Bloc 2 - Livrable 1

# Projet Administration et Sécurisation d'un système d'information

Lisa ACHOUR, Maéva CHALLIES, Enzo CADIÈRE, Rayane OULDALI, Alejandro BAGLIVO CRISTALDO

Année 2025-2026

# 1) Sommaire

Table des figures

# 2) Équipe

- Lisa ACHOUR : **Secrétaire**
- Maéva CHALLIES : **Animatrice** / **Scribe**
- Enzo CADIÈRE : **Animateur**
- Rayane OULDALI : **Groupe**
- Alejandro BAGLIVO CRISTALDO : **Gestionnaire du temps**

# 3) Rappel du contexte et objectifs

L'entreprise XANADU change de locaux. Ils souhaitent en profiter pour faire évoluer et sécuriser leur système informatique afin d'éviter un éventuel blocage de longue durée en cas d'incident, tel que produit dans une autre entreprise.

Ainsi, l'entreprise possèdera deux sites : Le premier se situera dans la métropole d'Atlantis et le second dans la ville de Springfield.

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

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

➔ Rajouter la notion d'appel d'offre

# 4) Contraintes

- Le site distant de Springfield raccordé au site principal via une liaison MPLS fourni par l'opérateur télécom, assurant une connectivité privée et une qualité de service garantie (SLA).
- L'ERP de l'entreprise restera le même
- Garantir la continuité d'activité, la reprise après incident, ainsi que la traçabilité des événements.
- En cas d'incident, retour à la normale requis sous 4 heures pour les services critiques, et 24 heures pour les autres.
- XANADU est une société de 50 collaborateurs sur le site de la technopole, plus 10 sur le site distant (Springfield).

- XANADU comprend plusieurs services :
    - Service Comptabilité et Gestion financière
    - Service commercial
    - Bureau d'étude
    - Service Juridique
    - Service des ressources humaines
    - Un Laboratoire sur un site distant
    - Direction de l'agence
- Chaque employé doit pouvoir se connecter à distance, soit en tant qu'itinérant, soit en télétravail.
- Partages de dossier :
    - 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.
- Un correspondant informatique par service devra pouvoir :
    - Créer ou modifier les comptes utilisateurs de son service ;
    - Gérer les droits d'accès ;
    - Intégrer de nouveaux postes de travail au domaine
- 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.
- Springfield hébergera :
    - 10 utilisateurs d'un laboratoire de recherche
    - 10 postes clients sur ce site distant

- 2 serveurs physiques sous Linux pour piloter des équipements et récupérer des données.
- 1 copieur
- 1 imprimante métier

Tout sera connecté au réseau local.

- Le bureau d'étude doit avoir accès aux données du laboratoire.
- XANADU utilise son propre domaine Active Directory, mais le déploiement du site distant pourra se faire différemment. L'architecture Active Directory fait partie de l'étude.

# 5) Mots inconnus

## a) Relatif au sujet

| | |
|---|---|
| Liaison VPN MPLS (Multiprotocol Label Switching) | Connexion à réseau privée. |
| Rançonlogiciel | Un logiciel malveillant qui prend en otage des données personnelles. |
| Vulnérabilité | Une faiblesse ou une faille dans un système, logiciel, réseau ou processus permettant à un attaquant de compromettre la sécurité (confidentialité, intégrité ou disponibilité) et d'exploiter le système. |
| Système d'information | Un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. |
| Domaine Active Directory | Ensemble logique d'objets (utilisateurs, ordinateurs, UO, etc.) géré par une même équipe administrative, généralement sur le même réseau physique, organisé en arbres et forêts avec un schéma commun. |
| ERP (Enterprise Resource Planning) | Type de logiciel que les entreprises utilisent pour gérer leurs activités quotidiennes telles que la comptabilité, les achats, la gestion de projets, la gestion des risques et la conformité, ainsi que les opérations de supply chain. |
| Serveur DNS (Domain Name System) | Un service informatique distribué qui associe les noms de domaine Internet avec leurs adresses IP. |
| Serveur DHCP (Dynamic Host Configuration Protocol) | Un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station ou d'une machine, notamment en lui attribuant automatiquement une adresse IP et un masque de sous-réseau. |
| NAS | Serveur de fichiers autonome, relié à un réseau, dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes. |
| Routeur | Un équipement réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers leur destination. |

| | |
|---|---|
| Un serveur physique ESXi | Un hyperviseur de type 1 (bare-metal), conçu pour transformer un serveur physique en plusieurs machines virtuelles indépendantes. |
| HTTP (Hypertext Transfer Protocol) | Un protocole de communication client-serveur développé pour le World Wide Web. |
| Serveur DC (contrôleur domaine) | Un contrôleur de domaine est un serveur qui répond aux demandes d'authentification de sécurité dans un domaine Windows Server. |

