Admin Win

- 1. Labo & outils
  - Préparer le labo : VM, snapshots, sysprep
  - Boîte à outils : raccourcis et commandes
- 2. Réseau & services
  - Réseau : configuration IP et plusieurs cartes (multi-NIC)
  - Routage et NAT avec RRAS
  - DNS
  - DHCP
- 3. Active Directory
  - Active Directory : promouvoir un contrôleur de domaine
  - Active Directory : utilisateurs, groupes et OU
  - Joindre un poste au domaine
- 4. À venir
  - À venir : GPO et partages (aperçu)
- 0. Prise de notes
  - 03-11-26
  - 05-11-26
  - 06-11-26
  - 09-11-26
  - 10-11-26

1. Labo & outils

Préparation des VM et boîte à outils

Préparer le labo : VM, snapshots, sysprep

Snapshot vs clone

	Snapshot (instantané)	Clone
Rôle	Photo de l'état d'une VM à un instant T, pour revenir en arrière	Nouvelle VM indépendante, copiée d'une autre
Disque	Fichier delta : les changements sont écrits à côté du disque d'origine	**Clone complet** : copie entière du disque. **Clone lié** : partage le disque parent, ne stocke que les différences
Usage typique	« Avant de promouvoir le DC », « avant d'installer RRAS »	Créer SRV01, RTRHP01, CLI01... à partir d'un même modèle

Bonnes pratiques snapshots

- Les nommer clairement : `01 - OS installé + IP fixe`, `02 - AD DS promu`, etc.
- Un snapshot **n'est pas une sauvegarde** : si le disque parent est corrompu, tous les snapshots sont perdus.
- Une longue chaîne de snapshots ralentit la VM et prend de la place : supprimer (consolider) ceux qui ne servent plus.
- ⚠ **Contrôleur de domaine** : ne pas restaurer un vieux snapshot d'un DC quand il y a **plusieurs DC**. Cela provoque un *USN rollback* et casse la réplication AD. Avec un seul DC en labo, c'est sans risque.

Pourquoi « préparer » une VM avant de la cloner ? (le SID)

Chaque installation de Windows reçoit un identifiant unique, le **SID machine** (`S-1-5-21-xxxx-yyyy-zzzz`). Si on clone une VM sans la préparer, toutes les copies ont **le même SID**.

Problème concret en cours : le domaine AD hérite du SID de la machine promue en premier DC. Si un poste cloné depuis la même VM essaie de rejoindre ce domaine, on obtient l'erreur :

> *The domain join cannot be completed because the SID of the domain you attempted to join was identical to the SID of this machine.*

➡ Solution : **généraliser** la VM modèle avec **Sysprep** avant de la cloner.

Sysprep

Emplacement : `C:\Windows\System32\Sysprep\sysprep.exe`

```
C:\Windows\System32\Sysprep\sysprep.exe /generalize /oobe /shutdown
```

Option	Effet
`/generalize`	Supprime ce qui est propre à la machine : SID, nom, pilotes spécifiques, journaux…
`/oobe`	Au prochain démarrage, affiche l'assistant de premier démarrage (OOBE : langue, compte, mot de passe)
`/audit`	Redémarre en mode audit au lieu de l'OOBE
`/shutdown`	Éteint la machine à la fin, **à ne pas redémarrer** : c'est elle qui devient le modèle

Méthode « VM modèle » :

1. Installer Windows Server sur une VM, puis faire les mises à jour et installer les VMware Tools ou Guest Additions.
2. Lancer `sysprep /generalize /oobe /shutdown`.
3. **Ne plus démarrer cette VM.** La convertir en modèle, ou prendre un snapshot « modèle sysprep ».
4. Cloner autant de VM que nécessaire : chacune passera l'OOBE et aura son propre SID.

Mode audit : `Ctrl + Shift + F3`

> ◫◫ Dans mes notes j'avais écrit `Ctrl + Alt + F3` : le bon raccourci est **`Ctrl + Shift + F3`**.

Sur l'écran OOBE (le tout premier écran après l'installation, par exemple le choix de la région), **`Ctrl + Shift + F3`** fait redémarrer Windows en **mode audit** :

- On est connecté automatiquement en Administrateur intégré, **sans créer de compte**.
- On peut installer des logiciels et des pilotes, et personnaliser l'image.

- La fenêtre Sysprep s'ouvre automatiquement : on termine en choisissant **OOBE + Généraliser + Arrêter**.

C'est donc la manière propre de préparer une image à cloner.

Vérifier le SID machine

```
whoami /user          # SID du compte : la partie avant le dernier -xxx est le SID machine (compte local)
```

Avec Sysinternals : `PsGetSid.exe` affiche directement le SID machine.

Questions de révision

1. Quelle est la différence entre un clone lié et un clone complet ?
2. Pourquoi faut-il faire un sysprep avant de cloner une VM qu'on va mettre dans un domaine ?
3. Que fait le raccourci `Ctrl + Shift + F3`, et à quel moment l'utilise-t-on ?
4. Pourquoi ne doit-on plus démarrer la VM modèle après le sysprep ?
5. Un snapshot remplace-t-il une sauvegarde ? Pourquoi ?

Boîte à outils : raccourcis et commandes

Tous ces raccourcis se lancent avec `Win + R`, dans `cmd` ou dans PowerShell.

Panneaux de configuration (`.cpl`)

Commande	Ouvre	Utile pour
`sysdm.cpl`	Propriétés système	Renommer le PC, **joindre un domaine**, bureau à distance, variables d'environnement
`ncpa.cpl`	Connexions réseau	Voir, renommer et configurer les cartes réseau (IP, masque, passerelle, DNS)
`appwiz.cpl`	Programmes et fonctionnalités	Désinstaller un programme, fonctionnalités Windows
`firewall.cpl`	Pare-feu Windows	Activer ou désactiver le pare-feu, règles
`timedate.cpl`	Date et heure	Fuseau horaire (important pour Kerberos)
`control userpasswords2`	Comptes d'utilisateurs	Gestion rapide des comptes locaux

Consoles de gestion (`.msc`)

Commande	Console
`compmgmt.msc`	Gestion de l'ordinateur (tout-en-un)
`lusrmgr.msc`	Utilisateurs et groupes **locaux** (absent sur un DC)
`services.msc`	Services
`eventvwr.msc`	Observateur d'événements, **le premier réflexe en cas de problème**
`diskmgmt.msc`	Gestion des disques
`devmgmt.msc`	Gestionnaire de périphériques

Commande	Console
`dsa.msc`	**Utilisateurs et ordinateurs Active Directory** (ADUC)
`dssite.msc`	Sites et services AD
`domain.msc`	Domaines et approbations AD
`dnsmgmt.msc`	Console DNS
`dhcpmgmt.msc`	Console DHCP
`rrasmgmt.msc`	Routage et accès distant (RRAS)
`gpmc.msc`	Gestion des stratégies de groupe (GPO)

> Sur Windows Server Core (sans interface graphique), `sconfig` ouvre un menu texte pour régler le nom, l'IP, le domaine et les mises à jour.

