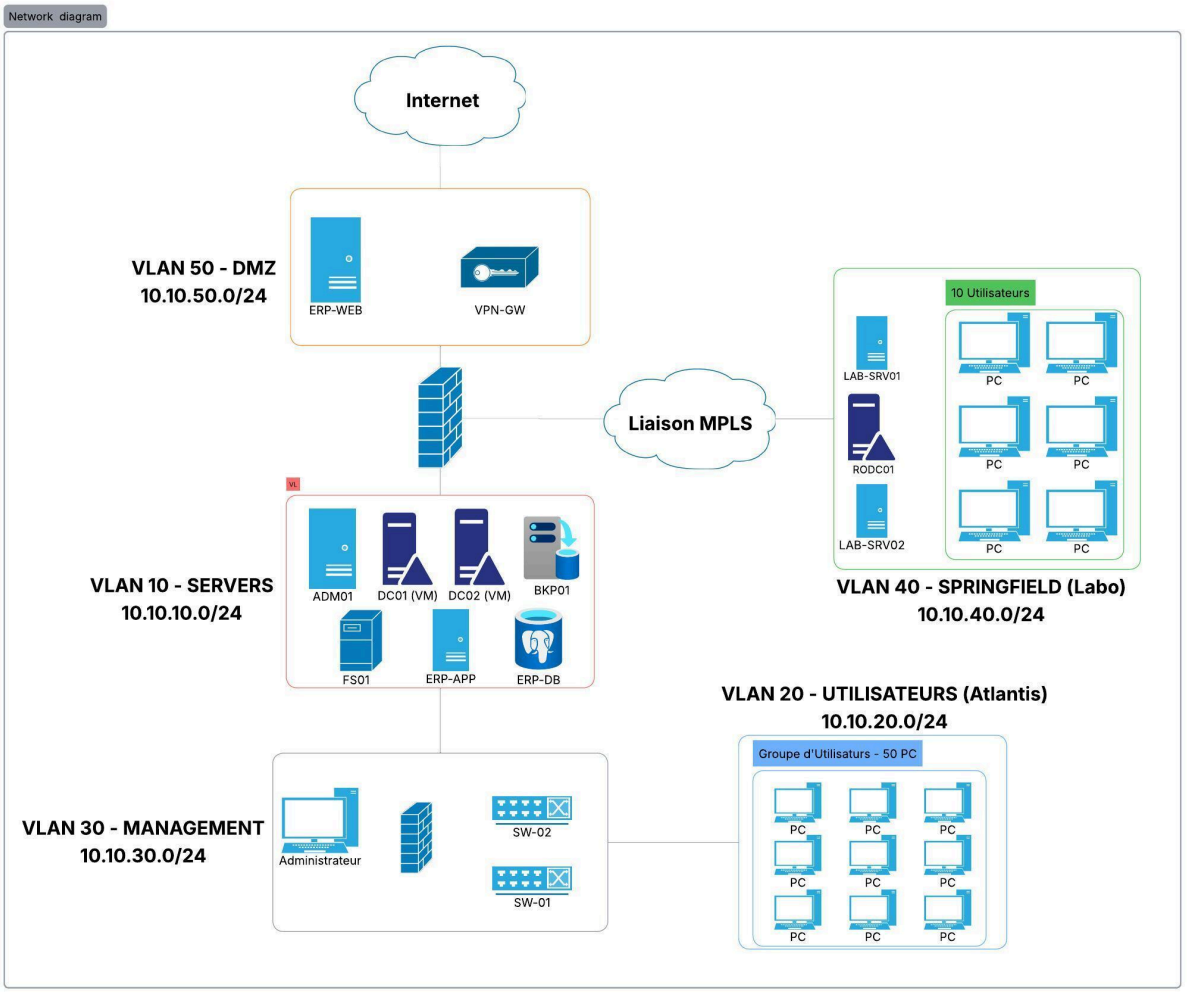
Schéma SI :
https://lucid.app/lucidchart/02b88f05-1609-4f79-b5d4-5dd324ba76e6/edit?viewport_loc=-2862%2C611%2C4912%2C2472%2C0_0&invitationId=inv_b8fabba7-759f-462d-b54b-8e783d21b0d7



Plan d'Adressage

VLAN	Plage d'Adresses IP	Description
VLAN 10 - Serveurs	10.10.10.0/24	Hébergement des serveurs critiques (DCs, ERP, Fichiers, Sauvegarde, Monitoring).