## b) Relatif au projet

| | |
|---|---|
| Bridge Linux (pont réseau) | Un bridge Linux (ou pont réseau Linux) est un composant du noyau qui permet de relier plusieurs interfaces réseau comme si elles étaient connectées à un switch Ethernet. |
| VLANs (Virtual Local Area Networks) | Réseaux locaux virtuels permettant de segmenter logiquement un réseau physique en domaines de diffusion isolés, indépendamment de la topologie physique. |
| Pare-feu (Firewall) | Dispositif de sécurité qui filtre le trafic réseau selon des règles prédéfinies (IP, ports, protocoles) pour bloquer les accès non autorisés entre différentes zones de confiance. |
| IPS (Intrusion Prevention System) | Système de prévention d'intrusions qui détecte et bloque automatiquement en temps réel les activités malveillantes sur le réseau. |
| Filtrage de niveau 7 | Inspection approfondie du trafic au niveau applicatif (couche 7 OSI) permettant un contrôle granulaire basé sur le contenu des données (URL, types de fichiers, comportements applicatifs). |
| Red Hat | Éditeur de solutions open source d'infrastructure, notamment Red Hat Enterprise Linux (RHEL), offrant support commercial et certifications pour environnements professionnels. |
| Sauvegarde immuable | Méthode de stockage où les copies de données sont verrouillées, inaltérables et impossibles à modifier ou supprimer, même par un administrateur, afin de garantir l'intégrité et la disponibilité des données face aux incidents, attaques (notamment ransomware) et exigences réglementaires. |
| ADDS (Active Directory Domain Service) | Permet de déployer un annuaire AD (Base de données AD : NTDS.dit) pour stocker et gérer de manière centralisée tous les objets réseaux et sécurité : ordinateurs, utilisateurs, imprimantes. |
| DNS (Domain Name System) | Système qui traduit les noms de domaine lisibles par l'homme en adresses IP lisibles par les machines |
| Windows Server | Système d'exploitation pour serveur de Microsoft, conçu pour exécuter et sécuriser des applications, services et charges de travail sur des environnements locaux, hybrides et cloud, et destiné à gérer des réseaux, du stockage et des services d'entreprise. |
| Niveau fonctionnel | Niveaux de support (N1, N2, N3) qui classent les compétences et les interventions selon la complexité des incidents et les domaines d'expertise. |

| | |
|---|---|
| Active directory | La mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows. |
| Souveraineté des données | Degré de contrôle et de conformité aux lois du pays où les données sont collectées ou traitées, incluant leur gestion, stockage, traitement et utilisation, afin de protéger la vie privée, la sécurité et l'intégrité des données. |
| LDAP | |
| Rôles FSMO | Les rôles FSMO (Flexible Single Master Operations) sont 5 rôles critiques dans Active Directory, chacun détenu par un seul contrôleur de domaine à la fois : |

# 6) Analyse de l'existant

De ce que nous savons de l'architecture de XANADU cette dernière se décompose de la façon suivante.

L'ERP repose sur une architecture en trois parties. Une base de données en PostgreSQL. Un serveur d'application contient les objet métier, le moteur de workflow. Pour finir XANADU dispose d'un serveur de présentation. De cette façon les utilisateurs peuvent se connecter via leur navigateur web.

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

**Infrastructure**

Pour le volume des données, XANADU respecte une nomenclature précise. Les données bureautiques occupent 800 Go. Les dossiers personnels ont une limite de 5 Go. La base de données de l'ERP fait quant à elle fait 10 Go.

En termes d'infrastructure nous savons que l'entreprise possède un serveur physique qui agit en tant que serveur DNS et serveur DHCP. L'Os est un Windows Server 2019.

Elle dispose également d'un NAS d'une capacité de 2 To. Celle-ci dispose d'une solution NAT. Un serveur physique, un copieur ainsi qu'une imprimante connecter aux réseaux.

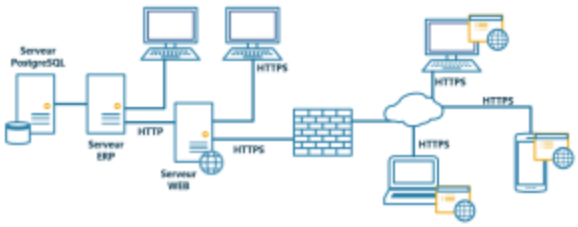


*Figure 1: schéma réseau actuel*

**Gestion des données**

Chaque utilisateur possède ses propres dossiers sur son PC pour 5 Go maximum par utilisateur. Tous les utilisateurs possèdent les droits administrateurs. L'ensemble des utilisateurs effectue leurs propres sauvegardes avec une clé USB. L'ERP est basé du de l'HTTP. Les utilisateurs itinérants copient sur leurs messageries Office, les documents importants avant de partir. Certains documents sont partagés sur leur Microsoft drive. A cause de cela certains documents ne sont pas toujours à jour cela créer un vrai problème ce qui fait que notre intervention est nécessaire. De plus les utilisateurs en télétravail n'ont pas accès à l'ERP.

**Sauvegardes**

XANADU possède sa propre politique de sauvegardes. A chaque fin de semaine un technicien connecte un disque externe au serveur DC. L'ensemble du serveur NAS y est copié. Deux disques sont utilisés en alternance pour les sauvegardes.

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

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

**Antivirus**

Le contrôleur de domaine est protégé par l'antivirus Microsoft, configuré avec les paramètres par défaut. Sur plusieurs postes utilisateurs, une version gratuite d'un antivirus est installée. Le paramétrage repose sur les réglages proposés par défaut et dépend des choix de chaque utilisateur, lesquels disposent des droits administrateurs sur leur machine.

**Mises à jour**

Les mises à jour sont appliquées selon la configuration par défaut, sans supervision centralisée. Les prestataires intervenant sur le système effectuent ponctuellement certaines mises à jour lors de leurs visites, notamment à l'occasion des opérations de maintenance liées à l'ERP.

# 7) Analyse du besoin

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

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

### *1. Infrastructure*

L'infrastructure actuelle repose sur un serveur physique unique sans redondance, créant un point de défaillance critique.

