Livrable 1

Projet : Sécurité et administration

Maxime STOFFEL, Youcef AFANE, Vincent CAUSSE, Romain TOUZÉ et Thaïs VIANES

Sommaire

Préambule *4*

Rappel du contexte **4**

Rappel des attentes du client **5**

Objectifs du livrable 1 ..... **8**

Infrastructure et cartographie *9*

1. Un schéma du SI, plan d'adressage TCP/IP **9**

1.1 Cloisonnement réseau et VLAN 10
1.2 Sécurisation périmétrique : Firewall, DMZ et VPN 11
1.3 Serveur Contrôleur de Domaine (DC) 11
1.4 Infrastructure de virtualisation et ERP 11
1.5 NAS et gestion des données 12
1.6 Site de Springfield 13
1.7 Plan d'adressage 13

2. Un schéma logique du service Active Directory **15**

2.1 Rôles FSMO 17
2.2 Stratégies de groupes 17
2.2 Solution antivirus et supervision de la sécurité 19

Confidentialité, Intégrité, disponibilité et traçabilité *20*

1. Confidentialité **20**

2. Intégrité **20**

3. Disponibilité **21**

4. Traçabilité **21**

Plan de sauvegarde *22*

1. Pourquoi réaliser un plan de sauvegarde **22**

2. Quelle stratégie a-t-on mis en place sur le réseau de XANADU **22**

3. Plan de sauvegarde de notre entreprise **24**

3.1 Objectifs et criticité des données 24
3.2 Topologie de sauvegarde, supports et règle 3–2–1 25
3.3 Stratégie de sauvegarde et calendrier 26
3.4 Classification des données et types de sauvegardes 27
3.5 Sauvegarde immuable 28
3.6 Volumes de données 28
3.8 Conservation, supervision et traçabilité des sauvegardes 29

Conclusion : *31*

Glossaire *32*

Table des figures

Figure 1 - Caractéristique SLA 6
Figure 2 - Schema du SI 9
Figure 3 - Tableaux des accès 12
Figure 4 - Adressage d'un VLAN du site principal 13
Figure 5 - Adressage des serveurs du site principal 14
Figure 6 - Adresses du routeur du bâtiment principal 14
Figure 7 - Adressage du site secondaire (springfield) 14
Figure 8 - Schéma de l'Active Directory 15
Figure 9 - Forêt de l'AD 16
Figure 10 - Rôles FSMO 17
Figure 11 - Eléments de confidentialités 20
Figure 12 - Eléments d'Intégrité 20
Figure 13 - Eléments de Disponibilité 21
Figure 14 - Eléments de Traçabilité 21
Figure 15 - Schéma du RAID 5 23
Figure 16 - Schéma de déduplication 23
Figure 17 - Tableau de classification des données 27
Figure 18 - Tableau de type de sauvegarde en fonction de la criticité des données 27
Figure 19 - Tableau du volume total de données 28
Figure 20 – Tableau récapitulatif du plan de sauvegarde 28

Préambule

Rappel du contexte

L'entreprise XANADU va changer de locaux. Son directeur souhaite profiter du déménagement pour sécuriser et faire évoluer son système d'information, sachant qu'un nouveau bureau va ouvrir. Ce bureau sera relié à Atlantis par une liaison VPN MPLS opérateur.

Le directeur de XANADU connaît une entreprise qui vient d'être bloquée 3 semaines par un rançongiciel et il n'a pas du tout envie que la sienne vive la même chose. Il souhaite que son système informatique soit stable, fiable, sécurisé et facile à administrer.

Il fait donc appel à CESITECH pour l'aider dans cette démarche. CESITECH demande à votre équipe projet de :

1. Proposer un questionnaire de sécurité à Xanadu pour détecter les vulnérabilités et proposer des mesures correctives basées sur des axes de remédiation.
2. Travailler sur le déploiement du nouveau système informatique de Xanadu, élaborer une cartographie cible du système d'information : vue administration, infrastructure logique et physique.

Cette architecture devra respecter les bonnes pratiques en matière de sécurisation des systèmes d'information, garantir la continuité d'activité, la reprise après incident, ainsi que la traçabilité des événements. Le directeur du groupe souhaite un retour à la normale sous 4 heures pour les services critiques, et 24 heures pour les autres. Vous devez aussi proposer un plan de sauvegarde.

Rappel des attentes du client

Chaque employé doit pouvoir se connecter à distance, soit en tant qu'itinérant (par exemple, les commerciaux), soit en télétravail.

Les besoins en matière de partage de dossiers sont les suivants :

- Un dossier partagé par service, accessible uniquement aux membres du service concerné.
- Un dossier personnel centralisé pour chaque salarié, avec un quota de stockage limité et un accès via le dossier « Mes documents ».
- Le service juridique doit avoir accès aux dossiers des services client et des ressources humaines.
- La direction doit avoir accès aux dossiers de l'ensemble des services.

Dans chaque service, un correspondant informatique sera désigné et devra pouvoir :

- Créer ou modifier les comptes utilisateurs de son service ;
- Gérer les droits d'accès ;
- Intégrer de nouveaux postes de travail au domaine.

Après une première étude, les données gérées ont été classées en trois catégories selon leur criticité :

Données critiques :

- Base de données de l'ERP : contient les informations sur les clients, les contrats, etc.
- Données partagées : documents des services sinistres, juridique et de la direction.

Données importantes :

- Données partagées : documents des services client, conseil et commerce.
- Emails professionnels : correspondances internes et externes importantes.

Données moins critiques :

- Dossiers personnels des employés.

L'entreprise continuera d'utiliser :

- Son ERP, qu'elle ne compte pas changer ;
- Un copieur multifonction (impression, copie, numérisation) et une imprimante couleur ;

- Office 365, incluant la messagerie Outlook.

Le site distant est de Springfield raccordé au site principal via un L3VPN MPLS fourni par l'opérateur télécom, assurant une connectivité privée et une qualité de service garantie (SLA).

SLA

Indicateur	Valeur Garantie
Disponibilité	≥ 99,9 %
Latence intra-France	< 50 ms
Jitter	< 10 ms
Perte de paquets	< 0,1 %
MTTR	≤ 4 heures ouvrées (standard)
Garantie d'intervention	4h ouvrées / 24/7 (en option)

Figure 1 - Caractéristique SLA

Ce que votre équipe connaît de l'infrastructure actuelle de XANADU

L'ERP (type Odoo) repose sur PostgreSQL en backend et suit une architecture en trois tiers :

- Un serveur de base de données PostgreSQL ;
- Un serveur d'applications (contenant les objets métiers, le moteur de workflow, le générateur d'états, etc.) ;
- Un serveur de présentation, qui permet aux utilisateurs de se connecter via n'importe quel navigateur web (Google Chrome, Firefox, etc.).

L'ERP utilise une base de comptes utilisateurs locale, enregistrée dans une table. Parfois, plusieurs utilisateurs partagent un compte générique : par exemple, les utilisateurs du service RH utilisent le login RH:RH.

Volume des données

- Les données bureautiques partagées occupent actuellement 800 Go.
- Les dossiers personnels doivent faire environ 5 Go chacun.
- La base de données de l'ERP fait 10 Go.

Infrastructure

- Un serveur physique contrôleur de domaine, serveur DNS et DHCP sous Windows Server 2019.

- Un NAS bureautique avec des points de partage ouverts à tous, d'une capacité de 2 To.
- Un routeur/box fournissant un accès fibre et un accès internet en NAT.
- Un serveur physique ESXi hébergeant les VM de l'ERP.
- Un copieur connecté au réseau.
- Une imprimante couleur connectée au réseau.

