

Durée	4 périodes
Format	Individuel
Matériel	PC individuel

Contexte :

LDAP (Lightweight Directory Access Protocol) est un protocole standard ouvert qui permet d'interroger et de modifier un annuaire centralisé contenant des informations sur les utilisateurs, groupes, machines et ressources. Dans les environnements d'entreprise, cet annuaire sert de « source de vérité » pour l'authentification, l'autorisation et la gestion des identités, évitant la duplication des comptes et simplifiant l'administration. Microsoft Active Directory (AD) implémente LDAP (ainsi que Kerberos et d'autres services) pour offrir un domaine Windows où les comptes, les stratégies et les appartenances aux groupes sont centralisés. En pratique, LDAP fournit la structure hiérarchique et les requêtes (filtres, attributs, DN), tandis que le contrôleur de domaine AD stocke et expose ces données de manière sécurisée et robuste.

Dans cet exercice, le rôle de serveur d'annuaire sera assuré par un contrôleur de domaine Windows Server 2022 avec Active Directory. Il hébergera les objets essentiels (utilisateurs, OU, groupes de sécurité) et publiera un point d'accès LDAP. Côté client, un serveur Linux Ubuntu 24 exécutera Nextcloud, une plateforme de collaboration (fichiers, partage, apps) qui interrogera l'annuaire AD via son module d'authentification LDAP. L'objectif est que Nextcloud délègue l'authentification à AD : les utilisateurs s'y connecteront avec leurs identifiants de domaine, et l'appartenance aux groupes AD permettra de contrôler l'accès aux ressources Nextcloud (mapping groupes→rôles, quotas, dossiers). Cette intégration illustre les bénéfices d'un annuaire unique : comptes centralisés, révocation simplifiée et cohérence des profils entre services.

Au final, vous disposerez d'une application Linux moderne consommant un annuaire Microsoft via LDAP, comme cela se pratique dans de nombreuses infrastructures mixtes.

Pré-requis

- VM Ubuntu Server et Desktop 22.04
- Accès administrateur (sudo).
- Connexion réseau fonctionnelle.
- Connaissances de base en administration Linux et réseau.

Exercice 1 – Installation du serveur Windows Server 2022 avec rôle Active Directory

1. Téléchargement et installation du système :

- Récupérez l'ISO officielle de Windows Server 2022 depuis le site Microsoft:
<https://www.microsoft.com/fr-fr/evalcenter/download-windows-server-2022>
- Installez le système sur une machine virtuelle ou physique dédiée.

2. Configuration réseau :

- VMNET10
- Adresse IP fixe : **10.10.10.6/24**
- Passerelle (Gateway) : **10.10.10.2**
- DNS : **127.0.0.1** (le serveur pointera vers lui-même)

3. Paramètres système :

- Nom d'hôte (Serveur Name) : **srv-win22.01**
- Fuseau horaire et synchronisation de l'heure correctement configurés.
- Désactiver la fonctionnalité **Internet Explorer Enhanced Security Configuration (IE ESC)** pour faciliter la gestion.

4. Installez VMware tool.

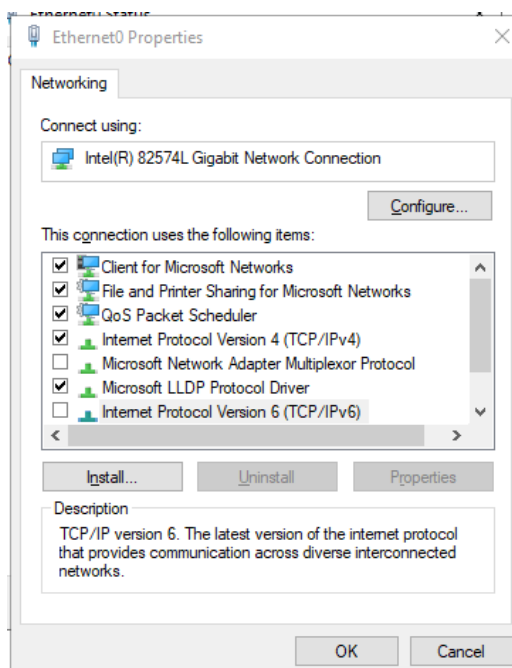
5. Faites un snapshot du la VM

6. Rôle Active Directory :

- Installer le rôle **Active Directory Domain Services (AD DS)**.
- Promouvoir le serveur en **contrôleur de domaine** pour le domaine : **emfldap.lan**.