Besoins : Virtualiser l'infrastructure pour séparer les rôles critiques (DNS, DHCP, fichiers, ERP) sur des VM distinctes. Ajouter un second serveur pour assurer la haute disponibilité. Déployer une solution de monitoring pour superviser l'état des systèmes et documenter l'architecture réseau complète.

### *2. Gestion des données*

Les données sont dispersées sur les postes individuels avec des droits administrateurs généralisés, causant des problèmes de versioning et empêchant l'accès distant à l'ERP.

Besoins : Centraliser le stockage sur un serveur de fichiers avec gestion des permissions par profils. Déployer une solution de partage collaboratif avec gestion de versions. Supprimer les droits administrateurs et mettre en place un accès distant sécurisé via VPN pour le télétravail.

### *3. Sauvegardes*

Les sauvegardes manuelles hebdomadaires sur deux disques locaux, sans externalisation ni tests de restauration, exposent l'entreprise à une perte de données majeure.

Besoins : Automatiser les sauvegardes régulières avec une solution professionnelle. Appliquer la stratégie 3-2-1-1-0 avec au moins une copie externalisée et protégée contre les ransomwares. Planifier des tests de restauration trimestriels et mettre en place des alertes automatiques en cas d'échec.

### *4. Antivirus*

La protection hétérogène sans supervision centralisée permet aux utilisateurs de désactiver leur antivirus, laissant le système vulnérable.

Besoins : Déployer une solution EDR/XDR centralisée sur tout le parc avec console d'administration unique. Configurer des mises à jour automatiques, des fonctionnalités anti-ransomware et restreindre les droits pour empêcher toute désactivation.

### *5. Mises à jour*

L'absence de gestion centralisée des mises à jour expose l'infrastructure à des failles de sécurité et des déploiements non maîtrisés.

Besoins : Implémenter un serveur WSUS pour centraliser et planifier les mises à jour. Établir une politique de déploiement progressif avec groupe de test, prioriser les correctifs critiques et étendre la gestion aux applications tierces et à l'ERP.

# 8) Problématique

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

# 9) Plan d'action

## Déploiement du nouveau système informatique

| ID | Partie | Tâche | Dépendances | Durée estimée (en jours) |
|---|---|---|---|---|
| **1** | CONCEPTION | Élaboration du schéma réseau | | 0.5j |
| **2** | CONCEPTION | Élaboration de la logique AD | | 0.5j |
| **3** | CONCEPTION | Élaboration de la stratégie de sauvegarde | | 1j |
| **4** | RÉSEAU | Mise en œuvre du routeur MPLS | | 1j |

| | | | | |
|---|---|---|---|---|
| **5** | RÉSEAU | Installation du pare-feu Atlantis 1 | Tâche 4 | 1j |
| **6** | RÉSEAU | Installation du pare-feu Springfield 1 | Tâche 4 | 1j |
| **7** | INFRA | Installation de DC2 | Tâche 5 et 6 | 0.5j |
| **8** | INFRA | Installation de DC1 | Tâche 5 et 6 | 0.5j |
| **9** | INFRA | Installation du NAS (FS-01) | | 0.5j |
| **10** | INFRA | Mise en place du monitoring (Prometheus + CheckMK) | Tâche 5 et 6 | 1j |
| **11** | INFRA | Configuration de WSUS | Tâche 7 | 1j |
| **12** | INFRA | Installation de PBS (Proxmox Backup Server) | | 1j |
| 13 | RÉSEAU | Configuration des accès VPN (Wiregard) | Tâche 5 et 6 | 1j |

# 10) Conception

## c) Liste des machines virtuelles et machines demandées

RAJOUTER LA SEPARATION DE LA LOGIQUE ATLANTIS / SPRINGFIELD

*ATLANTIS*

Le site d'Atlantis est assuré par deux pares-feux afin de garantir la sécurité du trafic en cas de panne d'un pare-feu.

**FIREWALL 1 et 2**

Voici la liste des machines virtuelles, elles ont été séparées en sept VLANs.

Le premier VLAN 10 est destiné à toute la partie administration, il utilise le sous-réseau suivants 10.0.10.0/24.

**VLAN 10 – ADMINISTRATEUR**

- DC-01 : machine hébergeant le contrôleur de domaine Active Directory principal.
- DC-02 : machine hébergeant le contrôleur de domaine Active Directory secondaire, garantissant la continuité d'activité en cas de défaillance du contrôleur principal.
- Monitor-01 : machine virtuelle de supervision qui est obligatoire pour la traçabilité ainsi que la détection d'incident.

- WSUS-01 : machine virtuelle qui permet de traiter les mises à jour non maîtrisées, réduction des failles de sécurité
- FS-01 : machine virtuelle de services de fichiers centralisés, avec application des droits par service et gestion des quotas utilisateurs.
- SIEM01 : machine virtuelle dédiée à l'hébergement de la solution SIEM et de la plateforme XDR.

Le second VLAN, le VLAN 20, est dédié aux différentes applications internes (ERP, CRM, etc.) et utilise le sous-réseau 10.0.20.0/24.

**VLAN 20 – APPLICATION**

- ERP-DB : machine virtuelle pour la base de données de l'ERP
- ERP-APP : machine virtuelle pour l'interface de gestion des données de l'ERP

**VLAN 30 – POSTES UTILISATEURS**

Le troisième VLAN 30 est à destination des postes utilisateurs avec pour adresse ip 172.16.0.0/16.

**VLAN 40 – BACKUP**

Le quatrième VLAN 40 est quant à lui dédié aux sauvegardes du SI et utilise le sous-réseau 10.0.40.0/24.