Commandes réseau

CMD	Équivalent PowerShell	Rôle
`ipconfig /all`	`Get-NetIPConfiguration`	IP, masque, passerelle, DNS, MAC, DHCP
`ipconfig /release` · `/renew`	—	Rendre ou redemander un bail DHCP
`ipconfig /flushdns`	`Clear-DnsClientCache`	Vider le cache DNS local
`ipconfig /registerdns`	`Register-DnsClient`	Réenregistrer le poste dans le DNS
`ping 10.19.1.254`	`Test-Connection 10.19.1.254`	Test de connectivité (ICMP)
`tracert 8.8.8.8`	`Test-NetConnection 8.8.8.8 -TraceRoute`	Chemin suivi, routeur par routeur
—	`Test-NetConnection srv01 -Port 389`	Tester un port TCP
`route print`	`Get-NetRoute`	Table de routage
`netstat -ano`	`Get-NetTCPConnection`	Connexions et ports ouverts
`nslookup nom`	`Resolve-DnsName nom`	Interroger le DNS
`arp -a`	`Get-NetNeighbor`	Cache ARP (IP ↔ MAC)

> ⚠ Par défaut, **le pare-feu Windows bloque le ping entrant**. En labo :

```
Enable-NetFirewallRule -DisplayName "*ICMPv4*"      # nom FR : "Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entrant ICMPv4)"
```

ou bien : `netsh advfirewall firewall add rule name="ICMP" protocol=icmpv4:8,any dir=in action=allow`

Identité, session et système

Commande	Rôle
`whoami`	Utilisateur connecté (`domaine\utilisateur` ou `machine\utilisateur`)
`whoami /all`	SID, **groupes**, privilèges : utile pour vérifier qu'un ajout de groupe est bien pris en compte (il faut se reconnecter)
`whoami /upn`	UPN (`user@domaine`), seulement pour un compte de domaine
`hostname`	Nom de la machine
`echo %logonserver%`	DC qui a authentifié la session
`systeminfo`	OS, domaine, mises à jour, RAM…
`Rename-Computer -NewName SRV01 -Restart`	Renommer la machine
`Get-WindowsFeature`	Lister les rôles et fonctionnalités (installés ou non)
`Install-WindowsFeature <nom> -IncludeManagementTools`	Installer un rôle avec ses consoles

Questions de révision

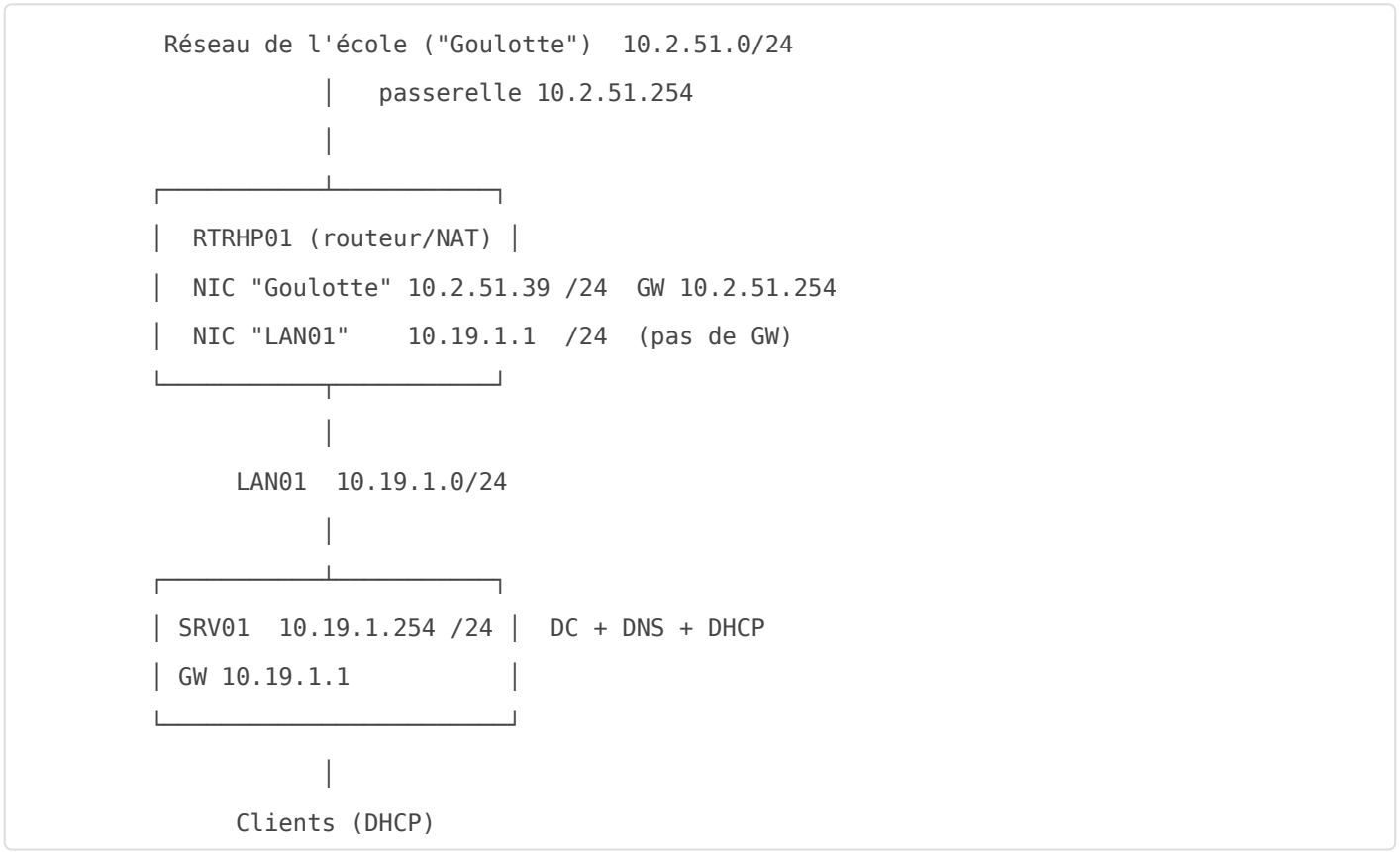
1. Quelle commande ouvre directement la fenêtre pour joindre un PC à un domaine ?
2. Tu ajoutes un utilisateur à un groupe, mais `whoami /groups` ne le montre pas. Pourquoi, et comment corriger ?
3. Ton ping vers SRV01 échoue alors que l'IP est correcte. Quelle est la première chose à vérifier ?
4. Quel est l'équivalent PowerShell de `ipconfig /all` ?

