

Livrable 3

Projet : Sécurité et administration



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

Sommaire

Préambule	7
Rappel du contexte	7
Rappel des attentes du client	8
Objectifs du livrable 3.....	11
Infrastructure et cartographie	12
Plateforme de visualisation Proxmox	12
Installation et initialisation de l'hôte Proxmox	12
Configuration réseau de l'hôte Proxmox.....	13
Accès distant sécurisé à Proxmox via Tailscale	14
Apport du travail réalisé sur Proxmox dans la maquette	15
Schéma du S.I.	16
Schéma du S.I. actuel.....	16
Schéma du S.I. modélisé par CesiTech	17
Configuration du réseau.....	18
Cloisonnement réseau et VLAN	18
Sécurisation périphérique : Firewall, DMZ et VPN	18
Serveur Contrôleur de Domaine	19
Interface de l'ERP	19
NAS et gestion des données	20
Plan d'adressage	20
Mise en place du routage avec PfSense.....	23
Mise en place de l'infrastructure réseau avec PfSense.....	23
Création de la machine virtuelle PfSense Atlantis et choix des interfaces ...	23
Segmentation du réseau par VLAN	24
Assignation et configuration des interfaces VLAN.....	25
Mise en place du service DHCP par VLAN.....	26
Configuration du lien MPLS entre Atlantis et Springfield	27
Gestion du NAT sortant.....	28
Mise en place de PfSense Springfield.....	29
Mise en place d'un VPN d'accès distant avec OpenVPN.....	30
1. Objectif de la mise en place du VPN	30
2. Architecture VPN retenue	30
3. Mise en place de l'infrastructure de certificats (PKI)	30
4. Création des certificats serveur et utilisateurs	31
5. Configuration du serveur OpenVPN	32
6. Mise en place des règles de pare-feu OpenVPN	33
7. Déploiement des clients VPN	33
8. Vérifications et tests de fonctionnement.....	34



Politique de filtrage.....	37
Politique de filtrage du pare-feu pfSense Atlantis.....	37
Politique de filtrage du pare-feu du PfSense Sprriegfeld	43
Un schéma logique du service Active Directory.....	45
Fonctionnement de l'AD	45
Stratégies de groupes	46
Paramétrage des GPO sur le serveur.....	47
Gestion des données	50
Plan de sauvegarde des données.....	50
Stratégie en place sur le réseau de XANADU	50
Objectifs et criticité des données	52
Plan de sauvegarde	52
Volumes de données	54
Conservation, supervision et traçabilité des sauvegardes	55
Network Attached Storage (NAS).....	57
Paramétrage du VM NAS	57
Déploiement de la machine virtuelle NAS (TrueNAS)	57
Organisation logique du stockage (datasets)	58
Mise en place des partages SMB	59
Gestion des droits d'accès via ACL	60
Cohérence entre ACL NAS et Active Directory	60
Activation de l'Access Based Enumeration (ABE).....	61
Rôle du NAS dans la stratégie globale de sauvegarde	61
Lien avec les stratégies de groupe (GPO).....	61
Apports de la solution NAS dans la maquette	62
Création d'un accès Web sécurisé	63
Création d'un serveur web	63
Sécurisation de l'accès web par certificat	64
Génération et signature du certificat.....	65
Mise en place du backend et de la base de données.....	67
Conception et développement du backend en Go	67
Mise en place des fonctionnalités de gestion des utilisateurs	67
Problématique d'exposition d'un service localhost	68
Sécurisation et validation de l'accès depuis l'extérieur	69
Supervision	70
Tableau des actions de Supervision	70
Description des actions de Supervision	71
Supervision d'authentification	71
Supervision de Sécurité	72
Supervision de sauvegarde	73
Solution de supervision	73



Sécurité des données.....	75
Confidentialité	75
Intégrité.....	75
Disponibilité	76
Traçabilité	76
Scripts	77
Gestion des utilisateurs.....	78
Sauvegarde de l'AD et DC.....	87
Sauvegarde et vérification de l'ERP	91
Conclusion générale	94
Questionnaire de Sécurité	95
Politique de sécurité.....	95
Formation des utilisateurs.....	96
Sécurisation des accès	96
Sécurisation des postes utilisateurs	97
Sécurisation des réseaux	97
Sécurisation des équipements.....	98
Sécurisation des sauvegardes.....	98
Sécurisation contre les malwares et ransomwares	99
Sécurisation en cas d'attaque.....	99
Conclusion	101
Glossaire	102
Annexes.....	104



Table des images

Figure 1 - Caractéristique SLA	9
Figure 2 - Interface Proxmox	12
Figure 3 - Adresse MAC	13
Figure 4 - Automatisation du réseau.....	14
Figure 5 - Statut du Systemctl	14
Figure 6 - Schéma du SI.....	16
Figure 7 - Schéma du S.I. modélisé par CESITech	17
Figure 8 - Tableaux des accès	20
Figure 9 - Adressage d'un VLAN du site principal	21
Figure 10 - Adressage des serveurs du site principal.....	21
Figure 11 - Adresses du routeur du bâtiment principal	21
Figure 12 - Adressage du site secondaire (Springfield).....	22
Figure 13 - Adressage de la DMZ.....	22
Figure 14 - Création des VLAN.....	24
Figure 15 - Création des VLAN sur le pfsense	25
Figure 16 – Activation de l'interface Vlan 10.....	26
Figure 17 – Activation du service DHCP sur le VLAN 10	27
Figure 18 - Activation de l'interface MPLS	28
Figure 19 – Création de la passerelle pointant sur Springfield	28
Figure 20 – Création de la route statique vers Springfield sur PfSense Atlantis.....	28
Figure 21 - Création autorité de certification.....	31
Figure 22 - Création du certificat du serveur OpenVPN	32
Figure 23 - Création du serveur OpenVPN.....	32
Figure 24 - Connection sur le VPN	33
Figure 25 - Connexion VPN Réussi.....	34
Figure 26 - Bien connecté au VPN	34
Figure 27 - Possibilité de ping	35
Figure 28 - Bon accès à la page Web	35
Figure 29 - Bonne résolution DNS	36
Figure 30 - Tableau de Filtrage de Atlantis.....	41
Figure 31 - Tableau de filtrage de Springfield.....	44
Figure 32 - Schéma de l'Active Directory.....	45
Figure 33 - Création d'une nouvelle GPO	48
Figure 34 - Stratégies de mot de passe.....	48
Figure 35 - Commande "gpupdate"	49
Figure 36 - Schéma du RAID 5.....	51
Figure 37 - Schéma de déduplication	51
Figure 38 - Plan de sauvegarde complet de Xanadu proposé par CesiTech.....	53
Figure 39 - Tableau du volume total de données	54
Figure 40 – Tableau récapitulatif du plan de sauvegarde	54



Figure 41 - Datasets	58
Figure 42 - Protocole SMB	59
Figure 43 - Installation du serveur IIS	63
Figure 44 - Gestionnaire IIS.....	63
Figure 45 - Liaisons du site web de Xanadu.....	64
Figure 46 - Connexion à l'interface web depuis un fichier client	64
Figure 47 - Version de Open SSL sur le serveur DNS	65
Figure 48 - Certificat signé (chiffré)	66
Figure 49 - Certificats sur le serveur IIS	66
Figure 50 - Certificats sur le serveur IIS	66
Figure 51 - Réécriture d'URL	68
Figure 52 - Configuration NSSM pour lancer le serveur Go	69
Figure 53 - Service API.....	69
Figure 54 - Tableau de Supervision.....	70
Figure 55 - Mail Exemple de Supervision	74
Figure 56 - Eléments de confidentialités.....	75
Figure 57 - Eléments d'Intégrité.....	75
Figure 58 - Eléments de Disponibilité	76
Figure 59 - Eléments de Traçabilité	76
Figure 60 - Architecture des scripts	79
Figure 61 - Fonction Select-FromList.....	80
<i>Figure 62 – Porte d'entrée du script</i>	81
Figure 63 - Fonction de création d'un utilisateur	82
Figure 64 - Récupération des OU	82
Figure 65 - Sélection d'un OU.....	82
Figure 66 - Création de l'utilisateur	83
Figure 67 - Exceptions dans la modification d'un utilisateur	83
Figure 68 - Affichage des OU et Users	84
Figure 69 - Suppression d'un utilisateur	85
Figure 70 - Fonction récursive de sélection d'un utilisateur de l'AD	86
Figure 71 - Initialize-EventLogSource.....	88
Figure 72 - Test-IsDC	88
Figure 73 - liste des tests réalisés sur le DC	89
Figure 74 - exécution des diagnostics du DC	89
Figure 75 - Résultat test-DC	90
Figure 76 - Informations de connexion au NAS	92
Figure 77 - test prérequis connexion au NAS	92
Figure 78 - Écriture BDD dans le NAS	93
Figure 79 - vérification des BDD dans le NAS	93
Figure 80 - Questionnaire de Sécurité récapitulatif proposé par CESITech	100
Annexe 1- L'affiche de bonnes pratiques informatique	104
Annexe 2 - Choix du paramètre à modifier 1	105



Préambule

Rappel du contexte

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

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

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

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

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



Rappel des attentes du client

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

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

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

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

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

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

Données critiques :

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

Données importantes :

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

Données moins critiques :

- Dossiers personnels des employés.

L'entreprise continuera d'utiliser :

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



- Office 365, incluant la messagerie Outlook.

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

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

Figure 1 - Caractéristique SLA

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

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

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

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

Volume des données

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

Infrastructure

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



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

Gestion des données

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

Sauvegardes

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

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

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

Antivirus

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

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

Mises à jour



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

Objectifs du livrable 3

Après avoir pris en compte toutes les requêtes du client nous allons mettre en place l'infrastructure complète ainsi que le réseau de l'entreprise Xanadu. Cette présentation sera proposée sous la forme d'une maquette réalisée sur des machines virtuelles (VM). Un serveur physique doté de Proxmox installé sur le réseau interne de CesiTech nous permettra de présenter notre travail et notre Proof Of Concept (POC) d'infrastructure et d'architecture.



Infrastructure et cartographie

Plateforme de visualisation Proxmox

Installation et initialisation de l'hôte Proxmox

Dans le cadre de la maquette du système d'information, nous avons mis en place une plateforme de virtualisation basée sur Proxmox VE. L'objectif est de disposer d'un environnement centralisé permettant d'héberger les machines virtuelles de l'infrastructure, de faciliter l'administration, et de démontrer la faisabilité des choix d'architecture proposés.

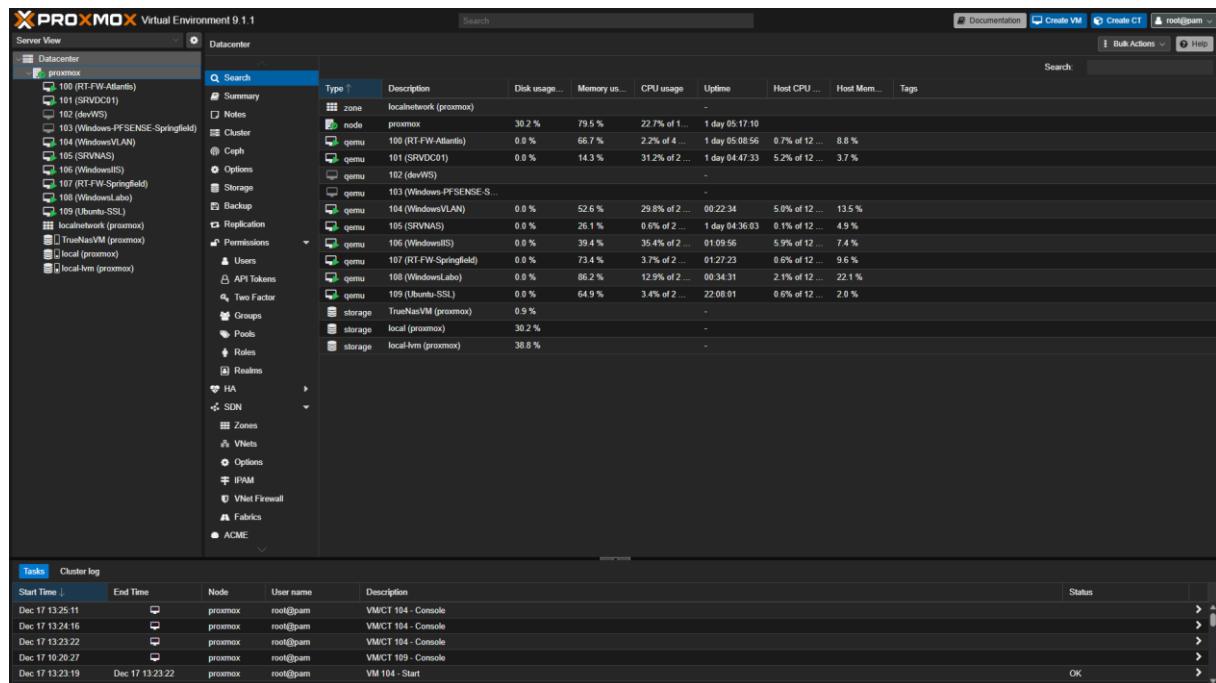


Figure 2 - Interface Proxmox

L'hôte Proxmox a été installé sur un serveur physique dédié. Une fois l'installation terminée, l'accès à l'administration se fait via l'interface web Proxmox, ce qui permet de gérer l'ensemble des paramètres de la plateforme : réseau, stockage, création de machines virtuelles, suivi de l'état des ressources et supervision de base.

Afin d'améliorer la résilience et de séparer les rôles, un NAS physique distinct a été mis en place et intégré à l'infrastructure. Ce NAS est utilisé comme espace de stockage pour héberger les disques des machines virtuelles. Il est déclaré comme stockage externe au niveau de Proxmox, ce qui permet de dissocier le calcul du stockage et de limiter l'impact d'une défaillance matérielle sur l'hôte.



Une attention particulière a été portée à la stabilité de l'hôte Proxmox, car il représente un point central de l'infrastructure : toute indisponibilité à ce niveau impacte l'ensemble des services virtualisés hébergés sur la plateforme.

Configuration réseau de l'hôte Proxmox

L'environnement de déploiement de la maquette impose une contrainte atypique pour un hyperviseur : l'accès au réseau se fait via un Wi-Fi protégé par un portail captif. Ce fonctionnement empêche l'hôte de disposer d'un accès Internet utilisable tant qu'une authentification n'a pas été réalisée, ce qui pose problème pour un serveur qui doit rester administrable et capable de mettre à jour ses composants.

Cette contrainte a nécessité une configuration réseau plus avancée que dans un déploiement classique en Ethernet, car Proxmox n'est pas conçu pour gérer de manière interactive un portail captif (absence de navigateur, usage serveur, redémarrages, démarrage sans interface graphique). La configuration réseau a été réalisée manuellement au niveau du système via le fichier `/etc/network/interfaces`. Ce choix permet de conserver une configuration persistante et maîtrisée, indépendante de manipulations ponctuelles.

Dans cet environnement, le portail captif repose sur une identification des équipements par adresse MAC. Or, sur un serveur Proxmox, l'usage n'est pas celui d'un poste utilisateur : l'authentification peut être perdue après un redémarrage ou lors d'un changement matériel, ce qui rend l'accès Internet instable. Pour stabiliser la situation, une adresse MAC de substitution a été configurée sur l'interface Wi-Fi. Cette configuration permet de présenter un identifiant constant au portail captif, facilitant la reconnexion et limitant les blocages liés aux changements de contexte réseau.

```
auto wlx0d362bfa046
iface wlx0d362bfa046 inet dhcp
    hwaddress ether 3c:a6:f6:4b:6a:d0
```

Figure 3 - Adresse MAC

Afin d'éviter une intervention manuelle après chaque redémarrage, une automatisation de la remise en service du Wi-Fi a été mise en place sur l'hôte Proxmox. L'objectif est que l'interface Wi-Fi soit activée, configurée et opérationnelle automatiquement, afin que l'accès à l'administration Proxmox soit rétabli le plus rapidement possible.



Cette automatisation contribue directement à la continuité d'activité de la plateforme de virtualisation. Dans le cadre du projet, elle sert également de preuve de viabilité : l'infrastructure doit pouvoir redémarrer et revenir à un état administrable sans dépendre d'actions manuelles longues ou incertaines.

```
root@proxmox:~# cat /usr/local/bin/wifi-start.sh
#!/bin/bash

# Attendre le chargement complet du noyau + réseau
sleep 5

# Activer l'interface
ip link set wlxe0d362bfa046 up

# Charger wpa_supplicant
wpa_supplicant -i wlxe0d362bfa046 -c /etc/wpa_supplicant/wpa_supplicant-wifi.conf -B

# DHCP pour récupérer une IP
dhclient wlxe0d362bfa046

echo 1 > /proc/sys/net/ipv4/ip_forward
```

Figure 4 - Automatisation du réseau

Accès distant sécurisé à Proxmox via Tailscale

Un accès distant sécurisé à l'hôte Proxmox a été mis en place via Tailscale, afin de garantir une administration possible même depuis un réseau externe. Ce point répond au besoin global d'accès distant, mais il est surtout utile dans la maquette pour conserver un accès d'administration fiable malgré les contraintes réseaux locaux.

Tailscale crée un réseau privé chiffré basé sur WireGuard, sans ouverture de ports côté pare-feu. Cette solution est adaptée à un environnement derrière NAT ou portail captif, car elle repose sur des connexions sortantes initiées par l'hôte. Grâce à cela, l'interface web de Proxmox peut être administrée à distance de manière sécurisée, et les opérations d'exploitation peuvent être réalisées sans dépendre d'un accès local direct.

```
root@proxmox:~# systemctl status tailscaled
● tailscaled.service - Tailscale node agent
   Loaded: loaded (/usr/lib/systemd/system/tailscaled.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-12-16 08:28:54 CET; 1 day 5h ago
     Invocation: aldc622312cf4830ace5510c40305e56
   Docs: https://tailscale.com/kb/
 Main PID: 837 (tailscaled)
   Status: "Connected: youcefafane@gmail.com; 100.73.141.77 fd7a:115c:ale0::8001:8d84"
    Tasks: 19 (limit: 37872)
   Memory: 87.4M (peak: 166.9M, swap: 13.1M, swap peak: 33M)
     CPU: 16min 46.882s
    CGroup: /system.slice/tailscaled.service
           └─837 /usr/sbin/tailscaled --state=/var/lib/tailscale/tailscaled.state --socket=/run/tailscale/tailscaled.sock --port=41641
```

Figure 5 - Statut du Systemctl



Apport du travail réalisé sur Proxmox dans la maquette

La configuration Proxmox mise en place démontre la capacité à déployer une plateforme de virtualisation administrable et exploitable même en environnement contraint. La maîtrise de la configuration réseau, la stabilisation de l'accès via le Wi-Fi captif, l'automatisation au démarrage et la mise en place d'un accès distant sécurisé constituent des éléments concrets répondant aux exigences de disponibilité et de facilité d'administration attendues dans le projet.

Cette partie fournit également des bases solides pour la suite de la maquette, notamment l'hébergement des VM d'infrastructure et l'intégration des services de stockage et de sauvegarde.



Schéma du S.I.

Schéma du S.I. actuel

Afin d'améliorer au mieux l'infrastructure du S.I. de Xanadu lors du déménagement, nous avons tout d'abord repris l'organisation actuelle de l'entreprise.

A l'aide des informations fournies, nous pouvons reconstituer le schéma du S.I.

Site Atlantis (central) :

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

Site Springfield (laboratoire) :

- Deux serveurs Linux pour pilotage et collecte
- Postes utilisateurs reliés au réseau local
- Photocopieuse, imprimante métier
- Routeur MPLS opérateur

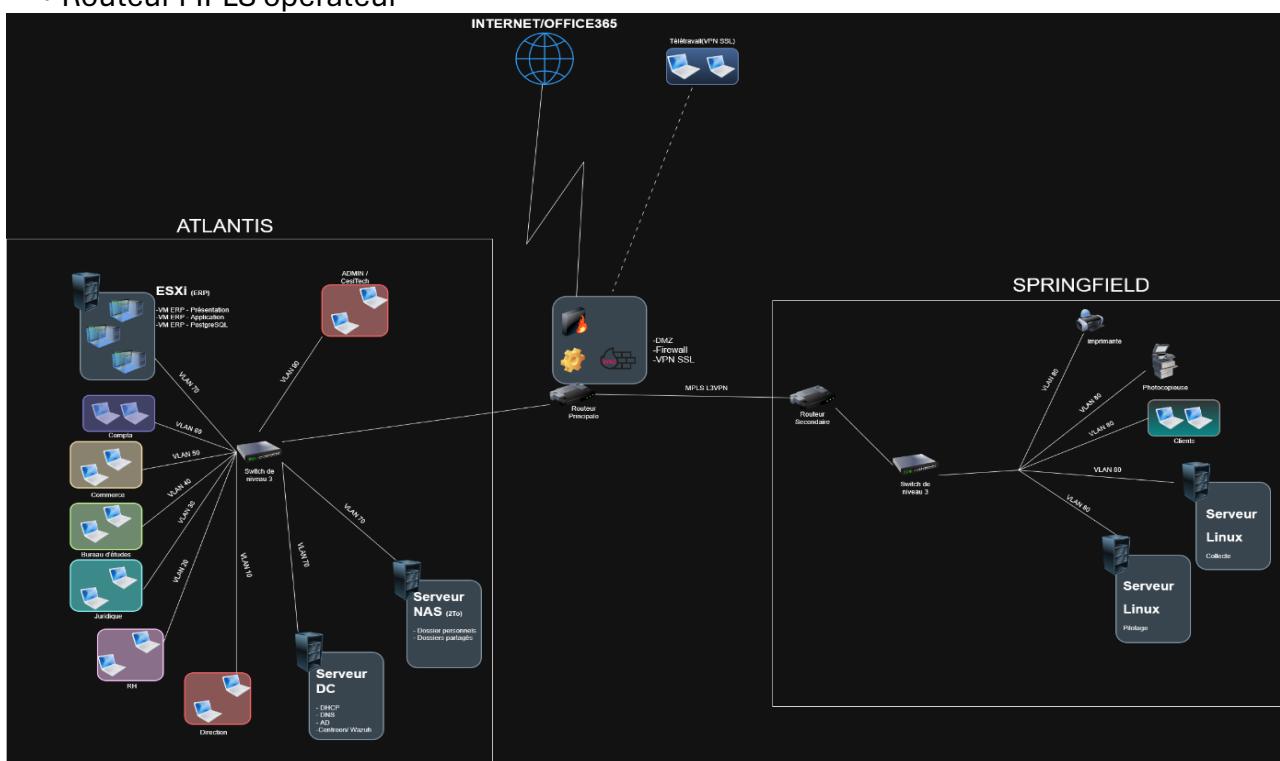


Figure 6 - Schéma du SI



Schéma du S.I. modélisé par CesiTech

Nous avons fait le choix de proposer une maquette épurée. En effet nous avons utilisé un serveur Proxmox sur lequel plusieurs Machines Virtuelles ont été mises en place.

