

Administration du SI & sécurité IT Livrable 1

CESI 
ÉCOLE D'INGÉNIEURS



Projet Administration et sécurisation d'un système d'information

Réalisé par

Alexandre RIVET

Allan BOUHAMED

Antonin RABATEL

Mathéo CARVAL

Philippe LUU

Projet encadré par

Djamel AOUAM

Année universitaire 2025-2026

Livrable 1 - 27/11/2025

Sommaire

Sommaire.....	3
1. Contexte.....	5
2. Objet du document.....	7
2.1. Cartographie logique et technique.....	7
2.2. Politique et plan de sauvegarde.....	8
2.3. Livrable destiné à la présentation et à la mise en production.....	8
3. Documentation d'infrastructure réseau.....	9
3.1 Site A : "ATLANTIS" (Siège).....	9
3.2 Site B : "SPRINGFIELD" (Site Distant).....	11
3.3 LAN.....	12
3.3.1 Segmentation par VLANs (Virtual LAN*s).....	12
3.3.2 Redondance et Haute Disponibilité.....	12
3.3.3 Architecture DMZ "Sandwich" (Double Barrière).....	13
3.3.4 Management.....	14
3.3.5 Tableau de synthèse Infrastructure & topologie des services.....	14
3.4 Rôles FSMO.....	19
3.5 Stratégies de groupe (GPO).....	19
3.6 Services de connexion à distance (itinérance, site-distant).....	22
3.6.1. Interconnexion des sites : choix d'un VPN MPLS* (site-à-site*).....	22
3.6.2 Accès des utilisateurs itinérants : choix d'OpenVPN (point-à-client).....	23
3.7 WAN (Routeurs).....	24
3.8 Sécurisation et amélioration continue du système d'information.....	26
3.8.1 Antivirus, EDR, XDR.....	26
3.8.2 Mise à jour.....	27
3.9 Inventaire.....	27
4. Vue administrative et gestion des identités.....	28
4.1 Service d'annuaire.....	28
4.2 Politique de nommage (Naming Convention).....	29
4.3 Forêt Active Directory et Arborescence LDAP (schéma complet).....	29
4.4 Partage de dossiers.....	31
4.5 Gestion des droits et groupes Shadow* (AGDLP* simplifié).....	32
4.6 Niveaux de priviléges et organisation des comptes administratifs.....	33
4.7 Délégation d'administration.....	33
5. Plan de sauvegarde.....	34
5.1 Analyse de criticité des données.....	34
5.1.1 Données critiques.....	34
5.1.2 Données importantes.....	34

5.1.3 Données moins critiques.....	34
5.2.1 Sauvegardes locales sur chaque site (Primary Storage).....	35
5.2.2 RéPLICATION inter-site (en “box-to-box”).....	35
5.2.3 Externalisation Cloud souverain (optionnelle).....	36
5.2.4 Sécurisation des sauvegardes.....	36
5.3 Fréquences, versionning, rétention et type de sauvegarde.....	37
5.3.1 Données critiques.....	38
5.3.2 Données importantes.....	39
5.3.3 Données moins critiques.....	41
5.3.4 Justification de rétention des données.....	42
5.3.5 Limites et possibilités d'évolution.....	42
5.3.6 Conformité RGPD.....	43
5.4 Support de sauvegarde.....	44
5.4.1 Type de stockage retenu.....	44
5.4.2 Choix du RAID.....	44
5.4.3 Capacité et dimensionnement.....	46
6. Glossaire.....	47
7. Annexes.....	52

1. Contexte

L'entreprise **XANADU**, composée de 50 collaborateurs sur le site principal d'Atlantis et 10 employés sur un site distant à Springfield, engage une modernisation complète de son système d'information dans le cadre d'un déménagement. Le directeur souhaite profiter de cette transition pour renforcer la sécurité globale, améliorer l'organisation technique, homogénéiser les usages numériques et garantir la continuité d'activité.

La direction est particulièrement sensible aux risques cyber, notamment après l'immobilisation récente d'une entreprise partenaire suite à un rançongiciel*. Le nouveau système d'information devra donc intégrer nativement les principes de **confidentialité, intégrité, disponibilité et traçabilité** des données.

XANADU exploite plusieurs services métiers essentiels (comptabilité, commercial, juridique, ressources humaines, bureau d'étude et laboratoire distant) ainsi qu'un ERP* structuré en trois tiers (base PostgreSQL*, serveur applicatif, serveur Web). L'infrastructure actuelle souffre de plusieurs lacunes critiques : stockage non centralisé, absence de contrôle des priviléges, accès externes très limités, sauvegardes manuelles et hétérogènes, administration non mutualisée, exposition en HTTP*, et utilisateurs administrateurs de leurs postes.

Le nouveau système doit répondre aux besoins supplémentaires suivants :

- permettre la connexion des utilisateurs itinérants et en télétravail via une solution sécurisée
- assurer une cartographie claire des responsabilités administratives, avec délégation par service
- proposer une architecture Active Directory cohérente entre les deux sites
- garantir un **RTO* de 4 h** pour les données critiques (ERP, services prioritaires) et **24 h** pour les autres

- offrir une gestion rigoureuse des partages de fichiers et des droits associés
- fournir une visibilité complète sur l'infrastructure, via des GPO*, des règles de filtrage, un cloisonnement réseau et un plan de sauvegarde professionnel.

Ce livrable s'inscrit dans ce contexte de refonte intégrale et constitue la base de référence pour la mise en place d'un système d'information robuste, cohérent et administrable.

2. Objet du document

Le présent document constitue le **Livrable 1 – Cartographie du Système d'Information** du projet CESITECH pour l'entreprise XANADU.

Il a pour objectif de présenter **l'architecture cible** du système d'information que notre équipe propose pour les nouveaux sites d'Atlantis et Springfield.

Le document couvre :

2.1. Cartographie logique et technique

Cette partie présente une vue globale et détaillée de l'infrastructure cible.

Elle inclut un schéma d'ensemble du SI* (plan d'adressage TCP/IP*, VLAN*, DMZ*, rôles serveurs) ainsi que la cartographie logique du service Active Directory.

Dans cette cartographie AD, sont précisés les sites Active Directory, les contrôleurs de domaine et le placement des rôles FSMO*.

La structure de l'annuaire (OU* et groupes) est détaillée à travers des schémas accompagnés de commentaires, avec une justification des groupes de sécurité et de leurs usages réels.

L'administration déléguée est décrite par service, en précisant la répartition des priviléges, les types de comptes existants, leurs rôles, leurs restrictions et leurs périmètres.

Les GPO utilisées dans le SI sont répertoriées, avec au minimum cinq GPO de sécurité et cinq GPO d'administration, en présentant leur contenu et leurs liens d'application.

La cartographie identifie également les éléments contribuant à la confidentialité (chiffrement*, filtrage, segmentation), à l'intégrité (GPO, durcissement, signatures), à la disponibilité (redondances, supervision, sauvegardes) et à la traçabilité (audits, logs, supervision SIEM*/light).

Enfin, cette partie répond aux recommandations de l'ANSSI concernant la cartographie SI, en assurant une visualisation claire des assets, des rôles, des flux et des dépendances.

2.2. Politique et plan de sauvegarde

Le livrable présente une politique de sauvegarde alignée sur les exigences RTO/RPO* ainsi que sur la criticité des données (critique, importante, personnelle).

La topologie de sauvegarde est illustrée par un schéma réseau logique faisant apparaître les équipements dédiés (serveurs, appliances*, liens intersite), les flux locaux et intersite, ainsi que les cycles de sauvegarde et de réPLICATION.

La description couvre les types de sauvegardes utilisés (complète*, différentielle*, incrémentielle*), leurs fréquences, les politiques de rétention, le versioning*, ainsi que le chiffrage des données sauvegardées en AES-256*.

L'ensemble du plan reste cohérent avec l'architecture globale du SI : organisation Active Directory, segmentation réseau, rôles applicatifs et dépendances.

2.3. Livrable destiné à la présentation et à la mise en production

Ce document est conçu comme une référence technique et organisationnelle destinée à être présenté à la direction de XANADU en semaine 51, à servir de base pour la décision de lancement du projet.

Il sert aussi à guider les équipes techniques chargées du déploiement et de la migration.

Une rigueur particulière a été apportée à la structuration du document : page de garde, numérotation, sommaire, table des figures, schémas lisibles, justification des choix techniques et administratifs.

3. Documentation d'infrastructure réseau

Le schéma d'infrastructure réseau étant de taille importante et complexe, nous avons préféré le placer en **annexe à la fin du document**, ainsi, il est en format SVG permettant le zoom dans l'image sans perte de clarté (qualité).