**VLAN 50 – DMZ + VPN pour le site web**

Le cinquième VLAN 50 a pour objectif de s'occuper de la DMZ avec le VPN pour le site web et utilise le sous-réseau 10.0.50.0/24.

**VLAN 60 – IMPRIMANTES**

Le sixième VLAN, le VLAN 60, est dédié à la gestion des imprimantes et utilise le sous-réseau 10.0.60.0/24.

**VLAN 66 – MANAGEMENT**

Le septième VLAN, le VLAN 66, est dédié à la gestion et à l'administration de l'ensemble de l'infrastructure virtuelle, et utilise le sous-réseau 10.0.66.0/24.

Cette architecture permet d'avoir une segmentation du réseau avec les VLANs, une supervision ainsi qu'un AD renforcé. Elle permet également de prévoir les rançongiciels en limitant les droits des utilisateurs et en isolant le réseau. Les machines du VLAN 10 protègent et administrent le système d'information. Les machines du VLAN 20 hébergent les services métiers critiques (ERP).

Le troisième VLAN, VLAN 30, est destiné à accueillir l'ensemble des postes utilisateurs. L'adresse réseau retenue pour ce segment est 172.16.0.0/16, permettant une large capacité d'adressage afin de supporter l'évolution future du parc informatique des collaborateurs.

Le quatrième VLAN, VLAN 40, est dédié aux machines virtuelles de sauvegarde des postes utilisateurs. Ce réseau, configuré en 10.0.40.0/24, permet d'isoler les flux de sauvegarde afin de garantir une meilleure sécurité et de ne pas impacter les performances du réseau de production.

Le cinquième VLAN, VLAN 50, est utilisé comme zone démilitarisée (DMZ), incluant notamment le VPN permettant l'accès au site web de l'entreprise depuis l'extérieur. Son adressage est défini en 10.0.50.0/24, offrant un périmètre réseau strictement contrôlé pour protéger les services exposés à Internet.

Le sixième VLAN, VLAN 60, est destiné à la gestion des imprimantes du réseau interne. Son adressage en 10.0.60.0/24 permet de séparer le trafic lié aux périphériques d'impression, contribuant à une meilleure organisation des flux et à la maîtrise de la sécurité.

Enfin, le septième VLAN, VLAN 66, est spécifiquement réservé au management des machines virtuelles. Le réseau 10.0.66.0/24 permet aux administrateurs d'accéder aux interfaces de gestion des hyperviseurs et des ressources virtualisées en toute sécurité, en évitant toute interférence avec les réseaux utilisateurs ou applicatifs.