VLAN 20 - Utilisateurs (Atlantis)	10.10.20.0/24	Postes clients des 50 utilisateurs d'Atlantis.
VLAN 30 - Management	10.10.30.0/24	Accès sécurisé pour l'administration des équipements réseau (Switchs, Firewall).
VLAN 40 - Springfield (Labo)	10.10.40.0/24	Postes clients et serveurs Linux des 10 utilisateurs du Labo, connecté via MPLS.
VLAN 50 - Périmètre/DMZ	10.10.50.0/24	Firewall, points d'entrée/sortie (VPN), serveurs exposés (Reverse Proxy ERP).

Liste des Serveurs Atlantis

Nom du Serveur (VM)	**Rôle Primaire**	**Services Clés**
DC01/DC02 (2 VMs)	Contrôleurs de Domaine	Active Directory, DNS, DHCP, NPS (RADIUS).
FS01	Serveur de Fichiers	Partages Bureautiques (Services), Dossiers Personnels, Quotas, ACLs.
ERP-WEB	Serveur de Présentation ERP	Interface Web (HTTPS), Reverse Proxy/WAF.
ERP-APP	Serveur d'Applications ERP	Moteur métier, Workflow.

ERP-DB	Serveur de Base de Données	PostgreSQL (Données Clients, Contrats, Comptabilité).
BKP01	Serveur de Sauvegarde	Veeam (Gestion des tâches, Restauration Instantanée).
ADM01	Serveur d'Administration	WSUS (Mises à jour), SIEM/Syslog (Traçabilité), Console EDR.
VPN-GW	Passerelle VPN	Termination des connexions itinérantes/télétravail (avec MFA).

serveurs Site Springfield

Nom du Serveur (Physique)	**Rôle Primaire**	**Services Clés**
RODC01	Contrôleur de Domaine en Lecture Seule	Authentification locale, DNS (RO).
LAB-SRV01/02	Serveurs Labo (Linux)	Pilotage d'équipements, Acquisition de données.

Administration Déléguée (Correspondants IT)

L'objectif est de décharger l'équipe informatique centrale tout en maintenant un haut niveau de sécurité.

1. **Création des Groupes :** Un groupe de sécurité par service est créé pour les correspondants informatiques (ex: `SG-ATL-RH-Admin`).
2. **Délégation de Contrôle :** Sur l'**OU Utilisateurs** et l'**OU Postes** de chaque service :
    - L'assistant de Délégation de Contrôle est utilisé pour accorder au groupe délégué les droits suivants :

- Créer, supprimer et gérer les comptes **Utilisateurs** (dans leur OU uniquement).
- Réinitialiser les mots de passe des utilisateurs.
- Gérer les propriétés des utilisateurs (Numéro de téléphone, service, etc.).
- Joindre les postes de travail au domaine (Gestion de l'**OU Postes**).
- **Justification :** Cette méthode empêche les correspondants d'avoir des droits sur l'infrastructure critique (DCs, Serveurs) et de compromettre d'autres services, respectant le principe du **moindre privilège**.

Types de Comptes et Rôles

Type de Compte	**Rôle et Utilisation**
Comptes Utilisateurs (Nommés)	Accès bureautique, emails, ERP, VPN. Utilisés par les 60 collaborateurs. **Interdiction formelle des comptes génériques.**
Comptes Administrateurs Séparés	Comptes dédiés utilisés uniquement pour les tâches d'administration (ex: Admin-Jdupont). Ces comptes ne doivent **pas** être utilisés pour la bureautique et n'ont pas accès à Internet.
Comptes de Service	Comptes utilisés par les applications (ex: Sauvegarde, monitoring, ERP vers la DB). Le mot de passe doit être long et complexe, stocké de manière sécurisée (PAM si possible).

Stratégies de Groupe (GPO)
Stratégies pour la Sécurité du SI (Confidentialité et Intégrité)

Nom de la GPO	**Contenu / Paramètre Clé**	**Liaison (OU)**	**Justification Sécurité**
GPO-SEC-MotsDePasse-Stricte	Longueur min. 12 car., historique 24, complexité activée.	Domaine (tous les Utilisateurs)	Défense contre le "brute force", renforce la **Confidentialité**.
GPO-SEC-Restriction-AdminLocal	Suppression des utilisateurs du groupe "Administrateurs" local.	OU Postes	Empêche les utilisateurs de compromettre leur poste et d'installer des malwares (**Intégrité**).
GPO-SEC-Firewall-Client	Activation du Firewall Windows, blocage des connexions entrantes non sollicitées.	OU Postes	Protection périmétrique des postes, réduit la surface d'attaque.
GPO-SEC-Accès-USB-LectureSeule	Restriction d'écriture sur les périphériques de stockage USB.	OU Postes	Empêche l'exfiltration de données non autorisée (**Confidentialité**) et la propagation de malwares.
GPO-SEC-Verrouillage-Session	Verrouillage automatique de la session après 15 minutes d'inactivité.	OU Utilisateurs	Protège l'accès physique aux données sur les postes.

