



Livrable 3 - Final

Projet Administration et Sécurisation
d'un Système d'Information

Entreprise XANADU

Lisa ACHOUR
Maéva CHALLIES
Enzo CADIÈRE
Rayane OULDALI
Alejandro BAGLIVO CRISTALDO

Équipe CESITECH

Année 2025-2026

Table des matières

1	Introduction	7
1.1	Présentation de l'équipe	7
1.2	Contexte du projet	7
1.3	Problématique	7
1.4	Objectifs généraux	8
2	Analyse Préalable	10
2.1	Analyse de l'existant	10
2.1.1	Architecture applicative : l'ERP	10
2.1.2	Infrastructure matérielle et réseau	10
2.1.3	Gestion des données utilisateurs	11
2.1.4	Politique de sauvegarde actuelle	11
2.1.5	Protection antivirus	12
2.1.6	Gestion des mises à jour	12
2.1.7	Synthèse des vulnérabilités critiques identifiées	13
2.2	Analyse des besoins	13
2.2.1	Besoin n°1 : Modernisation de l'infrastructure	14
2.2.2	Besoin n°2 : Centralisation et sécurisation de la gestion des données	14
2.2.3	Besoin n°3 : Professionnalisation de la stratégie de sauvegarde	15
2.2.4	Besoin n°4 : Unification et renforcement de la protection antivirus	16
2.2.5	Besoin n°5 : Centralisation et maîtrise des mises à jour	17
2.2.6	Synthèse des besoins prioritaires	17
2.3	Contraintes identifiées	18
2.3.1	Contraintes techniques et infrastructurelles	18
2.3.2	Contraintes de disponibilité et de continuité d'activité	19
2.3.3	Contraintes organisationnelles	19
2.3.4	Contraintes fonctionnelles : gestion des accès et partages	20
2.3.5	Contraintes spécifiques au site de Springfield	21
2.3.6	Contraintes liées à l'Active Directory	21
2.3.7	Synthèse des contraintes par catégorie	22
2.4	Glossaire et définitions	22
	Glossaire	22
3	Architecture Réseau et Infrastructure	24
3.1	Fondamentaux	24
3.1.1	Définition et enjeux de l'architecture réseau	24
3.1.2	Principe de segmentation réseau (VLANs)	24

3.1.3	Justification de la segmentation pour XANADU	24
3.2	Mise en œuvre technique	25
3.2.1	Cartographie cible du système informatique	25
3.2.2	Plan d'adressage IP détaillé	25
3.2.3	Architecture des VLANs par site (Atlantis et Springfield)	26
3.2.4	Liaison inter-sites MPLS	26
3.2.5	Architecture VPN pour le télétravail	27
4	Virtualisation et Hyperviseur	28
4.1	Fondamentaux	28
4.1.1	Définition de la virtualisation	28
4.1.2	Avantages de la virtualisation pour une PME	28
4.2	Mise en œuvre technique	29
4.2.1	Inventaire des machines virtuelles par VLAN	29
4.2.2	VLAN 66 - Management de l'infrastructure	29
5	Active Directory et Gestion des Identités	30
5.1	Fondamentaux	30
5.1.1	Définition et rôle d'Active Directory	30
5.1.2	Principe du contrôleur de domaine	30
5.1.3	Enjeux de la gestion centralisée des identités	31
5.1.4	Stratégie multi-sites avec RODC	31
5.2	Mise en œuvre technique	31
5.2.1	Schéma logique de l'Active Directory	31
5.2.2	Structure de l'annuaire (OUs et groupes)	31
5.2.3	Architecture des contrôleurs de domaine (DC-01, DC-02, DC-03)	32
5.2.4	Mise en place du serveur FS-01	36
5.2.5	Types de comptes et nomenclature	40
5.2.6	Validation et tests des droits d'accès	42
5.2.7	Administration déléguée par service	45
5.2.8	Politique de mots de passe et authentification (MFA)	45
6	Stratégies de Groupe (GPO)	47
6.1	Fondamentaux	47
6.1.1	Définition des GPO	47
6.1.2	Principe de moindre privilège	47
6.1.3	Rôle des GPOs dans la sécurisation du SI	47
6.2	Mise en œuvre technique	48
6.2.1	GPO de sécurité des postes	48
6.2.2	GPO de gestion des comptes	48
6.2.3	GPO de contrôle des applications	49
6.2.4	GPO de gestion des mises à jour (WSUS)	49
6.2.5	GPO de durcissement des serveurs	49
6.2.6	GPO d'administration (redirection, mappages, VPN)	49
6.2.7	Matrice de liaison des GPOs aux OUs	50

7 Sécurité Périmétrique et Filtrage	51
7.1 Fondamentaux	51
7.1.1 Qu'est-ce qu'un pare-feu et pourquoi en avons-nous besoin ?	51
7.1.2 La défense en profondeur : ne jamais mettre tous ses œufs dans le même panier	51
7.1.3 La haute disponibilité : parce qu'on ne peut pas se permettre de tomber	52
7.1.4 Pourquoi le filtrage réseau est-il si important ?	53
7.2 Mise en œuvre technique	53
7.2.1 Notre architecture de pare-feux : un sur chaque site, doublé pour la sécurité	53
7.2.2 Comment configurer CARP : le guide étape par étape	54
7.2.3 Notre politique de filtrage : les grands principes	55
7.2.4 Les règles de filtrage détaillées pour Atlantis	56
7.2.5 Les règles de filtrage pour Springfield	61
7.2.6 Vue d'ensemble : la matrice d'autorisation inter-VLAN	64
7.2.7 La liaison MPLS entre nos deux sites : un lien sécurisé et performant	66
8 Stratégie de Sauvegarde	71
8.1 Fondamentaux	71
8.1.1 Enjeux de la continuité d'activité	71
8.1.2 Politique 3-2-1-1-0	71
8.1.3 Objectifs RTO et RPO	71
8.1.4 Protection anti-ransomware	72
8.2 Mise en œuvre technique	72
8.2.1 Choix de la solution	72
8.2.2 Infrastructure de sauvegarde	73
8.2.3 Configuration ZFS	74
8.2.4 Politique de rétention	75
8.2.5 Réplication inter-sites	76
8.2.6 Sauvegardes offline (LTO)	76
8.2.7 Analyse AMDEC	76
8.2.8 Validation RTO/RPO	76
8.2.9 Sécurité et contrôle d'accès	77
8.2.10 Monitoring CheckMK	77
8.2.11 TCO sur 5 ans	78
9 Supervision et Monitoring	79
9.1 Fondamentaux	79
9.1.1 Définition de la supervision informatique	79
9.1.2 Enjeux de la supervision proactive	79
9.1.3 Importance pour le respect des RTO	80
9.1.4 Traçabilité et audit	80
9.2 Mise en œuvre technique	81
9.2.1 Analyse de l'existant	81
9.2.2 Analyse des besoins	82
9.2.3 Présentation des solutions étudiées	84
9.2.4 Critères d'évaluation	86
9.2.5 Histogramme d'évaluation des solutions de supervision	87

9.2.6 Choix de la solution : CheckMK Raw	87
9.2.7 Architecture de supervision	88
9.2.8 Éléments supervisés par site	89
9.2.9 Système d'alerting (niveaux, destinataires, anti-saturation)	89
9.2.10 10 exemples d'événements déclencheurs	91
10 Sécurité Opérationnelle : XDR, SIEM et Gestion des Logs	94
10.1 Fondamentaux	94
10.1.1 Définition XDR (Extended Detection and Response)	94
10.1.2 Définition SIEM (Security Information and Event Management)	94
10.1.3 Importance de la centralisation des logs	94
10.1.4 Enjeux de la détection et réponse aux incidents	94
10.1.5 Principe de corrélation d'événements de sécurité	95
10.2 Mise en œuvre technique	95
10.2.1 Choix de la solution : Wazuh	95
10.2.2 Comparatif des solutions étudiées	95
10.2.3 Architecture globale de la solution	96
10.2.4 Déploiement du serveur Wazuh	96
10.2.5 Configuration du service d'indexation	96
10.2.6 Collecte et centralisation des logs	96
10.2.7 Règles de détection et alertes de sécurité	97
10.2.8 Tableaux de bord et visualisation	97
10.2.9 Cas d'usage et scénarios de détection	97
10.2.10 Politique de rétention des logs et archivage	97
10.2.11 Intégration avec la supervision (CheckMK)	97
10.2.12 Déploiement du serveur Wazuh	97
10.2.13 Configuration du service d'indexation	98
10.2.14 Collecte et centralisation des logs	98
10.2.15 Règles de détection et alertes de sécurité	98
10.2.16 Tableaux de bord et visualisation	99
10.2.17 Cas d'usage et scénarios de détection	99
10.2.18 Politique de rétention des logs et archivage	99
10.2.19 Intégration avec la supervision (CheckMK)	99
11 Automatisation et Administration	101
11.1 Fondamentaux	101
11.1.1 Importance de l'automatisation en administration système	101
11.1.2 Réduction des erreurs humaines	101
11.1.3 Gain de temps et efficacité opérationnelle	102
11.1.4 Bonnes pratiques de scripting PowerShell	102
11.2 Mise en œuvre technique	102
11.2.1 Script : Création automatisée de l'arborescence AD	103
11.2.2 Script : Création automatique des groupes	104
11.2.3 Script : Création d'utilisateurs depuis CSV	105
11.2.4 Script : Désactivation automatique des comptes inactifs	106
11.2.5 Script : Inventaire AD (export CSV)	106
11.2.6 Script : Sauvegarde des GPOs horodatée	107
11.2.7 Script : Contrôle quotidien de santé du domaine	107
11.2.8 Script : Mutation d'utilisateur vers un autre service	108

11.2.9 Script : Alerte sur expiration des mots de passe	109
11.2.10 Script : Audit des comptes à priviléges	110
12 Audit de Sécurité	111
12.1 Fondamentaux	111
12.1.1 Définition et objectifs d'un audit de sécurité	111
12.1.2 Les 8 piliers de la cybersécurité	111
12.1.3 Méthodologie d'évaluation	112
12.2 Mise en œuvre technique	112
12.2.1 Présentation du questionnaire de sécurité	112
12.2.2 Analyse par thématique	113
12.2.3 Axes de remédiation identifiés	114
12.2.4 Plan d'actions correctif	114
13 Garanties DICT	115
13.1 Fondamentaux	115
13.1.1 Définition des principes DICT	115
13.1.2 Importance pour un SI d'entreprise	115
13.2 Éléments techniques garantissant le DICT	116
13.2.1 Confidentialité	116
13.2.2 Intégrité	116
13.2.3 Disponibilité	116
13.2.4 Traçabilité	116
14 Estimations Budgétaires	117
14.1 Coûts matériels	117
14.1.1 Infrastructure serveurs et virtualisation	117
14.1.2 Équipements réseau et sécurité	118
14.1.3 Liaison MPLS inter-sites	118
14.1.4 Postes de travail et périphériques	119
14.1.5 Récapitulatif des coûts matériels	119
14.2 Coûts logiciels et licences	119
14.2.1 Licences Microsoft	119
14.2.2 Licences de virtualisation	119
14.2.3 Solutions open source (gratuites)	119
14.2.4 Logiciels complémentaires et outils	120
14.2.5 Récapitulatif des coûts logiciels et licences	120
14.3 Coûts de mise en œuvre	120
14.3.1 Prestations d'installation et de configuration	120
14.3.2 Tests, validation et documentation	120
14.3.3 Formation des équipes	120
14.3.4 Gestion de projet et accompagnement	120
14.3.5 Récapitulatif des coûts de mise en œuvre	121
14.4 Coût total estimé	121
14.4.1 Investissement initial	121
14.4.2 Coûts récurrents annuels	121
14.4.3 Coût total de possession (TCO) sur 5 ans	121
14.4.4 Analyse et justification de l'investissement	121
14.4.5 Comparaison avec des solutions alternatives	122

14.4.6 Synthèse exécutive	123
15 Conclusion	127
15.1 Synthèse des apports du nouveau SI	127
15.2 Bénéfices attendus pour XANADU	127
15.3 Conformité aux exigences du cahier des charges	127
15.4 Perspectives d'évolution	128

Chapitre 1

Introduction

1.1 Présentation de l'équipe

- Lisa ACHOUR : **Secrétaire**
- Maéva CHALLIES : **Cheffe de projet / Scribe**
- Enzo CADIÈRE : **Directeur technique**
- Rayane OULDALI : **Groupe**
- Alejandro BAGLIVO : **Gestionnaire du temps**

1.2 Contexte du projet

L'entreprise XANADU change de locaux. Ils souhaitent en profiter pour faire évoluer et sécuriser leur système informatique afin d'éviter un éventuel blocage de longue durée en cas d'incident, tel que produit dans une autre entreprise. Ainsi, l'entreprise possèdera deux sites : le premier se situera dans la métropole d'**Atlantis** et le second dans la ville de **Springfield**.

Le but est d'éviter les risques d'attaque par rançongiciel et autres tout en optimisant les performances du système informatique.

Nous sommes membre de l'équipe **CesiTech** et XANADU fait appel à notre équipe pour réaliser la refonte de l'organisation de la structure réseau de l'entreprise pour répondre à leur demande. Cette démarche passe par un questionnaire de sécurité afin de détecter les vulnérabilités ainsi qu'un déploiement du nouveau système informatique.

1.3 Problématique

Comment mettre en place une infrastructure sécurisée, fiable et performante respectant les bonnes pratiques de l'entreprise, tout en garantissant la souveraineté des données et en renforçant nos chances de remporter l'appel d'offre ?

1.4 Objectifs généraux

Le projet de refonte du système d'information de XANADU s'articule autour de quatre axes stratégiques majeurs, déclinés en objectifs opérationnels concrets et mesurables.

Axe 1 : Sécurisation du système d'information

La principale préoccupation de la direction de XANADU concerne la protection contre les cyberattaques, notamment les rançongiciels. Les objectifs de sécurité sont les suivants :

- **Protéger l'infrastructure contre les rançongiciels** : mettre en place une architecture résiliente capable de résister aux attaques par chiffrement et de garantir la récupération des données en toute circonstance
- **Renforcer la sécurité périphérique** : déployer une solution de pare-feu redondante avec filtrage avancé pour contrôler l'ensemble des flux entrants et sortants
- **Appliquer le principe du moindre privilège** : éliminer les droits administrateurs généralisés actuels et mettre en place une gestion fine des droits d'accès basée sur les besoins métiers
- **Centraliser la gestion de la sécurité** : déployer des solutions d'administration centralisée (Active Directory, GPO, antivirus) pour garantir une politique de sécurité homogène et maîtrisée
- **Assurer la traçabilité** : mettre en place des systèmes de supervision et de journalisation permettant de détecter les incidents et de reconstituer leur déroulement

Axe 2 : Garantie de la continuité d'activité

XANADU souhaite éviter tout blocage prolongé de son activité en cas d'incident. Les objectifs liés à la disponibilité sont :

- **Respecter les objectifs de reprise (RTO)** : garantir un retour à la normale sous 4 heures maximum pour les services critiques (ERP, Active Directory) et sous 24 heures pour les autres services
- **Minimiser la perte de données (RPO)** : limiter la perte de données à 1 heure maximum pour les services critiques et 4 heures pour les services importants
- **Mettre en place la redondance** : éliminer les points de défaillance uniques en déployant une architecture hautement disponible (contrôleurs de domaine multiples, pare-feux redondants, réPLICATION inter-sites)
- **Automatiser les sauvegardes** : remplacer les sauvegardes manuelles actuelles par une solution professionnelle automatisée avec vérification et alertes
- **Externaliser les sauvegardes critiques** : appliquer la règle 3-2-1-1-0 avec au minimum une copie externalisée et une copie immuable hors ligne

Axe 3 : Optimisation et modernisation de l'infrastructure

Au-delà de la sécurité, XANADU souhaite disposer d'une infrastructure moderne et performante :

- **Virtualiser l'infrastructure** : migrer vers une architecture virtualisée permettant une meilleure utilisation des ressources, une flexibilité accrue et une gestion simplifiée

- **Segmenter le réseau** : implémenter une segmentation VLAN pour isoler les différents types de flux (administration, applications, utilisateurs, sauvegardes, DMZ, imprimantes, management)
- **Centraliser le stockage** : déployer un serveur de fichiers centralisé avec gestion des quotas, des versions et des droits d'accès par service, en remplacement des stockages locaux anarchiques actuels
- **Automatiser l'administration** : mettre en place des scripts PowerShell pour automatiser les tâches récurrentes et réduire les erreurs humaines
- **Superviser proactivement** : déployer une solution de monitoring permettant de détecter les problèmes avant qu'ils n'impactent les utilisateurs

Axe 4 : Support de l'organisation multi-sites et du télétravail

Le déménagement de XANADU s'accompagne d'une nouvelle organisation géographique qui doit être pleinement supportée :

- **Interconnecter les sites de manière fiable** : exploiter la liaison MPLS pour garantir une connectivité sécurisée et performante entre Atlantis (50 collaborateurs) et Springfield (10 collaborateurs du laboratoire)
- **Assurer la réPLICATION DES DONNÉES CRITIQUES** : synchroniser les données essentielles entre les deux sites pour garantir la continuité en cas de défaillance d'un site
- **Permettre l'accès distant sécurisé** : déployer une solution VPN robuste pour les collaborateurs itinérants et en télétravail, avec accès à l'ensemble des ressources (ERP, partages de fichiers, imprimantes)
- **Gérer les spécificités du laboratoire** : prendre en compte les besoins particuliers du site de Springfield (serveurs Linux, équipements spécifiques, accès aux données du bureau d'études)

Indicateurs de succès du projet

La réussite du projet sera évaluée selon les critères suivants :

- Conformité des exigences du cahier des charges
- Respect des délais de reprise (RTO) lors des tests de restauration
- Absence de droits administrateurs locaux non justifiés
- Taux de disponibilité des services critiques $\geq 99,5\%$
- Sauvegardes automatisées avec vérification quotidienne et alertes opérationnelles
- Traçabilité complète des accès et modifications sur les ressources sensibles
- Satisfaction des utilisateurs concernant l'accès distant et la disponibilité des ressources
- Validation du questionnaire de sécurité avec un niveau de conformité $\geq 85\%$

L'ensemble de ces objectifs s'inscrit dans une démarche globale visant à transformer le système d'information de XANADU en une infrastructure moderne, sécurisée et résiliente, capable de supporter la croissance de l'entreprise tout en protégeant efficacement ses actifs numériques contre les menaces contemporaines.

Chapitre 2

Analyse Préalable

2.1 Analyse de l'existant

D'après les informations recueillies auprès de XANADU, nous avons pu établir un état des lieux détaillé de leur infrastructure actuelle. Cette analyse révèle une architecture relativement simple mais présentant plusieurs vulnérabilités et axes d'amélioration significatifs.

2.1.1 Architecture applicative : l'ERP

L'ERP de XANADU repose sur une architecture trois-tiers classique :

- **Couche Base de données** : PostgreSQL héberge l'ensemble des données métier de l'entreprise
- **Couche Application** : Un serveur d'application contient les objets métier et le moteur de workflow, assurant la logique métier de l'ERP
- **Couche Présentation** : Un serveur de présentation permet aux utilisateurs de se connecter via leur navigateur web

Gestion des identités de l'ERP : L'ERP s'appuie sur une base de comptes utilisateurs interne, stockée dans une table dédiée. Il est à noter que certains comptes sont partagés entre plusieurs collaborateurs, notamment via des identifiants génériques. Par exemple, l'ensemble du service RH utilise le compte unique RH:RH.

Point critique : Le partage de comptes génériques empêche toute traçabilité individuelle et constitue une vulnérabilité majeure en matière de sécurité et d'audit.

2.1.2 Infrastructure matérielle et réseau

Volumétrie des données

XANADU respecte actuellement la nomenclature suivante en termes de volumes de données :

- **Données bureautiques** : 800 Go
- **Dossiers personnels** : 5 Go maximum par utilisateur
- **Base de données ERP** : 10 Go

Équipements déployés

L'infrastructure matérielle actuelle se compose des éléments suivants :

- **Un serveur physique** : agissant à la fois comme serveur DNS et serveur DHCP, fonctionnant sous Windows Server 2019
- **Un NAS** : d'une capacité de 2 To, disposant d'une solution NAT pour l'accès externe
- **Périphériques d'impression** : un copieur multifonction et une imprimante connectés au réseau

Observation : L'absence de redondance sur le serveur physique unique constitue un point de défaillance critique (SPOF - Single Point Of Failure). Une panne de ce serveur entraînerait l'arrêt complet des services DNS et DHCP, paralysant l'ensemble du réseau.

2.1.3 Gestion des données utilisateurs

La gestion actuelle des données présente plusieurs problématiques majeures :

Stockage local anarchique

- Chaque utilisateur possède ses propres dossiers **sur son PC local**, limités à 5 Go maximum par utilisateur
- **Tous les utilisateurs disposent des droits administrateurs** sur leur poste de travail
- Les utilisateurs effectuent leurs propres sauvegardes manuellement **sur clé USB**

Problèmes de synchronisation et d'accès

- L'ERP est accessible uniquement via **HTTP** (protocole non sécurisé)
- Les utilisateurs itinérants copient les documents importants sur leur **messagerie Office 365** avant de partir
- Certains documents sont partagés via **Microsoft OneDrive** de manière non structurée
- **Les documents ne sont pas toujours à jour**, créant des incohérences et des risques d'erreur
- **Les utilisateurs en télétravail n'ont pas accès à l'ERP**

Problème majeur : L'absence de centralisation et de versioning des documents engendre des pertes de productivité, des risques d'utilisation de versions obsolètes et une impossibilité de garantir l'intégrité des données.

2.1.4 Politique de sauvegarde actuelle

XANADU dispose d'une politique de sauvegarde rudimentaire présentant de nombreuses lacunes :

Sauvegarde hebdomadaire du NAS

- **Fréquence** : Une fois par semaine (chaque vendredi)
- **Procédure** : Un technicien connecte manuellement un disque dur externe au serveur DC
- **Support** : Deux disques durs externes utilisés en alternance
- **Contenu** : Copie complète du contenu du serveur NAS

Export de la base de données ERP

Un script PowerShell planifié réalise chaque nuit, à 23h00, l'export de la base de données PostgreSQL de l'ERP vers un partage du NAS.

Sauvegarde du contrôleur de domaine

Une tâche Windows Backup assure la sauvegarde hebdomadaire du contrôleur de domaine (DC). Cette opération, effectuée chaque dimanche, inclut l'état du système et est également stockée sur le NAS.

Vulnérabilités identifiées :

- Processus manuel sujet aux erreurs et oubli
- Aucune vérification automatique de la réussite des sauvegardes
- Absence d'externalisation (les disques restent sur site)
- RPO d'une semaine inacceptable pour les données critiques
- Vulnérabilité aux ransomwares (sauvegardes sur le même réseau)
- Absence de tests de restauration

2.1.5 Protection antivirus

La protection antivirus actuelle est **hétérogène et non centralisée** :

- **Contrôleur de domaine** : protégé par Windows Defender (Microsoft Defender Antivirus) configuré avec les paramètres par défaut
- **Postes utilisateurs** : équipés de diverses versions gratuites d'antivirus
- **Configuration** : repose sur les réglages par défaut, chaque utilisateur pouvant modifier les paramètres selon ses préférences
- **Administration** : aucune console centralisée, aucune politique uniforme

Risque majeur : Les utilisateurs disposant des droits administrateurs peuvent désactiver leur antivirus, laissant leur poste et potentiellement l'ensemble du réseau vulnérable aux malwares.

2.1.6 Gestion des mises à jour

La gestion des mises à jour suit actuellement une approche **non structurée et non supervisée** :

- Les mises à jour sont appliquées selon la **configuration par défaut** de Windows Update
- **Aucune supervision centralisée** (pas de serveur WSUS)
- Les mises à jour peuvent être différées ou refusées par les utilisateurs
- Les prestataires externes effectuent ponctuellement certaines mises à jour lors de leurs interventions, notamment pendant les opérations de maintenance de l'ERP

Conséquence : L'absence de maîtrise des mises à jour expose XANADU à des failles de sécurité connues et non corrigées, augmentant considérablement la surface d'attaque.

2.1.7 Synthèse des vulnérabilités critiques identifiées

L'analyse de l'existant révèle plusieurs vulnérabilités majeures nécessitant une intervention urgente :

1. **Absence de redondance** : serveur unique, pas de haute disponibilité
2. **Droits administrateurs généralisés** : violation du principe du moindre privilège
3. **Sauvegardes manuelles et non externalisées** : risque de perte de données majeur
4. **Comptes partagés dans l'ERP** : absence totale de traçabilité
5. **Absence de segmentation réseau** : propagation facilitée des attaques
6. **Protection antivirus hétérogène** : pas de politique de sécurité uniforme
7. **Mises à jour non maîtrisées** : exposition aux vulnérabilités connues
8. **Données dispersées** : problèmes de cohérence et de versioning
9. **Pas d'accès distant sécurisé** : télétravail impossible pour l'ERP
10. **Aucune supervision** : détection tardive des incidents

Ces constats justifient pleinement la nécessité d'une refonte complète du système d'information de XANADU, avec une priorité absolue donnée à la sécurisation et à la mise en place d'une architecture résiliente.

2.2 Analyse des besoins

Suite à l'étude approfondie de l'ensemble du système d'information de XANADU, plusieurs aspects critiques ont été décelés. Cela englobe à la fois des éléments liés à l'ergonomie et des failles majeures en termes de sécurité.

Dans ce cadre, notre objectif est d'offrir une solution plus performante, en prenant en compte l'équipement déjà présent au sein de XANADU. Le but est de leur offrir un cadre de travail idéal, afin de leur permettre d'atteindre leurs objectifs dans des conditions plus fiables et sereines.

L'analyse des besoins s'articule autour de cinq axes prioritaires, chacun répondant à une problématique critique identifiée dans l'existant.

2.2.1 Besoin n°1 : Modernisation de l'infrastructure

Constat actuel

L'infrastructure actuelle repose sur un **serveur physique unique sans redondance**, créant un point de défaillance critique (SPOF). Ce serveur centralise plusieurs rôles essentiels (DNS, DHCP, contrôleur de domaine), ce qui signifie qu'une panne matérielle entraînerait l'arrêt complet de l'ensemble du système d'information.

Impact : En cas de défaillance matérielle, l'entreprise serait totalement paralysée, sans possibilité d'authentification, de résolution de noms, ni d'attribution d'adresses IP. Le RTO de 4 heures exigé par la direction serait impossible à respecter.

Besoins identifiés

Pour répondre à cette problématique, les besoins suivants ont été identifiés :

- **Virtualiser l'infrastructure** pour séparer les rôles critiques (DNS, DHCP, fichiers, ERP) sur des machines virtuelles distinctes
 - Permet l'isolation des services
 - Facilite la gestion et la maintenance
 - Optimise l'utilisation des ressources matérielles
- **Ajouter un second serveur physique** pour assurer la haute disponibilité
 - Élimination du SPOF
 - Capacité de basculement automatique en cas de panne
 - Distribution de la charge de travail
- **Déployer une solution de monitoring** pour superviser l'état des systèmes en temps réel
 - Détection proactive des incidents
 - Alertes automatiques en cas d'anomalie
 - Tableaux de bord pour la direction
- **Documenter l'architecture réseau complète**
 - Facilite les interventions de maintenance
 - Assure la continuité en cas de départ d'un collaborateur
 - Permet l'audit et la validation de la conformité

2.2.2 Besoin n°2 : Centralisation et sécurisation de la gestion des données

Constat actuel

Les données sont actuellement **dispersées sur les postes individuels** avec des **droits administrateurs généralisés**, causant de multiples problématiques :

- Problèmes de versioning (plusieurs versions d'un même document)
- Impossibilité d'accès distant à l'ERP pour les télétravailleurs
- Absence de cohérence dans les partages (OneDrive, messagerie, stockage local)
- Risque de perte de données en cas de panne d'un poste
- Aucune traçabilité des modifications

Besoins identifiés

- **Centraliser le stockage** sur un serveur de fichiers dédié avec gestion des permissions par profils et par services
 - Dossiers partagés par service avec droits d'accès adaptés
 - Dossiers personnels centralisés avec quotas définis (5 Go par utilisateur)
 - Accès transverses pour les services supports (Juridique, Direction)
- **Déployer une solution de partage collaboratif** avec gestion de versions
 - Historisation des modifications
 - Possibilité de restauration d'anciennes versions
 - Prévention des conflits de versions
- **Supprimer les droits administrateurs locaux** sur les postes utilisateurs
 - Application du principe du moindre privilège
 - Réduction drastique de la surface d'attaque
 - Empêche l'installation de logiciels malveillants
- **Mettre en place un accès distant sécurisé via VPN** pour le télétravail
 - Accès chiffré à l'ensemble des ressources internes
 - Connexion possible à l'ERP depuis l'extérieur
 - Authentification renforcée (MFA recommandée)

2.2.3 Besoin n°3 : Professionnalisation de la stratégie de sauvegarde

Constat actuel

Les sauvegardes actuelles sont **manuelles, hebdomadaires, sur deux disques locaux**, sans externalisation ni tests de restauration. Cette situation expose l'entreprise à un risque majeur de perte de données.

Risque critique : En cas de sinistre (incendie, inondation, ransomware), XANADU perdrait l'intégralité de ses données sans possibilité de récupération. Le RPO d'une semaine est totalement inacceptable pour une activité professionnelle.

Besoins identifiés

- **Automatiser les sauvegardes régulières** avec une solution professionnelle
 - Sauvegardes quotidiennes des données critiques
 - Sauvegardes triquotidiennes des données standards
 - Élimination du facteur humain (oublis, erreurs)
- **Appliquer la stratégie 3-2-1-0**
 - **3** copies minimum des données
 - **2** supports de stockage différents (disques, bandes)
 - **1** copie externalisée (hors site)
 - **1** copie offline/immuable (protection ransomware)
 - **0** erreur de vérification (intégrité garantie)

- **Protéger spécifiquement contre les ransomwares**
 - Sauvegardes immuables (impossibles à chiffrer ou supprimer)
 - Isolation réseau du système de sauvegarde (VLAN dédié)
 - Snapshots réguliers avec rétention adaptée
- **Planifier des tests de restauration trimestriels**
 - Vérification effective de la capacité de récupération
 - Calcul précis des temps de restauration (RTO)
 - Formation des équipes aux procédures de reprise
- **Mettre en place des alertes automatiques** en cas d'échec
 - Notification immédiate de l'administrateur
 - Escalade à la direction si problème persistant
 - Journalisation complète pour audit

2.2.4 Besoin n°4 : Unification et renforcement de la protection antivirus

Constat actuel

La protection antivirus actuelle est **hétérogène et non supervisée**. Les utilisateurs disposant de droits administrateurs peuvent désactiver leur antivirus, laissant le système totalement vulnérable aux malwares, ransomwares et autres menaces.

Besoins identifiés

- **Déployer une solution XDR centralisée** sur l'ensemble du parc informatique
 - Console d'administration unique
 - Visibilité complète sur tous les équipements
 - Protection homogène et garantie sur tous les postes
- **Configurer des mises à jour automatiques** des définitions virales
 - Protection constante contre les nouvelles menaces
 - Déploiement automatique sans intervention utilisateur
 - Synchronisation régulière avec les bases de signatures
- **Activer les fonctionnalités anti-ransomware avancées**
 - Détection comportementale des chiffrements suspects
 - Blocage automatique des processus malveillants
 - Isolation immédiate des postes compromis
- **Restreindre les droits** pour empêcher toute désactivation par les utilisateurs
 - Protection verrouillée par GPO
 - Impossibilité de modifier les paramètres de sécurité
 - Seuls les administrateurs système peuvent intervenir

2.2.5 Besoin n°5 : Centralisation et maîtrise des mises à jour

Constat actuel

L'absence de gestion centralisée des mises à jour expose l'infrastructure à des **failles de sécurité connues** et à des **déploiements non maîtrisés**. Les utilisateurs peuvent différer ou refuser les mises à jour critiques, laissant des vulnérabilités exploitables par les attaquants.

Exemple concret : Une vulnérabilité critique comme EternalBlue (exploitée par WannaCry) aurait pu rester non corrigée pendant des mois sur certains postes, mettant en péril l'ensemble du réseau.

Besoins identifiés

- **Implémenter un serveur WSUS** (Windows Server Update Services) pour centraliser et planifier les mises à jour
 - Contrôle total du déploiement des correctifs
 - Optimisation de la bande passante (téléchargement unique)
 - Visibilité complète sur l'état de mise à jour du parc
- **Établir une politique de déploiement progressif** avec groupe de test
 - Phase 1 : Déploiement sur un groupe pilote (5-10% du parc)
 - Phase 2 : Validation sur 48h sans incident critique
 - Phase 3 : Déploiement généralisé sur l'ensemble du parc
- **Prioriser les correctifs critiques**
 - Déploiement express pour les vulnérabilités de sécurité critiques (< 72h)
 - Déploiement standard pour les correctifs importants (< 2 semaines)
 - Planification des mises à jour fonctionnelles (mensuel)
- **Étendre la gestion aux applications tierces** et à l'ERP
 - Suivi des versions d'Office 365
 - Gestion des mises à jour de l'ERP en coordination avec l'éditeur
 - Inventaire et suivi des logiciels métiers critiques

2.2.6 Synthèse des besoins prioritaires

Le tableau suivant récapitule les besoins identifiés par ordre de criticité :

Priorité	Besoin	Impact attendu
P1	Stratégie de sauvegarde professionnelle	Garantie de continuité d'activité
P1	Suppression des droits admin + EDR centralisé	Protection anti-ransomware
P2	Virtualisation et haute disponibilité	Respect du RTO de 4h
P2	Centralisation des données	Cohérence et accessibilité
P3	Serveur WSUS	Réduction des vulnérabilités
P3	VPN sécurisé	Support du télétravail
P3	Solution de monitoring	Détection proactive

TABLE 2.1 – Priorisation des besoins identifiés

Ces besoins constituent le socle minimal pour garantir un système d'information sécurisé, fiable et conforme aux exigences de continuité d'activité exprimées par la direction de XANADU. Leur mise en œuvre est détaillée dans les chapitres suivants de ce document.

2.3 Contraintes identifiées

Dans le cadre de la refonte du système d'information de XANADU, plusieurs contraintes techniques, organisationnelles et fonctionnelles doivent être impérativement respectées. Ces contraintes constituent le cadre dans lequel notre solution doit s'inscrire et conditionnent l'ensemble des choix architecturaux.