Site Atlantis (central) :

- Une VM Pfsense (modélisant les switchs de niveau 3 en cascade, le routeur et le pare-feu)
- Une VM Windows serveur (modélisant le contrôleur de domaine AD et DNS)
- Une VM Truenas (modélisant le NAS centralisé pour les données et sauvegardes)
- Une VM Windows serveur (modélisant l'accès web à l'ERP et sa base de données elle-même modélisés sur Sqlite pour répondre au besoin tout en étant mieux dimensionné)
- Une VM Zabbix (modélisant le système de supervision)
- Un poste utilisateur dont on changera le vlan pour les tests

Site Springfield (laboratoire) :

- Une VM Pfsense (modélisant le switch de niveau 2 et le routeur)
- Un poste utilisateur sur le vlan du laboratoire

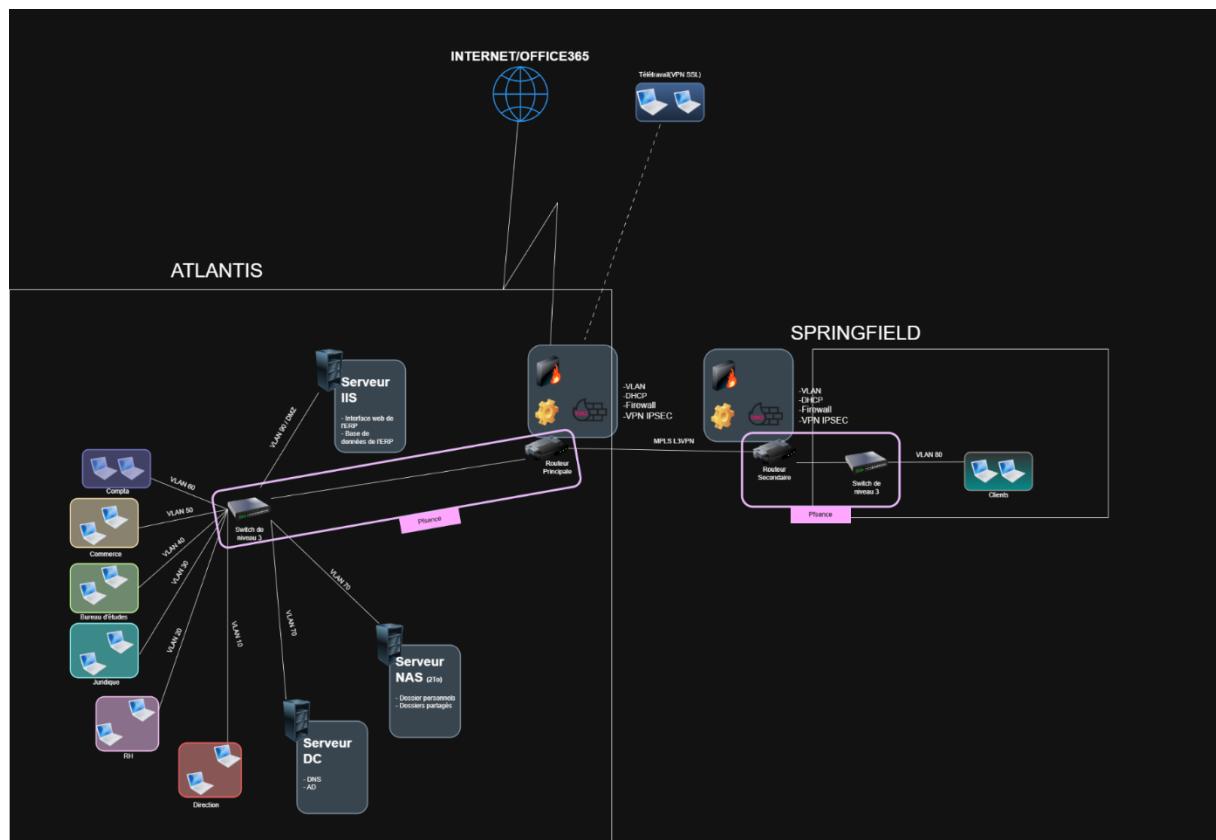


Figure 7 - Schéma du S.I. modélisé par CESITech



Configuration du réseau

Cloisonnement réseau et VLAN

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

- VLAN Direction (VLAN 10)
- VLAN Ressources Humaines (VLAN 20)
- VLAN Juridique (VLAN 30)
- VLAN Bureau d'étude (VLAN 40)
- VLAN Commercial (VLAN 50)
- VLAN Comptabilité (VLAN 60)
- VLAN Serveurs (VLAN 70)
- VLAN Laboratoire (VLAN 80)
- VLAN DMZ (VLAN 90)

Ce cloisonnement répond à plusieurs objectifs :

- **Sécurité et confidentialité** : Chaque service est isolé et ne peut accéder aux données des autres sans autorisation explicite. Chaque service bénéficie d'un isolement renforcé. De plus une DMZ est mise en place pour isoler les données accessibles depuis l'extérieur du reste du réseau.
- **Administration simplifiée** : Les règles de firewall inter-VLAN deviennent plus claires et maîtrisées.
- **Performance** : Le trafic de broadcast est réduit et le réseau mieux organisé, lui permettant d'être plus rapide.

Sécurisation périphérique : Firewall, DMZ et VPN

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

Une DMZ (zone démilitarisée) est mise en place pour héberger les services qui doivent être accessibles depuis l'extérieur évitant d'exposer directement le réseau interne. Elle constitue une zone tampon assurant la protection du cœur du SI. Le pare-



feu filtre strictement les flux Internet vers la DMZ, ainsi que les flux DMZ vers le LAN. Aucun des flux directs entre Internet et LAN n'est autorisé.

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

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

Serveur Contrôleur de Domaine

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

- Active Directory : Il permet de centraliser la gestion des utilisateurs, des groupes et des ordinateurs du domaine (authentifier les utilisateurs lorsqu'ils se connectent, appliquer les stratégies de groupe (GPO), gérer les droits d'accès aux dossiers partagés)
- DNS (Domaine Name System) : Le serveur DNS intégré au contrôleur de domaine utilise une zone principale AD-intégrée pour la résolution des noms (ex : www.xanadu.com). Pour les résolutions externes, le serveur DNS n'utilise pas les Root Hints par défaut. A la place, il est configuré avec des redirecteurs DNS, pointant vers les serveurs DNS de l'opérateur internet.

Interface de l'ERP

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

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

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



NAS et gestion des données

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

Il contient :

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

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

Figure 8 - Tableaux des accès

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

Plan d'adressage

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

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

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

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



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

Figure 9 - Adressage d'un VLAN du site principal

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

Nom du sous-réseau	Nb. d'hôtes souhaités	Nb. d'hôtes disponibles	Nb. d'hôtes restants	Notation CIDR	Masque sous-réseau	Plage utilisable	Adresse réseau	Adresse broadcast
Service Serveurs (VLAN 70)	5	16 (14 utilisables)	8	/28	255.255.255.240	192.168.1.97 - 192.168.1.110	192.168.1.96	192.168.1.111
Machine	Adresse	Masque						
Serveur Nas	192.168.1.98	/28						
Serveur DHCP, DNS, AD	192.168.1.99	/28						
Serveur ESXi	192.168.1.100	/28						
Serveur DHCP(Pfsense)	192.168.1.101	/28						
Liaison serveur proxmox	192.168.1.102	/28						
Zabbix	192.168.1.104	/28						
VM Ubuntu (SSL)	192.168.1.103	/28						

Figure 10 - Adressage des serveurs du site principal

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

Machine	Adresse	Masque	Vlan	Service
Routeur (Atlantis)	192.168.1.1	/28	10	Direction
	192.168.1.17	/28	20	RH
	192.168.1.33	/28	30	Juridique
	192.168.1.49	/28	40	Bureau d'étude
	192.168.1.65	/28	50	Commercial
	192.168.1.81	/28	60	Comptabilité
	192.168.1.97	/28	70	Serveur
	192.168.1.161	/30	100	DMZ

Figure 11 - Adresses du routeur du bâtiment principal

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



Nom du sous-réseau	Nb. d'hôtes souhaités	Nb. d'hôtes disponibles	Nb. d'hôtes restants	Notation CIDR	Masque sous-réseau	Plage utilisable	Adresse réseau	Adresse broadcast
Service Laboratoire (VLAN 80)	14	32 (30 utilisables)	15	/27	255.255.255.224	192.168.1.129 – 192.168.1.158	192.168.1.128	192.168.1.159
Machine	Adresse	Masque						
PC (10)	DHCP	/27						
Imprimante	192.168.1.130	/27						
photocopieuse	192.168.1.131	/27						
Serveur de collecte	192.168.1.132	/27						
Serveur de pilotage	192.168.1.133	/27						
Routeur (lab)	192.168.1.129	/27						

Figure 12 - Adressage du site secondaire (Springfield)

Afin d'isoler le serveur web accessible depuis l'extérieur du reste du réseau, nous avons mis en place une DMZ sur le routeur. Celle-ci est un réseau secondaire entier, qui est accessible depuis l'intérieur du réseau mais qui depuis l'extérieur semble indépendant du reste. Il est adressé de la même manière qu'un vlan classique.

Nom du réseau	Nom du sous-réseau	Nb. d'hôtes souhaités	Nb. d'hôtes disponibles	Nb. d'hôtes restants	Notation CIDR	Masque sous-réseau	Plage utilisable	Adresse réseau	Adresse broadcast
DMZ (VLAN 100)	1	4 (2 utilisables)	2	/30	255.255.255.248	192.168.1.161 – 192.168.1.162	192.168.1.160	192.168.1.163	192.168.1.163
Machine	Adresse	Masque							
Serveur IIS (DMZ)	192.168.1.162	/30							

Figure 13 - Adressage de la DMZ



Mise en place du routage avec PfSense

Mise en place de l'infrastructure réseau avec PfSense

Dans le cadre du projet, nous avons fait la conception et le déploiement de l'architecture réseau. Cela comprenait le routage entre les différents sites, la segmentation en VLAN, ainsi que la configuration du pare-feu et des services réseau.

Pour centraliser toutes ces fonctions et garantir une sécurité optimale, nous avons opté pour PfSense. C'est une solution open source très solide, particulièrement reconnue pour ses performances en routage, en filtrage et en sécurité réseau.

Nous avons donc déployé une machine virtuelle PfSense sur Proxmox, qui héberge l'ensemble des VMs du projet. Cette VM PfSense est devenue le cœur du réseau du site Atlantis. Elle assure le routage principal, fait office de pare-feu et de serveur DHCP, et sert également de passerelle vers le site distant de Springfield via la liaison MPLS.

Création de la machine virtuelle PfSense Atlantis et choix des interfaces

La machine virtuelle PfSense a été configurée avec trois interfaces réseau distinctes, chacune jouant un rôle bien défini :

- **Interface WAN** : elle correspond à la sortie vers Internet. Elle est utilisée pour l'accès externe et pour la mise en œuvre du NAT sortant.
- **Interface LAN** : cette interface est dédiée au réseau interne du site Atlantis. Elle sert de support à l'ensemble des VLAN afin de centraliser le trafic interne tout en assurant une segmentation logique.
- **Interface MPLS** : cette interface est réservée au lien privé MPLS reliant le site principal d'Atlantis au site distant de Springfield. Ce choix permet d'isoler totalement le trafic inter-sites du reste du réseau et d'assurer une meilleure sécurité et lisibilité des flux.



Segmentation du réseau par VLAN

Pour renforcer la sécurité, mieux isoler nos services et contrôler les flux réseau, nous avons segmenté notre réseau local en VLANs via l'interface LAN de PfSense.

Chaque service de XANADU a désormais son propre réseau virtuel. Ça nous permet de :

- Contenir plus facilement une éventuelle attaque,
- Limiter les risques de propagation latérale si un poste est compromis,
- D'appliquer des règles de filtrage sur mesure pour chaque métier.

Voici les VLANs que nous avons configurés :

- VLAN 10 : Direction
- VLAN 20 : Ressources Humaines
- VLAN 30 : Juridique
- VLAN 40 : Bureau d'Études
- VLAN 50 : Commercial
- VLAN 60 : Comptabilité
- VLAN 70 : Serveurs
- VLAN 100 : DMZ

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
vtnet1 (lan)	10		VLAN10_Direction	
vtnet1 (lan)	20		VLAN20_RH	
vtnet1 (lan)	30		VLAN30_Juridique	
vtnet1 (lan)	40		VLAN40_BE	
vtnet1 (lan)	50		VLAN50_Commercial	
vtnet1 (lan)	60		VLAN60_Comptabilite	
vtnet1 (lan)	70		VLAN70_Serveurs	
vtnet1 (lan)	100		VLAN100_DMZ	

Figure 14 - Création des VLAN

Chaque réseau est identifié par un tag unique et un nom clair, pour que l'administration reste simple et cohérente.



Assignation et configuration des interfaces VLAN

Une fois les VLAN configurés, nous les avons assignés comme interfaces réseau dans PfSense. C'est une étape clé pour pouvoir gérer chaque Vlan indépendamment : définir ses adresses IP, activer le DHCP, ou encore mettre en place des règles de pare-feu.

Interfaces / Interface Assignments									
Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs
Interface									Network port
WAN			vtnet0 (bc:24:11:01:f7:0a)						
LAN			vtnet1 (bc:24:11:41:89:4b)						 Delete
MPLS			vtnet2 (bc:24:11:21:30:be)						 Delete
VLAN10_Direction			VLAN 10 on vtnet1 - lan (VLAN10_Direction)						 Delete
VLAN20_RH			VLAN 20 on vtnet1 - lan (VLAN20_RH)						 Delete
VLAN30_Juridique			VLAN 30 on vtnet1 - lan (VLAN30_Juridique)						 Delete
VLAN40_BE			VLAN 40 on vtnet1 - lan (VLAN40_BE)						 Delete
VLAN50_Commercial			VLAN 50 on vtnet1 - lan (VLAN50_Commercial)						 Delete
VLAN60_Comptabilite			VLAN 60 on vtnet1 - lan (VLAN60_Comptabilite)						 Delete
VLAN70_Serveurs			VLAN 70 on vtnet1 - lan (VLAN70_Serveurs)						 Delete
VLAN100_DMZ			VLAN 100 on vtnet1 - lan (VLAN100_DMZ)						 Delete

Figure 15 - Création des VLAN sur le pfsense

Pour chaque interface VLAN, nous avons suivi la même logique :

- Activation de l'interface,
- Attribution d'un nom parlant (par exemple, « VLAN10_Direction »),
- Configuration d'une adresse IPv4 fixe.

Nous avons organisé le plan d'adressage de façon logique, en veillant à ce que chaque interface serve de passerelle par défaut pour les machines de son VLAN. Par exemple, le VLAN 10 (Direction) a reçu l'adresse 192.168.1.1/28, qui fait office de routeur pour tous les postes de ce réseau.

Enfin, nous avons appliqué cette logique à tous les VLAN, en réservant un sous-réseau distinct par service.



Interfaces / VLAN10_Direction (vtnet1.10)

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	VLAN10_Direction Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XXXX:XXXX:XXXX:XXXX The MAC address of a VLAN interface must be set on its parent interface
MTU	
MSS	
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	192.168.1.1
	/ 28

Figure 16 – Activation de l'interface Vlan 10

Mise en place du service DHCP par VLAN

Pour faciliter la gestion des postes clients et limiter les erreurs de configuration manuelle, nous avons activé le service DHCP de PfSense sur la plupart des VLAN.

Le DHCP est ainsi opérationnel sur tous les VLAN destinés aux utilisateurs, à l'exception de deux réseaux spécifiques :

- Le VLAN 70 (Serveurs),
- Le VLAN 100 (DMZ).

Ces deux VLAN hébergent des serveurs et services exposés qui nécessitent des adresses IP fixes. Cela permet d'assurer la stabilité des services, de maintenir des règles de sécurité cohérentes et de garantir une bonne traçabilité.

Sur chaque VLAN où le DHCP est actif, nous avons paramétré :

- Une plage d'adresses IP adaptée au sous-réseau concerné,
- Une passerelle par défaut correspondant à l'adresse de l'interface VLAN,



- Un serveur DNS pointant vers le contrôleur de domaine Active Directory, ce qui permet la résolution des noms internes et le bon fonctionnement des services AD.

Cette approche assure une intégration fluide des postes clients au domaine, tout en maintenant une gestion centralisée du réseau.

The screenshot shows the DHCP configuration for the VLAN10_DIRECTION interface. At the top, there are tabs for WAN, LAN, MPLS, VLAN10_DIRECTION (which is selected), VLAN20_RH, VLAN30_JURIDIQUE, VLAN40_BE, and VLAN50_COMMERCIAL. Below these are additional VLAN options: VLAN60_COMPTABILITE, VLAN70_SERVEURS, and VLAN100_DMZ.

General DHCP Options:

- DHCP Backend: ISC DHCP
- Enable: Enable DHCP server on VLAN10_DIRECTION interface
- BOOTP: Ignore BOOTP queries
- Deny Unknown Clients: Allow all clients (dropdown menu)
- Ignore Denied Clients: Ignore denied clients rather than reject (disabled)
- Ignore Client Identifiers: Do not record a unique identifier (UID) in client lease data if present in the client DHCP request (disabled)

Primary Address Pool:

- Subnet: 192.168.1.0/28
- Subnet Range: 192.168.1.1 - 192.168.1.14
- Address Pool Range: 192.168.1.2 to 192.168.1.14
- DNS Servers: 192.168.1.99

Figure 17 – Activation du service DHCP sur le VLAN 10

Configuration du lien MPLS entre Atlantis et Springfield

Pour relier le site principal d'Atlantis au site distant de Springfield, nous avons simulé un lien MPLS opérateur entre deux machines virtuelles PfSense.

Nous avons configuré l'interface MPLS avec un adressage en /30, idéal pour un lien point-à-point puisqu'il n'utilise que deux adresses IP. Cela permet d'économiser des adresses tout en respectant les bonnes pratiques réseau.



Interfaces / MPLS (vtnet2)

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	MPLS Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XXXXXXXXXXXXXX This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxxxx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPV4 header size) and minus 60 for IPv6 (TCP/IPV6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv4 Configuration	
IPv4 Address	10.10.10.1

Figure 18 - Activation de l'interface MPLS

Ensuite, nous avons défini une passerelle dédiée sur PfSense, pointant vers l'adresse IP du PfSense situé à Springfield. Cette passerelle indique à PfSense comment atteindre les réseaux distants.

System / Routing / Gateways

Gateways	Static Routes	Gateway Groups																					
<table border="1"> <thead> <tr> <th>Name</th> <th>Default</th> <th>Interface</th> <th>Gateway</th> <th>Monitor IP</th> <th>Description</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>WANGW</td> <td>Default (IPv4)</td> <td>WAN</td> <td>192.168.100.1</td> <td>192.168.100.1</td> <td>Interface wan Gateway</td> <td> </td> </tr> <tr> <td>GW_MPLS_SPRINGFIELD</td> <td></td> <td>MPLS</td> <td>10.10.10.2</td> <td>10.10.10.2</td> <td></td> <td> </td> </tr> </tbody> </table>	Name	Default	Interface	Gateway	Monitor IP	Description	Actions	WANGW	Default (IPv4)	WAN	192.168.100.1	192.168.100.1	Interface wan Gateway		GW_MPLS_SPRINGFIELD		MPLS	10.10.10.2	10.10.10.2				
Name	Default	Interface	Gateway	Monitor IP	Description	Actions																	
WANGW	Default (IPv4)	WAN	192.168.100.1	192.168.100.1	Interface wan Gateway																		
GW_MPLS_SPRINGFIELD		MPLS	10.10.10.2	10.10.10.2																			

Figure 19 – Création de la passerelle pointant sur Springfield

Pour finir, nous avons ajouté une route statique qui précise que le réseau du laboratoire distant (VLAN80_LABO) est accessible via la passerelle MPLS. La même configuration a été appliquée de façon symétrique sur le PfSense de Springfield, afin que la communication fonctionne dans les deux sens.

System / Routing / Static Routes

Gateways	Static Routes	Gateway Groups										
	<table border="1"> <thead> <tr> <th>Network</th> <th>Gateway</th> <th>Interface</th> <th>Description</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>192.168.1.128/28</td> <td>GW_MPLS_SPRINGFIELD - 10.10.10.2</td> <td>MPLS</td> <td>Route vers Springfield</td> <td> </td> </tr> </tbody> </table>	Network	Gateway	Interface	Description	Actions	192.168.1.128/28	GW_MPLS_SPRINGFIELD - 10.10.10.2	MPLS	Route vers Springfield		
Network	Gateway	Interface	Description	Actions								
192.168.1.128/28	GW_MPLS_SPRINGFIELD - 10.10.10.2	MPLS	Route vers Springfield									

Figure 20 – Création de la route statique vers Springfield sur PfSense Atlantis



Concernant la traduction d'adresses réseau (NAT), PfSense a été laissé en mode automatique.

Dans ce mode, PfSense génère automatiquement les règles de NAT nécessaires pour permettre aux réseaux internes d'accéder à Internet via l'interface WAN.

Ce choix est pertinent dans le cadre du projet car :

- Il réduit les risques d'erreur de configuration,
- Il garantit un fonctionnement fiable et standard,
- Il permet de se concentrer sur les aspects sécurité et segmentation.

Les règles générées automatiquement couvrent l'ensemble des réseaux internes et assurent la sortie vers Internet tout en conservant une configuration claire et maintenable.

Mise en place de PfSense Springfield

Pour le site distant de Springfield, une seconde machine virtuelle PfSense a été déployée afin d'assurer les fonctions de routage, de segmentation réseau et de sécurité locales. La méthodologie appliquée a volontairement été strictement identique à celle du site principal d'Atlantis, afin de garantir une architecture homogène, plus simple à administrer et à maintenir.

La machine virtuelle PfSense Springfield a été créée avec les interfaces nécessaires, notamment une interface dédiée au réseau local du laboratoire et une interface dédiée au lien MPLS reliant le site distant au site principal. Sur l'interface LAN, un VLAN 80_LABO a été mis en place afin d'isoler le réseau du laboratoire de recherche, qui regroupe les dix postes utilisateurs ainsi que les deux serveurs Linux du site.

Ce VLAN a ensuite été assigné comme interface PfSense, activé et configuré avec une adresse IPv4 statique servant de passerelle par défaut pour les équipements du laboratoire. Un serveur DHCP a été activé sur ce VLAN pour les postes clients, facilitant le déploiement et la gestion des adresses IP, tandis que les serveurs du laboratoire conservent une configuration IP statique afin de garantir la stabilité des services.

Enfin, le lien MPLS entre Springfield et Atlantis a été configuré de manière symétrique sur les deux pare-feu PfSense. L'interface MPLS utilise un adressage en /30, une Gateway dédiée a été définie, et des routes statiques ont été ajoutées afin de permettre la communication entre les réseaux des deux sites. Cette configuration assure une connectivité privée, sécurisée et performante entre Atlantis et Springfield, conforme aux exigences du projet et au SLA opérateur.



Mise en place d'un VPN d'accès distant avec OpenVPN

1. Objectif de la mise en place du VPN

L'un des besoins exprimés par la direction de XANADU est de permettre aux équipes de travailler à distance, que ce soit en télétravail ou lors de déplacements. L'idée est de leur offrir un accès simple, mais aussi sécurisé et maîtrisé, aux outils internes, serveurs, applications métier et différents réseaux.

Pour y répondre, nous avons déployé un VPN de type "client vers site". Concrètement, cela permet à chaque collaborateur de se connecter au réseau de l'entreprise depuis n'importe où, comme s'il était au bureau, avec la garantie que les échanges restent privés et intègres.

Nous avons opté pour la solution OpenVPN, directement intégrée à PfSense. Ce choix est en lien avec notre architecture réseau actuelle et nous permet de gérer tous les accès distants de façon centralisée, simple et sécurisée.

2. Architecture VPN retenue

Notre infrastructure VPN s'appuie sur un pare-feu PfSense Atlantis, qui fait office de serveur OpenVPN. Pour se connecter à distance, les collaborateurs utilisent simplement le client OpenVPN Connect sur leurs postes Windows.

Nous avons réservé un réseau spécifique pour le tunnel VPN : 10.8.0.0/24. Dès qu'un client se connecte, il reçoit automatiquement une adresse IP dans cette plage.

Une fois authentifié, l'utilisateur peut accéder aux différents réseaux internes de l'entreprise, comme les VLANs utilisateurs et serveurs, ou encore la DMZ, selon les autorisations qui lui sont accordées.

3. Mise en place de l'infrastructure de certificats (PKI)

Pour sécuriser les connexions VPN, nous avons opté pour une authentification forte via des certificats. Cela nous a conduit à créer notre propre autorité de certification (CA) directement sur PfSense.

Cette CA interne sert de point de confiance central pour tout notre VPN. C'est elle qui délivre et signe aussi bien le certificat du serveur OpenVPN que ceux de chaque utilisateur distant.



Nous l'avons configurée avec des paramètres de sécurité renforcés, en utilisant du RSA 4096 bits et l'algorithme SHA256, pour garantir une protection cryptographique optimale. L'avantage d'une CA maison, c'est qu'elle nous donne un contrôle total sur le cycle de vie des certificats : on peut les créer, les révoquer ou les renouveler en toute autonomie.

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA_OPENVPN_ATLANTIS	✓	self-signed	2	CN=internal-ca ⓘ Valid From: Mon, 15 Dec 2025 08:59:00 +0000 Valid Until: Thu, 13 Dec 2035 08:59:00 +0000		

Figure 21 - Crédit à la création d'autorité de certification

4. Crédit à la création des certificats serveur et utilisateurs

Après avoir mis en place l'autorité de certification, on a généré un certificat spécifique pour le serveur OpenVPN. Ce certificat joue un rôle clé : il permet au serveur de s'identifier auprès des clients quand ils établissent une connexion sécurisée. Comme il est signé par notre propre autorité de certification, il assure un lien de confiance entre le serveur et les utilisateurs qui se connectent.

Ensuite, on a créé un compte utilisateur VPN directement dans l'interface de gestion de pfSense. Pour cet utilisateur, on a configuré :

- Un identifiant et un mot de passe,
- Ainsi qu'un certificat personnel, lui aussi signé par notre autorité de certification.

Du coup, chaque utilisateur distant dispose de son propre certificat. Cela permet une authentification à deux facteurs, en combinant :

- Ce que l'utilisateur sait (son mot de passe),
- Et ce qu'il possède (son certificat).



Name	Issuer	Distinguished Name	In Use	Actions
GUI default (692ea1858a51b) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-692ea1858a51b Valid From: Tue, 02 Dec 2025 08:21:25 +0000 Valid Until: Mon, 04 Jan 2027 08:21:25 +0000	webConfigurator	
OpenVPN_Server Server Certificate CA: No Server: Yes	CA_OPENVPN_ATLANTIS	CN=openvpn-atlantis Valid From: Mon, 15 Dec 2025 09:01:46 +0000 Valid Until: Thu, 13 Dec 2035 09:01:46 +0000	OpenVPN Server	
user1 User Certificate CA: No Server: No	CA_OPENVPN_ATLANTIS	CN=openvpn-atlantis Valid From: Mon, 15 Dec 2025 09:33:50 +0000 Valid Until: Thu, 13 Dec 2035 09:33:50 +0000	User Cert	

Figure 22 - Crédit de la capture d'écran du serveur OpenVPN

5. Configuration du serveur OpenVPN

Ensuite, nous avons configuré le serveur OpenVPN sur PfSense en mode Remote Access (SSL/TLS), idéal pour les connexions à distance. Pour la sécurité, nous avons opté pour une double authentification : un identifiant utilisateur combiné à un certificat.

Nous avons attribué le réseau 10.8.0.0/24 au tunnel VPN, ce qui permet d'assigner automatiquement une adresse IP à chaque client qui se connecte.