2. Réseau & services

IP, multi-NIC, routage/NAT, DNS, DHCP

Réseau : configuration IP et plusieurs cartes (multi-NIC)

Topologie du labo



Machine	Carte	IP / masque	Passerelle	DNS
RTRHP01	Goulotte	10.2.51.39 / 255.255.255.0	10.2.51.254	DNS de l'école (ou SRV01 une fois le domaine créé)
RTRHP01	LAN01	10.19.1.1 / 255.255.255.0	**aucune**	10.19.1.254
SRV01	LAN	10.19.1.254 / 255.255.255.0	10.19.1.1	**10.19.1.254** (lui-même)

Règles d'or du multi-NIC

1. **Une seule passerelle par défaut** sur toute la machine : sur la carte qui mène vers « le reste du monde » (ici Goulotte). Si on en met deux, Windows choisit selon la métrique et le trafic part au hasard sur l'une ou l'autre.
2. **Renommer les cartes** dans `ncpa.cpl` (`Ethernet0` → `Goulotte`, `Ethernet1` → `LAN01`), sinon on ne sait plus laquelle est laquelle.
3. **Identifier la bonne carte** : comparer l'adresse **MAC** dans `ipconfig /all` avec celle de la carte virtuelle dans les paramètres de la VM, et vérifier à quel réseau virtuel (vSwitch, LAN segment, réseau interne…) chaque carte est connectée.
4. Pour joindre un réseau qui n'est pas derrière la passerelle par défaut, on ajoute une **route statique** plutôt qu'une deuxième passerelle.

Configurer en GUI

`ncpa.cpl` → clic droit sur la carte → **Propriétés** → **Protocole Internet version 4 (TCP/IPv4)** → saisir l'IP, le masque, la passerelle et le DNS.

Configurer en PowerShell

```
# Voir les cartes
Get-NetAdapter

# Renommer
Rename-NetAdapter -Name "Ethernet0" -NewName "Goulotte"
Rename-NetAdapter -Name "Ethernet1" -NewName "LAN01"

# IP fixe + passerelle (carte côté école)
New-NetIPAddress -InterfaceAlias "Goulotte" -IPAddress 10.2.51.39 -PrefixLength 24 -
DefaultGateway 10.2.51.254

# IP fixe SANS passerelle (carte côté LAN)
New-NetIPAddress -InterfaceAlias "LAN01" -IPAddress 10.19.1.1 -PrefixLength 24

# DNS
Set-DnsClientServerAddress -InterfaceAlias "LAN01" -ServerAddresses 10.19.1.254

# Vérifier
Get-NetIPConfiguration

# Supprimer une IP / une passerelle mal configurée
```

```
Remove-NetIPAddress -InterfaceAlias "LAN01" -Confirm:$false
Remove-NetRoute -InterfaceAlias "LAN01" -DestinationPrefix 0.0.0.0/0 -Confirm:$false

# Ajouter une route statique (ex : vers un autre LAN derrière 10.19.1.2)
New-NetRoute -DestinationPrefix 10.20.0.0/24 -InterfaceAlias "LAN01" -NextHop 10.19.1.2
# équivalent cmd : route -p add 10.20.0.0 mask 255.255.255.0 10.19.1.2
```

> □□ `/24` = `255.255.255.0` : 24 bits à 1 dans le masque, donc 254 adresses utilisables (de .1 à .254).

Questions de révision

1. Pourquoi ne met-on pas de passerelle sur la carte LAN01 du routeur ?
2. Quelle est la passerelle par défaut de SRV01 ? Pourquoi ?
3. Comment savoir quelle carte Windows correspond à quelle carte virtuelle de la VM ?
4. Que vaut le masque `/24` en notation décimale, et combien d'hôtes contient ce réseau ?

Routage et NAT avec RRAS

RRAS (*Routing and Remote Access Service*) transforme un Windows Server en **routeur**. Il peut aussi faire du **NAT**, servir de **serveur VPN** et d'**agent de relais DHCP**.

Dans le labo, **RTRHP01** relie le LAN `10.19.1.0/24` au réseau de l'école `10.2.51.0/24`.

Routage simple vs NAT

	Routage simple (LAN routing)	NAT
Fonctionnement	Transmet les paquets entre réseaux sans modifier les IP	Remplace l'IP source privée (10.19.1.x) par l'IP de la carte publique (10.2.51.39)
Condition	Le réseau en amont doit avoir une **route retour** vers 10.19.1.0/24	Aucune configuration nécessaire en amont
Usage labo	Rarement possible : on ne contrôle pas le routeur de l'école	**Ce qu'on utilise** pour que le LAN ait accès à Internet

> Sans NAT, un paquet du LAN atteint bien Internet, mais la réponse revient vers `10.19.1.x` et le routeur de l'école ne sait pas où se trouve ce réseau. La réponse est donc perdue.

Installation

```
Install-WindowsFeature RemoteAccess, Routing -IncludeManagementTools
```

GUI : **Gestionnaire de serveur** → Ajouter des rôles → **Accès à distance** → service de rôle **Routage**. Cocher aussi **DirectAccess et VPN** : il est requis avec Routage.

Configuration du NAT (GUI)

1. `rrasmgmt.msc` → clic droit sur le serveur → **Configurer et activer le routage et l'accès distant**.

2. Choisir **Traduction d'adresses réseau (NAT)**.
3. Interface publique (connectée à Internet) : **Goulotte**.
4. Si l'assistant le propose, **ne pas** activer ses services DNS/DHCP de base (c'est SRV01 qui s'en charge).
5. Terminer : le service démarre.

Configuration du NAT (ligne de commande)

```
Install-RemoteAccess -VpnType RoutingOnly
netsh routing ip nat install
netsh routing ip nat add interface "Goulotte" full      # interface publique, avec NAT
netsh routing ip nat add interface "LAN01" private      # interface privée
```

Vérifier

- Depuis SRV01 : `ping 10.19.1.1`, puis `ping 10.2.51.254`, puis `ping 8.8.8.8`, puis `nslookup google.com`.
- `tracert 8.8.8.8` depuis SRV01 : le premier saut doit être `10.19.1.1`.
- `rrasmgmt.msc` → IPv4 → **NAT** : les mappages en cours sont visibles.
- `route print` sur RTRHP01 : on doit voir une seule route `0.0.0.0` (via 10.2.51.254).

Dépannage

Symptôme	Cause probable
Ping 10.19.1.1 OK, ping 10.2.51.254 KO	NAT ou routage non activé, mauvaise interface publique, ou passerelle de SRV01 manquante
Ping 8.8.8.8 OK mais pas de navigation	Problème **DNS** et non de routage (voir le redirecteur sur SRV01)
Rien ne passe depuis RTRHP01 lui-même	Mauvaise passerelle, ou deux passerelles par défaut

Agent de relais DHCP (aperçu)

Les requêtes DHCP sont des **broadcasts** : elles ne traversent pas un routeur. Si le serveur DHCP se trouve sur un autre réseau que les clients, on configure un **agent de relais** sur le routeur :

RRAS → IPv4 → clic droit **Général** → *Nouveau protocole de routage* → **Agent de relais DHCP**. On indique l'IP du serveur DHCP, puis on ajoute l'interface côté clients.

