Mission 1 : Infrastructure système et réseau

1) Contexte de la mission

Dans le cadre du projet HVO, l'entreprise souhaite déployer une première **infrastructure interne** permettant :

- d'héberger des services pour ses clients,
- de gérer un réseau administratif interne,
- d'assurer la sécurité et la segmentation des flux entre les différentes zones,
- d'intégrer un service applicatif (Nextcloud) destiné au stockage/partage.

Vous êtes missionnés en tant qu'équipe technique pour **concevoir, installer, configurer et documenter** l'infrastructure système et réseau.

2) Objectif principal

Réaliser une infrastructure complète composée de **trois réseaux distincts** reliés et sécurisés par un **routeur/pare-feu pfSense** :

1. **Réseau Serveurs (Zone Serveur)**
2. **Réseau Administratif (Zone Admin)**
3. **Réseau Clients (Zone Clients)**

La zone serveurs comprendra :

- **1 serveur Windows** avec les rôles : **AD DS / DNS / DHCP**
- **1 serveur Linux** hébergeant l'application **Nextcloud**

La zone administrative comprendra :

- **2 postes clients Windows** (machines "Admin1" et "Admin2") intégrés au domaine.

La zone cliente comprendra :

- **2 postes linux par client** (machines "srv-web" et "srv-bdd").

3) Périmètre et contraintes

3.1 Segmentation et sécurité

- Les trois réseaux doivent être **séparés** (réseaux distincts).
- Les communications inter-zones doivent être **contrôlées par pfSense** (règles firewall). On autorise uniquement les flux nécessaires.
- Les flux doivent respecter le principe du **moindre privilège** :
    - Admin → Serveurs : autorisé selon besoins (administration, DNS, etc.)
    - Clients → Serveurs : autorisé selon besoins (DNS…)
    - Clients → Admin : **interdit** (par défaut)
    - Serveurs → Clients : **interdit** (par défaut)

3.2 Services attendus

- Les postes Admin doivent :
    - obtenir automatiquement une adresse IP (DHCP),
    - utiliser le DNS du domaine,
    - rejoindre le domaine Active Directory,
    - accéder à Nextcloud via le réseau (HTTP/HTTPS selon votre choix).
- Le serveur Linux doit :
    - être joignable depuis le réseau Admin (administration SSH),
    - publier Nextcloud pour les utilisateurs (accès web).

4) Contraintes techniques

L'infrastructure est composée de **4 réseaux distincts** :

Zone	Rôle	Réseau
WAN	Accès Internet (simulé ou réel)	DHCP (réseau SIO)
Zone Serveurs	Services internes	10.10.10.0/24
Zone Administrative	Postes internes	10.10.20.0/24
Zone Clients	Réseau clients	10.10.30.0/24

Zone Serveurs — 10.10.10.0/24

Machine	Rôle	Adresse IP
SRV-gestion	Windows Server (AD / DNS / DHCP)	10.10.10.10
SRV-CLOUD	Linux + Nextcloud	10.10.10.20

Passerelle : `10.10.10.254` (pfSense)

DNS principal : `10.10.10.10`

Zone Administrative — 10.10.20.0/24

Machine	Rôle	IP
ADMIN1	Poste Windows	DHCP (ex : 10.10.20.100)
ADMIN2	Poste Windows	DHCP (ex : 10.10.20.101)

DHCP fourni par : SRV-gestion

Passerelle : 10.10.20.254 (pfSense)

DNS : 10.10.10.10

Domaine : hvo.local

Zone clients— 10.10.30.0/24

Machine	Rôle	IP
cli1-srv-web	srv web	10.10.30.1
cli1-srv-bdd	srv mysql	10.10.30.2

Passerelle : 10.10.30.254 (pfSense)