2.3.1 Contraintes techniques et infrastructurelles

Liaison inter-sites

Le site distant de Springfield est raccordé au site principal via une **liaison MPLS** fournie par l'opérateur télécom, assurant :

- Une connectivité privée et sécurisée entre les deux sites
- Une qualité de service garantie (SLA - Service Level Agreement)
- Une bande passante dédiée pour les flux critiques

Implication : L'architecture réseau doit tirer parti de cette liaison MPLS pour assurer la réplication des données critiques, la haute disponibilité des services et l'accès transparent aux ressources entre les deux sites.

Conservation de l'ERP existant

L'ERP de l'entreprise restera inchangé. Cette contrainte implique :

- La nouvelle infrastructure doit garantir la compatibilité avec l'ERP actuel (PostgreSQL)
- L'architecture trois-tiers existante (Base de données / Application / Présentation) doit être préservée
- Les performances de l'ERP ne doivent pas être dégradées par la migration
- L'accès distant à l'ERP doit être mis en place via VPN

Équipements à conserver

L'entreprise continuera d'utiliser :

- Son **ERP actuel**, qu'elle ne souhaite pas remplacer
- Un **copieur multifonction** (impression, copie, numérisation) et une **imprimante couleur**
- **Office 365**, incluant la messagerie Outlook

2.3.2 Contraintes de disponibilité et de continuité d'activité

Objectifs de temps de reprise (RTO)

En cas d'incident, les objectifs de reprise suivants **doivent être garantis** :

Type de service	RTO maximal
Services critiques (ERP, Active Directory)	4 heures
Autres services (partages, imprimantes)	24 heures

TABLE 2.2 – Objectifs de temps de reprise imposés

Exigences générales de continuité

La solution déployée doit garantir :

- La **continuité d'activité** : minimiser les interruptions de service
- La **reprise après incident** : capacité de restauration rapide et complète
- La **traçabilité des événements** : journalisation complète des actions et incidents

2.3.3 Contraintes organisationnelles

Répartition géographique des collaborateurs

XANADU compte un effectif de **60 collaborateurs** répartis comme suit :

- **50 collaborateurs** sur le site principal d'Atlantis
- **10 collaborateurs** sur le site distant de Springfield (laboratoire de recherche)

Structure organisationnelle par services

XANADU comprend **sept services distincts** qui doivent être reflétés dans l'architecture Active Directory :

1. Service Comptabilité et Gestion financière
2. Service Commercial
3. Bureau d'Étude
4. Service Juridique
5. Service des Ressources Humaines
6. Laboratoire (site distant de Springfield)
7. Direction de l'agence

→ Cette structure doit se retrouver dans l'organisation des OUs (Organizational Units) de l'Active Directory.

2.3.4 Contraintes fonctionnelles : gestion des accès et partages

Accès distant obligatoire

Chaque employé doit pouvoir se connecter à distance, selon deux modalités :

- Mode itinérant : commerciaux et collaborateurs en déplacement professionnel
- Télétravail : accès complet aux ressources depuis le domicile

Cette contrainte nécessite le déploiement d'une solution VPN sécurisée avec authentification renforcée (MFA recommandée).

Politique de partage de dossiers

La gestion des partages de fichiers doit respecter strictement les règles suivantes :

Dossiers partagés par service

- Un dossier partagé par service
- Accessible uniquement aux membres du service concerné
- Exemples : Partage_Comptabilite, Partage_Commercial, etc.

Dossiers personnels centralisés

- Un dossier personnel pour chaque salarié
- Quota de stockage limité à 5 Go par utilisateur
- Accès via le dossier « Mes documents » (redirection de profil)
- Sauvegarde automatique dans le cadre de la stratégie globale

Accès transversaux spécifiques Deux cas particuliers d'accès transversal doivent être implémentés :

- Le service Juridique doit avoir accès aux dossiers :
 - Du service Commercial (dossiers clients)
 - Du service des Ressources Humaines
- La Direction doit avoir accès aux dossiers de l'ensemble des services

Implémentation technique : Ces accès transversaux seront gérés via des groupes de sécurité globaux (GG_) et des groupes d'accès (GA_) dans Active Directory, permettant une gestion fine et auditable des permissions.

Administration déléguée par service

Un correspondant informatique par service devra disposer des droits suivants :

- Créer ou modifier les comptes utilisateurs de son service uniquement
- Gérer les droits d'accès aux ressources partagées de son service
- Intégrer de nouveaux postes de travail au domaine Active Directory

→ Cette administration déléguée sera mise en œuvre via des permissions spécifiques au niveau des OUs concernées dans Active Directory.

2.3.5 Contraintes spécifiques au site de Springfield

Le site distant de Springfield présente des caractéristiques particulières qui doivent être prises en compte dans l'architecture :

Effectif et équipements

Springfield hébergera :

- **10 utilisateurs** du laboratoire de recherche
- **10 postes clients** dédiés à ces utilisateurs
- **2 serveurs physiques sous Linux** pour :
 - Piloter des équipements de laboratoire
 - Récupérer et traiter des données expérimentales
- **1 copieur multifonction**
- **1 imprimante métier**

Connectivité : L'ensemble de ces équipements sera connecté au réseau local du site de Springfield, segmenté en VLANs pour isoler les flux (utilisateurs, serveurs Linux, imprimantes).

Accès inter-services : Bureau d'Étude Laboratoire

Le Bureau d'Étude (Atlantis) doit avoir accès aux données du Laboratoire (Springfield).

Cette contrainte implique :

- La mise en place de partages réseau accessibles via la liaison MPLS
- Une configuration des droits d'accès permettant la lecture (et éventuellement l'écriture) des données du laboratoire par le service Bureau d'Étude
- Une bande passante suffisante pour le transfert de données potentiellement volumineuses

2.3.6 Contraintes liées à l'Active Directory

Conservation du domaine existant

XANADU utilise actuellement son propre **domaine Active Directory**, qui doit être :

- **Conservé et modernisé** (pas de création d'un nouveau domaine)
- Renforcé en termes de sécurité et de résilience
- Étendu pour supporter l'architecture multi-sites

Flexibilité pour le site distant

Le cahier des charges précise que « **le déploiement du site distant pourra se faire différemment** ».

Cela signifie que :

- L'architecture Active Directory peut être adaptée pour Springfield

- Plusieurs options sont envisageables :
 - Déploiement d'un contrôleur de domaine complet (DC)
 - Déploiement d'un contrôleur de domaine en lecture seule (RODC) - **recommandé**
 - Connexion directe au DC principal via MPLS (non recommandé)
- Le choix de l'architecture AD fait partie intégrante de notre étude et doit être justifié

2.3.7 Synthèse des contraintes par catégorie

Catégorie	Contraintes principales
Technique	Liaison MPLS, conservation ERP, Office 365
Disponibilité	RTO 4h (critique), RTO 24h (standard), traçabilité
Organisationnelle	60 utilisateurs (50+10), 7 services distincts
Accès	VPN obligatoire, partages par service, accès transverses
Administration	Délégation par service (correspondants IT)
Springfield	10 users, 2 serveurs Linux, accès Bureau d'Étude
Active Directory	Conservation domaine, flexibilité site distant

TABLE 2.3 – Récapitulatif des contraintes par catégorie

Ces contraintes constituent le cahier des charges technique et fonctionnel auquel notre solution doit répondre intégralement. Chaque décision architecturale présentée dans les chapitres suivants a été prise en tenant compte de l'ensemble de ces contraintes, tout en privilégiant les meilleures pratiques en matière de sécurité et de résilience.

2.4 Glossaire et définitions

Active Directory (AD) Service d'annuaire de Microsoft permettant de gérer de manière centralisée les identités, les droits d'accès et les ressources d'un réseau informatique.

AMDEC Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité. Méthode utilisée pour évaluer les risques et la fiabilité de la stratégie de sauvegarde de XANADU.

CARP (Common Address Redundancy Protocol) Protocole permettant la haute disponibilité des pare-feux en partageant une adresse IP virtuelle entre deux équipements redondants.

DC (Domain Controller) Serveur qui héberge les services Active Directory et assure l'authentification des utilisateurs sur le domaine.

DICT Acronyme pour Disponibilité, Intégrité, Confidentialité et Traçabilité. Ce sont les quatre piliers fondamentaux de la sécurité du SI.

DMZ (DeMilitarized Zone) Zone du réseau isolée et sécurisée destinée aux services accessibles depuis l'extérieur, comme le VPN ou l'accès distant.

ERP (Enterprise Resource Planning) Logiciel de gestion intégré utilisé par XANADU pour gérer ses processus métiers (RH, stocks, finance).

GPO (Group Policy Object) Stratégies de groupe permettant d'appliquer automatiquement des configurations de sécurité et des règles sur les postes et serveurs.

MFA (Multi-Factor Authentication) Authentification à plusieurs facteurs renforçant la sécurité en exigeant une preuve supplémentaire au simple mot de passe (ex : code sur smartphone).

MPLS (Multi-Protocol Label Switching) Technologie de liaison réseau utilisée pour interconnecter de manière performante et sécurisée les sites d'Atlantis et de Springfield.

NTFS Système de fichiers utilisé par Windows pour définir les permissions précises (lecture, écriture, modification) sur les dossiers du serveur FS-01.

Principe du moindre privilège Règle de sécurité consistant à ne donner à un utilisateur que les droits strictement nécessaires à son travail.

RODC (Read-Only Domain Controller) Contrôleur de domaine en lecture seule déployé sur le site distant de Springfield pour sécuriser l'annuaire local.

RPO (Recovery Point Objective) Durée maximale de perte de données jugée acceptable après un incident (ex : 1h pour les services critiques).

RTO (Recovery Time Objective) Durée maximale d'interruption admissible pour un service avant son rétablissement (ex : 4h).

SIEM (Wazuh) Solution de gestion des événements de sécurité permettant de centraliser et d'analyser les logs pour détecter des menaces en temps réel.

SSO (Single Sign-On) Authentification unique permettant à un utilisateur d'accéder à toutes ses ressources avec un seul identifiant (Session Windows, ERP, Fichiers).

VLAN (Virtual Local Area Network) Segmentation logique du réseau permettant d'isoler les flux (ex : isoler les sauvegardes des flux utilisateurs).

VPN (Virtual Private Network) Réseau privé virtuel permettant aux employés nomades d'accéder aux ressources internes de XANADU en toute sécurité.

WSUS (Windows Server Update Services) Service centralisé permettant de gérer et de déployer les mises à jour Windows sur l'ensemble du parc informatique.

Chapitre 3

Architecture Réseau et Infrastructure

3.1 Fondamentaux

3.1.1 Définition et enjeux de l'architecture réseau

definition : L'architecture réseau fait référence à la structure globale d'un réseau informatique, incluant la configuration physique et logique, les protocoles utilisés, la topologie du réseau et les méthodes de gestion et de mise en œuvre. Elle détermine comment les différents composants du réseau interagissent entre eux pour fournir une plateforme de communication efficace et sécurisée.

L'architecture réseau est un enjeux important du projet. La définir techniquement est essentiel pour le bon fonctionnement de XANADU

Le fondement technique du projet XANADU repose sur l'architecture réseau. Elle est déterminante pour la sécurité, l'efficacité et la capacité d'évolution du système d'information, tout en assurant la distinction des applications et le contrôle du trafic réseau.

Nous aborderons dans ce chapitre l'ensemble des solutions techniques utilisées.

3.1.2 Principe de segmentation réseau (VLANs)

Définition : Un VLAN (Virtual Local Area Network) est une segmentation logique d'un réseau local (LAN) qui permet de regrouper des équipements comme s'ils étaient sur le même réseau physique, indépendamment de leur emplacement réel. Exemple : Dans une infrastructure d'entreprise -VLAN 10 Service Backup -VLAN 20 Service Postes Utilisateurs

Créer un VLAN permet de séparer les flux et de segmenter le réseau. D'améliorer la sécurité via l'isolation.

3.1.3 Justification de la segmentation pour XANADU

La création de VLAN est nécessaire pour l'infrastructure de XANADU. Nous devons segmenter nos réseaux en plusieurs VLAN pour l'ensemble des services et fonctionnalités. Chaque site a des besoins différents. Les objectifs de la segmentation par VLAN permettent d'adapter au mieux la sécurité ainsi que l'administration des réseaux.

Ne pas segmenter le réseau pourrait avoir des conséquences critiques en termes de sécurité ou en gestion de réseau. Grâce aux VLAN nous avons une vue d'ensemble sur les différents services des VLAN de XANADU. Note importante, les différents services

(RH, Commercial...) de XANADU ne sont pas des VLANs. Ils appartiennent tous au VLAN utilisateurs la segmentation des groupes se fera via l'AD Windows Server.

3.2 Mise en œuvre technique

3.2.1 Cartographie cible du système informatique

La cartographie du système informatique est une étape essentielle. Elle permet de fournir une vue d'ensemble synthétique de l'architecture du système d'information, incluant les postes de travail, les serveurs et les périphériques tels que les imprimantes.

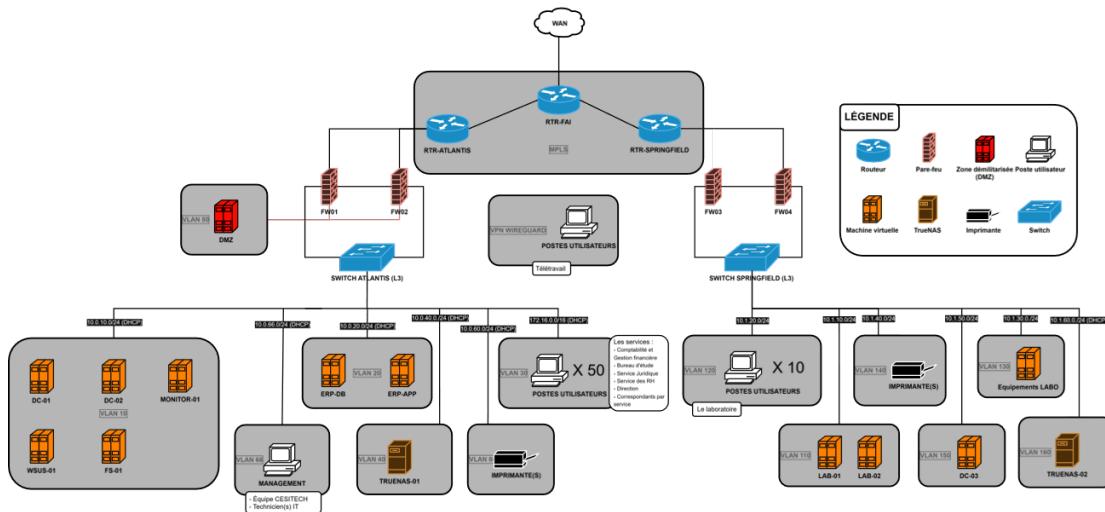


FIGURE 3.1 – Cartographie cible du système informatique

3.2.2 Plan d'adressage IP détaillé

La définition d'un plan d'adressage est nécessaire pour assurer une organisation optimale du système d'information. Elle permet de faciliter la gestion des VLANs sur les différents sites de XANADU (Springfield et Atlantis).

XANADU	Nom VLAN	Adresse IP	Masque sous réseau	Numéro VLAN
Atlantis				
	Administration	10.0.10.0/24	255.255.255.0	10
	Application	10.0.20.0/24	255.255.255.0	20
	Postes Utilisateurs	172.16.0.0/16	255.255.0.0	30
	Backup	10.0.40.0/24	255.255.255.0	40
	DMZ/VPN	10.0.50.0/24	255.255.255.0	50
	Imprimantes	10.0.60.0/24	255.255.255.0	60
	Management	10.0.66.0/25	255.255.255.0	66
Springfield				
	Supervision	10.1.10.0/24	255.255.255.0	110
	Postes Utilisateurs Labo	10.1.20.0/24	255.255.255.0	120
	Équipements Labo	10.1.30.0/24	255.255.255.0	130
	Imprimantes	10.1.40.0/24	255.255.255.0	140
	Active Directory	10.1.50.0/24	255.255.255.0	150
	AS	10.1.60.0/24	255.255.255.0	160

FIGURE 3.2 – Plan d'adressage

3.2.3 Architecture des VLANs par site (Atlantis et Springfield)

Pour plus de simplicité notre équipe a décidé de ségmenter le réseau en plusieurs VLANs

définition : Un VLAN est un domaine de broadcast logique, créé au niveau des commutateurs (switches), qui isole le trafic réseau entre groupes d'hôtes en utilisant un identifiant VLAN (VLAN ID), généralement défini par la norme IEEE 802.1Q

Nos différents VLAN s'organisent sur les différents services & fonctionnalités ainsi que le plan d'addresage de ces derniers

Site d'Atlantis

- VLAN 10 : Administration (10.0.10.0/24)
- VLAN 20 : Application (10.0.20.0/24)
- VLAN 30 : Postes Utilisateurs (172.16.0.0/16)
- VLAN 40 : Backup (10.0.40.0/24)
- VLAN 50 : DMZ/VPN (10.0.60.0/24)
- VLAN 60 : Management (10.0.66.0/24)

Site De Springfield

- VLAN 110 : Supervision (10.1.10.0/24)
- VLAN 120 : Postes Utilisateurs Labo (10.1.20.0/24)
- VLAN 130 : Équipements Labo (10.1.30.0/24)
- VLAN 140 : Imprimantes (10.1.40.0/24)
- VLAN 150 : Active Directory (10.1.50.0/24)
- VLAN 160 : Backup (10.1.60.0/24)

3.2.4 Liaison inter-sites MPLS

La connexion entre le site d'Atlantis et celui de Springfield repose sur une liaison *MPLS* (*Multi-Protocol Label Switching*). Cette liaison est dédiée aux échanges internes de l'entreprise et ne transite pas par Internet pour les flux inter-sites.

Dans les faits, ce lien permet aux deux sites de fonctionner comme un réseau étendu unique. Les utilisateurs du site de Springfield accèdent aux mêmes services que ceux d'Atlantis, notamment l'annuaire Active Directory, l'ERP et les partages de fichiers, sans configuration spécifique sur les postes de travail. Les flux liés à la réPLICATION DES DONNÉES ET AUX SAUVEGARDES INTER-SITES EMPRUNTENT ÉGALEMENT CETTE LIAISON.

Le MPLS offre une connexion plus stable qu'un VPN reposant sur Internet, avec une latence plus régulière et moins de variations, ce qui limite les impacts sur les applications sensibles. La sécurité n'est pas déportée sur la liaison elle-même : les flux inter-sites restent filtrés par les pare-feux de chaque site et la segmentation réseau par VLAN est strictement conservée.

Ce mode d'interconnexion permet ainsi de relier les deux sites de manière fiable et cohérente, tout en restant simple à administrer et adapté aux besoins actuels de l'entreprise XANADU.

3.2.5 Architecture VPN pour le télétravail

Pour permettre aux employés d'accéder au système d'information depuis l'extérieur de l'entreprise, un VPN basé sur WireGuard a été mis en place. Cette solution a été choisie parce qu'elle est simple à utiliser, offre de bonnes performances et demande peu de maintenance. Elle convient particulièrement bien aux besoins de télétravail et aux déplacements professionnels.

Chaque collaborateur se connecte à distance au réseau de l'entreprise via un VPN sécurisé depuis son poste. Une fois ce tunnel chiffré établi, il accède au réseau interne comme s'il était physiquement sur site. Il peut alors utiliser toutes les ressources dont il a besoin : l'ERP, les partages de fichiers, ainsi que les services Active Directory, sans différence notable par rapport à une connexion au bureau.

Chapitre 4

Virtualisation et Hyperviseur

4.1 Fondamentaux

4.1.1 Définition de la virtualisation

La virtualisation est une technologie qui consiste à faire fonctionner plusieurs environnements informatiques indépendants sur une même infrastructure matérielle physique. Elle repose sur l'utilisation d'un logiciel appelé **hyperviseur**, dont le rôle est de créer, gérer et isoler des machines virtuelles partageant les ressources matérielles telles que le processeur, la mémoire, le stockage et le réseau.

Chaque machine virtuelle dispose de son propre système d'exploitation et de ses applications, tout en étant isolée des autres environnements. Cette isolation permet d'exécuter différents systèmes ou services sur un même serveur physique sans interférence, tout en optimisant l'utilisation des ressources matérielles disponibles.

La virtualisation constitue aujourd'hui une composante essentielle des infrastructures informatiques modernes, aussi bien dans les centres de données que dans les environnements professionnels de taille réduite.

4.1.2 Avantages de la virtualisation pour une PME

Pour une PME, la virtualisation présente de nombreux avantages tant sur le plan technique qu'économique. Elle permet tout d'abord une **réduction des coûts** en limitant le nombre de serveurs physiques nécessaires, ce qui diminue les dépenses liées à l'achat de matériel, à la consommation électrique et à la maintenance.

La virtualisation offre également une **meilleure flexibilité** dans la gestion des systèmes. Le déploiement de nouveaux serveurs ou services est plus rapide, puisqu'il suffit de créer une nouvelle machine virtuelle sans intervention matérielle lourde. Cette souplesse facilite l'adaptation aux évolutions des besoins de l'entreprise.

En matière de **disponibilité et de continuité de service**, la virtualisation simplifie les opérations de sauvegarde, de restauration et de reprise après incident. Les machines virtuelles peuvent être sauvegardées, clonées ou restaurées plus facilement, contribuant ainsi à une meilleure résilience du système d'information.

Enfin, la virtualisation permet une **gestion centralisée** des ressources et des environnements, améliorant la supervision, la sécurité et l'administration globale de l'infrastructure informatique. Elle constitue ainsi une solution particulièrement adaptée aux PME

souhaitant disposer d'un système d'information performant, évolutif et maîtrisé.

4.2 Mise en œuvre technique

4.2.1 Inventaire des machines virtuelles par VLAN

Site d'Atlantis

VLAN	Nom	Réseau	Équipements
VLAN 10	Administration	10.0.10.0/24	DC-01, DC-02, MONITOR-01
VLAN 20	Application	10.0.20.0/24	ERP-DB, ERP-APP
VLAN 30	Postes Utilisateurs	172.16.0.0/16	50 postes répartis sur les différents groupes de l'AD (Comptabilité, Bureau d'étude...)
VLAN 40	Backup	10.0.40.0/24	TRUENAS-01
VLAN 50	DMZ/VPN	10.0.50.0/24	DMZ
VLAN 60	Imprimantes	10.0.60.0/24	Imprimantes
VLAN 66	Management	10.0.66.0/25	Équipe CESITECH, postes techniciens IT

TABLE 4.1 – Segmentation VLAN du site d'Atlantis

Site de Springfield

VLAN	Nom	Réseau	Équipements
VLAN 110	Supervision	10.1.10.0/24	LAB-01, LAB-02
VLAN 120	Postes Utilisateurs	10.1.20.0/24	10 postes utilisateurs
VLAN 130	Équipements Labo	10.1.30.0/24	Équipements laboratoire
VLAN 140	Imprimantes	10.1.40.0/24	Imprimantes
VLAN 150	Active Directory	10.1.50.0/24	DC-03
VLAN 160	AS	10.1.60.0/24	DC-04

TABLE 4.2 – Segmentation VLAN du site de Springfield

4.2.2 VLAN 66 - Management de l'infrastructure

Comme cela a été mentionné dans la section 4.2.2, le VLAN 66 est présent. L'objectif de la création du VLAN 66 était d'incorporer les équipes IT dans l'infrastructure XANADU. Ainsi, les autres services pourront solliciter le département informatique en cas de souci, grâce à un système de billetterie spécifique.

Cette option permet de regrouper la gestion des incidents, d'accroître la réactivité du service d'assistance et de garantir un suivi plus précis des requêtes. Par ailleurs, le fait de diviser le service IT dans un VLAN spécifique améliore la protection du réseau en restreignant les accès sensibles aux seuls utilisateurs autorisés, tout en rendant l'administration et la surveillance de l'infrastructure plus aisées.

Chapitre 5

Active Directory et Gestion des Identités

5.1 Fondamentaux

5.1.1 Définition et rôle d'Active Directory

Active Directory est un service d'annuaire développé par Microsoft, destiné à la gestion centralisée des ressources d'un réseau informatique. Il permet d'administrer les utilisateurs, les ordinateurs, les groupes et les politiques de sécurité au sein d'un domaine, en fournissant un cadre structuré et cohérent pour l'organisation du système d'information.

Le rôle principal d'Active Directory est de centraliser l'authentification et l'autorisation des utilisateurs et des équipements. Il permet de vérifier l'identité des utilisateurs lors de leur connexion et de contrôler l'accès aux ressources réseau en fonction des droits qui leur sont attribués. Cette centralisation facilite la gestion des accès, renforce la sécurité et simplifie l'administration des environnements informatiques.

Active Directory joue également un rôle clé dans l'application des stratégies de sécurité, notamment à travers les stratégies de groupe (GPO). Celles-ci permettent de définir et de déployer des règles de configuration, de sécurité et d'usage de manière homogène sur l'ensemble des postes et des utilisateurs du domaine.

5.1.2 Principe du contrôleur de domaine

Le contrôleur de domaine est un serveur chargé d'héberger les services **Active Directory** et d'assurer le bon fonctionnement du domaine. Il constitue le point central de l'authentification des utilisateurs et des ordinateurs, en vérifiant les identités et en autorisant ou refusant l'accès aux ressources du réseau.

Lorsqu'un utilisateur ou un poste tente de se connecter au domaine, le contrôleur de domaine assure les missions suivantes :

- **Validation** : Il vérifie les informations d'authentification ;
- **Application** : Il applique les politiques de sécurité définies ;
- **Gestion** : Il assure la gestion des objets Active Directory, tels que les comptes utilisateurs, les groupes et les unités d'organisation.

Dans un environnement professionnel, plusieurs contrôleurs de domaine peuvent être déployés afin d'assurer la **redondance** et la **disponibilité** du service. Cette réPLICATION entre contrôleurs permet de garantir la continuité de service en cas de panne et contribue à la fiabilité et à la résilience du système d'information.

5.1.3 Enjeux de la gestion centralisée des identités

La centralisation des identités via l'Active Directory est le cœur de la sécurité du système d'information de **XANADU**. Elle permet de passer d'une gestion éparpillée à une administration unifiée :

- **Réactivité** : La désactivation immédiate d'un compte suspend l'ensemble des accès au SI.
- **Expérience utilisateur** : Le principe du *Single Sign-On* (SSO) permet à l'utilisateur de n'utiliser qu'un seul mot de passe pour toutes ses ressources.
- **Efficacité administrative** : L'utilisation de groupes de sécurité automatise l'attribution des droits selon le service de l'employé.

5.1.4 Stratégie multi-sites avec RODC

Pour sécuriser le site distant (Laboratoire de Springfield), nous avons opté pour la mise en place d'un **RODC** (**Read-Only Domain Controller**). Ce choix répond à des problématiques spécifiques de sécurité et de performance :

- **Sécurité du site distant** : La base de données étant en lecture seule, une compromission physique du serveur à Springfield n'impacte pas l'intégrité de l'annuaire sur le site Atlantis.
- **Rapidité d'authentification** : Les utilisateurs se connectent sur le serveur local, évitant ainsi les lenteurs liées au lien VPN.
- **Politique de réPLICATION** : Seuls les secrets (mots de passe) des utilisateurs locaux sont stockés sur le RODC, protégeant ainsi les comptes d'administration globale.

5.2 Mise en œuvre technique

5.2.1 Schéma logique de l'Active Directory

Sur le schéma ci-dessous, est représentée l'organisation logique que nous avons choisi de mettre en place en ce qui concerne l'active directory XANADU. Celle-ci a été réfléchie de façon à ranger efficacement l'annuaire des utilisateurs selon leur fonction au sein de l'entreprise ainsi que pour administrer optimalement les droits d'accès de chacun selon les cas d'utilisation.

5.2.2 Structure de l'annuaire (OUs et groupes)

Unités organisationnelles et entités d'accès

L'annuaire de l'Active Directory permet de ranger intuitivement les entités d'accès (employé ou poste utilisateur) afin de faciliter la gestion.

Ainsi dans le cadre du domaine XANADU, la hiérarchie est la suivante : - Site (Atlantis ou Springfield) - Service, correspondant à une OU (unité organisationnelle) - Entité de l'employé

L'entité de chaque employé est accessible dans l'unité organisationnelle de son service. Nous avons classé ci-dessous la répartition des employés par service selon l'annuaire.

Répartition des utilisateurs par Unité Organisationnelle



FIGURE 5.1 – Schéma logique de l’active directory

Groupes globaux et groupes d’administrateur

Une fois, l’annuaire mis en place les employés sont rajoutés à des groupes d’accès globaux afin de définir le périmètre d’accès de chaque service.

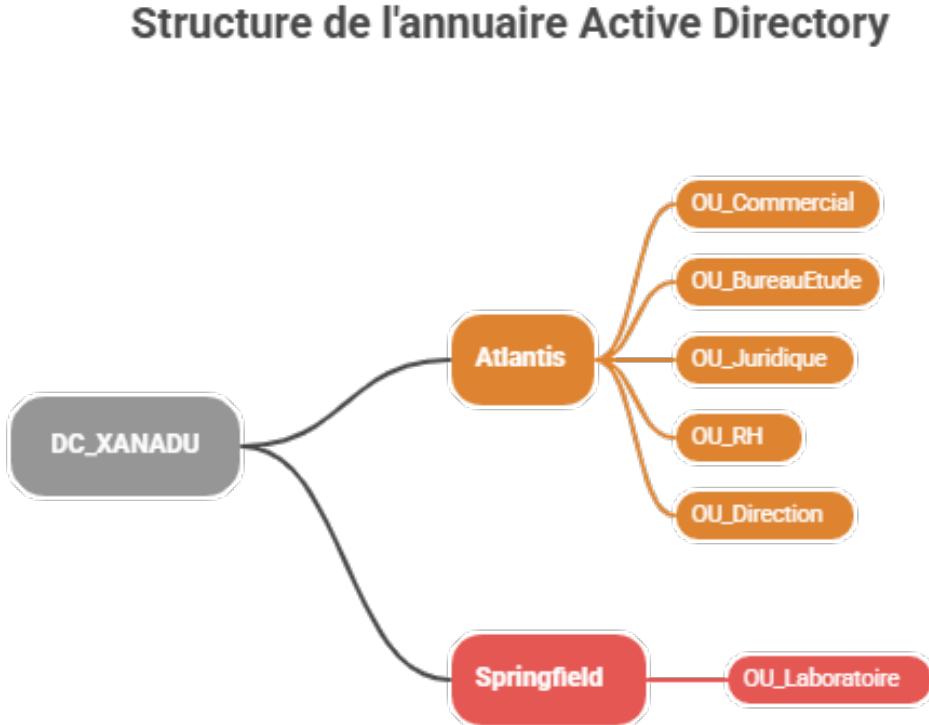
De surcroît, certains des employés font partie du groupe administrateur de leur service pour leur permettre davantage de permission dans le cadre de l’administration déléguée par service.

5.2.3 Architecture des contrôleurs de domaine (DC-01, DC-02, DC-03)

L’infrastructure Active Directory de XANADU repose sur une architecture multi-site distribuée conçue pour assurer la haute disponibilité et la résilience des services d’annuaire. Cette architecture s’articule autour de trois contrôleurs de domaine répartis sur deux sites géographiques distincts.

Architecture du site principal Atlantis Le site principal d’Atlantis héberge deux contrôleurs de domaine en configuration de haute disponibilité :

- **DC-01** : Contrôleur de domaine principal (Writable Domain Controller)



Made with Napkin

FIGURE 5.2 – Structure de l'annuaire active directory

— **DC-02** : Contrôleur de domaine secondaire (Writable Domain Controller)

Ces deux contrôleurs fonctionnent selon le modèle de réplication **multi-master**, caractéristique d'Active Directory. Contrairement à une architecture active/passive traditionnelle, les deux DCs sont simultanément opérationnels et capables de traiter des requêtes d'authentification, de modification d'objets AD et de réplication. Cette configuration offre plusieurs avantages :

- **Redondance automatique** : En cas de défaillance de DC-01, DC-02 assure instantanément la continuité de service sans intervention manuelle
- **Répartition de charge** : Les requêtes d'authentification et les opérations AD sont naturellement réparties entre les deux contrôleurs
- **Résilience des rôles FSMO** : Les rôles d'opérations à maître unique peuvent être transférés rapidement vers le DC survivant
- **Tolérance aux pannes** : La perte d'un contrôleur n'entraîne aucune interruption de service pour les utilisateurs

La réplication entre DC-01 et DC-02 s'effectue de manière bidirectionnelle et quasi-instantanée, garantissant la cohérence des données d'annuaire sur les deux serveurs.

OU_Commercial	OU_BureauEtude	OU_Juridique	OU_RH	OU_Direction
l_james	k_durant	j_embiid	a_davis	g_antetokounmpo
s_curry	n_jokic	j_tatum	d_booker	k_thompson
d_lillard	l_doncic	j_butler	k_irving	d_green
c_paul	k_leonard	j_harden	b_beal	r_westbrook
t_young	p_george	d_mitchell	b_adebayo	z_williamson
f_vanvleet	s_gilgeousalexander	d_derozan	j_brown	j_morant
l_ball	p_siakam	j_randle	b_ingram	a_edwards
j_brunson	m_bridges	o_anunoby	f_wagner	t_haliburton

TABLE 5.1 – Répartition des utilisateurs par Unité Organisationnelle (partie 1)

OU_Laboratoire
k_towns
d_sabonis
d_fox
j_jackson
p_banchero
s_barnes
c_holmgren
v_wembanyama
a_sengun
d_bane

TABLE 5.2 – Répartition des utilisateurs par Unité Organisationnelle (partie 2)

Architecture du site distant Springfield Le site de Springfield héberge un contrôleur de domaine en lecture seule :

- **DC-03** : Read-Only Domain Controller (RODC)

Cette configuration répond à la pratique recommandée par Microsoft. Le RODC présente les caractéristiques suivantes :

- **RéPLICATION UNIDIRECTIONNELLE** : DC-03 réplique les données depuis DC-01 (ou DC-02 en cas d'indisponibilité) mais ne peut pas modifier l'annuaire
- **Authentification locale** : Les utilisateurs du site Springfield s'authentifient localement auprès de DC-03, réduisant ainsi le trafic WAN
- **Sécurité renforcée** : En cas de compromission physique, aucune modification de l'AD global n'est possible depuis DC-03
- **Pas de secrets sensibles** : Par défaut, le RODC ne stocke pas tous les mots de passe utilisateurs, limitant l'exposition en cas d'attaque

Mécanisme de basculement et continuité de service Le mécanisme de basculement s'articule autour de plusieurs niveaux :

1. **Au niveau d'Atlantis** : En cas de panne de DC-01, DC-02 prend automatiquement le relais pour toutes les opérations. Les clients Windows sont configurés pour interroger les deux DCs, assurant une bascule transparente.

