

Projet 1: Intégration d'un poste Linux dans un domaine Active Directory (récit de réalisation)

Résumé :

J'ai monté un lab Windows Server pour créer un domaine **lab.local**, installé les rôles **AD DS/DNS**, puis créé une **OU**, deux **utilisateurs** (Alice, Bob) et un **groupe** (IT_Group). J'ai ensuite tenté d'intégrer ma VM **Kali Linux** au domaine. Le projet m'a permis de configurer la **résolution DNS**, comprendre la **jointure realm/SSSD/Kerberos**, gérer des **GPO** de base et résoudre plusieurs incidents (DNS du mauvais serveur, paquets manquants, service SSSD inactif).

Contexte & objectifs

Contexte. Je travaille sur un PC avec peu d'espace disque. J'ai choisi un lab minimal : 1 VM **Windows Server** (contrôleur de domaine) et ma VM **Kali** comme poste client.

Objectifs :

- 1) Créer le domaine **lab.local** (AD DS + DNS).
 - 2) Créer **OU/Groupes/Utilisateurs** et prouver la gestion centralisée.
 - 3) Intégrer **Kali** au domaine via **realm/SSSD/Kerberos**.
 - 4) Documenter précisément les **difficultés** et leurs **solutions**.
-

Architecture du lab

- **DC-TEST** (Windows Server 2019/2022) — AD DS + DNS
IP (host-only) utilisée : **192.168.56.101**
Domaine : **lab.local**
- **Kali Linux** (poste client) — tentative de jointure au domaine via realmd/sss
- Réseau **Host-Only** VirtualBox pour l'isolement + (au besoin) NAT pour Internet

Schéma logique (simple) :

Kali :

192.168.56.0/24 (Host-Only)

DC-TEST (AD DS/DNS)