Gestion des données

- Chaque utilisateur a ses dossiers sur son PC, d'environ 5 Go chacun.
- Chaque utilisateur est administrateur de son PC.
- Chacun effectue ses propres sauvegardes avec une clé USB.
- Les utilisateurs utilisent l'interface web de l'ERP en HTTP.
- Les utilisateurs itinérants utilisent leur messagerie Office 365 et Teams. Ils copient, avant de partir, les documents importants sur leur PC. Ils peuvent partager des documents sur leur Microsoft Drive pour communiquer avec leurs collègues, ce qui fait que parfois les documents de l'espace bureautique ne sont pas à jour.
- Les utilisateurs en télétravail n'ont pas accès à l'ERP.

Sauvegardes

Une personne connecte chaque fin de semaine un disque externe au serveur DC, sur lequel un script copie le contenu du NAS. Deux disques externes sont utilisés en alternance, une semaine sur deux.

Un script PowerShell planifié exporte chaque nuit à 23h la base de données de l'ERP vers un partage du NAS.

Un script Windows Backup sauvegarde le serveur DC une fois par semaine, le dimanche, sur le NAS (état du système).

Antivirus

L'antivirus installé sur le serveur DC est celui de Microsoft, configuré avec les paramètres par défaut.

Plusieurs PC utilisent la version gratuite d'un antivirus, avec un paramétrage par défaut laissé à la discrétion de l'utilisateur, qui est administrateur de son poste.

Mises à jour

Elles se font avec un paramétrage par défaut et ne sont pas contrôlées. Des prestataires informatiques les effectuent sur les serveurs lorsqu'ils ont l'occasion de venir pour une mise à jour de l'ERP.

Objectifs du livrable 1

Les objectifs exprimés par le client sont les suivants :

Accès distant
• Accès sécurisé pour les employés en télétravail et les commerciaux itinérants
• Accès VPN SSL pour l'ensemble des collaborateurs nécessitant une connexion externe

Gestion des données et partage des ressources
• Un dossier partagé par service, isolé des autres
• Un dossier personnel centralisé pour chaque employé
• Le service juridique peut accéder aux dossiers des services client et RH
• La direction a accès à tous les dossiers des services

Administration interne
• Désignation d'un correspondant informatique par service
• Chaque correspondant peut :
• Créer et modifier les comptes du service
• Gérer les droits d'accès
• Intégrer les postes au domaine

Catégorisation de la criticité des données
• Critiques : base ERP, dossiers juridique et direction
• Importantes : emails, documents commerciaux et client
• Faiblement critiques : dossiers personnels des employés

Contraintes techniques
• ERP existant conservé
• Copieurs et imprimantes conservés
• Office 365 maintenu
• Deux serveurs Linux sur site distant pour le laboratoire

Engagements opérateur MPLS
• Disponibilité ≥ 99,9 %
• Latence < 50 ms
• Jitter < 10 ms
• Temps moyen de réparation (MTTR) ≤ 4 h

Infrastructure et cartographie

1. Un schéma du SI, plan d'adressage TCP/IP

Le schéma fourni dans le document d'origine montre une architecture en deux zones principales :

Site Atlantis (central) :
- Serveur ESXi hébergeant les trois VM ERP
- Contrôleur de domaine Windows Server (AD, DNS, DHCP)
- NAS centralisé pour les données et sauvegardes
- Firewall NGFW gérant les flux Internet, DMZ et VPN
- Switch cœur de réseau L3
- Switchs d'accès pour postes et imprimantes

Site Springfield (laboratoire) :
- Deux serveurs Linux pour pilotage et collecte
- Postes utilisateurs reliés au réseau local
- Photocopieuse, imprimante métier
- Routeur MPLS opérateur

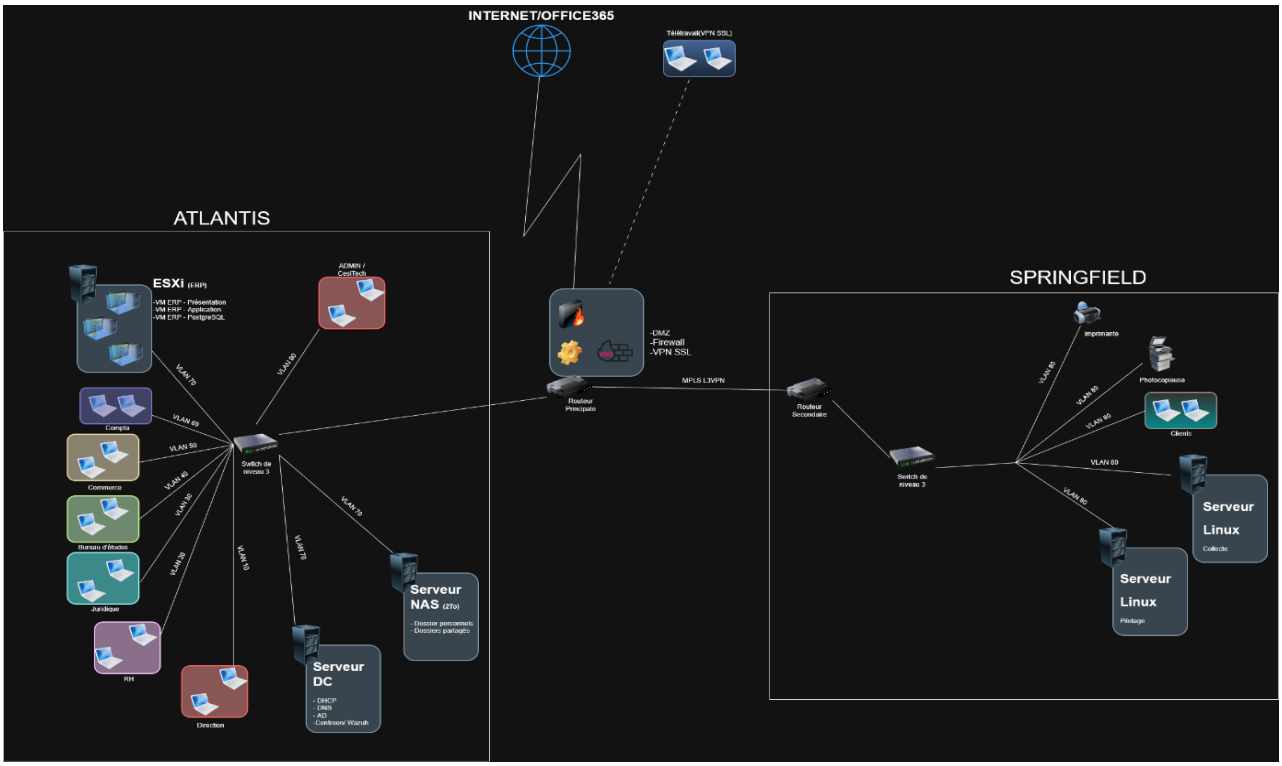


Figure 2 - Schema du SI

1.1 Cloisonnement réseau et VLAN

Nous avons mis en place un cloisonnement en VLAN afin de séparer logiquement les différents services de l'entreprise :

- VLAN Comptabilité (VLAN 60)
- VLAN Commercial (VLAN 50)
- VLAN Bureau d'étude (VLAN 40)
- VLAN Juridique (VLAN 30)
- VLAN Ressources Humaines (VLAN 20)
- VLAN Direction (VLAN 10)
- VLAN Administration (VLAN 90)
- VLAN Serveurs (VLAN 70)

Ce cloisonnement répond à plusieurs objectifs :

- **Sécurité** : chaque service est isolé et ne peut accéder aux données des autres sans autorisation explicite.
- **Confidentialité** : Chaque services bénéficient d'un isolement renforcé.
- **Administration simplifiée** : les règles de firewall inter-VLAN deviennent plus claires et maîtrisées.
- **Performance** : réduction du trafic de broadcast et meilleure organisation du réseau.