Stratégies pour l'Administration du SI

Nom de la GPO	**Contenu / Paramètre Clé**	**Liaison (OU)**	**Justification Administration**

GPO-ADM-Redirection-Dossiers	Redirection de "Mes Documents" vers le dossier personnel sur FS01.	OU Utilisateurs	Centralisation des données (facilite la sauvegarde et la récupération).
GPO-ADM-Installation-EDR	Déploiement du logiciel EDR centralisé sur tous les postes.	OU Postes	Assure la couverture Antivirus/EDR sur 100% du parc.
GPO-ADM-Configuration-Navigateur	Définition de la page d'accueil, installation des extensions de sécurité.	OU Utilisateurs	Homogénéisation de l'environnement de travail.
GPO-ADM-Service-WSUS	Configuration du poste client pour pointer vers le serveur **WSUS** pour les mises à jour.	OU Postes et Serveurs	Contrôle et validation centralisés des patchs (**Intégrité**).
GPO-ADM-Configuration-Imprimantes	Déploiement des imprimantes et copieurs réseau par service.	OU Utilisateurs/Postes	Simplification de l'ajout de périphériques pour les utilisateurs.

Garantie des Piliers de Sécurité (DICaT)

Les choix architecturaux et les stratégies ci-dessus contribuent à garantir les quatre piliers de la sécurité.

Confidentialité

- **Chiffrement des Communications :** Mise en œuvre de **HTTPS** pour l'accès à l'ERP et de **VPN chiffré (IPsec/SSL)** pour les accès distants.
- **Contrôle d'Accès Fin :** Utilisation des **Groupes de Sécurité AD** et des **ACLs NTFS** sur `FS01` pour garantir que seuls les membres autorisés accèdent aux dossiers de service.

- **MFA (Multi-Factor Authentication) :** Obligatoire pour tous les accès VPN et administrations critiques.

Intégrité

- **Gestion des Correctifs :** Utilisation de **WSUS** pour valider et déployer les mises à jour de manière contrôlée, assurant que les systèmes sont patchés contre les vulnérabilités connues.
- **Retrait des Droits Locaux :** GPO empêchant les utilisateurs d'être administrateurs de leur poste, limitant l'altération du système et l'installation de logiciels non validés.
- **Isolation des Tiers ERP :** Séparation de la Base de Données (`ERP-DB`) du serveur Web (`ERP-WEB`) pour qu'une compromission du frontal n'atteigne pas les données critiques.

Disponibilité (RTO/PRA)

- **Haute Disponibilité (HA) :** Infrastructure virtualisée en cluster (2 hôtes physiques) pour la bascule automatique des VMs critiques (DCs, ERP) en cas de défaillance d'un hôte.
- **Redondance des Rôles :** Deux **DCs** (DC01/DC02) pour l'authentification et les services DNS/DHCP.
- **PRA (Plan de Reprise) :** Le plan de sauvegarde utilise le **RTO 4h** via la **Restauration Instantanée** pour les services critiques (ERP, Partages Juridique/Direction).
- **Redondance de Liaison :** La liaison **MPLS** est sous **SLA ≥ 99,9%**, assurant la connectivité du site distant.

Traçabilité

- **Comptes Nominatifs :** Suppression des comptes génériques (ex: RH:RH), imposant l'usage d'un compte unique par employé (**G1**), permettant de lier chaque action à un utilisateur.
- **SIEM/Syslog :** Mise en place d'un serveur **ADM01** pour collecter et centraliser les logs (événements de sécurité AD, logs du Firewall, événements du EDR).
- **Audit AD :** Configuration des GPO pour activer l'audit des tentatives de connexion, des accès aux fichiers critiques et des modifications de privilèges, permettant de savoir *qui a fait quoi et quand*.

Structure de l'Annuaire (OU et Groupes)

L'organisation est basée sur la structure de l'entreprise et les besoins d'administration déléguée.

- **OU Racine :** `XANADU`
    - **OU Sites :** Regroupe les OU liées à la localisation physique.
        - `OU Atlantis`

        - `OU Utilisateurs (Par Service)` : `Compta`, `Commercial`, `Juridique`, `Direction`, `RH`, `BureauEtude`.
        - `OU Postes`
        - `OU Serveurs`
    - `OU Springfield`
        - `OU Utilisateurs (Labo)`
        - `OU Postes`
        - `OU Serveurs`
- **OU Administration :** Contient les comptes et groupes ayant des privilèges d'administration.
    - `OU Comptes Admin` : Comptes séparés pour les administrateurs.
    - `OU Groupes Délégués` : Groupes pour les correspondants IT.