Questions de révision

1. Pourquoi faut-il le NAT et pas seulement le routage dans notre labo ?
2. Dans l'assistant RRAS, quelle interface choisit-on comme « publique » ?
3. Un client ping 8.8.8.8 mais n'ouvre aucun site web. Où chercher ?
4. À quoi sert un agent de relais DHCP ?

DNS

Le DNS traduit un **nom** en **adresse IP** (et l'inverse). Dans un domaine Active Directory, **le DNS est indispensable** : les clients trouvent les contrôleurs de domaine grâce à des enregistrements DNS (SRV).

Fonctionnement d'une résolution

```
Client ──(récursive)──> SRV01 (DNS local)
                        │ pas dans ses zones ni dans son cache ?
                        ├──> serveur racine "."        → « demande à .be »
                        ├──> serveur TLD ".be"         → « demande à hugo-pierret.be »
                        └──> serveur faisant autorité   → « wiki = 1.2.3.4 »
Client <──── réponse ──── SRV01 (garde la réponse en cache pendant le TTL)
```

- **Requête récursive** : le client demande « donne-moi la réponse finale ».
- **Requête itérative** : le serveur DNS interroge les autres serveurs étape par étape.

Les serveurs racine (root servers)

- 13 **noms** de serveurs racine, de `a.root-servers.net` à `m.root-servers.net`, gérés par 12 organisations.
- Grâce à l'**anycast**, ce sont en réalité **plus de 1 500 instances** réparties dans le monde. Carte : https://root-servers.org/
- Windows Server connaît leurs adresses grâce aux **indications de racine** (*root hints*) : console DNS → propriétés du serveur → onglet **Indications de racine**.

Redirecteurs vs indications de racine

	Redirecteur (*forwarder*)	**Indications de racine**
Principe	« Je ne sais pas → je demande à **ce** serveur » (DNS de l'école, 1.1.1.1, 8.8.8.8…)	« Je ne sais pas → je fais moi-même la résolution itérative à partir des serveurs racine »
Avantage	Rapide, profite du cache du serveur amont, passe les pare-feu	Aucune dépendance à un autre serveur
Labo	Souvent nécessaire si le réseau de l'école bloque le DNS sortant	Utilisé si aucun redirecteur ne répond

Redirecteur conditionnel : « pour le domaine `ecole.local`, demande à `10.2.x.x` ». Utile entre deux domaines AD.

Zones

Type	Rôle	Exemple
Zone de recherche directe	Nom → IP	`hp.lan`
Zone de recherche inversée	IP → nom	`1.19.10.in-addr.arpa` (pour 10.19.1.0/24, octets à l'envers)

Types de stockage :

- **Principale** : copie modifiable.
- **Secondaire** : copie en lecture seule obtenue par transfert de zone.
- **Stub** : contient seulement les NS/SOA d'une autre zone.
- **Intégrée à Active Directory** : stockée dans AD, répliquée avec AD, **mises à jour dynamiques sécurisées**. C'est le choix par défaut sur un DC.

Enregistrements principaux

Type	Rôle	Exemple
A	Nom → IPv4	`srv01 → 10.19.1.254`
AAAA	Nom → IPv6	
PTR	IP → nom (zone inversée)	`254 → srv01.hp.lan`
CNAME	Alias vers un autre nom	`intranet → srv01.hp.lan`
MX	Serveur de mail du domaine	
NS	Serveurs faisant autorité pour la zone	
SOA	Infos de la zone : serveur principal, numéro de série, TTL...	
SRV	Localise un **service** : c'est ainsi que les clients trouvent le DC	`_ldap._tcp.dc._msdcs.hp.lan`

Installation et configuration (PowerShell)

Le rôle DNS s'installe **automatiquement** pendant la promotion du DC (`-InstallDns`). Sinon :

```
Install-WindowsFeature DNS -IncludeManagementTools

# Zone inversée pour le LAN, intégrée à AD
Add-DnsServerPrimaryZone -NetworkId "10.19.1.0/24" -ReplicationScope Domain

# Enregistrements
Add-DnsServerResourceRecordA     -ZoneName "hp.lan" -Name "rtrhp01" -IPv4Address 10.19.1.1 -
CreatePtr
Add-DnsServerResourceRecordCName -ZoneName "hp.lan" -Name "intranet" -HostNameAlias
"srv01.hp.lan"

# Redirecteur
Add-DnsServerForwarder -IPAddress 10.2.51.254      # ou le DNS de l'école, 1.1.1.1…
Get-DnsServerForwarder

# Vider le cache du serveur DNS
Clear-DnsServerCache
```

nslookup

```
C:\> nslookup
Serveur par défaut :   UnKnown
Address:  10.19.1.254
>
```

- **Sans argument**, `nslookup` passe en **mode interactif** et affiche **le serveur DNS utilisé** par la machine. Pratique pour vérifier rapidement la configuration DNS.
- `UnKnown` : nslookup essaie de résoudre l'**IP du serveur DNS en nom** (requête PTR). S'il n'y a **pas de zone inversée** (ou pas de PTR), il affiche `UnKnown`. Ce n'est pas grave, mais créer la zone inversée corrige l'affichage.

Commandes utiles :

```
nslookup srv01.hp.lan                # résolution A
nslookup 10.19.1.254                 # résolution inverse (PTR)
nslookup google.com 1.1.1.1          # interroger un serveur précis
nslookup -type=SRV _ldap._tcp.dc._msdcs.hp.lan   # trouver les DC du domaine
nslookup -type=MX gmail.com
```

En mode interactif : `server 1.1.1.1` (changer de serveur), `set type=ns`, `exit`.

PowerShell : `Resolve-DnsName srv01.hp.lan`, `Resolve-DnsName -Type SRV _ldap._tcp.dc._msdcs.hp.lan`.

Questions de révision

1. Quelle est la différence entre une requête récursive et une requête itérative ?
2. Combien y a-t-il de serveurs racine ? Et combien de machines réelles derrière ?
3. Pourquoi nslookup affiche-t-il `UnKnown` comme nom du serveur ? Comment corriger ?
4. Quel type d'enregistrement permet à un client de trouver un contrôleur de domaine ?
5. Quel DNS doit être configuré sur un poste membre du domaine : le DC ou 8.8.8.8 ? Pourquoi ?
6. Quand utilise-t-on un redirecteur plutôt que les indications de racine ?

DHCP

Le DHCP distribue **automatiquement** aux clients une IP, un masque, une passerelle, un DNS, etc.