Le switch L3 assure le routage inter-VLAN avec des ACL restrictives.
Le firewall applique le filtrage entre VLAN sensibles et vers Internet.

1.2 Sécurisation périmétrique : Firewall, DMZ et VPN

Le firewall principal est au cœur de la sécurité de l'architecture du SI et va remplir plusieurs fonctions essentielles. Tout d'abord il filtre tous les flux entrants et sortant vers internet afin de protéger le réseau interne contre les accès non autorisés.

Une DMZ (zone démilitarisée) est mise en place pour héberger les services qui doivent être accessibles depuis l'extérieur évitant d'exposer directement le réseau interne. Elle constitue une zone tampon assurant la protection du cœur du SI. Le pare-feu filtre strictement les flux Internet vers la DMZ, ainsi que les flux DMZ vers LAN. Aucun des flux directs entre Internet et LAN n'est autorisé.

La DMZ héberge le serveur de présentation de l'ERP (interface web), accessible via le VPN SSL, ainsi que le portail VPN SSL utilisé par les collaborateurs en télétravail ou itinérants pour s'authentifier de manière sécurisée.

Enfin, les utilisateurs itinérants et les télétravailleurs se connectent via un VPN SSL sécurisé, supprimant les accès non sécurisés et garantissant la confidentialité des échanges.

1.3 Serveur Contrôleur de Domaine (DC)

Le **serveur Contrôleur de Domaine (DC)** regroupe plusieurs services essentiels au fonctionnement du système d'information :

- Active Directory : Il permet de centraliser la gestion des utilisateurs, des groupes et des ordinateurs du domaine (authentifier les utilisateurs lorsqu'ils se connectent, appliquer les stratégies de groupe (GPO), gérer les droits d'accès aux dossiers partagés)
- DNS (Domaine Name System) : Le serveur DNS intégré au contrôleur de domaine utilise une zone principale AD-intégrée pour la résolution des noms (ex : erp.xanadu.local). Pour les résolutions externes, le serveur DNS n'utilise pas les Root Hints par défaut. A la place, il est configuré avec des redirecteurs DNS, pointant vers les serveurs DNS de l'opérateur internet.
- DHCP (Dynamic Host Control Protocol) : Le DHCP attribue automatiquement les adresses IP aux postes et aux équipements selon leur VLAN.
- Supervion (Centreon / Wazuh) : Ces outils surveillent en permanence l'état des serveurs, du réseau et les événements de sécurité.

1.4 Infrastructure de virtualisation et ERP

Le site Atlantis intègre un serveur ESXi qui héberge l'ERP dans une architecture en trois niveaux :

- Une machine virtuelle pour la base de données PostgreSQL,
- Une pour le serveur applicatif,
- Une pour le serveur web.

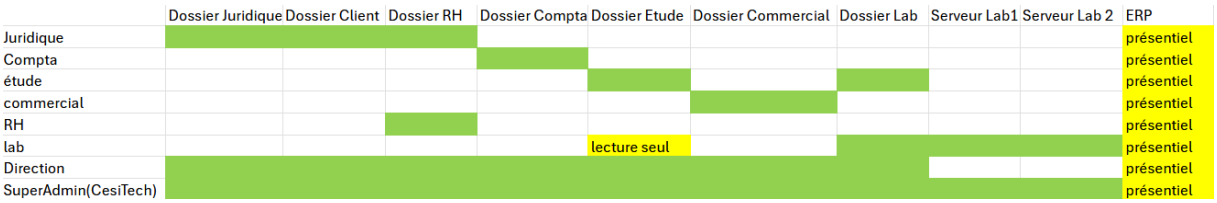
Cette architecture 3-tiers permet une meilleure performance, une maintenance facilitée et un niveau de sécurité plus élevé. L'ERP étant classé comme service critique, il est intégré à la politique de sauvegarde et doit respecter un RTO inférieur à 4 heures.

1.5 NAS et gestion des données

Le NAS est utilisé pour centraliser l'ensemble des données de l'entreprise.

Il contient :

- Les dossiers partagés par service ;
- Les dossiers personnels des utilisateurs ;
- Les exports et sauvegardes de la base de données ERP.



	Dossier Juridique	Dossier Client	Dossier RH	Dossier Compta	Dossier Etude	Dossier Commercial	Dossier Lab	Serveur Lab1	Serveur Lab 2	ERP
Juridique										présentiel
Compta										présentiel
étude										présentiel
commercial										présentiel
RH										présentiel
lab					lecture seul					présentiel
Direction										présentiel
SuperAdmin(CesiTech)										présentiel

Figure 3 - Tableaux des accès

Chaque service accède uniquement à ses dossiers, sauf exception (le service juridique peut accéder au dossier client et RH). Chaque service à un compte admin local chargé de gérer les comptes utilisateurs et les droits au sein de son service. Le service Laboratoire ne peut accéder qu'en lecture seule au dossier du Bureau d'Etude. La direction et le superAdmin disposent d'un accès global à tous les fichiers.

1.6 Site de Springfield

Le site distant de Springfield accueille 10 utilisateurs du laboratoire ainsi que deux serveurs Linux pilotant les équipements de recherche.

Le laboratoire est connecté à Atlantis via la liaison MPLS, ce qui lui garantit :

- Un accès en lecture seule au dossier du bureau d'étude,
- Un accès à l'ERP
- Tous les équipements du laboratoire (postes clients, imprimantes, serveurs Linux) sont regroupés dans un VLAN unique.

1.7 Plan d'adressage

Après avoir définis le besoin de l'entreprise et réaliser le schéma définitif du SI, il est temps de réaliser le plan d'adressage du SI. Pour l'entreprise, sur le site Atlantis nous avons fait le choix de de séparer les différents services sur des VLAN. Cette méthode permet de partitionner le réseau et d'isolé chaque services (le nombre d'hôte étaient prédéfinis) pour leur donner des droits et des accès différents.

Pour chaque service, 10 postes étaient attendus en moyenne, nous avons donc réalisé une technique VLSM (Variable Length Subnet Mask) nous permettant de créer des sous-réseaux de tailles différentes pour optimiser l'utilisation des adresses IP dans le réseau.

Cette méthode entraine par conséquent une modification du masque de sous-réseau qui est dépendant du nombre d'hôtes souhaité dans le VLAN.

L'adresse réseau et l'adresse Broadcast (de diffusion) sont la première et la dernière adresse de notre réseau. Chaque poste sera adressé en protocole DHCP (Dynamic Host Configuration Protocol).

Nom du sous-réseau	Nb. d'hôtes souhaités	Nb. d'hôtes disponibles	Nb. d'hôtes restants	Notation CIDR	Masque sous-réseau	Plage utilisable	Adresse réseau	Adresse broadcast
Service DIrection (VLAN 10)	10	16 (14 utilisables)	3	/28	255.255.255.240	192.168.1.1 - 192.168.1.14	192.168.1.0	192.168.1.15
Machine	**Adresse**	**Masque**						
PC (10)	DHCP	/28						

Figure 4 - Adressage d'un VLAN du site principal

Les serveurs seront assignés sur un VLAN isolé des autres pour garantir une meilleure sécurité.