3.1 Site A : "ATLANTIS" (Siège)

Passerelle* par défaut : Cluster* Switchs* SW1 / SW2

VLAN ID	Service / Nom du VLAN	Adresse Réseau	Masque*	Passerelle	Plage IP / Remarques
10	CGF	192.168.10.0	/24	.254	Clients DHCP*
20	COMMERCIAL	192.168.20.0	/24	.254	Clients DHCP
30	BDE	192.168.30.0	/24	.254	Clients DHCP
40	JURIDIQUE	192.168.40.0	/24	.254	Clients DHCP
50	RH	192.168.50.0	/24	.254	Clients DHCP
60	DIRECTION	192.168.60.0	/24	.254	Clients DHCP
70	INFORMATIQUE	192.168.70.0	/24	.254	Clients DHCP

1	IMPRIMANTES	192.168.0.0	/24	.254	IMP1: .1 / IMP2: .2
99	MANAGEMENT	192.168.99.0	/24	.254	Clients DHCP
100	SRV WINDOWS	192.168.100.0	/29	.6	SRV1: .1 / SRV2: .2
100	SRV LINUX	192.168.100.0	/29	.6	LN3: .3 / LN4: .4
DMZ A	ZONE DMZ	172.16.0.0	/24		Switchs SW3 & SW4
DMZ B	ZONE DMZ	172.17.0.0	/24	.254	Switchs SW7 & SW8

3.2 Site B : "SPRINGFIELD" (Site Distant)

Passerelle par défaut : Cluster Switchs SW5 / SW6

VLAN ID	Service / Name	Adresse Réseau	Masque	Passerelle	Plage IP / Remarques
80	LABO	192.168.80.0	/24	.254	Clients DHCP
1	IMPRIMANT ES	192.168.1.0	/24	.254	IMP3: .1 / IMP4: .2
110	SRV WINDOWS	192.168.110.4	/29	.10	SRV5: .5 / SRV6: .6
110	SRV LINUX	192.168.110.4	/29	.10	LN7: .7 / LN8: .8
DMZ	ZONE DMZ	172.17.0.0	/24		Switchs SW7 & SW8

3.3 LAN

3.3.1 Segmentation par VLANs (Virtual LAN*s)

Le découpage du réseau interne en plusieurs VLANs (10 à 70) répond à des impératifs de sécurité et de performance :

- **Cloisonnement de sécurité** : Chaque service (RH, Juridique, Direction) est isolé dans son propre domaine de diffusion. Un utilisateur du service "Commercial" ne peut pas accéder aux données du service "RH" ou "Juridique" sans passer par le routeur/pare-feu, où des règles de filtrage strictes (ACL*) sont appliquées.
- **Optimisation des performances** : En réduisant la taille des domaines de diffusion (Broadcast Domains*), on évite la saturation du réseau par des trames inutiles, garantissant une meilleure fluidité pour les applications critiques.

3.3.2 Redondance et Haute Disponibilité

L'infrastructure a été conçue pour éliminer tout point unique de défaillance (SPOF* - Single Point of Failure). La continuité de service est assurée à tous les niveaux :

- **Niveau Cœur de Réseau (Switchs L3)** : L'utilisation de paires de commutateurs (SW1/SW2 et SW5/SW6) permet, via des protocoles de redondance (type HSRP ou VRRP), de maintenir la passerelle par défaut active même si un équipement tombe en panne.
- **Niveau Pare-Feu** : Les firewalls* sont déployés par paires. En cas de défaillance matérielle de l'un d'eux, le trafic bascule instantanément sur le second sans couper les connexions vers Internet ou le VPN.
- **Niveau Serveurs** : Les serveurs Windows critiques sont doublés. Cette architecture en cluster permet soit de répartir la charge (Load Balancing*) pour absorber plus de demandes, soit d'assurer une reprise immédiate (Failover*) si un serveur devient indisponible.

3.3.3 Architecture DMZ "Sandwich" (Double Barrière)

La zone démilitarisée (DMZ) est isolée entre deux couches de pare-feux distinctes, offrant une sécurité maximale selon le principe de "Défense en Profondeur" :

1. **Pare-feu Frontal (FW_DMZ)** : Il constitue la première ligne de défense face à Internet. Son rôle est de filtrer le trafic "bruit" (scans de ports, attaques DDoS) et de ne laisser passer que les protocoles strictement nécessaires vers la DMZ (ex: VPN*, HTTPS*).
2. **Pare-feu Interne (FW_LAN)** : Il protège le cœur du réseau (LAN Atlantis) contre la DMZ elle-même. Si un serveur de la DMZ venait à être compromis par un attaquant, ce second pare-feu empêcherait l'intrusion de se propager vers les données sensibles de l'entreprise (VLANs internes), en l'occurrence aucun serveur n'est présent en DMZ car pour le moment XANADU est de l'ordre du privé, mais à l'avenir un serveur WEB ouvert au grand public pourrait être hébergé.

Cette séparation permet d'appliquer des politiques de filtrage granulaires : le pare-feu externe est permissif pour le public, tandis que le pare-feu interne est extrêmement restrictif pour protéger le LAN.

Les pare-feu suivront des matrices de filtrage afin de permettre / interdire les flux, la politique de filtrage sera en "Block All".

La politique "Block All" permettra d'interdire par défaut tous les flux, facilitant la gestion du trafic entrant et sortant et sécurisant au maximum l'infrastructure, ainsi les administrateurs n'auront qu'à définir une matrice de flux selon les demandes des différents services.

Nous utilisons pfSense comme solution de pare-feu car il offre un niveau de sécurité comparable aux solutions professionnelles propriétaires (Stormshield, Fortinet, Cisco), tout en apportant une intégration naturelle avec notre architecture et un coût total nettement plus faible. Cette solution open-source permet d'implémenter un filtrage avancé, un IDS/IPS, un proxy et une gestion centralisée des accès VPN, tout en restant accessible aux administrateurs internes. pfSense constitue ainsi le meilleur compromis entre performance

et administration pour une PME comme XANADU.

Le pfSense est virtuel ainsi, il doit être hébergé sur un serveur de haute performance.

La matrice **en annexe 1** peut être amenée à être modifiée à mesure que le projet avance.

3.3.4 Management

Adressage de Management (Switchs - VLAN 99)

Zone	Switchs	Réseau Management	IP Switch (Exemple)
LAN Atlantis	SW1, SW2	192.168.99.0 /24	SW1: .1 / SW2: .2
DMZ Atlantis	SW3, SW4	172.16.99.0 /24	SW3: .3 / SW4: .4
LAN Springfield	SW5, SW6	192.168.199.0 /24	SW5: .5 / SW6: .6
DMZ Springfield	SW7, SW8	172.17.99.0 /24	SW7: .7 / SW8: .8

3.3.5 Tableau de synthèse Infrastructure & topologie des services

SITE	Nom du SERVEUR	OS	ADRESSE IP	RÔLES & LOGICIELS	FONCTION PRINCIPALE
ATLANTIS	SRV-WIN1	Windows Srv 2022	192.168.100.1	AD DS*, DNS*, DHCP*, PROXY*, WSUS, Mail	Contrôleur de Domaine Principal (Maître FSMO). Détient les 5 rôles maîtres. Gère l'annuaire (AD), la résolution de noms (DNS), les baux IP (DHCP), le filtrage Web (Proxy) et le

					déploiement des mises à jour (WSUS) ainsi que les services de messagerie électronique.
ATLANTIS	SRV-WIN2	Windows Srv 2022	192.168.100.2	AD DS, DNS, DHCP, PROXY, WSUS, Mail	<p>Serveur de redondance.</p> <p>Redonde le SRV-WIN1. Assure la continuité de service (Failover DHCP, Réplication AD) en cas de panne</p>
ATLANTIS	SRV-LN3	Ubuntu LTS 24.04	192.168.100.3	NGINX*, POSTGRESQL, WAZUH*, ZABBIX*, Sauvegardes	<p>Serveur Web & SGBD*. Héberge l'application Web principale (Nginx) et la base de données relationnelle (PostgreSQL).</p> <p>Serveur de monitoring (Zabbix). Surveille l'état de santé du réseau (bande passante*, pannes matérielles) via SNMP et agents.</p> <p>Serveur de supervision (Wazuh). Récupère les données des équipements pour détecter et alertes les anomalies réseau.</p>

					Stockage des sauvegardes sur les disques en RAID 10*
ATLANTIS	SRV-LN4	Ubuntu LTS 24.04	192.168.100.4	NGINX, POSTGRESQL , WAZUH, Sauvegardes	Haute Disponibilité Web. RéPLICATION de la base de données et répartition de charge pour l'application métier RéPLICATION des services de supervision et de monitoring Stockage des sauvegardes sur les disques en RAID 6
SPRINGFIELD	SRV-WIN5	Windows Srv 2022	192.168.110.1	AD DS, DNS, DHCP, PROXY, Mail	Contrôleur de Site Distant. Authentification locale pour le Labo. Gère le DHCP local (VLAN 80). Réplique le serveur SRV-WIN1 du site Atlantis
SPRINGFIELD	SRV-WIN6	Windows Srv 2022	192.168.110.2	AD DS, DNS, DHCP, PROXY, Mail	Redondance Site Distant. Assure la haute disponibilité des services critiques sur le site de Springfield. Redonde et réplique le serveur SRV-WIN5 du site Springfield.