DNS : 10.10.10.10

Active directory

1) Structure des OU recommandée

```
DC=hvo,DC=local
│
└── OU=Admin
        ├── OU=Utilisateurs
        │   ├── OU=Service-Commercial
        │   └── OU=Service-Technique
        │
        ├── OU=Postes
        │   ├── OU=Service-Commercial
        │   └── OU=Service-Technique
        │
        └── OU=Groupes
```

2) Groupes de sécurité à créer

Groupes globaux

- `GG_COM_Users`
- `GG_TECH_Users`

Ces groupes serviront :

- à l'assignation des **GPO**
- aux **droits applicatifs** (Nextcloud plus tard)
- aux **permissions NTFS** (missions suivantes)

3) Liste des utilisateurs à créer

🟦 Service Commercial

Nom	Prénom	Login	Groupe
Martin	Claire	cmartin	GG_COM_Users
Dupont	Julien	jdupont	GG_COM_Users

Leroy	Sophie	sleroy	GG_COM_Users

Rôle métier :

- Utilisation bureautique
- Accès aux partages commerciaux
- Accès à Nextcloud (fichiers clients, devis)

🟩 Service Technique

Nom	Prénom	Login	Groupe
Bernard	Lucas	lbernard	GG_TECH_Users
Moreau	Thomas	tmoreau	GG_TECH_Users
Petit	Élodie	epetit	GG_TECH_Users

Rôle métier :

- Utilisation bureautique
- Accès aux outils techniques
- Accès étendu à Nextcloud
- Accès SSH / administration indirecte

4) GPO à appliquer par service

🔵 GPO – Service Commercial

Nom de la GPO : `GPO_COM_Utilisateurs`

Paramètres principaux

✅ Sécurité

- Interdire l'accès au panneau de configuration
- Désactiver l'invite de commandes (cmd)
- Interdire PowerShell
- Empêcher l'installation de logiciels

✅ **Session**

- Forcer la complexité du mot de passe (héritée du domaine)
- Verrouillage automatique après 10 minutes d'inactivité

✅ **Environnement utilisateur**

- Fond d'écran imposé (charte commerciale HVO) - choisissez une image professionnelle
- Redirection du dossier documents sur le serveur (profil itinérant)
- Mapping automatique lecteur réseau (ex : `S:` → Partage Commercial) - Dossier stocké sur le serveur srv-gestion

🟢 GPO – Service Technique

Nom de la GPO : `GPO_TECH_Utilisateurs`

Paramètres principaux

✅ **Sécurité**

- Accès limité au panneau de configuration (lecture seule)
- Invite de commandes **autorisée**
- PowerShell **autorisé**

✅ **Session**

- Verrouillage après 15 minutes

✅ **Environnement**

- Mapping lecteurs techniques (ex : `T:` → Partage Technique)
- Accès au bureau distant
- Observateur d'événements autorisé

🔒 GPO – Sécurité Générale

Nom : `GPO_Admin_Security_Base`

- Mot de passe :
  - 10 caractères minimum
  - Complexité activée
  - Expiration 90 jours
- Désactiver le stockage des mots de passe en clair
- Verrouillage de compte après 5 tentatives échouées

🖥️ GPO – Postes Administratifs

Nom : `GPO_Admin_Postes`

- Désactiver l'accès aux paramètres réseau
- Interdire le partage de fichiers local
- Activer le pare-feu Windows

ATTENTION :

- Pour votre DNS, vous devez utiliser comme redirecteur, le serveur DNS du lan_sio.
- Vous utilisez le serveur esxi des sio
- Vous devez créer des etiquettes réseau pour chacune de vos zones, respecter la nomenclature suivante initialesdugroupe-ap4-zone (ex : hlg-ap4-clients). Chaque étiquette réseau doit avoir un ID unique (principe du VLAN).
- Vous gardez les groupes de l'AP3.
- Vous créez une documentation technique accessible pour l'ensemble de l'équipe (schéma réseau, ip, login, mdp ….).
- Vous utilisez un outil de gestion de tâche (ex: Trello).