Nom du sous-réseau	Nb. d'hôtes souhaités	Nb. d'hôtes disponibles	Nb. d'hôtes restants	Notation CIDR	Masque sous-réseau	Plage utilisable	Adresse réseau	Adresse broadcast
Service Serveurs (VLAN 70)	3	8 (6 utilisables)	2	/29	255.255.255.248	192.168.1.97 - 192.168.1.102	192.168.1.96	192.168.1.103
Machine	**Adresse**	**Masque**						
Serveur ESXi	192.168.1.97	/29						
Serveur Nas	192.168.1.98	/29						
Serveur DHCP, DNS, AD	192.168.1.99	/29						

Figure 5 - Adressage des serveurs du site principal

Le routeur du site Atlantis est également accessible via une IP, et ce pour chaque VLAN. Nous avons de manière arbitraire définis la première adresse de la plage IP utilisable pour le routeur. Dans chaque adresse du routeur, le masque est différent en fonction du VLAN.

Machine	Adresse	Masque	Vlan	Service
Routeur (Atlantis)	192.168.1.1	/28	10	Direction
	192.168.1.17	/28	20	RH
	192.168.1.34	/28	30	Juridique
	192.168.1.51	/28	40	Bureau d'étude
	192.168.1.68	/28	50	Commercial
	192.168.1.85	/28	60	Comptabilité
	192.168.1.102	/29	70	Serveur

Figure 6 - Adresses du routeur du bâtiment principal

Le laboratoire (distant) état relié à notre réseau local comme un VLAN faisant parti du même réseau, nous avons réalisé un VLAN simple, comprenant la totalité du matériel du bâtiment. Les postes de travail disposent d'un adressage dynamique (DHCP) contrairement au routeur, serveurs, l'imprimante et le scanner qui eux sont adressés en statique.

Service Laboratoire (VLAN 80)	14	32 (30 utiliables)	15	/27	255.255.255.224	192.168.1.129 - 192.168.1.158	192.168.1.128	192.168.1.159
Machine	**Adresse**	**Masque**						
PC (10)	DHCP	/27						
Imprimante	192.168.1.130	/27						
photocopieuse	192.168.1.131	/27						
Serveur de collecte	192.168.1.132	/27						
Serveur de pilotage	192.168.1.133	/27						
Routeur (lab)	192.168.1.129	/27						

Figure 7 - Adressage du site secondaire (springfield)

2. Un schéma logique du service Active Directory

L'active Directory ou AD, est un annuaire qui regroupe les informations des différents utilisateurs. On peut également répertorier les ordinateurs et les autres ressources tout en contrôlant les accès sur le réseau. Dans notre cas, on utilise l'Active Direction pour gérer les différents accès des services comme la comptabilité ou le service commerciale. On y retrouve également les comtes administrateurs qui auront plus de permissions pour gérer les comptes utilisateurs de leurs services et pourront configurer de nouveaux postes de travails.

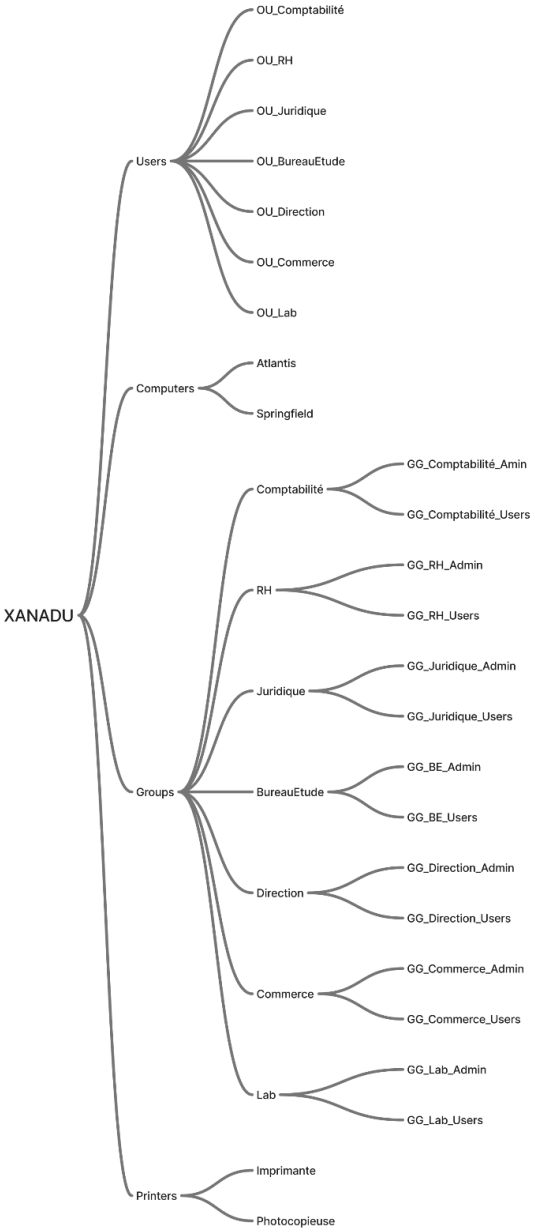


Figure 8 - Schéma de l'Active Directory

Comme le montre le schéma ci-dessus, nous avons divisés nos utilisateurs avec les services correspondant en y incluant le laboratoire. Dans la partie « Users », nous avons donc des Unités Organisationnelles (OU) pour chaque service. Cela nous permettra de savoir dans quel service un compte utilisateur se trouve. En plus de ces unités, nous avons mis en place des Groupes Globaux (GG) qui se trouvent tous dans la partie « groups ». Dans la même volonté que pour les unités organisationnelles, il y a un dossier pour chaque service avec les groupes correspondant dedans. On peut ainsi y retrouver les groupes pour les administrateurs des services qui auront accès à plus de dossier et qui pourront également gérer les autres comptes du service. Il y a également un groupe pour les utilisateurs attribués à tous les comptes utilisateurs du service pour nous permettre de mieux gérer certains droits ou fonctionnalités concernant ces comptes. En plus des comptes utilisateurs et des groupes, on retrouve également sur l'AD les appareils de Springfield comme l'imprimante ou la photocopieuse. Tous les postes que ce soit à Atlantis ou à Springfield seront présent dans l'AD et réparties dans la partie « computers » suivant leur localisation.