Domaine : lab.local

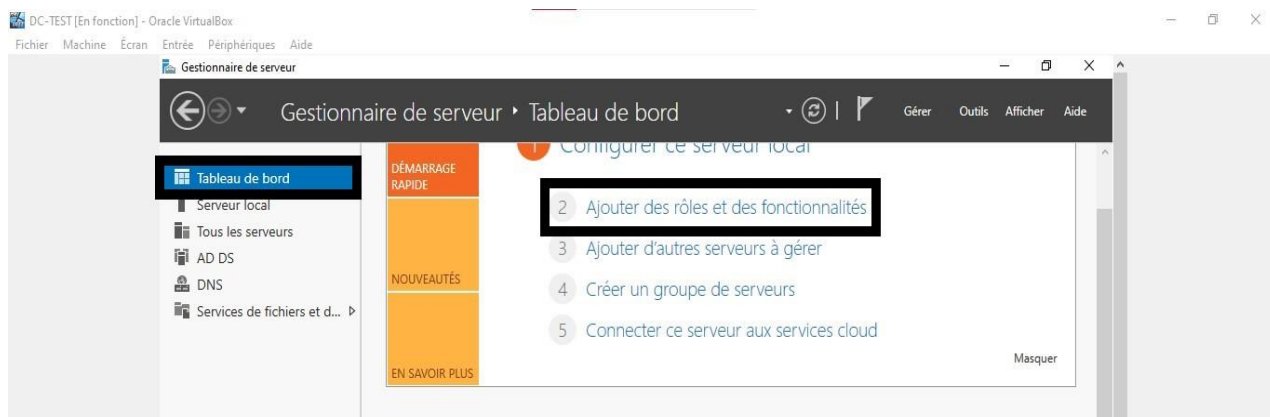
Journal de réalisation

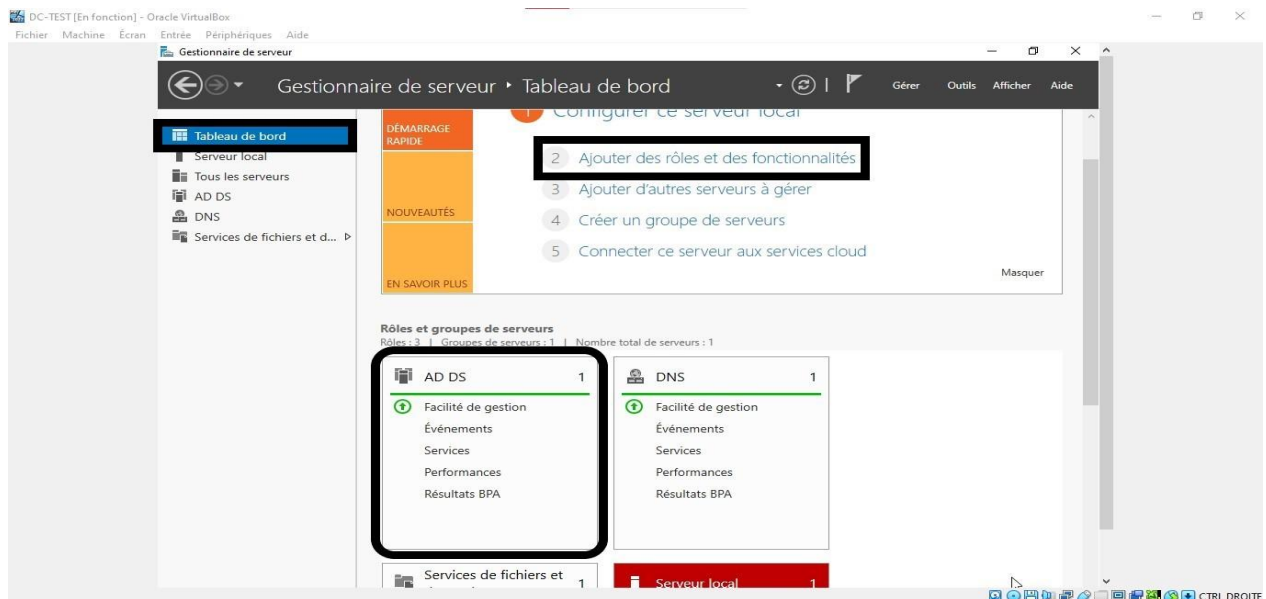
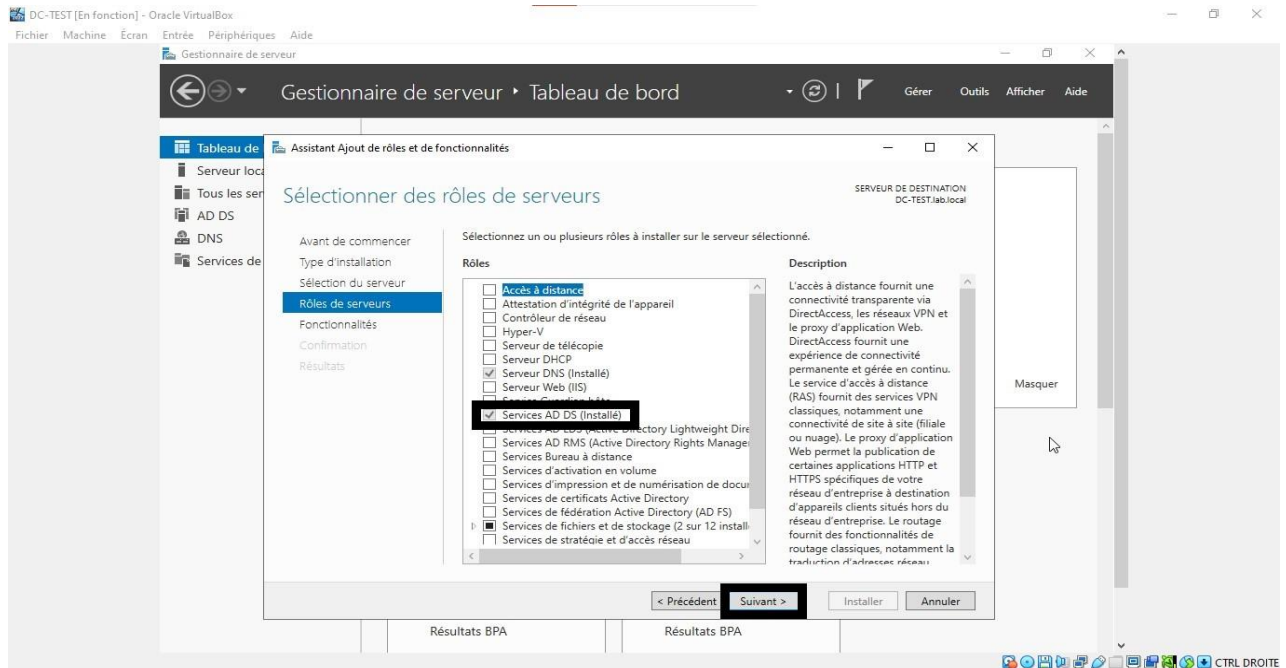
1) Installation & configuration du DC

