

UAA6 - Active Directory / DNS / DHCP

Pas de PowerShell ni CMD - 100% GUI

1. PRE-REQUIS VM (Page 1, sections 1-3)

1. Mots de passe partout : Tech2026. Ne expire jamais, ne peut pas etre modifie par l'utilisateur.
2. Creer 2 VM : Windows Server 2025 + Windows 11 UK a partir des ISOs. Commencer par le serveur.
3. RAM : 8 Go | vCPU : 4 | Reseau : meme segment LAN que Pfsense.
4. Installer VMware Tools sur chaque VM apres l'installation.
5. Snapshot apres mise a jour.
6. Configuration IP (sur chaque machine, via GUI reseau) :

Machine	IP	Gateway	DNS	Nom
Serveur (albert)	10.0.x.10/24	10.0.x.254	8.8.8.8	albert
Workstation (paola)	10.0.x.11/24	10.0.x.254	8.8.8.8	paola

Verifier le fuseau horaire et l'heure sur le serveur.

2. ACTIVE DIRECTORY (Page 1, section 4)

1. Sur le serveur albert, ouvrir Server Manager.
2. Clique droit "Ajouter des rôles et fonctionnalités".
3. Cochez "Active Directory Domain Services" (AD DS). Accepter l'installation du DNS automatique.
4. Valider et attendre la fin de l'installation.
5. Quand installe : cliquer sur le triangle d'alerte -> "Promouvoir ce serveur en controleur de domaine".
6. Selectionner "Cree une nouvelle forêt".
7. Nom de forêt : abc.local | Nom de domaine : abc.local.
8. Domain function level : Windows Server 2025 | Forest function level : Windows Server 2025.

9.
Mot de passe DS : Tech2026 (ne expire pas, non modifiable).

10.
Cocher "DNS server". Valider, laisser redemarrer.

Après redémarrage, sur la workstation (paola) : Panneau de config -> Système -> Nom de l'ordinateur -> Appartenance au domaine -> Saisir abc.local.

Identifier : abc.local\administrator / Tech2026. Redemarrer la PC.

Se connecter avec abc.local\administrator / Tech2026.

3. UNITES ORGANISATIONNELLES (Page 1, section 5)

1.
Ouvrir Utilisateurs et ordinateurs Active Directory (dsa.msc).
2.
Clic droit sur la racine abc.local -> Nouveau -> Unité organisationnelle -> "Système solaire".
3.
Clic droit sur "Système solaire" -> Nouveau -> "Terre".
4.
Idem -> "Mars".
5.
Idem -> "Lune".
6.
Chercher l'ordinateur paola (dans la racine) -> faire glisser dans "Système solaire".

4. UTILISATEURS (Page 2, section 6)

Via ADUC, clic droit sur la racine -> Nouvel utilisateur :

User logon name	Nom complet	Description
Doctor	Doctor Who	President de la Terre
Yoda	Maitre Yoda	President de Mars
Stallone	Silvester Stallone	President de la Lune
Martien1	Martien 1	Premier martien
Terrien1	Terrien 1	Premier terrien

Mot de passe : Tech2026 pour tous. Options par default.

5. GROUPES (Page 2, section 7)

1.
Via ADUC, dans l'OU Users (créer l'OU Users si nécessaire) :
2.
Nouveau groupe -> Présidents (Type : Securite, Portee : Domain).
3.
Nouveau groupe -> Habitants (Type : Securite, Portee : Domain).
- 4.

Membres du groupe Présidents : Yoda, Doctor, Stallone (ajouter membre par membre).

5.

Membres du groupe Habitants : Martien1, Terrien1.

6. CONFIGURATION DNS (Page 2, section 8)

Via Gestionnaire DNS (dnsmgmt.msc) :

1.

Zone inverse : Développer Serveurs DNS -> clic droit sur le serveur -> Nouvelle zone -> Zone inverse -> Suivant.

2.

Reseau : 10.0.4.0 -> Suivant -> Dynamique : Non -> Suivant -> Terminer.

Enregistrement alias (CNAME) dc1 -> albert :

1.

Développer Zones directes -> abc.local -> clic droit -> Nouvel alias (CNAME).

2.

Nom : dc1 | Serveur cible FQDN : albert.abc.local.

Enregistrement A pour mail (si pas existant) :

1.

Clic droit -> Nouvel host (A) -> Nom : mail, IP : 10.0.4.8.

Enregistrement mail (MX) :

1.

Clic droit sur abc.local -> Nouvel autre type d'enregistrement -> MX.

2.

Nom : (vide) | Serveur de messagerie : mail.abc.local | Priorite : 10.

7. INSTALLATION ET CONFIGURATION DHCP (Page 2, section 9)

1.