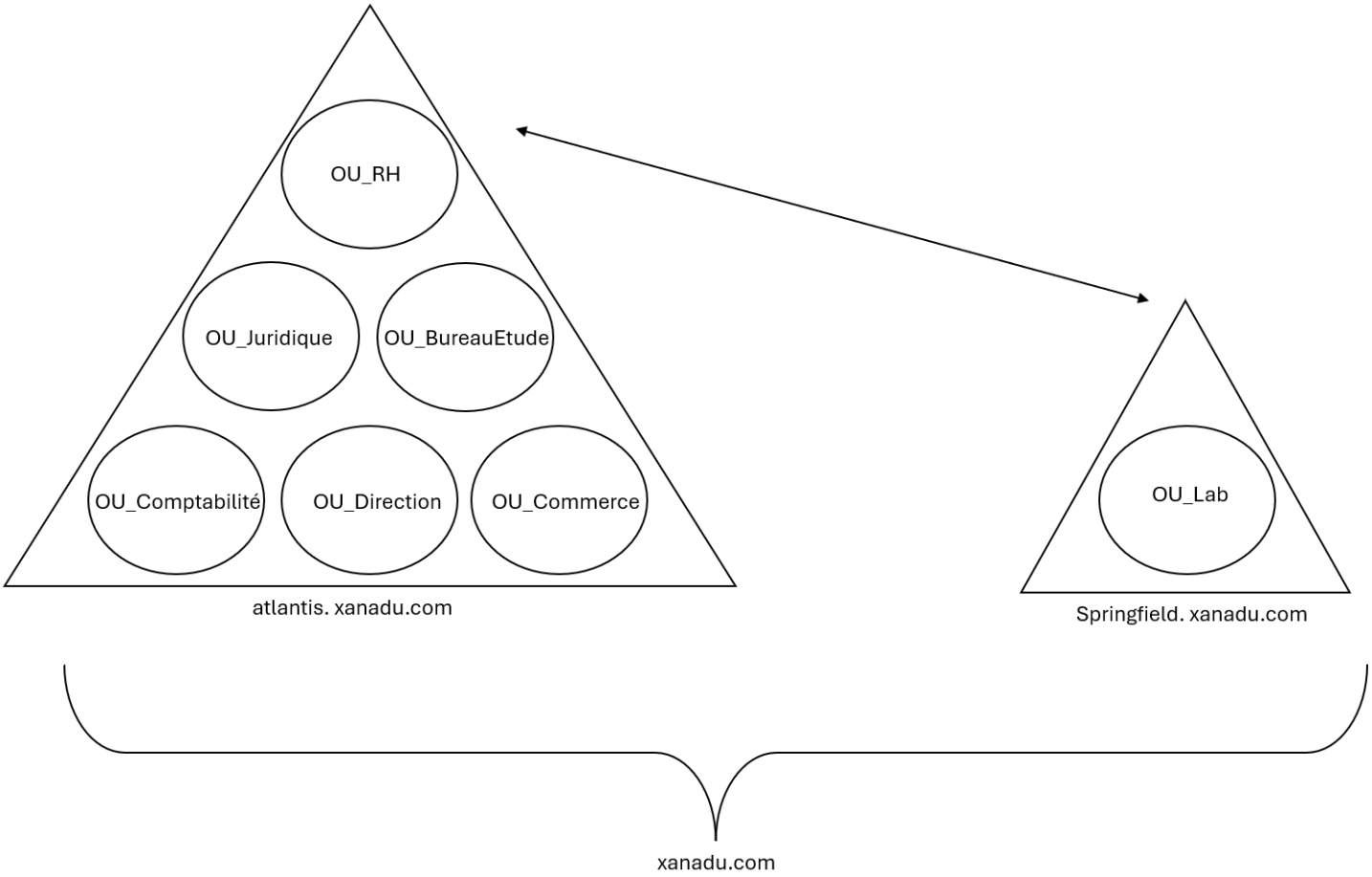


Figure 9 - Forêt de l'AD

Dans notre forêt de l'Active Directory, nous avons choisi « xanadu.com » comme domaine racine. A partir de ce domaine, nous avons deux arbres qui représentent les

deux sites que possèdent l'entreprise. D'un côté, nous avons l'arbre représentant le site principal situé à Atlantis avec le nom de domaine « atlantis.xanadu.com », héritant du nom de domaine racine. Nous pouvons ainsi retrouver les différentes OU représentant les services qui seront présent sur la technopole d'Atlantis comme la direction ou les commerciaux. De l'autre côté, nous retrouvons le site distant de Springfield avec « springfield.xanadu.com » comme nom de domaine. Le service du Laboratoire y est ainsi représenté par l'OU correspondante. Au vu du fait que les membres des deux sites peuvent communiquer les données dans les deux sens, nous avons décidé d'installer une relation bidirectionnelle entre ces deux arbres.

2.1 Rôles FSMO

Un rôle FSMO (Flexible Single Master Operation) est une responsabilité spéciale confiée à un contrôleur de domaine pour éviter les conflits dans Active Directory. Pour XANADU, nous utilisons seulement un seul serveur de contrôleur de domaine donc les 5 rôles FSMO seront concentrés sur ce même serveur.

Rôle FSMO	Description	Localisation
Schema Master	Modifier le Schéma de l'AD	Serveur DC
Domain Naming Master	Gérer les données des domaines	Serveur DC
RID Master	Attribuer des identifiants aux objets	Serveur DC
PDC Emulator	Sécuriser les authentifications	Serveur DC
Infrastructure Master	Permettre l'échange entre domaines	Serveur DC

Figure 10 - Rôles FSMO

2.2 Stratégies de groupes

Dans un Active Directory, on peut retrouver ce qu'on appelle des stratégies de groupes ou GPO (Group Policy Object). Ces stratégies sont des ensembles de paramètres permettant de configurer, sécuriser ou administrer un système d'information. Ces GPO peuvent être appliqués par utilisateurs, ordinateurs et autres objets de l'Active Directory. Pour l'entreprise XANADU, nous allons appliquer plusieurs stratégies de groupes.

Un GPO de sécurité de mot de passe sera appliquer à tous les utilisateurs. Cela permettra par exemple de garantir la sécurité du mot de passe à l'aide d'un regex sur sa taille ou des caractères obligatoires comme une majuscule ou un chiffre. Ce GPO pourra aussi offrir un changement obligatoire du mot de passe après une période définie.

Un GPO de verrouillage de compte appliqué à tous les utilisateurs et permettra également d'améliorer la sécurité d'authentification. En rajoutant des verrouillages après des connexion en échec et en rajoutant des périodes de verrouillages, les personnes voulant accéder à une session sans connaitre le mot de passe auront plus de difficultés à se connecter.

Un GPO de restriction logicielle pourra être appliqués sur tous les postes, donc « Computers » sur le schéma. Il pourra nous permettre de choisir quelles applications pourront être installés sur un poste de travail.

Un GPO de gestion de droits administrateurs servira à rendre chaque utilisateur administrateur de son propre poste de travail. Il sera donc appliqué à tous les postes de travail.

Un autre GPO pourra être mis en place pour la traçabilité des données qui sera appliqué sur tous les postes. On pourra y retrouver les logs de connexions, d'accès aux dossiers partagés ou de différentes actions sur le réseau.

Un GPO d'antivirus permettra de configurer un antivirus sur tous les postes de travails. Comme demandé, l'antivirus sera sous sa version gratuite et le paramétrage sera celui par défaut pour que l'utilisateur puisse les modifier à sa guise.

Un GPO pour Office 365 et Teams sera lui aussi sur tous les ordinateurs. Au vu du fait que les utilisateurs utiliseront Office 365 et Teams à distance ou en présentiel, cette stratégie permettra d'installer ces logiciels et de les configurer avec le mail entreprise des utilisateurs et un mot de passe par défaut qui leur sera donnée. Ils pourront ensuite modifier ce mot de passe.

Un GPO pour les dossiers partagés sera mis en place pour tous les utilisateurs. IL permettra aux utilisateurs d'accéder facilement aux données des services auquel ils ont accès et d'avoir un accès sécurisé à son dossier personnel.

En addition, Chaque service pourra avoir un GPO différent pour pouvoir gérer les accès aux différents services et à l'ERP. Ces stratégies sécuriseront les accès et lieront automatiquement les dossiers pouvant être accéder. Ils seront appliqués sur chaque groupes représentés par « Users » sur le schéma.

Pour finir, un GPO du VPN pourra être mis en place sur chaque poste de travail. Ce VPN servira aux moments où les employés travailleront en télétravail, le vpn ainsi configuré par cette stratégie leur permettra de se connecter aux dossiers partagés et à leurs données personnelles.