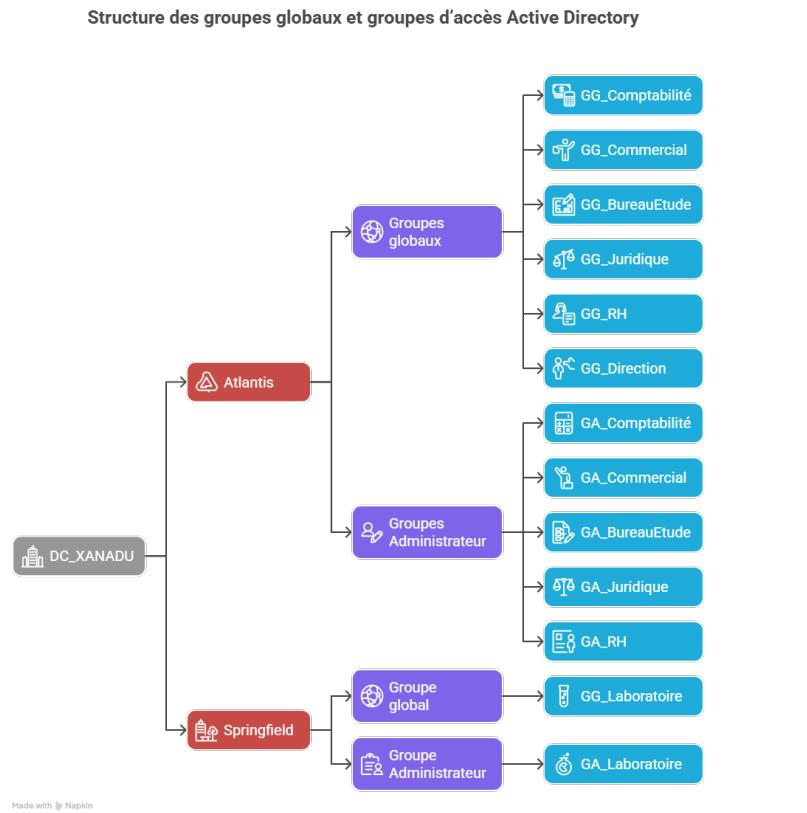


FIGURE 5.3 – Schéma logique de l'active directory

2. Pour le site Springfield : DC-03 se connecte prioritairement à DC-01 pour sa réPLICATION. Si DC-01 devient indisponible, DC-03 bascule automatiquement vers DC-02 grâce au mécanisme de découverte de sites Active Directory.
3. RéPLICATION inter-sites : La topologie de réPLICATION est configurée pour optimiser le trafic WAN tout en garantissant une synchronisation régulière entre les sites.

Schéma de l'architecture

Avantages de cette architecture Cette architecture multi-site avec RODC présente plusieurs bénéfices stratégiques :

- **Haute disponibilité** : Aucun point unique de défaillance sur le site principal
- **Performance optimisée** : Authentification locale sur chaque site, réduisant la latence
- **Sécurité renforcée** : Limitation des risques sur les sites distants grâce au RODC
- **Optimisation WAN** : Réduction du trafic réseau inter-sites
- **Conformité** : Respect des meilleures pratiques Microsoft pour les infrastructures distribuées
- **Évolutivité** : Architecture facilement extensible pour de nouveaux sites distants

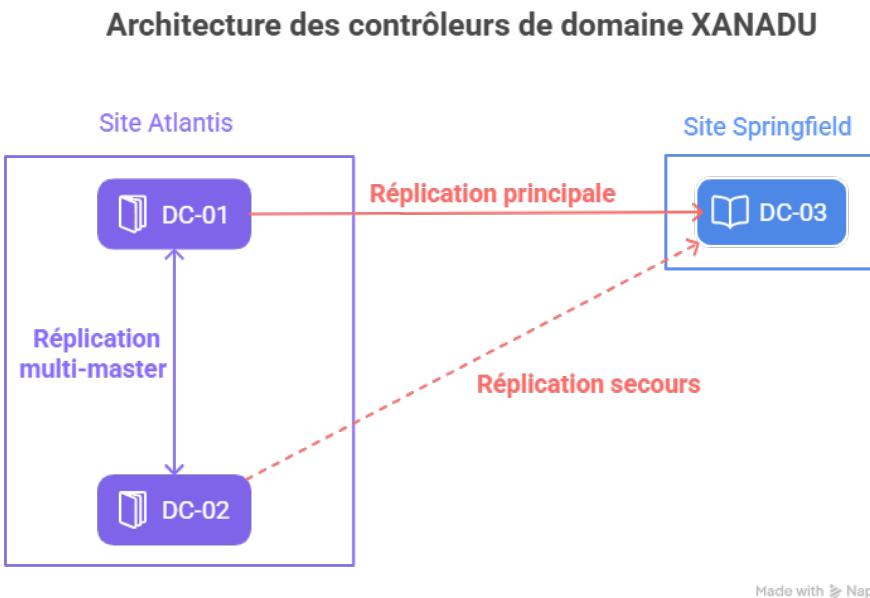


FIGURE 5.4 – Architecture des contrôleurs de domaine XANADU

5.2.4 Mise en place du serveur FS-01

Nous avons tout d'abord procédé à l'installation de **Windows Server 2025** sur la machine virtuelle destinée à devenir le serveur de fichiers **FS-01**

Les **pilotes VirtIO** ont ensuite été installés afin d'optimiser les performances du système et d'assurer une meilleure compatibilité avec l'environnement virtualisé, notamment pour la gestion du stockage et du réseau.

Une fois le système opérationnel, le serveur **FS-01** a été joint au domaine **Active Directory**, administré par le contrôleur de domaine **DC-01**. Cette intégration permet une gestion centralisée des comptes, des groupes et des droits d'accès.

Après son intégration au domaine, le serveur FS-01 apparaît comme un **objet ordinateur** dans l'annuaire Active Directory.

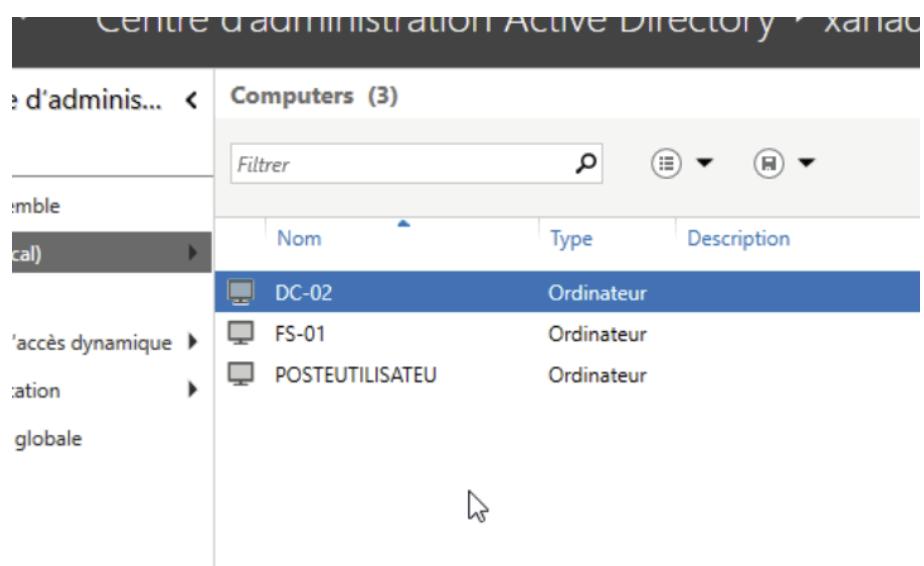


FIGURE 5.5 – Présence du serveur FS-01 dans l’annuaire Active Directory

Il a ensuite été positionné dans une **unité d’organisation dédiée aux serveurs**, afin de garantir une organisation logique de l’annuaire et de faciliter l’application de stratégies de groupe spécifiques.

Création des groupes de sécurité

Afin de structurer les accès aux ressources, des **groupes de sécurité globaux** ont été créés dans l’Active Directory. Ces groupes permettent de distinguer les utilisateurs par service ainsi que les administrateurs associés.

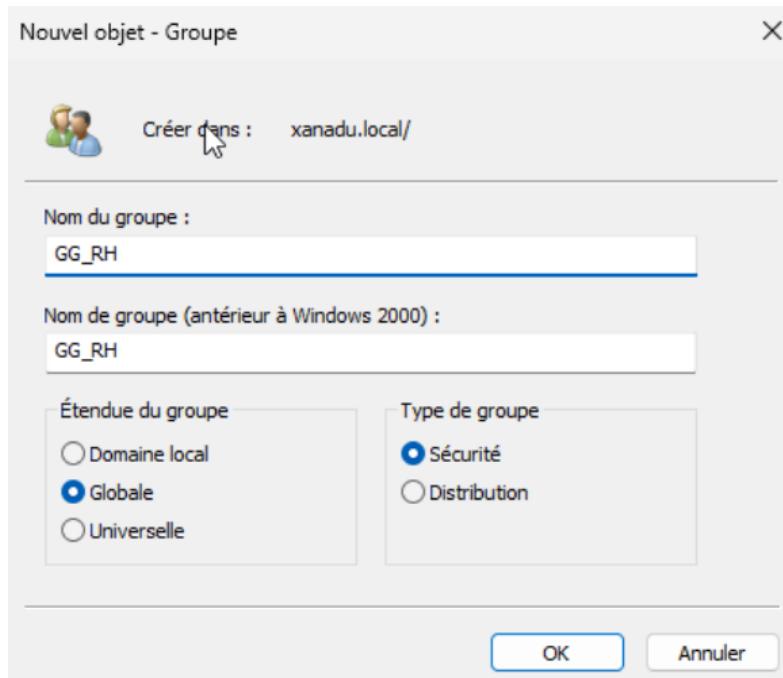


FIGURE 5.6 – Crédit d’un groupe de sécurité global utilisateur (GG)

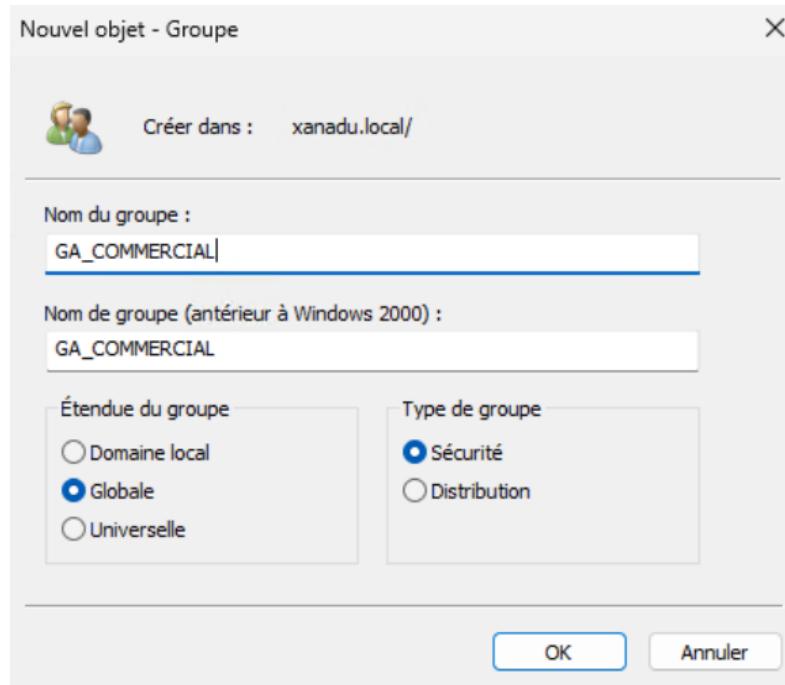


FIGURE 5.7 – Création d'un groupe de sécurité global administrateur (GA)

Ces groupes ont été nommés selon une convention claire distinguant les groupes d'utilisateurs (GG_) et les groupes d'administrateurs (GA_), facilitant l'attribution ultérieure des droits.

Mise en place de l'arborescence et des droits NTFS

Une **structure de dossiers** correspondant aux différents services de l'organisation a été créée sur le serveur FS-01.

Avant l'attribution des droits, l'héritage des permissions NTFS a été désactivé sur les dossiers de service afin d'éviter toute propagation de droits non souhaitée.

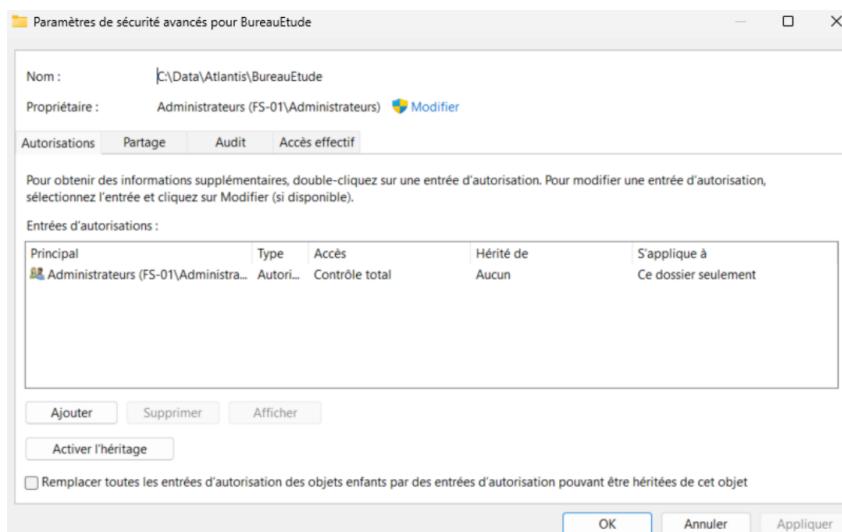


FIGURE 5.8 – Désactivation de l'héritage des permissions NTFS sur un dossier de service

Les groupes Active Directory ont ensuite été ajoutés manuellement aux dossiers afin de définir précisément les autorisations d'accès.

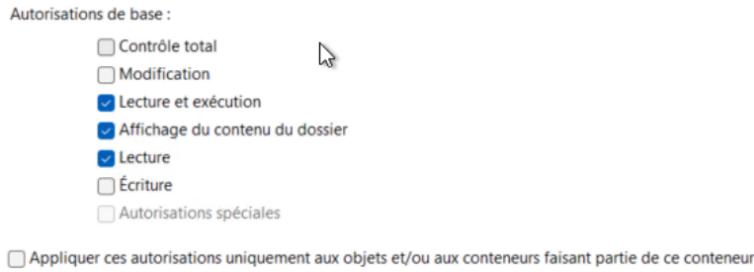


FIGURE 5.9 – Définition des autorisations NTFS appliquées aux groupes de service

Pour les groupes GA , on coche aussi la case contrôle total , et pour tous les groupes on coche aussi la case Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur

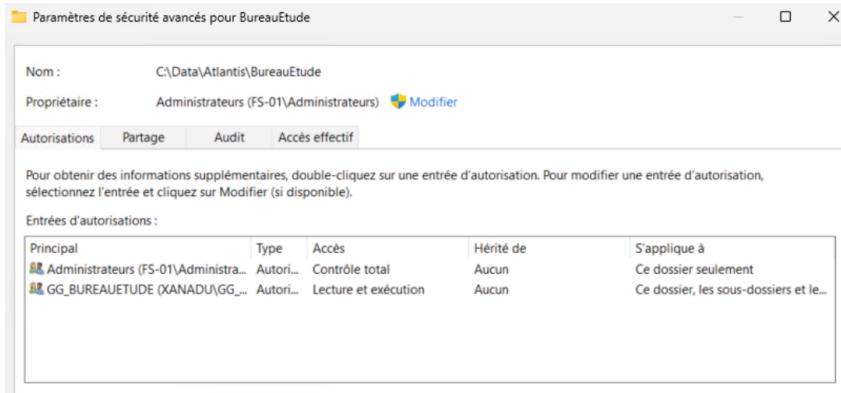


FIGURE 5.10 – Association d'un groupe Active Directory aux droits NTFS d'un dossier de service

Configuration des partages réseau

Enfin, les dossiers ont été **partagés via le protocole SMB**, rendant les ressources accessibles sur le réseau. Les autorisations de partage ont été configurées de manière cohérente avec les droits NTFS précédemment définis.

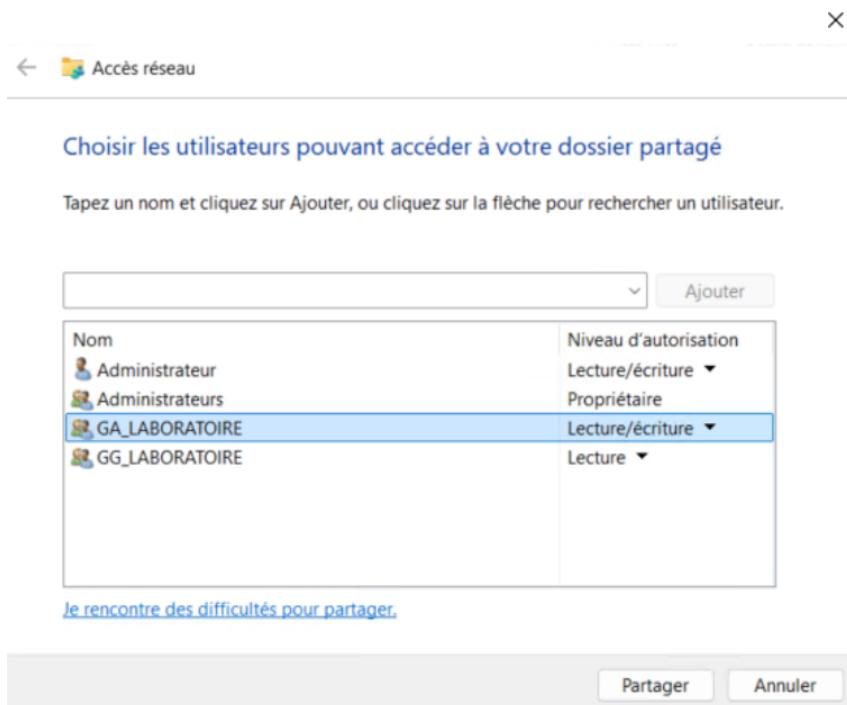


FIGURE 5.11 – Configuration des autorisations de partage réseau (SMB)

Cette configuration permet à l’Active Directory de piloter l’accès aux ressources partagées à l’aide des groupes et, par la suite, de déployer automatiquement les lecteurs réseau auprès des utilisateurs via des **stratégies de groupe (GPO)**.

5.2.5 Types de comptes et nomenclature

Dans le cadre de la mise en place de l’Active Directory, une nomenclature claire a été définie afin de structurer les comptes et les groupes de manière cohérente. Cette organisation facilite l’administration, améliore la lisibilité de l’annuaire et permet une gestion centralisée et sécurisée des droits d’accès.

Comptes utilisateurs

Les comptes utilisateurs correspondent aux employés de l’organisation. Chaque utilisateur dispose d’un compte personnel permettant l’authentification au domaine Active Directory et l’accès aux ressources partagées en fonction de son service.

La nomenclature retenue pour les comptes utilisateurs repose sur l’initiale du prénom suivie du nom, séparés par un underscore :

initialé_nom

Par exemple :

- Paul George : p_george
- LeBron James : l_james
- Anthony Davis : a_davis

La figure suivante illustre la création d’un compte utilisateur dans l’Active Directory en respectant cette nomenclature.

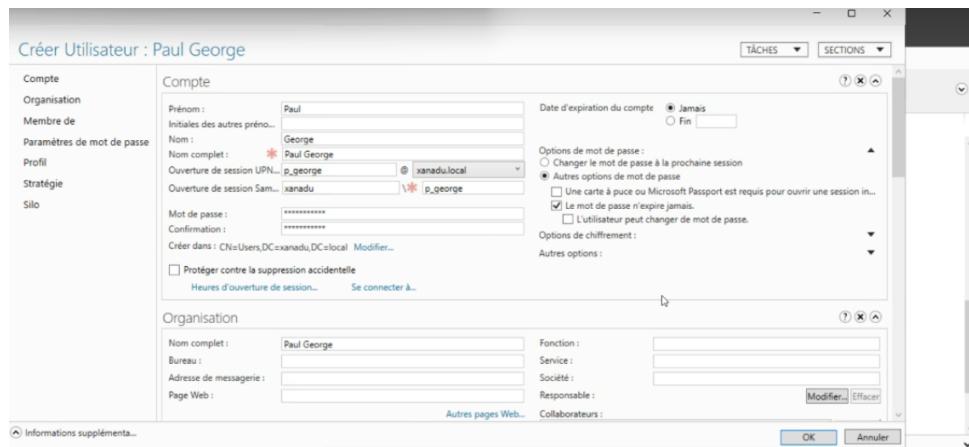


FIGURE 5.12 – Création d'un compte utilisateur dans l'Active Directory

Chaque compte utilisateur est membre d'un unique groupe global correspondant à son service, ce qui permet une attribution indirecte et centralisée des droits d'accès.

Groupes de sécurité

Les groupes de sécurité sont utilisés pour gérer les droits d'accès aux ressources du domaine. Deux types de groupes sont définis pour chaque service : les groupes globaux utilisateurs et les groupes administrateurs de service.

Groupes globaux utilisateurs (GG_service) Les groupes globaux, identifiés par le préfixe GG_, regroupent l'ensemble des utilisateurs d'un même service. Ces groupes permettent d'attribuer des droits d'accès aux ressources sans configuration individuelle des permissions.

Une fois le groupe créé, les utilisateurs du service sont ajoutés à celui-ci. L'exemple suivant montre l'ajout de l'utilisateur Paul George au groupe correspondant au service Juridique.

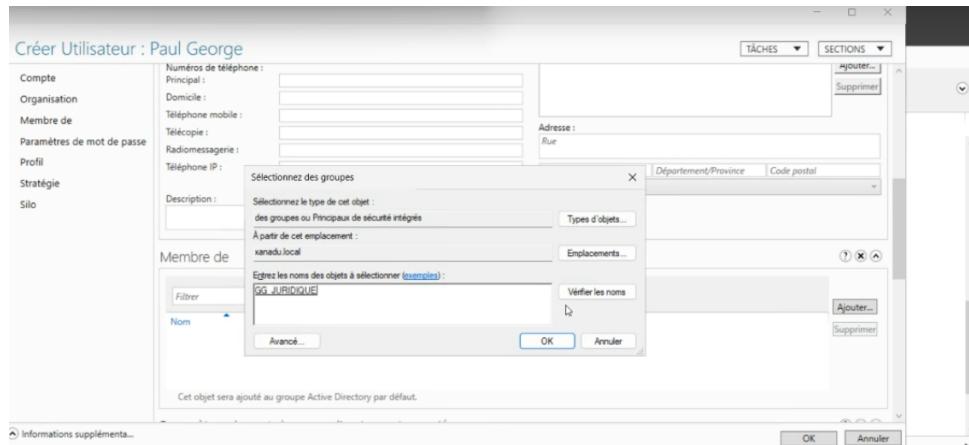


FIGURE 5.13 – Ajout d'un utilisateur à un groupe global de service

Groupes administrateurs de service (GA_service) Les groupes prefixés par GA_ correspondent aux comptes disposant de priviléges étendus au sein d'un service donné. Ils permettent une administration déléguée et contrôlée, notamment pour la gestion des ressources du service concerné.

Comptes administrateurs

Les comptes administrateurs du domaine sont réservés aux opérations pour donner les droits aux administrateurs de chaque service. Les administrateurs de chaque service auront donc les droits pour donner les permissions aux utilisateurs telles que :

- Les droits d'exécution des fichiers ;
- Les droits de création des fichiers ;
- Les droits de modification des fichiers ou de suppression des fichiers ;
- Ainsi que les droits de lecture.

Ils sont distincts des comptes utilisateurs standards et ne sont pas utilisés pour les tâches quotidiennes, conformément aux bonnes pratiques de sécurité.

Cette structuration des comptes et des groupes permet de respecter le principe de moindre privilège, de simplifier la gestion des droits d'accès et d'assurer une séparation claire entre les rôles utilisateurs et administratifs.

5.2.6 Validation et tests des droits d'accès

Afin de valider la bonne application des droits définis dans Active Directory et au niveau du serveur de fichiers FS-01, plusieurs tests ont été réalisés avec des comptes utilisateurs appartenant à différents services. Ces tests permettent de vérifier que les accès correspondent bien à la politique de sécurité définie et que le principe de moindre privilège est respecté.

Vérification des droits du service Direction

Le service Direction dispose de droits transversaux lui permettant de consulter l'ensemble des documents de l'infrastructure. Cette configuration vise à garantir une visibilité globale de l'activité de l'entreprise, tout en respectant le principe de moindre privilège.

La configuration des droits de partage montre que le groupe du service Direction est autorisé à accéder aux dossiers partagés en lecture sur l'ensemble de l'arborescence.

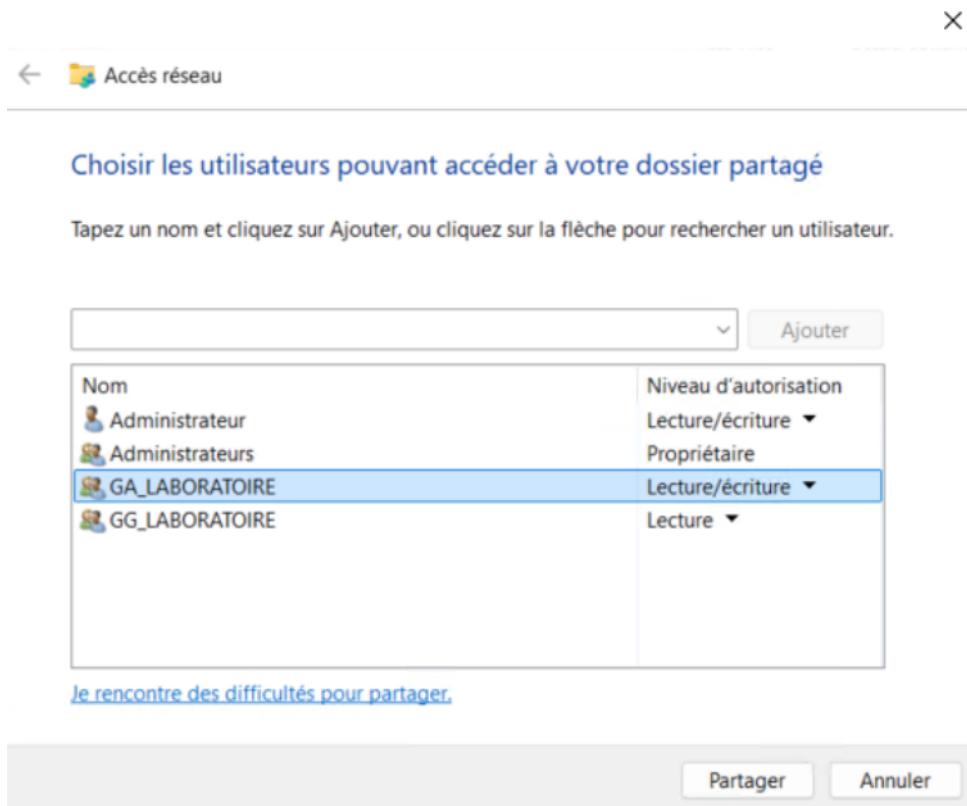


FIGURE 5.14 – Configuration des droits de lecture pour le service Direction

Un test de connexion a ensuite été réalisé avec un utilisateur appartenant au service Direction. Celui-ci peut accéder à l'ensemble des dossiers des différents services en lecture seule, confirmant que les droits globaux sont correctement appliqués.

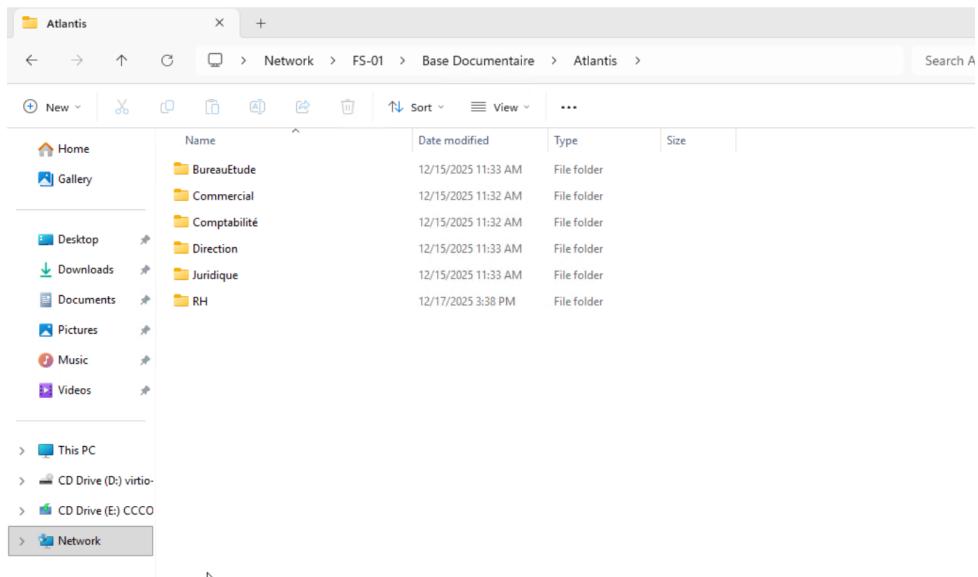


FIGURE 5.15 – Accès en lecture globale pour un utilisateur du service Direction

Vérification des droits du service Juridique

Le service Juridique dispose de droits spécifiques lui permettant de consulter et de modifier les documents relevant de son périmètre, tout en ayant également accès aux dossiers des services client et rh.

La configuration des groupes Active Directory montre que les utilisateurs du service Juridique sont membres du groupe correspondant, leur conférant des droits d'écriture sur leur dossier dédié.

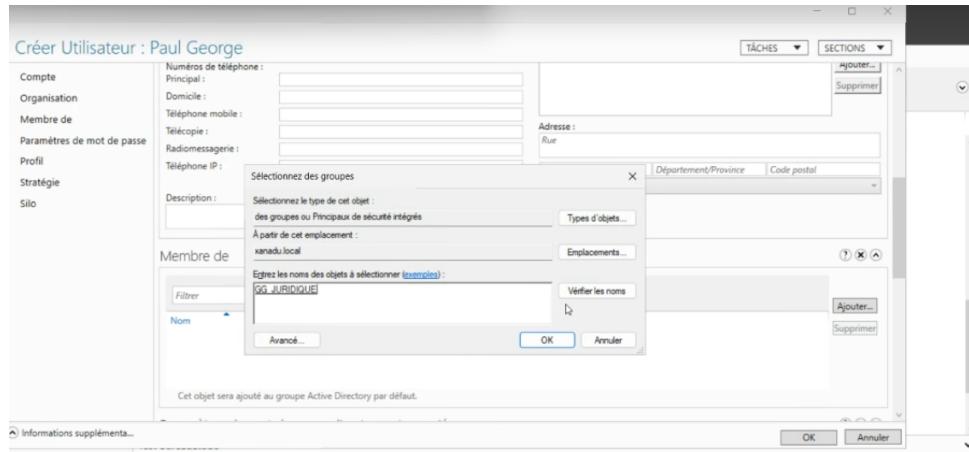


FIGURE 5.16 – Ajout d'un utilisateur au groupe du service Juridique

Un test de création de fichier a été effectué dans le dossier du service Juridique avec un utilisateur appartenant à ce service. L'utilisateur est en mesure de créer et modifier des documents, confirmant que les droits d'écriture sont correctement appliqués.

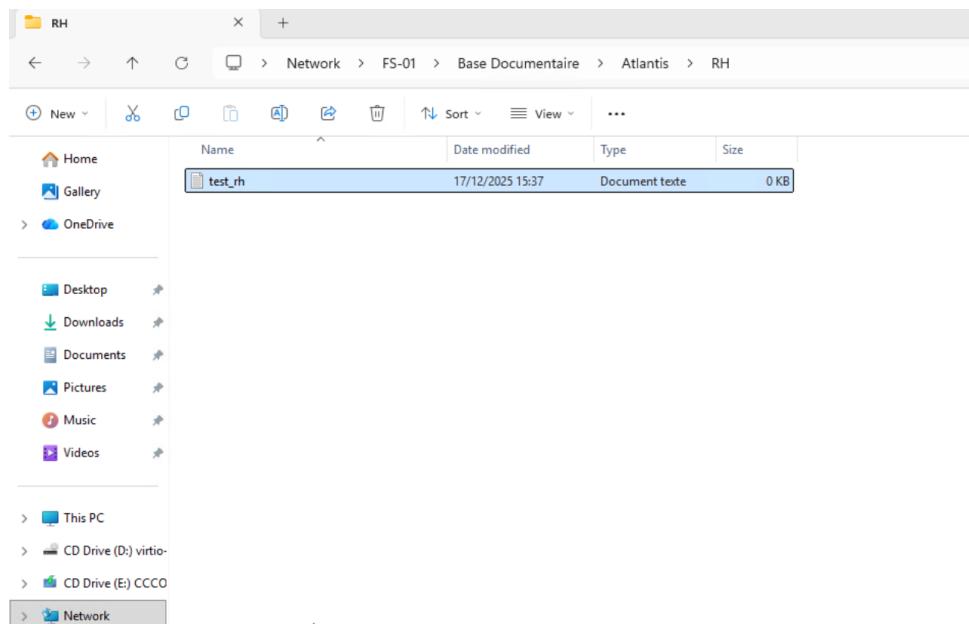


FIGURE 5.17 – Création d'un fichier dans le dossier Juridique

Ces tests confirment que les permissions NTFS et les droits de partage sont correctement configurés et appliqués selon les rôles définis dans Active Directory.

5.2.7 Administration déléguée par service

Dans une infrastructure comme celle de **XANADU**, donner tous les droits d'administration à une seule personne peut devenir un goulot d'étranglement ou un risque de sécurité. C'est pour cela que nous avons mis en place une **administration déléguée**.

L'idée est simple : permettre à des référents de chaque service de gérer leur propre périmètre sans pour autant avoir accès au reste du réseau.