SPRINGFIELD	SRV-LN7	Ubuntu LTS	192.168.95.3	WAZUH, ZABBIX	Serveur de monitoring (Zabbix). Surveille l'état de santé du réseau (bande passante*, pannes matérielles) via SNMP et agents. Serveur de supervision (Wazuh). Centralise les logs, détecte les intrusions et analyse les vulnérabilités du parc informatique.
SPRINGFIELD	SRV-LN8	Ubuntu LTS	192.168.95.4	WAZUH (SIEM), ZABBIX, Sauvegardes	Serveur de supervision. Centralise les logs, détecte les intrusions et analyse les vulnérabilités du parc informatique. Stockage des sauvegardes sur les disques en RAID 6

AD DS : Service permettant l'hébergement d'un annuaire Active Directory

DHCP : Service hébergé sur un serveur permettant l'attribution d'adresses IP via des plages d'adresses définies.

DNS : Service hébergé sur un serveur permettant de résoudre la correspondance entre les noms de domaines et les adresses IP (google.com ~= 8.8.8.8)

Pour le DNS, nous avons mis des enregistrements :

- Hôte (A) et PTR (reverse dns), permettant la résolution des adresses IP vers leurs FQDN, nous avons enregistré tous les équipements réseaux (firewalls, switchs, routeurs), serveurs (ex: srv-win1 = 192.168.100.1) et clients (PC1 = 192.168.10.1)

- CNAME, permet de rediriger la résolution DNS vers un autre enregistrement DNS évitant la répétition (ex: www.xanadu.local = srv-win1.xanadu.local = 192.168.100.1)

Nous comptons forwarder le DNS interne vers un DNS public (Cloudflare en 1.1.1.1 ou Google en 8.8.8.8).

Messagerie : Nous hébergerons les services de messagerie sur les Windows Server 2022 (SRV-WIN 1 / 2 / 3 / 4 avec le 2 et le 4 qui sont des redondances du 1 et 3 respectivement).

La solution utilisée sera hMailServer car elle permet l'administration compatible via Active Directory.

Proxy : Serveur intermédiaire relayant les requêtes Internet des postes clients. Il contrôle, filtre et journalise les accès Web avant de transmettre les flux vers l'extérieur. Il permet ainsi d'appliquer des politiques de sécurité centralisées et de protéger le réseau interne.

Nous avons choisi Squid* pour sa résilience à la charge, sa compatibilité Active Directory, son filtre et car il est open source*, il permet le cache, l'authentification et la journalisation complète. D'autres solutions comme pfSense, OPNsense, BlueCoat ou Zscaler existent mais sont plus coûteuses, plus complexes ou moins intégrables dans l'environnement actuel. Squid apporte un excellent compromis entre performance, sécurité et maîtrise.

Nous utilisons les services (DHCP, DNS, AD, partages de fichiers) de Windows Server car l'écosystème Windows permet la gestion intelligente, organisée et rapide des services et parce que l'utilisation de l'AD est imposée.

Sauvegardes : Nous utiliserons les serveurs linux de redondance (SRV-LN4 redondance du SRV-LN3, et SRV-LN8 redondant du SRV-LN7), puis nous répliquerons les sauvegardes entre les sites et enfin dans un cloud, comme convenu dans la partie "5.Plan de sauvegarde"

Aparté – Contraintes de la maquette pédagogique

Dans la maquette pédagogique, les serveurs disponibles (SRV-LN3, SRV-LN4, SRV-LN7, SRV-LN8) ne disposent pas du stockage nécessaire pour mettre en œuvre du RAID 10 ou RAID 6. Nous utiliserons donc un RAID 5, uniquement pour les besoins de la démonstration.

Ce choix est imposé par les limites de l'environnement et ne reflète pas l'architecture cible, plus robuste.

3.4 Rôles FSMO

Dans l'architecture Active Directory XANADU.local, la cohérence de la base de données est garantie par les 5 rôles de maîtres d'opérations (**FSMO** - Flexible Single Master Operations).

Pour des raisons de stabilité et de performance, **l'intégralité de ces 5 rôles est centralisée sur le serveur SRV-WIN1** (Site Siège). Les autres serveurs agissent comme des réplicas (Catalogues Globaux) pour assurer la redondance de l'authentification.

Les 5 rôles hébergés par SRV-WIN1 sont :

1. **Schema Master** : Gère la structure de l'annuaire (ajout d'attributs).
2. **Domain Naming Master** : Gère les noms de domaines dans la forêt.
3. **PDC Emulator*** : Le rôle le plus sollicité, il gère les changements de mots de passe, l'heure (NTP*) et les GPO.
4. **RID* Master** : Distribue les identifiants uniques (SID*) pour les nouveaux objets.
5. **Infrastructure Master** : Gère les références entre objets de différents domaines.

3.5 Stratégies de groupe (GPO)

L'administration du parc informatique (Windows 11) est entièrement centralisée et automatisée via les Stratégies de Groupe (GPO).

Cette approche permet de déployer massivement des configurations sur les postes clients sans intervention manuelle. Les stratégies sont divisées en deux catégories : le Durcissement (Sécurité/Restrictions) pour protéger le système, et l'Environnement (Confort/Outils) pour fournir un espace de travail prêt à l'emploi.

Nom de la GPO	Paramètres techniques appliqués	Cible (OU)	Type de la GPO
GPO_Default_Secu (2 GPO)	<ul style="list-style-type: none"> - Mots de passe complexes (12 car, Maj/Min/Chiffres/Caractères). - Verrouillage du compte après 3 échecs (15 min). 	Domaine (Tout le monde)	Sécurité
GPO_Lockdown_System (4 GPO)	<ul style="list-style-type: none"> - Blocage du Panneau de Configuration. - Désactivation de l'invite de commande (CMD/PowerShell). - Interdiction d'accès au Registre (Regedit). - Masquage du lecteur C: dans l'explorateur. 	Utilisateurs (Sauf Service Informatique)	Sécurité
GPO_USB_Block	<ul style="list-style-type: none"> - Interdiction de lecture/écriture sur les clés USB et disques 	Services Sensibles	Sécurité

(1 GPO)	externes pour éviter le vol de données.	(<i>Labo, RH, Direction</i>)	
GPO_Drive_Maps (2 GPO)	- Montage automatique du lecteur S: (Dossier Partagé du Service). - Montage automatique du lecteur H: (Espace Personnel).	Par Service	Administratif
GPO_Proxy_Config (1 GPO)	- Configuration forcée du proxy (SRV-WIN:8080) dans les navigateurs (Edge/Chrome) pour filtrer le web.	Tous les Utilisateurs	Sécurité
GPO_Branding (2 GPO)	- Application du fond d'écran corporatif "Xanadu" (verrouillé). - Verrouillage de la barre des tâches.	Tous les Utilisateurs	Administratif

GPO_Session_Lock (1 GPO)	- Verrouillage automatique de l'écran après 10 minutes d'inactivité.	Tous les Utilisateurs	Sécurité
GPO_Imprimantes (2 GPO car 2 sites)	- Déploiement automatique des imprimantes partagées par site	Tous les Utilisateurs	Administratif
GPO_Antivirus (1 GPO)	- Paramétrage de Windows Defender (activation, analyse planifiée quotidienne, protection en temps réel activée, blocage des modifications par l'utilisateur)	Tous les Utilisateurs	Sécurité

3.6 Services de connexion à distance (itinérance, site-distant)

3.6.1. Interconnexion des sites : choix d'un VPN MPLS* (site-à-site*)

L'entreprise XANADU a demandé la mise en place d'un réseau MPLS pour relier son siège (Atlantis) à sa nouvelle agence (Springfield). Ce choix repose sur des arguments techniques et organisationnels.

Le MPLS, en tant que solution opérateur dédiée et managée, offre un service avec SLA*, latence maîtrisée, priorisation des flux et supervision continue. Contrairement à un VPN IPSec* auto-géré, la DSI* n'a pas à administrer les tunnels, la redondance ou la gestion des incidents WAN.

L'interconnexion repose sur un réseau privé isolé d'Internet, garantissant des routes déterministes et des flux intersites stables même en période de charge. Ce fonctionnement est idéal pour une connexion permanente entre deux LAN (Active Directory, DNS, fichiers, applications internes).

Le MPLS répond également aux besoins fonctionnels de XANADU : réPLICATION Active Directory, accès direct aux partages réseau, consultation du serveur applicatif du siège et exécution des sauvegardes intersites. Tous ces usages exigent une liaison stable, continue et performante, caractéristique principale du MPLS.

3.6.2 Accès des utilisateurs itinérants : choix d'OpenVPN (point-à-client)

Pour répondre aux besoins de mobilité (ex. poste PC_TT_1), l'entreprise met en place un accès VPN destiné aux utilisateurs en télétravail ou en déplacement. La solution choisie est un VPN SSL* client-to-site, reposant sur OpenVPN, adapté aux connexions individuelles depuis Internet.

Les connexions distantes arrivent en DMZ via le pare-feu externe, sont authentifiées par l'Active Directory (RADIUS/NPS*), puis accèdent au LAN. Le chiffrement utilisé est l'AES-256, garantissant la confidentialité des échanges.

Contrairement au lien MPLS, pensé pour relier des sites, OpenVPN est conçu pour relier des personnes, depuis des environnements variés (domicile, 4G, hôtels). Il offre une compatibilité large avec Windows 10/11, Linux (dont Ubuntu pour le labo), macOS, iOS et Android, permettant aux utilisateurs de se connecter depuis n'importe quel poste autorisé.