Enfin, nous avons bien précisé dans la configuration du serveur quels réseaux internes seraient accessibles via le VPN. L'avantage, c'est que les routes sont automatiquement transmises aux clients, plus besoin de réglages manuels de leur côté. Comme ça, une fois connecté, l'utilisateur sait tout de suite vers quels réseaux internes il peut aller.

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.8.0.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits		

Figure 23 - Crédit de la capture d'écran du serveur OpenVPN



6. Mise en place des règles de pare-feu OpenVPN

Pour que le VPN fonctionne, nous avons dû configurer quelques règles spécifiques dans le pare-feu. PfSense génère automatiquement une règle implicite sur l'interface WAN afin d'autoriser les connexions entrantes vers le serveur VPN. Il n'est donc pas nécessaire d'ajouter une règle WAN manuelle dans notre contexte.

Sur l'interface OpenVPN, nous avons ajouté une règle qui autorise tout le trafic, dans le cadre de ce projet. Ainsi, une fois connectés via le tunnel VPN, les clients peuvent accéder aux réseaux internes prévus.

Cette approche a été choisie pour simplifier la démonstration et vérifier que le VPN fonctionne correctement. En conditions réelles, bien sûr, cette règle serait ajustée plus finement, en suivant le principe du moindre privilège.

7. Déploiement des clients VPN

Pour faciliter l'installation des clients VPN, nous avons ajouté l'utilitaire d'export de configuration OpenVPN directement sur PfSense. Grâce à cet outil, on peut générer en quelques clics des fichiers de configuration prêts à l'emploi pour les utilisateurs.

Nous avons ainsi exporté un fichier .ovpn pour l'utilisateur que nous venions de créer. Ce fichier rassemble tout le nécessaire :

- Les certificats d'authentification,
- La clé de chiffrement,
- L'adresse du serveur VPN,
- Ainsi que les routes réseau à appliquer.

Du côté de l'utilisateur, il suffit d'installer OpenVPN Connect, d'importer le fichier .ovpn et de se connecter avec ses identifiants. Cette méthode limite grandement les erreurs de configuration et rend la prise en main vraiment simple pour tout le monde.



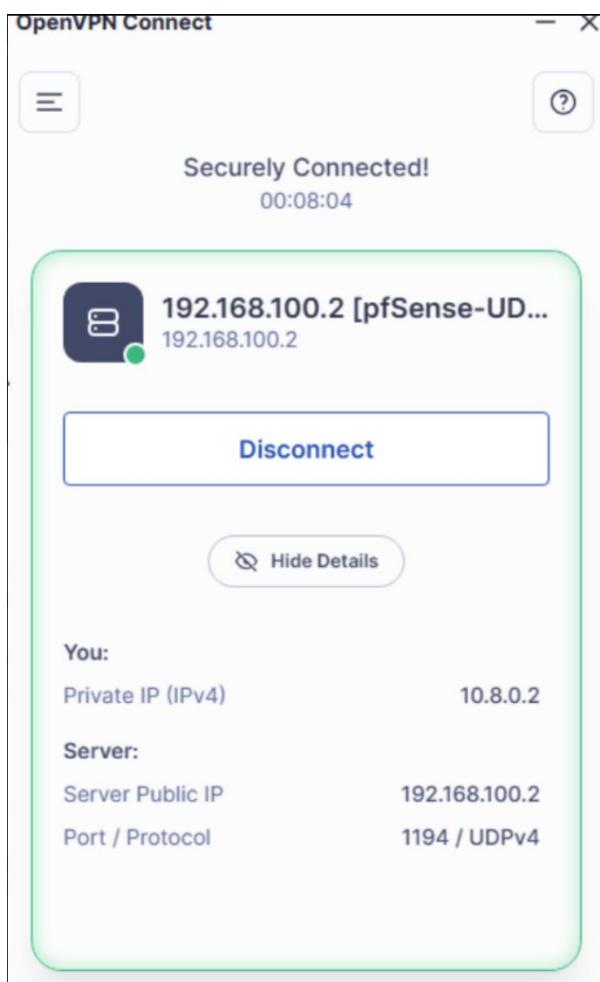


Figure 25 - Connexion VPN Réussi

8. Vérifications et tests de fonctionnement

Nous avons effectué plusieurs tests pour vérifier que le VPN fonctionne correctement. Une fois connecté, le client reçoit bien une adresse IP du réseau VPN (10.8.0.0/24), ce qui confirme que le tunnel est bien établi.

Ensuite, nous avons testé la connectivité en réalisant les vérifications suivantes :

- Ping des interfaces internes,
 - Accès aux serveurs internes (ex : serveur web)
 - Vérification de la résolution DNS interne.

Figure 26 - Bien connecté au VPN

```
C:\Users\maxime>ping 192.168.1.162

Envoi d'une requête 'Ping' 192.168.1.162 avec 32 octets de données :
Réponse de 192.168.1.162 : octets=32 temps=1 ms TTL=127
Réponse de 192.168.1.162 : octets=32 temps=1 ms TTL=127

Statistiques Ping pour 192.168.1.162:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
Ctrl+C
^C
C:\Users\maxime>ping 192.168.1.18

Envoi d'une requête 'Ping' 192.168.1.18 avec 32 octets de données :
Réponse de 192.168.1.18 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.1.18 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 192.168.1.18:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms
Ctrl+C
^C
C:\Users\maxime>
```

Figure 27 - Possibilité de ping

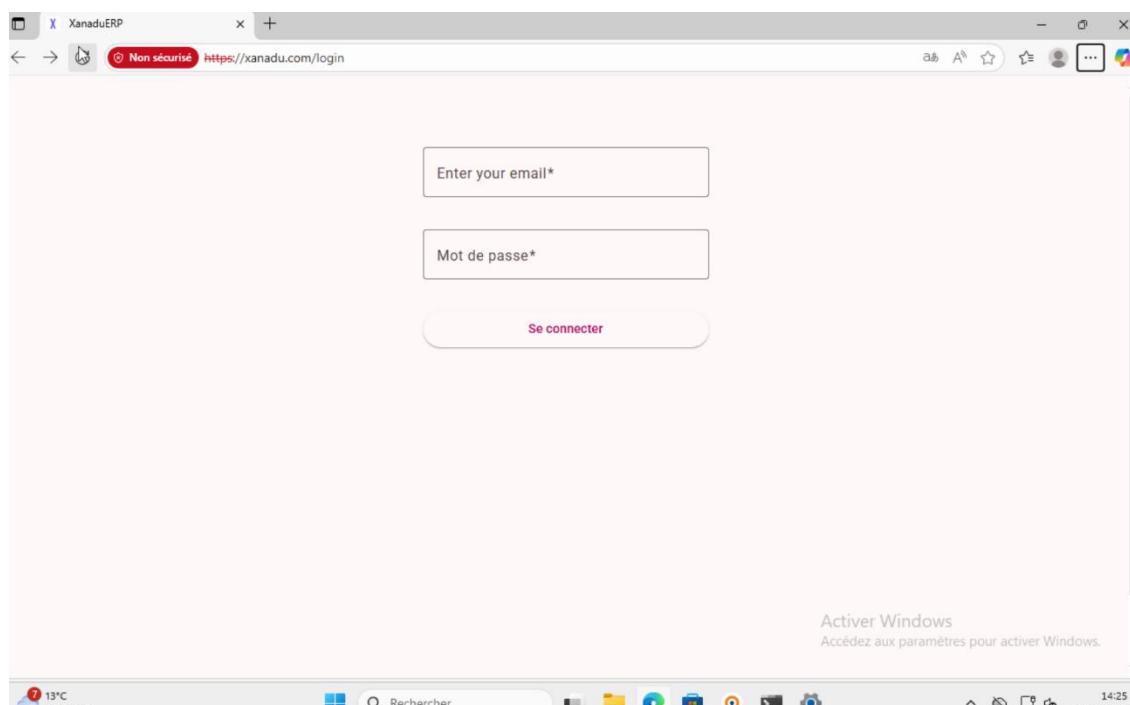


Figure 28 - Bon accès à la page Web



```
C:\Users\maxime>nslookup google.com
Serveur :      SRVDC01.xanadu.com
Address: 192.168.1.99

Réponse ne faisant pas autorité :
Nom :      google.com
Adresses:  2a00:1450:4007:819::200e
          216.58.214.174

C:\Users\maxime>
```

Figure 29 - Bonne résolution DNS

Les résultats sont conformes aux attentes : le poste distant se comporte exactement comme s'il était directement connecté au réseau local de l'entreprise, tout en profitant d'une connexion chiffrée et sécurisée.



Politique de filtrage

Politique de filtrage du pare-feu pfSense Atlantis

Le pare-feu Atlantis constitue le cœur de la sécurisation du réseau principal. Il applique des règles de filtrage par VLAN, permettant de cloisonner les services entre eux, tout en autorisant uniquement les flux strictement nécessaires.

VLAN Direction (VLAN10)

Le service Direction bénéficie d'un accès complet à l'ensemble du SI :

- Consultation de tous les partages
- Accès aux serveurs métiers
- Accès aux VLAN internes
- Trafic Internet autorisé

Justification :

La Direction a besoin d'une vision globale du SI, notamment pour superviser l'activité, consulter les tableaux de bord ERP, accéder aux services transverses et administrer certains paramètres du système.

VLAN Ressources Humaines (VLAN20)

Les RH disposent d'un accès restreint mais suffisant pour leurs missions :

- Accès autorisé : DNS, NAS, serveurs métiers (ERP), portail IIS
- Accès interdit : Laboratoire, VLAN Direction, Commercial, Comptabilité, Juridique, etc.
- Accès Internet autorisé (via !RFC1918)

Justification :

- Les RH manipulent des données sensibles → nécessité de cloisonner le service.



- Aucun besoin métier d'accéder aux systèmes du laboratoire ou aux autres services.
- Les flux nécessaires sont exclusivement orientés vers les serveurs du VLAN70.

VLAN Juridique (VLAN30)

Le service juridique bénéficie d'accès spécifiques :

- Accès autorisé : DNS, serveurs métiers (NAS/AD/ERP), IIS
- Accès interdit : tous les autres VLAN internes (RH, Commercial, BE, LAB, etc.)
- Accès Internet autorisé

Justification :

Le service juridique accède à des dossiers sensibles tels que RH et Client via le NAS. La segmentation permet de réduire l'exposition en cas de compromission et de respecter la confidentialité des échanges.

VLAN Bureau d'Étude (VLAN40)

Le Bureau d'Étude dispose d'un accès étendu vers les services centraux, ainsi que d'un accès spécifique vers le laboratoire :

- Accès autorisé : DNS, serveurs métiers, portail interne
- Accès au LABO autorisé **via le lien MPLS**, selon le cahier des charges
- Accès interdit : RH, Juridique, Commercial, Comptabilité
- Internet autorisé

Justification :

Le BE échange des données techniques avec le Laboratoire, notamment pour la récupération de fichiers et le traitement des résultats. Cet accès est également restreint par les ACL sur les partages du NAS pour garantir un mode **lecture seule**.

VLAN Commercial (VLAN50)



Le réseau Commercial est fortement limité :

- Accès autorisé : DNS, serveurs métiers
- Accès interdit : RH, Juridique, BE, Comptabilité, LABO
- Internet autorisé

Justification :

Les commerciaux n'ont besoin que des informations clients via l'ERP et le NAS. Le cloisonnement empêche toute propagation latérale, notamment depuis des postes potentiellement plus exposés (mobilité, télétravail).

[VLAN Comptabilité \(VLAN60\)](#)

La Comptabilité dispose de droits proches de ceux des RH :

- Accès autorisé : DNS, serveurs métiers
- Accès interdit : LABO, autres VLAN internes
- Internet autorisé

Justification :

Les besoins se limitent aux applications financières et au ERP. L'isolement est essentiel pour éviter un mouvement latéral vers des données critiques.

[VLAN Serveurs \(VLAN70\)](#)

Les serveurs nécessitent un accès global :

- Accès total interne
- Accès Internet (mises à jour, antivirus...)

Justification :

Les serveurs doivent communiquer avec l'ensemble des services et pouvoir effectuer des procédures d'administration, de sauvegarde et de synchronisation.



Interface MPLS (Atlantis)

Le pare-feu Atlantis filtre les flux provenant du site Springfield :

- Autorisation des flux nécessaires : DNS, AD/LDAP, NAS, ERP, IIS
- Accès autorisé au BE
- Accès strictement interdit à tous les autres VLAN
- Blocage des tentatives d'administration du firewall
- Blocage final pour la sécurité

Justification :

- Le LABO ne doit accéder qu'aux ressources métiers centrales.
- Cette segmentation protège Atlantis d'une éventuelle compromission du site distant.
- Les flux autorisés sont conformes aux besoins exprimés lors du cahier des charges.



Ordre	Équipement	Interface	Source	Destination	Protocole	Action	Description
1	pfSense Atlantis	VLAN10_DIRECTION	VLAN10_DIRECTION subnets	Any	Any	Pass	Direction – accès complet à tous les services et VLAN
2	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.99	TCP/UDP 53	Pass	RH → DNS (DC)
3	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	VLAN70_SERVEURS subnets	Any	Pass	RH → NAS / AD / ERP
4	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.162	TCP 80/443	Pass	RH → Web interne IIS DMZ
5	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.110	TCP 587	Pass	RH → Serveur Mail (SMTP Submission)
6	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.110	TCP 993	Pass	RH → Serveur Mail (IMAPS)
7	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.128/27	Any	Block	RH → LAB (interdit)
8	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	RFC1918	Any	Block	Blocage RH vers les autres VLAN
9	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	!RFC1918	Any	Pass	RH → Internet
10	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.99	TCP/UDP 53	Pass	Juridique → DNS
11	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	VLAN70_SERVEURS subnets	Any	Pass	Juridique → NAS / AD / ERP
12	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.110	TCP 587	Pass	Juridique → Serveur Mail (SMTP Submission)
13	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.110	TCP 993	Pass	Juridique → Serveur Mail (IMAPS)
14	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.128/27	Any	Block	Juridique → LAB interdit
15	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	RFC1918	Any	Block	Juridique → autres VLAN interdit
16	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	!RFC1918	Any	Pass	Juridique → Internet
17	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.99	TCP/UDP 53	Pass	BE → DNS
18	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	VLAN70_SERVEURS subnets	Any	Pass	BE → Serveurs (NAS, AD, ERP)
19	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.162	TCP 80/443	Pass	BE → IIS DMZ
20	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.128/27	Any	Pass	BE → LAB (autorisé via MPLS)
21	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.110	TCP 587	Pass	BE → Serveur Mail (SMTP Submission)
22	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.110	TCP 993	Pass	BE → Serveur Mail (IMAPS)
23	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	VLAN20_RH subnets	Any	Block	BE → RH interdit
24	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	VLAN30_JURIDIQUE subnets	Any	Block	BE → Juridique interdit
25	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	RFC1918	Any	Block	BE → autres VLAN internes
26	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	!RFC1918	Any	Pass	BE → Internet
27	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.99	TCP/UDP 53	Pass	Commercial → DNS
28	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	VLAN70_SERVEURS subnets	Any	Pass	Commercial → NAS / AD / ERP
29	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.110	TCP 587	Pass	Commercial → Serveur Mail (SMTP Submission)
30	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.110	TCP 993	Pass	Commercial → Serveur Mail (IMAPS)
31	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	VLAN20_RH subnets	Any	Block	Commercial → RH interdit
32	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	VLAN30_JURIDIQUE subnets	Any	Block	Commercial → Juridique interdit
33	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.128/27	Any	Block	Commercial → LAB interdit
34	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	!RFC1918	Any	Pass	Commercial → Internet
35	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.99	TCP/UDP 53	Pass	Compta → DNS
36	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	VLAN70_SERVEURS subnets	Any	Pass	Compta → Serveurs
37	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.110	TCP 587	Pass	Compta → Serveur Mail (SMTP Submission)
38	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.110	TCP 993	Pass	Compta → Serveur Mail (IMAPS)
39	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.128/27	Any	Block	Compta → LAB interdit
40	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	RFC1918	Any	Block	Compta → autres VLAN
41	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	!RFC1918	Any	Pass	Compta → Internet
42	pfSense Atlantis	VLAN70_SERVEURS	VLAN70_SERVEURS subnets	Any	Any	Pass	Serveurs → Accès global
43	pfSense Atlantis	MPLS	VLAN80_LABO subnets	192.168.1.99	TCP/UDP 53	Pass	LAB → DNS AD Atlantis
44	pfSense Atlantis	MPLS	VLAN80_LABO subnets	VLAN70_SERVEURS subnets	Any	Pass	LAB → Serveurs (NAS, AD, ERP)
45	pfSense Atlantis	MPLS	VLAN80_LABO subnets	192.168.1.162	TCP 80/443	Pass	LAB → IIS interne (DMZ)
46	pfSense Atlantis	MPLS	VLAN80_LABO subnets	VLAN40_BE subnets	Any	Pass	LAB → Bureau d'Étude (lecture via NAS/ERP)
47	pfSense Atlantis	MPLS	VLAN80_LABO subnets	RFC1918	Any	Block	LAB → Tous les VLAN Atlantis interdits (RH, Juridique, Compta...)
48	pfSense Atlantis	MPLS	10.10.10.0/30	Any	Any	Pass	Flux techniques MPLS : ping, traceroute, retour des connexions
49	pfSense Atlantis	MPLS	Any	pfSense Atlantis Address	Any	Block	Protection du firewall (pas d'admin via MPLS)
50	pfSense Atlantis	MPLS	Any	Any	Any	Block	Blocage final (sécurité maximale)

Figure 30 - Tableau de Filtrage de Atlantis





Politique de filtrage du pare-feu du PfSense Springfield VLAN Labo (VLAN80)

Les règles sont très restrictives :

- Accès autorisé : DNS, serveurs métiers (NAS, ERP, AD), IIS, Bureau d'Étude
- Accès interdit : tous les autres VLAN Atlantis
- Accès Internet autorisé
- Blocage final

Justification :

- Le LABO manipule des données techniques et potentiellement sensibles.
- Les postes sont variés et parfois connectés à des équipements spécialisés → risques accrus.
- L'accès au reste du réseau doit être strictement contrôlé.

Interface MPLS (Springfield)

Cette interface filtre les flux provenant d'Atlantis :

- Direction → accès complet LABO
- RH → accès LABO autorisé
- BE → accès LABO autorisé
- Tous les autres VLAN → interdits
- Pas d'administration du firewall via MPLS
- Blocage final

Justification :

- Le site Atlantis est la source légitime des accès vers le LABO.
- Les services autorisés correspondent exactement aux besoins métiers (Direction, RH, BE).
- Un cloisonnement fort garantit la sécurité du site distant.



Ordre	Équipement	Interface	Source	Destination	Protocole	Action	Description
1	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.99	TCP/UDP 53	Pass	LAB → DNS du DC (Atlantis)
2	pfSense	VLAN80_LABO	VLAN80_LABO subnets	VLAN70_SERVEURS subnets	Any	Pass	LAB → Serveurs Atlantis (NAS/AD/ERP)
3	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.162	TCP 80/443	Pass	LAB → IIS DMZ (site web interne)
4	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.48/28 (BE)	Any	Pass	NAS/ERP)
5	pfSense	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.110	TCP 587	Pass	LABO→ Serveur Mail (SMTP Submission)
6	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.110	TCP 993	Pass	LABO→ Serveur Mail (IMAPS)
7	pfSense	VLAN80_LABO	VLAN80_LABO subnets	RFC1918	Any	Block	LAB → Tout autre réseau privé Atlantis interdit
8	Springfield	VLAN80_LABO	VLAN80_LABO subnets	!RFC1918	Any	Pass	LAB → Internet autorisé
9	Springfield	VLAN80_LABO	VLAN80_LABO subnets	Any	Any	Block	Sécurité : bloque tout le reste
10	Springfield	MPLS	VLAN10_DIRECTION subnets	VLAN80_LABO subnets	Any	Pass	LABO
11	Springfield	MPLS	VLAN20_RH subnets	VLAN80_LABO subnets	Any	Pass	RH Atlantis → accès LABO autorisé
12	pfSense	MPLS	VLAN40_BE subnets	VLAN80_LABO subnets	Any	Pass	Bureau d'Étude → accès LABO (lecture/lecture seule via ACL)
13	Springfield	MPLS	RFC1918	VLAN80_LABO subnets	Any	Block	interdit
14	pfSense	MPLS	Any	pfSense Springfield Address	Any	Block	Protection du firewall (aucune admin depuis MPLS)
15	Springfield	MPLS	Any	Any	Block		Blocage final : sécurité Zero-Trust

Figure 31 - Tableau de filtrage de Springfield



Un schéma logique du service Active Directory

Fonctionnement de l'AD

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

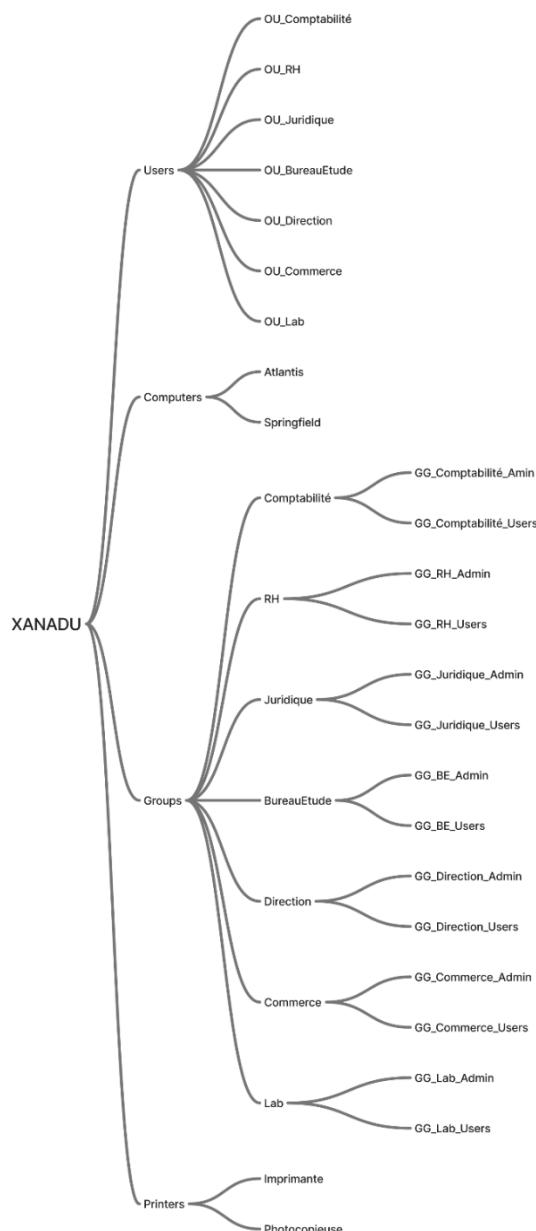


Figure 32 - Schéma de l'Active Directory



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

Dans notre forêt de l'Active Directory, nous avons choisi « xanadu.com » comme domaine racine qui contient la seule forêt de l'entreprise.

Au vu du fait que nous n'avons qu'un seul serveur contrôleur de domaine, tous les rôles FSMO seront actif sur celui-ci.

Stratégies de groupes

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

Un GPO de sécurité de mot de passe sera appliquer à tous les utilisateurs. Cela permettra par exemple de garantir la sécurité du mot de passe à l'aide d'un regex sur sa taille ou des caractères obligatoires comme une majuscule ou un chiffre. Ce GPO pourra aussi offrir un changement obligatoire du mot de passe après une période définie. Ce même GPO applique également un verrouillage de compte qui permet d'améliorer la sécurité d'authentification. En rajoutant des verrouillages après des connexion en échec et en rajoutant des périodes de verrouillages, les personnes voulant accéder à une session sans connaitre le mot de passe auront plus de difficultés à se connecter.

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



pourront être installés sur un poste de travail. Nous avons opté pour une utilisation en whitelist qui consiste à tout bloquer de base. Nous pouvons ensuite rajouter des règles pour autoriser certaines applications suivant leurs noms, leurs versions pour l'entreprise qui les produit. Quelques applications sont donc autorisées comme Internet Explorer, les applications systèmes de Windows et d'autres applications très utilisées par les employés.

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

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

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

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

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

Pour finir, nous avons mis en place un GPO pour propager le certificat de sécurité sur chaque poste de travail de l'entreprise. Ainsi, chaque employé de Xanadu pourra accéder à l'ERP de façon sécurisé avec le protocole HTTPS.

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

Paramétrage des GPO sur le serveur

Sur le serveur DC, après avoir configuré l'Active Directory avec les différentes Unités Organisationnelles et les Groupes Globaux, il était nécessaire de mettre en place des Stratégies de Groupes. Pour cela, le service de gestion de stratégies de groupes permet de créer des GPO et de les modifier facilement. Il suffit de quelques boutons pour les paramétrier.