7. Forcer l'utilisation d'IPv4 et désactivation d'IPv6

- Passez la commande **netsh interface ipv6 set prefixpolicy ::ffff:0:0/96 50 0** pour éviter d'utiliser IPv6 et forcer l'utilisation d'IPv4
- Décochez IPv6 :



8. Configuration du forwarder DNS :

- Vous avez installé l'AD sur **srv-win22-01** et l'avez promu contrôleur de domaine pour **emfldap.lan**. Vous avez configuré **127.0.0.1** comme serveur DNS sur le serveur, il n'a donc pas accès à Internet. Pour pallier ce problème, configurez un forwarder (8.8.8.8).

9. Configuration d'un conditional forwarder

- Le domaine **emf300.lan** n'est pas connu sur Internet. Si vous voulez pouvoir le résoudre depuis **srv-win22-01**, il faut configurer sur celui-ci un conditional forwarder qui définit que le serveur responsable de la zone **emf300.lan** est le serveur 10.10.10.5.

Exercice 2 – Création de la structure LDAP dans Active Directory

1. Connexion au serveur AD

- Connectez-vous à **srv-win22.01** avec un compte administrateur du domaine **emfldap.lan**.
- Ouvrez la console **Active Directory Users and Computers (ADUC)**.

2. Création de l'arborescence d'unités organisationnelles (OU)

- Dans la racine du domaine **emfldap.lan**, créez une OU principale : **emfldap**.
- À l'intérieur de cette OU, créez deux sous-OU :
 - **Groups**
 - **Users**

3. Création des groupes

- Dans l'OU **Groups**, créez les groupes de sécurité suivants :
 - **IT**
 - **Direction**
 - **Finance**
- Type de groupe : **Security**
- Portée du groupe : **Global** (par défaut, adaptée à ce scénario).

4. Création des utilisateurs

- Dans l'OU **Users**, créez les comptes suivants :
 - **Brad Pitt**
 - Nom d'utilisateur (logon) : **pittb**
 - Groupe : **G_IT**
 - Mot de passe : **Test123**
 - Paramètres du mot de passe :
 - **Le mot de passe n'expire jamais**
 - **L'utilisateur ne peut pas changer son mot de passe**
 - **Jolie Angelina**
 - Nom d'utilisateur (logon) : **joliea**
 - Groupe : **G_Finance**
 - Mot de passe : **Test123**
 - Paramètres du mot de passe :
 - **Le mot de passe n'expire jamais**
 - **L'utilisateur ne peut pas changer son mot de passe**
 - **Pacino Al**
 - Nom d'utilisateur (logon) : **pacinoa**
 - Groupe : **G_Direction**
 - Mot de passe : **Test123**
 - Paramètres du mot de passe :
 - **Le mot de passe n'expire jamais**
 - **L'utilisateur ne peut pas changer son mot de passe**

- **LDAP Reader**
 - Nom d'utilisateur (logon) : **ldapreader**
 - Groupe : Domain Users
 - Mot de passe : **Test123**
 - Paramètres du mot de passe :
 - **Le mot de passe n'expire jamais**
 - **L'utilisateur ne peut pas changer son mot de passe**

Exercice 3 – Configuration DNS de srv-keabind-01

1. Configuration d'un forwarder sur srv-keabind-01 pour la zone emfldap.lan

- Si vous voulez pouvoir résoudre le domaine **emfldap.lan** depuis votre serveur **srv-keabind-01**, il faut configurer sur celui-ci une zone et un forwarder qui définit que le serveur responsable de la zone **emfldap.lan** est le serveur **10.10.10.6**. Ajoutez cette configuration à la fin du fichier `named.conf.options`.

```
zone "emfldap.lan" {  
    type forward;  
    forwarders { 10.10.10.6; };  
};
```

- Redémarrer le service `bind9`

Exercice 4 – Installation et configuration de Nextcloud srv-keabind-01

Nextcloud est un logiciel libre de site d'hébergement de fichiers et une plateforme de travail collaboratif. Votre entreprise souhaite l'installer pour en profiter en interne gratuitement. Il va falloir l'installer sur votre serveur ubuntu avec le commande **sudo snap install nextcloud**

Astuce : désactivez le cache TTL pour que les modifications que vous ferez par la suite dans l'AD soient effectives immédiatement :

`sudo nextcloud.occ ldap:set-config s01 ldapCacheTTL 0`



Accédez à nextcloud en tapant l'adresse IP <http://10.10.10.5> dans votre navigateur.