Cette liste de stratégie n'est pas exhaustive et de nouvelles stratégies pourront être mis en place sur les différents postes de travails, services ou utilisateurs afin d'optimiser, d'administrer et de sécuriser les données de l'entreprise.

2.2 Solution antivirus et supervision de la sécurité

En matière de protection des postes de travail de la société XANADU, nous avons retenu Microsoft Defender Antivirus, administré via la GPO. Ce choix repose sur la volonté d'utiliser une solution intégrée nativement à l'écosystème Windows, déjà présente sur l'ensemble des postes clients et sur le contrôleur de domaine tout en s'appuyant sur un antivirus moderne et en mise à jour permanente.

Un second critère du choix de Microsoft Defender Antivirus, repose sur la compatibilité entre la solution de supervision et de détection d'évènement Wazuh déployée au sein de l'infrastructure. Bien que la solution de supervision collecte et analyse les journaux de Defender, la centralisation de l'alerte de sécurité est assurée par Wazuh.

Via la GPO nous appliquons une configuration uniforme dans l'environnement : activation obligatoire de l'antivirus, mise à jour automatique des signatures, analyses planifiées, interdiction par les utilisateurs d'y faire des modifications de configuration. Ce fonctionnement de la protection antivirus couplé à l'analyse des évènements par Wazuh nous permettre une couverture de sécurité fiable et simple à administrer.

Confidentialité, Intégrité, disponibilité et traçabilité

Pour garantir un réseau fiable et sécurité, nous avons pensé à mettre en place différents techniques et logiciels.

1. Confidentialité

Dans le réseau de XANADU, il faut garantir que l'accès aux données ne se fasse seulement pour les personnes ou groupes concernés. Que ce soient les dossiers partagés des services ou un accès à l'ERP, chaque utilisateur aura des droits spécifiques. La confidentialité du réseau assure qu'aucune personne externe malintentionné ne puisse accéder à des données privées.

Elément Technique	Description	Commentaire
VPN SSL	Tunnel Chiffré pour accès distant	Chiffrement des communications entre sites et pour télétravail
Active Directory	Groupes d'utilisateurs par services	Accès aux dossiers partagés et aux dossiers personnels
Pare feu	Filtrage des flux entrant et sortants	Isolation du réseau interne d'Internet
VLAN	Segmentation du réseau par service	Isolation des flux entre les services sur le même réseau

Figure 11 - Eléments de confidentialités

2. Intégrité

Pour garantir que les données ne soient pas modifiées de manière non autorisée, nous avons des éléments techniques qui protègent le réseau.

Elément Technique	Description	Commentaire
Antivirus	Solution Antivirus de Microsoft	Protège le serveur DC contre les attaques de virus
Sauvegardes	Sauvegardes journalières sur RAID 5	Possibilité de restaurer les données précédentes
Droits Administrateurs	Utilisateurs avec des droits limités	Gère les modifications système non contrôlées

Figure 12 - Eléments d'Intégrité

3. Disponibilité

Il faut garantir l'accès aux données et aux services quand c'est nécessaire à l'entreprise XANADU. Pour cela, les éléments techniques mis en place une récupération et disponibilité des données efficaces.

Elément Technique	Description	Commentaire
RTO	Objectif de temps de reprise	Services critiques restaurés sous 4h
RAID	RAID 5 sur les données	Tolérance à la panne disque
SLA MPLS	Disponibilité 99,9%	Connectivité garantie entre les deux sites

Figure 13 - Eléments de Disponibilité

4. Traçabilité

Assurer la traçabilité du réseau permet de garantir la capacité à suivre et contrôler toutes les actions qui peuvent arriver.

Elément Technique	Description	Commentaire
ERP	Enregistrement des connexions à l'ERP	Traçabilité des opérations des différents utilisateurs
Pare feu	Logs des flux bloqués et autorisés	Traçabilité des connexions au réseaux entrant et sortant
GPO de traçabilité	Logs des connexions et d'accès aux dossiers	Traçabilité des actions utilisateurs sur l'AD

Figure 14 - Eléments de Traçabilité

Plan de sauvegarde

1. Pourquoi réaliser un plan de sauvegarde

Afin de garantir une protection des données, il est important de mettre en place un plan de sauvegarde. Nous devons organiser nos données par ordre de criticité. Décider de l'emplacement de sauvegarde, des types de sauvegarde, des délais de récupération, de la limite à nous imposer sur la bande passante…

2. Quelle stratégie a-t-on mis en place sur le réseau de XANADU

Afin de garantir la sécurité de nos données, nous avons fait les choix de types de sauvegarde suivants :

- Le système de sauvegarde immuable reposant sur la protection aux changements. Elle est donc résistante aux erreurs humaines, à la suppression volontaire (pirate) ou involontaire (erreur humaine ou technique) et au ransomware (comme le chiffrage de données). (en avoir 1 minimum est une bonne pratique). Pour réaliser cette sauvegarde, nous allons une fois par mois faire appel à une société tierce tel que Veeam pour réaliser une sauvegarde immuable de nos données sur le Cloud.

- Une partie de la sauvegarde journalière sera différentielle (seul les données critiques sont concernées) : tous les soirs, une copie de toutes les données modifiées depuis la dernière sauvegarde complète (et non depuis les incrémentaux) est réalisée. La taille augmente chaque jour mais la récupération est plus rapide, nous permettant une remise à la normale plus rapide car seul la sauvegarde du dernier dimanche et la sauvegarde de la veille du problème doivent être rétablies.

- Une partie de la sauvegarde journalière sera incrémentielle (les données importantes et moins critiques sont concernées) : tous les soirs, une copie de toutes les données modifiées depuis la dernière sauvegarde incrémentielle est réalisée. La taille augmente de manière négligeable chaque jour mais la récupération est un peu moins rapide que la sauvegarde différentielle car la sauvegarde du dernier dimanche et la sauvegarde de tous les jours jusqu'à la veille du problème doivent être rétablies.

- Nous allons programmer notre NAS en Raid 5. Le disque pourra être divisé en 4 espaces distincts. Chaque espace pourra abriter ¾ de données brutes et ¼

de parité, permettant de récupérer des données si un espace disque est corrompu ou perdu. Les données seront ainsi séparées en 4 parties différentes de manière que la récupération des données soit garanti si une partie des données est perdue.