Le rôle des groupes GA (Gestion des Accès)

Pour organiser cela, nous avons créé des groupes spécifiques, appelés **GA** (ex : GA_Comptabilite, GA_RH). Ces groupes permettent de séparer les responsabilités :

- **Gestion locale** : Un responsable du service RH peut, par exemple, gérer les permissions sur les dossiers de son service sans avoir besoin de demander l'intervention de l'administrateur système global.
- **Cloisonnement des droits** : Un administrateur délégué du service Commercial ne pourra jamais modifier ou accéder aux données du service Juridique. Ses droits sont "bloqués" à l'intérieur de son propre service.
- **Sécurité et réactivité** : Cela permet de répondre plus vite aux besoins des utilisateurs tout en limitant les dégâts si un compte est compromis (puisque n'a pas les droits sur tout le domaine).

Une structure à trois niveaux

Pour que cette délégation fonctionne, nous avons structuré les rôles de la manière suivante :

1. **Les Admins du Domaine** : Ils gardent le contrôle total sur les serveurs et l'infrastructure de base.
2. **Les Admins de Service (GA)** : Ils s'occupent uniquement de la gestion des fichiers et des droits de leur équipe sur le serveur **FS-01**.
3. **Les Utilisateurs** : Ils n'ont aucun droit d'administration et utilisent simplement les ressources dont ils ont besoin pour travailler.

Cette organisation garantit que le principe du **moindre privilège** est respecté à tous les niveaux : on ne donne à chacun que les outils dont il a besoin pour ses missions, ni plus, ni moins.

5.2.8 Politique de mots de passe et authentification (MFA)

L'authentification simple par mot de passe n'est plus suffisante aujourd'hui face aux techniques de piratage modernes (phishing, force brute). Pour sécuriser l'accès au domaine de l'entreprise **XANADU**, nous avons intégré une réflexion sur le **MFA (Multi-Factor Authentication)**.

Le principe de la double vérification

Le MFA ajoute une étape de validation supplémentaire lors de la connexion. Pour s'authentifier, l'utilisateur doit fournir deux types de preuves distinctes :

- **Ce qu'il sait** : Son mot de passe de session*.

- **Ce qu'il possède :** Un smartphone recevant une notification ou un code à usage unique (OTP) via une application comme *Microsoft Authenticator*.

Déploiement ciblé et prioritaire

Pour ne pas alourdir inutilement le travail quotidien tout en garantissant une sécurité maximale, le MFA est appliqué en priorité sur les accès les plus critiques :

- **Comptes Administrateurs :** Les administrateurs réseau ont un contrôle total sur le SI. Le MFA est donc obligatoire pour prévenir toute prise de contrôle globale de l'AD.
- **Accès Distants (VPN) :** Toutes les connexions provenant de l'extérieur du réseau de l'entreprise (télétravail) doivent impérativement être validées par un deuxième facteur.
- **Services Sensibles :** L'accès aux dossiers de la Direction et des Ressources Humaines sur le serveur **FS-01** peut être renforcé par cette mesure.

Authentification Multi-Facteurs (MFA)

La mise en place du MFA permet de réduire drastiquement le risque d'usurpation d'identité, c'est un élément clé qui complète notre politique de durcissement des serveurs et des postes.

Configuration des accès lors du déploiement

Concernant la phase concrète de mise en place du serveur FS-01 et des postes clients, nous avons utilisé un mot de passe standardisé pour l'ensemble des comptes utilisateurs avec 10 caractères, des chiffres et des caractères spéciaux.

Ce choix permet de faciliter la phase de configuration et de test de l'infrastructure. Bien que l'option de changement forcé au premier accès n'ait pas été activée pour garantir la stabilité des connexions lors des phases d'essais, ce mot de passe respecte les critères de sécurité de base de l'Active Directory :

- **Complexité :** Il mélange des majuscules, des minuscules, des caractères spéciaux et des chiffres.
- **Robustesse :** Avec 10 caractères, il dépasse le minimum requis par défaut de Windows.
- **Évolution :** Dans un scénario de production réelle, chaque utilisateur recevrait ce mot de passe de manière confidentielle avant d'être invité à le modifier via le menu de session (Ctrl+Alt+Suppr) une fois sa machine opérationnelle.

Contrôle des tentatives d'accès

Même avec un mot de passe commun, la sécurité est assurée par la **stratégie de verrouillage de compte**. Si une personne tente de deviner un mot de passe en testant plusieurs combinaisons sur un compte :

- Le compte est automatiquement bloqué après un nombre défini d'échecs (par défaut 5 ou 10 tentatives).
- Cela protège l'infrastructure contre les attaques de type "Brute Force" sur le réseau.

Chapitre 6

Stratégies de Groupe (GPO)

6.1 Fondamentaux

6.1.1 Définition des GPO

Les stratégies de groupe, appelées GPOs (*Group Policy Objects*), sont des mécanismes intégrés à Active Directory permettant de définir et d'appliquer de manière centralisée des règles de configuration et de sécurité sur les utilisateurs et les ordinateurs d'un domaine. Elles offrent un moyen efficace de standardiser les paramètres du système d'information et d'assurer une cohérence globale des configurations.

Les GPOs peuvent être utilisées pour configurer de nombreux éléments, tels que les paramètres de sécurité, les restrictions d'accès, les politiques de mots de passe, les configurations logicielles ou encore les paramètres système des postes de travail. Elles sont appliquées automatiquement en fonction de l'appartenance des objets à des unités d'organisation, des groupes ou à l'ensemble du domaine.

6.1.2 Principe de moindre privilège

Le principe de moindre privilège est un concept fondamental en sécurité des systèmes d'information. Il consiste à attribuer à chaque utilisateur, application ou service uniquement les droits strictement nécessaires à l'exécution de ses tâches, et aucun privilège supplémentaire.

Ce principe permet de limiter l'impact potentiel d'une erreur humaine, d'un abus de privilèges ou d'une compromission de compte. En restreignant les droits d'accès, on réduit la surface d'attaque du système d'information et on empêche un utilisateur ou un programme de réaliser des actions non autorisées ou dangereuses.

La mise en œuvre du principe de moindre privilège repose sur une gestion rigoureuse des droits, des groupes et des rôles, ainsi que sur une réévaluation régulière des autorisations accordées.

6.1.3 Rôle des GPOs dans la sécurisation du SI

Les GPOs jouent un rôle essentiel dans la sécurisation du système d'information en permettant l'application contrôlée des politiques de sécurité. Elles facilitent la mise en œuvre du principe de moindre privilège en imposant des restrictions d'usage et des configurations adaptées aux profils des utilisateurs et des postes.

Grâce aux GPOs, il est possible de renforcer la sécurité des environnements de travail en limitant l'accès aux fonctionnalités sensibles, en imposant des politiques de mots de passe robustes, en configurant les pare-feu locaux ou en contrôlant l'exécution des applications. Elles permettent également de réduire les erreurs de configuration en automatisant l'application des règles de sécurité.

En centralisant la gestion des politiques de sécurité, les GPOs contribuent à une meilleure gouvernance du système d'information, à une réduction des risques et à une amélioration globale du niveau de sécurité de l'entreprise.

6.2 Mise en œuvre technique

6.2.1 GPO de sécurité des postes

Pour la sécurité de l'AD, on a prévu des stratégies de groupe, on a mis en place des postes utilisateurs pour assurer un niveau de sécurité homogène dans l'ensemble du SI.

Ces groupes de sécurité ont comme fonction principale de limiter les risques d'erreurs humaines, comme les erreurs de manipulation, mais aussi de limiter les menaces internes. On impose dans ces groupes des limitations, comme des règles de verrouillage automatique après une période d'inactivité, puis on va limiter les accès aux paramètres sensibles aux comptes non administrateur.

Ces stratégies de groupe vont être mises en place dans la totalité des utilisateurs, ce qui va garantir une uniformité des paramètres de sécurité dans tous les postes, surtout dans ce qui concerne le pare-feu et la désactivation de certaines fonctionnalités pour limiter les risques de sécurité.

- Les comptes administrateurs disposent d'un contrôle total sur les fichiers, leur permettant d'administrer l'infrastructure Active Directory, les serveurs et les ressources partagées.
- Les comptes appartenant à un groupe de sécurité dans l'Active Directory héritent des droits associés à ce groupe et disposent d'un accès en lecture, et en écriture le cas échéant, uniquement sur les dossiers correspondant à leur service sauf pour les services juridique et direction, qui eux, ont accès aux services commerciaux et rh pour le service Juridique et un accès à tous les services pour le service Direction.
- Les comptes utilisateurs standards, non rattachés à un groupe de sécurité, ne disposent d'aucun droit particulier sur les ressources partagées. Ils peuvent uniquement s'authentifier sur le domaine et accéder à leurs fichiers personnels.

6.2.2 GPO de gestion des comptes

La gestion de comptes est complètement faite à partir de l'AD, ce qui permet de centraliser la création, l'organisation et la modification de tous les utilisateurs appartenant au SI.

Les comptes utilisateurs sont d'abord dans l'AD, suivant bien sûr une nomenclature définie et uniforme pour tous les utilisateurs. Ces comptes utilisateurs ont initialement aucune permission attribuée à eux, cela garantit que l'on respecte bien le principe du moindre privilège.

Ensuite, ces comptes utilisateurs sans permission seront rattachés à des groupes selon leur fonction dans l'entreprise. C'est cette appartenance à un groupe qui leur donnera les

droits nécessaires, notamment l'accès aux fichiers partagés avec leur groupe respectif dans FS-01, et selon le groupe ils auront des droits à la lecture ou parfois aussi à l'écriture sur les dossiers de son service.

Les comptes administrateurs sont strictement séparés des comptes utilisateurs pour assurer une meilleure sécurité, les comptes administrateurs sont responsables de donner les droits de lecture/écriture aux utilisateurs. Cette séparation évite les risques d'une mauvaise utilisation de ces priviléges.

6.2.3 GPO de contrôle des applications

Le contrôle des applications repose sur des règles basiques et simples, pour nous éviter l'exécution de logiciels pas nécessaires au SI, notre objectif est de limiter l'installation ou l'utilisation de programmes non autorisés par les utilisateurs.

Donc, aucune application n'est déployée automatiquement par GPO. les postes utilisateurs ne disposent pas de droits qui vont leur permettre d'installer librement des logiciels ou programmes

Cette approche permet de garantir la réduction des risques de sécurité liés aux logiciels malveillants et aussi une homogénéité de tous les postes utilisateurs.

6.2.4 GPO de gestion des mises à jour (WSUS)

Pour notre SI, on a mis en place des systèmes de mises à jour de manière centralisée, pour garantir que les postes et les serveurs soient tous dans le même niveau de sécurité. les mises à jour sont donc gérées de façon contrôlée et obligatoire pour tous les postes. On va donc utiliser un mécanisme centralisé pour la gestion des mises à jour, appelé WSUS, qui va nous permettre de valider les mises à jour avant leur déploiement, et s'assurer que toutes les machines concernées soient bien mises à jour. Cette organisation va limiter les interruptions de service et assurer une stabilité supérieure.

6.2.5 GPO de durcissement des serveurs

Le durcissement des serveurs vise à limiter leur surface d'attaque et à renforcer la sécurité globale de l'infrastructure. Les serveurs n'exécutent que les services strictement nécessaires à leur rôle.

Les comptes administrateurs sont séparés des comptes utilisateurs pour d'éviter les utilisations abusives des priviléges. Les accès aux serveurs sont limités aux personnes autorisées, et les droits sont attribués selon le principe du moindre privilège.

Cette configuration permet de réduire les risques liés aux erreurs de manipulation et aux attaques, en assurant un fonctionnement stable des services critiques de l'infrastructure.

6.2.6 GPO d'administration (redirection, mappages, VPN)

L'administration des accès a été organisée autour de l'Active Directory. Les accès aux ressources ne sont pas configurés poste par poste. Tout passe par les comptes et les groupes définis dans l'annuaire.

Les utilisateurs n'ont pas de droits attribués directement sur les dossiers. L'accès dépend uniquement du groupe auquel l'utilisateur est rattaché dans l'Active Directory.

Les dossiers partagés sont stockés sur le serveur FS-01. Les permissions sont définies sur ces dossiers en fonction des groupes.

Lorsqu'un utilisateur se connecte, il peut accéder aux dossiers de son service. Il ne voit pas les autres dossiers. Aucun réglage particulier n'est fait sur le poste utilisateur. Les droits sont déjà en place côté serveur.

Si un utilisateur change de service, son accès est modifié en changeant simplement son groupe dans l'Active Directory. Les droits sont appliqués automatiquement. Il n'y a pas besoin d'intervenir sur les dossiers ni sur le poste.

6.2.7 Matrice de liaison des GPOs aux OUs

GPO	OU Utilisateurs	OU Direction	OU Postes	OU Serveurs
GPO de sécurité des postes			X	
GPO de gestion des comptes	X	X		
GPO de contrôle des applications			X	
GPO de gestion des mises à jour (WSUS)			X	X
GPO de durcissement des serveurs				X
GPO d'administration	X	X		

X : la GPO est appliquée à l'unité d'organisation correspondante

Cellule vide : la GPO n'est pas appliquée à l'unité d'organisation

FIGURE 6.1 – Matrice de liaison entre les GPOs et les unités d'organisation

Chapitre 7

Sécurité Périmétrique et Filtrage

7.1 Fondamentaux

Imaginez votre infrastructure informatique comme un château fort : vous ne laisseriez pas n'importe qui entrer et circuler librement entre les différentes pièces, n'est-ce pas ? C'est exactement le rôle de la sécurité périmétrique dans notre projet XANADU. Face aux menaces qui guettent constamment les systèmes d'information, nous avons besoin d'un gardien vigilant : le pare-feu. C'est lui qui va décider qui peut entrer, où il peut aller, et ce qu'il peut faire une fois à l'intérieur.

7.1.1 Qu'est-ce qu'un pare-feu et pourquoi en avons-nous besoin ?

Le pare-feu, c'est un peu le vendeur d'une boîte de nuit version numérique. Il se positionne aux portes de notre réseau et vérifie chaque personne qui veut entrer ou sortir. Plus précisément, il analyse chaque paquet de données qui circule et décide de le laisser passer ou de le bloquer selon des règles bien définies.

Concrètement, voici ce que font nos pare-feux au quotidien :

- Ils empêchent les intrus d'accéder à notre réseau interne depuis Internet
- Ils surveillent et contrôlent les échanges entre nos différents services (les fameux VLANs dont on parlera plus tard)
- Ils appliquent la politique de sécurité qu'on a définie pour l'entreprise
- Ils gardent une trace de tout ce qui se passe pour qu'on puisse enquêter en cas de problème
- Ils assurent les communications sécurisées entre nos sites d'Atlantis et Springfield via la liaison MPLS

Dans notre infrastructure XANADU, on a choisi OPNsense comme solution de pare-feu. Au-delà du filtrage classique, nos pare-feux gèrent aussi les connexions VPN pour nos télétravailleurs, le NAT pour l'accès Internet, et tout le routage entre nos différents VLANs avec leurs règles de sécurité spécifiques.

7.1.2 La défense en profondeur : ne jamais mettre tous ses œufs dans le même panier

On pourrait se dire qu'un bon pare-feu suffit, mais en sécurité informatique, mieux vaut prévoir plusieurs lignes de défense. C'est ce qu'on appelle la "défense en profondeur" :

si une barrière cède, il en reste d'autres derrière. Pensez aux poupées russes, mais version sécurité !

Voici comment on a organisé nos différentes couches de protection :

- **Premier rempart : la couche périphérique** - Nos pare-feux principaux qui filtrent tout ce qui entre et sort d'Internet et gèrent les flux entre nos deux sites
- **Deuxième niveau : la segmentation réseau** - On a divisé notre réseau en plusieurs VLANs (des sous-réseaux isolés) avec des règles strictes qui contrôlent ce qui peut circuler entre eux
- **Troisième barrière : la couche applicative** - Au niveau de nos applications elles-mêmes (comme l'ERP ou l'Active Directory), on vérifie à nouveau les droits d'accès
- **Quatrième protection : le durcissement système** - Chaque serveur et poste de travail est configuré pour résister aux attaques
- **Dernier filet : la supervision** - On surveille en permanence pour détecter toute activité suspecte et réagir rapidement

L'idée, c'est qu'un pirate qui franchirait une couche se retrouverait face à une nouvelle barrière. Ça lui complique sérieusement la vie et nous donne du temps pour détecter l'intrusion et réagir.

7.1.3 La haute disponibilité : parce qu'on ne peut pas se permettre de tomber

Maintenant, parlons d'un sujet crucial : que se passe-t-il si notre pare-feu tombe en panne ? Eh bien, c'est simple : plus personne ne peut accéder à rien. Pour éviter ce cauchemar, on a mis en place ce qu'on appelle la "haute disponibilité" avec le protocole CARP.

Comment ça marche concrètement ?

On a installé deux pare-feux à chaque site. Imaginez-les comme deux gardes à une porte : l'un est actif et fait le boulot, l'autre est en stand-by et observe. Si le premier a un problème (panne matérielle, coupure électrique, bug logiciel...), le second prend immédiatement le relais. On appelle ça le "failover".

Le pare-feu actif (Primary) est celui qui bosse réellement. Il examine tout le trafic, applique les règles de filtrage, gère les translations d'adresses (NAT), bref, il fait tourner la boutique.

Le pare-feu passif (Standby) reste en alerte. Il reçoit en continu toutes les informations sur ce que fait son collègue actif : les connexions en cours, les configurations, tout. Comme ça, s'il doit prendre le relais, il peut continuer exactement là où l'autre s'est arrêté, sans perdre les connexions en cours.

Le protocole CARP : le chef d'orchestre de cette danse

CARP (Common Address Redundancy Protocol), c'est le système qui permet à nos deux pare-feux de travailler ensemble harmonieusement. Voici comment il opère sa magie :

- Les deux pare-feux partagent des adresses IP virtuelles (VIP) - c'est-à-dire que pour le reste du réseau, on dirait qu'il n'y a qu'un seul pare-feu

- Ils s'envoient régulièrement des "messages de vie" (heartbeat) pour vérifier que tout va bien
- Si le pare-feu actif ne répond plus, le passif détecte le problème en quelques secondes
- Le basculement est automatique et prend généralement moins de 2 secondes
- Grâce à la synchronisation de l'état des connexions (pfsync), même les sessions en cours ne sont pas interrompues

Du point de vue des utilisateurs, c'est totalement transparent : ils ne remarquent même pas qu'il y a eu un changement.

7.1.4 Pourquoi le filtrage réseau est-il si important ?

Le filtrage réseau n'est pas juste une question de cocher une case "sécurité". Il répond à plusieurs enjeux vraiment critiques pour l'entreprise :

- **Minimiser les risques d'attaque** - En n'autorisant que les flux strictement nécessaires, on réduit drastiquement les points d'entrée potentiels pour un pirate. Moins il y a de portes, moins il y a de risques qu'on en oublie une ouverte
- **Rester en conformité** - Avec le RGPD, ISO 27001 et autres réglementations, on doit pouvoir prouver qu'on contrôle qui accède à quoi. Nos règles de filtrage sont notre preuve tangible
- **Optimiser les performances** - Un réseau encombré de trafic inutile, c'est un réseau lent. En bloquant ce qui ne sert à rien, on améliore les performances pour ce qui compte vraiment
- **Garder une trace de tout** - Tous les événements sont journalisés. Si un incident se produit, on peut remonter le fil et comprendre ce qui s'est passé
- **Protéger ce qui est vraiment critique** - Nos systèmes de sauvegarde et d'administration sont particulièrement isolés du reste, parce que ce sont des cibles de choix pour les attaquants

Point d'attention ANSSI

L'ANSSI (l'autorité française de cybersécurité) est très claire dans sa recommandation R1 : il faut appliquer le principe du « **deny by default** ». En français dans le texte : tout ce qui n'est pas explicitement autorisé doit être interdit. C'est exactement ce qu'on applique dans notre infrastructure.

7.2 Mise en œuvre technique

Passons maintenant aux choses concrètes : comment on a vraiment mis tout ça en place dans notre infrastructure XANADU.

7.2.1 Notre architecture de pare-feux : un sur chaque site, doublé pour la sécurité

On a déployé une paire de pare-feux redondants sur chacun de nos deux sites. Voici comment c'est organisé :

Sur le site d'Atlantis (notre siège) :

- FIREWALL-01 joue le rôle de pare-feu principal (c'est lui qui est actif la plupart du temps)
- FIREWALL-02 est son fidèle second (en mode passif, prêt à bondir si besoin)
- Les deux partagent une adresse IP virtuelle grâce à CARP
- Ils protègent et routent le trafic de 7 VLANs différents :
 - VLAN 10 - Administration (où vivent nos serveurs critiques comme les contrôleurs de domaine)
 - VLAN 20 - Application (c'est là que tourne notre ERP)
 - VLAN 30 - Utilisateurs (tous les postes de travail du personnel)
 - VLAN 40 - Backup (notre système de sauvegarde, bien isolé)
 - VLAN 50 - DMZ/VPN (pour les accès de l'extérieur)
 - VLAN 60 - Imprimantes (parce qu'elles aussi ont besoin de leur coin)
 - VLAN 66 - Management (l'accès d'administration ultra-sécurisé)

Sur le site de Springfield (notre laboratoire) :

- FIREWALL-03 et FIREWALL-04 fonctionnent exactement sur le même principe
- Ils gèrent 6 VLANs adaptés aux besoins du labo :
 - VLAN 110 - Supervision (la surveillance du labo)
 - VLAN 120 - Postes Utilisateurs Labo (les chercheurs et techniciens)
 - VLAN 130 - Équipements Labo (les machines de test et de mesure)
 - VLAN 140 - Imprimantes
 - VLAN 150 - Active Directory (le contrôleur de domaine local)
 - VLAN 160 - Backup

Les pare-feux des deux sites communiquent entre eux via une liaison MPLS sécurisée, ce qui nous permet d'avoir un réseau d'entreprise unifié tout en gardant une séparation physique entre les sites.

7.2.2 Comment configurer CARP : le guide étape par étape

La configuration CARP suit les mêmes principes sur les deux sites. Voici comment on procède concrètement :

1. Première étape : préparer les interfaces physiques

Avant de parler de haute disponibilité, il faut que chaque pare-feu ait ses interfaces réseau bien configurées :

- Interface WAN - celle qui donne sur Internet (attention, terrain hostile !)
- Interface LAN - la connexion vers notre réseau interne (territoire sûr)
- Interface SYNC - une connexion directe entre les deux pare-feux, uniquement pour qu'ils se synchronisent (c'est leur canal privé de communication)
- Interfaces VLAN - une interface virtuelle pour chaque VLAN qu'on gère

2. Deuxième étape : créer les adresses IP virtuelles (VIP)

C'est là que la magie CARP opère. On va créer des adresses IP que les deux pare-feux vont partager :

- On va dans le menu : Firewall → Virtual IPs
- On choisit le type : CARP

- On définit un VHID (identifiant unique) pour chaque adresse virtuelle - pensez-y comme un numéro de badge
- On configure un mot de passe partagé entre les deux pare-feux pour qu'ils puissent s'authentifier mutuellement
- On règle la fréquence d'annonce (par défaut 1 seconde, ce qui veut dire qu'ils se disent "je suis toujours là" toutes les secondes)

3. Troisième étape : activer la synchronisation pfsync

Cette partie est cruciale : il faut que le pare-feu passif sache exactement ce que fait l'actif pour pouvoir reprendre la main sans accro :

- Direction : System → High Availability Sync
- On active "Synchronize States" - ça va synchroniser toutes les connexions en cours
- On choisit l'interface SYNC qu'on a créée à l'étape 1
- On indique l'adresse IP du pare-feu partenaire
- On active aussi "Configuration Sync" pour que les règles de filtrage soient automatiquement copiées d'un pare-feu à l'autre (pratique quand on fait des changements !)

4. Dernière étape : tester que tout fonctionne

Une haute disponibilité qui n'a jamais été testée, c'est une fausse sécurité. Voici notre check-list de validation :

- On vérifie le statut CARP dans le menu : Status → CARP (failover) - les deux pare-feux doivent apparaître, un en MASTER et l'autre en BACKUP
- On fait un vrai test de basculement : on éteint (proprement) le pare-feu actif et on chronomètre
- Le pare-feu passif doit prendre le relais en moins de 2 secondes
- On vérifie que les connexions actives (comme une session SSH ou un téléchargement en cours) continuent sans interruption
- Une fois le premier pare-feu rallumé, il doit reprendre son rôle de BACKUP sans tout casser

Conseil d'expert

Ne lésinez pas sur l'interface SYNC dédiée ! On pourrait être tenté de faire passer la synchronisation par le réseau de production pour économiser un câble, mais c'est une très mauvaise idée. Quand les pare-feux échangent l'état de milliers de connexions, ça génère pas mal de trafic. Mieux vaut que ce trafic circule sur son propre câble direct entre les deux pare-feux.

7.2.3 Notre politique de filtrage : les grands principes

Avant de plonger dans le détail de chaque règle, expliquons notre philosophie générale en matière de filtrage. Tout repose sur quelques principes simples mais stricts :

1. Interdit par défaut, autorisé sur demande

C'est notre règle d'or : si on n'a pas explicitement dit "oui, ce flux peut passer", alors il est bloqué. Point. Certains diraient que c'est paranoïaque, nous on appelle ça prudent.

2. Chaque liste de règles se termine par un refus explicite

À la fin de chaque ensemble de règles pour un VLAN, on met une règle qui dit "tout le reste = interdit". Elle porte toujours le numéro 999 pour qu'elle soit bien la dernière à être évaluée.

3. L'ordre des règles suit une logique claire

On a organisé nos règles par priorité selon leur fonction. C'est comme des étages dans un immeuble :

- Numéros 100-199 : L'auto-protection (l'accès d'administration aux pare-feux)
 - priorité absolue
- Numéros 200-299 : Le MCO, Maintien en Condition Opérationnelle (les mises à jour, la réPLICATION de données) - très important pour que tout tourne bien
- Numéros 300-399 : Les flux métiers (les utilisateurs qui accèdent aux services dont ils ont besoin) - le cœur de l'activité
- Numéros 400-499 : Les échanges inter-sites et l'accès distant (VPN, flux MPLS)
 - la collaboration entre sites
- Numéro 999 : La règle de refus par défaut - le filet de sécurité final

4. Le principe du moindre privilège

Quand on autorise un flux, on ne donne que le strict minimum : le protocole exact nécessaire, les ports précis, rien de plus. Si l'ERP n'a besoin que du HTTPS sur le port 443, on n'ouvre que ça. Pas question d'ouvrir "tout HTTP" ou "tout le réseau".

5. Une isolation renforcée pour les zones sensibles

Nos VLANs de sauvegarde (40 et 160) et de management (66) sont particulièrement verrouillés. Ce sont des cibles privilégiées pour les attaquants, donc on ne rigole pas avec leur sécurité.

Pour replacer les choses dans leur contexte : une politique de filtrage, ça sert à décider qui peut utiliser quoi et quand. Ça nous protège aussi contre la propagation de virus ou de malware en les bloquant avant qu'ils ne se répandent partout. On l'a mise en place à la périphérie de notre réseau, comme un douanier qui contrôle ce qui rentre et sort.

Dans notre architecture, chaque VLAN a ses propres règles adaptées à son usage. Et parfois, même à l'intérieur d'un VLAN, certaines machines peuvent avoir des règles supplémentaires plus restrictives.

7.2.4 Les règles de filtrage détaillées pour Atlantis

Rentrions maintenant dans le vif du sujet : voici comment on a configuré le filtrage pour chaque VLAN du site d'Atlantis. Pour chaque règle, on va expliquer non seulement ce qu'elle fait, mais surtout pourquoi elle existe.

VLAN 10 : Administration - Le saint des saints

Ce VLAN héberge nos serveurs les plus critiques : les contrôleurs de domaine DC-01 et DC-02, le serveur WSUS pour les mises à jour, et le serveur de fichiers FS-01. Autant dire qu'on ne plaisante pas avec sa sécurité.

Ordre	Source	Destination	Protocole	Action	Description
210	WSUS-01	Internet	HTTPS (443), TCP/8530- 8531	Autoriser	Le serveur WSUS télécharge les mises à jour Microsoft
230	DC-01/02	Internet	DNS (53), TCP/88, TCP/389, TCP/636	Autoriser	Nos contrôleurs de domaine peuvent résoudre des noms sur Internet
310	VLAN 30/VPN	FS-01	SMB (445)	Autoriser	Les utilisateurs accèdent à leurs fichiers partagés
400	DC-01/02	VLAN 150 (RODC)	Ports AD	Autoriser	RéPLICATION de l'annuaire vers Springfield
420	VLAN 120 (Labo)	FS-01 (Bureau d'étude)	SMB (445)	Autoriser	Le labo peut consulter les docs du bureau d'études (en lecture seule)
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.1 – Règles de filtrage VLAN 10 - Administration

Pourquoi ces règles ?

La règle 210 permet à notre serveur WSUS de télécharger les mises à jour depuis Microsoft. Sans ça, impossible de maintenir nos postes de travail à jour et sécurisés. C'est un passage obligé pour la sécurité.

La règle 230 peut sembler contre-intuitive (pourquoi nos contrôleurs de domaine ont-ils besoin d'Internet ?), mais c'est nécessaire pour qu'ils puissent résoudre des noms de domaine externes. Par exemple, quand un utilisateur veut accéder à Office 365, le DC doit pouvoir résoudre les noms Microsoft.

La règle 310, c'est le flux métier de base : les employés doivent pouvoir accéder à leurs fichiers. On autorise le protocole SMB (le partage de fichiers Windows) depuis le VLAN utilisateurs et le VPN.

La règle 400 est vitale pour que nos deux sites restent synchronisés. Les contrôleurs de domaine d'Atlantis répliquent régulièrement l'annuaire Active Directory vers Springfield pour que les utilisateurs là-bas puissent se connecter même si la liaison tombe.

La règle 420 répond à un besoin métier spécifique : les gens du laboratoire ont parfois besoin de consulter des documents techniques du bureau d'études. On leur donne un accès en lecture seule pour qu'ils puissent lire mais pas modifier ou supprimer.

VLAN 20 : Application - Le cœur de notre ERP

Ce VLAN, c'est là où tourne notre ERP, l'application métier critique de l'entreprise. Il comprend le serveur d'application ERP-APP et sa base de données ERP-DB.

Ordre	Source	Destination	Protocole	Action	Description
320	VLAN 30/VPN	ERP-APP	HTTPS (443)	Autoriser	Les utilisateurs se connectent à l'interface web de l'ERP
330	ERP-APP	ERP-DB	PostgreSQL (5432)	Autoriser	Le serveur d'application parle à sa base de données
410	VLAN (Labo) 120	ERP-APP	HTTPS (443)	Autoriser	Les utilisateurs de Springfield accèdent aussi à l'ERP
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.2 – Règles de filtrage VLAN 20 - Application

La logique derrière ces règles

La règle 320 est essentielle : c'est elle qui permet aux utilisateurs de travailler ! Ils se connectent à l'ERP via leur navigateur web en HTTPS. On insiste sur le HTTPS parce que l'ERP manipule des données sensibles (commandes, facturation, etc.) qui doivent être chiffrées pendant le transport.

La règle 330, c'est la communication interne de l'ERP : le serveur applicatif doit pouvoir interroger la base de données PostgreSQL. Sans cette règle, l'ERP ne pourrait tout simplement pas fonctionner. C'est comme autoriser le cerveau à parler à la mémoire.

La règle 410 étend l'accès à l'ERP aux utilisateurs du site de Springfield. Ils ont les mêmes besoins que leurs collègues d'Atlantis, donc ils ont la même autorisation. Le flux passe par notre liaison MPLS sécurisée entre les deux sites.

VLAN 30 : Postes Utilisateurs - Là où travaille tout le monde

C'est le plus grand VLAN en nombre de machines : tous les postes de travail du personnel d'Atlantis sont ici. On parle d'environ 60 postes répartis dans différents services (RH, Commercial, Bureau d'étude...).

Ordre	Source	Destination	Protocole	Action	Description
300	VLAN 30	Internet	DNS (53), HTTP (80), HTTPS (443)	Autoriser	Navigation Internet et services cloud (Office 365)
310	VLAN 30	FS-01 (VLAN 10)	SMB (445)	Autoriser	Accès aux dossiers partagés et personnels
320	VLAN 30	ERP-APP (VLAN 20)	HTTPS (443)	Autoriser	Utilisation de l'ERP
340	VLAN 30	VLAN 60 (Imprimantes)	TCP 9100, SNMP	Autoriser	Impression de documents
430	VLAN 30 (Bureau d'étude)	Équipements Labo (VLAN 130)	Spécifique	Autoriser	Le bureau d'études pilote les équipements du labo
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.3 – Règles de filtrage VLAN 30 - Postes Utilisateurs

Explications détaillées

La règle 300, c'est l'accès Internet classique. Les employés ont besoin de naviguer sur le web pour leur travail et d'accéder aux services cloud comme Office 365 (mail, SharePoint, Teams, etc.). On autorise le DNS pour résoudre les noms de sites, et HTTP/HTTPS pour le web.

Les règles 310 et 320 donnent accès aux deux applications métier principales : le serveur de fichiers et l'ERP. C'est le minimum vital pour travailler au quotidien.

La règle 340 permet l'impression. On autorise le port 9100 (protocole d'impression standard) et SNMP pour que les postes puissent interroger l'état des imprimantes (niveau d'encre, papier coincé, etc.).

La règle 430 est plus spécifique : elle ne s'applique qu'aux postes du bureau d'études. Ces ingénieurs ont besoin de piloter à distance les équipements de test du laboratoire de Springfield. Les protocoles varient selon les équipements (certains utilisent du Modbus, d'autres du HTTP, etc.), d'où le "Spécifique" dans le tableau.

VLAN 40 : Backup - La zone ultrasensible

Notre système de sauvegarde TrueNAS vit ici, complètement isolé du reste. C'est notre filet de sécurité en cas de désastre, donc on le protège comme le Saint Graal.

Ordre	Source	Destination	Protocole	Action	Description
220	TRUENAS-01	VLAN 10/20/130/150	SMB/SSH/etc.	Autoriser	TrueNAS lance ses sauvegardes vers les serveurs
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.4 – Règles de filtrage VLAN 40 - Backup

Pourquoi une seule règle (en plus du refus par défaut) ?

C'est voulu ! Remarquez qu'on n'autorise que le trafic SORTANT du VLAN de backup. C'est TrueNAS qui va chercher les données à sauvegarder, jamais l'inverse. Pourquoi cette rigueur ?

Imaginez qu'un ransomware infecte un serveur du VLAN 10. Si ce serveur pouvait se connecter librement au VLAN de backup, le ransomware pourrait chiffrer nos sauvegardes aussi, et là on serait vraiment dans le pétrin. En interdisant tout trafic entrant vers le VLAN 40, on s'assure que même si un serveur est compromis, il ne pourra jamais toucher à nos sauvegardes.