- Installation de Windows Server en VM → rôle **AD DS + DNS**.
- **Promotion** en contrôleur de domaine : **lab.local**.
- **Renommage** de l'hôte en DC-TEST.

Captures :

- *Rôles AD DS & DNS installés (vert dans Server Manager)*
AD DS & DNS OK



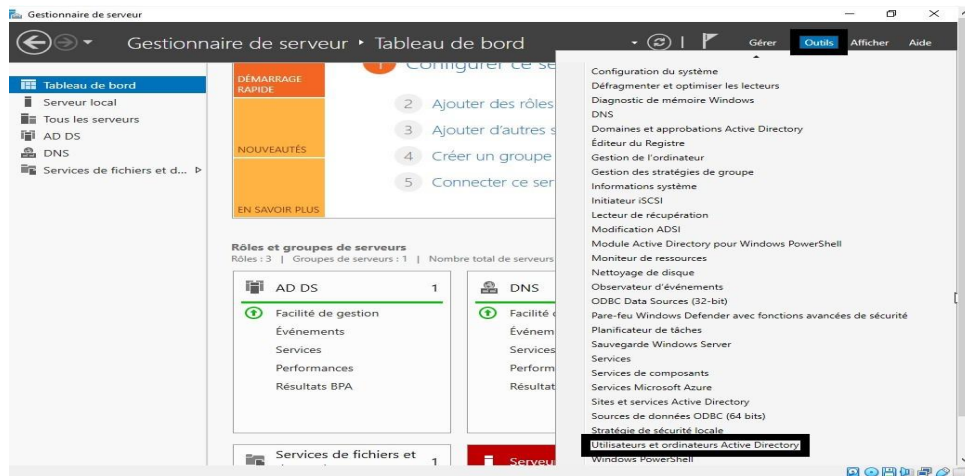


2) Organisation AD : OU, utilisateurs, groupes

- Création de l'**OU** IT et (si besoin) Users.
- Création des **utilisateurs** : Alice IT (login alice.it), Bob User (login bob.it).
- Création du **groupe** IT_Group et ajout d'**Alice** comme membre.

Captures :

- *Création d'utilisateur dans l'OU IT*
Création d'utilisateur (Alice)



Nouvel objet - Utilisateur

Créer dans : lab.local/IT

Prénom : Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur : @lab.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent **Suivant >** Annuler

- Création de l'OU IT :

Nouvel objet - Unité d'organisation

Créer dans : lab.local/


Nom :

☒ Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

- Création du **groupe** IT_Groupe

Nouvel objet - Groupe ✕

 Créer dans : lab.local/IT

Nom du groupe :

Nom de groupe (antérieur à Windows 2000) :

<p>Étendue du groupe</p> <p><input type="radio"/> Domaine local</p> <p><input checked="" type="radio"/> Globale</p> <p><input type="radio"/> Universelle</p>	<p>Type de groupe</p> <p><input checked="" type="radio"/> Sécurité</p> <p><input type="radio"/> Distribution</p>
--	--