- Définissez un user password : admin – Test123
- Cliquez sur le rond avec un « A » en haut à droite de l'écran.
- Cliquez sur **Apps**, puis choisissez **App Bundles**.
- Repérez **LDAP user and group backend**, et cliquez sur **Enable**.
- Cliquez sur le rond avec un « A » en haut à droite de l'écran.
- Cliquez sur **Administration Settings**, puis choisissez **LDAP/AD integration**
- Configurez le serveur LDAP

Exercice 5 – Création de shares dans Nextcloud

Dans le portail nextcloud, créez un share par groupe avec les droits correspondants
Share_IT -> RW ->G_IT

- Share_Finance -> RW ->G_Finance
Share_Direction -> RW ->G_Direction
- Share_Common -> RW ->G_IT, G_Finance, G_Direction

Déconnectez-vous du portail et loguez-vous avec chacun des users définis dans l'AD.
Supprimez les fichiers/dossiers autres que les shares créés précédemment.
Contrôlez à chaque fois que vous avez bien les 2 shares que le user doit avoir en fonction de ce qui a été configuré précédemment.

Arrivez-vous vous logguer avec le user ldapreader ? Pourquoi ?

Exercice 6 – Modifications dans l'AD

Pour démontrer l'avantage de l'utilisation de LDAP avec un système comme Nextcloud, nous allons simuler des changements au sein de l'entreprise dans l'AD, ce qui devrait entraîner des conséquences dans Nextcloud.

1. Angelina Jolie a pris du galon, elle est maintenant membre de la direction (mais plus des finances). Effectuez ce changement dans l'AD, puis logout/login dans nextcloud. Constatez-vous un changement au niveau des shares auxquels elle a accès ?

2. Brad Pitt a voulu fricoter avec Angelina Jolie, mais s'est fait licencié pour cette raison. Désactivez son user dans l'AD et essayez de vous connecter dans Nextcloud avec son user. Est-ce toujours possible ?

Vous pouvez constater les avantages d'une gestion centralisée des utilisateurs au sein de l'AD. Le protocole LDAP, qui est multiplateforme, permet à un serveur Linux d'interroger un serveur Windows AD.

3. Angelina n'a pas supporté la pression liée à son poste à la direction, elle est revenue aux Finances.
 4. Brad Pitt s'est fait réembaucher à l'IT.
- ➔ Reconfigurer les users dans leur bon groupe 😊

Exercice 7 – Nextcloud client (Nextcloud Desktop)

Installez le client Nextcloud Desktop sur srv-win22-01, loguez-vous avec joliaa.
Installez le client Nextcloud Desktop sur srv-keabind-01, loguez-vous avec pacinoa.

Mettez des fichiers dans Share_Common. Regardez qu'ils apparaissent chez l'autre utilisateur. Voilà vous venez de monter votre propre petit cloud pour du stockage fichier.

Exercice 6 – Test sur le client avec ldapsearch

Pour explorer un annuaire LDAP, vous pouvez utiliser la commande ldap search pour faire du debug.

Installez le paquet ldap-utils sur srv-keabind-01.

En vous basant sur cette commande, modifiez-la pour essayer de récupérer les utilisateurs que vous avez créé dans l'AD précédemment :

```
ldapsearch -x -H ldap:// SRV-AD-IP -D "ldapreader@emfldap.lan" -w 'Password' -b "OU=...,OU=...,DC=emfldap,DC=lan" "(objectClass=user)" cn sAMAccountName
```




Annexes :

Configuration du serveur LDAP :

LDAP/AD integration

Server Users Login Attributes Groups

1. Server: +



ldap://srv-win22-01.emfldap.lan


389

Detect Port

ldapreader@emfldap.lan

Save Credentials

OU=emfldap,DC=emfldap,DC=lan



Detect Base DN

Test Base DN

☐ Manually enter LDAP filters (recommended for large directories)

Configuration OK Continue Help

LDAP/AD integration

Server **Users** Login Attributes Groups

Listing and searching for users is constrained by these criteria:

Only these object classes: person

The most common object classes for users are organizationalPerson, person, user, and inetOrgPerson. If you are not sure which object class to select, please consult your directory admin.

