StadiumCompany

Mission 2

Active Directory, DNS, DHCP, GPO

Domaine	Serveur principal	Système
stadiumcompany.com	SRV-AD01	Windows Server 2022

1. Installation et configuration

1.1 Active Directory Domain Services (AD DS)

Active Directory Domain Services (AD DS) est le rôle central de Windows Server qui permet de gérer de manière centralisée les utilisateurs, les ordinateurs, les groupes et les politiques d'un réseau d'entreprise.

Prérequis

- Adresse IP statique configurée sur le serveur
- Nom d'hôte défini (exemple : SRV-AD01)
- Windows Server 2022 installé et à jour

Installation du rôle AD DS via PowerShell

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools    # Installe le rôle AD DS avec les outils de gestion
```

Une fois le rôle installé, promouvoir le serveur en contrôleur de domaine :

```
Install-ADDSForest `
    -DomainName "stadiumcompany.com" `
    -DomainNetBIOSName "STADIUMCOMPANY" `
    -InstallDNS `
    -SafeModeAdministratorPassword (ConvertTo-SecureString "MotDePasseDS" -AsPlainText -Force) `
    -Force
```

> ⚠ *Le serveur redémarre automatiquement après la promotion. Après redémarrage, se connecter avec le compte STADIUMCOMPANY\Administrateur.*

> ✓ *La commande -InstallDNS installe et configure automatiquement le rôle DNS lors de la promotion.*

Vérification

```
Get-ADDomain    # Vérifie que le domaine est bien créé
Get-ADDomainController    # Vérifie que le serveur est bien contrôleur de domaine
```

1.2 DNS Primaire et Secondaire

Le DNS (Domain Name System) traduit les noms de domaine en adresses IP. Dans notre infrastructure, le contrôleur de domaine fait office de DNS primaire. Un second serveur assure la redondance.

Configuration du DNS primaire (SRV-AD01)

Le DNS primaire est automatiquement configuré lors de la promotion AD. Il faut néanmoins vérifier et compléter les enregistrements :

```
Add-DnsServerPrimaryZone -Name 'stadiumcompany.com' -ReplicationScope 'Forest'    # Crée la zone DNS principale (si non créée)
Add-DnsServerResourceRecordA -ZoneName 'stadiumcompany.com' -Name 'SRV-AD01' -IPv4Address '172.20.0.1'    # Ajoute un enregistrement A pour le serveur AD
```

```
Add-DnsServerResourceRecordPtr -ZoneName '0.20.172.in-addr.arpa' -Name '1' -
PtrDomainName 'SRV-AD01.stadiumcompany.com'    # Ajoute l'enregistrement DNS inverse
```

Configuration du DNS secondaire (SRV-AD02)

Le DNS secondaire réplique les données du DNS primaire pour assurer la haute disponibilité :

```
Install-WindowsFeature -Name DNS -IncludeManagementTools    # Installation du rôle
DNS sur SRV-AD02
Add-DnsServerSecondaryZone -Name 'stadiumcompany.com' -ZoneFile
'stadiumcompany.com.dns' -MasterServers 172.20.0.1    # Création de la zone
secondaire pointant vers le DNS primaire
```

> ✓ *Vérifier la réplication DNS avec : dnscmd /zonerefresh stadiumcompany.com*

Vérification DNS

```
nslookup SRV-AD01.stadiumcompany.com    # Résolution de nom → doit retourner
172.20.0.1
nslookup 172.20.0.1    # Résolution inverse → doit retourner SRV-
AD01.stadiumcompany.com
Resolve-DnsName stadiumcompany.com    # Test de résolution via PowerShell
```

1.3 DHCP

Le DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP aux équipements du réseau selon les étendues définies par VLAN/service.

Installation du rôle DHCP