## d) Cartographie cible du système informatique

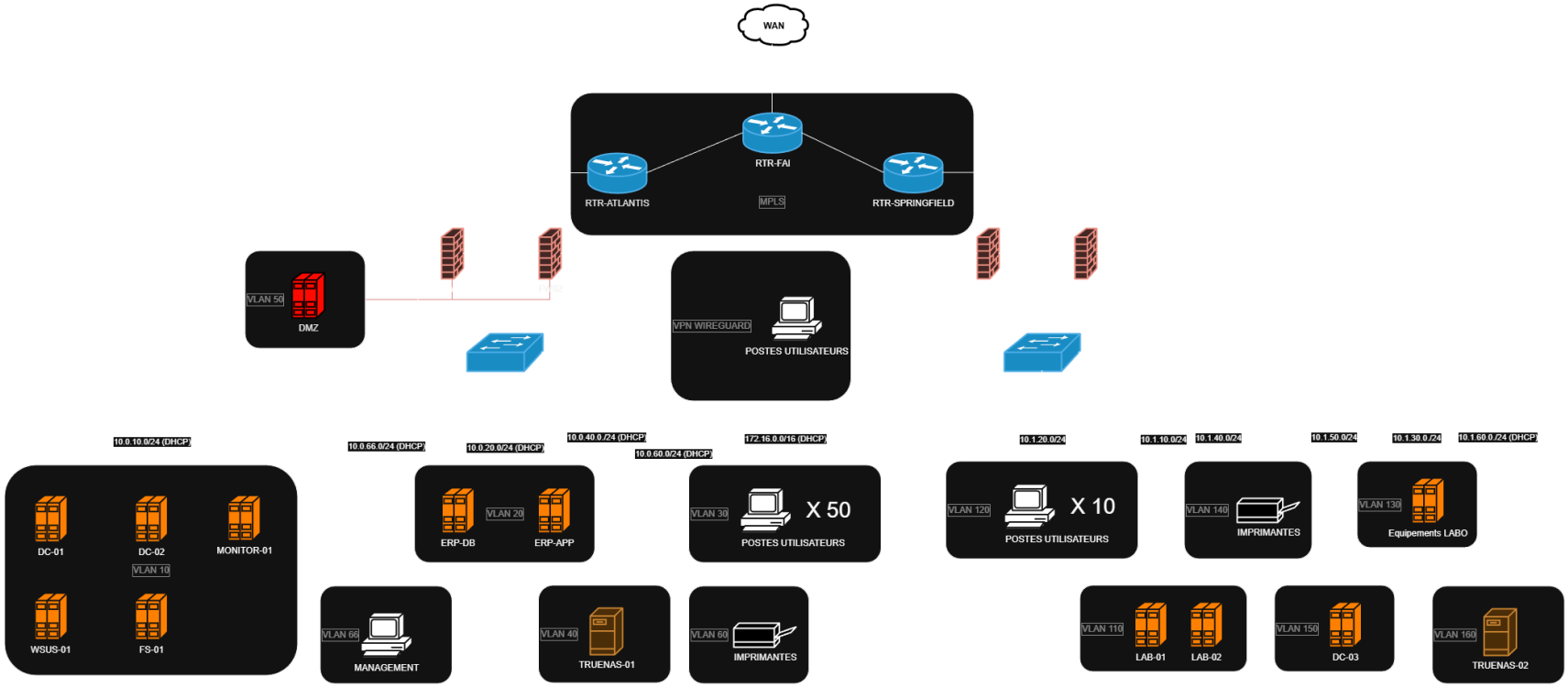


*Figure 2 : schéma réseau de l'infrastructure*

## Schéma logique du service Active Directory

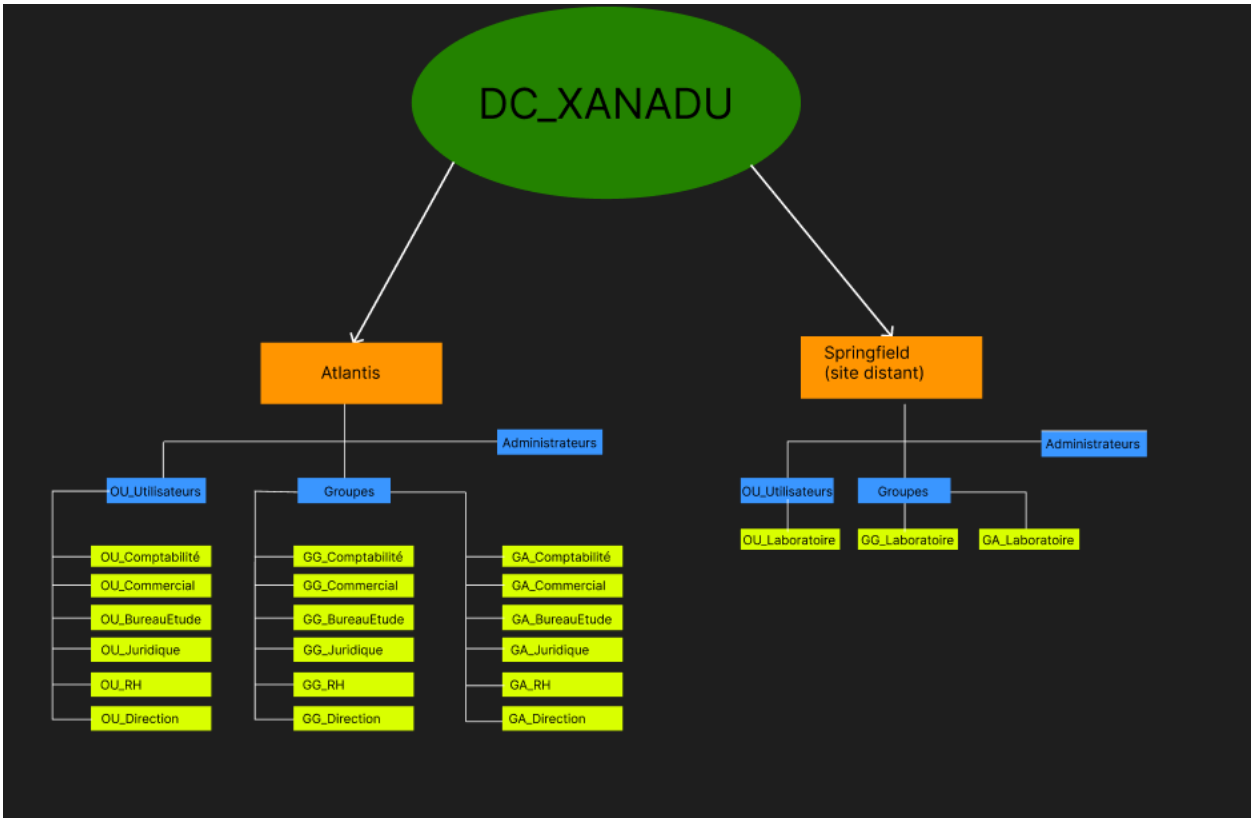


*Figure : schéma logique de l'active directory*

### e) La structure de l'annuaire (OU, groupes), schématisée et commentée

La structure de l'annuaire a été réalisée de manière à séparer en unité organisationnelle les utilisateurs pour chaque service : comptabilité, commercial, bureau d'étude, juridique, ressources humaines et direction pour le site Atlantis. Il y'a également un bloc groupe afin d'administrer les accès de chaque service du site. Le groupe administrateur aura un accès total et sans restriction sur les autres objets du domaine contrôleur (dc).

En parallèle, pour le site distant de Springfield, la même logique de fonctionnement pour les OU. C'est à dire un OU pour le Laboratoire ainsi qu'un groupe pour le Laboratoire et enfin un administrateur qui aura accès sur les objets Laboratoire.

## f) Description de l'administration déléguée

Pour l'administration déléguée, dans chaque service un correspondant informatique pourra créer ou modifier les comptes utilisateurs de son service, gérer les droits d'accès, ainsi que la possibilité d'intégrer des nouveaux postes utilisateurs et cela pour chaque site (Atlantis et Springfield).

## g) Les types de comptes et leurs rôles

- Comptes standards : user.nom (moindre privilège) avec la MFA obligatoire pour l'accès distant/O365, les comptes standards représentent les employés.
- Comptes administrateurs : adm-user.nom (A2F obligatoire, interdit sur postes utilisateurs), les comptes administrateurs représentent les correspondants informatiques des services. Ils ont des droits limités aux UO de service et ne sont pas admins de domaine.
- Comptes de service (AD) : svc-backup, svc-WSUS, svc-ERP (forte complexité, non interactifs). Permet l'exécution des services système (Sauvegarde, WSUS). Les comptes de services ont des mots de passe longs et complexes et non interactifs, c'est à dire qu'ils ne sont pas destinés à être utilisés par une personne pour se connecter.
- Services ERP : SVR-ERP. Les services ERP ont une connexion du serveur d'application ERP à la base de données. Ils ont des mots de passe renouvelés régulièrement et non interactifs.