Le processus DORA

Étape	Message	De → vers	Type
Discover	« Y a-t-il un serveur DHCP ? »	Client → tous	Broadcast (`255.255.255.255`, port UDP 67)
Offer	« Je te propose 10.19.1.100 »	Serveur → client	(port UDP 68)
Request	« J'accepte l'offre de SRV01 »	Client → tous	Broadcast (pour prévenir les autres serveurs)
Ack	« C'est confirmé, bail de 8 jours »	Serveur → client	

- **Bail** : durée de validité de l'adresse. Le client tente de le **renouveler à 50 %** de sa durée, puis à 87,5 %.
- Pas de serveur qui répond → le client prend une adresse **APIPA** `169.254.x.x` : c'est le signe d'un problème DHCP.

Vocabulaire

Terme	Signification
Étendue (*scope*)	Plage d'adresses distribuables pour un réseau (ex. 10.19.1.100 → 10.19.1.200)
Exclusion	Adresses de la plage à **ne pas** distribuer (IP fixes des serveurs, imprimantes)
Réservation	Toujours la même IP pour une **adresse MAC** donnée
Options	Paramètres envoyés avec l'IP
Autorisation	Dans un domaine, un serveur DHCP doit être **autorisé dans AD**, sinon il ne distribue rien (protection contre les serveurs DHCP « pirates »)

Options importantes

N°	Option	Labo
003	Routeur (passerelle)	`10.19.1.1`
006	Serveurs DNS	`10.19.1.254`
015	Nom de domaine DNS	`hp.lan`
051	Durée du bail	

Les options peuvent être définies **au niveau du serveur** (pour toutes les étendues), **de l'étendue** ou **d'une réservation**. Le niveau le plus précis l'emporte.

Installation et configuration (PowerShell)

```
Install-WindowsFeature DHCP -IncludeManagementTools

# Crée les groupes de sécurité locaux DHCP (Administrateurs DHCP, Utilisateurs DHCP)
Add-DhcpServerSecurityGroup
Restart-Service DHCPServer

# Autoriser le serveur dans AD
Add-DhcpServerInDC -DnsName srv01.hp.lan -IPAddress 10.19.1.254

# Indiquer au Gestionnaire de serveur que la configuration post-installation est faite
Set-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name
ConfigurationState -Value 2

# Étendue
Add-DhcpServerv4Scope -Name "LAN01" -StartRange 10.19.1.100 -EndRange 10.19.1.200 `
    -SubnetMask 255.255.255.0 -LeaseDuration 8.00:00:00 -State Active

# Options de l'étendue
Set-DhcpServerv4OptionValue -ScopeId 10.19.1.0 -Router 10.19.1.1 `
    -DnsServer 10.19.1.254 -DnsDomain "hp.lan"

# Exclusion
Add-DhcpServerv4ExclusionRange -ScopeId 10.19.1.0 -StartRange 10.19.1.100 -EndRange
10.19.1.109
```

```
# Réservation
Add-DhcpServerv4Reservation -ScopeId 10.19.1.0 -IPAddress 10.19.1.150 `
    -ClientId "00-15-5D-01-02-03" -Name "IMP01" -Description "Imprimante"

# Vérifier
Get-DhcpServerv4Scope
Get-DhcpServerv4Lease -ScopeId 10.19.1.0
Get-DhcpServerInDC
```

GUI : `dhcpmgmt.msc` → IPv4 → **Nouvelle étendue** (l'assistant demande la plage, les exclusions, la durée du bail et les options 003/006/015) → clic droit sur le serveur → **Autoriser**.

> □□ Laisser les IP fixes (serveur .254, routeur .1) **en dehors** de la plage de l'étendue : c'est plus simple que de gérer des exclusions.

Côté client

```
ipconfig /release
ipconfig /renew
ipconfig /all        :: vérifier "Serveur DHCP", "Bail obtenu", "Bail expirant"
```

Dépannage

Symptôme	Piste
Client en `169.254.x.x`	Serveur non autorisé, étendue désactivée, client sur un autre réseau virtuel, ou pas de relais DHCP entre les deux
IP OK mais pas d'Internet	Option 003 (routeur) manquante ou fausse
IP OK mais pas de résolution de noms	Option 006 (DNS) manquante ou fausse
Icône rouge (flèche vers le bas) dans la console	Serveur non autorisé dans AD

Questions de révision

1. Cite les 4 étapes du DORA. Lesquelles sont en broadcast ?
2. Que signifie une adresse en 169.254.x.x sur un client ?
3. Quelle est la différence entre une exclusion et une réservation ?

4. Pourquoi faut-il « autoriser » un serveur DHCP dans Active Directory ?
5. Quelles options DHCP envoient la passerelle et le serveur DNS ?
6. Le serveur DHCP est sur un autre réseau que les clients : que faut-il ajouter ?

3. Active Directory

Promotion DC, objets AD, jonction au domaine

Active Directory : promouvoir un contrôleur de domaine

Vocabulaire

Terme	Définition
AD DS	*Active Directory Domain Services* : l'annuaire qui centralise les comptes, ordinateurs, groupes et stratégies
Contrôleur de domaine (DC)	Serveur qui héberge une copie de l'annuaire et authentifie les utilisateurs (Kerberos)
Domaine	Ensemble d'objets partageant la même base AD et le même nom DNS (`hp.lan`)
Arborescence (*tree*)	Domaine parent + domaines enfants (`hp.lan`, `bxl.hp.lan`)
Forêt	Ensemble d'arborescences : c'est la **limite de sécurité**. Le premier domaine créé est le *domaine racine de la forêt*
OU (*Organizational Unit*)	« Dossier » dans le domaine pour ranger les objets, déléguer des droits et appliquer des GPO
NetBIOS	Nom court du domaine (`HP`), utilisé dans `HP\hugo`
NTDS.dit	Fichier de la base AD (`C:\Windows\NTDS`)
SYSVOL	Partage répliqué entre DC qui contient les scripts et les GPO

Prérequis avant promotion

- ☐ **Nom définitif** de la machine (`SRV01`) : on évite de renommer un DC après coup.
- ☐ **IP fixe** (10.19.1.254 /24, GW 10.19.1.1).
- ☐ **DNS préféré = lui-même** (`10.19.1.254` ou `127.0.0.1`). Le serveur deviendra son propre DNS.
- ☐ Machine **sysprepée** si c'est un clone (SID unique).
- ☐ Heure et fuseau horaire corrects.
- ☐ Snapshot « avant promotion ».

Choisir le nom de domaine

- Utiliser un nom DNS complet : `hp.lan`, `lab.hugo-pierret.be`...
- La recommandation Microsoft est un **sous-domaine d'un domaine qu'on possède** (`ad.hugo-pierret.be`).
- **Éviter** `.local`, qui entre en conflit avec mDNS/Bonjour, et les noms en une seule partie (`HP` tout seul).

Promotion en GUI

1. **Gestionnaire de serveur** → Ajouter des rôles → **Services AD DS**.
2. Cliquer sur le drapeau jaune ⚠ → **Promouvoir ce serveur en contrôleur de domaine**.
3. **Ajouter une nouvelle forêt** → nom de domaine racine `hp.lan`.
4. Niveaux fonctionnels, options **DNS** + **Catalogue global** (cochés), mot de passe **DSRM**.
5. Délégation DNS : l'avertissement est normal pour une nouvelle forêt.
6. Nom NetBIOS (`HP`), chemins (laisser par défaut), vérification des prérequis, **Installer**. Le serveur redémarre.