```
Install-WindowsFeature -Name DHCP -IncludeManagementTools    # Installation du rôle
DHCP
Add-DhcpServerInDC -DnsName 'SRV-AD01.stadiumcompany.com' -IPAddress 172.20.0.1    #
Autorisation du serveur DHCP dans l'Active Directory
Set-ItemProperty -Path
registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ServerManager\Roles\12 -Name
ConfigurationState -Value 2    # Marquer la configuration DHCP comme terminée
```

Création des étendues DHCP par service

Chaque service dispose de sa propre étendue DHCP, cohérente avec le plan d'adressage VLSM de la Mission 1 :

Service	Étendue (plage)	Masque	Passerelle	Durée bail
Administration	172.20.0.10 – 172.20.0.200	/24	172.20.0.1	8 jours
Équipes	172.20.1.10 – 172.20.1.200	/24	172.20.1.1	8 jours
WiFi	172.20.2.10 – 172.20.2.120	/25	172.20.2.1	4 heures
Caméra IP	172.20.2.130 – 172.20.2.250	/25	172.20.2.129	30 jours

Service	Étendue (plage)	Masque	Passerelle	Durée bail
VIP-Presse	172.20.3.10 – 172.20.3.120	/25	172.20.3.1	4 heures
Fournisseurs	172.20.3.130 – 172.20.3.185	/26	172.20.3.129	4 heures
Restaurant	172.20.3.194 – 172.20.3.205	/28	172.20.3.193	4 heures

Exemple de création de l'étendue pour le service Administration :

```
Add-DhcpServerv4Scope -Name 'Administration' -StartRange 172.20.0.10 -EndRange
172.20.0.200 -SubnetMask 255.255.255.0 -LeaseDuration 8.00:00:00    # Création de
l'étendue
Set-DhcpServerv4OptionValue -ScopeId 172.20.0.0 -Router 172.20.0.1 -DnsServer
172.20.0.1    # Ajout de la passerelle et du DNS sur l'étendue
Set-DhcpServerv4OptionValue -ScopeId 172.20.0.0 -DnsDomain 'stadiumcompany.com'    #
Ajout du suffixe DNS
```

> *⚠ Répéter ces commandes pour chaque service en adaptant les valeurs. La durée de bail plus courte pour WiFi et accès temporaires est intentionnelle pour libérer les IP rapidement.*

2. Création de la structure Active Directory

2.1 Unités d'organisation (OU)

Les unités d'organisation (OU — Organizational Units) permettent de structurer l'annuaire AD par service, facilitant la délégation d'administration et l'application ciblée des GPO.

Structure des OU pour StadiumCompany :

- OU=StadiumCompany (racine)
  - OU=Administration
  - OU=Équipes
  - OU=WiFi
  - OU=VIP-Presse
  - OU=Fournisseurs
  - OU=Restaurant
  - OU=Serveurs
  - OU=Ordinateurs

Application — Création des OU via PowerShell

```
New-ADOrganizationalUnit -Name 'StadiumCompany' -Path 'DC=stadiumcompany,DC=com'
# OU racine
New-ADOrganizationalUnit -Name 'Administration' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADOrganizationalUnit -Name 'Equipes' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADOrganizationalUnit -Name 'WiFi' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADOrganizationalUnit -Name 'VIP-Presse' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADOrganizationalUnit -Name 'Fournisseurs' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADOrganizationalUnit -Name 'Restaurant' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADOrganizationalUnit -Name 'Serveurs' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADOrganizationalUnit -Name 'Ordinateurs' -Path
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
```

2.2 Groupes d'utilisateurs

Les groupes permettent de gérer les droits d'accès aux ressources de façon centralisée. On utilise des groupes de type Sécurité, portée Globale.

Groupe	Type	Description
GRP_Administration	Sécurité / Globale	Personnel du service administration
GRP_Equipes	Sécurité / Globale	Personnel des équipes terrain
GRP_WiFi	Sécurité / Globale	Accès WiFi visiteurs
GRP_VIP_Presse	Sécurité / Globale	Journalistes et VIP
GRP_Fournisseurs	Sécurité / Globale	Prestataires et fournisseurs

Groupe	Type	Description
GRP_Restaurant	Sécurité / Globale	Personnel restauration
GRP_IT	Sécurité / Globale	Administrateurs informatiques