OpenVPN fonctionne même dans des environnements réseau restrictifs grâce à la possibilité d'utiliser le port TCP 443, ce qui lui permet de passer derrière les box Internet, dans les réseaux fortement filtrés ou sur les WiFi publics. Cette capacité est essentielle pour les profils nomades comme les commerciaux et techniciens.

La solution s'intègre facilement avec l'Active Directory : authentification LDAP*/AD, gestion centralisée des droits et possibilité d'utiliser un système de certificats pour renforcer la sécurité.

WireGuard, bien que performant, repose sur des clés statiques et n'offre pas d'intégration AD native, ce qui le rend moins adapté au contexte de XANADU.

Enfin, OpenVPN bénéficie de plus de vingt ans de maturité en entreprise : solution stable, auditée, abondamment documentée et largement supportée par les firewalls et appliances du marché.

Par contraste, **WireGuard**, même excellent, est encore jeune dans les environnements professionnels (peu de fonctionnalités d'entreprise, pas d'intégration AD native).

3.7 WAN (Routeurs)

Routeur	Zone	IP Publique / Transit	Fonction
R1	Atlantis	20.20.20.1 /24	Sortie Internet Site A
R2	Springfield	30.30.30.1 /24	Sortie Internet Site B
R3	Télétravail	40.40.40.1 /24	Accès distant isolé
-	Transit Interne	10.0.0.254 /24	Liaison Routeur vers DMZ

Légende et Notes Techniques

Réseaux /24 : Réseaux standards pour postes clients (254 hôtes disponibles)

Réseaux /29 : Réseaux serveurs (6 hôtes disponibles, optimisation de l'espace IP, interdiction de potentiels menaces qui se branchent sur le réseau des serveurs)

VLAN DMZ : Zones démilitarisées isolées avec adressage RFC1918 distinct

SRV : Serveurs Windows

LN : Serveurs Linux

IMP : Imprimantes réseau

SW : Switch de distribution/accès

R : Routeur WAN

Justification des choix d'architecture

L'architecture réseau retenue pour le projet Atlantis/Springfield repose sur trois piliers fondamentaux : la segmentation, la haute disponibilité et la défense en profondeur. Voici le détail des décisions techniques.

3.8 Sécurisation et amélioration continue du système d'information

3.8.1 Antivirus, EDR, XDR

Nous garderons Windows Defender comme antivirus* de base car il est fiable, intégré et gratuit, protégeant efficacement contre les malwares* classiques (score 6/6 via AV-TEST*).

Nous ajouterons l'EDR* "OpenEDR*" permettant de détecter les attaques avancées (ransomware, APT*) ainsi que de corrélérer les événements et automatiser la réponse aux incidents car l'antivirus ne se limite que à la vérification des signatures connues des malwares. A l'avenir, l'intégration de Microsoft Defender for Endpoint (solution payante) sera à envisager pour remplacer l'EDR open source.

Et nous ajouterons l'XDR* Wazuh afin de détecter le trafic réseau malveillant, là où l'EDR ne se limite qu'aux actions du clients. Nous choisissons Wazuh plutôt que d'autres XDR comme CrowdStrike Falcon XDR ou Palo Alto Cortex XDR ou encore Splunk, car ces solutions sont payantes ou alors doivent être intégrées dans des infrastructures de taille importante.

Cette combinaison assure une protection complète, nous permet de filtrer et d'écartier les logiciels malveillants connus (via antivirus), les attaques avancées ou l'empoisonnement de fichiers (via l'EDR) et les fuites ou requêtes réseau malveillantes (via l'XDR), tout en facilitant l'administration et la traçabilité du système d'information.

Des ateliers de formation et des séances de sensibilisation à la cybersécurité seront mis en application en réponse aux questionnaires de sécurité envoyés aux employés pour le livrable 2.

3.8.2 Mise à jour

Le choix de WSUS permet de centraliser, contrôler et planifier le déploiement des mises à jour sur tous les postes et serveurs, tout en optimisant la bande passante et en garantissant la conformité et la sécurité du système d'information. Il s'intègre parfaitement à l'environnement Windows existant et facilite la gestion sur un SI multi-sites comme celui de XANADU.

Ainsi les mises à jour des postes ne se feront pas localement par les clients, mais plutôt via l'approbation et le déploiement du service informatique prévenant les mises à jour potentiellement défectueuses ou non compatibles avec l'existant.

3.9 Inventaire

Catégorie	Type d'équipement	Modèle / Version	Quantité	Prix unitaire
Réseau	Routeur	Cisco 7200 VXR (IOS 15.x)	3	
Réseau	Commutateur (Switch L3)	Cisco Catalyst 3650 (Virtuel)	8	

Réseau	Pare-Feu (Firewall)	pfSense* (Appliance Virtuelle)	8	
Système	Serveur (OS Microsoft)	Windows Server 2022 Standard	4	
Système	Serveur (OS Linux)	Ubuntu Server 22.04 LTS	4	
Client	Poste de travail	Windows 11 Pro	10+	

4. Vue administrative et gestion des identités

4.1 Service d'annuaire

L'infrastructure repose sur le service d'annuaire Microsoft Active Directory (AD DS), permettant la centralisation de l'authentification, de la gestion des utilisateurs, des groupes, des postes de travail et des ressources réseau. Le domaine utilisé est : **XANADU.local**.

4.2 Politique de nommage (Naming Convention)

Une convention stricte est appliquée afin d'assurer l'homogénéité et de faciliter les automatisations au sein de l'annuaire.

Identifiant de connexion (sAMAccountName)

Format : p.nom

Exemple : Jean Dupont → j.dupont

Nom d'affichage (Display Name)

Format : Prénom Nom

Exemple : Jean Dupont

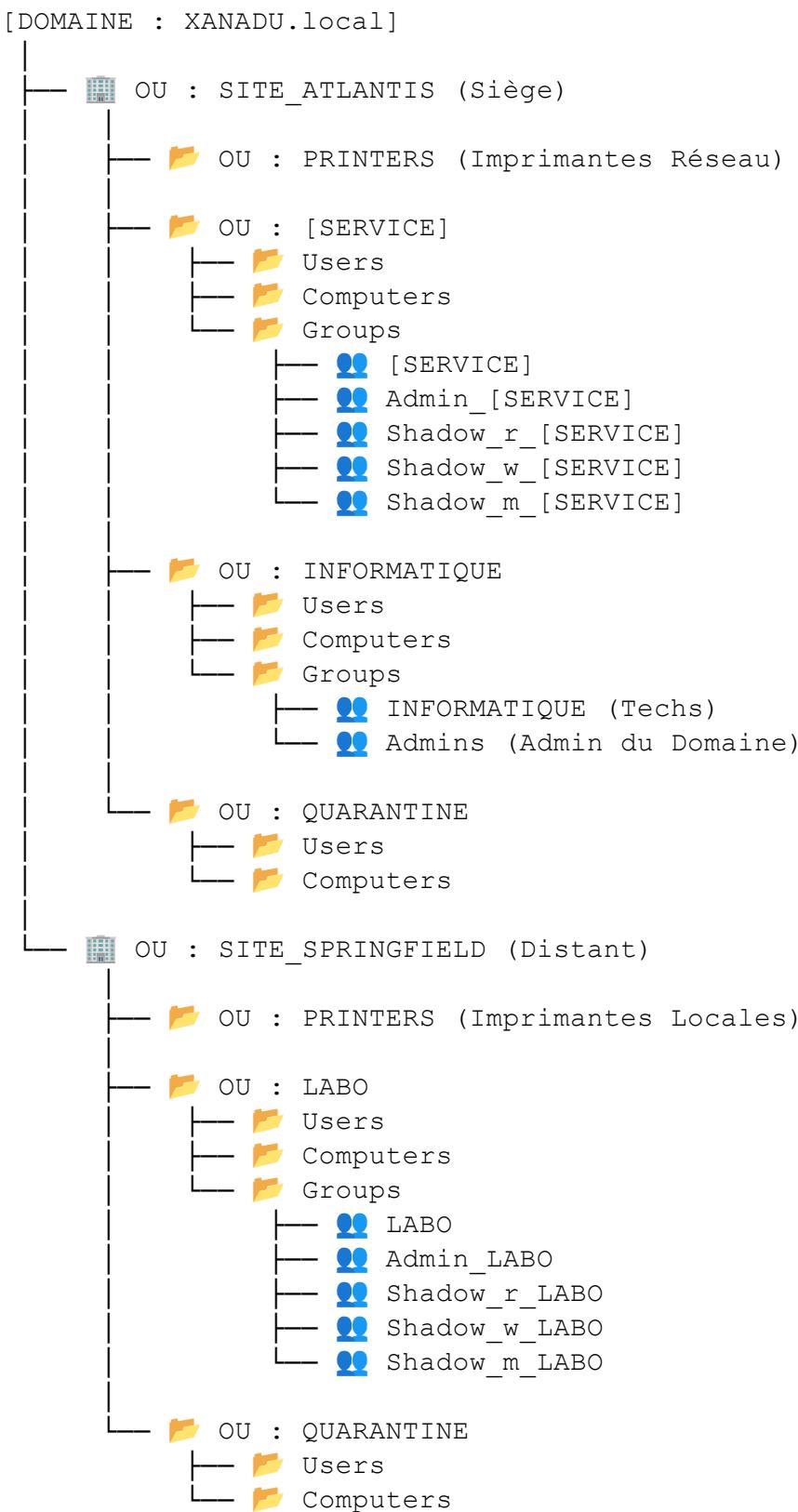
Messagerie de contact (E-mail) :

p.nom@xanadu.local

Exemple : j.dupont@xanadu.local

4.3 Forêt Active Directory et Arborescence LDAP (schéma complet)

L'organisation logique des Unités d'Organisation (OU) reflète la structure fonctionnelle de l'entreprise. La structure sera insérée dans la zone prévue ci-dessous.