## h) Description des stratégies de groupe (contenu, liaison) pour sécuriser le SI et pour administrer le SI

Pour les stratégies de groupe, l'objectif est de corriger les vulnérabilités et de se protéger des rançongiciels pour cela, il faut appliquer une politique GPO de sécurisation des postes clients (GPO_Sécurité Postes). Elle vise à imposer une configuration de sécurité stricte sur tous les postes de travail de XANADU.

**Stratégies de Groupe pour la Sécurité**

*GPO_Securite_Base_Postes*

Cette politique instaure le principe de sécurité le plus important pour les postes clients.

Elle supprime les utilisateurs standards du groupe Administrateurs local sur leur PC. Elle active également le Pare-feu Windows avec un profil strict (blocage des connexions entrantes non sollicitées) et désactive l'exécution automatique sur les médias amovibles.

Cette GPO applique le moindre privilège, minimisant ainsi la surface d'attaque. En l'absence de droits administratifs locaux, un rançongiciel ou autre logiciel malveillant exécuté accidentellement rencontrera des difficultés à s'installer ou à se propager, protégeant l'ensemble du réseau.

*GPO_Politiques_Comptes_AD*

Cette politique s'applique au niveau du domaine pour imposer des règles d'hygiène des identifiants.

Elle impose une longueur minimale de mot de passe de 14 caractères et conserve un historique de 24 mots de passe pour empêcher la réutilisation rapide. Elle configure également le verrouillage des comptes après 3 tentatives échouées, pour une durée de 30 minutes.

Elle renforce la sécurité des identifiants et protège les comptes contre les attaques par force brute (déchiffrement automatique ou tentatives manuelles), répondant directement au besoin de sécurisation global du SI.

*GPO_Controles_Applications_Securite*

Cette politique est essentielle pour centraliser et contrôler la protection des points de terminaison.

Elle définit la configuration centralisée de la suite de sécurité (analyse planifiée, exclusions minimales des chemins critiques). De plus, elle met en place des mesures de restriction pour bloquer l'exécution des exécutables depuis des emplacements sensibles comme les dossiers temporaires ou les profils utilisateurs (méthode d'attaque courante).

Elle garantit la conformité des Endpoints et met en place une barrière supplémentaire pour empêcher l'exécution de charges utiles de rançongiciels à partir des emplacements que les utilisateurs peuvent manipuler facilement.

*GPO_Gestion_MisesAJour_WSUS*

Cette politique corrige l'absence actuelle de contrôle des mises à jour.

Elle force tous les postes et serveurs à pointer vers le serveur WSUS interne (ou solution équivalente) comme source de mise à jour. Elle planifie l'installation automatique et le redémarrage forcé des machines en dehors des heures de bureau.

Elle assure que les vulnérabilités sont corrigées rapidement et de manière contrôlée, garantissant un SI stable et à jour. Ceci est vital pour la sécurité, car les rançongiciels exploitent souvent des failles non corrigées.

***GPO_Durcissement_Serveurs_Critiques***

Cette politique cible spécifiquement les actifs les plus sensibles de XANADU (serveurs ERP, bases de données).

Elle restreint l'accès RDP et les sessions console aux seuls groupes administrateurs dédiés (`ADM-Serveurs`). Elle impose une configuration d'audit stricte pour l'accès aux fichiers et les connexions aux serveurs.

Elle limite l'accès aux systèmes sensibles (ERP) et assure la traçabilité des événements, permettant à l'équipe de sécurité de savoir précisément qui a accédé au serveur et quand, ce qui est un besoin exprimé pour la reprise après incident.

## *Stratégies de Groupe pour l'Administration*

### *GPO_Redirection_Profils_Utilisateurs*

Cette politique est essentielle pour sécuriser les données utilisateur et garantir la fiabilité du SI.

Elle configure la Redirection de Dossiers pour centraliser les dossiers critiques comme « Mes Documents » et « Bureau » vers le dossier personnel centralisé de chaque employé sur le nouveau serveur de fichiers (partage U:).

Elle assure la Fiabilité et la Reprise après Incident (PRA). En centralisant les données de 5 Go/utilisateur, elle garantit que ces informations sont systématiquement incluses dans le plan de sauvegarde professionnel, mettant fin à la pratique non sécurisée des sauvegardes sur clé USB.

### *GPO_Mappage_Lecteurs_Ressources*

Cette politique standardise l'accès aux ressources partagées pour tous les employés.

Elle automatise le Mappage des lecteurs réseau pour les dossiers partagés des services. L'application de ces mappages est contrôlée par des Filtres de Sécurité basés sur l'appartenance aux Groupes de Sécurité (ex: seul le groupe GRP_ACCES_Comptabilite voit apparaître le lecteur C:).

Elle facilite l'Administration et la Gestion des Droits d'Accès. En utilisant les groupes, elle gère efficacement les accès croisés complexes (ex. : la Direction accédant à tous les dossiers, le service Juridique accédant à RH et Client).

### *GPO_Admin_Délégation_Outils*

Cette politique est un pilier du modèle de gestion des correspondants informatiques.