```
New-ADGroup -Name 'GRP_Administration' -GroupScope Global -GroupCategory Security -
Path 'OU=Administration,OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
New-ADGroup -Name 'GRP_Equipes' -GroupScope Global -GroupCategory Security -Path
'OU=Equipes,OU=StadiumCompany,DC=stadiumcompany,DC=com'    # undefined
# Répéter pour chaque groupe...    #
```

2.3 Comptes utilisateurs

Les comptes utilisateurs sont créés selon la règle de nommage définie : première lettre du prénom + nom de famille (en minuscules). Exemple : Jean Dupont → jdupont

Règle de nommage

Champ	Format	Exemple
Login (SamAccountName)	1ère lettre prénom + nom	jdupont
UPN (UserPrincipalName)	login@stadiumcompany.com	jdupont@stadiumcompany.com
Mot de passe initial	Sc@XXXX (XXXX = 4 chiffres)	Sc@2024
Description	Service + poste	Administration - Responsable

Création d'un utilisateur — exemple

```
New-ADUser `
    -Name "Jean Dupont" `
    -GivenName "Jean" `
    -Surname "Dupont" `
    -SamAccountName "jdupont" `
    -UserPrincipalName "jdupont@stadiumcompany.com" `
    -Path "OU=Administration,OU=StadiumCompany,DC=stadiumcompany,DC=com" `
    -AccountPassword (ConvertTo-SecureString "Sc@2024" -AsPlainText -Force) `
    -ChangePasswordAtLogon $true `
    -Enabled $true
```

Ajout de l'utilisateur dans son groupe

```
Add-ADGroupMember -Identity 'GRP_Administration' -Members 'jdupont'    # Ajout de
jdupont dans le groupe Administration
```

> ⚠ *Le paramètre -ChangePasswordAtLogon $true force l'utilisateur à changer son mot de passe à sa première connexion, ce qui est une bonne pratique de sécurité.*

3. Dossiers personnels, partages réseau et profils

3.1 Structure des dossiers

Les dossiers sont créés sur le serveur de fichiers (ou le serveur AD). La structure proposée est la suivante :

- D:\Partages\
  - Utilisateurs\ (dossiers personnels)
  - Administration\
  - Equipes\
  - VIP-Presse\
  - Restaurant\
  - Commun\

```
New-Item -ItemType Directory -Path 'D:\Partages\Utilisateurs'    # undefined
New-Item -ItemType Directory -Path 'D:\Partages\Administration'    # undefined
New-Item -ItemType Directory -Path 'D:\Partages\Equipes'    # undefined
New-Item -ItemType Directory -Path 'D:\Partages\VIP-Presse'    # undefined
New-Item -ItemType Directory -Path 'D:\Partages\Restaurant'    # undefined
New-Item -ItemType Directory -Path 'D:\Partages\Commun'    # undefined
```

3.2 Partages réseau

Chaque dossier est partagé sur le réseau avec les permissions adaptées. On distingue les permissions de partage (SMB) et les permissions NTFS.

Dossier partagé	Nom du partage	Groupe autorisé	Droits NTFS
D:\Partages\Administration	Administration$	GRP_Administration	Modifier
D:\Partages\Equipes	Equipes$	GRP_Equipes	Modifier
D:\Partages\VIP-Presse	VIP-Presse$	GRP_VIP_Presse	Lecture
D:\Partages\Restaurant	Restaurant$	GRP_Restaurant	Modifier
D:\Partages\Commun	Commun$	Domain Users	Lecture
D:\Partages\Utilisateurs	Utilisateurs$	Domain Users	Personnel uniquement

Exemple — Création du partage Administration

```
New-SmbShare -Name 'Administration$' -Path 'D:\Partages\Administration' -FullAccess
'GRP_Administration'    # Création du partage SMB
$acl = Get-Acl 'D:\Partages\Administration'    # undefined
$rule = New-Object
System.Security.AccessControl.FileSystemAccessRule('STADIUMCOMPANY\GRP_Administratio
n','Modify','ContainerInherit,ObjectInherit','None','Allow')    # undefined
$acl.SetAccessRule($rule)    # undefined
Set-Acl -Path 'D:\Partages\Administration' -AclObject $acl    # Application des
droits NTFS
```

3.3 Dossiers personnels

Chaque utilisateur dispose d'un dossier personnel accessible uniquement par lui. Le dossier est défini dans les propriétés du compte AD et monté automatiquement à la connexion.