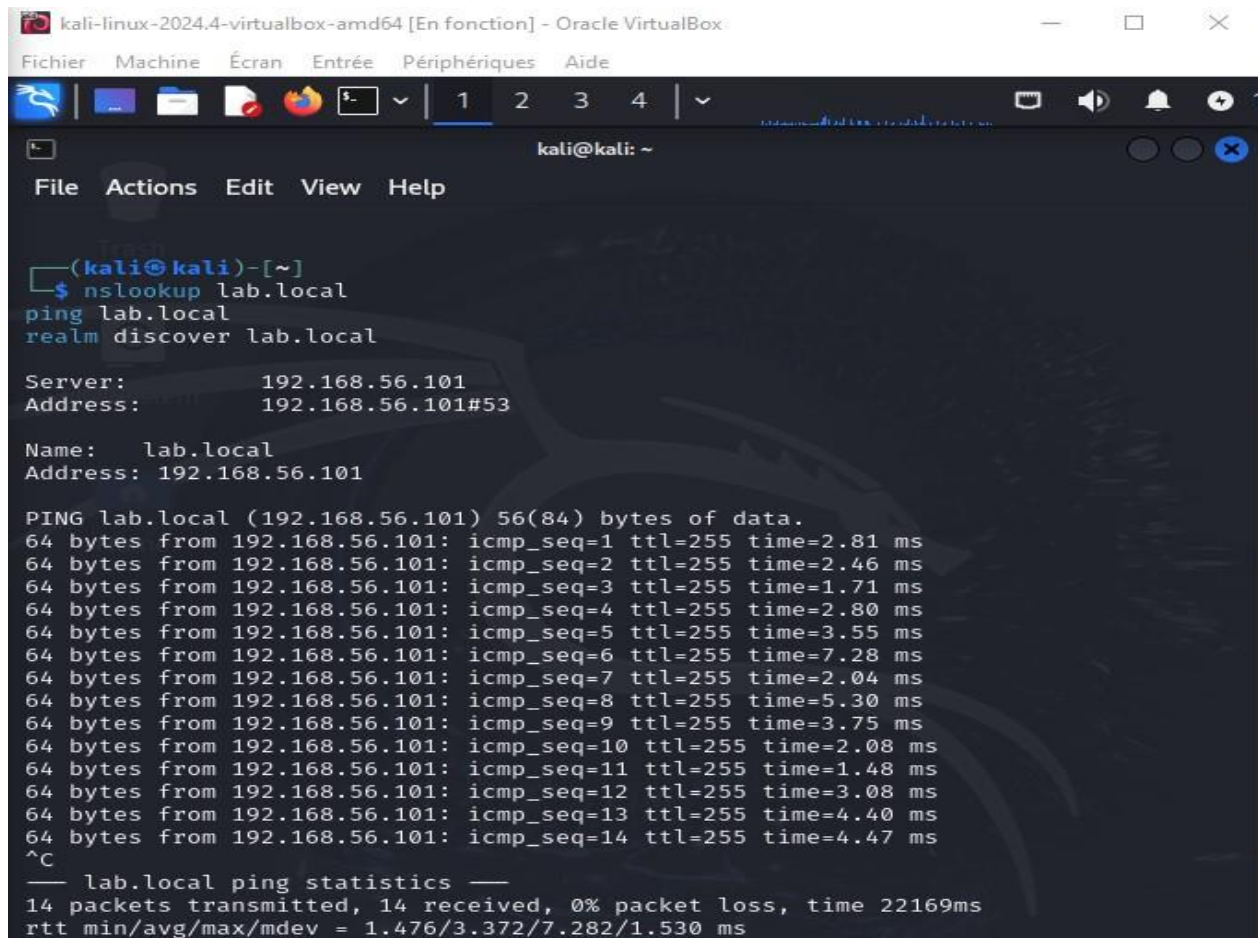
3) Préparation de Kali & vérifs réseau/DNS

- Sur Kali, tests de connectivité vers le DC : ping 192.168.56.101.
- **DNS** : premier blocage — /etc/resolv.conf pointait vers **10.0.2.3** (DNS NAT VirtualBox).
Correction : j'ai forcé

```
nameserver 192.168.56.101
nameserver 8.8.8.8
```
- Vérifs : nslookup lab.local et ping lab.local OK.