Elle déploie des outils d'administration spécifiques (ex. : des consoles MMC personnalisées ou des raccourcis scriptés) pour les comptes des Correspondants Informatiques (del-user.nom). Elle supporte le modèle d'Administration Déléguée.

Elle permet aux correspondants de réaliser leurs tâches (créer des comptes, réinitialiser des mots de passe) sur leur périmètre (leur UO de service) sans nécessiter les droits d'administrateur de domaine global, assurant ainsi la sécurité.

### *GPO_Configuration_VPN_Commerciaux*

Cette politique est essentielle pour la flexibilité du travail et la continuité d'activité.

Elle automatise le Déploiement de la configuration du client VPN sur les postes des commerciaux itinérants et des télétravailleurs. Elle peut également imposer des paramètres de sécurité additionnels (certificats, etc.).

Elle répond au besoin du directeur d'assurer la Continuité d'Activité et l'accès à l'information pour tous les employés, y compris ceux qui sont hors site, en garantissant une connectivité sécurisée au réseau interne.

*GPO_Parametres_Locaux_Springfield*

Cette politique permet de gérer le nouveau site distant de manière efficace.

Elle configure spécifiquement le déploiement des imprimantes (copieur et imprimante métier) du laboratoire de Springfield et fixe les paramètres réseau locaux (comme les serveurs DNS ou les réglages de fuseaux horaires).

Elle permet une Administration ciblée et efficace du site distant. En liant cette GPO uniquement à l'UO de Springfield, elle assure que les configurations locales n'interfèrent pas avec le site principal d'Atlantis, améliorant la stabilité opérationnelle.

## i) L'indication et le commentaire des éléments garantissant la confidentialité, l'intégrité, la disponibilité et la traçabilité.

Pour garantir un système d'information fiable et réellement sécurisé, nous avons structuré notre approche autour des quatre grands principes de la sécurité informatique : la confidentialité, l'intégrité, la disponibilité et la traçabilité.

*1. Confidentialité : protéger les informations sensibles*

La confidentialité consiste à faire en sorte que seules les personnes autorisées aient accès aux données et aux services.

Pour cela, plusieurs mécanismes ont été mis en place :

La segmentation en VLAN : permet d'isoler les environnements : les postes utilisateurs, l'administration, les sauvegardes, les imprimantes ou encore la DMZ ne se croisent plus directement. En cas de problème sur un poste, l'attaque ne peut pas se propager au reste du SI.

Les pares-feux OPNSense : filtrent strictement les flux et empêchent les connexions non autorisées.

L'Active Directory a été renforcé :

-comptes utilisateurs limités,

-comptes admin séparés,

-MFA obligatoire pour les accès distants,

-droits définis précisément via les groupes AD.

Les GPO : suppriment les droits d'administrateur local, ce qui réduit fortement les risques d'installation de malware.

Le VPN chiffré : garantit que les connexions extérieures se font dans un tunnel sécurisé.

Le chiffrement AES-256 : protège les sauvegardes même en cas de vol d'un support.

### *2. Intégrité : garantir que la donnée reste correcte et non altérée*

L'intégrité signifie que la donnée reste fidèle, intacte et non modifiée par erreur ou par attaque.

L'intégrité signifie que la donnée reste fidèle, intacte et non modifiée par erreur ou par attaque.

Pour cela :

ZFS assure un stockage fiable grâce à ses mécanismes de détection et de correction automatique des corruptions.

Les snapshots créent des "photos instantanées" immuables, rendant impossible la modification rétroactive.
En cas d'attaque, on revient en arrière immédiatement.

Les comptes de service ont été conçus pour limiter les actions humaines non désirées.

Les GPO de contrôle d'applications empêchent l'exécution de fichiers suspects dans les répertoires critiques.

Les audits AD renforcés permettent de suivre toute modification importante des objets du domaine.

La réplication ZFS échange uniquement les changements validés et vérifiés entre les sites, ce qui évite toute altération silencieuse.

### *3. Disponibilité : assurer que les services restent accessibles*

La disponibilité est essentielle pour l'activité de XANADU, notamment pour l'ERP ou l'authentification AD.

Nous garantissons cette disponibilité grâce à :

-La redondance des pares-feu: si l'un tombe, l'autre prend le relais.

-Deux contrôleurs de domaine pour assurer l'authentification même en cas de panne.

-La liaison MPLS avec SLA entre Atlantis et Springfield, qui garantit une qualité de service constante.

-Le réseau virtualisé Proxmox et son VLAN dédié au management, pour assurer une administration stable.

-La stratégie 3-2-1-1-0 de sauvegarde, qui prévoit plusieurs copies sur des supports différents, dont une hors site et une hors ligne.

-Des objectifs de reprise adaptés aux différents types de données :

-ERP / AD : retour maximal en 4 heures

-Données métiers : 24 heures

-Données standard : 48 heures

*4. Traçabilité : savoir qui fait quoi, quand et comment*

La traçabilité permet de comprendre, vérifier et retracer toutes les actions importantes réalisées sur le système d'information.

Pour cela, nous avons mis en place :

Un serveur SIEM dédié (SIEM01) qui centralise l'ensemble des logs du SI : pare-feu, AD, VPN, serveurs, etc.
Il permet également d'envoyer des alertes en temps réel en cas de comportement suspect.

Monitor-01, qui assure la supervision continue de l'infrastructure (services, ressources, disponibilité).

Un audit renforcé des serveurs critiques, notamment pour l'accès aux dossiers sensibles et pour les connexions RDP.