```
# Création du dossier personnel pour jdupont    # undefined
New-Item -ItemType Directory -Path 'D:\Partages\Utilisateurs\jdupont'    # undefined
# Définir le dossier personnel dans AD    # undefined
Set-ADUser -Identity 'jdupont' `
    -HomeDirectory '\\SRV-AD01\Utilisateurs$\jdupont' `
    -HomeDrive 'H:'
```

> ✓ *Le lecteur H: sera automatiquement monté à la connexion de l'utilisateur grâce au paramètre -HomeDrive.*

3.4 Profils utilisateurs itinérants (optionnel)

Les profils itinérants permettent à un utilisateur de retrouver son environnement (bureau, favoris, etc.) quel que soit le poste sur lequel il se connecte.

```
New-Item -ItemType Directory -Path 'D:\Partages\Profils'    # undefined
New-SmbShare -Name 'Profils$' -Path 'D:\Partages\Profils' -FullAccess 'Domain Users'
# undefined
Set-ADUser -Identity 'jdupont' -ProfilePath '\\SRV-AD01\Profils$\jdupont'    #
Assignation du profil itinérant
```

> ⚠ *Les profils itinérants peuvent alourdir les connexions si les profils sont volumineux. Utiliser la redirection de dossiers (GPO) pour externaliser Documents, Bureau, etc.*

4. Définition et application des GPO

Les GPO (Group Policy Objects) permettent d'appliquer des configurations et des restrictions de façon centralisée sur les utilisateurs et les ordinateurs du domaine.

4.1 Politique de mots de passe

La politique de mots de passe est définie au niveau du domaine via la GPO Default Domain Policy :

Paramètre	Valeur recommandée	Description
Longueur minimale	12 caractères	Limite les mots de passe trop courts
Complexité requise	Activée	Majuscule, minuscule, chiffre, caractère spécial
Durée de vie maximale	90 jours	Force le renouvellement régulier
Durée de vie minimale	1 jour	Empêche le changement immédiat
Historique	10 mots de passe	Interdit la réutilisation
Verrouillage après	5 tentatives	Blocage en cas d'attaque par force brute
Durée de verrouillage	30 minutes	Déverrouillage automatique après 30 min

```
Set-ADDefaultDomainPasswordPolicy -Identity 'stadiumcompany.com' `     # undefined
    -MinPasswordLength 12 `     # undefined
    -PasswordHistoryCount 10 `     # undefined
    -MaxPasswordAge 90.00:00:00 `     # undefined
    -MinPasswordAge 1.00:00:00 `     # undefined
    -LockoutThreshold 5 `     # undefined
    -LockoutDuration 00:30:00 `     # undefined
    -LockoutObservationWindow 00:30:00 `     # undefined
    -ComplexityEnabled $true     # Application de la politique
```

4.2 Restrictions machines

Ces GPO sont liées aux OU d'ordinateurs pour restreindre l'usage des postes :

Création et liaison d'une GPO

```
New-GPO -Name 'GPO_Restrictions_Machines' -Domain 'stadiumcompany.com'     # Création de la GPO
New-GPLink -Name 'GPO_Restrictions_Machines' -Target 'OU=Ordinateurs,OU=StadiumCompany,DC=stadiumcompany,DC=com'     # Liaison à l'OU Ordinateurs
```

Paramètres recommandés (via Gestion des stratégies de groupe)

Chemin : Configuration Ordinateur → Modèles d'administration

- **Désactiver l'accès au Panneau de configuration :** Empêche la modification des paramètres système

- **Désactiver le gestionnaire des tâches :** Limite les interruptions des processus système
- **Désactiver l'accès aux périphériques USB :** Prévient les fuites de données
- **Définir un économiseur d'écran avec mot de passe :** Verrouillage automatique après 10 minutes d'inactivité
- **Désactiver l'installation de logiciels :** Réservé aux administrateurs IT

4.3 Règles de sécurité

Chemin : Configuration Ordinateur → Paramètres Windows → Paramètres de sécurité

GPO_Securite_Reseau

- **Pare-feu Windows :** Activé sur tous les profils (domaine, privé, public)
- **Audit des connexions :** Succès et échecs journalisés dans l'Observateur d'événements
- **Désactiver les partages administratifs :** Sauf pour les machines serveurs
- **Renommer le compte Administrateur local :** Remplacer par un nom non standard (ex : SC_Admin)