Captures :

- *resolv.conf incorrect (10.0.2.3) → cause du « realm not found »*
resolv.conf mauvais DNS
- *Après correction : lab.local résolu et joignable*
Ping & nslookup OK



```
kali-linux-2024.4-virtualbox-amd64 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

kali@kali: ~
File  Actions  Edit  View  Help

(kali@kali)-[~]
$ nslookup lab.local
ping lab.local
realm discover lab.local

Server:          192.168.56.101
Address:         192.168.56.101#53

Name:   lab.local
Address: 192.168.56.101

PING lab.local (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=255 time=2.81 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=255 time=2.46 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=255 time=1.71 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=255 time=2.80 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=255 time=3.55 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=255 time=7.28 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=255 time=2.04 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=255 time=5.30 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=255 time=3.75 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=255 time=2.08 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=255 time=1.48 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=255 time=3.08 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=255 time=4.40 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=255 time=4.47 ms
^C
— lab.local ping statistics —
14 packets transmitted, 14 received, 0% packet loss, time 22169ms
rtt min/avg/max/mdev = 1.476/3.372/7.282/1.530 ms
```

4) Découverte du domaine & tentative de jointure

- `realm discover lab.local` → **OK** (domaine détecté).
- `sudo realm join -U Administrator lab.local` → erreurs successives :
 - **Paquets manquants** signalés (sssd, libnss-sss, libpam-sss, adcli...).
 - **sssd** inactive (dead) puis **échec** sans `/etc/krb5.keytab` (normal tant que la jointure n'a pas abouti).
 - Besoin de **réinstaller/forcer** certains paquets et de lancer `realmd/sssd` quand la conf existe.

Captures :

- *Découverte du domaine réussie (realm discover)*

```
(kali@kali)-[~]
$ realm discover lab.local

lab.local
type: kerberos
realm-name: LAB.LOCAL
domain-name: lab.local
configured: no
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: libnss-sss
required-package: libpam-sss
required-package: adcli
required-package: samba-common-bin

(kali@kali)-[~]
$
```

État au moment de la mise en pause :

- AD DS/DNS opérationnels, OU/Users/Groupes créés et testés.
- DNS Kali corrigé, découverte du domaine **OK**.
- Jointure non finalisée à cause d'un enchaînement **paquets/SSSD** (et contrainte d'espace disque pour poursuivre confortablement).

Difficultés rencontrées & comment je les ai traitées :

- 1) **DNS côté Kali pointait vers 10.0.2.3 (NAT VirtualBox) :**
correction du resolv.conf pour pointer d'abord sur **192.168.56.101** (DC), avec **8.8.8.8** en secours.
 - 2) **realm join** se plaignait de **paquets manquants** malgré des installations :
j'ai relancé apt update + réinstallé **realmd/sss/libnss-sss/libpam-sss/adcli** et vérifié dpkg -l.
 - 3) **sssd inactive / keytab absente** : j'ai compris que /etc/krb5.keytab est généré **après** une jointure réussie : inutile d'insister à démarrer sssd tant que realm join échoue.
 - 4) **Contraintes de stockage** : j'ai limité les VMs et conservé uniquement l'essentiel pour documenter le process.
-

Résultats obtenus

- Domaine **lab.local** opérationnel, DNS configuré.
 - OU/Users/Groupes créés (Alice dans IT_Group).
 - Kali configure le DNS correctement et **voit** le domaine (realm discover).
 - La jointure complète sera reprise plus tard une fois l'environnement allégé.
-