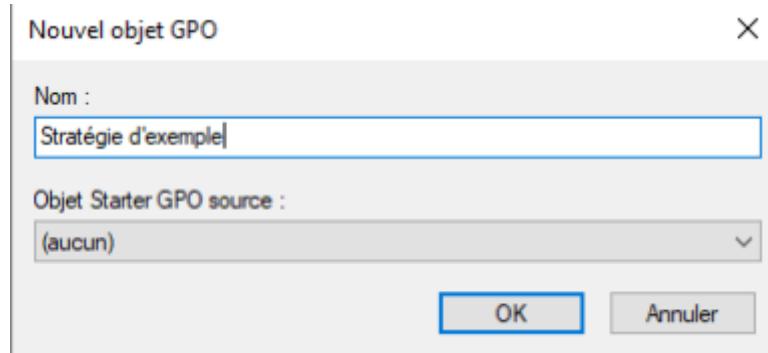


Figure 33 - Crédit de la nouvelle GPO

Après avoir créé une GPO et lui avoir donné un nom, on peut la modifier et lui attribuer les paramètres souhaités. Par exemple, pour la stratégie de sécurité de mot de passe, il faut savoir où se rendre et comme le montre la figure ci-dessous, aller dans les paramètres de sécurité pour retrouver les règles de sauvegarde. Ce chemin d'accès concerne seulement cette GPO et chacune des règles a un chemin différent et peut avoir une configuration différente.

Nom	Description
Stratégie de mot de passe	Stratégie de mot de passe
Stratégie de verrouillage du compte	Stratégie de verrouillage du compte
Stratégie Kerberos	Stratégie Kerberos

Figure 34 - Stratégies de mot de passe

Une fois que les règles et les paramètres sont configurés, le GPO devrait être fonctionnel mais avant de continuer, il faut s'assurer qu'il soit appliqué au bon endroit. Dans notre cas, les GPOs sont principalement appliqués soit à tous les utilisateurs



donc à l'OU « Users » ou à tous les postes de travail donc à l'OU « computers ». Pour être sûr que les stratégies de groupes soient opérationnelles immédiatement, la commande « gpupdate /force » sur le serveur et sur les postes clients concernés. Pour s'assurer de la bonne application de la stratégie de groupe, il est possible de voir un rapport détaillé en faisant la commande « gpresult /h rapport.html »

```
PS C:\Users\Administrateur> gpupdate /force
Mise à jour de la stratégie...
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

Figure 35 - Commande "gpupdate"



Gestion des données

Plan de sauvegarde des données

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

Stratégie en place sur le réseau de XANADU

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

- Le modèle de sauvegarde sera de la forme 3-2-1. Cette méthode, recommandée par l'ANSSI, consiste à disposer de 3 copies des données, stocker sur 2 supports différents, dont 1 hors du réseau. Nous utiliserons sur Xanadu un NAS interne (modélisé), un NAS externe et un stockage cloud.
- Le système de sauvegarde immuable reposant sur la protection aux changements. Elle est donc résistante aux erreurs humaines, à la suppression volontaire (pirate) ou involontaire (erreur humaine ou technique) et au ransomware (comme le chiffrement de données). (en avoir 1 minimum est une bonne pratique). Pour réaliser cette sauvegarde, nous allons une fois par mois faire appel à une société tierce tel que Veeam pour réaliser une sauvegarde immuable de nos données sur le Cloud.
- Une partie de la sauvegarde journalière sera différentielle (seul les données critiques sont concernées) : tous les soirs, une copie de toutes les données modifiées depuis la dernière sauvegarde complète (et non depuis les incrémentaux) est réalisée. La taille augmente chaque jour mais la récupération est plus rapide, nous permettant une remise à la normale plus rapide car seul la sauvegarde du dernier dimanche et la sauvegarde de la veille du problème doivent être rétablies.
- Une partie de la sauvegarde journalière sera incrémentielle (les données importantes et moins critiques sont concernées) : tous les soirs, une copie de toutes les données modifiées depuis la dernière sauvegarde incrémentielle est réalisée. La taille augmente de manière négligeable chaque jour mais la récupération est un peu moins rapide que la sauvegarde différentielle car la sauvegarde du dernier dimanche et la sauvegarde de tous les jours jusqu'à la veille du problème doivent être rétablies.



- Nous allons programmer notre NAS en Raid 5. Le disque pourra être divisé en 4 espaces distincts. Chaque espace pourra abriter $\frac{3}{4}$ de données brutes et $\frac{1}{4}$ de parité, permettant de récupérer des données si un espace disque est corrompu ou perdu. Les données seront ainsi séparées en 4 parties différentes de manière que la récupération des données soit garanti si une partie des données est perdue.

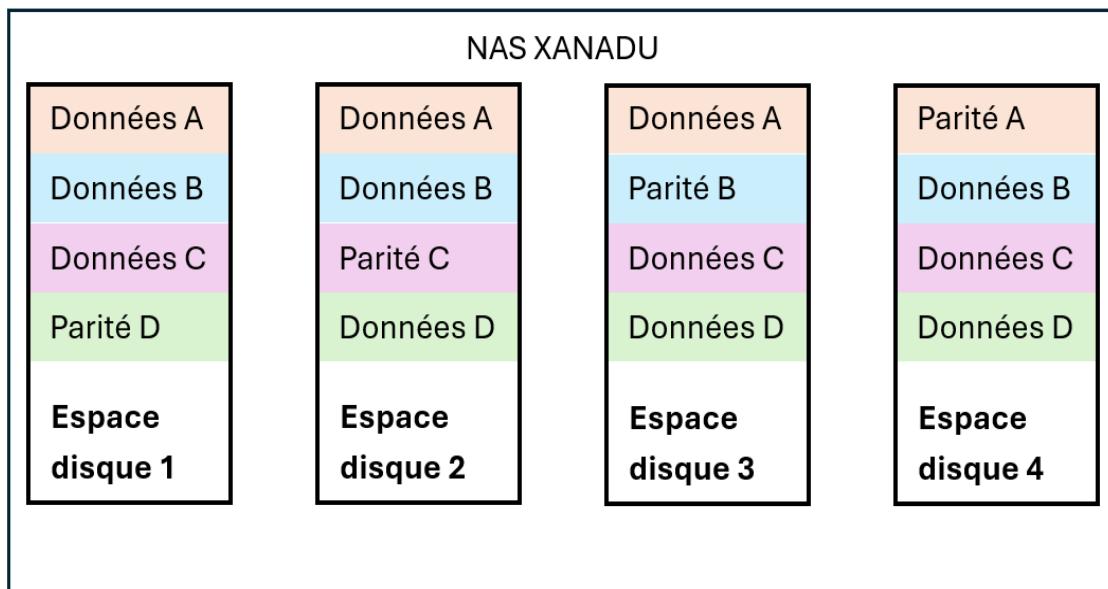


Figure 36 - Schéma du RAID 5

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

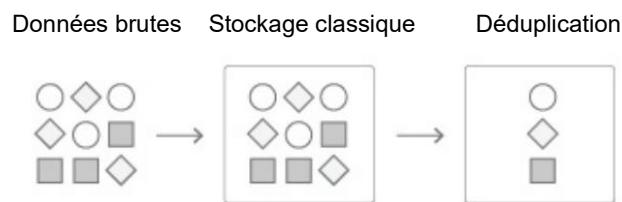


Figure 37 - Schéma de déduplication



Objectifs et criticité des données

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

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

Les données sont classées en trois niveaux de criticité :

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

Les objectifs de continuité d'activité sont les suivants :

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

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

Plan de sauvegarde

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

Du lundi au vendredi : snapshots ERP toutes les 4h sur le stockage local ERP

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



On peut donc proposer le plan de sauvegarde suivant :

Date	Données	Criticité	Type de sauvegarde	Localisation
Tous les dimanche 23h	Base ERP, Dossiers Direction, Dossiers Juridique, Dossiers Sinistres	Très élevée	Complète et immuable	Nas Interne, externe et Cloud
	Dossiers Client, Dossiers Commerce, Dossiers Conseil, Emails	Elevée	Complète	Nas Interne, externe et Cloud
	Dossiers personnels	Moyenne	Complète	Nas Interne, externe et Cloud
Tous les dimanche 23h	Base ERP, Dossiers Direction, Dossiers Juridique, Dossiers Sinistres	Très élevée	Complète	Nas Interne et externe
	Dossiers Client, Dossiers Commerce, Dossiers Conseil, Emails	Elevée	Complète	Nas Interne et externe
	Dossiers personnels	Moyenne	Complète	Nas Interne et externe
Du lundi au samedi 23h	Base ERP, Dossiers Direction, Dossiers Juridique, Dossiers Sinistres	Très élevée	Différentielle	Nas Interne
	Dossiers Client, Dossiers Commerce, Dossiers Conseil, Emails	Elevée	incrémentielle	Nas Interne
	Dossiers personnels	Moyenne	incrémentielle	Nas Interne

Figure 38 - Plan de sauvegarde complet de Xanadu proposé par CesTech

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

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

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



Volumes de données

Afin de prévoir au mieux les types de sauvegarde et l'évolutivité au cours du temps nous avons conjecturé le volume de données modifié chaque semaine.

Les volumes suivants sont retenus comme base de calcul :

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

Figure 39 - Tableau du volume total de données

Nous allons considérer les valeurs suivantes :

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

Figure 40 – Tableau récapitulatif du plan de sauvegarde

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

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

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



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

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

Le NAS de sauvegarde de 2 To bruts offre environ 1,5 To utiles. Un seuil d'alerte est fixé à 80 % d'occupation, soit 1,2 To.

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

Conservation, supervision et traçabilité des sauvegardes

Les durées de conservation sont les suivantes :

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

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

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



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



Network Attached Storage (NAS)

Dans le cadre de la maquette du système d'information, une solution de stockage centralisée a été mise en place sous la forme d'un NAS virtualisé. Ce NAS joue un rôle structurant dans l'architecture, en assurant à la fois le partage des données entre les utilisateurs et l'hébergement des sauvegardes des serveurs.

Le NAS est déployé sous forme d'une machine virtuelle TrueNAS hébergée sur l'hyperviseur Proxmox. Ce choix permet d'isoler le service de stockage, de faciliter son administration et de mettre en œuvre des mécanismes avancés de sécurité et de gestion des droits.

Paramétrage du VM NAS

Déploiement de la machine virtuelle NAS (TrueNAS)

Une machine virtuelle dédiée a été créée sur Proxmox afin d'héberger le NAS. Cette VM dispose de ressources allouées spécifiquement pour le stockage et l'accès aux données (CPU, mémoire, disques).

Le NAS virtualisé s'appuie sur des volumes de stockage présentés à la VM depuis l'infrastructure sous-jacente. Cette approche permet :

- Une séparation claire entre l'hyperviseur et les données,
- Une meilleure flexibilité dans la gestion des volumes,
- Une évolution facilitée de la capacité de stockage.

La VM TrueNAS constitue ainsi un point central unique pour la gestion des données de l'entreprise.



Organisation logique du stockage (datasets)

Le stockage est organisé de manière logique à l'aide de datasets distincts. Cette organisation permet de cloisonner les usages, d'appliquer des règles de sécurité spécifiques et de faciliter l'administration.

Les principaux datasets mis en place sont :

- Des datasets dédiés aux partages par service,
- Des datasets dédiés aux dossiers personnels des utilisateurs,
- Des datasets dédiés aux sauvegardes des serveurs.

Cette séparation permet d'appliquer des politiques différentes selon la nature des données (données métiers, données personnelles, données techniques) et répond aux exigences de sécurité et de confidentialité exprimées dans le cahier des charges.

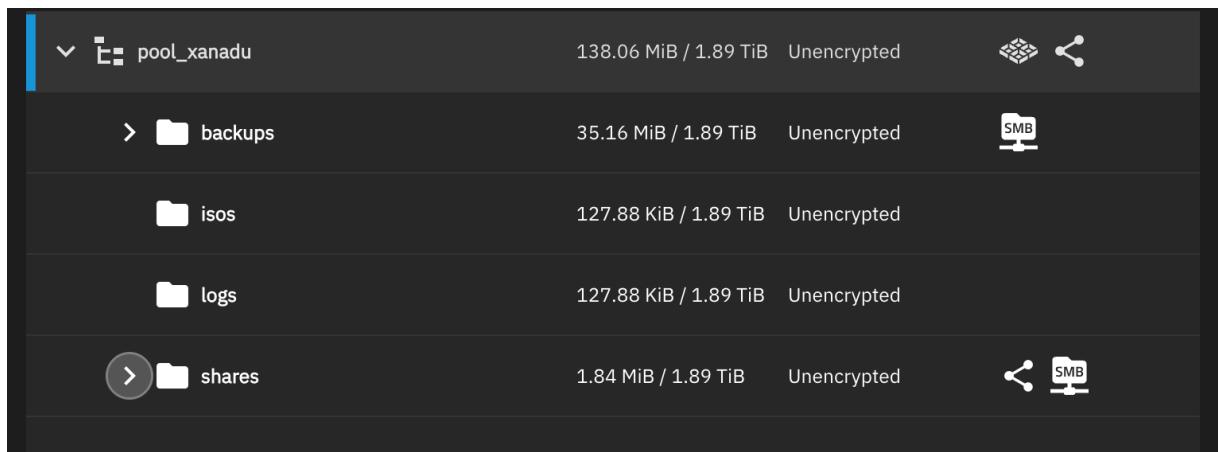


Figure 41 - Datasets



Mise en place des partages SMB

Les datasets destinés aux utilisateurs sont exposés via des partages SMB, afin de garantir une compatibilité native avec les postes clients Windows.

Les partages SMB sont organisés conformément aux besoins métiers :

- Un partage par service, accessible uniquement aux membres du service concerné,
- Un espace de dossiers personnels centralisés pour chaque utilisateur,
- Des partages spécifiques réservés aux sauvegardes, non accessibles aux utilisateurs standards.

Le protocole SMB a été retenu pour sa compatibilité avec Active Directory et sa gestion avancée des permissions.

Windows (SMB) Shares				RUNNING	Add	⋮
Name	Path	Description	Enabled			
users	/mnt/poo l_xanad...	Dossier personnel	<input checked="" type="checkbox"/>			
commun	/mnt/poo l_xanad...	Dossier partagé	<input checked="" type="checkbox"/>			
admin	/mnt/poo l_xanad...	Dataset réservé	<input checked="" type="checkbox"/>			
juridique	/mnt/poo l_xanad...		<input checked="" type="checkbox"/>			

Figure 42 - Protocole SMB



Gestion des droits d'accès via ACL

La sécurité des données repose sur une gestion fine des droits d'accès au niveau du NAS. Des ACL avancées ont été mises en place sur l'ensemble des datasets.

Pour les dossiers personnels :

- Chaque utilisateur est propriétaire de son dossier,
- L'utilisateur dispose d'un contrôle total sur ses données,
- Aucun autre utilisateur n'a accès à ces dossiers.

Pour les dossiers partagés par service :

- Seuls les membres du groupe Active Directory correspondant au service disposent des droits d'accès,
- Les permissions sont définies de manière explicite afin d'éviter tout héritage non maîtrisé.

Pour les datasets de sauvegarde :

- Seuls les comptes techniques des serveurs sont autorisés à accéder aux données,
- Aucun accès utilisateur standard n'est autorisé.

Cette gestion par ACL permet un contrôle précis des accès et garantit la confidentialité des données.

Cohérence entre ACL NAS et Active Directory

Les droits appliqués sur le NAS sont définis en cohérence avec la structure Active Directory. Les groupes de sécurité AD sont utilisés comme référence pour l'attribution des permissions sur les partages SMB.

Cette approche permet :

- Une administration centralisée des droits via l'annuaire,
- Une délégation possible de la gestion des comptes et groupes,
- Une réduction des erreurs de configuration.

Les modifications de droits sont ainsi réalisées côté Active Directory, puis automatiquement prises en compte sur le NAS via les ACL.



Activation de l'Access Based Enumeration (ABE)

La fonctionnalité Access Based Enumeration a été activée sur l'ensemble des partages SMB. Elle permet de masquer automatiquement les dossiers auxquels un utilisateur n'a pas accès.

Grâce à l'ABE :

- Un utilisateur ne visualise que les dossiers pour lesquels il dispose de droits,
- Les dossiers des autres services sont invisibles,
- Les espaces de sauvegarde ne sont jamais visibles par les utilisateurs standards.

Cette fonctionnalité renforce la sécurité et améliore l'ergonomie pour les utilisateurs finaux.

Rôle du NAS dans la stratégie globale de sauvegarde

En complément de son rôle de serveur de fichiers, le NAS virtualisé est utilisé comme cible principale des sauvegardes des serveurs du système d'information.

Les sauvegardes sont stockées dans des datasets dédiés, séparés des données utilisateurs, et protégés par des droits stricts. Cette organisation permet :

- Une meilleure traçabilité des sauvegardes,
- Une limitation des risques de suppression accidentelle,
- Une gestion adaptée à la criticité des données.

Le NAS constitue ainsi un élément clé de la stratégie de continuité et de reprise d'activité.

Lien avec les stratégies de groupe (GPO)

La configuration du NAS est pensée en cohérence avec les stratégies de groupe mises en place dans Active Directory.

Les GPO permettent notamment :



- Le mappage automatique des lecteurs réseau en fonction du service de l'utilisateur,
- La redirection des dossiers utilisateurs (ex. "Documents") vers les dossiers personnels centralisés sur le NAS,
- L'application cohérente des droits d'accès sans intervention manuelle sur les postes.

Cette intégration entre NAS, Active Directory et GPO garantit une expérience utilisateur homogène et simplifie l'administration du système.

Apports de la solution NAS dans la maquette

La mise en place d'un NAS virtualisé permet de répondre aux exigences du projet XANADU en matière de confidentialité, d'intégrité, de disponibilité et de traçabilité.

L'organisation des datasets, la gestion des droits via ACL, l'activation de l'ABE et l'intégration avec Active Directory et les GPO démontrent la cohérence et la viabilité de la solution proposée dans le cadre de la maquette.



Création d'un accès Web sécurisé

Création d'un serveur web

Afin de proposer à Xanadu une interface web, nous avons mis en place un serveur IIS sur le réseau. Pour cela nous avons généré une machine virtuelle Windows Serveur sur lequel nous avons installé un serveur IIS.

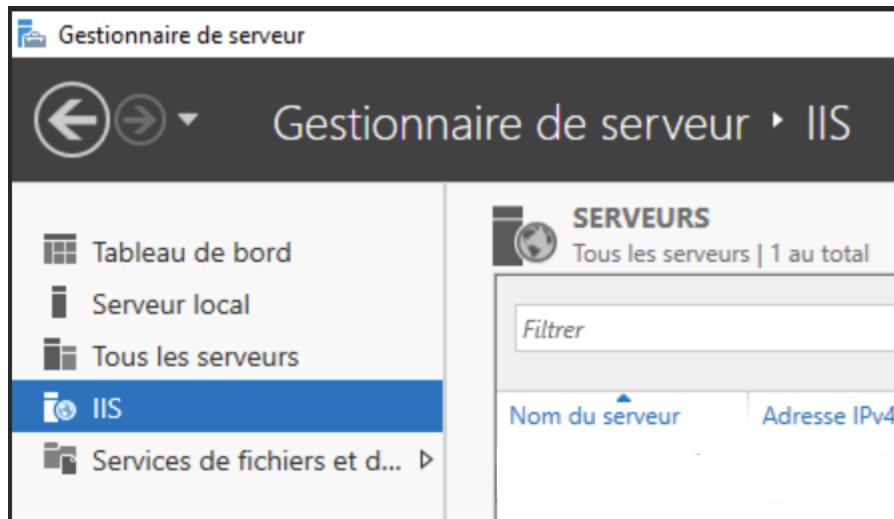


Figure 43 - Installation du serveur IIS

Une fois le service installé, nous avons accès au gestionnaire des services internet. Ce gestionnaire IIS nous permet d'administrer notre site web et notre interface interne destinée aux collaborateurs.

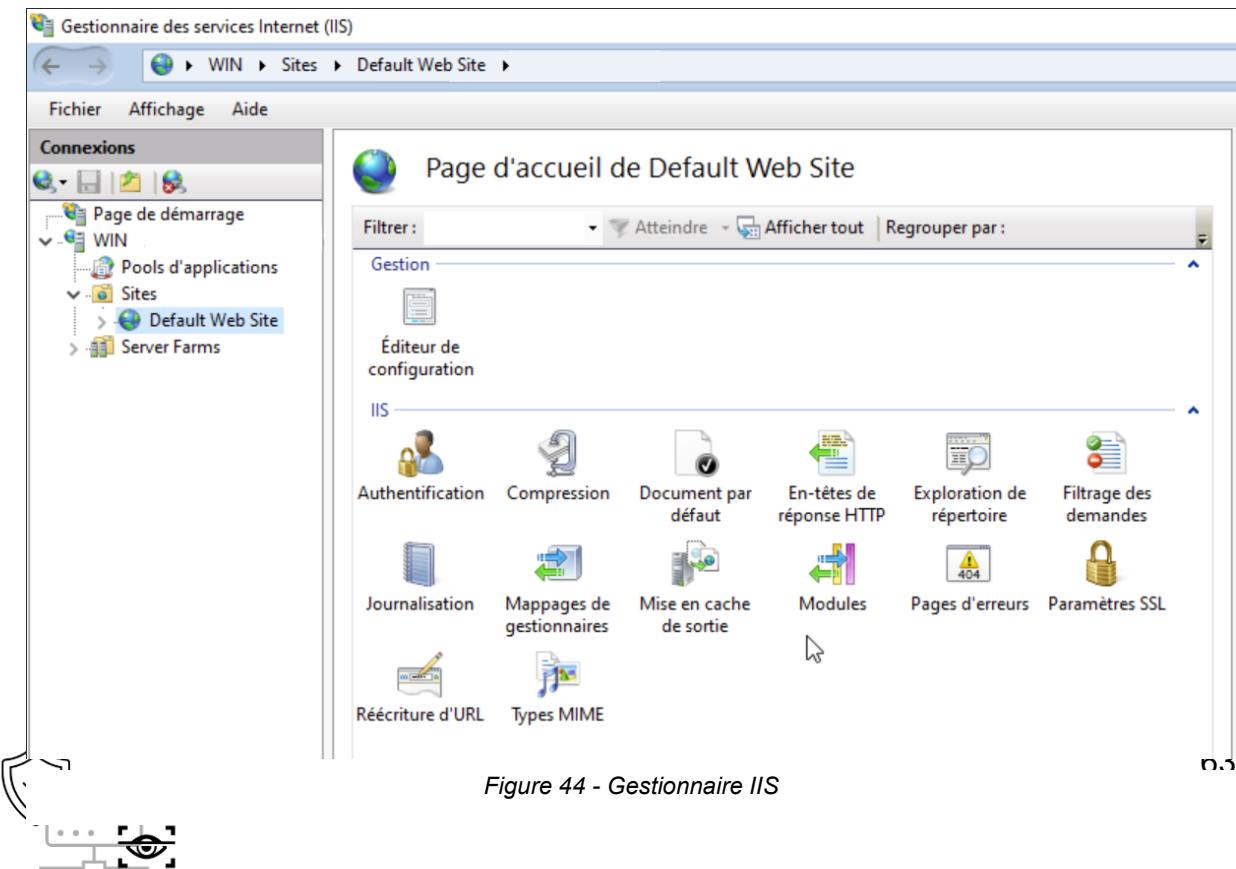


Figure 44 - Gestionnaire IIS

Afin de mettre en place le site et le rendre accessible depuis les postes de l'entreprise, il est important de paramétrer les bindings (liaisons) qui vont permettre au serveur DNS de résoudre le nom de domaine lorsqu'il sera saisi dans une barre d'URL. On peut notamment voir (figure 19) que le nom d'hôte est bien xanadu.com et que le site est paramétré en http (HyperText Transfer Protocol) sur le port 80. On peut donc confirmer que le site est accessible mais non sécurisé.

Liaisons de sites				
Type	Nom de l'hôte	Port	Adresse IP	Informations sur...
http	xanadu.com	80	*	

Figure 45 - Liaisons du site web de Xanadu

On peut donc accéder à l'interface front du site depuis les postes du réseau pointant sur notre serveur DNS. Le site est en http donc non sécurisé.

XanaduERP

Non sécurisé https://xanadu.com/login

Enter your email*

pat@example.com

Mot de passe*

Se connecter

Figure 46 - Connexion à l'interface web depuis un fichier client

Sécurisation de l'accès web par certificat

Afin de proposer aux collaborateurs de Xanadu des échanges sûr et sécurisés, nous avons mis en place un certificat Open SSL.

Un certificat OpenSSL est utilisé pour sécuriser les communications entre deux systèmes informatiques. L'objectif est de garantir :



- La sécurité par le chiffrement des échanges : les personnes qui ne sont pas autorisées à lire le flux ne peuvent pas y accéder. On peut ainsi éviter une attaque de type Man in the Middle (MitM) où les données sont interceptées et lues par une entité malveillante.
- L'authentification par la signature : les données échangées sont signées par une clé afin d'en garantir la provenance.
- L'intégrité par l'utilisation de clés de chiffrement et déchiffrement : il assure que les informations échangées n'ont pas été modifiées durant le transport.

Le principe du certificat SSL est le suivant : il repose sur la cryptographie asymétrique, qui utilise deux clés complémentaires. Une clé de chiffrement et une clé de déchiffrement qui assurent que les données en transit sont illisibles. On retrouve donc 2 clés, une publique et une privée, toutes 2 sont nécessaires pour tout échange.

- La clé privée : conservée secrètement sur le serveur.
- La clé publique : intégrée au certificat et partagée avec les clients.

Lorsqu'un client se connecte à un serveur sécurisé, le serveur lui transmet son certificat numérique. Le poste client vérifie la validité du certificat par son identité, sa date d'expiration... Une fois le certificat jugé fiable, une session est ouverte. Les flux sont alors chiffrés, empêchant toute interception ou altération.

Génération et signature du certificat

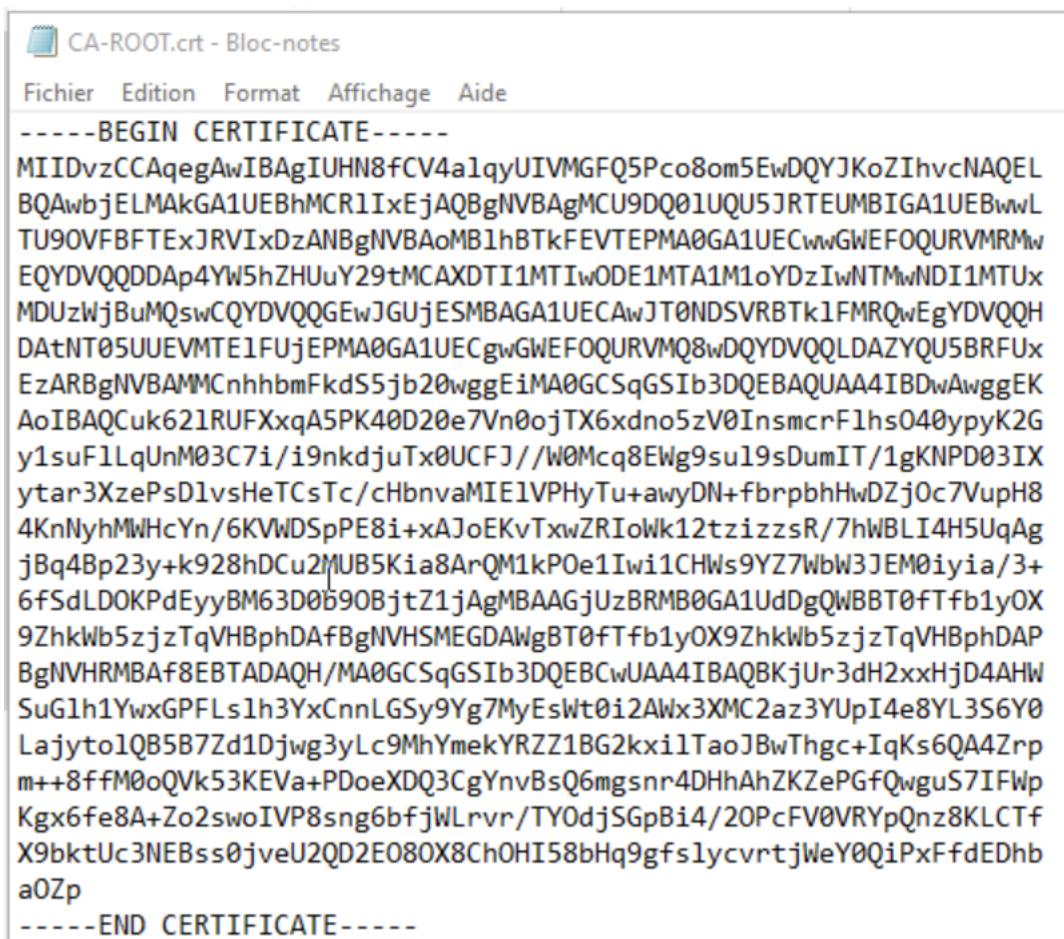
Nous avons commencé par générer le certificat sur le serveur DNS. Pour cela nous avons installé Open SSL.