Justification

Pour le projet de migration et de sécurisation du système d'information de XANADU, une monoforêt avec un seul domaine est la solution la plus adaptée.

Avec 50 collaborateurs sur le site principal et 10 sur le site distant, cette architecture permet de centraliser la gestion des comptes, des groupes et des droits d'accès, tout en simplifiant l'administration et la délégation par OU.

Elle garantit également une application uniforme des stratégies de sécurité, une traçabilité complète, et facilite les sauvegardes et la reprise d'activité en cas d'incident.

Enfin, elle optimise les flux entre Atlantis et Springfield via le VPN MPLS, réduisant la complexité et les coûts liés à la gestion de plusieurs domaines ou forêts.

Cette approche assure ainsi stabilité, sécurité et simplicité de gestion, conformément aux objectifs du projet.

Ainsi, nous retrouvons :

- 4 Contrôleurs de domaine (SRV-WIN1 / 2 / 3 / 4)
- 60 Comptes utilisateurs
- X comptes administrateurs
- 60 postes clients
- 4 imprimantes

4.4 Partage de dossiers

Les règles de partage des données sont définies comme suit :

- Un dossier partagé par service, accessible uniquement aux membres du service concerné.
- Un dossier personnel centralisé pour chaque salarié, accessible via « Mes documents » et limité par un quota.

- Le service Juridique doit accéder aux dossiers du Service Client et des Ressources Humaines.
- La Direction doit disposer d'un accès à l'ensemble des dossiers de tous les services.

Ces droits sont gérés exclusivement via les groupes de sécurité Active Directory.

4.5 Gestion des droits et groupes Shadow* (AGDLP* simplifié)

Afin d'assurer une gestion cohérente et évolutive des permissions NTFS, chaque service dispose de trois groupes fonctionnels :

Groupe Shadow_r_[SERVICE]

Type d'accès : Lecture seule

Usage : Consultation sans modification.

Groupe Shadow_w_[SERVICE]

Type d'accès : Modification standard (lecture/écriture)

Usage : Collaborateurs du service, production documentaire.

Groupe Shadow_m_[SERVICE]

Type d'accès : Contrôle total

Usage : Responsables de service et gestion avancée des dossiers.

Ces groupes permettent d'attribuer les permissions sans agir directement sur les comptes utilisateurs.

4.6 Niveaux de privilèges et organisation des comptes administratifs

Dans un objectif de sécurité et conformément au modèle de séparation des privilèges, le personnel informatique (uniquement les administrateurs réseau & systèmes) utilise deux comptes distincts :

Compte standard (ex. : j.dupont)

Utilisé pour les activités quotidiennes : messagerie, navigation, bureautique. Aucune permission d'administration.

Compte administrateur (ex. : adm_j.dupont)

Utilisé exclusivement pour les tâches d'administration du domaine, des serveurs et de l'infrastructure réseau. Membre du groupe Domain Admins.

4.7 Délégation d'administration

Un utilisateur lambda a le droit d'interagir avec les fichiers contenus dans son répertoire personnel et ceux de son service (selon ses droits shadow).

Un correspondant informatique est désigné dans chaque service. La délégation est strictement limitée à l'OU du service concerné. Le correspondant peut :

- Créer et mettre à jour les comptes utilisateurs de son service.
- Gérer les appartenances aux groupes Shadow du service.
- Intégrer les postes de travail au domaine.

La délégation est appliquée via l'assistant de délégation Active Directory et des GPO adaptées, garantissant qu'aucune action ne peut dépasser le périmètre du service concerné.

5. Plan de sauvegarde

L'objectif du plan de sauvegarde de XANADU est d'assurer la continuité d'activité en garantissant :

- un **RTO** de 4 heures pour les données critiques,
- un **RTO de 24 heures** pour les données importantes,
- un **RPO (Recovery Point Objective)** adapté à la nature de chaque donnée.

La stratégie repose sur le principe **3-2-1**, avec un double site (Atlantis et Springfield) permettant une externalisation naturelle des sauvegardes.

5.1 Analyse de criticité des données

Les données ont été classées en trois niveaux, selon leur importance pour l'activité :

5.1.1 Données critiques

Les données critiques regroupent la base PostgreSQL de l'ERP, d'environ 10 Go, ainsi que les partages des services Direction, Juridique et Sinistres. Leur impact métier est majeur : toute indisponibilité compromet gravement l'activité.

5.1.2 Données importantes

Les données importantes regroupent les documents partagés des services Client, Conseil et Commerce, ainsi que les courriels professionnels hébergés sur les serveurs de messagerie. Elles sont essentielles au fonctionnement quotidien de l'entreprise.

5.1.3 Données moins critiques

Les dossiers personnels des collaborateurs présentent un impact limité en cas d'indisponibilité temporaire.

5.2 Architecture du système de sauvegarde

La stratégie de sauvegarde retenue s'articule autour de trois niveaux de protection complémentaires, conçus pour répondre aux exigences de disponibilité du directeur de XANADU.

L'architecture exploite pleinement la présence de deux sites interconnectés (Atlantis et Springfield) afin de garantir une continuité d'activité même en cas de sinistre majeur.

5.2.1 Sauvegardes locales sur chaque site (Primary Storage)

Chaque site dispose d'un serveur ou d'un NAS* de sauvegarde dédié, placé dans le réseau interne (hors DMZ). Ce stockage local constitue le premier niveau de protection : il permet des restaurations rapides en cas d'incident, comme une suppression accidentelle, une corruption ou une panne logicielle, et autorise des sauvegardes fréquentes pour les données critiques.

Cette proximité réduit la charge réseau, facilite la reprise d'activité et garantit des points de restauration très récents, indispensables au respect des contraintes RTO.

5.2.2 RéPLICATION inter-site (en “box-to-box”)

Les sites d'Atlantis et de Springfield assurent une réPLICATION bidirectionnelle de leurs sauvegardes, ce qui permet au site distant de jouer pleinement le rôle de copie hors-site. Cette duplication géographique constitue un élément essentiel de résilience : elle protège l'entreprise contre les rançongiciels, contre les sinistres physiques tels que l'incendie ou le vol, et contre toute panne matérielle majeure compromettant l'infrastructure locale.

Les flux de réPLICATION sont chiffrés en AES-256 et transitent au travers de la liaison MPLS opérateur, garantissant des échanges performants et confidentiels.

Ce second niveau de sauvegarde assure ainsi une véritable continuité d'activité, même en cas d'indisponibilité totale d'un site principal.

5.2.3 Externalisation Cloud souverain (optionnelle)

L'externalisation des données critiques vers un cloud chiffré et souverain* peut constituer un troisième niveau de sécurité. Cette couche supplémentaire garantirait une capacité de restauration même dans les scénarios les plus extrêmes, comme la compromission simultanée des deux sites, le chiffrement massif provoqué par un ransomware* particulièrement avancé ou un sinistre d'ampleur exceptionnelle.

Dans le cadre de ce projet, cette option est recommandée pour atteindre une résilience maximale, mais elle n'est pas indispensable : la réPLICATION intersite fournit déjà une copie hors-site solide et conforme aux exigences de la règle 3–2–1.

5.2.4 Sécurisation des sauvegardes

La protection des sauvegardes s'appuie sur un ensemble de mesures complémentaires destinées à garantir leur intégrité et leur confidentialité. Les données sont chiffrées en AES-256, aussi bien au repos que lors de leur transfert, et les opérations sont réalisées à l'aide de comptes de service dédiés, strictement limités aux priviléges nécessaires. Lorsque l'infrastructure le permet, les sauvegardes sont rendues immuables* afin d'empêcher toute modification, notamment en cas d'attaque par ransomware.

L'ensemble du dispositif fait l'objet d'une supervision quotidienne : l'état des sauvegardes et des réPLICATIONS est suivi en continu, des alertes automatiques sont déclenchées en cas d'erreur, et des tests de restauration hebdomadaires (le week-end) garantissent la validité des données et la capacité effective à les récupérer.

Afin de limiter la surface d'attaque en cas de ransomware tout en conservant une gestion du stockage efficace, les sauvegardes immuables seront supprimées au-delà de 3 versions antérieures ou de 30 jours.

Les sauvegardes immuables suivent la rétention définie dans les tableaux de la section 5.3. Elles ne sont toutefois supprimées qu'après l'existence d'au moins trois versions plus récentes, ce qui peut prolonger leur conservation. Néanmoins, pour garantir la conformité au RGPD, aucune sauvegarde immuable ne sera conservée au-delà de cinq ans.