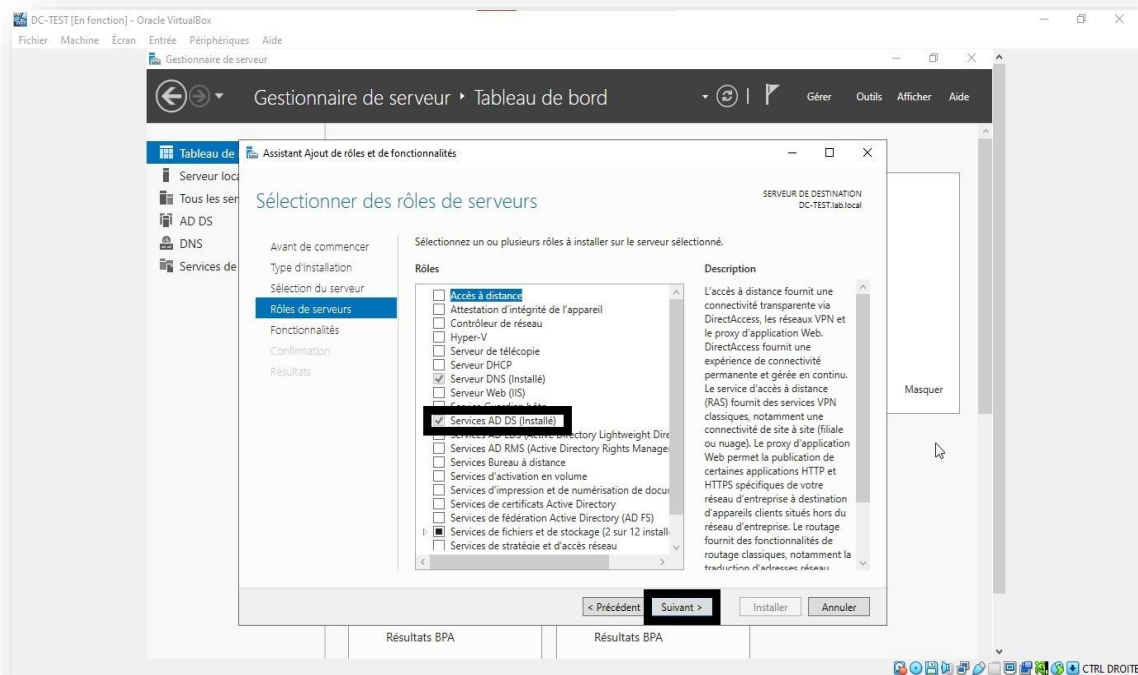
Compétences que j'ai réellement pratiquées

