}
```

6. Crédit en Masse d'Utilisateurs dans Active Directory

Ce script permet de créer plusieurs utilisateurs Active Directory à partir d'un fichier texte contenant des noms, avec un mot de passe par défaut et une organisation dédiée.

```
# Variables de configuration
$PASSWORD_FOR_USERS = "Password1"          # Mdp par défaut
$USER_FIRST_LAST_LIST = Get-Content .\names.txt # Fichier
avec "Prénom Nom"
# Mot de passe en chaîne sécurisée
$password = ConvertTo-SecureString $PASSWORD_FOR_USERS -
AsPlainText -Force
# Créer une unité d'organisation (OU)
New-ADOrganizationalUnit -Name _USERS -
ProtectedFromAccidentalDeletion $false
# Création des utilisateurs
foreach ($n in $USER_FIRST_LAST_LIST) {
    $first = $n.Split(" ")[0].ToLower()
    $last = $n.Split(" ")[1].ToLower()
    $username = "$($first.Substring(0,1))$($last)".ToLower()
    Write-Host "Création de l'utilisateur : $($username)" -
BackgroundColor Black -ForegroundColor Cyan
    New-AdUser -AccountPassword $password `

        -GivenName $first `

        -Surname $last `

        -DisplayName $username `

        -Name $username `

        -EmployeeID $username `

        -PasswordNeverExpires $true `

        -Path "ou=_USERS,$(([ADSI]`""").distinguishedName)" `

        -Enabled $true
}
```

Glossaire des Termes et Outils

Technologies et Sécurité Réseau

- Active Directory (AD) : Service de répertoire Microsoft pour la gestion des utilisateurs et des ressources dans un réseau.
- Group Policy : Fonctionnalité dans Active Directory pour contrôler les environnements utilisateur et informatique.
- NAC (Network Access Control) : Approche de sécurité pour restreindre les appareils non autorisés à se connecter.
- EDR (Endpoint Detection and Response) : Technologie de sécurité pour le monitoring des points de terminaison.
- AAA (Authentication, Authorization, and Accounting) : Framework de sécurité pour le contrôle d'accès.
- Firewall : Système de sécurité qui surveille et contrôle le trafic réseau.
- VPN (Virtual Private Network) : Protocole de connexion sécurisée chiffrée.
- 802.1x : Protocole d'authentification basé sur le port réseau.

- Port Security : Fonctionnalité de sécurité réseau pour la restriction des interfaces.
- Protocole et Gestion du Réseau
- TCP/IP : Protocoles fondamentaux pour la communication sur internet.
- DNS (Domain Name System) : Protocole pour la traduction des noms de domaine en adresses IP.
- DHCP : Protocole pour l'affectation automatique des adresses IP.
- Load Balancing : Technique pour distribuer le trafic réseau.

Sécurité et Investigation Numérique

- Protocoles d'Authentification : Mécanismes de vérification d'identité.
- Chiffrement : Sécurité des données par encodage.
- Logiciels Malveillants : Logiciels conçus pour nuire aux systèmes.
- SIEM : Système de gestion des informations et des événements de sécurité.
- Surveillance Réseau : Technique de surveillance du trafic réseau.
- Analyse Mémoire : Technique d'analyse de la mémoire vive.
- Volatility : Framework d'analyse de mémoire forensique.

- Tests d'Intrusion : Évaluation de la sécurité par des attaques simulées.

Outils et Logiciels

- Windows Server : Système d'exploitation du serveur Microsoft.
- VirtualBox : Logiciel de virtualisation multiplateforme.
- Cisco Packet Tracer : Outil de simulation réseau.
- Wireshark : Analyseur de protocole réseau.
- Metasploit : Framework de test de pénétration.
- MDT : Microsoft Deployment Toolkit.

Informatique en Nuage et Virtualisation

- VPS : Serveur Privé Virtuel.
- IaaS : Infrastructure en tant que Service.
- PaaS : Plateforme en tant que Service.
- SaaS : Logiciel en tant que Service.
- Orchestration Cloud : Gestion automatisée des services cloud.
- Conteneurisation : Technologie d'encapsulation d'applications.
- Kubernetes : Plateforme d'orchestration de conteneurs.