En cas d'échec d'une sauvegarde ou d'une réplication, une alerte automatique est immédiatement envoyée par courriel à l'administrateur réseau afin de permettre une intervention rapide.

Chaque opération de sauvegarde génère des journaux détaillés, conservés sur le serveur de sauvegarde, retraçant l'ensemble du processus (fichiers traités, anomalies détectées, durée, taille, état final).

Une procédure interne encadre le traitement de ces incidents : consultation systématique des logs, identification de la cause (erreur réseau, corruption d'un fichier, absence d'accès, dépassement de quota), relance manuelle du job si nécessaire, puis validation d'une restauration de test pour garantir le bon fonctionnement du cycle de sauvegarde.

Cette méthodologie assure une détection précoce des défaillances et permet d'éviter qu'un incident isolé ne compromette la résilience globale du système.

Ce niveau de contrôle et de durcissement réduit drastiquement le risque d'altération, de corruption ou de suppression malveillante des sauvegardes.

5.3 Fréquences, versionning, rétention et type de sauvegarde

Les stratégies de sauvegarde sont adaptées aux besoins métiers, aux contraintes de restauration (RTO) et à l'optimisation réseau/stockage.

Les sauvegardes inter-site suivent un cycle structuré : les incrémentiels sont réinitialisés à chaque nouvelle sauvegarde complète, garantissant des restaurations fiables et évitant l'allongement des chaînes.

Toutes les sauvegardes quotidiennes et hebdomadaires sont planifiées durant les plages nocturnes sauf indication contraire dans les tableaux de manière à limiter la charge sur le réseau en période de production et à ne pas impacter l'activité des utilisateurs.

Les sauvegardes des données critiques et importantes seront immuables.

Chaque sous-partie présente un tableau récapitulatif suivi d'une justification.

5.3.1 Données critiques

(ERP – Direction – Juridique – Sinistres)

Objectif : RTO ≤ 4 heures

Paramètres retenus

Niveau	Fréquence	Type	Rétention
Local	Toutes les 3 heures	Différentiel	7 jours
Local	Quotidien	Complète	7 jours
Inter-site	Toutes les 6 heures	Différentiel	30 jours
Inter-site	Hebdomadaire	Complète	30 jours
Cloud	Quotidien	Complète	2 mois

La fréquence retenue donne un RPO de 3 heures, ce qui reste cohérent avec l'objectif de restauration fixé à un RTO de 4 heures.

Justification

Nous avons choisi le différentiel toutes les 3 heures sur les données critiques, car en cas d'incident majeur, la restauration doit être extrêmement rapide : un seul différentiel à

restaurer après la sauvegarde complète quotidienne. Cela minimise le risque d'erreur et garantit un retour en production compatible avec le RTO de 4 heures.

La réPLICATION inter-SITE plus espacée (6h) réduit la pression réseau tout en conservant une copie hors-SITE récente.

Une sauvegarde complète intersite hebdomadaire casse la chaîne des différentiels distants, garantissant une restauration simple même hors site, tout en maîtrisant la bande passante.

5.3.2 Données importantes

(Client, Commerce, Conseil, Emails)

Objectif : RTO \leq 24 heures

Paramètres retenus

Niveau	Fréquence	Type	Rétention
Local	Quotidien (à 1h)	Complète	7 jours
Local	Quotidien (à 13h)	Incrémentiel	7 jours
Intersite	Quotidien	Incrémentiel	30 jours
Intersite	Hebdomadaire	Complète	30 jours

Une sauvegarde locale sera faite toutes les 12h.

La fréquence retenue donne un RPO de 12 heures, ce qui reste cohérent avec l'objectif de restauration fixé à un RTO de 24 heures.

Justification

La planification d'une sauvegarde complète à 1h du matin et d'une incrémentielle à 13h permet d'établir un espacement d'environ douze heures entre les deux opérations, garantissant ainsi un RPO de 12 heures.

La sauvegarde complète est programmée durant une plage de faible activité (heures non ouvrées et pause de repas) afin de ne pas perturber le réseau ou les utilisateurs. L'incrémentielle, exécutée entre midi et deux, reste très légère puisqu'elle ne traite que les modifications réalisées durant la matinée.

Cette organisation assure une protection continue des données importantes sans impacter la production, tout en évitant la perte d'une journée d'activité.

Une alternative consisterait à lancer les sauvegardes à 6h et 19h, mais la sauvegarde incrémentielle du matin n'apporterait alors aucune valeur ajoutée, d'où le choix d'une cadence plus pertinente.

Les données importantes nécessitent une stratégie efficace en stockage, car elles peuvent représenter une volumétrie élevée. Le choix de l'incrémentiel permet de transférer uniquement les blocs modifiés, ce qui réduit l'impact sur le réseau et optimise l'espace utilisé par les sauvegardes.

Le RTO de 24 heures autorise une restauration plus lente (complète + incrémentiels), ce qui rend ce compromis optimal.

La sauvegarde complète intersite hebdomadaire évite l'allongement de la chaîne d'incrémentiels distants et garantit un cycle propre chaque semaine.

5.3.3 Données moins critiques

(Dossiers personnels utilisateur)

Objectif : RTO ≤ 24h

Paramètres retenus

Niveau	Fréquence	Type	Rétention
Local	Quotidien	Incrémentiel	7 jours
Local	Hebdomadaire	Complète	7 jours
Inter-site	Hebdomadaire (mercredi)	Incrémentiel	30 jours
Inter-site	Hebdomadaire (samedi)	Complète	30 jours

La fréquence retenue donne un RPO de 24 heures, ce qui reste cohérent avec l'objectif de restauration fixé à un RTO de 24 heures. Avec ce dispositif on a également 2 réplications par semaine.

Justification

Le recours à l'incrémentiel est particulièrement adapté aux dossiers personnels, car même si le volume moyen par employé est relativement limité (environ 5 Go), l'ensemble représente une quantité de données non négligeable pour une organisation d'une soixantaine de collaborateurs.

Le recours à l'incrémentiel est donc le plus pertinent :

- il limite le stockage consommé,
- évite de saturer le réseau inutilement,
- reste cohérent avec un RTO pouvant aller jusqu'à 24 heures.

Comme pour les autres catégories, la sauvegarde complète intersite hebdomadaire réinitialise la chaîne et assure une restauration simple.

Ainsi, le fait d'alterner une sauvegarde incrémentielle en semaine (le mercredi) et une sauvegarde complète le week-end (le samedi) permet de maintenir des sauvegardes légères durant la période d'activité, tout en consolidant l'ensemble des modifications dans une version complète en fin de semaine. Cette organisation assure un bon équilibre entre charge réseau, volume de stockage et simplicité de restauration.

5.3.4 Justification de rétention des données

La rétention locale est volontairement limitée à 7 jours, car ce stockage est dédié aux restaurations rapides et reste plus exposé aux incidents (erreurs utilisateur, ransomware, pannes locales).

À l'inverse, la rétention intersite est fixée à 30 jours : le site distant constitue une copie hors-site sécurisée permettant de restaurer des données plus anciennes sans risque de surcharge ou de compromission.

Cette dissymétrie local / intersite répond aux bonnes pratiques de la règle 3-2-1* et optimise les performances tout en assurant une profondeur d'historique suffisante pour le métier.

5.3.5 Limites et possibilités d'évolution

Cette stratégie représente un compromis équilibré entre rapidité de restauration, maîtrise du stockage et gestion de la charge réseau. Comme toute politique de sauvegarde, elle comporte néanmoins certaines limites : une augmentation significative de la volumétrie peut conduire à ajuster la fréquence des sauvegardes complètes, l'utilisation d'incrémentiels

rallonge parfois la durée de restauration, et les sauvegardes différentielles tendent à s'alourdir en fin de cycle.

L'un de ses atouts majeurs réside toutefois dans sa flexibilité. La fréquence des sauvegardes, la rétention, ou même le type de sauvegarde qu'il s'agisse de complètes, différentielles, incrémentielles ou de sauvegardes synthétiques* peuvent être ajustés rapidement en fonction des retours d'expérience, de l'évolution du réseau, des besoins métiers ou des variations de volume de données. Cette capacité d'adaptation garantit une évolutivité naturelle du dispositif de sauvegarde.

5.3.6 Conformité RGPD

Les sauvegardes contenant des données personnelles sont soumises à la réglementation du RGPD.

Type de données	Finalité	Durée indicative
Données des salariés (RH)	Gestion administrative et paie	5 ans après fin du contrat (conformité légale)
Données clients / contrats	Obligations contractuelles et preuve	10 ans (conformité Code civil / preuve)
Emails professionnels	Archivage légal, preuve	6 mois à 5 ans selon usage et nécessité
Données ERP (comptabilité)	Obligations fiscales et comptables	10 ans (loi française)
Données moins critiques (personnelles temporaires)	Usage opérationnel	Dès que plus nécessaire, suppression ou anonymisation

Les sauvegardes non immuables respecteront la durée de rétention définie dans le tableau (maximum 30 jours), ce qui reste largement inférieur aux exigences du RGPD et ne pose donc aucun problème de conformité.