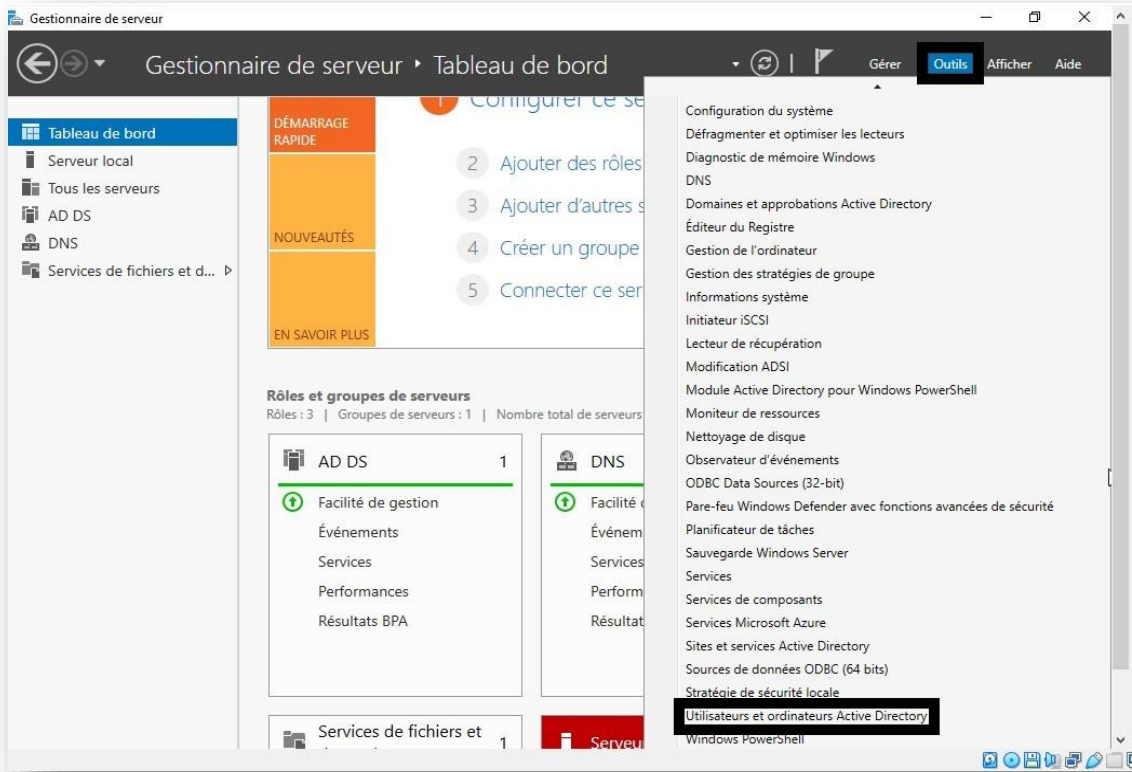
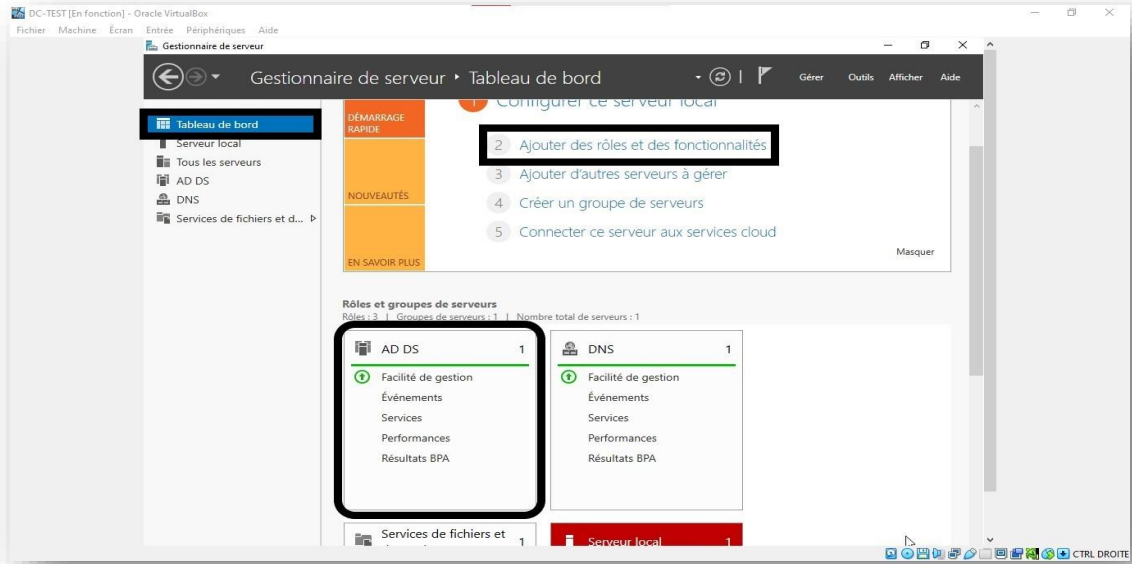
- **Windows Server / AD DS / DNS** : installation, promotion en DC, gestion OU/Users/Groupes.
- **Réseau VirtualBox** : Host-Only, adressage, isolation.
- **Linux (Kali)** : DNS, realmd, sssd, Kerberos (notions de keytab), dépannage resolv.conf.
- **Méthodo** : diagnostic d'incidents, tests (ping/nslookup/realm), documentation par captures.

Prochaines étapes

- Finaliser la jointure Kali ↔ AD (après nettoyage d'espace disque), vérifier realm list + id alice.it@lab.local.
- (Option) Ajouter une VM client Windows et lier des **GPO** ciblées (mot de passe, bannière, etc.).