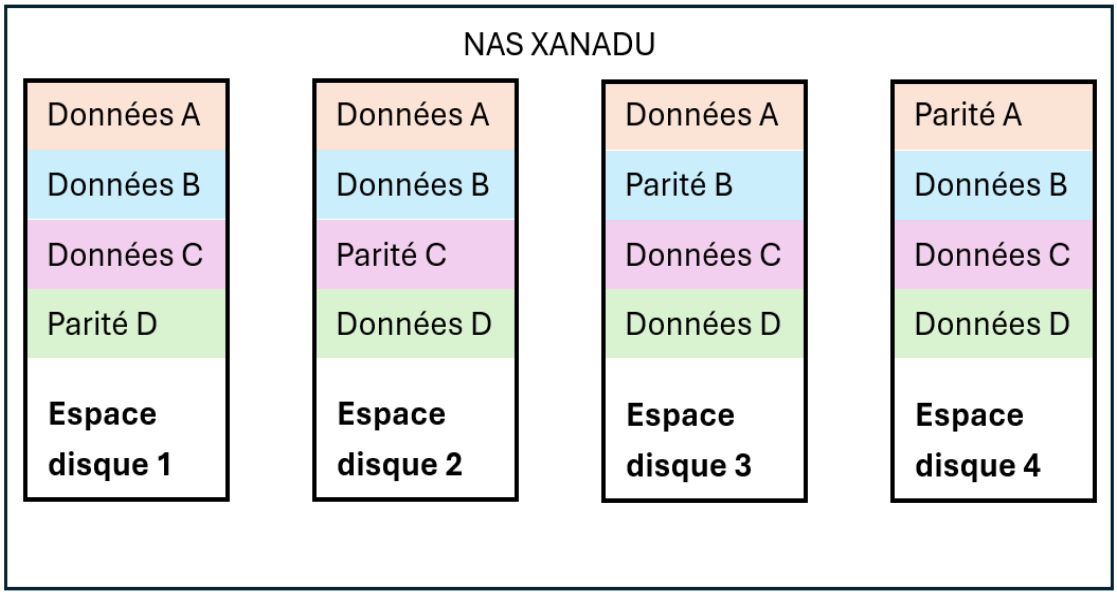


Figure 15 - Schéma du RAID 5

- Afin de favoriser la place sur notre serveur NAS interne qui fais 2 To nous allons utiliser un algorithme de déduplication. L'objectif est de trouver une correspondance entre les fichiers et de n'enregistre que les différences entre ces mêmes fichiers. Les fichiers étant des fichiers de bureau on peut compter 2pour1 au niveau de la concaténation des fichiers et 1,5pour1 pour les bases de données.

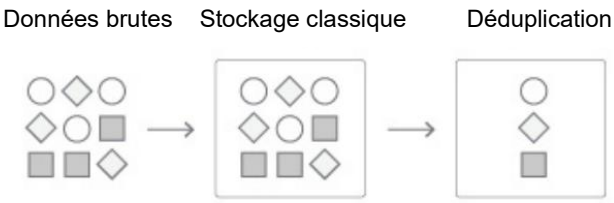


Figure 16 - Schéma de déduplication

3. Plan de sauvegarde de notre entreprise

3.1 Objectifs et criticité des données

Objectifs du plan de sauvegarde :

Afin de garantir la disponibilité et la pérennité des données de XANADU, un plan de sauvegarde structuré est mis en place.

Il décrit les objectifs, la stratégie utilisée, le calendrier hebdomadaire, les volumes, les procédures de restauration, la classification des données, les supports utilisés, la durée de rétention et les outils de supervision. Le document est rédigé de manière à être compréhensible à la fois par l'équipe informatique interne et par un prestataire externe.

Les données sont classées en trois niveaux de criticité :

- Données critiques : base de données ERP, dossiers de la Direction, du service Juridique et du service Sinistres
- Données importantes : dossiers des services Client, Commerce, Conseil, ainsi que l'ensemble des emails professionnels
- Données moins critiques : dossiers personnels des employés

Les objectifs de continuité d'activité sont les suivants :

- RTO de 4 heures pour les services critiques (ERP, direction, juridique, sinistres)
- RTO de 24 heures pour les services importants (client, commerce, conseil, messagerie)
- RPO de 24 heures pour l'ensemble des données métiers

L'intensité des sauvegardes (fréquence, type, rétention) est directement pilotée par cette classification.

3.2 Topologie de sauvegarde, supports et règle 3–2–1

Dans la nouvelle infrastructure, les rôles sont séparés :

- 2 disques de sauvegardes que l'on échange chaque semaines (utiliser comme de la sauvegarde externe)

- Un NAS de sauvegarde dédié (2 To bruts, environ 1.5 To utiles en RAID 5) utilisé uniquement pour les sauvegardes

- Une sauvegarde immuable mensuelle externalisée dans le cloud (type Veeam / S3 Glacier)

Le NAS de sauvegarde est placé dans un VLAN dédié, accessible uniquement depuis les serveurs (ERP, fichiers, DC). Il n'est pas directement accessible par les utilisateurs. Cette organisation permet de respecter la règle 3–2–1 : 3 copies des données, sur 2 supports différents, dont 1 hors site.

Cette organisation permet de respecter la règle 3–2–1 :

Afin de minimiser la surface d'attaque, en particulier face aux ransomwares :

- Le VLAN de sauvegarde est isolé des VLAN utilisateurs

- Les sauvegardes immuables cloud sont en écriture seule (WORM) et protégées contre toute modification ou suppression

- Les comptes ayant accès aux sauvegardes sont limités et appliquent le principe de moindre privilège

- Les exports ERP sont chiffrés et déposés dans un espace non accessible en écriture par les utilisateurs

3 copies des données, sur 2 supports différents, dont 1 hors site.

3.3 Stratégie de sauvegarde et calendrier

Le plan repose sur une combinaison de sauvegardes complètes, différentielles, incrémentielles, ainsi que sur une sauvegarde immuable externalisée et des snapshots fréquents de l'ERP.

Les types de sauvegarde utilisés sont les suivants :

- Sauvegarde complète : hebdomadaire
- Sauvegarde différentielle : quotidienne pour les données critiques
- Sauvegarde incrémentielle : quotidienne pour les données importantes et pour les données moins critiques
- Snapshots ERP : plusieurs fois par jour (toutes les 4 heures)
- Sauvegarde immuable : mensuelle pour les données critiques

Les sauvegardes planifiées sont réalisées en dehors des heures de production, afin de limiter l'impact sur les performances :

- Toutes les sauvegardes planifiées sont lancées à 23 h
- La plage de sauvegarde s'étend entre 23 h
- Les snapshots ERP, très peu impactant, sont réalisés en journée, toutes les 4h

Le calendrier hebdomadaire se synthétise ainsi :

- Dimanche, 23h00 : sauvegarde complète de l'ensemble des données (critiques, importantes, moins critiques) vers le NAS internet et sur un disque dur pour la sauvegarde externe des données
- Du lundi au samedi, 23h00 :
    - Sauvegarde différentielle des données critiques (base ERP, dossiers Direction/Juridique/Sinistres) vers le NAS
    - Sauvegarde incrémentielle des données importantes et non importantes avec application d'un algorithme de déduplication (dossiers Client/Commerce/Conseil, emails et dossiers personnels) vers le NAS interne
- Premier dimanche de chaque mois, 23h00 : sauvegarde immuable des données critiques vers le stockage cloud externe
- Du lundi au vendredi : snapshots ERP toutes les 4h sur le stockage local ERP

Les anciennes sauvegardes manuelles sur clé USB réalisées par les utilisateurs sont supprimées dans la nouvelle organisation. Les sauvegardes sont désormais entièrement centralisées et automatisées au niveau des serveurs.

3.4 Classification des données et types de sauvegardes

Les données sont classées selon le cahier des charges :

Catégorie de données	Contenu	Criticité
Données critiques	Base ERP, dossiers Direction, Juridique, Sinistres	Très élevée
Données importantes	Dossiers Client, Commerce, Conseil, emails professionnels	Élevée
Données moins critiques	Dossiers personnels des employés	Faible

Figure 17 - Tableau de classification des données

La stratégie de sauvegarde retenue est la suivante :

Catégorie	Type de sauvegarde	Fréquence	Justification
Données critiques	Sauvegarde complète + différentiel + snapshots ERP	Full hebdo, différentiel quotidienne, snapshots ERP plusieurs fois par jour	Activité forte, RTO 4 h
Données importantes	Sauvegarde complète + incrémentiel	Full hebdo, incrémentiel quotidiennes	Restauration simple (1 full + 1 diff)
Données moins critiques	Sauvegarde complète + incrémentielle légère	Full hebdo, incrémentielle bi-hebdomadaire	Faible criticité, optimisation de l'espace

Figure 18 - Tableau de type de sauvegarde en fonction de la criticité des données

3.5 Sauvegarde immuable

Une fois par mois, une sauvegarde immuable des données critiques est externalisée vers un stockage cloud :

- Contenu : base ERP, dossiers Direction, Juridique, Sinistres
- Périodicité : mensuelle
- Rétention : 6 mois minimum

Cette sauvegarde est en écriture seule basée sur le modèle WORM (Write Once, Read Many) et permet de se protéger des suppressions volontaires, des erreurs humaines et des rançongiciels touchant les sauvegardes locales.