```
PS C:\Users\Administrateur> openssl -v
OpenSSL 3.6.0 1 Oct 2025 (Library: OpenSSL 3.6.0 1 Oct 2025)
```

Figure 47 - Version de Open SSL sur le serveur DNS

Nous avons poursuivi en générant une clé privée RSA sur l'autorité de certificat. Il s'agit d'une clé privée au format .pem ou .crt qui est protégée par un texte unique servant de mot de passe afin de le déchiffrer (figure 2.). Il s'agit du certificat racine qui va signer tous les échanges.





```

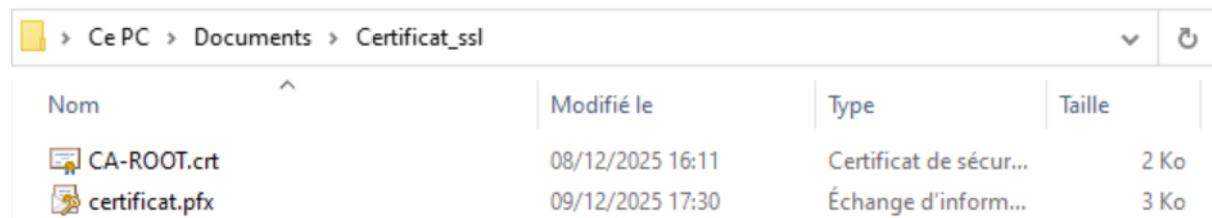
CA-ROOT.crt - Bloc-notes
Fichier Edition Format Affichage Aide
-----BEGIN CERTIFICATE-----
MIIDvzCCAqegAwIBAgIUHN8fCV4a1qyUIVMGFQ5Pco8om5EwDQYJKoZIhvcNAQEL
BQAwbjELMAkGA1UEBhMCR1IxEjaQBgNVBAgMCU9DQ01UQU5JRTUMBIGA1UEBwwL
TU90VFBFTExJRVIxDzANBgNVBAoMB1hBTkFEVTEPMA0GA1UECwwGWEFOQURVMRMw
EQYDVQQDDAp4YW5hZHUuY29tMCAXDTI1MTIwODE1MTA1M1oYDzIwNTMwNDI1MTUx
MDUzWjBuMQswCQYDVQQGEwJGUjESMBAGA1UECAwJT0NDSVRBTk1FMRQwEgYDVQOH
DAcNT05UUVEVMTExFUjEPMA0GA1UECgwGWEFOQURVMQ8wDQYDVQQLDAZYQU5BRFUx
EzARBgNVBAMMCnhhbmkFdS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQcuk621RUFXxqA5PK40D20e7Vn0ojTX6xdno5zV0InsmcrFlhs040ypyK2G
y1suF1LqUnM03C7i/i9nkdjuTx0UCFJ//W0Mcq8EWg9su19sDumIT/1gKNPD03IX
ytar3XzePsD1vsHeTCsTc/cHbnvaMIE1VPhTu+awyDN+fbrpbhHwDZj0c7VupH8
4KnNyhmWhcYn/6KVWDSpPE8i+xAJoEKvTxwZRIoWk12tzizzsR/7hWBLI4H5UqAg
jBq4Bp23y+k928hDCu2MUB5Kia8ArQM1kP0e1Iwi1CHWs9YZ7WbW3JEM0iyia/3+
6fSdLDOKPdEyyBM63D0b90BjtZ1jAgMBAAGjUzBRMB0GA1UdDgQWBBD0fTfb1y0X
9ZhkB5zjzTqVHBphDAfBgNVHSMEGDAwBT0fTfb1y0X9ZhkB5zjzTqVHBphDAP
BgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBKjUr3dH2xxHjD4AHW
SuG1h1YwxGPFLs1h3YxCnnLGSy9Yg7MyEsWt0i2AWx3XMC2az3YUpI4e8YL3S6Y0
Lajyto1QB5B7Zd1Djwg3yLc9MhYmekYRZZ1BG2kxi1TaoJBwThgc+IqKs6QA4Zrp
m++8ffM0oQVk53KEVa+PDoeXDQ3CgYnvBsQ6mgnsnr4DHhAhZKZePGfQwguS7IFWp
Kgx6Fe8A+Zo2swoIVP8sng6bfjWLrvr/TY0djSGpBi4/20PcFV0VRYpQnz8KLCTf
X9bktUc3NEBss0jveU2QD2E080X8ChOHI58bHq9gfslycvrtjWeY0QiPxFfdEDhb
a0Zp
-----END CERTIFICATE-----

```

Figure 48 - Certificat signé (chiffré)

La demande de certificat est alors signée.

Une fois le certificat généré avec succès sur le serveur DNS, nous pouvons le



Nom	Modifié le	Type	Taille
CA-ROOT.crt	08/12/2025 16:11	Certificat de sécurité	2 Ko
certificat.pfx	09/12/2025 17:30	Échange d'informations	3 Ko

Figure 49 - Certificats sur le serveur IIS



Mise en place du backend et de la base de données

Conception et développement du backend en Go

Le backend a été conçu et développé en Go afin de disposer d'un service applicatif léger, performant et adapté à une exposition réseau contrôlée. Le choix de ce langage repose sur sa capacité à produire des binaires autonomes et sa pertinence pour le développement d'API REST destinées à une utilisation serveur. L'objectif était de mettre en place un composant fiable du système d'information, capable de fournir des services précis sans dépendances excessives.

L'architecture du backend a été pensée de manière modulaire, avec une séparation claire des responsabilités. La couche HTTP est dédiée à la réception et au routage des requêtes, la logique métier gère les règles fonctionnelles liées aux utilisateurs, et l'accès aux données est isolé afin de garantir une meilleure maintenabilité. Cette organisation permet de faire évoluer chaque partie indépendamment, tout en limitant les risques de régression.

Dès sa conception, le backend a été développé pour s'intégrer dans l'infrastructure existante de Xanadu. Les paramètres critiques, tels que le port d'écoute ou les points de connexion vers l'API interne, sont externalisés afin de faciliter le passage d'un environnement local à un environnement de production. Cette approche garantit une transition fluide vers une exposition réseau ultérieure, sans modification structurelle du service.

Mise en place des fonctionnalités de gestion des utilisateurs

Le but de l'API était simplement de réaliser un POC d'un ERP. Une seul table quelques routes permettaient de très simplement démontrer la possibilité de notre infrastructure. Pour démontrer ça, nous avons simplement créé des utilisateurs, permettant de démontrer une relation directe entre une application front-end et une application back-end. Lors du développement l'appel à l'API se faisait via l'adresse Localhost:3000, dû au fait de l'environnement de développement front et back qui étaient sur le même poste.

Notre front en Angular permet donc de démontrer le fonctionnement de l'API grâce à la page de connexion, avec validation côté back des logs, et un affichage de page home, avec les informations du user connecté.



Problématique d'exposition d'un service localhost

Lors des phases de développement et de test, le backend était accessible uniquement via l'adresse localhost, ce qui limite son utilisation à la machine sur laquelle le service est exécuté. Dans un contexte de système d'information, cette configuration n'est pas viable, car elle empêche tout accès depuis des postes clients ou d'autres serveurs possédant une autre adresse IP. Il a donc été nécessaire de repenser l'exposition du service afin de le rendre accessible de manière contrôlée depuis l'extérieur, sans modifier son fonctionnement interne.

La solution retenue a été la mise en place d'un reverse proxy jouant le rôle de passerelle entre le réseau et le backend. Ce composant permet d'associer un nom de domaine, en l'occurrence xanadu.com, à un service interne fonctionnant sur localhost. Les requêtes adressées à xanadu.com sont ainsi redirigées vers le backend local, tout en conservant un cloisonnement réseau strict car le port interne du service n'est jamais exposé directement. Cela permet de centraliser l'exposition des services, de renforcer la sécurité et de fournir un point d'accès unique et maîtrisé au backend.



Réécriture d'URL

Fournit des fonctions de réécriture basée sur des règles pour l'adresse URL demandée et le contenu d'une réponse HTTP.

Règles de trafic entrant appliquées à l'adresse de l'URL demandée :

Nom	Entrée	Correspondance	Modèle	Type ...	URL d'action
Api...	Chemin de l'URL ...	Correspondances	<code>^api/(.*)\$</code>	Réécr...	<code>http://localhost:3000/{...</code>

Figure 51 - Réécriture d'URL

L'avantage de Go est d'avoir un exécutable pouvant être relancé automatiquement lors du démarrage du serveur. Notre exécutable nous permet d'éviter tout soucis de compilations lors du démarrage de la machine, et relancer proprement notre service. Pour cela nous avons utilisé l'outil NSSM qui se charge de lancer automatiquement des exécutables à l'ouverture du serveur.



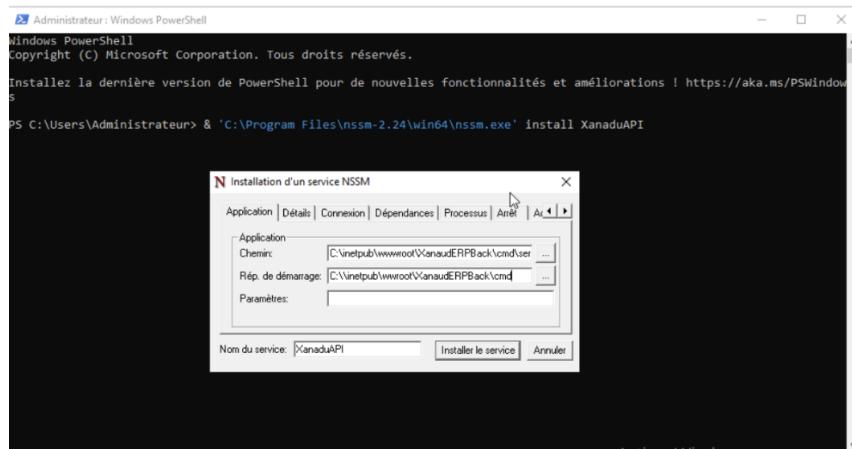


Figure 52 - Configuration NSSM pour lancer le serveur Go

```
PS C:\Users\Administrateur> net start XanaduAPI
Le service demandé a déjà été démarré.

Vous obtiendrez une aide supplémentaire en entrant NET HELPMSG 2182

PS C:\Users\Administrateur> Get-Service XanaduAPI
Status    Name          DisplayName
-----  -----
Running   XanaduAPI    XanaduAPI
```

Figure 53 - Service API

Sécurisation et validation de l'accès depuis l'extérieur

La dernière étape a consisté à sécuriser l'accès au backend exposé et à valider son fonctionnement depuis des machines externes au serveur. L'exposition du service a été limitée au strict nécessaire, en s'appuyant sur le reverse proxy comme unique point d'entrée. Le backend interne reste inaccessible directement depuis le réseau, ce qui réduit significativement la surface d'attaque et renforce le cloisonnement de l'architecture.

Des contrôles ont ensuite été réalisés depuis des postes distants afin de vérifier que le nom de domaine xanadu.com permettait bien d'accéder aux fonctionnalités prévues de l'API. Ces tests ont permis de valider la redirection des flux, la disponibilité du service et la cohérence des réponses. Cette phase de vérification garantit que le backend est exploitable dans un contexte réel, tout en respectant les exigences de sécurité et de fiabilité attendues dans un environnement professionnel.



Supervision

Pour améliorer la sécurité de l'entreprise XANADU, il est important de mettre en place des fonctionnalités de supervision. Cela nous permettra à nous et aux personnels de XANADU en charge de la surveillance de pouvoir voir et analyser les données des différents serveurs, comptes utilisateurs ou autres objets qui compose l'infrastructure mis en place.

Tableau des actions de Supervision

Description	Criticité	Source	Action déclenchée	Justification sécurité
Tentative de connexion échouées	Haute	Active Directory (DC)	Alerte mail + blocage du compte	Détection d'attaques par brute force
Connexion Administrateur	Haute	Active Directory (DC)	Alerte mail	Suivi des accès sensibles
Modification de GPO	Haute	Contrôleur de Domaine	Alerte mail	Prévention des modifications non autorisées
Désactivation de l'antivirus	Haute	Antivirus	Alerte mail + isolement automatique	Risque immédiat de compromission
Activité réseau anormale	Moyenne	Routeur	Alerte + capture réseau automatique	Analyse de comportements suspects
Appareil inconnu sur le réseau	Moyenne	Switch	Alerte + blocage automatique	Protection contre les intrusions physiques
Arrêt d'une fonctionnalité système	Haute	Serveur DC	Alerte + Tentative de relance	Prévention d'un arrêt imprévu d'une fonctionnalité
Échec de sauvegarde complète	Haute	Sauvegarde	Tentative de relance de sauvegarde	Protection de l'intégrité des données
Échec de sauvegarde critique	Haute	Sauvegarde	Tentative de relance de sauvegarde	Données hautement sensibles à restaurer
Échec de sauvegarde ERP	Moyenne	Sauvegarde	Tentative de relance de sauvegarde	Continuité de service applicative

Figure 54 - Tableau de Supervision



Description des actions de Supervision

Comme vu dans le tableau ci-dessus, nous avons décidé de mettre en place plusieurs mécanismes de surveillance pour suivre les actions suspectes pouvant se produire dans l'infrastructure. En utilisant les différents outils de supervision, nous pouvons mettre en place des alertes, isolement, relance de sauvegarde qui seront dédiés à la sécurité et la maintenance.

Supervision d'authentification

Nous avons prévu plusieurs actions de supervision concernant des problèmes pouvant survenir lors de la connexion des utilisateurs. Par exemple, si l'outil de supervision détecte que, pour un même compte utilisateur, il y a eu 3 tentatives de mots de passes échoués en moins de 1 minute, le compte utilisateur sera bloqué temporairement, le temps d'analyser la situation. On va également recevoir une alerte par mail pour nous communiquer des informations comme le compte utilisé, le poste de travail concernés ainsi que l'heure des tentatives. Avec cet ensemble d'information, on peut dans un premier temps déterminer s'il s'agit d'une attaque par brute force ou simplement d'un utilisateur maladroit. Dans un second temps, on élaborera une stratégie pouvant éviter que ce genre de situation se reproduise en sensibilisant le personnel ou en renforçant la sécurité.

Dans la même volonté, il est important de veiller à ce que le compte administrateur ne soit pas accessible par tout le monde à tout moment. Pour cela, une supervision de ce compte sera mise en place. S'il y a une quelconque tentative de connexion qui semble anormale par rapport au poste de travail, ou à l'horaire de connexion par exemple, le compte administrateur sera automatiquement bloqué. Il faudra attendre l'intervention d'un autre compte administrateur pour le débloquer. De plus, de la même manière que pour la supervision précédente, une alerte par mail est également mise en place. Que cela soit une tentative réussie ou échouée, nous aurons des informations comme l'horaire de l'événement, le compte administrateur ciblé, le poste de travail utilisé ou tout autre indication permettant d'identifier l'auteur de l'événement. Grâce à cela, nous pourrons, comme pour la connexion échouée, établir une stratégie pour identifier la menace et éviter que cela se reproduise.



Supervision de Sécurité

Pour veiller à une sécurité du réseau, plusieurs autres actions de supervision sont mises en place comme la présence d'alertes sur des modifications non autorisés ou une anomalie sur le réseau. Dans le cas où un utilisateur désactiverait son antivirus, un mail nous sera envoyé pour nous prévenir et nous transmettre les informations descriptives de l'événement. La présence d'un antivirus, la désactivation non autorisée provoquerait une faille dans l'infrastructure du réseau. Pour éviter cela, le poste de travail sera isolé du réseau pour contrer une attaque globale sur l'entièreté du réseau de l'entreprise.

Certains des GPO mis en place ne devraient pas être modifiés. Afin de vérifier qu'ils restent intacts, une supervision vérifie l'état de modification des GPO définis. Comme pour la plupart des autres actions de supervisions, nous recevrons une alerte mail pour nous prévenir et nous communiquer les principales informations sur changement. Nous estimons que la modification de ces GPO pourrait résulter d'un outrepassage des autorisations accordées à un utilisateur et qu'il est important de prévenir ce genre de cas.

Concernant les possibles anomalies pouvant survenir sur le réseau, il est possible qu'un poste de travail se rajoute sur celui-ci alors qu'il n'est pas prévu. Ne connaissant pas la provenance de ce poste de travail, nous avons décidé d'appliquer un blocage automatique de cet appareil. Ainsi, le temps d'analyser ce nouvel ordinateur, nous évitons une potentiel intrusion physique et renforçons la sécurité du réseau.

Dans le cas où une fonctionnalité du serveur DC tombe en panne, une action de supervision nous alertera de la fonctionnalité avec les informations importantes. De plus, il sera automatiquement exécuté une tentative pour relancer le service tombé en panne. Nous pourrons ainsi analyser cette panne et si elle persiste, trouver un moyen par nous-même de relancer le service ou la fonctionnalité qui est tombé en panne.

Au sein du réseau de XANADU, le réseau entre les appareils ainsi que le réseau internet ont besoin d'être stables pour garantir un environnement de travail adéquat à tous les utilisateurs. Pour éviter de perturber ce réseau, nous avons mis en place de la supervision pour détecter un usage anormal du réseau par un utilisateur. De cette manière, nous pouvons détecter ces anomalies et constater des téléchargements anormaux ou la lecture de média trop conséquent.



Supervision de sauvegarde

En accord avec le plan de sauvegarde décrit dans le livrable précédent, nous devons pouvoir restaurer les données suivant leur criticité et leur importance. Nous avons donc établi que pour chacune des sauvegardes, il faut anticiper le cas où celle-ci ne s'exécute pas correctement. Lors de la sauvegarde complète du dimanche, si une erreur survient, une action de supervision pourra la capter. Dans ce cas, une nouvelle tentative de sauvegarde sera effectuée. L'action de supervision pourra détecter si la sauvegarde échoue 3 fois à la suite et ainsi nous prévenir pour analyser et lancer la réparation. Cela nous permet de protéger l'intégrité des données et d'assurer la restauration des données.

Il y a également la même action appliquée sur la sauvegarde quotidienne et prioritairement sur les données critiques afin de pouvoir plus facilement restaurer ces données dans le temps donné. De la même manière, les sauvegardes de l'ERP sont aussi soumises à une supervision qui nous permet de prévenir la perte de données.

Solution de supervision

Pour avoir accès à une supervision complète et sécurisé, nous avons décidé d'utiliser Zabbix. Nous avons ainsi créé un serveur Ubuntu qui contient les données de l'outil de supervision. Sur ce serveur, nous avons installé docker puis docker-compose. Puis, nous avons créé un fichier « docker-compose.yml » regroupant les informations du serveur Zabbix, une base de données, et le composant web adéquat. Avec la commande « docker-compose up -d », le serveur Zabbix s'est construit et fonctionne depuis en continu. Chaque utilisateur peut se rendre sur l'ip du serveur Zabbix avec un navigateur web pour pouvoir monitoner les différentes machines. En revanche, il faudra les accès d'un compte pour pouvoir s'y connecter.

Pour pouvoir analyser et maintenir au mieux les données, nous avons installé des agents sur chaque poste de travail et serveurs qu'il faut surveiller. Si nous prenons l'exemple du serveur DC, configuré l'agent nous permet de voir les performances du serveur et détecter des tentatives de connexions non autorisés ou des arrêts anormaux de services. Après avoir généré une clé avec openssl et l'avoir enregistré dans un fichier sécurisé, nous avons utilisé cette clé pour l'encryptage psk.

Au sein de l'outil de supervision Zabbix, nous avons paramétrier plusieurs configurations pour nous permettre d'avoir une meilleure gestion et d'augmenter la prévention d'anomalies. L'administration de Zabbix a notamment un utilisateur créer



paramétrier avec le mail adéquat de l'entreprise. Si nous gardons l'exemple du serveur contrôleur de domaine, un hôte a été créer sur Zabbix auquel a été associé l'IP correspondante. Après avoir créé des items adéquats et un trigger sur l'hôte souhaité, un mail a été configuré pour s'envoyer quand une action a été détecté. Pour continuer avec cet exemple, une connexion échouée sur le serveur DC va envoyer un mail aux utilisateurs administrateurs de Zabbix.

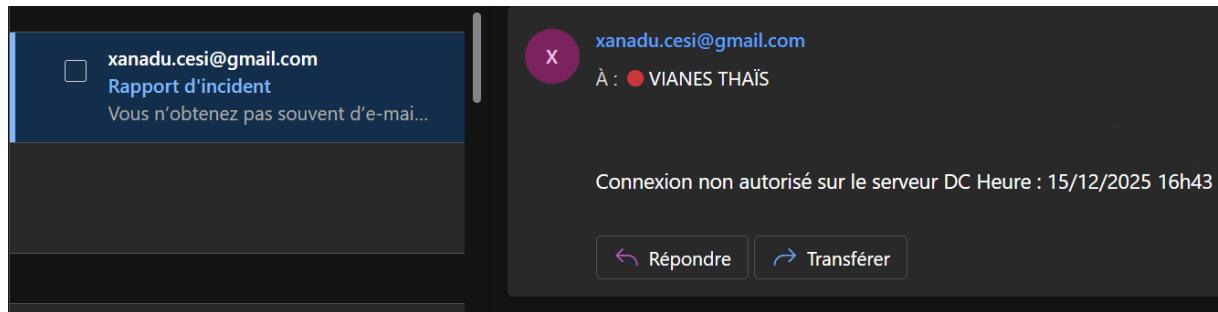


Figure 55 - Mail Exemple de Supervision



Sécurité des données

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

Confidentialité

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

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

Figure 56 - Eléments de confidentialités

Intégrité

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

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

Figure 57 - Eléments d'intégrité



Disponibilité

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

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

Figure 58 - Eléments de Disponibilité

Traçabilité

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

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

Figure 59 - Eléments de Traçabilité



Scripts

Afin de faciliter la maintenance du S.I. et garantir une scalabilité efficace dans un contexte de croissance, nous avons mis en place des scripts PowerShell faciles d'utilisation et structurés sous la forme d'un module unique nommé XanaduScripts.

Le recours au module permet d'utiliser les commandes PowerShell afin de répondre aux enjeux du projet avec une automatisation des tâches récurrentes, une réduction des erreurs, une homogénéisation des procédures et une traçabilité des actions.

Parmi les fonctionnalités proposées par les scripts nous retrouvons :

- Gestion des utilisateurs
 - Création
 - Modification
 - Suppression
 - Affichage de la liste complète des utilisateurs
 - Réinitialisation de mot de passe utilisateur
- Gestion du serveur DC
 - Vérifications du DC
 - Vérification de l'AD
 - Vérifications complètes
- Gestion de l'ERP
 - Sauvegarde des bases de données dans l'ERP
 - Vérification de l'ERP
 - Vérifications complètes



Gestion des utilisateurs

Contexte

Ce script PowerShell a été développé pour répondre à un besoin de gestion centralisée et sécurisée des comptes utilisateurs Active Directory du domaine Xanadu. Il vise à fournir aux administrateurs un outil unique permettant d'effectuer l'ensemble des opérations courantes sur les comptes utilisateurs, tout en limitant les manipulations manuelles directement dans la console Active Directory.

L'objectif principal est de fiabiliser les actions d'administration en standardisant les processus de création, de modification, de suppression et de maintenance des comptes. Le script propose à la fois un mode interactif, adapté à l'usage quotidien des administrateurs, et un mode non interactif basé sur des paramètres, permettant son intégration dans des scénarios d'automatisation ou d'exploitation plus avancés.

Périmètre fonctionnel

Ce script permet à un administrateur d'exécuter, via une seule commande PowerShell, cinq actions distinctes sur les utilisateurs de l'Active Directory. Les fonctionnalités couvertes sont la création, la modification, la suppression, le listage des utilisateurs ainsi que la réinitialisation des mots de passe.

Deux modes d'exécution sont disponibles. La première repose sur l'utilisation de paramètres passés à la commande, permettant de déclencher directement l'action souhaitée dans un contexte non interactif ou automatisé. Le second s'appuie sur un menu interactif guidé, rendant l'outil accessible à tout administrateur sans connaissance préalable des paramètres internes du script.

Chaque action sensible est systématiquement associée à une confirmation explicite de l'utilisateur afin de limiter les erreurs de manipulation et de sécuriser les opérations effectuées sur l'Active Directory.



Architecture générale

Le script est structuré selon une logique modulaire inspirée des principes SOLID, avec une séparation claire des responsabilités. L'architecture repose sur deux catégories principales de fichiers : *Public* et *Private*. Les fichiers *Public* contiennent les points d'entrée exposés à l'utilisateur final, avec des fonctions nommées de manière cohérente avec les commandes PowerShell exécutées.

Le fichier principal agit comme orchestrateur. Il reçoit les instructions de l'utilisateur, qu'elles proviennent de paramètres ou du menu interactif (*cf figure 47*), puis redirige l'exécution vers la logique métier appropriée. Cette approche permet de centraliser le contrôle du flux tout en maintenant des fonctions métiers indépendantes et lisibles.

Afin d'assurer une expérience utilisateur homogène et de normaliser les traitements, le script s'appuie sur des fonctions utilitaires regroupées dans un répertoire *Utils*. Ce répertoire contient notamment les fonctions d'affichage et de navigation, comme le menu interactif, utilisées de manière transversale par l'ensemble du script. Cette organisation améliore la maintenabilité, la réutilisabilité du code et la clarté globale du projet.

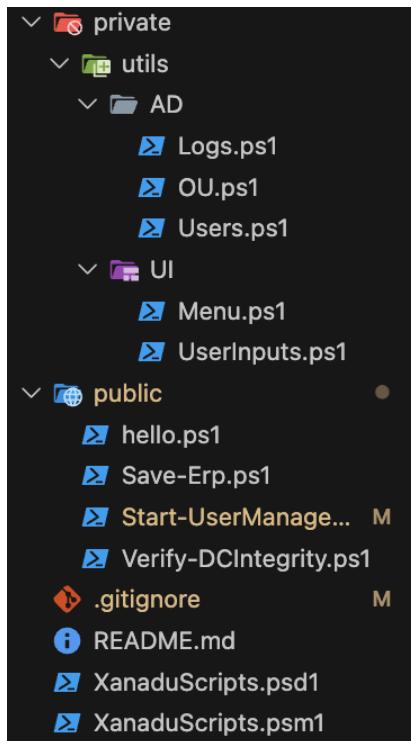


Figure 60 - Architecture des scripts



Je vais prendre pour exemple la fonction permettant d'afficher une liste de choix et retourner l'élément choisi. L'astuce ici est de stocker la première position du curseur pour pouvoir réafficher la ligne sélectionnée en vert avec ‘->’ pour pouvoir identifier le choix de l'utilisateur. Lorsque l'utilisateur appuie sur ‘Entrer’ on renvoie le choix à la fin de la fonction. Cela permet de créer une UI Simple afin de réduire le nombre d'erreur possible et d'harmoniser les processus.