Comme mentionné en section 5.2.4, les sauvegardes immuables seront obligatoirement supprimées au bout de 5 ans.

5.4 Support de sauvegarde

5.4.1 Type de stockage retenu

Les serveurs de sauvegarde des sites Atlantis et Springfield reposent sur un stockage interne basé sur des SSD NVMe. L'utilisation de disques NVMe (PCIe Gen 4 minimum) garantit des performances adaptées aux exigences du plan de sauvegarde : temps d'écriture élevés pour absorber les sauvegardes nocturnes, forte capacité d'IOPS pour accélérer les restaurations, et meilleure résilience mécanique que les disques HDD traditionnels.

Les SSD de génération PCIe 5.0 ne sont pas nécessaires dans ce contexte : leur vitesse dépasse largement les limites physiques imposées par le réseau (1 à 10 Gb/s). Les modèles NVMe Gen 5 représentent donc un choix optimal en termes de performance, fiabilité et coûts.

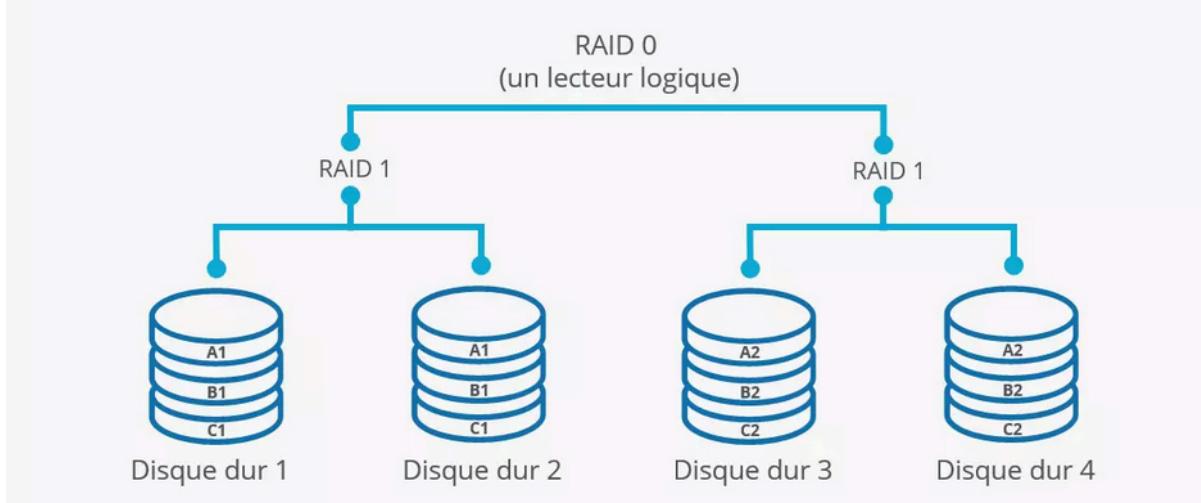
5.4.2 Choix du RAID

Un système RAID matériel est déployé sur chaque serveur de sauvegarde afin de garantir la disponibilité du stockage et la tolérance aux pannes. Le choix du niveau RAID varie selon les contraintes spécifiques de chaque site.

RAID 10 (Atlantis, site principal)

Le serveur de sauvegarde d'Atlantis utilise un RAID 10, offrant simultanément des performances élevées et une tolérance accrue aux pannes. Ce niveau RAID permet une latence très faible et des débits optimisés, essentiels pour soutenir les sauvegardes fréquentes et assurer une restauration rapide des données critiques. Malgré un ratio de capacité moins avantageux (50 % utilisable), ce choix s'impose pour respecter le RTO \leq 4 heures exigé pour l'ERP et les services sensibles.

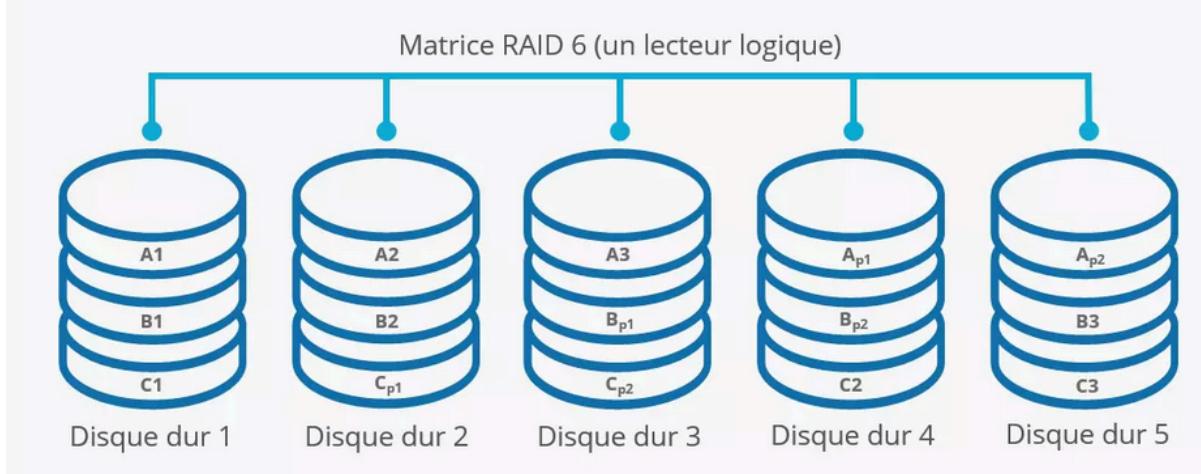
RAID 10 (Redundant Array of Independent Disks Niveau 10)



RAID 6 (Springfield, site distant)

Le serveur de Springfield est configuré en RAID 6, qui tolère la panne de deux disques tout en maximisant la capacité disponible. Ce niveau RAID est particulièrement adapté aux copies inter-sites, où la priorité est la robustesse et la capacité plutôt que les performances extrêmes. Il représente un compromis pertinent pour un site dont la charge d'écriture est plus modérée.

RAID 6 (Redundant Array of Independent Disks Niveau 6)



5.4.3 Capacité et dimensionnement

Chaque serveur de sauvegarde doit pouvoir contenir :

- l'ensemble des sauvegardes locales (rétenzione 7 jours minimum),
- la copie intersite (rétenzione 30 jours),
- les métadonnées, catalogues, journaux et snapshots éventuels.

Une réserve d'au moins **25 à 30 % d'espace libre** est recommandée pour éviter la dégradation des performances, en particulier sur des SSD.

À titre d'ordre de grandeur, le volume total de données en production chez XANADU est d'environ 1,1 To (données partagées, dossiers personnels et base ERP). En tenant compte de la politique de rétention (7 jours en local, 30 jours en intersite) et du mélange de sauvegardes complètes, différentielles et incrémentielles, le stockage de sauvegarde est dimensionné à environ quatre à cinq fois le volume de production, soit de l'ordre de 5 à 6 To utiles par site. En ajoutant une marge opérationnelle de 25 à 30 % pour absorber la croissance et éviter la dégradation des performances, on vise une capacité utile d'environ 7 à 8 To par serveur de sauvegarde.

Avec un RAID 10 sur le site principal, cela implique une capacité brute environ deux fois supérieure (par exemple 4 SSD de 4 To donnant environ 8 To utiles). Sur le site distant, un RAID 6 permet d'obtenir une capacité utile similaire avec davantage de disques (par exemple 6 SSD de 4 To offrant 16 To bruts, soit une capacité largement suffisante pour les sauvegardes locales et la copie intersite). Ces ordres de grandeur montrent que le dimensionnement retenu reste réaliste tout en laissant une marge confortable pour la croissance future.

6. Glossaire

ACL (Access Control List) : Liste de règles définissant les flux réseau autorisés ou bloqués.

AD DS (Active Directory Domain Services) : Annuaire Microsoft centralisant utilisateurs, machines, droits et authentification.

AES-256 : Algorithme de chiffrement très sécurisé utilisé pour protéger les données.

AGDLP : Modèle Microsoft d'organisation des droits : Accounts → Global Groups → Domain Local → Permissions.

Antivirus (AV) : Logiciel de sécurité détectant et supprimant les logiciels malveillants (virus, trojans, worms, etc.) via analyse de signatures, heuristique et comportements suspects.

Appliance : Équipement logiciel ou matériel dédié à une fonction précise (sécurité, sauvegarde...).

APT (Advanced Persistent Threat) : Menace informatique sophistiquée et ciblée, caractérisée par une intrusion furtive et prolongée dans un système pour exfiltrer des données sensibles ou compromettre des infrastructures critiques.

AV-TEST : Institut indépendant allemand de certification et d'évaluation des solutions de sécurité informatique (antivirus, EDR, pare-feu). Référence mondiale pour tester l'efficacité des produits de cybersécurité.

Bandé passante : Quantité maximale de données pouvant être transmise sur un réseau.

Broadcast Domain : Zone réseau où tous les appareils reçoivent les messages de diffusion.

Chiffrement : Technique garantissant la confidentialité des données en les rendant illisibles sans clé.

Cloud souverain : Infrastructure Cloud hébergée et gérée dans un pays garantissant la protection juridique nationale.