3.6 Volumes de données

Les volumes suivants sont retenus comme base de calcul :

Élément	Volume
Données partagées	800 Go
Dossiers personnels (60 × 5 Go)	300 Go
Base de données ERP	10 Go

Figure 19 - Tableau du volume total de données

Nous allons considérer les valeurs suivantes :

Données	Volume total (Go)	Volume modifié par jours (Go)	Volume modifié par semaine (Go)	Commentaire	Volume total à la sauvegade (Go)	Volume dédupliqué de la sauvegade (Go)
Critique	**470**	**10**	**210**	Sauvegarde différentielle	210 par semaines et 470 par sauvegarde complète	680 Go
Base de donne de l'ERP	10					
Service Direction	115					
Service R.H.	115	10				
Service Juridique	115					
Service Compta	115					
Important	**345**	**14**	**84**	Sauvegarde incrémentielle	84 par semaines et 345+mails par sauvegarde complète	242 Go + mails
Service Commerce	115					
Service Bureau d'étude	115	5	30			
Laboratoire	115					
Email		9	54			
Non important	**300**	**10**	**60**	Sauvegarde incrémentielle	60 par semaines et 300 par sauvegarde complète	180 Go
Dossiers personnels des employés	60 x 5	10				
					Total :	1102 Go

Figure 20 – Tableau récapitulatif du plan de sauvegarde

Une solution de déduplication logicielle est activée sur les données importantes et moins critiques. On considère :

- Un ratio 2 pour 1 sur les documents bureautiques
- Pas de déduplication sur les données critiques (ERP, Direction, Juridique, Sinistres)

Le calcul des mails se fait sur l'hypothèse suivante : chaque employé reçoit en moyenne 3 mails par jour, d'un volume moyen de 0,05 Go par mail.

En prenant en compte la politique de sauvegarde et la déduplication, le volume de données stocké sur le NAS en fin de semaine est estimé à environ 1,1 To, ce qui laisse une marge d'environ 400 Go pour les mails et les données supplémentaires.

Croissance annuelle estimée des données : 20 % (environ 240 Go par an). Création nette moyenne : environ 1 Go de nouvelles données par jour ouvré. Taille moyenne d'une sauvegarde incrémentielle : environ 2 Go par jour (création + modifications).

Le NAS de sauvegarde de 2 To bruts offre environ 1,5 To utiles. Un seuil d'alerte est fixé à 80 % d'occupation, soit 1,2 To.
En tenant compte du fait que les sauvegardes occupent en moyenne 1,5 fois le volume des données primaires (combinaison de full, différentielles et incrémentielles), ce seuil sera atteint lorsque les données primaires approcheront 1,2 To. Avec une croissance de 20 % par an, cet état est atteint au bout d'environ un an. Une montée en capacité (ajout de disques ou second NAS de sauvegarde) doit donc être planifiée à moyen terme.

3.8 Conservation, supervision et traçabilité des sauvegardes

Les durées de conservation sont les suivantes :

- Sauvegardes sur NAS interne : conservées une semaine au maximum avant d'être écrasées par la sauvegarde de la semaine suivante
- Sauvegardes sur disques durs externes : conservées deux semaines, les disques étant utilisés en alternance
- Sauvegardes cloud immuables : conservées pendant au moins six mois

Un système de supervision et de traçabilité est mis en place :

- Les logs du NAS enregistrent le succès ou l'échec des tâches de sauvegarde, l'état du RAID et le taux d'occupation des volumes

- Des alertes mails automatisés sont envoyés en cas d'échec de sauvegarde, de capacité faible ou d'erreur détectée
- Centreon supervise l'état du NAS, des serveurs et des jobs de sauvegarde
- Wazuh est utilisé pour la traçabilité des accès aux données de sauvegarde et la détection de comportements suspects
- Un journal de restauration est tenu par l'équipe IT, consignant chaque opération de restauration (date, périmètre, durée, résultat)

Ce plan de sauvegarde, documenté, testé et supervisé, permet de respecter les objectifs RPO/RTO définis avec le client, de limiter l'impact d'un incident majeur et de répondre aux exigences de la grille d'évaluation en matière de documentation, de criticité, de calendrier, de minimisation de la surface d'attaque, de traçabilité et de choix des supports.

Conclusion :

Pour mettre en place la nouvelle infrastructure de XANADU, nous avons pris en considérations les différents services de l'entreprise ainsi que les différentes contraintes des dossiers partagés. Pour construire le nouveau réseau, nous avons distingué les serveurs étant présents sur le site principal d'Atlantis et le laboratoire distant de Springfield.

Avec la mise en place de VLAN, les différents services sont isolés dans le réseau et peuvent tout de même accéder aux données de l'entreprise. Le serveur DC contenant l'Active Directory, le DNS et le DHCP est gardé à Atlantis. En fonction de ce SI, nous avons pu déclarer le plan d'adressage des différents appareils et l'Active Directory. Concernant le plan de sauvegarde, nous avons opté pour du RAID 5 en prenant en compte la criticité des données. Les sauvegardes pourront suivre le plan fourni avec des description des sauvegardes par jour.

Glossaire

VPN (Virtual Private Network) : Réseau privé virtuel reliant des ordinateurs distants

MPLS (MultiProtocol Label Switching) : technique de communication sur un réseau

Rançongiciel : Logiciel bloquant l'accès aux données et demandant une rançon

ERP (Entreprise Resource Planning) : logiciel gérant les processus d'une entreprise

SLA (Service Level Agreement) : partie d'un contrat entre un prestataire informatique et son client

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

DHCP (Dynamic Host Configuration Protocol) : Protocole réseau attribuant une IP à une machine

DC (Domain Controller) : ordinateur serveur assurant l'authentification de sécurité

NAS (Network Attached Storage) : serveur de fichier stockant les données

ESXI (Elastic Sky X integrated) : Hyperviseur de type 1 déployant des ordinateurs virtuels

AD (Active Directory) : Fournit services d'identification et d'authentification des membres d'un réseau

DMZ (Delimitarized Zone) : sous réseau séparé du local et de l'internet par un pare feu

NGFW (Next Generation Firewall) : autorise et bloque les passages en fonction des politiques de pare feu

VLAN (Virtual Local Area Network) : Réseau local virtuel indépendant

Firewall : logiciel permettant d'assurer la sécurité d'un réseau

GPO (Group Policy Object) : fonctions de gestions des ordinateurs et des utilisateurs de l'Active Directory

RTO (Recovery Time Objective) : Durée maximal d'interruption admissible dans une organisation

VLSM (Variable Length Subnet Mask) : technique créant des sous-réseaux de tailles différentes

FSMO (Flexible Single Master Operation) : Types de contrôleurs de domaines dans l'Active Directory

RAID (Redundant Array of Independent Disk) : technique de virtualisation de stockage répartissant les données sur plusieurs espaces de stockages.