Promotion en PowerShell

```
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools


Install-ADDSForest `
    -DomainName "hp.lan" `
    -DomainNetbiosName "HP" `
    -InstallDns `
    -SafeModeAdministratorPassword (Read-Host -AsSecureString "Mot de passe DSRM") `
    -Force
```

Autres cas (pour plus tard) :

- `Install-ADDSDomainController -DomainName hp.lan -InstallDns -Credential (Get-Credential)` : **ajouter un 2e DC** dans un domaine existant.
- `Install-ADDSDomain` : créer un domaine enfant.

DSRM

Directory Services Restore Mode : mode de démarrage spécial pour **réparer ou restaurer AD**, base AD hors ligne. Le mot de passe DSRM est celui de l'administrateur **local** utilisé dans ce mode.

Il est différent du mot de passe Administrateur du domaine : **à noter quelque part !**

Ce qui change après la promotion

- Le compte `Administrateur` local devient `HP\Administrateur` (administrateur du domaine).
- Plus de comptes locaux : `lusrmgr.msc` ne fonctionne plus sur un DC.
- La zone DNS `hp.lan` est créée, ainsi que `_msdcs.hp.lan` avec les enregistrements SRV.
- Les partages `SYSVOL` et `NETLOGON` apparaissent (`net share`).
- La carte réseau peut afficher DNS `127.0.0.1` : c'est normal, c'est le serveur lui-même.

Vérifications

```
Get-ADDomain
Get-ADForest
Get-ADDomainController
dcdiag                                          # tests de santé du DC (tout doit être
"passed")
nslookup -type=SRV _ldap._tcp.dc._msdcs.hp.lan  # le DC est-il annoncé dans le DNS ?
netdom query fsmo                               # qui détient les 5 rôles FSMO
```

Rôles FSMO (pour info)

5 rôles uniques, tous sur le premier DC :

- **Par forêt** : Contrôleur de schéma, Maître d'attribution des noms de domaine.
- **Par domaine** : Émulateur PDC (heure, mots de passe), Maître RID (distribue les blocs de SID), Maître d'infrastructure.

Questions de révision

1. Quelle est la différence entre un domaine et une forêt ?
2. Quel DNS doit être configuré sur la carte réseau du DC avant la promotion ?
3. À quoi sert le mot de passe DSRM ?
4. Quel enregistrement DNS vérifier pour s'assurer que le DC est bien annoncé ?
5. Pourquoi éviter un nom de domaine en `.local` ?
6. Quelle commande teste la santé d'un contrôleur de domaine ?

Active Directory : utilisateurs, groupes et OU

Console : `dsa.msc` (Utilisateurs et ordinateurs Active Directory, « ADUC »).

> Menu **Affichage → Fonctionnalités avancées** : affiche l'onglet **Éditeur d'attributs**, l'onglet **Objet** (chemin, protection contre la suppression) et des conteneurs cachés.

Conteneurs par défaut vs OU

Élément	Type	Remarque
`Builtin`	Conteneur	Groupes locaux intégrés (Administrateurs, Utilisateurs…)
`Computers`	Conteneur	Destination par défaut des PC qui rejoignent le domaine
`Users`	Conteneur	Comptes et groupes par défaut (Admins du domaine, etc.)
`Domain Controllers`	**OU**	Contient les DC
Vos OU	**OU**	On peut y **lier des GPO** et **déléguer** l'administration, ce qui est impossible sur un conteneur

Exemple de structure :

```
hp.lan
 └─ HP (OU)
     ├─ Utilisateurs
     │   ├─ Direction
     │   ├─ Compta
     │   └─ IT
     ├─ Ordinateurs
     │   ├─ Postes
```

```
    │   └─ Serveurs
    └─ Groupes
```

On peut rediriger les nouveaux PC vers une OU plutôt que vers `Computers` :

```
redircmp "OU=Postes,OU=Ordinateurs,OU=HP,DC=hp,DC=lan"
```

Comptes utilisateur

Attribut	Exemple	Remarque
Nom d'ouverture de session (pré-Windows 2000) / **sAMAccountName**	`HP\hpierret`	20 caractères max
UPN (*User Principal Name*)	`hpierret@hp.lan`	Ressemble à une adresse mail
DN (*Distinguished Name*)	`CN=Hugo Pierret,OU=IT,OU=Utilisateurs,OU=HP,DC=hp,DC=lan`	Chemin complet dans l'annuaire

Options courantes : *L'utilisateur doit changer le mot de passe à la prochaine ouverture de session*, *Le compte est désactivé*, date d'expiration, horaires d'accès (onglet Compte).

Groupes

Type

- **Sécurité** : sert à donner des **permissions** (et peut aussi servir de liste de distribution).
- **Distribution** : uniquement pour les listes de mail (Exchange), sans permissions.

Étendue (*scope*)

Étendue	Peut contenir	Utilisable pour des permissions
Domaine local (DL)	Utilisateurs et groupes de **n'importe quel domaine** de la forêt	Seulement dans **son** domaine
Globale (G)	Utilisateurs et groupes globaux de **son** domaine	Partout dans la forêt
Universelle (U)	Utilisateurs et groupes de toute la forêt	Partout dans la forêt (stockée dans le catalogue global)

Stratégie AGDLP (bonne pratique)

> **A**ccounts → **G**lobal → **D**omain **L**ocal → **P**ermissions

1. Les **comptes** (A) vont dans des groupes **globaux** organisés **par métier** : `GG_Compta`.
2. Les groupes globaux vont dans des groupes **domaine local** organisés **par ressource et par droit** : `DL_Partage-Compta_RW`.
3. On donne les **permissions** au groupe domaine local, **jamais** directement à un utilisateur.

➡ Un nouvel employé à la compta ? On l'ajoute à `GG_Compta` et il obtient tous les accès d'un coup.