Cluster : Groupe de serveurs travaillant ensemble pour assurer continuité et performances.

Complète (Sauvegarde) : Sauvegarde intégrale de toutes les données.

DMZ (Demilitarized Zone) : Zone réseau isolée hébergeant les services accessibles depuis Internet.

DNS (Domain Name System) : Service associant un nom de domaine à une adresse IP.

Différentielle (Sauvegarde) : Sauvegarde des données modifiées depuis la dernière complète.

DHCP (Dynamic Host Configuration Protocol) : Service attribuant automatiquement des adresses IP.

DSI (Direction des Systèmes d'Information) : Service responsable du système d'information de l'entreprise.

EDR (Endpoint Detection and Response) : Solution de sécurité avancée surveillant en continu les endpoints (postes de travail, serveurs) pour détecter, analyser et répondre aux menaces en temps réel. Va au-delà de l'antivirus traditionnel en offrant analyse comportementale, forensic et réponse automatisée aux incidents.

ERP (Enterprise Resource Planning) : Logiciel de gestion intégrée (comptabilité, RH, commercial...).

Failover : Bascule automatique vers un système de secours en cas de panne.

Firewall (Pare-feu) : Système filtrant les flux réseau entrants et sortants.

FSMO (Flexible Single Master Operations)** : Rôles maîtres assurant la cohérence d'Active Directory.

GPO (Group Policy Object) : Stratégie appliquant des configurations automatiques aux postes et utilisateurs.

HTTPS (HyperText Transfer Protocol Secure) : Version sécurisée du protocole Web HTTP.

HTTP (HyperText Transfer Protocol) : Protocole utilisé pour afficher des pages Web.

Immuabilité (Sauvegarde) : Propriété d'une sauvegarde protégée contre toute modification.

Incrémentielle (Sauvegarde) : Sauvegarde des données modifiées depuis la dernière sauvegarde, quelle qu'elle soit.

IPSec (Internet Protocol Security) : Protocole chiffrant et sécurisant les communications réseau.

LAN (Local Area Network) : Réseau local interne à un site.

LDAP (Lightweight Directory Access Protocol) : Protocole d'accès aux services d'annuaire (dont AD DS).

Load Balancing : Répartition de charge entre plusieurs serveurs pour améliorer les performances.

Malware : Terme générique désignant tout logiciel malveillant conçu pour nuire, espionner ou prendre le contrôle d'un système (virus, trojans, ransomware, spyware, rootkits, etc.).

Masque de sous-réseau : Valeur définissant quelle partie de l'adresse IP représente le réseau et quelle partie représente les machines.

MPLS (Multiprotocol Label Switching) : Technologie opérateur permettant d'interconnecter plusieurs sites de manière privée et stable.

NAS (Network Attached Storage) : Serveur dédié au stockage sur le réseau.

Nginx : Serveur Web et reverse proxy performant.

NTP (Network Time Protocol) : Protocole de synchronisation de l'heure entre serveurs.

OpenEDR : Solution EDR open source permettant la détection et la réponse aux menaces sur les endpoints. Alternative libre aux EDR commerciaux.

Open Source : Logiciel dont le code source est librement accessible, modifiable et redistribuable. Permet transparence, collaboration communautaire et audit de sécurité.

OU (Organizational Unit) : Conteneur logique d'Active Directory permettant d'organiser objets et utilisateurs.

Passerelle : Adresse réseau permettant à un appareil de communiquer avec d'autres réseaux.

PDC Emulator : Rôle AD gérant les mots de passe, l'heure et certaines GPO.

Pfsense : Pare-feu open source basé sur FreeBSD.

PostgreSQL : Système de gestion de base de données relationnelle.

Proxy : Serveur filtrant les accès Internet et contrôlant la navigation.

RADIUS / NPS : Services d'authentification réseau centralisés sur Active Directory.

RAID 5 : Configuration de disques durs répartissant données et parité sur au moins 3 disques. Tolère la panne d'un disque sans perte de données tout en optimisant capacité de stockage et performances.

RAID 10 : Combinaison de RAID 1 (miroir) et RAID 0 (répartition). Nécessite au minimum 4 disques. Offre d'excellentes performances en lecture/écriture et une forte tolérance aux pannes grâce au mirroring. Priorisé pour les systèmes nécessitant rapidité et disponibilité.

RAID 6 : Variante du RAID 5 utilisant une double parité. Nécessite au minimum 4 disques et tolère la panne simultanée de deux disques. Offre une grande résilience et une capacité utile élevée, avec des performances légèrement inférieures au RAID 5.

Ransomware / Rançongiciel : Logiciel malveillant chiffrant les données pour demander une rançon.

Règle 3-2-1 (Sauvegarde) : Bonne pratique de sauvegarde : conserver 3 copies des données, sur 2 supports différents, dont 1 externalisée hors site.

RID (Relative Identifier) : Identifiant permettant de créer les SIDs des objets AD.

RPO (Recovery Point Objective) : Perte de données maximale acceptable (en durée).

RTO (Recovery Time Objective) : Temps maximal acceptable pour restaurer un service après incident.

Sauvegarde synthétique : Sauvegarde complète générée à partir d'autres sauvegardes sans relire les données source.

SI (Système d'Information) : Ensemble des ressources informatiques d'une organisation.

SIEM (Security Information and Event Management) : Plateforme centralisant et analysant les logs de sécurité.

Site-à-site (VPN) : Connexion permanente entre deux réseaux locaux d'entreprise.

SLA (Service Level Agreement) : Engagement contractuel sur la qualité de service d'un prestataire.

SGBD (Système de Gestion de Base de Données) : Logiciel gérant les bases de données.

Shadow Group : Groupe AD appliquant des droits NTFS (lecture / écriture / contrôle) sans les gérer directement sur les utilisateurs.

SID (Security Identifier) : Identifiant unique d'un utilisateur ou groupe dans Active Directory.

SPOF (Single Point of Failure) : Élément unique dont la panne interrompt un service.

Squid : Serveur proxy open source permettant le filtrage Web, la mise en cache des contenus et le contrôle d'accès Internet. Utilisé pour optimiser la bande passante et sécuriser la navigation.

SSL (Secure Sockets Layer) : Protocole de chiffrement utilisé pour sécuriser les communications.

Switch : Commutateur réseau permettant de relier plusieurs appareils.

TCP/IP : Ensemble de protocoles de communication sur les réseaux.

Tierce sauvegarde : Copie supplémentaire externalisée hors des sites de l'entreprise (généralement Cloud).

Versioning : Conservation de plusieurs versions anciennes d'un fichier.

VLAN (Virtual Local Area Network) : Réseau local virtuel séparant logiquement plusieurs sous-réseaux.

VPN (Virtual Private Network) : Tunnel chiffré permettant d'accéder au réseau de l'entreprise depuis l'extérieur.

WSUS (Windows Server Update Services) : Serveur interne distribuant les mises à jour Windows.

Wazuh : Plateforme de sécurité détectant intrusions, vulnérabilités et anomalies.

XDR (Extended Detection and Response) : Évolution de l'EDR intégrant la surveillance et la corrélation de multiples couches de sécurité (endpoints, réseau, cloud, emails, applications). Offre une vision unifiée des menaces et une réponse coordonnée sur l'ensemble de l'infrastructure.

Zabbix : Logiciel de supervision surveillant serveurs, services et équipements réseau.

7. Annexes

Annexe 1 :

Equipements / Services	VLAN 10 (CGF)	VLAN 20 (Comm)	VLAN 30 (BDE)	VLAN 40 (JURIDIQUE)	VLAN 50 (RH)	VLAN 60 (DIRECTION)	VLAN 70 (INFORMATIQUE)	VLAN 80 (LABO)	VLAN 99 (MGMT)	VLAN 100 (SRV)	IMP 1	IMP 2	Internet
VLAN 10 (CGF)	ICMP									DNS(53), LDAPS(636)	Oui	Oui	Oui
VLAN 20 (Comm)		ICMP								DNS(53), LDAPS(636)	Oui	Oui	Oui
VLAN 30 (BDE)			ICMP							DNS(53), LDAPS(636)	Oui	Oui	Oui
VLAN 40 (JURIDIQUE)				ICMP						DNS(53), LDAPS(636)	Oui	Oui	Oui
VLAN 50 (RH)					ICMP					DNS(53), LDAPS(636)	Oui	Oui	Oui
VLAN 60 (DIRECTION)						ICMP				DNS(53), LDAPS(636)	Oui	Oui	Oui
VLAN 70							ICMP			DNS(53),	Oui	Oui	Oui

(INFORMATIQUE)									LDAPS(636)			
VLAN 80 (LABO)								ICMP		DNS(53), LDAPS(636)	Oui	Oui
VLAN 99 (MGMT)									ICMP	DNS(53), LDAPS(636)		
VLAN 100 (SRV ATLANTIS)	DNS(53), LDAPS(636)	LDAPS(636)										
VLAN 110 (SRV SPRINGFIELD)	DNS(53), LDAPS(636)	LDAPS(636)										
IMP 1	Oui											
IMP 2	Oui											
Internet	Oui											

Annexe 2