```
# Mémorise la position de départ du menu pour pouvoir le réafficher proprement
$menuStartPos = $Host.UI.RawUICursorPosition

try {
    while ($true) {
        # Replace le curseur au début du menu pour réécrire les options à chaque itération
        $Host.UI.RawUICursorPosition = $menuStartPos
        for ($i = 0; $i -lt $options.Count; $i++) {
            # Met en surbrillance l'option sélectionnée, les autres restent en blanc
            $lineContent = if ($i -eq $selectedIndex) {
                " -> $($options[$i])"
                $color = 'DarkGreen'
            } else {
                "   $($options[$i])"
                $color = 'White'
            }
            Write-Host "$lineContent" -ForegroundColor $color
        }
        # Attend une touche clavier de l'utilisateur (sans affichage)
        $key = [Console]::ReadKey($true)

        switch ($key.Key) {
            'UpArrow' {
                # Déplace la sélection vers le haut (ou boucle à la fin)
                if ($selectedIndex -gt 0) { $selectedIndex-- }
                else { $selectedIndex = $options.Count - 1 }
            }
            'DownArrow' {
                # Déplace la sélection vers le bas (ou boucle au début)
                if ($selectedIndex -lt $options.Count - 1) { $selectedIndex++ }
                else { $selectedIndex = 0 }
            }
            'Enter' {
                # Valide le choix, replace le curseur après le menu et retourne l'option sélectionnée
                $endPos = [System.Management.Automation.Host.Coordinates]::new(0, $menuStartPos.Y + $options.Count)
                $Host.UI.RawUICursorPosition = $endPos
                Write-Host ""
                return $options[$selectedIndex]
            }
            # Annule la sélection, replace le curseur et retourne $null
            'Escape' {
                $endPos = [System.Management.Automation.Host.Coordinates]::new(0, $menuStartPos.Y + $options.Count)
                $Host.UI.RawUICursorPosition = $endPos
                Write-Host ""
                return $null
            }
            # Permet de quitter explicitement avec la touche "q"
            'q' {
                $endPos = [System.Management.Automation.Host.Coordinates]::new(0, $menuStartPos.Y + $options.Count)
                $Host.UI.RawUICursorPosition = $endPos
                Write-Host ""
                return 'Quitter'
            }
        }
    }
}
```

Figure 61 - Fonction Select-FromList



Fonctionnalités disponibles

L'utilisateur a le choix entre 4 arguments de fonction, *Create*, *Update*, *Delete*, *List*. Cet argument est facultatif et peut être couplé à des arguments de *Nom* ou *Prénom* permettant de fluidifier les processus pour les utilisateurs plus aguerris.

```
[CmdletBinding(DefaultParameterSetName="Encode")]
param(
    [ValidateSet("Create", "Update", "Delete", "List")]
    [string]$Action, # Action à effectuer (optionnel)

    [string]$Nom, # Nom de famille de l'utilisateur (optionnel)
    [string]$Prenom, # Prénom de l'utilisateur (optionnel)
    [string]$Group, # Groupe/OU pour l'utilisateur (optionnel)
    [string]$SamAccountName # SamAccountName de l'utilisateur (optionnel)
)

# Si une action est spécifiée, on l'exécute directement sans menu
if ($Action) {
    # Switch pour appeler la fonction appropriée selon l'action
    switch ($Action) {
        "Create" { Invoke-CreateUser -Nom $Nom -Prenom $Prenom -Group $Group }
        "Update" { Invoke-UpdateUser }
        "Delete" { Invoke-DeleteUser }
        "List"   { Invoke-ListUsers }
    }
    return
}

# Mode interactif avec menu principal
$continue = $true
while ($continue) {
    # Affiche le menu principal et récupère le choix de l'utilisateur
    $choice = Show-MainMenu

    # Exécute la fonction correspondant au choix
    switch ($choice) {
        "Créer un utilisateur"  { Invoke-CreateUser }
        "Modifier un utilisateur" { Invoke-UpdateUser }
        "Supprimer un utilisateur" { Invoke-DeleteUser }
        "Lister les utilisateurs" { Invoke-ListUsers }
        "Réinitialiser le mot de passe utilisateur" { Invoke-ResetUserPassword }
        "Quitter"               { $continue = $false }
        $null                   { $continue = $false }
    }
}

Write-Host "Au revoir !" -ForegroundColor Cyan
```

Figure 62 – Porte d'entrée du script

Création d'un utilisateur

Cette fonction a pour rôle de préparer et structurer l'ensemble des données nécessaires à la création d'un utilisateur dans l'Active Directory avant leur transmission aux commandes Microsoft dédiées. Elle accepte plusieurs paramètres facultatifs qui, lorsqu'ils ne sont pas fournis, sont demandés dynamiquement à l'administrateur via la fonction *Read-HostWithEscape*, ce qui facilite l'utilisation du script tout en permettant une annulation contrôlée.



```

param (
    [string]$Nom,           # Nom de famille de l'utilisateur à créer (optionnel)
    [string]$Prenom,        # Prénom de l'utilisateur à créer (optionnel)
    [string]$Group          # Groupe/OU fonctionnel pour l'utilisateur (optionnel)
)

# Si le nom n'est pas fourni, on le demande à l'utilisateur
if (-not $Nom) {
    $Nom = Read-HostWithEscape "Veuillez spécifier le nom (ESC pour annuler)"
    if (-not $Nom) {
        Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
        return
    }
}

# Si le prénom n'est pas fourni, on le demande à l'utilisateur
if (-not $Prenom) {
    $Prenom = Read-Host "Veuillez spécifier le prénom (ESC pour annuler)"
    if (-not $Prenom) {
        Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
        return
    }
}

# Si le groupe n'est pas valide, on demande à l'utilisateur de le sélectionner
if ($Group -notin $myGroups) {
    $Group = Select-OUGroup
    if (-not $Group -or $Group -eq "Quitter") {
        Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
        return
    }
}

```

Figure 63 - Fonction de création d'un utilisateur

Afin de limiter les erreurs de saisie et de garantir la cohérence organisationnelle, le choix du groupe ou de l'unité d'organisation est géré par la fonction `Select-OUGroup`. Celle-ci affiche une liste normalisée des groupes disponibles en s'appuyant sur le système de menu interactif commun au reste du script.

```

# Si aucun SearchBase n'est fourni, on utilise la racine des utilisateurs Xanadu
if (-not $SearchBase) {
    $DomainDN = (Get-ADDomain).DistinguishedName
    $SearchBase = "OU=Users,OU=Xanadu,$DomainDN"
}

# Récupère toutes les OU situées directement sous le SearchBase
$myGroups = Get-ADOrganizationalUnit -Filter * -SearchBase $SearchBase -SearchScope OneLevel |
# Extrait uniquement le nom de chaque OU
Select-Object -ExpandProperty Name |
# Trie les noms par ordre alphabétique
Sort-Object

# Retourne la liste des noms de groupes/OU
return $myGroups

```

Figure 64 - Récupération des OU

```

[CmdletBinding()]
param (
    [string]$SearchBase
)
# Récupère la liste des groupes/OU utilisateurs via la fonction dédiée

$myGroups = Get-UsersGroups

# Affiche un menu interactif pour sélectionner un groupe/OU
return Select-FromList -Title "Sélectionnez un groupe" -Options $myGroups

```

Figure 65 - Sélection d'un OU

Une fois les informations collectées et validées, les attributs de l'utilisateur sont normalisés, notamment pour la génération du `SamAccountName`, du nom d'affichage et de l'`UPN`. L'utilisateur est alors créé dans l'Active Directory via les commandes Microsoft appropriées, en respectant les conventions de nommage et l'arborescence définie.



```

# Génère le SamAccountName en concaténant prénom.nom en minuscules
$SamAccountName = "$($Prenom.ToLower()).$($Nom.ToLower())"
# Prépare le nom d'affichage complet
$DisplayName = "$Prenom $Nom"
# Construit l'UPN à partir du SamAccountName et du domaine AD courant
$UserPrincipalName = "$SamAccountName@$(Get-ADDomain).DNSRoot"
# Ajoute le groupe/OU logique en tête du chemin DN
$Path = "OU=$Group,$Path"

# Vérifie si un utilisateur avec ce SamAccountName existe déjà pour éviter les doublons
$existingUser = Get-ADUser -Filter { SamAccountName -eq $SamAccountName } -ErrorAction SilentlyContinue
if ($existingUser) {
    Write-Host "L'utilisateur '$SamAccountName' existe déjà dans Active Directory." -ForegroundColor Yellow
    return $null
}

# Récupère l'année courante pour générer le mot de passe initial
$year = Get-Date -Format "yyyy"

# Crée l'utilisateur AD avec tous les paramètres nécessaires et le mot de passe standardisé
try {
    # Write-Host New-ADUser
    $newUser = New-ADUser `n
        -Name $displayName `n
        -GivenName $Prenom `n
        -Surname $Nom `n
        -SamAccountName $SamAccountName `n
        -UserPrincipalName $UserPrincipalName `n
        -Path $Path `n
        -AccountPassword (ConvertTo-SecureString "Xanadu$year!" -AsPlainText -Force) `n
        -Enabled $true `n
        -ChangePasswordAtLogon $true
}

```

Figure 66 - Création de l'utilisateur

Modification d'un utilisateur

Comme pour la création d'un utilisateur, la fonction de modification accepte des paramètres facultatifs afin de faciliter l'exécution du script. Lorsque ces paramètres ne sont pas renseignés, l'administrateur peut saisir manuellement le nom et le prénom de l'utilisateur ciblé, permettant ainsi une utilisation flexible en mode Interactif.

```

# Si aucun utilisateur trouvé, propose une sélection manuelle
if (-not $user) {
    Write-Host "Aucun utilisateur trouvé." -ForegroundColor Yellow
    $user = Select-XanaduUser # Appelle une fonction pour sélectionner un utilisateur dans la liste
    if (-not $user) {
        Write-Host "Opération annulée." -ForegroundColor Yellow
        return # Arrête la fonction si aucun utilisateur n'est sélectionné
    }
}

# Si plusieurs utilisateurs correspondent, propose de choisir lequel
if ($user -is [array]) {
    Write-Host "Plusieurs utilisateurs trouvés :" -ForegroundColor Yellow
    $userNames = $user | ForEach-Object { "$_.Name" } # Liste les noms
    $selectedName = Select-FromList -Title "Sélectionnez l'utilisateur" -Options $userNames
    if (-not $selectedName) {
        Write-Host "Opération annulée." -ForegroundColor Yellow
        return
    }
    $selectedSam = ($selectedName -split '\(')[1].TrimEnd(')') # Extrait le SamAccountName choisi
    $user = $user | Where-Object { $_.SamAccountName -eq $selectedSam }
}

```

Figure 67 - Exceptions dans la modification d'un utilisateur

La principale difficulté de cette fonctionnalité réside dans la gestion des cas d'exception liés à la recherche de l'utilisateur dans l'Active Directory. Deux situations doivent être traitées : l'absence totale de correspondance avec les informations fournies, ou au contraire la présence de plusieurs utilisateurs correspondants. Dans ce second cas, le script réutilise le mécanisme de sélection dans une liste afin de permettre à l'administrateur de choisir explicitement l'utilisateur concerné, garantissant ainsi la précision de l'action.



Une fois l'utilisateur identifié, le script affiche ses informations principales et propose un menu de sélection des attributs modifiables. L'édition s'effectue au sein d'une boucle contrôlée, permettant de modifier plusieurs champs successivement sans avoir à relancer la fonction, jusqu'à ce que l'utilisateur décide de quitter le processus de modification.

Liste des utilisateurs

La fonction de listing des utilisateurs se distingue des autres fonctionnalités par l'absence totale de paramètres requis. Elle a pour unique objectif de fournir une vision globale et structurée des utilisateurs et des unités d'organisation du domaine Xanadu.

Le script s'appuie sur une fonction récursive qui parcourt l'ensemble de l'arborescence Active Directory à partir de l'OU racine des utilisateurs. Pour chaque unité d'organisation, la fonction récupère à la fois les sous-OU et les comptes utilisateurs associés, puis les affiche de manière hiérarchique.

L'affichage est volontairement orienté lisibilité. Des caractères ASCII sont utilisés pour représenter les branches de l'arbre, permettant à l'administrateur de visualiser clairement les relations entre les OU et les utilisateurs. Les couleurs et l'indentation renforcent cette lisibilité et offrent une représentation fidèle de la structure de l'Active Directory sans nécessiter d'action ou d'interaction supplémentaire.

```
# Définit les caractères Unicode pour dessiner l'arbre (lignes, branches)
$verticalLine = [char]0x2502 # |
$branchEnd   = [char]0x2514 # \
$branchTee   = [char]0x251C # |
$horizontal   = [char]0x2500 # - 

# Si aucun SearchBase n'est fourni, on part de la racine des utilisateurs Xanadu
if (-not $SearchBase) {
    $DomainDN = (Get-ADDomain).DistinguishedName
    $SearchBase = "OU=Users,OU=Xanadu,$DomainDN"

    Write-Host """
    Write-Host "USERS" -ForegroundColor Cyan
}

# Calcule le préfixe d'indentation pour l'affichage arborescent
$prefix = "" * ($Indent * 4)
for ($i = 0; $i -lt $Indent; $i++) {
    if ($IsLast) {
        $prefix += "      "
    } else {
        $prefix += " $verticalLine "
    }
}
```

Figure 68 - Affichage des OU et Users



Suppression d'un utilisateur

La fonction de suppression d'un utilisateur repose sur un processus volontairement simple et sécurisé. L'administrateur sélectionne l'utilisateur à supprimer via le mécanisme de choix interactif déjà utilisé dans les autres fonctionnalités du script, garantissant une identification explicite du compte ciblé.

Avant toute action, une confirmation claire est systématiquement demandée afin d'éviter toute suppression accidentelle, cette opération étant irréversible sans restauration depuis une sauvegarde Active Directory. En cas d'annulation ou de refus de confirmation, aucune modification n'est appliquée. Une fois validée, la suppression est effectuée via les commandes Microsoft dédiées à l'Active Directory.

```
# Appelle une fonction pour sélectionner l'utilisateur à supprimer
$user = Select-XanaduUser

# Si aucun utilisateur n'est sélectionné, on annule l'opération
if (-not $user) {
    Write-Host "Opération annulée." -ForegroundColor Yellow
    return
}

# Demande une confirmation explicite à l'administrateur avant suppression
$confirmation = Read-Host "Confirmez-vous la suppression de l'utilisateur '$($user.DisplayName)' ? (O/N)"
if ($confirmation -ine '0') {
    Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
    return
}

# Si confirmation reçue, supprime l'utilisateur de l'Active Directory
Remove-ADUser -Identity $user.SamAccountName
```

Figure 69 - Suppression d'un utilisateur

Réinitialisation du mot de passe

La réinitialisation du mot de passe repose sur un mécanisme similaire aux autres actions ciblant un utilisateur. L'administrateur sélectionne le compte concerné via la fonction de sélection des utilisateurs, qui parcourt récursivement les unités d'organisation et affiche les comptes disponibles jusqu'au choix final.

Une fois l'utilisateur identifié, le script génère un mot de passe temporaire selon une règle prédéfinie, applique ce nouveau mot de passe au compte Active Directory et force son changement lors de la prochaine ouverture de session. Cette approche permet de rétablir rapidement l'accès à un compte tout en respectant les bonnes pratiques de sécurité.



```

# Si l'utilisateur choisit de revenir en arrière, on remonte d'un niveau dans l'arborescence
if ($selection -eq ".. Retour" -or $selection -eq "Quitter") {
    if ($searchBase -eq $rootOU) {
        Write-Host "Annulation" -ForegroundColor Yellow
        return $null
    }
    $parentOU = ($searchBase -split ',', 2)[1]
    return Select-XanaduUser -SearchBase $parentOU
}

# Si une sous-OU est sélectionnée, on descend dans cette OU
if ($selection -match '^(\[OU\] (.+)$') {
    $selectedOUname = $matches[1]
    $newSearchBase = "$OU-$selectedOUname,$searchBase"
    return Select-XanaduUser -SearchBase $newSearchBase
}

# Si un utilisateur est sélectionné, on le récupère et on le retourne
if ($selection -match '^(\[User\] .+\((.+)\)\$') {
    $selectedSam = $matches[1]
    $selectedUser = Get-ADUser -Filter "SamAccountName -eq '$selectedSam'" -Properties * -ErrorAction SilentlyContinue

    if ($selectedUser) {
        Write-Host "l'Utilisateur sélectionné : $($selectedUser.DisplayName)" -ForegroundColor Green
        return $selectedUser
    } else {
        Write-Host "Erreur: Utilisateur non trouvé." -ForegroundColor Red
        return $null
    }
}

```

Figure 70 - Fonction récursive de sélection d'un utilisateur de l'AD

Limites et évolutions

Le script répond aux besoins principaux de gestion des comptes, mais certaines fonctionnalités restent simples ou incomplètes. Par exemple la génération du mot de passe temporaire suit une règle fixe, ce qui reste fonctionnel mais peu adaptable à des politiques de sécurité plus strictes ou à des exigences de complexité variables selon l'entreprise.

Des évolutions naturelles consisteraient à ajouter un système de journalisation (logs) détaillant chaque action (création, modification, suppression, reset) avec horodatage et identité de l'administrateur, afin d'améliorer l'audibilité.

Il serait aussi pertinent d'intégrer des contrôles plus avancés avant exécution, comme la vérification de l'existence du compte avant création, la validation stricte des formats (email, conventions de nommage) ou la détection explicite des collisions de SamAccountName. On pourrait ajouter une sécurité d'exécution via le blocage de certaines fonctionnalités si l'utilisateur ne dispose pas des autorisations nécessaires.

Enfin, le script pourrait être renforcé en ajoutant une gestion de configuration centralisée (fichier JSON/YAML), permettant de définir facilement les OU cibles, les groupes disponibles, et les règles de mot de passe sans modifier le code.



Sauvegarde de l'AD et DC

Contexte

Ce script a pour objectif de contrôler l'intégrité d'un contrôleur de domaine Windows en s'appuyant sur l'outil Microsoft DCDiag. Il exécute un ensemble de tests ciblés sur la santé du DC et de l'annuaire Active Directory, puis transforme la sortie brute de DCDiag en un résumé exploitable en console.

L'objectif est double : fournir un diagnostic lisible immédiatement (tests réussis/échoués et détails des erreurs) et assurer une traçabilité côté système en journalisant les anomalies dans le journal Application de Windows via une source dédiée (XanaduScripts). Le script peut lancer uniquement des tests orientés DC, uniquement des tests orientés AD, ou l'ensemble des tests, afin d'adapter le contrôle au besoin.

Périmètre fonctionnel

Ce script permet de vérifier l'état de santé d'un contrôleur de domaine en exécutant des tests DCDiag ciblés et en analysant automatiquement leurs résultats. Il contrôle en amont que l'exécution a bien lieu sur un Domain Controller afin d'éviter toute utilisation inappropriée.

Selon le mode sélectionné, le script peut lancer des tests orientés contrôleur de domaine, des tests orientés annuaire Active Directory ou l'ensemble des tests disponibles. Les résultats sont ensuite structurés pour distinguer clairement les tests réussis et ceux en échec, avec un affichage synthétique en console.

En complément de l'affichage, les erreurs détectées ainsi qu'un résumé global de l'exécution sont journalisés dans le journal d'événements Windows. Cette fonctionnalité permet une exploitation ultérieure des diagnostics, notamment dans un contexte de supervision ou d'audit système.

Déroulé logique du script

La première étape consiste à préparer la journalisation Windows via la fonction Initialize-EventLogSource. Cette étape vérifie l'existence de la source XanaduScripts dans le journal Application afin d'éviter une erreur lors de l'écriture d'événements. Si la création de la source échoue, par exemple pour des problèmes de droits, la journalisation est désactivée et le script continue.



```

try {
    # Vérifie si la source Event Log existe déjà, sinon la crée
    if (-not [System.Diagnostics.EventLog]::SourceExists($source)) {
        [System.Diagnostics.EventLog]::CreateEventSource($source, $logName)
        Write-Host "Source '$source' créée dans le journal '$logName'." -ForegroundColor Green
        # Petite pause pour s'assurer que la source est bien enregistrée
        Start-Sleep -Seconds 2
    }
}

```

Figure 71 - Initialize-EventLogSource

Ensute, le script vérifie que la machine exécutant le script est bien un Domain Controller via la fonction interne `Test-IsDomainController`. Si ce n'est pas le cas, l'exécution s'arrête immédiatement, car les diagnostics DCDiag ciblent spécifiquement un contrôleur de domaine.