PowerShell (module ActiveDirectory)

```
# OU
New-ADOrganizationalUnit -Name "HP" -Path "DC=hp,DC=lan"
New-ADOrganizationalUnit -Name "Utilisateurs" -Path "OU=HP,DC=hp,DC=lan"
New-ADOrganizationalUnit -Name "Compta" -Path "OU=Utilisateurs,OU=HP,DC=hp,DC=lan"

# Utilisateur
New-ADUser -Name "Alice Dupont" -GivenName Alice -Surname Dupont `
    -SamAccountName adupont -UserPrincipalName adupont@hp.lan `
    -Path "OU=Compta,OU=Utilisateurs,OU=HP,DC=hp,DC=lan" `
    -AccountPassword (Read-Host -AsSecureString "MDP") `
    -ChangePasswordAtLogon $true -Enabled $true

# Groupes
New-ADGroup -Name "GG_Compta" -GroupScope Global -GroupCategory Security -Path
"OU=Groupes,OU=HP,DC=hp,DC=lan"
New-ADGroup -Name "DL_Partage-Compta_RW" -GroupScope DomainLocal -GroupCategory Security -Path
"OU=Groupes,OU=HP,DC=hp,DC=lan"
Add-ADGroupMember -Identity "GG_Compta" -Members adupont
Add-ADGroupMember -Identity "DL_Partage-Compta_RW" -Members "GG_Compta"

# Consulter
Get-ADUser adupont -Properties *
Get-ADGroupMember GG_Compta
Get-ADUser -Filter * -SearchBase "OU=HP,DC=hp,DC=lan" | Select Name, SamAccountName

# Gestion courante
Set-ADAccountPassword adupont -Reset -NewPassword (Read-Host -AsSecureString)
```

```
Unlock-ADAccount adupont
Disable-ADAccount adupont
Move-ADObject -Identity "CN=Alice Dupont,OU=Compta,..." -TargetPath "OU=IT,..."
Search-ADAccount -LockedOut
```

Création en masse depuis un CSV :

```
Import-Csv .\users.csv -Delimiter ";" | ForEach-Object {
    New-ADUser -Name "$($_.Prenom) $($_.Nom)" -SamAccountName $_.Login `
        -UserPrincipalName "$($_.Login)@hp.lan" -Path $_.OU `
        -AccountPassword (ConvertTo-SecureString $_.MDP -AsPlainText -Force) -Enabled $true
}
```

Protection contre la suppression accidentelle

Les OU créées via la GUI sont **protégées** par défaut : on ne peut pas les supprimer directement. Pour en supprimer une :

- GUI : *Fonctionnalités avancées* → propriétés de l'OU → onglet **Objet** → décocher la protection.
- PowerShell : `Set-ADOrganizationalUnit "OU=Test,DC=hp,DC=lan" -ProtectedFromAccidentalDeletion $false`

Questions de révision

1. Quelle est la différence entre une OU et un conteneur comme `Users` ?
2. Explique AGDLP avec un exemple.
3. Quelle est la différence entre un groupe global et un groupe domaine local ?
4. Quelle est la différence entre sAMAccountName, UPN et DN ?
5. Pourquoi n'arrives-tu pas à supprimer une OU, et comment faire ?
6. Groupe de sécurité ou de distribution : lequel pour donner accès à un partage ?

Joindre un poste au domaine

Prérequis côté client

1. **DNS = le contrôleur de domaine** (`10.19.1.254`), par DHCP (option 006) ou en manuel. ⚠ C'est **la cause n°1 des échecs**. Avec 8.8.8.8 en DNS, le client ne trouve jamais `hp.lan` .
2. Connectivité : `ping srv01.hp.lan`.
3. SID unique : machine clonée → **sysprep** obligatoire.
4. Heure synchronisée : Kerberos tolère **5 minutes** d'écart maximum.
5. Édition **Pro / Entreprise / Éducation** de Windows : **Windows Famille ne peut pas rejoindre un domaine**.
6. Un compte du domaine autorisé : tout utilisateur du domaine peut joindre **jusqu'à 10 machines** par défaut, un admin du domaine sans limite.

Test rapide avant de joindre :

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.hp.lan
```

Si le DC apparaît, le DNS est bon.

En GUI

`sysdm.cpl` → onglet **Nom de l'ordinateur** → **Modifier** → **Membre d'un domaine** : `hp.lan` → identifiants `HP\Administrateur` → « Bienvenue dans le domaine hp.lan » → **redémarrer**.

En PowerShell

```
# Renommer et joindre en une seule fois
Add-Computer -DomainName "hp.lan" -NewName "CLI01" -Credential HP\Administrateur `
    -OUPath "OU=Postes,OU=Ordinateurs,OU=HP,DC=hp,DC=lan" -Restart

# Quitter le domaine
Remove-Computer -UnjoinDomainCredential HP\Administrateur -WorkgroupName WORKGROUP -Restart
```

Pré-créer le compte ordinateur dans AD (par exemple pour le placer directement dans la bonne OU) :

```
New-ADComputer -Name "CLI01" -Path "OU=Postes,OU=Ordinateurs,OU=HP,DC=hp,DC=lan"
```

Ouvrir une session de domaine

Sur l'écran de connexion → **Autre utilisateur** → `HP\adupont` ou `adupont@hp.lan`. Pour une session **locale** : `.\Administrateur` (le `.` désigne la machine locale).

Vérifier :