Via Gestionnaire DHCP (dhcpmgmt.msc), clic droit sur IPv4 -> Nouvelle étendue.

2.

Nom : Scope1. Plage : 10.0.4.101 -> 10.0.4.254 (recouvre tout le réseau 10.0.4.0/24).

3.

Duree bail : 8 jours (par default). Ignorer les plages exclues : 10.0.4.1 a 10.0.4.100.

4.

Activer DHCP. OK.

5.

Options de l'étendue :

Option	Valeur
003 Routeur	10.0.4.254
006 DNS Serveurs	10.0.4.10 (le serveur albert)
015 Nom de domaine DNS	abc.local

6.

Sur la workstation : changer IP en DHCP (obtenir automatiquement).

7.
Clic droit sur l'étendue -> Nouvelles réservations.
8.
Nom : paola | IP : 10.0.4.101 | MAC : (adresse MAC de paola) | Type : DHCP.
9.
VERIFIER : ipconfig /all sur paola -> doit avoir 10.0.4.101, DNS 10.0.4.10, GW 10.0.4.254. Ping albert, ping internet.

8. STRATEGIE DE SECURITE - Default Domain Policy (Page 2, section 10)

Via Gestionnaire des stratégies de groupe (gpmc.msc) :

1.
Ouvrir Gestionnaire des stratégies de groupe.
2.
Domaines -> abc.local -> Default Domain Policy -> Modifier.
3.
Politiques de mot de passe -> "Mots de passe doivent être changés tous les" : 60 jours.
4.
Politiques de verrouillage de compte -> "Seuil de verrouillage du compte" : 5 tentatives incorrectes.
5.
Politiques de verrouillage de compte -> "Secondes de durée de verrouillage du compte" : 10 minutes.

9. GESTION DES PARTAGES (Page 3, section 11)

Dossier C:\data :

1.
Créer le dossier C:\data.
2.
NTFS (Propriétés -> Sécurité) : Désactiver l'héritage -> Conserver les droits existants.
3.
Supprimer le groupe Users (tous droits).
4.
Ajouter Présidents -> Lecture & exécution + Modification.
5.
Ajouter Habitants -> Lecture.
6.
Terrien1 -> Entrée explicite : Refus total (Deni).
7.
Martien1 -> Entrée explicite : Autorisation Ecriture.

Partage (Propriétés -> Partage) :

1.
Partager -> Avance -> Partage.
2.
Supprimer Tout le monde.
- 3.

Ajouter Administrateurs -> Controle total.

4.

Ajouter Habitants -> Lecture.

5.

Ajouter Présidents -> Modification.

Partage habitants (home folders) :

1.

Creer le dossier C:\habitants.

2.

Partager avec : Administrateurs = Controle total, Habitants = Lecture/Ecriture (NTFS + partage).

3.

Pour chaque utilisateur du groupe Habitants (Martien1, Terrien1) :

4.

Dans ADUC, Proprietes de l'utilisateur -> Profil -> Dossier principal -> Chemin : \\albert\habitants\%USERNAME%.

5.

Cela mappe automatiquement sur Q: a la connexion.

10. STRATEGIE DE GROUPE (Page 3, section 12)

Via GPO :

1.

Interdiction panneau de configuration affichage (pour Habitants) :

2.

Nouvelle GPO liée à l'OU (ouverts la ou se trouvent les utilisateurs concernés).

3.

Modifier -> Configuration ordinateur -> Stratégies -> Parametres Windows -> Gestion de la securite -> Stratégies de controle d'accès aux ressources -> Interdiction d'accès au Panneau de configuration -> Elements spécifiques.

4.

Activer -> Lister les elements : Microsoft.Windows.ControlPanel -> Deni pour les membres du groupe Habitants.

5.

Interdiction ecriture média amovible (pour Terriens) :

6.

Nouvelle GPO -> Modifier -> Configuration ordinateur -> Stratégies -> Parametres Windows -> Configurations de la plateforme -> Suppression d'accès au stockage amovible.

7.

Activer -> Supprimer l'accès a la lecture/ecriture sur tous les médias amovibles -> Deni pour le groupe Terriens.

11. SCRIPT NETLOGON (Page 3, section 13)

Script mapping_script.bat :

1.

Ouvrir le dossier netlogon (partage : \\albert\netlogon).

2.

Creer le fichier mapping_script.bat avec ce contenu :

```
@echo off  
net use Z: \\albert\data /persistent:yes
```

3.
Assigner aux President : ouvrir la GPO pour les President.
4.
Configuration utilisateur -> Stratégies -> Windows -> Scripts de démarrage -> Ajouter -> Saisir mapping_script.bat.