C'est ce qu'on appelle le principe du "flux unidirectionnel" pour les sauvegardes : les données coulent dans un seul sens, du serveur de production vers le système de backup, jamais dans l'autre sens.

VLAN 50 : DMZ / VPN - La zone d'échange avec l'extérieur

Ce VLAN héberge tout ce qui doit être accessible depuis l'extérieur, notamment notre serveur VPN WireGuard pour les télétravailleurs.

Ordre	Source	Destination	Protocole	Action	Description
440	VPN WireGuard	VLAN 10/20/30	Services autorisés	Autoriser	Les télétravailleurs accèdent aux ressources internes
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.5 – Règles de filtrage VLAN 50 - DMZ/VPN

Le télétravail en toute sécurité

La règle 440 permet aux employés en télétravail ou en déplacement de se connecter au réseau de l'entreprise via le VPN. Une fois authentifiés, ils peuvent accéder aux mêmes ressources que s'ils étaient au bureau : fichiers partagés, ERP, etc.

On utilise WireGuard, un protocole VPN moderne et rapide, avec une authentification forte par clés cryptographiques. Chaque télétravailleur a sa propre clé, et on peut révoquer un accès individuellement si nécessaire (départ d'un employé, perte d'un ordinateur portable...).

VLAN 60 : Imprimantes - Les périphériques qu'on oublie souvent

Les imprimantes réseau, on a tendance à les négliger en matière de sécurité, mais c'est une erreur. Elles tournent souvent avec des firmwares obsolètes et peuvent servir de porte d'entrée à un attaquant. D'où leur isolation dans un VLAN dédié.

Ordre	Source	Destination	Protocole	Action	Description
340	VLAN 60	VLAN 30	TCP 9100	Autoriser	L'imprimante répond aux demandes d'impression
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.6 – Règles de filtrage VLAN 60 - Imprimantes

Un flux unidirectionnel maîtrisé

Notez que les imprimantes peuvent uniquement RÉPONDRE au VLAN utilisateurs, mais elles ne peuvent pas initier de connexions ailleurs. C'est volontaire : si une imprimante était compromise (et ça arrive plus souvent qu'on ne pense), l'attaquant serait bloqué dans ce VLAN et ne pourrait pas se propager au reste du réseau.

VLAN 66 : Management - L'accès d'administration ultra-sécurisé

C'est le VLAN le plus restreint de tous. Seuls quelques postes d'administration spécifiques peuvent y accéder, et c'est depuis ce VLAN qu'on gère nos pare-feux et autres équipements réseau critiques.

Ordre	Source	Destination	Protocole	Action	Description
100	VLAN 66	FIREWALL 1/2	SSH (22), HTTPS (443)	Autoriser	Administration des pare-feux depuis les postes dédiés
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.7 – Règles de filtrage VLAN 66 - Management

L'auto-protection au plus haut niveau

Cette règle porte le numéro 100, ce qui lui donne la priorité absolue sur toutes les autres. C'est crucial : même en cas de problème sur le réseau, on doit toujours pouvoir accéder aux pare-feux pour corriger la situation.

L'ANSSI insiste beaucoup là-dessus dans sa recommandation R1 : les équipements de sécurité doivent avoir leur propre système d'administration isolé. On ne peut pas gérer un pare-feu depuis n'importe quel poste du réseau, ce serait prendre un risque énorme.

Dans la pratique, on a trois postes dédiés dans le VLAN 66, dans une salle sécurisée, accessibles uniquement aux administrateurs système. Ces postes n'ont pas d'accès Internet et servent uniquement à l'administration de l'infrastructure.

7.2.5 Les règles de filtrage pour Springfield

Le site de Springfield, c'est notre laboratoire de R&D. Il a des besoins un peu différents d'Atlantis, d'où une organisation en VLANs légèrement différente. Passons-les en revue.

VLAN 110 : Supervision - L'œil qui surveille le labo

Ce VLAN héberge nos serveurs de supervision Linux (LAB-01 et LAB-02) qui collectent les logs et métriques de tous les équipements du laboratoire.

Ordre	Source	Destination	Protocole	Action	Description
200	Any (VLAN 120/130/140)	LAB-01/02	Syslog	Autoriser	Les équipements envoient leurs logs aux serveurs de supervision
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.8 – Règles de filtrage VLAN 110 - Supervision

Pourquoi centraliser les logs ?

Dans un laboratoire, il se passe plein de choses : tests, mesures, manipulations sur les équipements. Avoir une trace centralisée de tout ça est essentiel pour plusieurs raisons :

- Diagnostiquer les problèmes quand une expérience échoue
- Reconstituer la chronologie des événements en cas d'incident
- Prouver la conformité aux procédures qualité
- Déetecter des comportements anormaux qui pourraient signaler un problème de sécurité

La règle 200 permet à tous les équipements du labo d'envoyer leurs logs via le protocole Syslog standard.

VLAN 120 : Postes Utilisateurs Labo - Les chercheurs et techniciens

Ce sont les 10 postes de travail des gens qui travaillent au labo. Ils ont des besoins spécifiques liés à leurs activités.

Ordre	Source	Destination	Protocole	Action	Description
410	VLAN 120	ERP-APP (VLAN 20)	HTTPS (443)	Autoriser	Accès à l'ERP du siège (commandes, congés, notes de frais...)
420	VLAN 120	FS-01 (VLAN 10)	SMB (445)	Autoriser	Consultation des documents techniques du bureau d'études
450	VLAN 120	VLAN 140 (Imprimantes)	TCP 9100, SNMP	Autoriser	Impression des rapports et résultats d'expériences
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.9 – Règles de filtrage VLAN 120 - Postes Utilisateurs Labo

Le labo reste connecté au siège

Même si Springfield est un site distant, les employés là-bas restent des employés de l'entreprise avec les mêmes besoins administratifs. La règle 410 leur permet d'accéder à l'ERP pour gérer leurs congés, leurs notes de frais, passer des commandes de matériel, etc.

La règle 420 répond au besoin inverse de celle qu'on a vue pour Atlantis : ici, les gens du labo consultent les documents techniques produits par le bureau d'études du siège. Collaboration bidirectionnelle entre les deux sites !

VLAN 130 : Équipements Labo - Les machines de test

C'est là que vivent tous les équipements spécialisés du laboratoire : oscilloscopes, analyseurs, machines de test, etc. Certains sont pilotés à distance depuis Atlantis.

Ordre	Source	Destination	Protocole	Action	Description
430	VLAN 30 (Bureau d'étude)	VLAN 130	Spécifique	Autoriser	Les ingénieurs d'Atlantis pilotent les équipements du labo
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.10 – Règles de filtrage VLAN 130 - Équipements Labo

Le pilotage à distance en toute sécurité

Cette règle est le pendant de celle qu'on a vue dans le VLAN 30 d'Atlantis. Elle permet aux ingénieurs du bureau d'études de lancer des tests sur les équipements du labo sans avoir à se déplacer à Springfield.

Le terme "Spécifique" dans les protocoles s'explique par la diversité des équipements : certains utilisent du HTTP/HTTPS, d'autres du Modbus TCP, du SCPI, voire des protocoles propriétaires. On configure les autorisations au cas par cas selon les équipements installés.

Cette forte isolation du VLAN 130 est importante : ces équipements sont souvent fournis par des fabricants tiers, avec des systèmes d'exploitation parfois anciens. En les isolant, on limite les risques si l'un d'eux s'avérait vulnérable.

VLAN 140 : Imprimantes du labo

Même principe qu'à Atlantis : les imprimantes dans leur propre VLAN isolé.

Ordre	Source	Destination	Protocole	Action	Description
450	VLAN 140	VLAN 120	TCP 9100	Autoriser	Les imprimantes répondent aux travaux d'impression
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.11 – Règles de filtrage VLAN 140 - Imprimantes

Rien de particulier à ajouter ici : même logique que pour Atlantis. Les imprimantes sont des périphériques souvent négligés en sécurité, donc on les isole par principe de précaution.

VLAN 150 : Active Directory - Le contrôleur de domaine local

Springfield a son propre contrôleur de domaine, DC-03, mais c'est un RODC (Read-Only Domain Controller). Il ne fait que répliquer les données depuis les DC d'Atlantis, il ne peut pas les modifier.

Ordre	Source	Destination	Protocole	Action	Description
400	DC-03 (RODC)	VLAN 10 (Atlantis DC)	Ports AD	Autoriser	Le RODC se synchronise avec les DC maîtres d'Atlantis
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.12 – Règles de filtrage VLAN 150 - Active Directory

Pourquoi un RODC plutôt qu'un DC classique ?

Le choix d'un RODC pour Springfield n'est pas anodin. Un RODC, comme son nom l'indique, ne contient qu'une copie en lecture seule de l'annuaire. Il ne peut pas modifier les données, juste les lire et les répliquer depuis Atlantis.

Avantages pour un site distant :

- Si le site de Springfield est compromis, l'attaquant ne peut pas modifier l'annuaire global de l'entreprise
- Les mots de passe ne sont pas tous stockés sur le RODC (seulement ceux des utilisateurs locaux mis en cache)
- Ça améliore les performances locales (les utilisateurs de Springfield s'authentifient sur leur RODC local, pas besoin d'aller jusqu'à Atlantis à chaque fois)
- Si la liaison MPLS tombe temporairement, les utilisateurs de Springfield peuvent quand même travailler

VLAN 160 : Backup - Le système de sauvegarde du labo

Même logique que le VLAN 40 d'Atlantis : isolation maximale du système de sauvegarde.

Ordre	Source	Destination	Protocole	Action	Description
220	TRUENAS-02	VLAN 110/120/130/150	SMB/SSH/etc.	Autoriser	TrueNAS lance les sauvegardes des équipements du labo
999	Any	Any	Any	Interdire (Drop)	Tout le reste : interdit

TABLE 7.13 – Règles de filtrage VLAN 160 - Backup

La protection anti-ransomware

Encore une fois, on applique le principe du flux unidirectionnel : seul TrueNAS peut initier des connexions, jamais l'inverse. C'est notre protection principale contre les ransomwares qui voudraient chiffrer nos sauvegardes.

De plus, TrueNAS-02 réplique quotidiennement ses sauvegardes vers TrueNAS-01 à Atlantis. Donc même si le labo entier était détruit (incendie, inondation...), on pourrait récupérer les données depuis Atlantis.

7.2.6 Vue d'ensemble : la matrice d'autorisation inter-VLAN

Pour avoir une vue globale de qui peut parler à qui, voici un tableau récapitulatif des autorisations entre VLANs du site Atlantis. C'est comme un tableau de permissions : chaque case indique si un VLAN source (en ligne) peut communiquer avec un VLAN destination (en colonne).

Destination → / Source ↓	VLAN 10 (Admin)	VLAN 20 (App)	VLAN 30 (Utilisateurs)	VLAN 40 (Backup)	VLAN 50 (DMZ/VPN)	VLAN 60 (Imprimantes)	VLAN 66 (Management)
VLAN 10 (Admin)	Propre VLAN	Autoriser	Bloquer	Autoriser	Bloquer	Bloquer	Autoriser
VLAN 20 (App)	Autoriser	Propre VLAN	Bloquer	Autoriser	Bloquer	Bloquer	Autoriser
VLAN 30 (Utilisateurs)	Autoriser	Autoriser	Propre VLAN	Bloquer	Bloquer	Autoriser	Bloquer
VLAN 40 (Backup)	Autoriser	Autoriser	Bloquer	Propre VLAN	Bloquer	Bloquer	Bloquer
VLAN 50 (DMZ/VPN)	Autoriser	Autoriser	Bloquer	Bloque	Propre VLAN	Bloquer	Bloquer
VLAN 60 (Imprimantes)	Bloquer	Bloquer	Autoriser	Bloquer	Bloquer	Propre VLAN	Bloquer
VLAN 66 (Management)	Bloquer	Bloquer	Bloquer	Bloquer	Bloquer	Bloquer	Propre VLAN

FIGURE 7.1 – Matrice d'autorisation inter-VLAN site Atlantis

Comment lire cette matrice ?

Prenons un exemple : cherchez la ligne "VLAN 30 (Utilisateurs)" et la colonne "VLAN 10 (Admin)". Vous voyez un ? Ça veut dire que les utilisateurs peuvent initier des connexions vers le VLAN Administration (pour accéder au serveur de fichiers par exemple).

Maintenant, regardez l'inverse : ligne "VLAN 10 (Admin)" et colonne "VLAN 30 (Utilisateurs)". Vous voyez un ? Ça veut dire que les serveurs d'administration ne peuvent PAS initier de connexions vers les postes utilisateurs. C'est volontaire : on ne veut pas qu'un serveur se connecte aux postes de travail, ce serait bizarre et potentiellement dangereux.

Les grands principes qui ressortent de cette matrice :

- Les VLANs Backup (40) et Management (66) sont comme des bunkers : personne ne peut les atteindre (sauf pour le Management depuis lui-même, évidemment)
- Les utilisateurs (VLAN 30) peuvent consommer des services (Admin, App, Imprimantes) mais ne peuvent pas accéder à l'infrastructure sensible
- Les imprimantes (VLAN 60) sont dans leur bulle : elles ne peuvent parler qu'aux utilisateurs, et uniquement en réponse
- Les serveurs (VLANs 10 et 20) peuvent se sauvegarder (accès au VLAN 40) mais ne peuvent pas initier de connexions vers les utilisateurs
- Le VPN (VLAN 50) a un accès limité : uniquement aux services dont les télétravailleurs ont vraiment besoin

Cette segmentation stricte fait qu'un attaquant qui compromet un poste utilisateur se retrouve coincé dans le VLAN 30. Il ne peut pas rebondir vers les serveurs d'administration ou les sauvegardes. Ça limite considérablement les dégâts potentiels d'une intrusion.

7.2.7 La liaison MPLS entre nos deux sites : un lien sécurisé et performant

Nos deux sites, Atlantis et Springfield, ne sont pas des îlots isolés. Ils doivent communiquer entre eux de manière fluide et sécurisée. Pour ça, on a opté pour une liaison MPLS plutôt qu'un VPN classique. Voyons pourquoi et comment on gère cette liaison.

Qu'est-ce que le MPLS et pourquoi on l'a choisi ?

MPLS (MultiProtocol Label Switching), c'est un peu comme une autoroute privée entre nos deux sites. Contrairement à un VPN qui passerait par Internet public, le MPLS nous offre une liaison dédiée fournie par notre opérateur télécom.

Nos caractéristiques techniques :

- **Bandé passante** : 100 Mbps garantis dans les deux sens. "Garanti" est le mot important ici : ce n'est pas du "jusqu'à 100 Mbps", c'est 100 Mbps disponibles en permanence
- **Latence** : Moins de 10 millisecondes entre Atlantis et Springfield. Ça donne une impression de quasi-instantanéité
- **Disponibilité** : SLA (Service Level Agreement) à 99,9%. Ça signifie que l'opérateur s'engage contractuellement à moins de 9 heures de panne par an
- **Sécurité** : Le réseau MPLS est privé, complètement isolé d'Internet. Nos données ne traversent jamais le réseau public

Quels flux passent par notre liaison MPLS ?

On n'a pas connecté n'importe quoi n'importe comment via MPLS. Chaque flux autorisé répond à un besoin métier précis et est strictement contrôlé. Voici les cinq types de flux qui circulent entre nos sites :

1. La réPLICATION de l'Active Directory

C'est le flux le plus critique. Nos contrôleurs de domaine doivent rester synchronisés pour que les utilisateurs des deux sites puissent se connecter, que les droits d'accès soient cohérents, et que l'annuaire global reste à jour.

- Depuis : DC-03 (le RODC de Springfield)
- Vers : DC-01 et DC-02 (les contrôleurs maîtres d'Atlantis)
- Protocoles utilisés :
 - Kerberos (port 88) pour l'authentification
 - LDAP (ports 389 et 636) pour les requêtes d'annuaire
 - DNS (port 53) pour la résolution de noms
 - RPC (port 135) pour la communication entre contrôleurs
- Fréquence : La réPLICATION se fait automatiquement toutes les 15 minutes, ou immédiatement en cas de changement important

2. L'accès à l'ERP depuis Springfield

Les employés du laboratoire doivent pouvoir utiliser l'ERP comme leurs collègues d'Atlantis pour gérer leurs activités quotidiennes.

- Depuis : Les postes du VLAN 120 (utilisateurs labo)

- Vers : Le serveur ERP-APP dans le VLAN 20 d'Atlantis
- Protocole : HTTPS sur le port 443 (connexion chiffrée)
- Usage : Consultation des stocks, saisie des rapports d'expérience, gestion administrative

3. Le partage de documents entre sites

La collaboration entre le bureau d'études d'Atlantis et le laboratoire de Springfield nécessite un accès aux fichiers techniques.

- Depuis : VLAN 120 (labo Springfield)
- Vers : Serveur de fichiers FS-01 dans le VLAN 10 d'Atlantis
- Protocole : SMB (port 445), le protocole de partage de fichiers Windows
- Mode d'accès : Lecture seule pour le labo. Ils peuvent consulter et télécharger les documents, mais pas les modifier directement sur le serveur
- Raison du mode lecture seule : On évite ainsi les conflits de versions et les modifications accidentelles. Si le labo a besoin de modifier un document, ils le téléchargent, le modifient localement, et le renvoient au bureau d'études

4. Le pilotage des équipements de laboratoire

Les ingénieurs du bureau d'études à Atlantis peuvent lancer des tests sur les équipements du labo sans se déplacer à Springfield.

- Depuis : VLAN 30 d'Atlantis (spécifiquement les postes du bureau d'études)
- Vers : VLAN 130 de Springfield (les équipements de test)
- Protocoles : Variables selon les équipements (HTTP, Modbus TCP, SCPI, parfois des protocoles propriétaires)
- Cas d'usage typique : Un ingénieur configure un test le matin, lance les mesures à distance, et récupère les résultats quelques heures plus tard sans avoir à faire l'aller-retour jusqu'au labo

5. La réPLICATION DES SAUVEGARDES

C'est notre filet de sécurité ultime : les sauvegardes de chaque site sont répliquées sur l'autre site.

- Depuis : TRUENAS-01 (Atlantis)
- Vers : TRUENAS-02 (Springfield)
- Protocole : SSH (port 22) pour des transferts sécurisés via rsync ou ZFS send
- Fréquence : Une fois par jour, pendant la nuit pour ne pas encombrer la liaison pendant les heures de travail
- Objectif : Si un site entier était détruit (incendie, inondation, catastrophe naturelle...), on pourrait reconstituer ses données depuis l'autre site

Les règles de filtrage spécifiques au MPLS

Même si le MPLS est une liaison privée, on ne fait pas confiance aveuglément. On applique des règles de filtrage strictes sur les pare-feux pour contrôler exactement ce qui peut passer par cette liaison.

Ordre	Source	Destination	Protocole	Action	Description
400	DC-03 (Springfield)	DC-01/02 (At-lantis)	Ports AD	Autoriser	Synchronisation de l'annuaire Active Directory
410	VLAN 120 (Springfield)	VLAN 20 (At-lantis)	HTTPS (443)	Autoriser	Les utilisateurs du labo accèdent à l'ERP
420	VLAN 120 (Springfield)	VLAN 10 (At-lantis)	SMB (445)	Autoriser	Consultation des documents techniques
430	VLAN 30 (At-lantis)	VLAN 130 (Springfield)	Spécifique	Autoriser	Pilotage des équipements de test
440	TRUENAS-01 (Atlantis)	TRUENAS-02 (Springfield)	SSH (22)	Autoriser	RéPLICATION quotidienne des sauvegardes
999	Any	Any	Any	Interdire (Drop)	Tout le reste est bloqué par défaut

TABLE 7.14 – Règles de filtrage pour la liaison MPLS inter-sites

Notez que malgré le "réseau privé", on applique quand même notre principe fondamental : tout est interdit sauf ce qui est explicitement autorisé. Même entre nos propres sites, on ne fait pas de confiance aveugle.

Pourquoi le MPLS plutôt qu'un VPN IPsec ?

On aurait pu opter pour une solution VPN IPsec classique passant par Internet. C'est d'ailleurs ce que font beaucoup d'entreprises. Mais le MPLS nous offre des avantages significatifs pour notre cas d'usage :

Les avantages du MPLS dans notre contexte

1. Performance prévisible

Avec Internet, on ne sait jamais : parfois c'est rapide, parfois ça rame. Avec le MPLS, on a une bande passante garantie et une latence constante. Crucial quand nos ingénieurs pilotent des équipements de test en temps réel.

2. Pas de surcharge de chiffrement

Un VPN IPsec doit chiffrer et déchiffrer tous les paquets, ce qui consomme de la puissance processeur et ajoute de la latence. Avec le MPLS, le réseau est déjà privé, donc pas besoin de cette surcharge.

3. Qualité de Service (QoS)

On peut prioriser certains types de trafic. Par exemple, la réPLICATION Active Directory passe avant le transfert de gros fichiers. Avec Internet, impossible de garantir ça.

4. Configuration simplifiée

Pas de tunnel VPN à gérer, pas de certificats à renouveler, pas de problèmes de MTU ou de fragmentation. La liaison MPLS est transparente : nos deux sites apparaissent comme un seul réseau étendu.

5. Support opérateur

Si on a un problème, on peut appeler notre opérateur télécom qui a contractuellement obligation de le résoudre rapidement. Avec Internet public, on est seuls.

Bien sûr, le MPLS coûte plus cher qu'une connexion Internet classique. Mais pour une infrastructure critique comme la nôtre, c'est un investissement justifié par la fiabilité et les performances qu'il apporte.

La surveillance de notre liaison MPLS

Une liaison, aussi bonne soit-elle, doit être surveillée. Nos pare-feux OPNsense génèrent des logs détaillés sur tout ce qui passe par le MPLS :

- **Journalisation exhaustive** : Chaque connexion autorisée ou bloquée est enregistrée avec l'heure, la source, la destination, le protocole et l'action prise
- **Alertes en temps réel** : Si quelqu'un essaie d'utiliser un port ou un protocole non autorisé via le MPLS, on reçoit immédiatement une alerte. Ça pourrait être le signe d'une machine compromise qui essaie de se propager à l'autre site
- **Statistiques de bande passante** : On suit en continu l'utilisation de la bande passante par VLAN. Si le VLAN utilisateurs consomme soudainement 80% de la bande passante MPLS, c'est anormal et on enquête
- **Détection d'anomalies** : Notre système de monitoring (qu'on détaillera au chapitre 9) analyse les patterns de trafic. Un pic inhabituel à 3h du matin ? Un serveur qui envoie soudainement 10 fois plus de données que d'habitude ? Ça déclenche une alerte
- **Intégration centralisée** : Tous ces logs sont remontés vers notre solution de supervision centralisée où ils sont corrélés avec les événements des autres systèmes pour avoir une vue d'ensemble de la sécurité

Cette surveillance continue nous permet de détecter rapidement tout problème de sécurité ou de performance sur notre liaison inter-sites, qui est vraiment l'épine dorsale de notre infrastructure distribuée.

Voilà, on a fait le tour complet de notre sécurité périphérique et de notre politique de filtrage. Ça peut paraître lourd et compliqué à première vue, mais chaque règle a sa raison d'être, forgée par l'expérience et les meilleures pratiques du secteur. L'objectif, c'est d'avoir un système à la fois sécurisé et utilisable : on protège l'infrastructure sans empêcher les gens de travailler efficacement. C'est tout l'art de la sécurité informatique moderne !

Chapitre 8

Stratégie de Sauvegarde

8.1 Fondamentaux

8.1.1 Enjeux de la continuité d'activité

La stratégie de sauvegarde constitue un pilier essentiel de la continuité d'activité de XANADU. L'entreprise fait face à plusieurs contraintes critiques :

- **Données sensibles** : RH, juridique, finances nécessitant protection maximale
- **Disponibilité critique** : RTO de 4h maximum pour services critiques
- **Architecture multi-sites** : Atlantis et Springfield reliés par MPLS
- **Menace ransomware** : Préoccupation principale du directeur
- **Budget limité** : PME de 60 personnes sans équipe IT dédiée

8.1.2 Politique 3-2-1-1-0

XANADU applique la stratégie de sauvegarde 3-2-1-1-0 :

- **3 copies minimum** : Production + 2 sauvegardes
- **2 supports différents** : TrueNAS + bandes LTO
- **1 copie hors site** : Réplication Atlantis Springfield via MPLS
- **1 copie offline** : Bandes LTO mensuelles déconnectées
- **0 erreur** : Scrub ZFS hebdomadaire avec checksum SHA256

8.1.3 Objectifs RTO et RPO

Le RTO (Recovery Time Objective) définit le délai maximum de restauration, tandis que le RPO (Recovery Point Objective) indique la perte de données acceptable. Ces objectifs sont définis selon la criticité des services : les systèmes critiques (ERP, AD) bénéficient d'un RTO de 4h et d'un RPO de 1h grâce aux sauvegardes horaires, tandis que les services moins critiques tolèrent des délais plus longs.

Services	RTO	RPO	Solution
Critiques (ERP, AD)	4h	1h	Sauvegarde horaire + quotidienne
Importants (Fichiers)	24h	4h	Sauvegarde semi-quotidienne + mensuelle
Standard (Personnel)	48h	24h	Sauvegarde triquotidienne + mensuelle

TABLE 8.1 – Objectifs RTO/RPO par criticité

8.1.4 Protection anti-ransomware

Mesures déployées :

- **Snapshots ZFS immutables** : Impossibles à modifier ou chiffrer
- **Copies offline LTO** : Bandes physiquement déconnectées
- **Isolation réseau** : VLAN 40 (Atlantis) et 160 (Springfield) dédiés
- **RBAC strict** : 3 rôles (Administrateur, Opérateur, Auditeur)
- **Sauvegardes lecture seule** : Write-once-read-many

8.2 Mise en œuvre technique

8.2.1 Choix de la solution

Solutions évaluées

1. **TrueNAS SCALE avec ZFS** : Open-source, Linux + ZFS
2. **Veeam Backup & Replication** : Leader marché virtualisation
3. **Bacula Enterprise** : Solution professionnelle souveraine
4. **Acronis Cyber Protect** : Intégré backup + sécurité

Critères d'évaluation (par ordre d'importance)

1. Souveraineté des données (données sensibles RH/juridique/finances)
2. Protection anti-ransomware (préoccupation principale directeur)
3. Fiabilité RTO/RPO (exigence contractuelle stricte)
4. Compatibilité multi-sites (architecture 2 sites + MPLS)
5. Coût total (budget PME limité)
6. Facilité installation/maintenance (correspondants IT non-experts)
7. Intégration existant (infrastructure mixte Windows/Linux)
8. Scalabilité (croissance prévue)

Histogramme d'évaluation

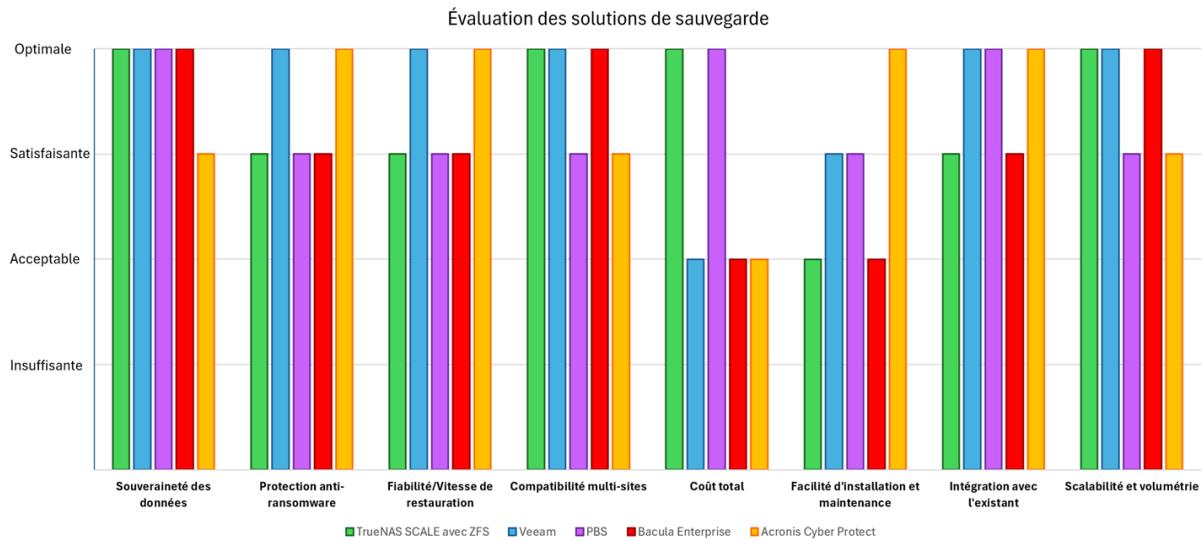


FIGURE 8.1 – Histogramme d'évaluation des solutions de sauvegarde

Justification du choix : TrueNAS SCALE

TrueNAS SCALE + ZFS répond parfaitement aux 3 critères prioritaires :

1. Souveraineté des données (10/10)

- Solution 100% open-source
- Données exclusivement sur sites Atlantis et Springfield
- Aucune dépendance éditeur ou cloud externe

2. Protection anti-ransomware maximale (10/10)

- Snapshots ZFS immutables
- Architecture copy-on-write
- Copie offline LTO mensuelle
- Isolation VLAN 40/160

3. Fiabilité et coût maîtrisé (9/10 et 10/10)

- ZFS ultra-fiable avec auto-réparation
- Coût total : 22 200 € sans licence annuelle
- Déduplication 2.5 :1 optimise l'espace
- Interface intuitive pour correspondants IT

8.2.2 Infrastructure de sauvegarde

Topologie

Site Atlantis (Principal)

- Serveur TrueNAS : backup-atlantis (10.0.40.10/24)
- VLAN 40 dédié Backup
- Liaison MPLS 1 Gbps vers Springfield

Site Springfield (Secondaire)

- Serveur TrueNAS : backup-springfield (10.1.60.10/24)
- VLAN 160 dédié Backup
- Liaison MPLS 1 Gbps vers Atlantis

Spécifications matérielles

Chaque serveur :

- **CPU** : Intel Xeon / AMD EPYC (8+ coeurs)
- **RAM** : 64 Go (déduplication nécessite 5 Go/To)
- **Stockage** : 6× 4 To en RAID-Z2 (16 To utilisables)
- **Cache L2ARC** : 2× SSD NVMe 1 To
- **Réseau** : 2× 10GbE redondant
- **Onduleur** : APC 3000VA (30 min autonomie)

Capacité effective : 16 To × 2.5 (déduplication) × 1.8 (compression) 72 To

Coût total

Composant	Prix (€)
Serveur TrueNAS Atlantis	8 500
Serveur TrueNAS Springfield	8 500
Lecteur LTO-8	3 000
Bandes LTO-8 (×10)	600
Onduleurs (×2)	1 200
Installation	400
Total	22 200

TABLE 8.2 – Budget infrastructure sauvegarde

8.2.3 Configuration ZFS

Caractéristiques ZFS

- **Copy-on-Write** : Données existantes jamais écrasées, snapshots instantanés
- **Intégrité native** : Checksum SHA256 sur chaque bloc, auto-réparation
- **Pool unifié** : Tous disques contribuent à espace cohérent

RAID-Z2

- **Configuration** : 6 disques 4 To → 16 To utilisables (double parité)
- **Tolérance** : 2 disques défaillants simultanés sans perte
- **Avantage vs RAID-Z1** : Élimine fenêtre vulnérabilité rebuild (24-48h)

Paramètres pool : ashift=12 (secteurs 4K), compression=lz4, dedup=sha256, atime=off

Déduplication et compression

Déduplication : Hash SHA256 par bloc, référence si existant

- Ratio attendu : 2.5 :1 (fichiers système Windows répétitifs)
- RAM nécessaire : 5 Go par To de données uniques

Compression LZ4 : Ultra-rapide (>2 GB/s décompression), overhead <3%

- Ratio moyen : 1.5-2 :1
- Gain cumulatif : $2.5 \times 1.8 = 4.5 :1$ total

Vérification :

```
zpool list -o name,size,alloc,free,dedup,compressratio
```

Scrub hebdomadaire

Vérification proactive intégrité (dimanche 01 :00, seuil 35 jours) :

- Lecture tous blocs + validation checksums
- Auto-réparation corruptions via RAID-Z2
- Détection "bit rot" (rayonnement cosmique, dégradation magnétique)
- Durée : 6-8h pour 8 To, impact 10-15%

8.2.4 Politique de rétention

Criticité	Fréquence	Rétention	Planification
Critique	Horaire	48h	Toutes les heures
	Quotidien	14 jours	3h00
	Hebdomadaire	8 semaines	Dimanche 2h00
	Mensuel	24 mois	1er mois 3h00
Important	Semi-quotidien	7 jours	12h15 et 3h00
	Mensuel	12 mois	1er mois 3h00
Standard	Triquotidien	3 semaines	Tous les 3 jours 3h00
	Mensuel	12 mois	1er mois 3h00

TABLE 8.3 – Programmation des sauvegardes par criticité

8.2.5 RéPLICATION inter-sites

Configuration

- **Source** : backup-atlantis
- **Destination** : backup-springfield
- **Planification** : Quotidienne 23h30 (post-sauvegardes)
- **Chiffrement** : SSH + TLS
- **Bandé passante** : Limitée à 500 Mbps

Type	Fréquence	Méthode	Cible
Complète	Mensuelle	ZFS send complet	Bandé LTO + Springfield
Incrémentale	Quotidienne	ZFS send -i	Springfield
Differentielle	Hebdomadaire	ZFS send -I	Intermédiaire

TABLE 8.4 – Stratégie de réPLICATION

Types de réPLICATION

8.2.6 Sauvegardes offline (LTO)

Configuration bandes LTO-8

- **Set** : 10 bandes (LTO-01 à LTO-10)
- **Rotation** : Mensuelle, réutilisation après 10 mois
- **Durée vie** : 3 ans maximum
- **Stockage** : Coffre-fort ignifuge hors site
- **Vérification** : Intégrité mensuelle

Procédure Script automatisé (1er mois 3h00) : snapshot complet → compression gzip → copie LTO → éjection

8.2.7 Analyse AMDEC

L'analyse AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité) évalue les risques pesant sur l'infrastructure de sauvegarde. Chaque risque est noté selon sa gravité (G), sa fréquence (F) et sa détectabilité (D), produisant un indice de criticité ($C = G \times F \times D$). Les trois risques prioritaires identifiés sont le ransomware ($C=30$), la défaillance des bandes LTO ($C=18$) et la panne du serveur principal ($C=16$), nécessitant des actions préventives renforcées.