```
whoami                 :: hp\adupont
whoami /upn            :: adupont@hp.lan
echo %logonserver%     :: \\SRV01
systeminfo | findstr /i "domaine"
```

Dépannage

Erreur ou symptôme	Cause / solution
« Un contrôleur de domaine AD pour le domaine hp.lan n'a pas pu être contacté »	**DNS** du client ≠ IP du DC, ou zone/enregistrements SRV absents
« The SID of the domain … was identical to the SID of this machine »	VM clonée sans sysprep : faire un sysprep et réessayer
Erreur liée à l'heure / Kerberos	Corriger l'heure ou le fuseau horaire (`w32tm /resync`)
« La relation d'approbation entre cette station de travail et le domaine principal a échoué »	Mot de passe du compte ordinateur désynchronisé (souvent après restauration d'un **snapshot** du client). `Test-ComputerSecureChannel -Repair -Credential HP\Administrateur`, ou retirer puis rejoindre le domaine
Joindre fonctionne mais la session est lente ou les GPO ne s'appliquent pas	DNS secondaire public (8.8.8.8) sur le client : ne mettre **que** les DC en DNS

Vérifier le canal sécurisé : `Test-ComputerSecureChannel -Verbose` ou `nltest /sc_verify:hp.lan`.

Questions de révision

1. Quel paramètre réseau du client est indispensable pour joindre le domaine ?
2. Quelle édition de Windows 10/11 ne peut pas rejoindre un domaine ?
3. Où arrivent par défaut les comptes ordinateurs ? Comment les placer ailleurs ?

4. Comment se connecter avec un compte **local** sur un PC membre du domaine ?
5. Après restauration d'un snapshot du client, la connexion échoue avec une erreur de relation d'approbation. Pourquoi ?

4. À venir

Aperçu des notions pas encore vues

À venir : GPO et partages (aperçu)

> Notions pas encore vues en cours : cette page n'est qu'un aperçu, à compléter quand on les verra.

GPO (stratégies de groupe)

- Console : `gpmc.msc`. Une GPO est créée puis **liée** à un site, un domaine ou une **OU**.
- Deux parties : **Configuration ordinateur** (appliquée au démarrage) et **Configuration utilisateur** (appliquée à l'ouverture de session).
- Ordre d'application : **L**ocal → **S**ite → **D**omaine → **OU** (**LSDOU**). La dernière appliquée l'emporte.
- Commandes : `gpupdate /force` (appliquer maintenant), `gpresult /r` (voir les GPO appliquées), `gpresult /h rapport.html`.
- Exemples classiques : fond d'écran imposé, mappage de lecteurs, blocage du panneau de configuration, politique de mots de passe (uniquement dans la *Default Domain Policy*).

Partages et permissions NTFS

- Deux couches de permissions : les **permissions de partage** (accès réseau) et les **permissions NTFS** (accès au disque). **La plus restrictive des deux l'emporte.**
- Bonne pratique : partage en *Tout le monde : Contrôle total* (ou Utilisateurs authentifiés), puis gestion fine en **NTFS**, avec des groupes DL (AGDLP).
- Chemin UNC : `\\SRV01\Compta`. Mapper un lecteur : `net use P: \\SRV01\Compta` ou via GPO.
- PowerShell : `New-SmbShare -Name Compta -Path D:\Partages\Compta -FullAccess "HP\DL_Partage-Compta_RW"`.

0. Prise de notes

03-11-26

Création d'Organisation Unit :

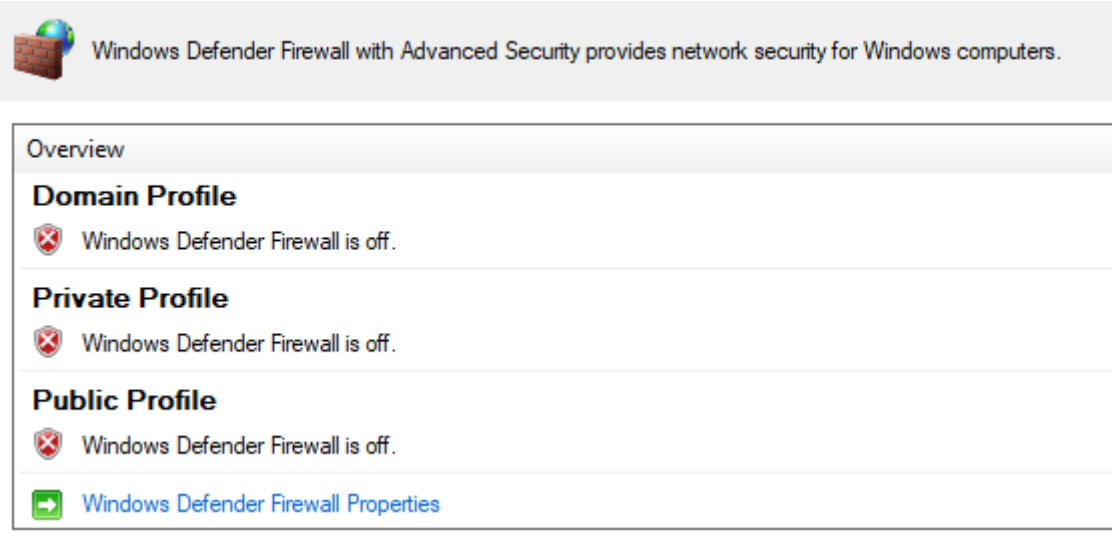
déplacement des computer et user dedans

Prohibit access to Control Panel and PC settings -> enabled car c'est un gpo qu'on a voulu mettre en place comme exemple
gpupdate
On a créé 2 Organizatioanl Unit, Domain Computers et Domain Users où on a mis respectivement les CLNT et utilisateurs
puis placé les gpos dans les domain, crtl panel dans celui user et power managment dans celui computer
un gpo aussi à la racine s1901.local pour expliquer la hierarchie des gpos
GPO status: Computer configuration settings disabled (si j'ai bien compris c'est pour gagner des performances; à disable quans ce sont des clés machines) On a disable DDP mais pas DDCP
Niveau de GPO

EXO :

Firewall off (domain profile) pour toutes les machines
Firewall always off (all profiles) pour les DC's
depuis SRV01 -> ping clnt01.local -> time out (ça ne devrait pas)
commande wf

Ajout d'une gpo dans DC "Firewall always off" avec une priorité supp à DDCP
computer config settings disabled car settings machine



Ajout d'une gpo à la racine "Firewall always off" avec une priorité supp à DDP
user config settings disabled
même gpo mais on met juste le domain profile à off

0. Prise de notes

05-11-26

EXO :

Environnement domanial s121901.tfdom
Un DC \\SRV01, 10.112.0.30/27
DNS forwarders : 10.2.0.1 et 10.2.0.2
Un member \\SRV02, 10.112.0.29/27
Un routeur (ce que vous voulez comme solution), deux NIC's, 10.112.0.1/27 d'un côté et DHCP de l'autre côté (goulotte), routeur qui fait juste du NAT et de permettre au réseau 10.112.0.0/27 d'accéder à Internet
Deux clients, en DHCP
Firewall off pour tous, profil domanial
Firewall off, tous les profils, pour les dc's
Désactiver IEESC pour tous les profils
Supprimer le Ctrl+Alt+Delete pour tous
Console de mgmt (fichier .msc) uniquement pour les admin's
Accès au registre idem, uniquement pour les admin's
Ne pas afficher le derneir nom d'utilisateur (à l'ouverture de session)

J'ai rencontrer un probleme VMWare courant, lors de la config réseau du srv01 avant de le promettre, il m'affichait une gateway 0.0.0.0 en plus de 10.112.0.1. C'est un problème au niveau de la NIC donc il faut carrément la désinstaller puis la résinstaller (via `devmgmt` + vmware carte réseaux)

ATTENTION de mettre en place les user dans les OU avec dsa pour ne pas se retrouver à ne plus pouvoir rien faire en tant qu'admin si on désactive les .msc et/ou regedit

TODO une page qui répertorie tous les path de gpo utiles
https://gpo.tools/#v=srv2022

`Computer Configuration` > `Policies` (or `Windows Settings`) > `Security Settings` > `Local Policies` > `Security Options` -> **`Interactive logon: Do not require CTRL+ALT+DEL`**
SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A8-37EF-4b3f-8CFC-4F3A74704073} -> for user
SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073} -> for admin

C:\Windows\SYSVOL\sysvol\s121901.tfdom\Policies -> dans la vm l'emplacement des gpo's

admx -> model de gpo

0. Prise de notes

06-11-26

gpresult

SRV02 -> member server -> files server
On change la partition D: en B: puis on en créé une nouvelle en D: de 100Go
ACL : access control list

NTFS
notions de permissions de partage

0. Prise de notes

09-11-26

Installationn d'un debian sous vmware

/etc/apt/source.list

```
deb https://deb.debian.org/debian trixie main contrib non-free
deb https://security.debian.org/debian-security trixie-security main contrib non-free
deb https://deb.debian.org/debian trixie-updates main contrib non-free
```

10-11-26

Setup ESXi sur les Z440 qui nous sont à disposition
On l'a booté
on a setup :
- rename localhost
- disable ipv6
- password
- écraser disque dur de 500 Go

diskpart pour fusionner deux partitions et delete une