Annexes — Captures (reprises en grand)





Nouvel objet - Groupe

Créer dans : lab.local/IT

Nom du groupe :
IT_Group

Nom de groupe (antérieur à Windows 2000) :
IT_Group

Étendue du groupe

- ☐ Domaine local
- ☒ Globale
- ☐ Universelle

Type de groupe

- ☒ Sécurité
- ☐ Distribution

OK Annuler

Nouvel objet - Unité d'organisation

Créer dans : lab.local/

Nom :
IT

☒ Protéger le conteneur contre une suppression accidentelle

OK Annuler Aide

Nouvel objet - Utilisateur

Créer dans : lab.local/IT

Prénom : Alice Initiales :

Nom : IT

Nom complet : Alice IT

Nom d'ouverture de session de l'utilisateur :
alice.it @lab.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
LAB\ alice.it

< Précédent Suivant > Annuler

Nouvel objet - Utilisateur

Créer dans : lab.local/Users

Prénom : Bob Initiales :

Nom : IT

Nom complet : Bob IT

Nom d'ouverture de session de l'utilisateur :
bob.it @lab.local

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
LAB\ bob.it

< Précédent Suivant > Annuler

```
(kali@kali)-[~]  
$ realm discover lab.local  
  
lab.local  
type: kerberos  
realm-name: LAB.LOCAL  
domain-name: lab.local  
configured: no  
server-software: active-directory  
client-software: sssd  
required-package: sssd-tools  
required-package: sssd  
required-package: libnss-sss  
required-package: libpam-sss  
required-package: adcli  
required-package: samba-common-bin  
  
(kali@kali)-[~]  
$
```

```
(kali@kali)-[~]  
$ sudo nano /etc/resolv.conf
```

kali-linux-2024.4-virtualbox-amd64 [En fonction] - Oracle VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

1 2 3 4

kali@kali: ~

File Actions Edit View Help

GNU nano 8.6 /etc/resolv.conf *

```
# Generated by NetworkManager  
nameserver 192.168.56.101  
search lab.local
```

^G Help ^O Write Out ^F Where Is ^X Cut ^T Execute
^X Exit ^R Read File ^E Replace ^U Paste ^J Justify ^C Location
Go To Line

```
kali-linux-2024.4-virtualbox-amd64 [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide

kali@kali: ~
File  Actions  Edit  View  Help

(kali@kali)-[~]
$ nslookup lab.local
ping lab.local
realm discover lab.local

Server:      192.168.56.101
Address:     192.168.56.101#53

Name:   lab.local
Address: 192.168.56.101

PING lab.local (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=255 time=2.81 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=255 time=2.46 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=255 time=1.71 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=255 time=2.80 ms
64 bytes from 192.168.56.101: icmp_seq=5 ttl=255 time=3.55 ms
64 bytes from 192.168.56.101: icmp_seq=6 ttl=255 time=7.28 ms
64 bytes from 192.168.56.101: icmp_seq=7 ttl=255 time=2.04 ms
64 bytes from 192.168.56.101: icmp_seq=8 ttl=255 time=5.30 ms
64 bytes from 192.168.56.101: icmp_seq=9 ttl=255 time=3.75 ms
64 bytes from 192.168.56.101: icmp_seq=10 ttl=255 time=2.08 ms
64 bytes from 192.168.56.101: icmp_seq=11 ttl=255 time=1.48 ms
64 bytes from 192.168.56.101: icmp_seq=12 ttl=255 time=3.08 ms
64 bytes from 192.168.56.101: icmp_seq=13 ttl=255 time=4.40 ms
64 bytes from 192.168.56.101: icmp_seq=14 ttl=255 time=4.47 ms
^C
— lab.local ping statistics —
14 packets transmitted, 14 received, 0% packet loss, time 22169ms
rtt min/avg/max/mdev = 1.476/3.372/7.282/1.530 ms
```