```

function Test-IsDomainController {
    $OS = if ($PSVersionTable.PSVersion.Major -lt 5) {
        Get-WmiObject -Class Win32_OperatingSystem
    }
    else {
        Get-CimInstance -ClassName Win32_OperatingSystem
    }

    # ProductType = 2 signifie Domain Controller
    if ($OS.ProductType -eq "2") {
        return $true
    }
}

```

Figure 72 - Test-IsDC



```

# Définit les listes de tests selon le mode choisi
$ADTests = @(
    "Replications",          # RéPLICATION AD
    "ObjectsReplicated",     # Objets répliqués
    "NCSecDesc",             # Permissions partitions AD
    "KnowsOfRoleHolders",    # Rôles FSMO
    "VerifyReferences",      # Intégrité références AD
    "CrossRefValidation",    # Cross-references
    "CheckSDRefDom",         # Security Descriptors
    "MachineAccount",        # Compte machine AD
    "RidManager",            # Pool RID
    "Intersite",              # RéPLICATION inter-sites
    "KccEvent"                # Topologie réPLICATION
)
$DCTests = @(
    "Connectivity",           # Connectivité réseau
    "Advertising",            # Annonces DNS
    "Services",               # Services Windows
    "NetLogons",              # Service Netlogon
    "SysVolCheck",             # Partage SYSVOL
    "FrsEvent",                 # RéPLICATION SYSVOL (FRS)
    "DFSREvent",                # RéPLICATION SYSVOL (DFS-R)
    "SystemLog",                  # Erreurs système
    "LocatorCheck"             # Localisation DC
)

# Sélectionne les tests à exécuter selon le mode
$DCDiagTestsToRun = switch ($Mode) {
    "DC" { $DCTests }
    "AD" { $ADTests }
    "All" { $DCTests + $ADTests }
}

```

Figure 73 - liste des tests réalisés sur le DC

La fonction Get-DCDiagResults construit ensuite la liste des tests à exécuter selon le mode sélectionné (DC, AD ou All), puis lance DCDiag test par test. Pour chaque test, la sortie est redirigée vers un fichier temporaire (%TEMP%\dc-diag-<Test>.txt) afin de faciliter l'analyse et la récupération des résultats.

```

$DCDiag = Start-Process -FilePath "DCDiag.exe" -ArgumentList "/test:$DCTest", "/f:$outputFile" -PassThru
-Wait -NoNewWindow

# Si le test échoue (code retour non nul), affiche une erreur et passe au suivant
if ($DCDiag.ExitCode -ne 0) {
    Write-Host "[Error] Running $DCTest!" -ForegroundColor Red
    continue
}

# Récupère le contenu du fichier de sortie (en brut et en lignes)
$RawContent = Get-Content -Path $outputFile -Raw -ErrorAction SilentlyContinue
$RawLines = Get-Content -Path $outputFile -ErrorAction SilentlyContinue | Where-Object { $.Trim() }

```

Figure 74 - exécution des diagnostics du DC

Si DCDiag renvoie un code de sortie non nul, le test est ignoré et le script passe au suivant, évitant ainsi un arrêt global.



```

# Ajoute le résultat structuré au tableau
$results += [PSCustomObject]@{
    Test    = $DCTest
    Status  = $Status
    Result  = $RawLines
}

```

Figure 75 - Résultat test-DC

Enfin, Verify-DCIntegrity récupère l'ensemble des résultats sous forme d'objets (nom du test, statut, détail), puis sépare les tests réussis et ceux en échec. Le script affiche un résumé lisible (nombre de tests réussis/échoués et liste associée). En cas d'échec, il affiche également le détail complet de la sortie DCDiag pour chaque test concerné, ce qui évite d'avoir à ouvrir manuellement les fichiers temporaires.

Limites et évolutions

Le script repose sur l'analyse textuelle de la sortie de DCDiag pour déterminer si un test est réussi ou échoué. Cette approche fonctionne dans les cas courants, mais reste dépendante du format exact des messages, de la langue du système et des variations possibles selon les versions de Windows.

La collecte des résultats passe par des fichiers temporaires par test ce qui est simple à maintenir et à relire, mais laisse des fichiers sur le poste et ajoute des accès disque évitables. Une évolution consisterait à capturer directement la sortie standard de DCDiag en mémoire, tout en conservant la possibilité d'exporter dans un fichier si nécessaire.

La journalisation est un point fort, mais elle peut être renforcée. Il serait pertinent de conditionner explicitement l'écriture dans l'Event Log à la réussite de l'initialisation de la source, d'enrichir les événements (nom du serveur, horodatage, mode, tests échoués) et d'ajouter un export complémentaire (CSV/JSON) pour intégration dans une supervision ou un outil de reporting.

Enfin, le script pourrait évoluer vers une exécution plus “exploitable” en production avec un code de retour standardisé (0 si tout est OK, 1 si échecs), des seuils configurables (ex : tolérer certains tests), et une configuration externalisée (liste de tests, chemins, EventId) pour éviter de modifier le code lors des changements d'environnement.



Sauvegarde et vérification de l'ERP

Contexte

Dans un cadre de POC (Proof of Concept) nous avons modélisé un ERP permettant de simuler un logiciel de gestion accessible depuis internet pour les agents en télétravail. Ce logiciel est modélisé selon une application web Angular couplé à un API en Go. Pour stocker les informations nous avons utilisé une BDD Sqlite. Ce choix nous a permis de simuler la sauvegarde via la recopie d'un simple fichier dans le NAS.

Pour cela il a fallu créer une connexion ssh sécurisée entre notre IIS contenant l'ERP et la base de données et notre NAS. En effet, notre IIS étant en DMZ, donc accessible via internet, nous avons dû créer et sécuriser ce tunnel unique entre réseau interne et internet.

Périmètre fonctionnel

Ce script permet d'assurer la sauvegarde de la base de données SQLite utilisée par XanaduERP vers un espace de stockage distant situé sur un NAS. Il automatisé la copie du fichier de base de données en ajoutant un horodatage au nom du fichier afin de conserver un historique des sauvegardes.

Le script intègre également un mécanisme de rotation des sauvegardes en supprimant automatiquement les fichiers datant de plus de 30 jours, ce qui permet de limiter l'espace disque utilisé sur le NAS. En complément, il offre une fonction de vérification permettant d'afficher les informations de la dernière sauvegarde disponible, notamment son emplacement, sa taille et sa date de création.

L'exécution du script peut être adaptée selon le besoin grâce à un paramètre de mode, permettant soit de réaliser uniquement la sauvegarde, soit uniquement la vérification, soit d'enchaîner les deux opérations.

Déroulé logique du script

La première étape du script consiste à charger une configuration centralisée dans un objet \$config permettant une réutilisabilité tout au long du script. On y définit le chemin de la base SQLite locale, la clé SSH utilisée, l'utilisateur de service du NAS, l'hôte, le port, le répertoire distant de stockage ainsi que des paramètres de fonctionnement comme la durée de conservation (KeepDays) et le timeout SSH. Cette approche évite les valeurs "en dur" éparpillées et rend le script plus maintenable.



```

$config = @{
    # Chemins locaux
    DbPath      = "C:\inetpub\wwwroot\XanaudERPBack\cmd\xanadu.db"
    KeyPath     = "$env:USERPROFILE\.ssh\id_ed25519"

    # Configuration NAS
    NasUser     = "svc_backup_iis"
    NasHost     = "192.168.1.98"
    NasPort     = 22
    NasDir      = "/mnt/pool_xanadu/backups/iis/backups_sqlite"

    # Paramètres de sauvegarde
    KeepDays   = 30
    Timeout    = 10
    Compression = $true
}

```

Figure 76 - Informations de connexion au NAS

Ensuite, lorsque le mode inclut une sauvegarde, la fonction Save-Database commence par exécuter des contrôles de prérequis via Test-Prerequisites pour valider l'existence de la base, l'accessible de la clé SSH est et que la connexion distante est possible avant de lancer une copie réseau, afin d'éviter une sauvegarde partielle ou silencieusement invalide.

```

Write-Info "Vérification des prérequis..."
Write-Info $config.DbPath

# Vérifier commandes
$requiredCommands = @("ssh", "scp")
foreach ($cmd in $requiredCommands) {
    if (-not (Get-Command $cmd -ErrorAction SilentlyContinue)) {
        throw "Commande manquante: $cmd. Installez OpenSSH Client."
    }
}

# 1) Pré-checks : la sauvegarde ne se lance que si tout est OK
Test-Ssh $config
Check-RemoteDir $config

# Vérifier fichiers locaux
if (-not (Test-Path -LiteralPath $config.DbPath)) {
    throw "Base SQLite introuvable: $($config.DbPath)"
}

if (-not (Test-Path -LiteralPath $config.KeyPath)) {
    throw "Clé SSH privée introuvable: $($config.KeyPath)"
}

# Vérifier permissions clé SSH (sécurité)
$keyAcl = Get-Acl $config.KeyPath
Write-Verbose "Clé SSH trouvée avec permissions appropriées"

Write-Ok "Prérequis validés" -Level Success

```

Figure 77 - test prérequis connexion au NAS



Une fois validés, le script génère un nom de sauvegarde horodaté (xanadu_YYYY-MM-dd_HH-mm.db) dans le répertoire NAS permettant de conserver un historique lisible et triable des sauvegardes sans dépendre d'un outil externe. Le transfert est ensuite réalisé via scp en utilisant la clé privée et le port configuré. Le code de retour est contrôlé : si scp échoue, le script lève une erreur explicite avec le détail de la sortie.

```
$scpTarget = "${config.NasUser}@${config.NasHost}:$remoteFile"
$scpOut = & scp -i $config.KeyPath -P $config.NasPort -v -- "${config.DbPath}" "$scpTarget" 2>&1
$code = $LASTEXITCODE

if ($code -ne 0) {
    throw "SCP KO (code=$code). Détails: $scpOut"
}

Write-Ok "Sauvegarde envoyée"

# 4) Rotation : suppression des sauvegardes trop anciennes sur le NAS
Write-Info "Rotation: suppression des sauvegardes de plus de ${config.KeepDays} jours..."

# Normalisation
$keepDays = [int]$config.KeepDays
$nasDir = $config.NasDir
$target = "{0}@{1}" -f $config.NasUser, $config.NasHost

# Construction commande distante
$rotateCmd = "find '$nasDir' -maxdepth 1 -type f -name 'xanadu_*.db' -mtime +$keepDays -print -delete; echo OK"

# Exécution SSH
$r = & ssh ` 
    -i $config.KeyPath ` 
    -p $config.NasPort ` 
    -o BatchMode=yes ` 
    -o ConnectTimeout=${config.Timeout} ` 
    $target ` 
    $rotateCmd 2>&1
```

Figure 78 - Écriture BDD dans le NAS

Après une sauvegarde réussie, le script applique une rotation côté NAS. Il construit une commande distante find exécutée via SSH, qui supprime les sauvegardes plus anciennes que KeepDays. La réussite est validée à la fois par le code de retour SSH et par la présence d'un marqueur (OK) dans la sortie, ce qui évite de considérer comme "OK" une commande distante tronquée ou incomplète.

Enfin, lorsque le mode inclut la vérification, Verify-LastBackup contrôle d'abord la disponibilité SSH (Test-Ssh) et l'existence du répertoire distant (Check-RemoteDir). Le script cherche ensuite la sauvegarde la plus récente via un listing trié (ls -t ... | head -n 1). Si aucune sauvegarde n'est trouvée, il affiche un message clair et s'arrête proprement (cas normal lors du premier lancement). Si une sauvegarde existe, il récupère ses métadonnées via stat (chemin, taille, date) et les affiche, ce qui permet de prouver rapidement qu'une sauvegarde récente est bien présente sur le NAS.

```
$cmd = "ls -t ${config.NasDir}/xanadu_*.db 2>/dev/null | head -n 1"
$last = & ssh -i $config.KeyPath -P $config.NasPort -o BatchMode=yes "${config.NasUser}@${config.NasHost}" $cmd 2>&1

# Si aucune sauvegarde n'existe encore, on ne crash pas : on affiche un message clair.
if ($LASTEXITCODE -ne 0 -or [string]::IsNullOrEmpty($last)) {
    Write-Warn "Aucune sauvegarde trouvée dans ${config.NasDir} (normal si premier lancement)."
    return
}

$last = $last.Trim()

# Affiche les métadonnées (nom, taille, date) pour prouver que la sauvegarde existe.
$cmd2 = "stat -c '%n%|y' '$last'"
$meta = & ssh -i $config.KeyPath -P $config.NasPort -o BatchMode=yes "${config.NasUser}@${config.NasHost}" $cmd2 2>&1
if ($LASTEXITCODE -ne 0) {
    throw "Impossible de lire les métadonnées: $meta"
}

$parts = $meta.Trim() -split "\\|"
Write-Ok "Dernière sauvegarde: ${parts[0]}"
Write-Ok "Taille: ${parts[1]} octets"
Write-Ok "Date : ${parts[2]}"
```

Figure 79 - vérification des BDD dans le NAS



Limites et évolutions

Le script repose sur l'utilisation de commandes externes (scp, ssh, find, stat) exécutées via le système, ce qui implique la présence et la bonne configuration de ces outils sur le serveur hébergeant l'ERP. Toute modification de l'environnement (chemins, version OpenSSH, politiques de sécurité) peut impacter le bon fonctionnement sans modification directe du script.

La sauvegarde consiste en une copie brute du fichier SQLite. Cette approche est adaptée dans un contexte de POC, mais ne prend pas en compte des problématiques plus avancées comme la cohérence applicative en cas d'écriture concurrente, le chiffrement des sauvegardes ou la compression côté NAS. De plus, la gestion des erreurs repose principalement sur les codes de retour des commandes distantes, sans mécanisme de reprise automatique.

Des évolutions possibles incluraient l'ajout d'un chiffrement des sauvegardes, une compression optionnelle réellement exploitée, une journalisation centralisée (Event Log ou fichier de logs), ainsi qu'un retour de code standardisé pour intégration dans une tâche planifiée ou un outil de supervision. L'externalisation complète de la configuration dans un fichier dédié permettrait également d'adapter le script à différents environnements sans modification du code.

Conclusion générale

Ces scripts s'inscrivent dans une logique cohérente d'administration et de sécurisation d'un système d'information. Le 1^{er} script permet une gestion centralisée et sécurisée des comptes Active Directory, en réduisant les erreurs de manipulation grâce à des contrôles systématiques et une interface accessible. Le 2^{ème} apporte un outil de diagnostic fiable pour le contrôle de l'intégrité des contrôleurs de domaine, en transformant les résultats bruts de DCDiag en informations exploitables et traçables. Le 3^{ème} automatise la sauvegarde d'une base applicative dans un contexte exposé, en s'appuyant sur des transferts sécurisés et une politique de rétention maîtrisée.

Le choix de PowerShell est cohérent avec le contexte Active Directory et réseau du projet permettant de gérer la lecture et l'écriture dans l'AD, la vérification de l'état du système et la communication avec des ressources distantes. Dans ce cadre, PowerShell s'impose comme un langage adapté et pertinent pour ce type d'automatisations.

Ils illustrent une approche pragmatique orientée exploitation, avec des choix techniques adaptés à un contexte réel tout en restant suffisamment modulaires pour évoluer vers des usages plus avancés en environnement de production.



Questionnaire de Sécurité

En sécurité informatique il est important de vérifier la sécurité de 4 aspects principaux du S.I. : la sécurité physique des équipements, la sécurité logicielle contre les attaques, la formation des collaborateurs et le suivi des échanges et des comportements sur le réseau.

Pour permettre à la société de s'auto évaluer sur le sujet de la sécurité, nous proposons à Xanadu un questionnaire comprenant des questions sur plusieurs aspects de la sécurité. A l'aide de ce questionnaire, l'entreprise pourra s'évaluer sur la majorité des aspects de la sécurité de leur S.I. et ainsi s'améliorer en continue.

Les différents thèmes abordés sont les suivants : la politique de sécurité interne à l'entreprise, la formation des utilisateurs, la sécurisation des postes (accès non autorisés et malwares), la sécurisation du réseau et de ses équipements, la sécurisation des données et la surveillance régulière des flux.

Afin de former au mieux les collaborateurs de l'entreprise, nous fournissons également une affiche, plus simple qu'une charte qui peut ne pas être comprise par le personnel non technique, expliquant les 4 principales bonnes habitudes informatique pouvant protéger le système en cas d'attaque. On y retrouve la création de mots de passe fort, la méfiance sur des fichiers reçus d'inconnus, la mise à jour régulière des applications du bureau et la sauvegarde régulière de ses documents dans les dossiers de l'entreprise donc la sauvegarde automatique est réalisée selon le plan de sauvegarde sécurisé fournis par CesiTech.

(retrouvez l'affiche en annexe)

Politique de sécurité

Une charte de sécurité est une bonne solution pour mettre en place les bases de la sécurité auprès des collaborateurs.

- Une charte de sécurité a-t-elle été distribuée à tous les collaborateurs ?

Remédiation : Mettre en place une charte de sécurité officielle à l'entreprise, la diffuser régulièrement à l'ensemble des employés (penser à la distribuer aux nouveaux employés).



- La charte de sécurité précise-t-elle : que les comptes ne peuvent être partagés, que le mot de passe doit être changé tous les 3 à 6 mois ou que seul une liste d'applications autorisée par l'administration ne peut être utilisées?

Remédiation : Mettre à jour la charte pour inclure les règles de mots de passe, l'interdiction des comptes partagés et la liste des logiciels autorisés, cela représente les enjeux majeurs de la sécurité des postes.

Formation des utilisateurs

La formation des utilisateurs du réseau est un des éléments les plus importants dans la sécurisation d'un réseau.

- Les utilisateurs sont-ils formés à ne pas ouvrir de pièces jointes ou liens provenant d'expéditeurs inconnus ?

Remédiation : Mettre en place une formation annuelle anti-phishing et organiser des tests réguliers de sensibilisation (ex: mails de phishing interne).

- Les utilisateurs ont-ils connaissances des notions de "mot de passe fort" ?

Remédiation : Fournir une formation simple sur les bonnes pratiques de gestion des mots de passe et imposer des règles techniques via GPO.

Sécurisation des accès

La sécurisation des accès aux postes des collaborateurs doit être correctement appréhendée.

- Les comptes de chaque utilisateur sont-ils protégés par un mot de passe répondant aux normes de sécurité ?

Remédiation : Mettre en place une politique de blocage si un mot de passe initialisé est non conforme à la norme de l'entreprise. (10 caractères minimum, 1 chiffre, 1 majuscule, 1 caractère spécial).



Sécurisation des postes utilisateurs

Les postes des utilisateurs représentent des failles, il faut savoir les protéger.

- Un antivirus est-il mis en place sur les postes de tous les utilisateurs ?

Remédiation : Déployer un antivirus centralisé sur tous les postes et activer les alertes en temps réel. Utiliser les GPO pour bloquer des accès à des types de téléchargements.

- Les utilisateurs mettent-ils régulièrement leurs logiciels et systèmes d'exploitation à jour ?

Remédiation : Les utilisateurs doivent activer les mises à jour automatiques des logiciels. Un mail automatique peut être programmé pour prévenir les utilisateurs d'une nouvelle version disponible pour un logiciel pour leur permettre de vérifier.

Sécurisation des réseaux

Le réseau doit être sécurisé pour filtrer les flux entrants et sortants et dans le réseau en lui-même.

- Un pare-feu existe-t-il pour filtrer le trafic ?

Remédiation : Installer et configurer un pare-feu professionnel avec des règles restrictives et un filtrage. Ils peuvent être ajoutés sous un format physique ou virtualisé sur le routeur.

- Le routeur inclut-il une DMZ ?

Remédiation : Identifier les services accessibles depuis l'extérieur de l'entreprise (clients ou accès web). Une DMZ peut alors être mise en place pour isoler ces services et les isoler du reste du réseau en cas d'attaque malveillante.

- Des VLAN sont-ils en place pour séparer les différents espaces du réseau ?



Remédiation : Segmenter le réseau en VLAN pour limiter la propagation d'un incident. Le pare feu peut également analyser les échanges entre les VLANs.

Sécurisation des équipements

La DMZ représente un excellent rempart entre le SI interne et l'extérieur.

- Une DMZ est-elle en place sur le réseau pour isoler des accès non autorisés ?

Remédiation : Identifier les services accessibles depuis l'extérieur de l'entreprise (clients ou accès web). Une DMZ peut alors être mise en place pour isoler ces services et les isoler du reste du réseau en cas d'attaque malveillante.

Sécurisation des sauvegardes

Les sauvegardes mettent en sécurité les données à un instant T.

- Un plan de sauvegarde est-il mis en place ?

Remédiation : Un plan de sauvegarde peut être mis en place en prenant en compte la RTO et la RPO garantissant une sécurité optimale des données en cas d'attaque.

- Le plan de sauvegarde répond-il aux attentes 3-2-1 ?

Remédiation : Le plan de sauvegarde doit prendre en compte une sauvegarde internet (NAS) une sauvegarde externe (NAS externe ou disque dur) et une sauvegarde Cloud.

- Le plan de sauvegarde prend il en compte une sauvegarde immuable ?

Remédiation : Une sauvegarde immuable peut être mise en place sur le cloud pour conserver les données en lecture seule et bloquer toutes tentatives de corruption.



Sécurisation contre les malwares et ransomwares

Les malwares sont le pire ennemi des entreprises, il est donc important de s'en protéger.

- Un VPN est-il utilisé pour les connexions à distance ?

Remédiation : L'utilisation d'un VPN sécurisé (avec authentification forte) permet de protéger les connexions distantes contre les interceptions et les attaques visant à compromettre le réseau interne.

- Les logiciels antivirus sont-ils configurés pour bloquer les comportements suspects(chiffrement) ?

Remédiation : Les antivirus modernes doivent être configurés pour détecter le chiffrement massif de fichiers, les accès anormaux et les comportements typiques des ransomwares afin de bloquer l'attaque avant propagation.

Sécurisation en cas d'attaque

La sauvegarde régulière des données peut considérablement réduire le temps de remise en route en cas d'attaque.

- Les données sauvegardées ont une durée de sauvegarde de plus de 7jours ?

Remédiation : Une rétention de sauvegarde d'au moins 7 jours permet de disposer de points de restauration multiples en cas de compromission progressive des données.

- Le RTO maximale est inférieure à 24h ?

Remédiation : Un RTO inférieur à 24h garantit une reprise d'activité rapide et limite les pertes opérationnelles liées à l'interruption du service.

Journalisation et surveillance des logs

Une surveillance du réseau est indispensable pour réagir rapidement en cas d'attaque.



- Une surveillance est-elle mise en place sur le réseau ?

Remédiation : La mise en place d'une supervision du réseau permet de détecter rapidement les anomalies, les intrusions et les comportements atypiques permettant une réaction rapide.

- Les logs sont-ils accessibles sur les flux dans le réseau ?

Remédiation : Les journaux doivent être centralisés et accessibles de manière sécurisée pour permettre l'analyse rapide des événements et faciliter les investigations.

Questionnaire de sécurité	Remédiation
Politique de sécurité	Une charte de sécurité est une bonne solution pour mettre en place les bases de la sécurité auprès des collaborateurs
Une charte de sécurité a-t-elle été distribuée à tous les collaborateurs ?	Mettre en place une charte de sécurité officielle à l'entreprise, la diffuser régulièrement à l'ensemble des employés (pensé à la distribuer aux nouveaux employés).
La charte de sécurité précise elle : que les comptes ne peuvent être partagés, que le mot de passe doit être changé tous les 3 à 6 mois ou que seul une liste d'applications autorisée par l'administration ne peuvent être utilisées?	Mettre à jour la charte pour inclure les règles de mots de passe, l'interdiction des comptes partagés et la liste des logiciels autorisés, cela représente les enjeux majeurs de la sécurité des postes.
Formation des utilisateurs	La formation des utilisateurs du réseau est un des éléments les plus importants dans la sécurisation d'un réseau.
Les utilisateurs sont-ils formés à ne pas ouvrir de pièces jointes ou liens provenant d'expéditeurs inconnus ?	Mettre en place une formation annuelle anti-phishing et organiser des tests réguliers de sensibilisation (ex: mails de phishing interne).
Les utilisateurs ont-ils connaissances des notions de "mot de passe fort" ?	Fournir une formation simple sur les bonnes pratiques de gestion des mots de passe et imposer des règles techniques via GPO.
Sécurisation des accès	La sécurisation des accès aux postes des collaborateurs doit être correctement appréhendée.
Les comptes de chaque utilisateur sont-ils protégés par un mot de passe répondant aux normes de sécurité ?	Mettre en place une politique de blocage si un mot de passe initialisé est non conforme à la norme de l'entreprise. (10 caractères minimum, 1 chiffre, 1 majuscule, 1 caractère spécial).
Sécurisation des postes utilisateurs	Les Postes des utilisateurs représentent des failles, il faut savoir les protéger.
Un antivirus est-il mis en place sur les postes de tous les utilisateurs ?	Déployer un antivirus centralisé sur tous les postes et activer les alertes en temps réel. Utiliser les GPO pour bloquer des accès à des types de téléchargements.
Les utilisateurs mettent-ils régulièrement leurs logiciels et systèmes d'exploitation à jour ?	Les utilisateurs doivent activer les mises à jour automatiques des logiciels. Un mail automatique peut être programmé pour prévenir les utilisateurs d'une nouvelle version disponible pour un logiciel pour leur permettre de vérifier.
Sécurisation des réseaux	Le réseau doit être sécurisé pour filtrer les flux entrants et sortants et dans le réseau en lui-même.
Un pare-feu existe-t-il pour filtrer le trafic ?	Installer et configurer un pare-feu professionnel avec des règles restrictives et un filtrage. Ils peuvent être ajoutés sous un format physique ou virtualisé sur le routeur.
Le routeur inclus t'il une DMZ ?	Identifier les services accessibles depuis l'extérieur de l'entreprise (clients ou accès web). Une DMZ peut alors être mise en place pour isoler ces services et les isoler du reste du réseau en cas d'attaque malveillante.
Des VLAN sont-ils en place pour séparer les différents espaces du réseau ?	Segmenter le réseau en VLAN pour limiter la propagation d'un incident. Le pare feu peut également analyser les échanges entre les VLAN.
Sécurisation des équipements	La DMZ représente un excellent rempart entre le SI interne et l'extérieur.
Une DMZ est-elle en place sur le réseau pour isoler des accès non autorisés ?	Mettre en place une DMZ sur un VLAN correctement isolé.
Sécurisation des sauvegardes	Les sauvegardes mettent en sécurité les données à un instant T.
Un plan de sauvegarde est-il mis en place ?	Un plan de sauvegarde peut être mis en place et prennent en compte la RTO et la RPO garantissant une sécurité optimale des données en cas d'attaque.
Le plan de sauvegarde répond-il aux attentes 3-2-1 ?	Le plan de sauvegarde doit prendre en compte une sauvegarde internet (NAS), une sauvegarde externe (NAS externe ou disque dur) et une sauvegarde Cloud.
Le plan de sauvegarde prend-il en compte une sauvegarde immuable ?	Une sauvegarde immuable peut être mise en place sur le cloud pour conserver les données en lecture seule et bloquer toutes tentatives de corruption.
Sécurisation contre les malwares et ransomwares	Les malwares sont le pire ennemi des entreprises, il est donc important de s'en protéger.
Un VPN est-il utilisé pour les connexions à distance ?	L'utilisation d'un VPN sécurisé (avec authentification forte) permet de protéger les connexions distantes contre les interceptions et les attaques visant à compromettre le réseau interne.
Les logiciels antivirus sont-ils configurés pour bloquer les comportements suspects (chiffrement) ?	Les antivirus modernes doivent être configurés pour détecter le chiffrement massif de fichiers, les accès anormaux et les comportements typiques des ransomwares afin de bloquer l'attaque avant propagation.
Sécurisation en cas d'attaque	La sauvegarde régulière des données peut considérablement réduire le temps de remise en route en cas d'attaque.
Les données sauvegardées ont une durée de sauvegarde de plus de 7 jours ?	Une rétention de sauvegarde d'au moins 7 jours permet de disposer de points de restauration multiples en cas de compromission progressive des données.
Le RTO maximale est inférieure à 24h ?	Un RTO inférieur à 24h garantit une reprise d'activité rapide et limite les pertes opérationnelles liées à l'interruption du service.
Journalisation et surveillance des logs	Une surveillance du réseau est indispensable pour réagir rapidement en cas d'attaque.
Une surveillance est-elle mise en place sur le réseau ?	La mise en place d'une supervision du réseau permet de détecter rapidement les anomalies, les intrusions et les comportements atypiques permettant une réaction rapide.
Les logs sont-ils accessibles sur les flux dans le réseau ?	Les journaux doivent être centralisés et accessibles de manière sécurisée pour permettre l'analyse rapide des événements et faciliter les investigations.

Figure 80 - Questionnaire de Sécurité récapitulatif proposé par CESITech



Conclusion

L'architecture mise en place répond aux exigences de sécurité, de disponibilité et de performance. La segmentation du réseau en VLAN isole efficacement les services, tandis que PfSense assure le routage et le filtrage centralisé des flux. La liaison MPLS entre Atlantis et Springfield garantit une connectivité privée conforme au SLA opérateur, et le VPN OpenVPN permet un accès distant sécurisé pour les collaborateurs itinérants.

L'Active Directory structure l'organisation avec des GPO automatisant la configuration et renforçant la sécurité. Le NAS centralisé offre un stockage sécurisé avec gestion fine des droits via ACL. Le plan de sauvegarde respecte la stratégie 3-2-1 recommandée par l'ANSSI, avec classification des données par criticité et objectifs RTO atteints (4h pour les services critiques, 24h pour les autres). La DMZ et le certificat SSL sécurisent l'accès web à l'ERP.

Les scripts PowerShell développés automatisent les tâches d'administration, tandis que la supervision Zabbix détecte rapidement les anomalies. Le questionnaire de sécurité et l'affiche de bonnes pratiques complètent le dispositif technique par une sensibilisation des utilisateurs.

Conformité et perspectives

L'infrastructure déployée répond à l'ensemble des attentes du client : stabilité, fiabilité, sécurité et facilité d'administration. La maquette Proxmox a validé la faisabilité technique des solutions proposées malgré les contraintes de l'environnement.

À moyen terme, une montée en capacité du stockage sera nécessaire, ainsi qu'un enrichissement de la supervision et le déploiement progressif d'une authentification multi facteur.

Nous avons donc réussi à concevoir et préparer le déploiement d'une infrastructure moderne et sécurisée, parfaitement adaptée aux besoins de XANADU. Le projet est prêt pour une phase de déploiement en production, avec l'assurance que les objectifs de sécurité, de disponibilité et de facilité d'administration seront atteints.



Glossaire

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



S.I. (Système d'Information) : Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

RH(Ressources Humaines) : Services de Xanadu.

BE (Bureau d'Etude) : Services de Xanadu.

IIS (Internet Information Server) : Un serveur Web (HTTP).

ACL (Access Control List) : Une liste des adresses et ports autorisés ou interdits par un pare-feu.



Annexes

Annexe 1- L'affiche de bonnes pratiques informatique

XANADU

4 Bonnes pratiques qui peuvent sauver notre cyberquotidien !

Un mot de passe sécurisé c'est :

- 10 caractères minimum
- 1 chiffre minimum
- 1 caractère spécial




Un fichier inconnu reçu ?

On ne télécharge pas de fichier dont on ne connaît pas la provenance.



Une mise à jour disponible ?

Si une mise à jour est disponible, il est important de la faire rapidement.



Des données importantes ?

Une sauvegarde régulière dans son dossier personnel peut sauver vos données.



Plus d'informations sur les bonnes pratiques sur
www.xanadu.com



Annexe 2 - Choix du paramètre à modifier 1