Priorités : Ransomware ($C=30$), Bandes LTO ($C=18$), Panne serveur ($C=16$)

8.2.8 Validation RTO/RPO

Paramètres

- Débit local TrueNAS : 800 MB/s
- Débit MPLS inter-sites : 62.5 MB/s (500 Mbps)

Défaillance	Causes	Effets	G	F	D	C	Actions
Panne TrueNAS Atlantis	Défaillance HW, surtension	Perte sauvegarde principale	4	2	2	16	Monitoring CheckMK 24/7, Onduleur, Bascule Springfield
Rupture MPLS	Coupe opérateur	Réplication impossible	3	2	1	6	Monitoring liaison, Synchro différée
Corruption pool ZFS	Erreur disque, bug	Données irrécupérables	5	1	2	10	Scrub hebdo, RAID-Z2, SHA256, LTO
Saturation disque	Croissance non anticipée	Échec sauvegardes	4	2	1	8	Monitoring 80%, Dédup 2.5 :1, Purge auto
Ransomware	Phishing, vulnérabilité	Chiffrement sauvegardes	5	3	2	30	Snapshots immutables, VLAN isolé, LTO, RBAC
Erreurs humaines	Mauvaise manipulation	Érassement données	3	2	2	12	Procédure, Test mensuel, Validation
Panne électrique	Coupe secteur	Arrêt systèmes	3	1	1	3	Onduleur 30min, Groupe électrogène, Shutdown auto
Défaillance LTO	Usure, stockage	Perte offline	3	2	3	18	Rotation 3 ans, Coffre ignifuge, Test mensuel
Perte clés chiffrement	Vol, destruction	Restauration impossible	5	1	1	5	HSM/coffre, Double, Escrow

TABLE 8.5 – AMDEC - Analyse des risques ($G \times F \times D$, seuil alerte >15)

Temps de restauration

Service	Volume	RTO	Local	MPLS
Critiques (ERP, AD)	500 GB	4h	40 min	3h
Importants (Fichiers)	3 TB	24h	2h	16h
Standard (Personnel)	1.5 TB	48h	1h15	8h

TABLE 8.6 – Validation RTO (tous objectifs respectés même en restauration distante)

8.2.9 Sécurité et contrôle d'accès

Chiffrement

- **Algorithm** : AES-256-GCM (confidentialité + intégrité)
- **Gestion clés** : HSM ou coffre physique sécurisé
- **Rotation** : Annuelle

RBAC

- **Administrateur** : Gestion complète (2FA obligatoire)
- **Opérateur** : Lancement sauvegardes, consultation logs
- **Auditeur** : Lecture seule

8.2.10 Monitoring CheckMK

Métriques supervisées

- Santé pool ZFS, disques défaillants
- Espace disponible (seuil 80%)
- Statut sauvegardes, réplication
- Performance (IOPS, latence)
- SMART disques

Alertes

- **Critical** : Email + SMS (espace >90%, 2 disques HS)
- **Warning** : Email (espace >80%, 1 échec sauvegarde)
- Anti-saturation : délai 30 min, regroupement 5 min

8.2.11 TCO sur 5 ans

Le coût total de possession (TCO) sur 5 ans inclut l'investissement initial de 22 200 € et les coûts d'exploitation annuels de 3 200 € (électricité, bandes LTO, maintenance). Le TCO total s'élève à 38 200 €, soit 7 640 € par an ou 127 € par utilisateur et par an. Cette solution représente une économie de 36 à 47% par rapport aux alternatives commerciales comme Veeam, Acronis ou une solution cloud pure.

Poste	Coût (€)
Investissement initial	22 200
Coûts annuels (électricité, bandes, maintenance)	3 200/an
Total 5 ans	38 200
Par an	7 640
Par utilisateur/an	127

TABLE 8.7 – TCO - Économie 36-47% vs Veeam/Acronis/Cloud

Chapitre 9

Supervision et Monitoring

9.1 Fondamentaux

9.1.1 Définition de la supervision informatique

La supervision informatique consiste à surveiller en temps réel l'état de santé d'un système d'information. Concrètement, il s'agit d'observer en permanence le fonctionnement des serveurs, des équipements réseau, des applications et des services pour détecter immédiatement toute anomalie ou dégradation des performances.

Imaginez la supervision comme un tableau de bord de voiture : au lieu de vérifier manuellement le niveau d'huile, la pression des pneus ou la température du moteur, vous disposez d'indicateurs qui vous alertent instantanément en cas de problème. C'est exactement le même principe pour une infrastructure informatique.

Pour XANADU, la supervision prend tout son sens avec l'infrastructure multi-sites déployée. Il devient essentiel de pouvoir observer simultanément l'état des contrôleurs de domaine DC-01, DC-02 et DC-03, des pare-feux OPNsense, des systèmes de sauvegarde TrueNAS sur les deux sites, et de l'ensemble des services critiques comme l'ERP. Sans cette vision globale, l'équipe informatique navigue à l'aveugle et ne peut que constater les problèmes une fois que les utilisateurs s'en plaignent.

9.1.2 Enjeux de la supervision proactive

La supervision proactive représente un changement fondamental dans la manière de gérer un système d'information. Au lieu de réagir aux incidents après qu'ils se soient produits, l'objectif est de les anticiper et de les prévenir avant qu'ils n'impactent les utilisateurs.

Dans la situation actuelle de XANADU, l'équipe informatique fonctionne en mode purement réactif. Une sauvegarde peut échouer pendant plusieurs semaines sans que personne ne s'en aperçoive. Un disque dur peut se remplir progressivement jusqu'à saturation totale, provoquant un blocage complet du service. Un contrôleur de domaine peut tomber en panne la nuit sans qu'aucune alerte ne soit déclenchée. Résultat : l'équipe découvre les problèmes avec plusieurs heures, voire plusieurs jours de retard, ce qui rallonge considérablement les temps de résolution et génère un stress permanent.

La supervision proactive inverse cette logique. Elle permet de détecter les signaux faibles avant qu'ils ne deviennent des incidents majeurs. Par exemple, si un disque commence à montrer des signes de défaillance matérielle, la supervision va alerter l'équipe

plusieurs jours avant la panne effective, laissant le temps de remplacer le composant défaillant pendant une fenêtre de maintenance planifiée plutôt que dans l'urgence à 3 heures du matin.

Pour XANADU, cela signifie concrètement pouvoir observer que l'espace disque du serveur de fichiers FS-01 atteint 75% de sa capacité et planifier une extension de stockage, plutôt que d'attendre le blocage à 100%. Cela permet également de surveiller que les trois contrôleurs de domaine communiquent correctement entre eux et que la réPLICATION Active Directory fonctionne normalement entre Atlantis et Springfield.

9.1.3 Importance pour le respect des RTO

Le respect des objectifs de temps de reprise (RTO) fixés par la direction de XANADU repose intégralement sur une supervision efficace. Rappelons que XANADU s'est engagé sur un RTO de 4 heures maximum pour les services critiques comme l'ERP et Active Directory, et de 24 heures pour les autres services.

Ces délais peuvent sembler confortables, mais dans la réalité d'un incident, chaque minute compte. Le chronomètre ne démarre pas au moment où l'équipe informatique commence à résoudre le problème, mais dès l'instant où le service devient indisponible. Sans supervision, un incident survenu à 2 heures du matin ne sera découvert qu'à 8 heures lorsque les utilisateurs arrivent au bureau et signalent le problème. Dans ce scénario, 6 heures précieuses ont déjà été perdues avant même de commencer à intervenir.

La supervision change complètement cette équation. Grâce aux alertes automatiques, l'équipe informatique est prévenue immédiatement par SMS, email ou notification, quelle que soit l'heure. Le technicien d'astreinte peut alors commencer son diagnostic dès les premières minutes de l'incident, maximisant ainsi les chances de respecter le RTO de 4 heures.

Mais l'importance de la supervision pour le RTO ne se limite pas à la détection rapide. Elle fournit également des informations précieuses pour le diagnostic. Lorsqu'un incident survient, les graphiques historiques permettent de comprendre rapidement ce qui s'est passé. Par exemple, si le contrôleur de domaine DC-01 ne répond plus, la supervision montrera peut-être que la mémoire RAM était saturée depuis plusieurs heures, ou que le nombre de requêtes DNS avait explosé suite à une attaque. Ces informations accélèrent considérablement le processus de résolution.

Pour XANADU, avec son infrastructure distribuée sur deux sites reliés par MPLS, la supervision permet également de localiser immédiatement l'origine d'un problème : est-ce un incident local à Atlantis, un problème sur le site de Springfield, ou un dysfonctionnement de la liaison inter-sites ? Cette rapidité de diagnostic est déterminante pour tenir les engagements de service.

9.1.4 Traçabilité et audit

La traçabilité constitue le dernier pilier fondamental de la supervision, souvent sous-estimé mais absolument essentiel. Il s'agit de conserver un historique détaillé de l'état du système d'information sur plusieurs mois, voire plusieurs années, pour pouvoir analyser, comprendre et justifier a posteriori.

Cette fonction d'historisation répond à plusieurs besoins critiques pour XANADU. D'abord, elle permet l'analyse post-incident. Lorsqu'un problème survient, il est rarement isolé. En consultant l'historique, on peut découvrir que le même type d'alerte s'était déjà

produit trois semaines auparavant, permettant d'identifier une tendance ou une cause racine qui aurait sinon échappé à l'analyse. Par exemple, si le serveur de sauvegarde TrueNAS affiche régulièrement des pics d'utilisation CPU le mardi soir, cela peut révéler un conflit entre plusieurs tâches de sauvegarde programmées au même moment.

La traçabilité joue également un rôle déterminant dans la planification de l'évolution de l'infrastructure. Grâce aux données historiques, l'équipe informatique peut prouver factuellement à la direction que les serveurs virtuels atteignent régulièrement 90% d'utilisation de leur RAM, justifiant ainsi un investissement dans de la mémoire supplémentaire. Ces données chiffrées sont infiniment plus convaincantes qu'une simple intuition ou qu'un ressenti basé sur quelques observations ponctuelles.

Pour XANADU, la traçabilité revêt une importance particulière dans le contexte des exigences de continuité d'activité. En cas d'incident majeur comme un ransomware, les logs de supervision permettront de reconstituer précisément le déroulé de l'attaque : quand l'intrusion a-t-elle commencé ? Par quel vecteur ? Quels systèmes ont été compromis et dans quel ordre ? Ces informations sont essentielles non seulement pour restaurer le système de manière sécurisée, mais aussi pour faire valoir une éventuelle assurance cyber ou pour apporter des éléments factuels dans un contexte juridique.

Enfin, la traçabilité facilite grandement les audits de conformité. Si XANADU doit un jour prouver qu'elle a effectivement sauvegardé ses données critiques tous les jours pendant l'année écoulée, ou démontrer que ses systèmes de sécurité ont bien fonctionné en permanence, les historiques de supervision fourniront ces preuves de manière incontestable. C'est la différence entre dire « nous pensons avoir bien fait notre travail » et pouvoir affirmer « voici les données qui prouvent que nous avons respecté nos engagements ».

9.2 Mise en œuvre technique

9.2.1 Analyse de l'existant

XANADU ne dispose d'aucun système de supervision digne de ce nom. Actuellement, la détection des problèmes se fait uniquement après coup, ce qui compromet gravement la capacité de l'entreprise à respecter ses objectifs de RTO.

État actuel de la supervision

L'existant chez XANADU :

- Quelques scripts PowerShell gèrent les sauvegardes, mais sans aucun contrôle pour vérifier qu'elles se sont bien déroulées
- Consultation manuelle et ponctuelle des interfaces d'administration (ESXi, NAS, etc.)
- Aucun système d'alerte automatique lors de la survenue d'un problème
- Absence de traçabilité et d'historique des événements système

Impacts de la situation actuelle

Conséquences critiques

- **Détection tardive** : Les pannes sont découvertes plusieurs heures, voire plusieurs jours après leur survenue
- **RTO compromis** : L'objectif de 4 heures exigé par la direction devient totalement irréaliste
- **Manque de visibilité** : Aucune vision sur l'évolution des ressources critiques (saturation progressive des disques, dégradation des performances)
- **Sauvegardes non surveillées** : Des sauvegardes peuvent échouer pendant plusieurs semaines sans que l'équipe en soit informée
- **Gestion réactive** : L'équipe IT fonctionne en permanence dans l'urgence au lieu de pouvoir anticiper les incidents

Manques identifiés

Le diagnostic met en évidence les carences suivantes :

- **Vision temps réel** : Impossible d'obtenir une vue d'ensemble instantanée de l'état du système d'information
- **Alertes proactives** : Personne n'est averti automatiquement lorsqu'un seuil critique est franchi
- **Données historiques** : Absence totale de métriques pour justifier les investissements ou préparer les budgets
- **Supervision centralisée** : Avec l'intégration du site de Springfield, XANADU a besoin de tout piloter depuis une interface unique
- **Traçabilité des incidents** : Impossible de reconstituer précisément le déroulé d'un problème après coup

9.2.2 Analyse des besoins

L'analyse des besoins en supervision s'articule autour de plusieurs axes stratégiques pour garantir la disponibilité du système d'information et le respect des engagements de service.

Besoins fonctionnels exprimés

Les objectifs de la supervision sont les suivants :

- Déetecter les problèmes **avant** que les utilisateurs ne s'en plaignent
- Garantir les délais de remise en service (RTO de 4 heures pour les services critiques, 24 heures pour les services standards)
- Disposer d'un tableau de bord compréhensible permettant une vision d'ensemble instantanée
- Collecter des métriques concrètes pour justifier les demandes de matériel ou de budget

Éléments à superviser

Serveurs et infrastructure :

- Contrôleurs de domaine (DC-01, DC-02, DC-03) :
 - Espace disque disponible
 - Fonctionnement de l'Active Directory, DNS et DHCP
 - État de la réplication entre contrôleurs
 - Délais d'authentification
- Hyperviseur ESXi :
 - État de santé du serveur physique
 - État des machines virtuelles hébergées
 - Utilisation du stockage et des ressources
- Serveur ERP :
 - Temps de réponse de l'application
 - Performances de la base de données
 - Disponibilité des services
- Serveur de fichiers (FS-01) :
 - Taux de remplissage des disques
 - Indicateurs SMART pour anticiper les pannes
 - Disponibilité des partages SMB

Infrastructure réseau :

- Liaison MPLS (Atlantis Springfield) :
 - Latence (objectif : < 50ms)
 - Gigue (objectif : < 10ms)
 - Perte de paquets (objectif : < 0,1%)
- Équipements réseau :
 - Pare-feux OPNsense (Atlantis et Springfield)
 - Routeurs MPLS
 - Switchs des deux sites

Services applicatifs :

- Interface web de l'ERP
- Partages de fichiers réseau
- Services Office 365

Système de sauvegarde :

- Statut de chaque sauvegarde (succès/échec)
- Fraîcheur des sauvegardes (dernière copie < 24h)
- Volumétrie des données sauvegardées
- Espace de stockage disponible

Site de Springfield :

- Contrôleur de domaine DC-03 (RODC)
- Serveurs Linux du laboratoire
- Infrastructure réseau locale

Contrainte	Description
Budget limité	Solution gratuite privilégiée (CheckMK Raw plutôt qu'une version payante)
Délai court	Déploiement rapide nécessaire (présentation semaine 51), solution rapidement opérationnelle
Compétences	Interface accessible sans expertise pointue, courbe d'apprentissage raisonnable
Scalabilité	Solution évolutive pour accompagner la croissance de l'infrastructure
Pérennité	Communauté active et mises à jour régulières garanties

TABLE 9.1 – Contraintes du projet de supervision

Contraintes identifiées

Synthèse des besoins

Aspect	Existant	Besoin	Écart
Détection	Manuelle, a posteriori	Automatique, temps réel	red !30CRI-TIQUE
Alertes	Aucune	Email/SMS selon criticité	red !30CRI-TIQUE
Visibilité	Nulle	Dashboards multi-profil	orange !30MA-JEUR
Historique	Inexistant	90 jours + tendances	orange !30MA-JEUR
Multi-sites	N/A	Supervision Atlantis + Springfield	yellow !30NÉ-CESSAIRE
Traçabilité	Aucune	Logs 90j + rapports RTO	yellow !30IMPOR-TANT

TABLE 9.2 – Écart entre situation actuelle et besoins identifiés

Priorisation de la supervision

- **P1 (impact immédiat)** : Services ERP, contrôleurs de domaine, espace disque serveurs, liaison MPLS, sauvegardes
- **P2 (dégradation rapide)** : Performances serveurs (CPU/RAM), ESXi, NAS/partages réseau, santé matérielle
- **P3 (optimisation)** : Imprimantes, métriques réseau avancées, métriques applicatives

9.2.3 Présentation des solutions étudiées

Quatre solutions de supervision ont été évaluées en fonction des besoins spécifiques de XANADU.

Zabbix

Points forts :

- Solution open source mature et reconnue
- Communauté d'utilisateurs importante et documentation abondante
- Très flexible et personnalisable
- Support natif de la plupart des protocoles (SNMP, ICMP, IPMI, etc.)

Points faibles :

- Courbe d'apprentissage abrupte
- Configuration initiale relativement complexe
- Installation et maintenance demandant des bases solides
- Templates nécessitant souvent des ajustements importants

Nagios / Nagios XI

Points forts :

- Solution très stable et éprouvée depuis de nombreuses années
- Large écosystème de plugins disponibles
- Version Core gratuite et open source

Points faibles :

- Interface graphique très vieillissante
- Configuration via fichiers textes uniquement pour la version Core
- Absence d'auto-découverte des équipements réseau
- Configuration laborieuse pour atteindre un niveau fonctionnel satisfaisant

PRTG Network Monitor

Points forts :

- Interface web très moderne et ergonomique
- Installation simple et rapide sous Windows
- Auto-découverte efficace avec configuration automatique des capteurs
- Support technique commercial réactif

Points faibles :

- Solution commerciale propriétaire avec coûts par capteur
- Moins adaptée aux environnements Linux (limitation pour Springfield)
- Historisation des données limitée dans la version de base
- Coût prohibitif pour une infrastructure de la taille de XANADU

CheckMK

Points forts :

- Interface moderne et intuitive
- Auto-découverte automatique des services avec configuration des seuils
- Version RAW (gratuite) très complète et sans limitation
- Excellente gestion des environnements hétérogènes (Windows/Linux)

- Documentation claire et disponible en français
- Historisation native sur plusieurs mois

Points faibles :

- Moins connu que Zabbix ou Nagios, donc ressources communautaires plus limitées
- Nécessite un serveur Linux pour l'installation

9.2.4 Critères d'évaluation

Nous avons choisi les critères d'évaluation suivants par ordre décroissant d'importance :

1. Coût total

Pourquoi ? PME de 60 personnes, budget limité.

2. Facilité d'installation et maintenance

Pourquoi ? Pas d'équipe IT dédiée, correspondants informatiques par service.

3. Auto-découverte

Pourquoi ? Infrastructure diverse et évolutive (serveurs, VMs, équipements réseau, imprimantes) nécessitant une détection automatique pour réduire la charge de configuration manuelle.

4. Support Windows / Linux

Pourquoi ? Infrastructure hétérogène avec serveurs Windows (DC, DNS, DHCP), serveurs Linux (2 serveurs sur le site distant du laboratoire) et VMs sous ESXi.

5. Adaptabilité à une PME de 60 utilisateurs

Pourquoi ? Solution proportionnée à la taille de l'entreprise (50 utilisateurs sur Atlantis + 10 sur Springfield) sans complexité excessive ni sous-dimensionnement.

6. Courbe d'apprentissage

Pourquoi ? Correspondants informatiques non experts devant administrer la solution sans formation longue, prise en main rapide indispensable.

7. Compatibilité multi-sites

Pourquoi ? Architecture à 2 sites distants avec liaison MPLS.

8. Scalabilité et volumétrie

Pourquoi ? Croissance prévue de l'entreprise.

9.2.5 Histogramme d'évaluation des solutions de supervision

Les solutions ont été évaluées selon huit critères essentiels, notés de 1 (insuffisant) à 4 (optimal).

Note : Bien que PRTG obtienne un bon score, son coût de licence par capteur le disqualifie pour le contexte budgétaire de XANADU.

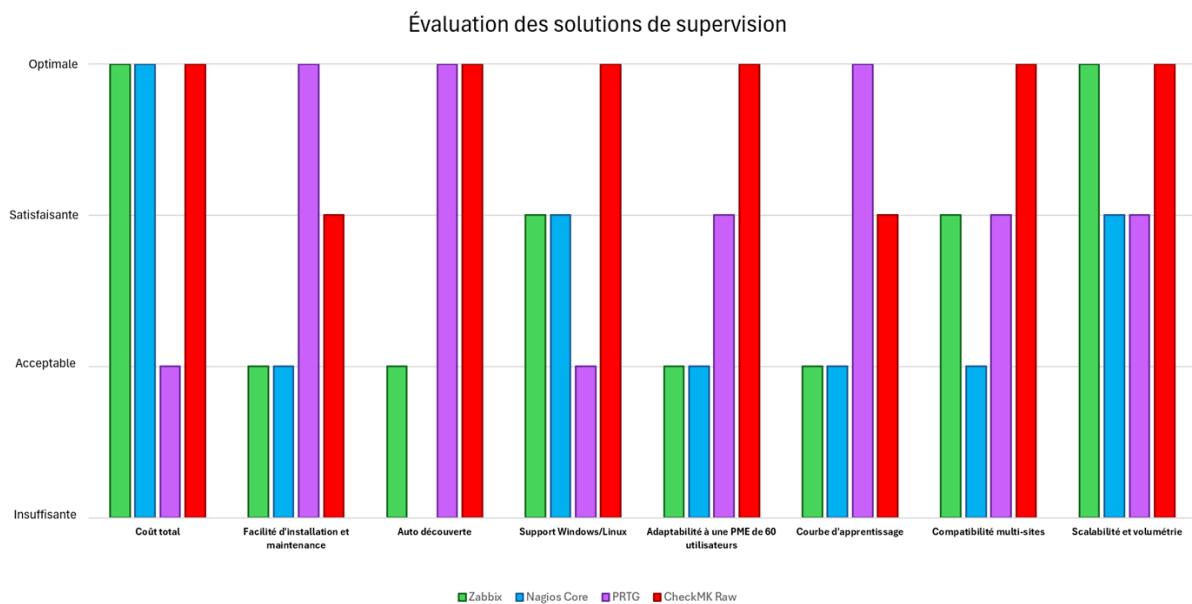


FIGURE 9.1 – Histogramme d'évaluation des solutions de supervision

9.2.6 Choix de la solution : CheckMK Raw

Après analyse approfondie, **CheckMK Raw** s'impose comme le meilleur choix pour XANADU.

Justification du choix

Pourquoi CheckMK Raw ?

Adéquation parfaite aux besoins

- Configuration d'alertes distinguant les services critiques (ERP, RTO 4h) des services standards (RTO 24h)
- Tableaux de bord offrant à la direction une vision claire du SI sans compétences techniques particulières

Économique

- Version gratuite offrant toutes les fonctionnalités nécessaires sans limite d'équipements
- Contrairement à PRTG qui facture par capteur, CheckMK surveille l'ensemble de l'infrastructure sans surcoût

Compatible multi-sites

- Agents consommant peu de bande passante
- Latence MPLS garantie assurant des remontées temps réel
- Gestion native de la supervision multi-sites avec filtrage par localisation

Évolutif et simple d'utilisation

- Ajout de nouveaux serveurs en quelques clics
- Migration transparente vers la version Enterprise si besoin futur

Sécurité intégrée

- Conservation des logs pendant 90 jours
- Traçabilité complète des notifications envoyées
- Parfait pour les audits de conformité

9.2.7 Architecture de supervision

L'architecture de supervision repose sur un serveur central CheckMK déployé à Atlantis, supervisant l'ensemble de l'infrastructure des deux sites via des agents déployés sur chaque équipement.

Composants de l'architecture

Serveur de supervision :

- **Hébergement** : Machine virtuelle dédiée sur l'hyperviseur ESXi d'Atlantis
- **Système d'exploitation** : Linux (Ubuntu Server 22.04 LTS)

Ressources allouées :

- 4 vCPU
- 8 Go de RAM
- 100 Go de stockage (extensible selon historisation)

Interfaces :

- Interface web de supervision accessible via HTTPS

- Moteur d'analyse et corrélation d'alertes
- Base de données RRD (Round Robin Database) pour historisation sur 90 jours
- Service d'envoi de notifications (email/SMS)

Agents de supervision :

— Site Atlantis :

- DC-01 et DC-02 (agents Windows)
- Serveur ESXi (monitoring via API)
- VM hébergeant l'ERP (agent Windows)
- FS-01 - Serveur de fichiers (agent Windows)
- Pare-feu OPNsense (monitoring SNMP)
- Switchs réseau (monitoring SNMP)

— Site Springfield :

- DC-03 (agent Windows pour RODC)
- Serveurs Linux du laboratoire (agents Linux)
- Pare-feu OPNsense local (monitoring SNMP)
- Switch local (monitoring SNMP)
- Postes de travail laboratoire (agents Linux)

Protocoles utilisés :

- **Agents CheckMK** : Communication chiffrée sur port TCP 6556
- **SNMP** : Monitoring des équipements réseau (version 3 avec authentification)
- **ICMP** : Tests de disponibilité et latence
- **API VMware** : Monitoring de l'infrastructure virtualisée

[Insérer ici le schéma de l'architecture générale de la supervision]

FIGURE 9.2 – Schéma de l'architecture générale de la supervision

9.2.8 Éléments supervisés par site

La stratégie de supervision distingue les éléments critiques des éléments secondaires pour optimiser les ressources et prioriser les alertes.

Site Atlantis (siège)

Site Springfield (laboratoire)

9.2.9 Système d'alerting (niveaux, destinataires, anti-saturation)

Le système d'alerting est conçu pour garantir une notification appropriée selon la criticité de l'événement, tout en évitant la saturation des canaux de communication.

Équipement	Métriques supervisées	Criticité
DC-01 (Contrôleur principal)	CPU, RAM, Disques, Réplication AD, Services DNS/DHCP, Authentifications	P1 - Critique
DC-02 (Contrôleur secondaire)	CPU, RAM, Disques, Réplication AD, Services DNS/DHCP	P1 - Critique
ESXi Hyperviseur	État serveur physique, Ressources VMs, Stockage, Santé matérielle	P1 - Critique
VM ERP	Disponibilité application, Temps de réponse, Base de données, Services web	P1 - Critique
FS-01 (Serveur fichiers)	Espace disque, SMART disques, Partages SMB, Débit réseau	P1 - Critique
Pare-feu OPNsense	État HA, Trafic réseau, Utilisation CPU/RAM, VPN, Logs sécurité	P2 - Élevé
Routeur MPLS	Disponibilité, Latence, Taux d'erreurs, Bande passante	P1 - Critique
Switchs réseau	État ports, Utilisation bande passante, Taux d'erreurs	P2 - Élevé
Imprimantes réseau	Disponibilité, Niveau toner/-papier	P3 - Moyen

TABLE 9.3 – Éléments supervisés - Site Atlantis

Niveaux d'alerte et déclencheurs

Destinataires des alertes

- **Administrateur SI** : Reçoit toutes les alertes critiques et de niveau élevé (email + SMS pour les critiques)
- **Direction** : Reçoit uniquement les alertes critiques impactant la disponibilité des services métier (ERP, MPLS)
- **Correspondants métier** : Reçoivent des notifications filtrées concernant uniquement leur périmètre (ex : saturation quotas de stockage, état des partages de leur service)

Mécanismes anti-saturation

Pour éviter la surcharge de notifications et maintenir l'efficacité du système d'alerting :

- **Délai entre alertes similaires** : Intervalle minimal de 30 minutes entre deux notifications identiques
- **Regroupement d'alertes** : Les alertes survenant dans une fenêtre de 5 minutes sont consolidées en une seule notification
- **Escalade progressive** : Pour les alertes non critiques, escalade automatique vers un niveau supérieur si le problème persiste plus de 2 heures

Équipement	Métriques supervisées	Criticité
DC-03 (RODC)	CPU, RAM, Disques, Services DNS, Disponibilité RODC	P1 - Critique
Serveurs Linux laboratoire	CPU, RAM, Disques, Services applicatifs, Processus critiques	P2 - Élevé
Pare-feu OPNsense local	État, Trafic réseau, Tunnel MPLS	P2 - Élevé
Switch local	État ports, Disponibilité	P2 - Élevé
Postes laboratoire	Disponibilité, Espace disque	P3 - Moyen
Agent CheckMK distant	Connectivité avec le serveur central, Latence MPLS	P1 - Critique

TABLE 9.4 – Éléments supervisés - Site Springfield

- **Plages horaires** : Notifications limitées aux heures ouvrées pour les alertes de niveau MOYEN et INFO (7h-20h en semaine)
- **Accusé de réception** : Obligation d'acquitter les alertes critiques pour confirmer leur prise en compte
- **Notifications de résolution** : Email envoyé automatiquement lorsqu'un problème est résolu

9.2.10 10 exemples d'événements déclencheurs

Le système de monitoring génère différents types d'alertes en fonction de la criticité des événements détectés. Ces alertes sont classées par niveau de严重性 et déclenchent des notifications adaptées (mail, SMS, tickets) selon leur importance.

Niveau	Déclencheurs	Notification
red !20 CRITIQUE	<ul style="list-style-type: none"> — Services ERP indisponibles — Contrôleur de domaine arrêté — Liaison MPLS coupée — Disque > 95% saturé — Sauvegarde échouée > 24h 	Email + SMS 24/7 Destinataires : Admin SI + Direction
orange !20 ÉLEVÉ	<ul style="list-style-type: none"> — CPU > 85% pendant 15 min — Disque > 85% saturé — Tentatives d'authentification suspectes — Erreurs matérielles (SMART) — Perte de réPLICATION AD 	Email immédiat (heures ouvrées) Destinataires : Admin SI
yellow !20 MOYEN	<ul style="list-style-type: none"> — CPU > 70% de manière prolongée — Certificats SSL < 30 jours — Dégradations de performances — Mises à jour disponibles critiques 	Email quotidien/hebdomadaire regroupé Destinataires : Admin SI
green !20 INFO	<ul style="list-style-type: none"> — Sauvegarde réussie — Redémarrages planifiés — Mises à jour appliquées — Événements de routine 	Log uniquement (consultation dans l'interface web)

TABLE 9.5 – Niveaux d'alerte et notifications associées

Classification des événements par niveau de criticité

Événement	Description	Action automatique
Niveau CRITIQUE		
Disque du DC presque plein	L'espace disque du contrôleur de domaine est critique : seulement 5% restant	Notifications par mail et SMS envoyées immédiatement
Liaison MPLS Springfield	Le lien MPLS est actuellement indisponible, bloquant l'activité du laboratoire	Alerte immédiate transmise à l'équipe IT
Sauvegarde ERP échouée	Aucune sauvegarde valide de l'ERP depuis plus de 24 heures, représentant un risque en cas de défaillance	Alerte critique déclenchée avec escalade
Niveau ÉLEVÉ		
Charge CPU sur ESXi élevée	Le processeur d'un serveur ESXi dépasse 85% d'utilisation depuis plus de 15 minutes	Alerte de niveau élevé transmise
ERP inaccessible	L'interface web de l'ERP est indisponible, bloquant les processus métiers	Notification de niveau élevé transmise
Disque NAS à risque	Les indicateurs SMART signalent	Alerte élevée activée pour intervention pré-

Principe de classification

Niveau CRITIQUE : Impact direct sur la disponibilité ou la sécurité du SI. Nécessite une intervention immédiate avec notification multi-canal (mail + SMS).

Niveau ÉLEVÉ : Risque important sur les services métiers ou l'infrastructure. Intervention requise dans les meilleurs délais.

Niveau MOYEN : Situation nécessitant une attention mais sans urgence immédiate. Permet une planification d'intervention.

Niveau INFORMATIF : Confirmation du bon fonctionnement. Utilisé pour l'audit et la traçabilité.

Canaux de notification par niveau de criticité

- **Critique** : Mail + SMS + Ticket avec escalade automatique si non traité sous 30 minutes
- **Élevé** : Mail + Ticket avec priorité haute
- **Moyen** : Mail + Ticket avec priorité normale
- **Informatif** : Mail uniquement (rapport quotidien consolidé)

Chapitre 10

Sécurité Opérationnelle : XDR, SIEM et Gestion des Logs

10.1 Fondamentaux

10.1.1 Définition XDR (Extended Detection and Response)

L’XDR représente une évolution naturelle des solutions de détection. Là où un EDR se concentre uniquement sur les postes de travail, l’XDR surveille l’ensemble du système : réseau, serveurs, applications cloud. Cette vision globale permet de repérer des attaques complexes qui exploitent plusieurs vecteurs d’entrée simultanément. En croisant les données de différentes sources, l’XDR détecte des comportements suspects invisibles quand on analyse chaque élément séparément.

10.1.2 Définition SIEM (Security Information and Event Management)

Un SIEM centralise tous les journaux d’événements du système d’information. Il collecte ces données, les normalise pour faciliter leur analyse, puis les corrèle pour identifier des menaces. Le SIEM génère des alertes quand il repère un comportement anormal et conserve l’historique pour les analyses post-incident. C’est l’outil central qui donne une vue d’ensemble de ce qui se passe sur l’infrastructure.

10.1.3 Importance de la centralisation des logs

Sans centralisation, les logs restent dispersés sur des dizaines de machines différentes. Reconstituer le fil d’une attaque devient alors un véritable casse-tête. La centralisation facilite les investigations en regroupant toutes les informations au même endroit. Elle garantit aussi que les traces ne disparaissent pas avec une panne de serveur. Pour les audits de conformité, disposer d’un historique centralisé fait gagner un temps considérable.

10.1.4 Enjeux de la détection et réponse aux incidents

Plus une menace est détectée tôt, moins elle cause de dégâts. Un ransomware identifié en quelques minutes peut être stoppé avant de chiffrer l’ensemble du système. À l’inverse, une détection tardive entraîne des pertes de données massives et des arrêts d’activité

coûteux. La capacité de réaction repose sur des procédures claires et des outils permettant d'agir rapidement. Automatiser certaines réponses, comme l'isolement d'une machine compromise, limite considérablement la propagation des attaques.

