1. Labo & outils

Préparation des VM et boîte à outils

- Préparer le labo : VM, snapshots, sysprep
- Boîte à outils : raccourcis et commandes

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
`dsa.msc`	**Utilisateurs et ordinateurs Active Directory** (ADUC)

Commande	Console
`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` ?