```
while ($continue) {
    # Affiche le menu de choix d'attribut à modifier
    $attributeChoice = Select-FromList -Title "Sélectionnez l'attribut à modifier" -Options $attributesToUpdate
    switch ($attributeChoice) {
        "Nom" {
            Write-Host "`nMise à jour du nom de $($user.Surname)" -ForegroundColor Cyan
            $newNom = Read-HostWithEscape -Prompt "Nouveau nom (Esc pour annuler)"
            if (-not $newNom) {
                Write-Host "Modification annulée." -ForegroundColor Yellow
            } else {
                Update-UserName -Nom $newNom -Prenom $user.GivenName -SamAccountName $user.SamAccountName
            }
        }
        "Prénom" {
            Write-Host "`nMise à jour du prénom de $($user.Surname)" -ForegroundColor Cyan
            $newPrenom = Read-HostWithEscape -Prompt "Nouveau prénom (Esc pour annuler)"
            if (-not $newPrenom) {
                Write-Host "Modification annulée." -ForegroundColor Yellow
            } else {
                Update-UserName -Nom $user.Surname -Prenom $newPrenom -SamAccountName $user.SamAccountName
            }
        }
        "Email" {
            Write-Host "`nMise à jour de l'email de $($user.EmailAddress)" -ForegroundColor Cyan
            $newEmail = Read-HostWithEscape -Prompt "Nouvel email (Esc pour annuler)"
            if (-not $newEmail) {
                Write-Host "Modification annulée." -ForegroundColor Yellow
            } else {
                try {
                    Set-ADUser -Identity $user.SamAccountName -EmailAddress $newEmail -ErrorAction Stop
                    Write-Host "Email mis à jour avec succès en '$newEmail'." -ForegroundColor Green
                } catch {
                    Write-Host "Erreur lors de la mise à jour de l'email : $_" -ForegroundColor Red
                }
            }
        }
        "Groupe" {
            Write-Host "`nMise à jour du groupe de $($user.SamAccountName)" -ForegroundColor Cyan
            $newGroup = Select-OUGroup
            if (-not $newGroup) {
                Write-Host "Modification annulée." -ForegroundColor Yellow
            } else {
                try {
                    $currentOU = $($user.DistinguishedName -split ',')[1..($user.DistinguishedName.Length)] -join ','
                    $newOU = "OU=$newGroup,$currentOU"
                    Write-Host "Old OU: $currentOU, New OU: $newOU" -ForegroundColor Yellow
                    # Move-ADObject -Identity $user.DistinguishedName -TargetPath $newOU
                    # Write-Host "Groupe mis à jour avec succès en '$newGroup'." -ForegroundColor Green
                } catch {
                    Write-Host "Erreur lors de la mise à jour du groupe : $_" -ForegroundColor Red
                }
            }
        }
        "Activer/Désactiver le compte" {
            $newState = -not $user.Enabled
            try {
                Set-ADUser -Identity $user.SamAccountName -Enabled $newState -ErrorAction Stop
                $stateText = if ($newState) { "activé" } else { "désactivé" }
                Write-Host "Le compte utilisateur a été $stateText avec succès." -ForegroundColor Green
            } catch {
                Write-Host "Erreur lors de la mise à jour de l'état du compte : $_" -ForegroundColor Red
            }
        }
        "Quitter" {
            $continue = $false # Sort de la boucle et termine la fonction
        }
    }
}
```



Annexe 3 – Mise en place des GPO

Résultats de stratégie de groupe																																		
XANADU\emma.carena sur XANADU\ATLPC003																																		
Données recueillies le : 17/12/2025 15:55:35																																		
afficher tout																																		
masquer																																		
Résumé																																		
<p>Au cours des précédentes stratégies d'ordinateur actualisées le 17/12/2025 14:20:22</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15px; vertical-align: top;">●</td> <td>Aucune erreur détectée</td> </tr> <tr> <td style="width: 15px; vertical-align: top;">! ●</td> <td>Une liaison rapide a été détectée Plus d'informations...</td> </tr> <tr> <td style="width: 15px; vertical-align: top;">! ●</td> <td>Les objets de stratégie de groupe suivants ont des alertes spéciales</td> </tr> <tr> <td style="width: 15px;"></td> <td>Nom d'objet de stratégie de groupe Alerte</td> </tr> <tr> <td></td> <td>Activer Découverte Réseau Appliquée</td> </tr> </table>					●	Aucune erreur détectée	! ●	Une liaison rapide a été détectée Plus d'informations...	! ●	Les objets de stratégie de groupe suivants ont des alertes spéciales		Nom d'objet de stratégie de groupe Alerte		Activer Découverte Réseau Appliquée																				
●	Aucune erreur détectée																																	
! ●	Une liaison rapide a été détectée Plus d'informations...																																	
! ●	Les objets de stratégie de groupe suivants ont des alertes spéciales																																	
	Nom d'objet de stratégie de groupe Alerte																																	
	Activer Découverte Réseau Appliquée																																	
<p>Au cours des précédentes stratégies d'utilisateur actualisées le 17/12/2025 14:20:47</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15px; vertical-align: top;">●</td> <td>Aucune erreur détectée</td> </tr> <tr> <td style="width: 15px; vertical-align: top;">! ●</td> <td>Une liaison rapide a été détectée Plus d'informations...</td> </tr> <tr> <td style="width: 15px; vertical-align: top;">! ●</td> <td>Les objets de stratégie de groupe suivants ont des alertes spéciales</td> </tr> <tr> <td style="width: 15px;"></td> <td>Nom d'objet de stratégie de groupe Alerte</td> </tr> <tr> <td></td> <td>Activer Découverte Réseau Appliquée</td> </tr> <tr> <td></td> <td>Xanadu Home-Bureau Appliquée</td> </tr> </table>					●	Aucune erreur détectée	! ●	Une liaison rapide a été détectée Plus d'informations...	! ●	Les objets de stratégie de groupe suivants ont des alertes spéciales		Nom d'objet de stratégie de groupe Alerte		Activer Découverte Réseau Appliquée		Xanadu Home-Bureau Appliquée																		
●	Aucune erreur détectée																																	
! ●	Une liaison rapide a été détectée Plus d'informations...																																	
! ●	Les objets de stratégie de groupe suivants ont des alertes spéciales																																	
	Nom d'objet de stratégie de groupe Alerte																																	
	Activer Découverte Réseau Appliquée																																	
	Xanadu Home-Bureau Appliquée																																	
Détails de l'ordinateur																																		
masquer																																		
Général																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Nom de l'ordinateur</td> <td>XANADU\ATLPC003</td> </tr> <tr> <td>Domaine</td> <td>xanadu.com</td> </tr> <tr> <td>Site</td> <td>Default-First-Site-Name</td> </tr> <tr> <td>Unité d'organisation</td> <td>xanadu.com\XANADU\Computers\Atlantis</td> </tr> <tr> <td>Adhésion au groupe de sécurité</td> <td>afficher</td> </tr> </table>					Nom de l'ordinateur	XANADU\ATLPC003	Domaine	xanadu.com	Site	Default-First-Site-Name	Unité d'organisation	xanadu.com\XANADU\Computers\Atlantis	Adhésion au groupe de sécurité	afficher																				
Nom de l'ordinateur	XANADU\ATLPC003																																	
Domaine	xanadu.com																																	
Site	Default-First-Site-Name																																	
Unité d'organisation	xanadu.com\XANADU\Computers\Atlantis																																	
Adhésion au groupe de sécurité	afficher																																	
masquer																																		
État du composant																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Nom de composant</th> <th>Statut</th> <th>Heure photo</th> <th>Heure du dernier processus</th> <th>Journal des événements</th> </tr> </thead> <tbody> <tr> <td>Infrastructure de stratégie de groupe</td> <td>Opération réussie</td> <td>2 seconde(s) 850 milliseconde(s)</td> <td>17/12/2025 14:20:22</td> <td>Afficher le journal</td> </tr> <tr> <td>Group Policy Local Users and Groups</td> <td>Opération réussie</td> <td>1 seconde(s) 672 milliseconde(s)</td> <td>17/12/2025 14:20:21</td> <td>Afficher le journal</td> </tr> <tr> <td>Group Policy Services</td> <td>Opération réussie</td> <td>766 milliseconde(s)</td> <td>17/12/2025 14:20:22</td> <td>Afficher le journal</td> </tr> <tr> <td>Registre</td> <td>Opération réussie</td> <td>2 seconde(s) 438 milliseconde(s)</td> <td>16/12/2025 11:45:31</td> <td>Afficher le journal</td> </tr> <tr> <td>Security</td> <td>Opération réussie</td> <td>1 seconde(s) 46 milliseconde(s)</td> <td>16/12/2025 11:45:33</td> <td>Afficher le journal</td> </tr> </tbody> </table>					Nom de composant	Statut	Heure photo	Heure du dernier processus	Journal des événements	Infrastructure de stratégie de groupe	Opération réussie	2 seconde(s) 850 milliseconde(s)	17/12/2025 14:20:22	Afficher le journal	Group Policy Local Users and Groups	Opération réussie	1 seconde(s) 672 milliseconde(s)	17/12/2025 14:20:21	Afficher le journal	Group Policy Services	Opération réussie	766 milliseconde(s)	17/12/2025 14:20:22	Afficher le journal	Registre	Opération réussie	2 seconde(s) 438 milliseconde(s)	16/12/2025 11:45:31	Afficher le journal	Security	Opération réussie	1 seconde(s) 46 milliseconde(s)	16/12/2025 11:45:33	Afficher le journal
Nom de composant	Statut	Heure photo	Heure du dernier processus	Journal des événements																														
Infrastructure de stratégie de groupe	Opération réussie	2 seconde(s) 850 milliseconde(s)	17/12/2025 14:20:22	Afficher le journal																														
Group Policy Local Users and Groups	Opération réussie	1 seconde(s) 672 milliseconde(s)	17/12/2025 14:20:21	Afficher le journal																														
Group Policy Services	Opération réussie	766 milliseconde(s)	17/12/2025 14:20:22	Afficher le journal																														
Registre	Opération réussie	2 seconde(s) 438 milliseconde(s)	16/12/2025 11:45:31	Afficher le journal																														
Security	Opération réussie	1 seconde(s) 46 milliseconde(s)	16/12/2025 11:45:33	Afficher le journal																														
masquer																																		
Paramètres																																		
Stratégies																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Paramètres Windows</td> <td>masquer</td> </tr> <tr> <td>Paramètres de sécurité</td> <td>afficher</td> </tr> <tr> <td>Modèles d'administration</td> <td>afficher</td> </tr> </table>					Paramètres Windows	masquer	Paramètres de sécurité	afficher	Modèles d'administration	afficher																								
Paramètres Windows	masquer																																	
Paramètres de sécurité	afficher																																	
Modèles d'administration	afficher																																	
masquer																																		
Préférences																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Paramètres du Panneau de configuration</td> <td>masquer</td> </tr> <tr> <td>Utilisateurs et groupes locaux</td> <td>afficher</td> </tr> <tr> <td>Services</td> <td>afficher</td> </tr> </table>					Paramètres du Panneau de configuration	masquer	Utilisateurs et groupes locaux	afficher	Services	afficher																								
Paramètres du Panneau de configuration	masquer																																	
Utilisateurs et groupes locaux	afficher																																	
Services	afficher																																	
masquer																																		
Objets de stratégie de groupe																																		
Objets GPO appliqués																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Activer Découverte Réseau [[B0CB85B1-223F-40DB-8E68-81A0FB346485]]</td> <td>masquer</td> </tr> <tr> <td>Default Domain Policy [[1B12F340-016D-11D2-945F-00C04FB984F9]]</td> <td>afficher</td> </tr> <tr> <td>Droits Administrateurs locaux [[D1F126BF-73B2-4C35-B094-AD81733C09BE]]</td> <td>afficher</td> </tr> <tr> <td>Stratégie d'antivirus [[F1C1321B-A0D8-41ED-84BF-1DBFFFAC4A9F]]</td> <td>afficher</td> </tr> <tr> <td>Stratégie de certificat [[F4A1BF20-AD36-4A56-A45A-42D6B3A122A0]]</td> <td>afficher</td> </tr> <tr> <td>Stratégie de Restriction d'Application [[6A1ACBA2-2A30-4E63-ABC0-251ED268E4E0]]</td> <td>afficher</td> </tr> <tr> <td>Stratégie de sécurité de mot de passe [[33D1FE69-55D6-4CE0-BE03-01C42F6095BA]]</td> <td>afficher</td> </tr> </table>					Activer Découverte Réseau [[B0CB85B1-223F-40DB-8E68-81A0FB346485]]	masquer	Default Domain Policy [[1B12F340-016D-11D2-945F-00C04FB984F9]]	afficher	Droits Administrateurs locaux [[D1F126BF-73B2-4C35-B094-AD81733C09BE]]	afficher	Stratégie d'antivirus [[F1C1321B-A0D8-41ED-84BF-1DBFFFAC4A9F]]	afficher	Stratégie de certificat [[F4A1BF20-AD36-4A56-A45A-42D6B3A122A0]]	afficher	Stratégie de Restriction d'Application [[6A1ACBA2-2A30-4E63-ABC0-251ED268E4E0]]	afficher	Stratégie de sécurité de mot de passe [[33D1FE69-55D6-4CE0-BE03-01C42F6095BA]]	afficher																
Activer Découverte Réseau [[B0CB85B1-223F-40DB-8E68-81A0FB346485]]	masquer																																	
Default Domain Policy [[1B12F340-016D-11D2-945F-00C04FB984F9]]	afficher																																	
Droits Administrateurs locaux [[D1F126BF-73B2-4C35-B094-AD81733C09BE]]	afficher																																	
Stratégie d'antivirus [[F1C1321B-A0D8-41ED-84BF-1DBFFFAC4A9F]]	afficher																																	
Stratégie de certificat [[F4A1BF20-AD36-4A56-A45A-42D6B3A122A0]]	afficher																																	
Stratégie de Restriction d'Application [[6A1ACBA2-2A30-4E63-ABC0-251ED268E4E0]]	afficher																																	
Stratégie de sécurité de mot de passe [[33D1FE69-55D6-4CE0-BE03-01C42F6095BA]]	afficher																																	
masquer																																		
Objets GPO refusés																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Stratégie de groupe locale [LocalGPO]</td> <td>masquer</td> </tr> </table>					Stratégie de groupe locale [LocalGPO]	masquer																												
Stratégie de groupe locale [LocalGPO]	masquer																																	
afficher																																		
Filtres WMI																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Nom</th> <th>Valeur</th> <th>Référence (GPO)</th> </tr> </thead> <tbody> <tr> <td>Aucun(e)</td> <td></td> <td></td> </tr> </tbody> </table>					Nom	Valeur	Référence (GPO)	Aucun(e)																										
Nom	Valeur	Référence (GPO)																																
Aucun(e)																																		
masquer																																		
Détails de l'utilisateur																																		
Général																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Nom d'utilisateur</td> <td>XANADU\emma.carena</td> </tr> <tr> <td>Domaine</td> <td>xanadu.com</td> </tr> <tr> <td>Unité d'organisation</td> <td>xanadu.com\XANADU\Users\OU_BureauEtude</td> </tr> <tr> <td>Adhésion au groupe de sécurité</td> <td>afficher</td> </tr> </table>					Nom d'utilisateur	XANADU\emma.carena	Domaine	xanadu.com	Unité d'organisation	xanadu.com\XANADU\Users\OU_BureauEtude	Adhésion au groupe de sécurité	afficher																						
Nom d'utilisateur	XANADU\emma.carena																																	
Domaine	xanadu.com																																	
Unité d'organisation	xanadu.com\XANADU\Users\OU_BureauEtude																																	
Adhésion au groupe de sécurité	afficher																																	
masquer																																		
État du composant																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Nom de composant</th> <th>Statut</th> <th>Heure photo</th> <th>Heure du dernier processus</th> <th>Journal des événements</th> </tr> </thead> <tbody> <tr> <td>Infrastructure de stratégie de groupe</td> <td>Opération réussie</td> <td>1 seconde(s) 170 milliseconde(s)</td> <td>17/12/2025 14:20:47</td> <td>Afficher le journal</td> </tr> <tr> <td>Group Policy Drive Maps</td> <td>Opération réussie</td> <td>5 seconde(s) 78 millisecondes</td> <td>17/12/2025 12:24:38</td> <td>Afficher le journal</td> </tr> <tr> <td>Group Policy Shortcuts</td> <td>Opération réussie</td> <td></td> <td>12/12/2025 15:50:26</td> <td></td> </tr> </tbody> </table>					Nom de composant	Statut	Heure photo	Heure du dernier processus	Journal des événements	Infrastructure de stratégie de groupe	Opération réussie	1 seconde(s) 170 milliseconde(s)	17/12/2025 14:20:47	Afficher le journal	Group Policy Drive Maps	Opération réussie	5 seconde(s) 78 millisecondes	17/12/2025 12:24:38	Afficher le journal	Group Policy Shortcuts	Opération réussie		12/12/2025 15:50:26											
Nom de composant	Statut	Heure photo	Heure du dernier processus	Journal des événements																														
Infrastructure de stratégie de groupe	Opération réussie	1 seconde(s) 170 milliseconde(s)	17/12/2025 14:20:47	Afficher le journal																														
Group Policy Drive Maps	Opération réussie	5 seconde(s) 78 millisecondes	17/12/2025 12:24:38	Afficher le journal																														
Group Policy Shortcuts	Opération réussie		12/12/2025 15:50:26																															
masquer																																		
Paramètres																																		
Préférences																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Paramètres Windows</td> <td>masquer</td> </tr> <tr> <td>Mappages de lecteurs</td> <td>afficher</td> </tr> <tr> <td>Raccourcis</td> <td>afficher</td> </tr> </table>					Paramètres Windows	masquer	Mappages de lecteurs	afficher	Raccourcis	afficher																								
Paramètres Windows	masquer																																	
Mappages de lecteurs	afficher																																	
Raccourcis	afficher																																	
masquer																																		
Objets de stratégie de groupe																																		
Objets GPO appliqués																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Activer Découverte Réseau [[B0CB85B1-223F-40DB-8E68-81A0FB346485]]</td> <td>masquer</td> </tr> <tr> <td>Xanadu Home-Bureau [[F9784113-00EA-40A2-82D0-B890C9C2E812]]</td> <td>afficher</td> </tr> </table>					Activer Découverte Réseau [[B0CB85B1-223F-40DB-8E68-81A0FB346485]]	masquer	Xanadu Home-Bureau [[F9784113-00EA-40A2-82D0-B890C9C2E812]]	afficher																										
Activer Découverte Réseau [[B0CB85B1-223F-40DB-8E68-81A0FB346485]]	masquer																																	
Xanadu Home-Bureau [[F9784113-00EA-40A2-82D0-B890C9C2E812]]	afficher																																	
masquer																																		
Objets GPO refusés																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20px; vertical-align: top;">Stratégie de groupe locale [LocalGPO]</td> <td>masquer</td> </tr> </table>					Stratégie de groupe locale [LocalGPO]	masquer																												
Stratégie de groupe locale [LocalGPO]	masquer																																	
afficher																																		
Filtres WMI																																		
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Nom</th> <th>Valeur</th> <th>Référence (GPO)</th> </tr> </thead> <tbody> <tr> <td>Aucun(e)</td> <td></td> <td></td> </tr> </tbody> </table>					Nom	Valeur	Référence (GPO)	Aucun(e)																										
Nom	Valeur	Référence (GPO)																																
Aucun(e)																																		
masquer																																		