10.1.5 Principe de corrélation d'événements de sécurité

La corrélation consiste à relier des événements distincts pour révéler une menace. Plusieurs échecs de connexion suivis d'une authentification réussie signalent probablement une attaque par force brute. Pris isolément, chaque événement semble banal. C'est leur enchaînement qui trahit l'attaquant. Les règles de corrélation définissent ces scénarios caractéristiques et permettent de détecter des attaques en plusieurs étapes.

10.2 Mise en œuvre technique

10.2.1 Choix de la solution : Wazuh

Après avoir étudié plusieurs solutions, Wazuh s'est imposé comme le choix le plus adapté. Cette plateforme open source combine SIEM, XDR et gestion de la conformité dans une seule interface. Son caractère gratuit représente un atout majeur pour une PME comme XANADU. La solution bénéficie d'une documentation complète et d'une communauté active. Son architecture modulaire permet de l'adapter facilement aux besoins spécifiques sans complexité excessive.

10.2.2 Comparatif des solutions étudiées

Trois solutions majeures ont été évaluées selon plusieurs critères clés.

Critères	Poids	Wazuh	Elastic Stack	Splunk
Coût initial	20%	5	3	1
Facilité de déploiement	15%	4	2	3
Fonctionnalités SIEM	20%	4	5	5
Capacités XDR	15%	4	4	5
Documentation	10%	4	4	5
Conformité réglementaire	10%	5	3	5
Performances	10%	3	5	5
Note finale pondérée		4.25	3.65	3.80

TABLE 10.1 – Analyse matricielle des solutions SIEM/XDR (échelle de 1 à 5)

Analyse détaillée :

Wazuh arrive en tête principalement grâce à son coût nul et ses fonctionnalités complètes. La solution couvre tous les besoins identifiés sans nécessiter de licence commerciale. Son déploiement reste accessible pour une équipe de taille moyenne. Les capacités de conformité réglementaire natives représentent un véritable plus.

Elastic Stack offre d'excellentes performances et une scalabilité remarquable. Cependant, les fonctions avancées de sécurité nécessitent une licence payante. La complexité de configuration pénalise également cette solution pour une PME disposant de ressources limitées.

Splunk reste la référence du marché avec des capacités analytiques puissantes. Son modèle de tarification basé sur le volume de données généreraient des coûts importants pour XANADU. Les performances et la maturité de l'écosystème ne compensent pas le surcoût pour notre contexte.

Le choix de Wazuh permet d'investir le budget sécurité sur d'autres aspects critiques tout en disposant d'une solution complète et évolutive.

10.2.3 Architecture globale de la solution

L'architecture Wazuh repose sur trois composants principaux qui travaillent ensemble. Le serveur Wazuh centralise les événements et mène les analyses de sécurité. Wazuh Indexer stocke les données et permet des recherches rapides dans l'historique. Wazuh Dashboard fournit l'interface où les administrateurs consultent alertes et statistiques.

Des agents sont installés sur tous les postes Windows et serveurs Linux. Ces agents surveillent en permanence ce qui se passe sur chaque machine : connexions, modifications de fichiers, processus lancés. Ils transmettent ces informations au serveur de manière chiffrée.

10.2.4 Déploiement du serveur Wazuh

Le serveur Wazuh fonctionne sur une VM dédiée dans le VLAN Management avec 8 cœurs, 16 Go de RAM et 500 Go de stockage. Ces ressources permettent de traiter tous les événements en temps réel sans problème de performance.

L'installation utilise le script automatisé fourni par l'éditeur. Cette méthode évite les erreurs de configuration manuelle et accélère la mise en production. Les certificats TLS sont générés automatiquement pour sécuriser les échanges. Les règles par défaut sont activées puis enrichies avec des règles spécifiques à XANADU.

10.2.5 Configuration du service d'indexation

Wazuh Indexer s'appuie sur OpenSearch pour organiser et retrouver rapidement les événements. Le système conserve 90 jours de données détaillées en ligne, ce qui permet des investigations approfondies sur les incidents récents. Au-delà, les données sont compressées et archivées sur un espace de stockage moins coûteux.

Les données sont organisées par index quotidiens pour optimiser les performances. Un alias pointe automatiquement vers les données récentes, ce qui simplifie grandement les recherches.

10.2.6 Collecte et centralisation des logs

Les agents Wazuh collectent plusieurs types d'informations. Sur Windows, ils récupèrent les événements système, les logs de sécurité et les journaux applicatifs. Sur Linux, ils surveillent les fichiers de logs standards et les commandes exécutées.

Les pare-feux pfSense envoient leurs logs via syslog, permettant de surveiller les tentatives de connexion suspectes. Les contrôleurs Active Directory transmettent tous les événements d'authentification. Le serveur WSUS communique ses logs de mise à jour. Toutes ces sources alimentent le serveur central qui corrèle l'information.

10.2.7 Règles de détection et alertes de sécurité

Wazuh embarque plus de 3000 règles couvrant les menaces courantes : intrusions, modifications de fichiers critiques, élévations de priviléges, connexions depuis des pays inhabituels. Chaque règle possède un niveau de sévérité qui détermine la priorité de traitement.

Des règles personnalisées répondent aux besoins spécifiques de l'entreprise. Par exemple, une règle détecte les connexions VPN hors horaires ouvrables. Une autre signale les accès aux dossiers RH depuis des comptes non autorisés. Les alertes critiques déclenchent une notification immédiate par email.

10.2.8 Tableaux de bord et visualisation

Le tableau de bord principal affiche les alertes récentes, les machines générant le plus d'événements et les règles souvent déclenchées. Un coup d'œil suffit pour évaluer l'état de sécurité. Le tableau de conformité vérifie automatiquement le respect des référentiels PCI DSS, GDPR ou CIS Benchmarks, simplifiant la préparation des audits.

Des tableaux personnalisés suivent les indicateurs propres à XANADU : taux de mise à jour des postes, logiciels non autorisés détectés, historique des connexions VPN.

10.2.9 Cas d'usage et scénarios de détection

Plusieurs scénarios couvrent les menaces principales :

Ransomware : détection de modifications massives de fichiers en peu de temps avec création de fichiers suspects (.encrypted, .locked).

Force brute : identification de séries d'échecs d'authentification suivis d'une connexion réussie.

Élévation de privilège : alerte sur toute modification des groupes d'administration.

Exfiltration : surveillance des transferts volumineux vers l'extérieur.

10.2.10 Politique de rétention des logs et archivage

Les logs restent 90 jours en ligne pour des investigations rapides. Au-delà, ils sont compressés et archivés sur le NAS pendant un an pour répondre aux obligations réglementaires. Une procédure automatique supprime les archives de plus d'un an, équilibrant traçabilité et contraintes de stockage.

10.2.11 Intégration avec la supervision (CheckMK)

Wazuh fonctionne en synergie avec CheckMK qui surveille l'état du serveur Wazuh : disponibilité, CPU, mémoire, espace disque. Cette supervision garantit que le système de détection reste opérationnel. Lorsqu'une alerte Wazuh remonte un incident, les données CheckMK aident à comprendre le contexte technique, facilitant le diagnostic et accélérant la résolution.

10.2.12 Déploiement du serveur Wazuh

Le serveur Wazuh tourne sur une machine virtuelle dédiée dans le VLAN Management. Cette VM dispose de ressources suffisantes pour traiter tous les événements en temps réel :

8 cœurs, 16 Go de mémoire et 500 Go d'espace disque. Ces caractéristiques permettent de gérer sans difficulté l'ensemble des logs générés par l'infrastructure.

L'installation s'effectue via le script automatisé fourni par l'éditeur. Cette méthode évite les erreurs de configuration manuelle et accélère la mise en production. Des certificats TLS sont générés automatiquement pour sécuriser les échanges entre les agents et le serveur. Les règles de détection par défaut sont activées puis complétées par des règles spécifiques aux besoins de XANADU.

10.2.13 Configuration du service d'indexation

Wazuh Indexer s'appuie sur OpenSearch pour stocker et indexer les événements. Le système est configuré pour conserver 90 jours de données détaillées en ligne. Cette durée permet de mener des investigations approfondies sur des incidents récents sans problème de performance. Au-delà de ce délai, les données sont compressées et archivées sur un espace de stockage moins coûteux.

Les données sont organisées par index quotidiens. Cette organisation simplifie la gestion et améliore les performances des recherches. Un alias pointe automatiquement vers les index récents, ce qui évite aux utilisateurs de manipuler des noms d'index compliqués.

10.2.14 Collecte et centralisation des logs

Les agents Wazuh installés sur les postes et serveurs collectent plusieurs types d'informations. Sur Windows, ils récupèrent les événements système, les logs de sécurité et les journaux applicatifs. Sur Linux, ils surveillent les fichiers de logs standards et les commandes exécutées par les utilisateurs.

Les pare-feux pfSense envoient leurs logs via le protocole syslog. Cette configuration permet de surveiller les tentatives de connexion suspectes et les blocages de trafic. Les contrôleurs de domaine Active Directory transmettent tous les événements d'authentification, ce qui permet de détecter rapidement les comptes compromis ou les tentatives d'intrusion.

Le serveur WSUS communique également ses logs. On peut ainsi vérifier que les mises à jour se déploient correctement et identifier les machines qui accusent du retard. Toutes ces sources alimentent le serveur Wazuh qui centralise et corrèle l'information.

10.2.15 Règles de détection et alertes de sécurité

Wazuh embarque plus de 3000 règles de détection prêtes à l'emploi. Ces règles couvrent les menaces courantes : tentatives d'intrusion, modifications de fichiers critiques, élévations de priviléges non autorisées, connexions depuis des pays inhabituels. Chaque règle est associée à un niveau de严重性 qui détermine la priorité de traitement.

Des règles personnalisées ont été créées pour répondre aux besoins spécifiques de l'entreprise. Par exemple, une règle détecte les connexions VPN en dehors des heures ouvrables. Une autre signale les tentatives d'accès aux dossiers RH depuis des comptes qui ne devraient pas y avoir accès. Ces règles métier augmentent la pertinence des alertes.

Les alertes critiques déclenchent une notification immédiate par email aux administrateurs. Les alertes de niveau moyen sont consultables dans le tableau de bord. Cette priorisation évite la submersion des équipes par des alertes peu importantes tout en garantissant qu'aucune menace sérieuse ne passe inaperçue.

10.2.16 Tableaux de bord et visualisation

Wazuh Dashboard propose plusieurs tableaux de bord préconfigurés qui facilitent la supervision quotidienne. Le tableau de bord principal affiche les alertes récentes, les machines qui génèrent le plus d'événements et les règles les plus souvent déclenchées. Un coup d'œil suffit pour avoir une vue d'ensemble de l'état de sécurité.

Le tableau de conformité vérifie automatiquement si les systèmes respectent les référentiels de sécurité. Il identifie rapidement les écarts par rapport aux standards PCI DSS, GDPR ou CIS Benchmarks. Cette fonction simplifie grandement la préparation des audits de conformité.

Des tableaux personnalisés ont été créés pour suivre des indicateurs propres à XANADU. On y retrouve le taux de mise à jour des postes, la liste des logiciels non autorisés détectés, ou encore l'historique des connexions VPN. Ces vues métier facilitent le pilotage de la sécurité au quotidien.

10.2.17 Cas d'usage et scénarios de détection

Plusieurs scénarios de détection ont été mis en place pour couvrir les menaces principales.

Détection de ransomware : Wazuh surveille les modifications massives de fichiers en peu de temps. Si un poste modifie brutalement des centaines de documents et crée des fichiers avec des extensions suspectes (.encrypted, .locked), une alerte critique est levée immédiatement.

Attaque par force brute : Le système détecte les séries d'échecs d'authentification suivis d'une connexion réussie. Ce pattern révèle souvent une attaque par dictionnaire qui a fini par trouver le bon mot de passe.

Elévation de privilèges : Toute modification des groupes d'administration ou ajout de compte administrateur génère une alerte. Ces actions sont légitimes uniquement dans des contextes précis et doivent être tracées.

Exfiltration de données : Les transferts de fichiers volumineux vers l'extérieur sont surveillés. Un utilisateur qui télécharge soudainement des gigaoctets de données déclenche une investigation.

10.2.18 Politique de rétention des logs et archivage

Les logs sont conservés 90 jours en ligne pour permettre des investigations rapides. Cette durée répond aux exigences légales de base et couvre la majorité des besoins opérationnels. Les recherches sur cette période restent très rapides grâce à l'indexation.

Au-delà de 90 jours, les données sont automatiquement compressées et transférées sur le NAS de l'entreprise. L'archivage est conservé pendant un an pour répondre aux obligations réglementaires et permettre les audits rétrospectifs en cas de besoin.

Une procédure automatique supprime définitivement les archives de plus d'un an. Cette politique équilibre les besoins de traçabilité avec les contraintes de stockage. Elle reste conforme aux recommandations de la CNIL sur la conservation des logs.

10.2.19 Intégration avec la supervision (CheckMK)

Wazuh fonctionne en synergie avec CheckMK, la solution de supervision déployée sur l'infrastructure. CheckMK surveille l'état de santé du serveur Wazuh : disponibilité des

services, utilisation CPU et mémoire, espace disque restant. Si le serveur Wazuh tombe en panne, CheckMK alerte immédiatement les administrateurs.

Cette supervision garantit que le système de détection reste opérationnel en permanence. Elle permet aussi de prévoir les montées en charge et d'ajuster les ressources avant que des problèmes n'apparaissent.

L'intégration va dans les deux sens. Lorsqu'une alerte Wazuh remonte un incident de sécurité, les données CheckMK aident à comprendre le contexte : y avait-il un problème réseau au même moment ? Un serveur était-il surchargé ? Cette corrélation facilite le diagnostic et accélère la résolution des incidents complexes.

Chapitre 11

Automatisation et Administration

11.1 Fondamentaux

11.1.1 Importance de l'automatisation en administration système

L'automatisation en administration système consiste à utiliser des scripts et des outils logiciels afin d'exécuter automatiquement des tâches répétitives, complexes ou critiques. Elle occupe une place centrale dans la gestion moderne des systèmes d'information, où la taille des infrastructures et le nombre d'utilisateurs rendent une administration entièrement manuelle difficile, voire impossible.

Grâce à l'automatisation, les administrateurs peuvent standardiser les configurations, assurer une application homogène des règles de sécurité et garantir la cohérence des environnements. Elle permet également d'améliorer la fiabilité globale du système d'information en réduisant la dépendance aux interventions humaines ponctuelles.

11.1.2 Réduction des erreurs humaines

Les erreurs humaines constituent l'une des principales causes d'incidents et de failles de sécurité dans les systèmes d'information. Elles peuvent résulter d'une mauvaise manipulation, d'une configuration incorrecte, d'un manque de vigilance ou d'une méconnaissance des procédures. Dans un environnement informatique complexe, ces erreurs peuvent avoir des conséquences importantes sur la disponibilité des services, l'intégrité des données ou la confidentialité des informations.

Plusieurs études récentes mettent en évidence l'ampleur de ce phénomène. Selon le *Data Breach Investigations Report* de Verizon, environ **74 % des violations de données impliquent un facteur humain**, qu'il s'agisse d'erreurs, d'identifiants compromis ou d'attaques par ingénierie sociale. D'autres analyses, notamment relayées par des organismes spécialisés en cybersécurité, indiquent que **jusqu'à 95 % des incidents de sécurité comportent une composante liée à l'erreur humaine**.

Dans ce contexte, l'automatisation joue un rôle essentiel dans la réduction de ces risques. En remplaçant les actions manuelles par des scripts standardisés, testés et reproductibles, elle permet de limiter les oubliers, les erreurs de saisie et les configurations incohérentes. Les tâches critiques sont ainsi exécutées de manière fiable et uniforme, indépendamment de l'intervention humaine directe.

L'automatisation contribue également à renforcer la traçabilité des opérations, facilitant l'identification des actions réalisées et l'analyse des incidents éventuels. Elle constitue

ainsi un levier majeur pour améliorer la sécurité, la stabilité et la qualité de l'administration des systèmes d'information en entreprise.

Sécurité du réseau

La sécurité du réseau repose en grande partie sur une segmentation efficace via des VLANs, permettant d'isoler les différents services et de limiter la propagation d'attaques internes. L'absence d'un filtrage par défaut de type deny-all expose le réseau à des flux non maîtrisés, notamment en provenance d'emails malveillants. La mise en place de solutions de sécurité périphérique avancées (NGFW, IDS/IPS, WAF), ainsi qu'une surveillance continue des flux réseau, est indispensable pour détecter et prévenir les comportements suspects. Les accès VPN inter-sites doivent également être sécurisés par des mécanismes d'authentification renforcés.

11.1.3 Gain de temps et efficacité opérationnelle

L'automatisation offre un gain de temps significatif pour les équipes d'administration système. Des tâches telles que la création de comptes utilisateurs, la gestion des droits, les sauvegardes, les contrôles de conformité ou les audits peuvent être exécutées rapidement et à grande échelle.

Ce gain de temps permet aux administrateurs de se concentrer sur des missions à plus forte valeur ajoutée, comme l'optimisation des infrastructures, l'amélioration de la sécurité ou la gestion de projets. L'efficacité opérationnelle s'en trouve renforcée, tout en améliorant la réactivité face aux incidents et aux évolutions des besoins métiers.

11.1.4 Bonnes pratiques de scripting PowerShell

Le scripting PowerShell est un outil particulièrement adapté à l'automatisation dans les environnements Windows et Active Directory. Afin de garantir la fiabilité et la maintenabilité des scripts, certaines bonnes pratiques doivent être respectées.

Il est recommandé de structurer les scripts de manière claire, avec des commentaires explicatifs et des noms de variables explicites. La gestion des erreurs doit être intégrée afin d'anticiper les échecs d'exécution et d'éviter des impacts non maîtrisés sur le système. L'utilisation de modules, de fonctions et de paramètres permet de rendre les scripts réutilisables et évolutifs.

Enfin, les scripts doivent être testés dans des environnements de validation avant leur déploiement en production, et stockés dans un espace sécurisé avec un contrôle de version. Ces bonnes pratiques contribuent à une administration plus sûre, plus efficace et plus professionnelle du système d'information.

11.2 Mise en œuvre technique

11.2.1 Script : Création automatisée de l’arborescence AD

```
1 Import-Module ActiveDirectory
2
3 $root = "DC=berria,DC=local"
4
5 # Liste de toutes les OUs à créer.
6 $OUList = @(
7     "OU=Atlantis,$root",
8     "OU=Springfield,$root",
9
10    "OU=Utilisateurs,OU=Atlantis,$root",
11    "OU=Groupes,OU=Atlantis,$root",
12    "OU=Administrateurs,OU=Atlantis,$root",
13
14    "OU=Utilisateurs,OU=Springfield,$root",
15    "OU=Groupes,OU=Springfield,$root",
16    "OU=Administrateurs,OU=Springfield,$root",
17
18    # Sous-OU des services Atlantis
19    "OU_Commercial,OU=Utilisateurs,OU=Atlantis,$root",
20    "OU_BureauEtude,OU=Utilisateurs,OU=Atlantis,$root",
21    "OU_Juridique,OU=Utilisateurs,OU=Atlantis,$root",
22    "OU_RH,OU=Utilisateurs,OU=Atlantis,$root",
23    "OU_Direction,OU=Utilisateurs,OU=Atlantis,$root",
24    "OU_Comptabilite,OU=Utilisateurs,OU=Atlantis,$root",
25
26    # Laboratoire à Springfield
27    "OU_Laboratoire,OU=Utilisateurs,OU=Springfield,$root"
28 )
```

FIGURE 11.1 – Script PowerShell de création automatisée de l’arborescence Active Directory

Ce script automatise la création de l’arborescence de l’AD, ce qui va éliminer la nécessité de faire des configurations de manière manuelle à chaque fois, cela nous permettra de gagner du temps et d’éviter les erreurs humaines

11.2.2 Script : Création automatique des groupes

```

1 Import-Module ActiveDirectory
2
3 $root = "DC=berria,DC=local"
4
5 # Table des groupes à créer : nom + OU cible
6 $groups = @(
7     @{Name="GG_Commercial";      Path="OU=Groupes,OU=Atlantis,$root"},
8     @{Name="GG_BureauEtude";    Path="OU=Groupes,OU=Atlantis,$root"},
9     @{Name="GG_Juridique";       Path="OU=Groupes,OU=Atlantis,$root"},
10    @{Name="GG_RH";              Path="OU=Groupes,OU=Atlantis,$root"},
11    @{Name="GG_Direction";      Path="OU=Groupes,OU=Atlantis,$root"},
12    @{Name="GG_Comptabilite";   Path="OU=Groupes,OU=Atlantis,$root"},
13
14    @{Name="GA_Commercial";      Path="OU=Groupes,OU=Atlantis,$root"},
15    @{Name="GA_BureauEtude";    Path="OU=Groupes,OU=Atlantis,$root"},
16    @{Name="GA_Juridique";       Path="OU=Groupes,OU=Atlantis,$root"},
17    @{Name="GA_RH";              Path="OU=Groupes,OU=Atlantis,$root"},
18    @{Name="GA_Direction";      Path="OU=Groupes,OU=Atlantis,$root"},
19    @{Name="GA_Comptabilite";   Path="OU=Groupes,OU=Atlantis,$root"},
20
21    @{Name="GG_Laboratoire";     Path="OU=Groupes,OU=Springfield,$root"},
22    @{Name="GA_Laboratoire";     Path="OU=Groupes,OU=Springfield,$root"}
23 )
24
25 foreach ($g in $groups) {
26     if (-not (Get-ADGroup -Filter "Name='$(($g.Name))'" -ErrorAction SilentlyContinue)) {
27
28         # Création du groupe Global (standard pour la gestion des droits)
29         New-ADGroup `-
30             -Name $g.Name `-
31             -GroupScope Global `-
32             -GroupCategory Security `-
33             -Path $g.Path
34
35         Write-Host "Création du groupe : $($g.Name)"
36     }
37 }
```

FIGURE 11.2 – Script de création automatique des groupes Active Directory

Ce script crée automatiquement tous les groupes de sécurité nécessaires (GG, GA, etc.), ce qui standardise la gestion des droits, évite les incohérences entre services et garantit une base propre et homogène pour l'attribution des accès.

11.2.3 Script : Cr éation d'utilisateurs depuis CSV

```

1 Import-Module ActiveDirectory
2 # Chemin du CSV contenant les futurs utilisateurs
3 # Colonnes : SamAccountName;Prenom;Nom;Service;Site
4 $users = Import-Csv "C:\Admin\users.csv" -Delimiter ';' 
5 $root = "DC=berria,DC=local"
6 foreach ($u in $users) {
7
8     # D étermine la bonne OU selon le site
9     switch ($u.Site) {
10         "Atlantis" {
11             $ou = "OU_${$u.Service},OU=Utilisateurs,OU=Atlantis,$root"
12             $gg = "GG_${$u.Service}"
13         }
14
15         "Springfield" {
16             $ou = "OU_Laboratoire,OU=Utilisateurs,OU=Springfield,$root"
17             $gg = "GG_Laboratoire"
18         }
19     }
20     # Evite la cr éation en double
21     if (Get-ADUser -Filter "SamAccountName='$$u.SamAccountName'" -ErrorAction SilentlyContinue) {
22         Write-Host "Utilisateur $$u.SamAccountName existe d ej a."
23         continue
24     }
25     # Cr éation du compte utilisateur
26     New-ADUser ` 
27         -SamAccountName $u.SamAccountName ` 
28         -UserPrincipalName "$($u.SamAccountName)@berria.local" ` 
29         -GivenName $u.Prenom ` 
30         -Surname $u.Nom ` 
31         -Name "$($u.Prenom) $($u.Nom)" ` 
32         -AccountPassword (ConvertTo-SecureString "P@ssw0rd!" -AsPlainText -Force) ` 
33         -Enabled $true ` 
34         -ChangePasswordAtLogon $true ` 
35         -Path $ou
36
37     # Ajout dans le groupe approprié
38     Add-ADGroupMember -Identity $gg -Members $u.SamAccountName

```

FIGURE 11.3 – Script d'importation et de cr éation d'utilisateurs Active Directory depuis un fichier CSV

Ce script g n er e les comptes utilisateurs à partir d'un fichier CSV et les place directement dans les bonnes OUs et groupes, ce qui accélère l'onboarding, supprime les manipulations r é pétitives et assure une configuration correcte dès la cr éation du compte.

11.2.4 Script : Désactivation automatique des comptes inactifs

```

1 Import-Module ActiveDirectory
2
3 # Comptes inactifs depuis plus de 90 jours
4 $limitDate = (Get-Date).AddDays(-90)
5
6 $quar = "OU=Quarantaine,OU=Utilisateurs,OU=Atlantis,DC=berria,DC=local"
7
8 # Recherche des utilisateurs actifs mais inactifs depuis 90 jours
9 $users = Get-ADUser -Filter {
10   Enabled -eq $true -and LastLogonDate -lt $limitDate
11 } -Properties LastLogonDate
12
13 foreach ($u in $users) {
14
15   # Désactivation du compte
16   Disable-ADAccount -Identity $u.SamAccountName
17
18   # Déplacement dans une OU dédiée
19   Move-ADObject -Identity $u.DistinguishedName -TargetPath $quar
20
21   Write-Host "Compte désactivé et déplacé : $($u.SamAccountName)"
22 }
23

```

FIGURE 11.4 – Script de désactivation automatique des comptes utilisateurs inactifs

Ce script identifie les comptes inactifs depuis un certain temps, les désactive puis les déplace en quarantaine, ce qui améliore la sécurité du domaine, évite les comptes dormants et maintient un environnement Active Directory propre et maîtrisé.

11.2.5 Script : Inventaire AD (export CSV)

```

# Script d'inventaire Active Directory
1 Import-Module ActiveDirectory
2
3 # Inventaire des utilisateurs
4 Get-ADUser -Filter * -Properties Enabled,LastLogonDate,Department |
5 Select-Object SamAccountName,Name,Enabled,Department,LastLogonDate |
6 Export-Csv "C:\Admin\inventaire_utilisateurs.csv" -NoTypeInformation -Delimiter ';'
7
8 # Inventaire des ordinateurs
9 Get-ADComputer -Filter * -Properties OperatingSystem,IPv4Address,LastLogonDate |
10 Select-Object Name,OperatingSystem,IPv4Address,LastLogonDate |
11 Export-Csv "C:\Admin\inventaire_ordis.csv" -NoTypeInformation -Delimiter ';'
12
13 Write-Host "Inventaires générés."
14

```

FIGURE 11.5 – Script d'inventaire Active Directory avec export des données au format CSV

Ce script exporte un inventaire complet des utilisateurs et des ordinateurs dans des fichiers CSV, ce qui permet d'avoir une visibilité immédiate et exploitable du parc, facilitant ainsi les audits, la gestion du cycle de vie et les décisions d'administration.

11.2.6 Script : Sauvegarde des GPOs horodatée

```
Script Sauvegarde des GPO.ps1 > ...
1 Import-Module GroupPolicy
2 # Module nécessaire pour manipuler et sauvegarder les GPO.
3
4 # Répertoire de destination pour les sauvegardes
5 $backupRoot = "C:\BackupGPO"
6
7 # On crée un sous-dossier avec la date et l'heure → meilleure traçabilité
8 $dateFolder = Join-Path $backupRoot (Get-Date -Format "yyyyMMdd_HHmm")
9 New-Item -ItemType Directory -Path $dateFolder -Force | Out-Null
10
11 # Sauvegarde de toutes les GPO existantes dans le domaine
12 Backup-GPO -All -Path $dateFolder
13
14 Write-Host "Sauvegarde GPO effectuée dans : $dateFolder"
15
```

FIGURE 11.6 – Script de sauvegarde horodatée des stratégies de groupe (GPO)

Ce script sauvegarde automatiquement toutes les GPOs dans des dossiers horodatés, ce qui garantit la possibilité de restaurer rapidement la configuration en cas d'erreur ou de corruption et renforce la résilience de l'infrastructure.

11.2.7 Script : Contrôle quotidien de santé du domaine

```
1 # Répertoire où l'on stocke les rapports
2 $logDir = "C:\Admin\Rapports_AD"
3 New-Item -ItemType Directory -Path $logDir -Force | Out-Null
4
5 # Nom du fichier de rapport avec date
6 $logFile = Join-Path $logDir ("Rapport_AD_" + (Get-Date -Format "yyyyMMdd") + ".log")
7
8 # Entête
9 "___ Rapport santé AD - $($Get-Date) ===" | Out-File $logFile
10
11 "___ DCDIAG : Tests détaillés du contrôleur de domaine ---" | Out-File $logFile -Append
12 dcdiag /v | Out-File $logFile -Append
13
14 "___ REPADMIN : Résumé de réPLICATION ---" | Out-File $logFile -Append
15 repadmin /replsummary | Out-File $logFile -Append
16
17 Write-Host "Rapport de santé généré : $logFile"
18
```

FIGURE 11.7 – Script de contrôle quotidien de l'état de santé du domaine Active Directory

Ce script génère un rapport de santé du domaine en exécutant DCDIAG et REPADMIN, ce qui permet de détecter de manière proactive les problèmes de réPLICATION ou de contrôleur de domaine avant qu'ils n'impactent les utilisateurs.

11.2.8 Script : Mutation d'utilisateur vers un autre service

```

1  <#
2  Ce script deplace un utilisateur vers sa nouvelle OU de service
3  et met automatiquement a jour son appartenance aux groupes GG_Service.
4  #>
5  param(
6      [Parameter(Mandatory=$true)]
7      [string]$SamAccountName,
8
9      [Parameter(Mandatory=$true)]
10     [ValidateSet("Commercial","BureauEtude","Juridique","RH","Direction","Comptabilite")]
11     [string]$NouveauService
12 )
13
14 Import-Module ActiveDirectory
15
16 $root = "DC=berria,DC=local"
17
18 # Recuperation du compte utilisateur
19 $user = Get-ADUser $SamAccountName -Properties MemberOf,DistinguishedName
20
21 if (-not $user) {
22     Write-Error "Utilisateur introuvable"
23     exit 1
24 }
25
26 # Definition de la nouvelle OU et du groupe associe
27 $newOU  = "OU_$NouveauService,OU=Utilisateurs,OU=Atlantis,$root"
28 $newGG  = "GG_$NouveauService"
29
30 # On deplace le utilisateur dans sa nouvelle OU
31 Move-ADObject -Identity $user.DistinguishedName -TargetPath $newOU
32
33 # On retire le utilisateur de tous les anciens groupes GG_*
34 $oldGG = $user.MemberOf | Where-Object { $_ -like "CN=GG_*,OU=Groupes,OU=Atlantis,$root" }
35 foreach ($g in $oldGG) {
36     Remove-ADGroupMember -Identity $g -Members $user -Confirm:$false
37 }
38
39 # Puis on ajoute dans son nouveau groupe
40 Add-ADGroupMember -Identity $newGG -Members $user
41
42 Write-Host "Mutation effectuée : $SamAccountName → $NouveauService"

```

FIGURE 11.8 – Script de mutation d'un utilisateur vers un autre service Active Directory

Ce script automatise le changement de service des utilisateurs en mettant à jour leur OU et leurs groupes d'accès, ce qui assure que leurs droits restent toujours cohérents avec leur fonction et supprime les erreurs lors des mobilités internes.

11.2.9 Script : Alerte sur expiration des mots de passe

```

1 Import-Module ActiveDirectory
2
3 # Delai d'avertissement
4 $JoursAvantExpiration = 155
5 $rapport = "C:\Admin\mdp_expirations.csv"
6
7 # Recuperation de la politique de mot de passe du domaine
8 $policy = Get-ADDefaultDomainPasswordPolicy
9 $maxAge = $policy.MaxPasswordAge.Days
10
11 $today = Get-Date
12 $limit = $today.AddDays($JoursAvantExpiration)
13
14 $users = Get-ADUser -Filter {Enabled -eq $true -and PasswordNeverExpires -eq $false} ` 
15      -Properties PasswordLastSet, DisplayName, EmailAddress
16
17 $resultats = @()
18
19 foreach ($u in $users) {
20
21     if (-not $u.PasswordLastSet) { continue }
22
23     # Calcul de la date d'expiration du mot de passe
24     $expiration = $u.PasswordLastSet.AddDays($maxAge)
25
26     # Est-ce que l'on est dans la periode d'avertissement ?
27     if ($expiration -le $limit -and $expiration -gt $today) {
28         $resultats += [pscustomobject]@{
29             Utilisateur = $u.SamAccountName
30             NomComplet = $u.DisplayName
31             ExpireLe = $expiration
32             JoursRestants = (New-TimeSpan -Start $today -End $expiration).Days
33             Email = $u.EmailAddress
34         }
35     }
36 }
37
38 $resultats | Export-Csv $rapport -NoTypeInformation -Delimiter ';'
39 Write-Host "Rapport genere : $rapport"

```

FIGURE 11.9 – Script d’alerte concernant l’expiration prochaine des mots de passe utilisateurs

Ce script recense les utilisateurs dont le mot de passe va expirer prochainement, ce qui permet d’anticiper la communication, de réduire les incidents de comptes verrouillés et d’améliorer la fluidité du support

11.2.10 Script : Audit des comptes à privilèges

```

1 Import-Module ActiveDirectory
2
3 $rapportDir = "C:\Admin\Rapports_AD"
4 $rapportFile = Join-Path $rapportDir ("admins_privilégiés_" + (Get-Date -Format "yyyyMMdd") + ".csv")
5 New-Item -ItemType Directory -Path $rapportDir -Force | Out-Null
6
7 # Liste des groupes critiques à auditer
8 $groupesCritiques = @(
9     "Domain Admins",
10    "Enterprise Admins",
11    "Schema Admins",
12    "Administrators",
13    "DnsAdmins",
14    "Backup Operators"
15 )
16 $resultats = @()
17
18 foreach ($gName in $groupesCritiques) {
19
20     # Ignore si groupe absent dans ce domaine
21     $g = Get-ADGroup -Identity $gName -ErrorAction SilentlyContinue
22     if (-not $g) { continue }
23
24     # Recuperation recursive des membres
25     $membres = Get-ADGroupMember -Identity $g -Recursive |
26         Where-Object { $_.ObjectClass -eq "user" }
27
28     foreach ($m in $membres) {
29         $u = Get-ADUser $m.SamAccountName -Properties DisplayName,Enabled,LastLogonDate
30         $resultats += [pscustomobject]@{
31             Groupe      = $gName
32             Utilisateur = $u.SamAccountName
33             NomComplet   = $u.DisplayName
34             Actif        = $u.Enabled
35             DernierLogon = $u.LastLogonDate
36         }
37     }
38 }
39
40 $resultats | Sort-Object Groupe,Utilisateur |
41 Export-Csv $rapportFile -NoTypeInformation -Delimiter ';' |
42 Write-Host "Rapport comptes à privilèges : $rapportFile"
43

```

FIGURE 11.10 – Script d’audit des comptes disposant de privilèges élevés dans Active Directory

Ce script audite les comptes à privilèges en listant tous les membres des groupes administratifs sensibles, ce qui renforce la sécurité du domaine et permet de détecter rapidement toute dérive ou ajout non autorisé dans les groupes critiques.