Only from these groups: G_Direction, G_Finance, G_IT

>

<

[Edit LDAP Query](#)

LDAP Filter: (&((objectclass=person))(|(|(memberof=CN=G_Direction,OU=Groups,OU=emfldap,DC=emfldap,DC=lan)(primaryGroupID=1117))(|(memberof=CN=G_Finance,OU=Groups,OU=emfldap,DC=emfldap,DC=lan)(primaryGroupID=1118))(|(memberof=CN=G_IT,OU=Groups,OU=emfldap,DC=emfldap,DC=lan)(primaryGroupID=1116))))

Verify settings and count users

Configuration OK Back Continue Help

LDAP/AD integration

ServerUsersLogin AttributesGroups

When logging in, Nextcloud will find the user based on the following attributes:

LDAP/AD Username: ☒

LDAP/AD Email Address: ☐

Other Attributes:

[Edit LDAP Query](#)

LDAP Filter: (&(&((objectclass=person))((memberof=CN=G_Direction,OU=Groups,OU=emfldap,DC=emfldap,DC=lan)(primaryGroupID=1117))((memberof=CN=G_Finance,OU=Groups,OU=emfldap,DC=emfldap,DC=lan)(primaryGroupID=1118))((memberof=CN=G_IT,OU=Groups,OU=emfldap,DC=emfldap,DC=lan)(primaryGroupID=1116))))(samaccountname=%uid)(sAMAccountName=%uid)))

Test Loginname

Verify settings

Configuration OK BackContinueHelp

LDAP/AD integration

ServerUsersLogin AttributesGroups

Groups meeting these criteria are available in Nextcloud:

Only these object classes:

Only from these groups:

>

<

[Edit LDAP Query](#)

LDAP Filter: (&((objectclass=group))((cn=G_Direction)(cn=G_Finance)(cn=G_IT)))





Verify settings and count the groups

Configuration OK BackHelp

	Display name	Account name	Password	Email	Groups	Group admin for	Quota	Manager
All accounts	Brad Pitt	61528112-89C4-4462-8D...			G_IT		Unlimited (0 B used)	
Admins	Angeline Jolie	781D43F0-8959-4254-99...			G_Direction		Unlimited (0 B used)	
Recently active	admin	admin			admin		Unlimited (12 B used)	
Disabled accounts	Al Pacino	EA48F26A-8A67-4E5A-8...			G_Direction		Unlimited (0 B used)	
Groups								
Search groups...								
G_Direction								
G_Finance								
G_IT								

Configuration des shares :

Name ▾

			Size	Modified
<div><div></div><div>Share_Common</div></div>	Shared 	...	0 KB	a few seconds ...
<div><div></div><div>Share_Direction</div></div>	Shared 	...	0 KB	1 minute ago
<div><div></div><div>Share_Finance</div></div>	Shared 	...	0 KB	a few seconds ...
<div><div></div><div>Share_JT</div></div>	Shared 	...	< 1 KB	a few seconds ...
4 folders			< 1 KB	

Share with accounts and teams ▾

G_Direction (group)

Can edit

...

G_Finance (group)

Can edit

...


G_JT (group)

Can edit

...

Internal link

Only works for people with access to this folder



External shares ⓘ

Email, federated cloud id ▾

Create public link

+

Additional shares ⓘ

Name ▾

			Size	Modified
<div><div></div><div>Share_Common</div></div>	Shared 	...	0 KB	1 minute ago
<div><div></div><div>Share_Direction</div></div>	Shared 	...	0 KB	1 minute ago
<div><div></div><div>Share_Finance</div></div>	Shared 	...	0 KB	1 minute ago
<div><div></div><div>Share_JT</div></div>	Shared 	...	< 1 KB	1 minute ago
4 folders			< 1 KB	

Share with accounts and teams ▾

G_Direction (group)

Can edit

...

Internal link

Only works for people with access to this folder



External shares ⓘ

Email, federated cloud id ▾

Create public link

+

Additional shares ⓘ