```
New-GPO -Name 'GPO_Securite_Reseau' -Domain 'stadiumcompany.com'    # undefined
New-GPLink -Name 'GPO_Securite_Reseau' -Target
'OU=StadiumCompany,DC=stadiumcompany,DC=com'    # Liaison à l'OU racine (s'applique
à tout le domaine)
```

4.4 Redirection de dossiers

La redirection de dossiers permet de stocker les Documents, Bureau et Téléchargements de l'utilisateur sur le serveur plutôt que localement.

Chemin : Configuration utilisateur → Paramètres Windows → Redirection de dossiers

- **Documents :** \\SRV-AD01\Utilisateurs$\%username%\Documents
- **Bureau :** \\SRV-AD01\Utilisateurs$\%username%\Bureau

> *✓La redirection de dossiers combinée aux profils itinérants garantit que l'utilisateur retrouve son environnement complet sur n'importe quel poste du domaine.*

5. Tests et validation

5.1 Test de l'authentification

Depuis un poste client joint au domaine :

```
nltest /dsgetdc:stadiumcompany.com    # Vérifie que le contrôleur de domaine est joignable
whoami /fqdn    # Affiche le nom complet de l'utilisateur connecté
klist    # Affiche les tickets Kerberos actifs (preuve d'authentification AD)
```

Via PowerShell (depuis SRV-AD01) :

```
Test-ComputerSecureChannel -Verbose    # Teste la liaison sécurisée entre le poste et le domaine
Get-ADUser jdupont -Properties *    # Vérifie les propriétés du compte utilisateur
```

5.2 Test d'attribution IP (DHCP)

Depuis un poste client :

```
ipconfig /release    # Libère l'adresse IP actuelle
ipconfig /renew    # Demande une nouvelle adresse IP au serveur DHCP
ipconfig /all    # Affiche la configuration IP complète (vérifier passerelle, DNS, bail)
```

Depuis le serveur DHCP :

```
Get-DhcpServerv4Lease -ScopeId 172.20.0.0    # Affiche les baux DHCP actifs pour le service Administration
Get-DhcpServerv4Statistics    # Statistiques globales du serveur DHCP
```

5.3 Test de résolution DNS

```
nslookup SRV-AD01.stadiumcompany.com    # Résolution directe → doit retourner 172.20.0.1
nslookup 172.20.0.1    # Résolution inverse → doit retourner SRV-AD01.stadiumcompany.com
nslookup stadiumcompany.com    # Vérifie la résolution du domaine
dcdiag /test:dns /v    # Diagnostic complet DNS lié à Active Directory
```

5.4 Test d'accès aux ressources partagées

Depuis un poste client authentifié :

```
net use * \\SRV-AD01\Administration$    # Monte le partage Administration en lecteur réseau
Test-Path '\\SRV-AD01\Administration$'    # Vérifie l'accessibilité du partage
Get-SmbConnection    # Liste les connexions SMB actives depuis le serveur
```

5.5 Test des GPO

```
gpupdate /force    # Force la mise à jour des GPO sur le poste client
gpresult /h C:\gpresult.html    # Génère un rapport HTML des GPO appliquées
rsop.msc    # Ouvre la console 'Jeu de stratégies résultant' (interface graphique)
```

> ✓*Le rapport gpresult /h est très utile pour vérifier quelles GPO sont bien appliquées sur un utilisateur ou un ordinateur précis.*

5.6 Récapitulatif des tests

Test	Commande / Méthode	Résultat attendu
Authentification AD	nltest / whoami	Connexion avec compte du domaine
Attribution IP DHCP	ipconfig /renew	IP dans la bonne plage selon VLAN
Résolution DNS directe	nslookup SRV-AD01	Retourne 172.20.0.1
Résolution DNS inverse	nslookup 172.20.0.1	Retourne SRV-AD01.stadiumcompany.com
Accès partage réseau	net use / Test-Path	Partage accessible selon groupe
Dossier personnel H:	Connexion utilisateur	Lecteur H: monté automatiquement
GPO appliquées	gpresult /h	GPO listées dans le rapport