Chapitre 12

Audit de Sécurité

12.1 Fondamentaux

12.1.1 Définition et objectifs d'un audit de sécurité

Un audit de sécurité est une démarche méthodique visant à évaluer le niveau de sécurité d'un système d'information. Il consiste à analyser les politiques, les procédures, les configurations techniques et les pratiques organisationnelles afin d'identifier les vulnérabilités, les non-conformités et les risques potentiels.

L'objectif principal d'un audit de sécurité est de mesurer l'efficacité des dispositifs de protection existants face aux menaces internes et externes. Il permet de vérifier le respect des bonnes pratiques, des normes et des réglementations en vigueur, tout en évaluant la capacité du système d'information à garantir la confidentialité, l'intégrité, la disponibilité et la traçabilité des données.

Un audit de sécurité vise également à formuler des recommandations d'amélioration adaptées au contexte de l'entreprise. Ces recommandations permettent de renforcer la posture de sécurité globale, de réduire les risques identifiés et d'améliorer la gouvernance du système d'information. L'audit constitue ainsi un outil essentiel d'aide à la décision pour les responsables informatiques et les dirigeants.

12.1.2 Les 8 piliers de la cybersécurité

La cybersécurité repose sur un ensemble de principes fondamentaux, souvent regroupés en huit piliers complémentaires, qui permettent de structurer une stratégie de protection efficace du système d'information.

Gouvernance La gouvernance définit le cadre organisationnel, les responsabilités et les politiques de sécurité. Elle assure l'alignement de la cybersécurité avec les objectifs stratégiques de l'entreprise et garantit une prise de décision cohérente en matière de sécurité.

Gestion des risques La gestion des risques consiste à identifier, analyser et prioriser les menaces et les vulnérabilités afin de mettre en place des mesures de sécurité adaptées aux enjeux métiers et techniques.

Protection des actifs Ce pilier concerne la protection des systèmes, des réseaux, des applications et des données. Il repose sur des mécanismes tels que le contrôle d'accès, le chiffrement, la segmentation des environnements et la sécurisation des équipements.

Gestion des identités et des accès La gestion des identités et des accès vise à garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources nécessaires, selon le principe du moindre privilège et une authentification adaptée.

Détection des incidents La détection des incidents repose sur la supervision des systèmes, la journalisation des événements et l'analyse des comportements afin d'identifier rapidement toute activité anormale ou malveillante.

Réponse aux incidents Ce pilier définit les procédures et les moyens à mettre en œuvre en cas d'incident de sécurité, afin de limiter les impacts, de contenir l'attaque et de restaurer les services dans les meilleurs délais.

Continuité et résilience La continuité et la résilience visent à assurer le maintien ou la reprise des activités critiques malgré un incident majeur, grâce à des plans de continuité et de reprise d'activité adaptés.

Sensibilisation et formation des utilisateurs La sensibilisation et la formation permettent de réduire les risques liés au facteur humain en développant une culture de cybersécurité et en adoptant des comportements responsables au sein de l'organisation.

Ces huit piliers constituent un cadre structurant pour évaluer, renforcer et maintenir un niveau de cybersécurité cohérent avec les enjeux d'un système d'information d'entreprise.

12.1.3 Méthodologie d'évaluation

12.2 Mise en œuvre technique

12.2.1 Présentation du questionnaire de sécurité

Le questionnaire de sécurité s'organise autour de huit grands thèmes, qui reprennent l'ensemble des piliers essentiels de la cybersécurité au sein d'un système d'information. Il aide à faire le point sur le niveau de sécurité de l'entreprise, à mettre en lumière les atouts, mais aussi à cibler les zones de vulnérabilité. L'objectif ? Permettre de définir clairement les priorités d'action. Chaque catégorie rassemble des questions concrètes, conçues pour fournir un diagnostic solide et directement utilisable. Pour chaque question, un tableau Excel s'organisera sous trois colonnes. Question booléen, état de la SI actuelle, Point de remédiation et bonne pratique, c'est-à-dire les solutions à mettre en place.

Le questionnaire est créé pour XANADU. Ils doivent répondre de façon à nous en apprendre plus sur leur infrastructure. L'ensemble des questions sont posées de façon à recevoir une sortie booléenne en réponse. La partie Solution et bonne pratique est déjà préremplie par précaution. L'ensemble du questionnaire est disponible sous forme de fichier Excel en document séparé sous le nom « Questionnaire_{des}securit^z ».

Sécurité applicative

Les applications métiers, notamment l'ERP ainsi que les services Office 365, doivent bénéficier de système de sécurité tels qu'une authentification forte, le chiffrement des data sans oublié la journalisation des accès. La gestion des versions applicatives via des pipelines CI/CD limite fortement les risques d'erreurs humaines et améliore la traçabilité des déploiements. Des audits de sécurité réguliers, incluant des tests du pentesting, sont fortement conseiller pour identifier les vulnérabilités applicatives

12.2.2 Analyse par thématique

Gestion des identités et des accès (IAM)

L'analyse des identités est des accès pointe l'importance de renforcer les mécanismes d'authentification et du contrôle des comptes utilisateurs. Une politique doit être effectuer sur les points suivants. Les mots de passes, la gestion des comptes générique ainsi que la séparation des priviléges. Le laxisme pourrait engendrer un risque de sécurité majeurs si ces points ne sont pas traiter dans notre questionnaire.

Protection des postes de travail.

Les postes de travail constitue un vecteur d'attaque priviliégié. Les droits des utilisateur doivent êtres limité. Cela réduit les risques d'erreurs qui pourrait venir des erreurs humaines. Bien qu'une protection antivirus soit envisagé, un EDR pourrait être déployer sur l'ensbles des postes de travail.

Sécurité du réseau

La sécurité du réseau repose avant tout sur une bonne segmentation à l'aide de VLANs, afin de séparer les différents services et de limiter la propagation d'attaques en cas d'incident interne. Sans filtrage par défaut type : deny-all, le réseau reste exposé à des flux non contrôlés, notamment issus de mails malveillants. Il devient donc essentiel de déployer des solutions de sécurité périmétrique adaptées (IDS/IPS,) et d'assurer la surveillance continue des flux réseau pour détecter rapidement tout comportement anormal. Enfin, les connexions VPN inter-sites doivent être protégées via des mécanismes d'authentification renforcés pour assurer les échanges sécurisés entre les sites.

Protection des données

La protection des données se base sur une approche globale visant à mieux identifier et sécuriser les informations sensibles. Cela peut passer par une classification des data, le chiffrement, aussi bien au repos que lors des échanges, ainsi que par la mise en place de mécanismes de prévention des fuites de données (DLP). En effet, sans une politique de rétention clairement définie, l'entreprise s'expose à de lourds risques juridiques et réglementaires,(Norme européenne RGPD)

Continuité d'activité

L'analyse de la continuité d'activité démontre que les RPO et RTO doivent être clairement définis pour tous les services critiques. Le respect de la règle de sauvegarde 3-2-1/3-2-1 ainsi que la réalisation régulière de tests de restauration sont obligatoire pour garantir la reprise rapide des activités en cas de problèmes. La mise en place des plans PCA et PRA permet de structurer les actions à réaliser en cas de crise et d'assurer une coordination efficace entre les équipes.

Sensibilisation et gouvernance

La dernière partie du questionnaire se base sur la sensibilisation des utilisateurs et la gouvernance de la sécurité sont des leviers essentiels. La création d'une formation anti-phishing, la diffusion d'une charte informatique dans des endroit stratégiques(Machine à

café, mail de distribution) et la désignation d'un RSSI permettent de structurer la politique de sécurité de l'entreprise. La mise en place de procédures formelles de gestion des incidents ainsi que des exercices de crise renforce la capacité de réaction face aux cybermenaces.

12.2.3 Axes de remédiation identifiés

- Renforcement de la gestion des identités et des accès (IAM).
- Sécurisation des postes de travail et des serveurs.
- Amélioration de la segmentation du réseau.
- Mise en conformité des pratiques de sauvegarde et de continuité d'activité.
- Adoption de standards de sécurité reconnus.
- Automatisation des processus critiques.
- Centralisation de la supervision et des journaux (logs).
- Intégration de solutions de sécurité avancées :
 - EDR (Endpoint Detection and Response),
 - SIEM (Security Information and Event Management),
 - DLP (Data Loss Prevention).

12.2.4 Plan d'actions correctif

- **Court terme**
 - Mise en place de politiques de mots de passe conformes aux standards NIST.
 - Déploiement de l'authentification multifacteur (MFA) sur l'ensemble des accès sensibles.
 - Suppression progressive des comptes partagés.
- **Moyen terme**
 - Généralisation du chiffrement des postes de travail et des serveurs.
 - Segmentation complète du réseau en VLANs.
 - Intégration d'une supervision centralisée via un SIEM.
- **Long terme**
 - Renforcement de la gouvernance de la sécurité par la nomination d'un RSSI.
 - Formalisation des plans de continuité et de reprise d'activité (PCA/PRA).
 - Mise en œuvre de campagnes régulières de sensibilisation à la sécurité.
 - Organisation d'exercices de gestion de crise.

Chapitre 13

Garanties DICT

13.1 Fondamentaux

13.1.1 Définition des principes DICT

Les garanties DICT sont les principes de base de la sécurité des systèmes d'information. Utilisées pour définir les objectifs essentiels permettant de protéger les données, les ressources et les services du système d'information face aux incidents, aux erreurs humaines ou aux attaques.

La **Disponibilité** correspond au fait que les services du système d'information soient accessibles lorsque les utilisateurs en ont besoin. Ce qui signifie que les serveurs, les applications et les données doivent rester opérationnels le plus possible. Pour arriver à faire ça, on s'appuie notamment sur la redondance des équipements, les sauvegardes, la surveillance des serveurs et la mise en place de plans de continuité ou de reprise d'activité en cas de panne.

L'**Intégrité** cherche à garantir que les données restent fiables et cohérentes. Les informations ne doivent pas être modifiées, supprimées ou altérées sans autorisation. Cette garantie est assurée par des contrôles d'accès, des droits bien définis et des mécanismes de journalisation permettant de détecter toute modification non prévue.

La **Confidentialité** assure que seules les personnes autorisées peuvent accéder aux données sensibles. Elle repose principalement sur l'authentification des utilisateurs, la gestion des droits via les groupes Active Directory, ainsi que sur la séparation des accès entre les différents services. L'objectif est d'éviter toute fuite ou consultation non autorisée d'informations.

Enfin, la **Traçabilité** est le fait de conserver une trace des actions réalisées sur le système d'information. Grâce aux journaux d'événements et aux logs, il est possible d'identifier qui a fait quoi, et à quel moment. Cette traçabilité est essentielle pour analyser un incident, comprendre l'origine d'un problème ou répondre à des besoins d'audit et de sécurité.

13.1.2 Importance pour un SI d'entreprise

Dans un système d'information d'entreprise, le respect des garanties DICT est indispensable pour assurer le bon fonctionnement des activités et la protection des ressources numériques. La disponibilité des services informatiques conditionne directement la continuité de l'activité et la productivité des utilisateurs. Une indisponibilité prolongée peut

entraîner des pertes financières importantes et nuire à l'image de l'entreprise.

L'intégrité des données est essentielle pour garantir la fiabilité des informations utilisées dans les processus métiers et la prise de décision. Toute altération non maîtrisée des données peut engendrer des erreurs opérationnelles, des dysfonctionnements applicatifs ou des incohérences dans les systèmes.

La confidentialité revêt une importance particulière dans un contexte où les entreprises manipulent des données sensibles, stratégiques ou personnelles. Une violation de la confidentialité peut avoir des conséquences juridiques, notamment au regard des réglementations en vigueur, ainsi que des impacts économiques et réputationnels.

Enfin, la traçabilité constitue un élément clé pour la détection des incidents de sécurité, l'audit des systèmes et la responsabilisation des utilisateurs et des administrateurs. Elle permet également de répondre aux exigences de conformité et de renforcer la gouvernance du système d'information.

Ainsi, les garanties DICT forment un socle fondamental pour concevoir, exploiter et sécuriser un système d'information d'entreprise de manière fiable et durable.

13.2 Éléments techniques garantissant le DICT

Assurer les garanties DICT dans un système d'information passe par des mesures concrètes qui protègent les données et les services.

13.2.1 Confidentialité

Il s'agit de faire en sorte que seules les personnes autorisées puissent accéder aux informations. Cela se fait via une authentification fiable, la gestion des droits et des groupes, ainsi que le chiffrement des données et la segmentation du réseau pour limiter les risques de fuite.

13.2.2 Intégrité

Les données doivent rester exactes et cohérentes. Pour cela, on contrôle les accès, on enregistre les modifications et on réalise des sauvegardes régulières pour pouvoir restaurer les informations en cas d'erreur ou d'incident.

13.2.3 Disponibilité

les services doivent être accessibles quand les utilisateurs en ont besoin. La redondance des équipements, la supervision des systèmes et les plans de continuité permettent de limiter les interruptions et de reprendre rapidement les activités après un incident.

13.2.4 Traçabilité

Chaque action sur le système doit pouvoir être suivie. Les journaux et logs enregistrent les accès et modifications, ce qui permet d'analyser les incidents, de répondre aux audits et d'assurer la responsabilité des utilisateurs et administrateurs.

Chapitre 14

Estimations Budgétaires

Ce chapitre présente une estimation complète des coûts associés au déploiement du nouveau système d'information de XANADU. L'objectif est de fournir à la direction une vision claire et transparente de l'investissement nécessaire pour transformer l'infrastructure actuelle en un environnement moderne, sécurisé et hautement disponible.

L'estimation budgétaire se structure en trois grandes catégories : les coûts matériels (serveurs, équipements réseau, stockage), les coûts logiciels et licences (systèmes d'exploitation, outils de supervision), et enfin les coûts de mise en œuvre (installation, configuration, formation). Cette approche permet d'identifier précisément chaque poste de dépense et d'anticiper les besoins de trésorerie sur la durée du projet.

14.1 Coûts matériels

Les coûts matériels représentent l'investissement initial le plus important du projet. Ils couvrent l'ensemble des équipements physiques nécessaires au fonctionnement de l'infrastructure : serveurs, équipements réseau, systèmes de stockage et périphériques.

14.1.1 Infrastructure serveurs et virtualisation

L'infrastructure de virtualisation constitue le socle technique du nouveau système d'information. Elle repose sur deux serveurs physiques haute performance déployés sur chaque site, permettant d'héberger l'ensemble des machines virtuelles nécessaires.

Serveurs physiques pour hyperviseurs ESXi

Équipement	Spécifications	Prix unitaire (€)
Serveur ESXi Atlantis 1	Intel Xeon 16 cœurs, 128 Go RAM, 2× SSD 1 To NVMe, RAID	8 500
Serveur ESXi Atlantis 2	Intel Xeon 16 cœurs, 128 Go RAM, 2× SSD 1 To NVMe, RAID	8 500
Serveur ESXi Springfield	Intel Xeon 12 cœurs, 64 Go RAM, 2× SSD 512 Go NVMe, RAID	6 000
Sous-total Infrastructure Serveurs		23 000

TABLE 14.1 – Coûts serveurs physiques pour virtualisation

Justification : Le dimensionnement des serveurs a été calculé pour supporter l'ensemble des machines virtuelles identifiées dans le projet, avec une marge de 30% pour anticiper la croissance future. La redondance sur le site d'Atlantis garantit une haute disponibilité conforme aux exigences RTO de 4 heures.

Infrastructure de sauvegarde

Comme détaillé dans le chapitre 8, l'infrastructure de sauvegarde repose sur TrueNAS avec réPLICATION inter-sites et sauvegardes offline LTO.

Composant	Prix (€)
Serveur TrueNAS Atlantis (8 cœurs, 64 Go RAM, 6× 4 To)	8 500
Serveur TrueNAS Springfield (8 cœurs, 64 Go RAM, 6× 4 To)	8 500
Lecteur LTO-8	3 000
Bandes LTO-8 (×10)	600
Onduleurs APC 3000VA (×2)	1 200
Installation et câblage	400
Sous-total Infrastructure Sauvegarde	22 200

TABLE 14.2 – Coûts infrastructure de sauvegarde

14.1.2 Équipements réseau et sécurité

La segmentation réseau par VLANs et la sécurité périphérique nécessitent des équipements réseau performants et fiables, capables de gérer le trafic entre les deux sites via la liaison MPLS.

Pare-feux et équipements de sécurité

Équipement	Spécifications	Prix unitaire (€)
Appliance OPNsense Atlantis	8 cœurs, 16 Go RAM, 4× ports 1 GbE	2 500
Appliance OPNsense Atlantis (HA)	8 cœurs, 16 Go RAM, 4× ports 1 GbE	2 500
Appliance OPNsense Springfield	4 cœurs, 8 Go RAM, 4× ports 1 GbE	1 800
Sous-total Pare-feux		6 800

TABLE 14.3 – Coûts pare-feux OPNsense

Commutateurs réseau

14.1.3 Liaison MPLS inter-sites

Note : Les coûts récurrents mensuels de la liaison MPLS (environ 800 €/mois) ne sont pas inclus dans l'investissement initial mais seront intégrés au budget de fonctionnement annuel.

Équipement	Spécifications	Prix unitaire (€)
Switch manageable Atlantis (Core)	48 ports GbE, 4× SFP+, support VLAN	3 500
Switch manageable Atlantis (Accès)	24 ports GbE, support VLAN	1 200
Switch manageable Springfield	24 ports GbE, support VLAN	1 200
Câbles réseau et baies de brassage	Câbles Cat6, panneaux de brassage	800
Sous-total Équipements Réseau		6 700

TABLE 14.4 – Coûts commutateurs et câblage réseau

Composant	Coût initial (€)
Frais de mise en service MPLS 1 Gbps	2 000
Routeur MPLS Atlantis (fourni par opérateur)	Inclus
Routeur MPLS Springfield (fourni par opérateur)	Inclus
Sous-total Liaison MPLS	2 000

TABLE 14.5 – Coûts liaison MPLS

14.1.4 Postes de travail et périphériques

14.1.5 Récapitulatif des coûts matériels

14.2 Coûts logiciels et licences

L’architecture technique du projet XANADU privilégie les solutions open source lorsque cela est possible, permettant de réduire significativement les coûts de licences tout en garantissant des solutions robustes et éprouvées.

14.2.1 Licences Microsoft

Windows Server

Justification : Les licences Windows Server Standard incluent les droits de virtualisation pour 2 machines virtuelles par licence physique. Les CAL (Client Access Licenses) sont nécessaires pour chaque utilisateur accédant aux services Windows Server.

Office 365 et services Microsoft

Note : Office 365 est un abonnement annuel. Le coût indiqué correspond à la première année d’utilisation et sera reconduit annuellement.

14.2.2 Licences de virtualisation

Justification : Le projet utilise la version gratuite d’ESXi, suffisante pour les besoins de XANADU. Proxmox VE est open source et ne nécessite pas de licence.

14.2.3 Solutions open source (gratuites)

Le projet s’appuie sur un ensemble de solutions open source performantes et éprouvées, permettant d’éliminer les coûts de licences sur plusieurs composants critiques de l’infrastructure.

Équipement	Quantité	Prix unitaire (€)	Total (€)
Postes utilisateurs (renouvellement)	20	800	16 000
Imprimantes réseau professionnelles	4	1 500	6 000
Onduleurs pour postes critiques	10	150	1 500
Sous-total Postes et Périphériques			23 500

TABLE 14.6 – Coûts postes de travail et périphériques

Catégorie	Montant (€)
Infrastructure serveurs et virtualisation	23 000
Infrastructure de sauvegarde	22 200
Pare-feux et sécurité	6 800
Équipements réseau	6 700
Liaison MPLS (mise en service)	2 000
Postes et périphériques	23 500
TOTAL COÛTS MATERIELS	84 200

TABLE 14.7 – Récapitulatif des coûts matériels

14.2.4 Logiciels complémentaires et outils

14.2.5 Récapitulatif des coûts logiciels et licences

Observation importante : L'utilisation massive de solutions open source (OPNsense, TrueNAS, CheckMK, PostgreSQL) permet une économie substantielle estimée à plus de 40 000 € par rapport à des solutions commerciales équivalentes (Fortinet, Veeam, PRTG, Oracle Database).

14.3 Coûts de mise en œuvre

Les coûts de mise en œuvre englobent l'ensemble des prestations nécessaires pour installer, configurer et déployer la nouvelle infrastructure, ainsi que pour former les utilisateurs et les administrateurs.

14.3.1 Prestations d'installation et de configuration

Installation infrastructure physique

Configuration services et applications

14.3.2 Tests, validation et documentation

14.3.3 Formation des équipes

La formation constitue un élément essentiel pour garantir l'autonomie de l'équipe informatique de XANADU dans l'administration quotidienne de la nouvelle infrastructure.

14.3.4 Gestion de projet et accompagnement

Produit	Quantité	Prix unitaire (€)	Total (€)
Windows Server 2022 Standard (DC-01, DC-02, DC-03, FS-01, ERP-APP)	5	1 200	6 000
CAL utilisateur Windows Server	60	45	2 700
Sous-total Windows Server			8 700

TABLE 14.8 – Coûts licences Windows Server

Produit	Quantité	Coût annuel/unité (€)	Total annuel (€)
Microsoft 365 Business Standard	60	144	8 640
Coût annuel Office 365			8 640

TABLE 14.9 – Coûts licences Office 365

14.3.5 Récapitulatif des coûts de mise en œuvre

14.4 Coût total estimé

Cette section présente une vue consolidée de l'ensemble des investissements nécessaires au déploiement du nouveau système d'information de XANADU, ainsi qu'une projection des coûts récurrents sur 5 ans.

14.4.1 Investissement initial

14.4.2 Coûts récurrents annuels

Au-delà de l'investissement initial, le fonctionnement de la nouvelle infrastructure engendre des coûts récurrents annuels qu'il convient d'anticiper dans le budget de fonctionnement de l'entreprise.

14.4.3 Coût total de possession (TCO) sur 5 ans

Le coût total de possession (Total Cost of Ownership - TCO) permet d'évaluer l'investissement global sur une période de 5 ans, incluant l'investissement initial et les coûts de fonctionnement récurrents.

14.4.4 Analyse et justification de l'investissement

Comparaison avec les risques de l'existant

L'infrastructure actuelle de XANADU présente des risques critiques qui, en cas de matérialisation, entraîneraient des coûts bien supérieurs à l'investissement proposé :

- **Panne du serveur unique** : Arrêt complet des activités pendant plusieurs jours, coût estimé à 50 000 € par jour d'interruption (perte de chiffre d'affaires, pénalités clients, heures supplémentaires)
- **Attaque ransomware** : Rançon potentielle de 100 000 à 500 000 €, plus les coûts de récupération et la perte de réputation
- **Perte de données** : Coût estimé entre 80 000 et 200 000 € selon l'ampleur (reconstitution, impact commercial)

Produit	Coût (€)
VMware vSphere ESXi (version gratuite)	0
Proxmox VE (open source)	0
Sous-total Virtualisation	0

TABLE 14.10 – Coûts licences de virtualisation

Solution	Usage	Coût (€)
OPNsense	Pare-feu et filtrage réseau	0
TrueNAS Core	Système de sauvegarde	0
CheckMK Raw Edition	Supervision et monitoring	0
PostgreSQL	Base de données ERP	0
Rocky Linux	Serveurs Linux (laboratoire Springfield)	0
WireGuard	VPN pour télétravail	0
Sous-total Solutions Open Source		0

TABLE 14.11 – Solutions open source utilisées

Retour sur investissement (ROI)

L’investissement se justifie par plusieurs gains tangibles :

- **Gains de productivité** : Réduction de 30% du temps consacré aux tâches d’administration système grâce à l’automatisation et la supervision, soit environ 15 000 €/an
- **Réduction des temps d’arrêt** : Passage d’un RTO théorique de plusieurs jours à 4 heures maximum, évitant des pertes estimées à 40 000 €/an
- **Économies sur solutions propriétaires** : L’utilisation de solutions open source permet d’éviter 40 000 € de licences annuelles par rapport à des alternatives commerciales
- **Évolutivité** : L’infrastructure virtualisée permet d’absorber une croissance de 50% sans nouvel investissement majeur

Le retour sur investissement est estimé à 3,2 ans, ce qui est excellent pour un projet d’infrastructure de cette envergure.

Phasage budgétaire recommandé

Pour faciliter le financement du projet, un phasage de l’investissement peut être envisagé :

Recommandation : Bien que le phasage soit possible, il est fortement recommandé de déployer l’ensemble de la solution en une seule phase pour bénéficier immédiatement de la redondance et de la haute disponibilité, conformément aux objectifs RTO/RPO définis.

14.4.5 Comparaison avec des solutions alternatives

Pour mettre en perspective l’investissement proposé, voici une comparaison avec des solutions alternatives :

Analyse : La solution proposée offre le meilleur rapport coût/performance sur 5 ans, avec une économie de 175 860 € par rapport à une solution 100% commerciale, tout en conservant la maîtrise totale de l’infrastructure et des données.

Logiciel	Quantité	Prix unitaire (€)	Total (€)
Antivirus entreprise (3 ans)	60 postes	35/an/poste	6 300
Logiciel de ticketing	Licence PME	1 200	1 200
Outils d'administration réseau	Suite complète	800	800
Sous-total Logiciels Complémentaires			8 300

TABLE 14.12 – Coûts logiciels complémentaires

Catégorie	Montant (€)
Licences Windows Server (ponctuel)	8 700
Office 365 (première année)	8 640
Virtualisation (open source)	0
Solutions open source	0
Logiciels complémentaires	8 300
TOTAL COÛTS LOGICIELS (investissement initial)	25 640

TABLE 14.13 – Récapitulatif des coûts logiciels et licences

14.4.6 Synthèse exécutive

Le projet de refonte du système d’information de XANADU représente un investissement total de **175 940 €**, avec des coûts récurrents annuels de **30 640 €**, soit un TCO sur 5 ans de **329 140 €**.

Points clés :

- L’investissement élimine le point de défaillance unique actuel et garantit un RTO de 4 heures
- Le recours massif à l’open source permet une économie de plus de 175 000 € sur 5 ans par rapport aux solutions propriétaires
- Le ROI est atteint en 3,2 ans grâce aux gains de productivité et à la réduction des risques
- La solution proposée offre une évolutivité permettant d’absorber 50% de croissance sans investissement supplémentaire majeur
- Les coûts récurrents annuels (30 640 €) représentent 511 € par utilisateur et par an, ce qui est très compétitif pour une infrastructure de cette qualité

Recommandation finale : L’investissement proposé est cohérent avec les enjeux stratégiques de XANADU et représente une solution pérenne, évolutive et économiquement viable pour sécuriser et moderniser le système d’information de l’entreprise.

Prestation	Durée estimée	Coût (€)
Installation serveurs physiques Atlantis	2 jours	2 000
Installation serveur physique Springfield	1 jour	1 000
Configuration hyperviseurs ESXi	2 jours	2 000
Mise en place infrastructure réseau	3 jours	3 000
Installation et configuration pare-feux	2 jours	2 500
Configuration liaison MPLS	1 jour	1 500
Sous-total Installation Infrastructure		12 000

TABLE 14.14 – Coûts installation infrastructure physique

Prestation	Durée estimée	Coût (€)
Déploiement Active Directory (3 DC)	2 jours	2 500
Configuration DNS et DHCP	1 jour	1 000
Mise en place serveur de fichiers (FS-01)	1 jour	1 200
Configuration VLANs et segmentation réseau	2 jours	2 500
Déploiement infrastructure de sauvegarde	2 jours	2 500
Configuration CheckMK (supervision)	1 jour	1 500
Configuration VPN WireGuard	1 jour	1 200
Migration données existantes	2 jours	2 500
Sous-total Configuration Services		14 900

TABLE 14.15 – Coûts configuration services et applications

Prestation	Durée estimée	Coût (€)
Tests de charge et performance	2 jours	2 000
Tests de basculement et haute disponibilité	2 jours	2 500
Validation sauvegardes et restauration	1 jour	1 500
Tests de sécurité et audits	2 jours	3 000
Documentation technique complète	3 jours	3 500
Procédures d'exploitation	2 jours	2 000
Sous-total Tests et Documentation		14 500

TABLE 14.16 – Coûts tests, validation et documentation

Formation	Participants	Durée	Coût (€)
Administration Windows Server et AD	3 personnes	3 jours	3 500
Gestion pare-feu OPNsense	2 personnes	2 jours	2 000
Administration TrueNAS et sauvegardes	2 personnes	2 jours	2 000
Utilisation CheckMK (supervision)	2 personnes	1 jour	1 200
Sensibilisation sécurité utilisateurs	60 personnes	0,5 jour	2 500
Sous-total Formation			11 200

TABLE 14.17 – Coûts formation des équipes

Prestation	Coût (€)
Chef de projet (suivi sur 3 mois)	8 000
Accompagnement post-déploiement (1 mois)	3 000
Support technique garantie (3 mois)	2 500
Sous-total Gestion de Projet	13 500

TABLE 14.18 – Coûts gestion de projet et accompagnement

Catégorie	Montant (€)
Installation infrastructure physique	12 000
Configuration services et applications	14 900
Tests, validation et documentation	14 500
Formation des équipes	11 200
Gestion de projet et accompagnement	13 500
TOTAL COÛTS DE MISE EN ŒUVRE	66 100

TABLE 14.19 – Récapitulatif des coûts de mise en œuvre

Catégorie	Montant (€)	% du total
Coûts matériels	84 200	47,9%
Coûts logiciels et licences	25 640	14,6%
Coûts de mise en œuvre	66 100	37,5%
INVESTISSEMENT INITIAL TOTAL	175 940	100%

TABLE 14.20 – Investissement initial total

Poste de dépense	Coût annuel (€)
Liaison MPLS (800 €/mois × 12)	9 600
Office 365 (60 licences)	8 640
Renouvellement antivirus	2 100
Maintenance matérielle (serveurs, équipements réseau)	4 500
Électricité (serveurs et équipements)	3 200
Bandes LTO (renouvellement annuel)	600
Support et mises à jour logicielles	2 000
TOTAL COÛTS RÉCURRENTS ANNUELS	30 640

TABLE 14.21 – Coûts récurrents annuels

Poste	Montant (€)
Investissement initial (année 0)	175 940
Coûts récurrents annuels	30 640
Coûts récurrents sur 5 ans (30 640 × 5)	153 200
COÛT TOTAL DE POSSESSION (TCO 5 ans)	329 140
Coût annuel moyen	65 828
Coût par utilisateur par an	1 097

TABLE 14.22 – Coût total de possession sur 5 ans

Phase	Composants	Montant (€)
Phase 1 (critique)	Serveurs Atlantis, pare-feux, AD, sauvegardes, formation	95 000
Phase 2 (3 mois)	Site Springfield, MPLS, réPLICATION	50 000
Phase 3 (6 mois)	Postes utilisateurs, périphériques	30 940
TOTAL		175 940

TABLE 14.23 – Phasage budgétaire recommandé

Solution	Investissement initial (€)	Coûts annuels (€)	TCO 5 ans (€)
Solution proposée (open source + Microsoft)	175 940	30 640	329 140
Solution 100% commerciale (Fortinet, Veeam, PRTG)	245 000	52 000	505 000
Solution cloud hybride (Azure + on-premise)	95 000	48 000	335 000
Solution 100% cloud (tout en SaaS)	25 000	65 000	350 000

TABLE 14.24 – Comparaison TCO 5 ans avec solutions alternatives

Chapitre 15

Conclusion

15.1 Synthèse des apports du nouveau SI

La refonte du système d'information a permis de transformer une infrastructure fragile en un environnement solide et moderne. Le premier grand apport est la **centralisation** : grâce à l'Active Directory, toutes les identités et les accès sont gérés au même endroit, ce qui met fin au désordre des comptes locaux.

Ensuite, la mise en place de serveurs dédiés (FS-01 pour les fichiers, WSUS pour les mises à jour) apporte une structure claire. L'utilisation de la virtualisation offre également une souplesse qu'on n'avait pas avant : on peut désormais sauvegarder, cloner ou restaurer un serveur en quelques minutes en cas de problème.

15.2 Bénéfices attendus pour XANADU

Pour l'entreprise et ses employés, les bénéfices sont concrets :

- **Gain de temps** : Les nouveaux arrivants ont leurs accès instantanément grâce aux groupes de sécurité, et les mises à jour ne bloquent plus les postes pendant les heures de travail.
- **Sécurité renforcée** : Le principe du moindre privilège et le MFA protègent les données sensibles. Même si un mot de passe est volé, l'infrastructure reste protégée.
- **Sérénité** : Avec un vrai plan de sauvegarde et une supervision constante (Wazuh, CheckMK), la direction peut être rassurée sur la continuité de son activité, même en cas d'incident technique.

15.3 Conformité aux exigences du cahier des charges

Ce nouveau SI répond point par point aux demandes initiales du projet. Nous avons respecté les piliers de la sécurité informatique :

- **Confidentialité** : Les dossiers sont cloisonnés par service.
- **Intégrité** : Seules les personnes autorisées peuvent modifier les documents officiels.
- **Disponibilité** : La stratégie multi-sites avec le RODC à Springfield garantit que le travail continue même si la connexion avec le siège est perturbée.
- **Traçabilité** : Toutes les actions importantes sont loguées, ce qui permet de savoir "qui a fait quoi" en cas d'anomalie.

15.4 Perspectives d'évolution

Le système que nous avons livré est évolutif. Pour la suite, XANADU pourrait envisager plusieurs pistes pour renforcer encore son avance technologique :

- **Passage au Cloud hybride** : Déporter une partie des sauvegardes sur Azure ou AWS pour une sécurité maximale hors site.
- **Zéro Trust** : Renforcer encore les accès distants pour que chaque connexion soit vérifiée scrupuleusement, peu importe d'où elle vient.
- **Automatisation avancée** : Utiliser davantage de scripts pour gérer l'inventaire matériel et logiciel de manière totalement autonome.

En résumé, XANADU dispose aujourd'hui d'une base saine et sécurisée, capable de soutenir son développement pour les années à venir.