La journalisation complète des accès VPN, permettant de suivre précisément les connexions à distance.

Les snapshots immuables, qui offrent une preuve que la donnée n'a pas été modifiée.

Une gestion stricte des rôles (RBAC) au niveau des sauvegardes et du stockage.

# 11) Mise en de place de l'environnement technique

L'environnement technique du système d'information de XANADU sera composé d'une infrastructure virtualisée et sécurisée afin de répondre aux exigences de la direction. La virtualisation du serveur se fera par l'hyperviseur Proxmox. Le contrôle du réseau se fera par l'intermédiaire du pare-feu OPNSense. La gestion du routage et l'interconnexion des réseaux reposent sur VyOS.

Les services Linux, seront déployés sous Rocky Linux, distribution robuste et compatible avec l'écosystème Red Hat. Enfin, deux commutateurs réseau seront déployés : un sur le site de la technopole Atlantis et un sur le site distant de Springfield, permettant une segmentation du réseau et une qualité de service conforme aux impératifs de sécurité et de disponibilité. Cette architecture

constituera une base fiable, sécurisée pour le futur système d'information de XANADU.

# 12) Stratégie de sauvegarde

## j) Stratégie globale

*Infrastructure*

- TrueNAS SCALE sur chaque site (Atlantis et Springfield) pour les NAS
- ZFS avec déduplication SHA256 et compression LZ4
- RAID-Z2 avec SSD L2ARC pour cache
- Réplication automatique via lien MPLS

*Topologie*

- Site Atlantis (Principal)
    - Serveur TrueNAS Atlantis
    - VLAN dédié (VLAN 40 - Backup)
    - Connexion MPLS 1 Gbps vers Springfield

- Site Springfield (Secondaire)
    - Serveur TrueNAS Springfield
    - VLAN dédié (VLAN 40 - Backup)
    - Connexion MPLS 1 Gbps vers Atlantis

*Coût*

Environ 22 200€

## k) Configuration ZFS

Création pools avec déduplication

Données à sauvegarder : ~10 TB

Ratio déduplication estimé : 2.5:1

## l) Politique de rétention (3-2-1-1-0)

La politique de rétention se compose de la manière suivante :

- 3 copies minimum

- 2 supports différents (TrueNAS + Cloud Local)
- 1 copie hors site (réplication inter-sites)
- 1 copie offline (bandes LTO mensuelles)
- 0 erreur (scrub ZFS hebdomadaire)

## m)Snapshots ZFS

| Criticité | Fréquence | Rétention | Configuration |
|---|---|---|---|
| Critique (ERP, ADDS) | Horaire<br>Quotidien<br>Hebdomadaire<br>Mensuel | 48 heures<br>14 jours<br>8 semaines<br>24 mois | Toutes les heures<br>Tous les jours à 23 h<br>Tous les dimanches à 2h<br>1er du mois 3h |
| Important (Docs) | Horaire<br>Quotidien<br>Mensuel | 24 heures<br>7 jours<br>12 mois | Toutes les 2 heures<br>Tous les jours à 23h<br>1er du mois 3h |

## n) Réplication Inter-Sites

La réplication inter-sites se compose de cette manière :

- Configuration TrueNAS
- Source: backup-atlantis
- Destination : backup-springfield
- Planification : Quotidienne à 23h30 (post-snapshots)
- Chiffrement : SSH + TLS
- Limite bande passante : 500 Mbps
- Lien MPLS requis

| Type | Fréquence | Méthode | Cible |
|---|---|---|---|
| Complète<br>Incrémentale<br>Différentielle | Mensuelle<br>Quotidienne<br>Hebdomadaire | ZFS send complet<br>ZFS send incrémental<br>ZFS send depuis dernière complète | Bande LTO + Cloud Springfield<br>Stockage intermédiaire |

## o) Objectif de Reprise (RTO/RPO)

| Services | RTO | RPO | Solution |
|---|---|---|---|
| Critiques (ERP, ADDS) | 4h | 1h | Snapshots horaires + réplication quotidienne |

| | | | |
|---|---|---|---|
| Importants (Fichiers clients) | 24h | 4h | Snapshots 2h + réplication quotidienne |
| Standards (Personnel) | 48h | 24h | Snapshots quotidiens + réplication hebdomadaire |

Le tableau classe les services selon leur criticité. Il indique leurs objectifs de reprise (RTO) et de perte de données (RPO), ainsi que les solutions de sauvegarde. Les services critiques, comme l'ERP ou Active Directory, doivent être restaurés rapidement. Pour cela, des snapshots sont pris chaque heure et la réplication est quotidienne. Les services importants, tels que les fichiers clients, ont des snapshots toutes les deux heures et une réplication quotidienne. Enfin, les services standards, comme les données du personnel, sont protégés par des snapshots quotidiens et une réplication hebdomadaire. Les délais de restauration sont plus longs pour ces services.

## p) Sécurité

On protège les données avec du chiffrement AES-256-GCM, ce qui assure à la fois la confidentialité et l'intégrité.

Pour les clés, on les garde soit dans un HSM soit dans un coffre physique bien sécurisé. On les renouvelle chaque année afin de limiter la casse si jamais une clé venait à être compromise.

## q) Contrôle d'accès

On gère les accès avec un système RBAC qui définit trois rôles principaux : Administrateur, Opérateur et Auditeur.

Pour se protéger des ransomwares, on utilise des snapshots en lecture seule - impossible de les modifier ou chiffrer. Le trafic de sauvegarde passe par un VLAN dédié (VLAN 40 - Backup) qui isole tout ça du reste du réseau.