Administration du SI
&
sécurité IT
Livrable 2

CESI
ÉCOLE D'INGÉNIEURS

CESI
ÉCOLE D'INGÉNIEURS

XANADU

Projet Administration et sécurisation d'un système d'information

Réalisé par

Alexandre RIVET

Allan BOUHAMED

Antonin RABATEL

Mathéo CARVAL

Philippe LUU

Projet encadré par

Djamel AOUAM

Année universitaire 2025-2026

Livrable 2 - 11/12/2025

Sommaire

Sommaire **3**
1. Contexte **5**
2. Objet du document **7**
2.1. Audit de sécurité et Politique de filtrage 7
2.2. Automatisation (Scripts) et Supervision 7
2.3. Livrable destiné à la présentation et à la mise en production 8
3. Questionnaire de sécurité et audit de l'existant **9**
3.1 Méthodologie d'audit et périmètre 9
3.1.1 Référentiels et approche 10
3.1.2 Périmètre de l'audit 12
3.1.3 Objectifs de l'audit 14
3.2 Gestion des accès et des identités (IAM) 14
3.2.1 Analyse des comptes, privilèges et authentification 15
3.2.2 Journalisation des accès 16
3.3 Sécurisation des réseaux et des flux 17
3.3.1 Cloisonnement, VPN et Monitoring réseau 17
3.4 Sécurité des terminaux (Postes et Serveurs) 18
3.4.1 Protection virale (Malwares et Ransomwares) 18
3.4.2 Durcissement et verrouillage des postes 18
3.4.3 Verrouillage du BIOS et chiffrement des disques 19
3.5 Gouvernance et Maintenance 19
3.5.1 Politiques et réglementation 19
3.5.2 Gestion des mises à jour et correctifs 19
3.5.3 Politique de sauvegarde et tests de restauration 20
3.5.4 Formation et sensibilisation des utilisateurs 20
3.6 Continuité et Sécurité physique 20
3.6.1 Plan de continuité et de reprise après sinistre (PCA/PRA) 20
3.6.2 Redondance 21
3.6.3 Protection physique des locaux et équipements 22
3.7 Synthèse des risques et Plan de remédiation (Bonnes pratiques) 23
4. Filtrage 23
4.1 Principes directeurs de la sécurité périmétrique 23
4.1.1 Principe du "Block All" et moindre privilège 23
4.1.2 Gestion des objets et groupes d'adresses 23
4.2 Matrice de flux : Site "ATLANTIS" (Siège) 24
4.2.1 Filtrage Inter-VLANs (Segmentation interne) 24
4.2.2 Règles d'accès vers la DMZ 24

4.2.3 Protection des interfaces WAN (Publiques)..... 24
4.3 Matrice de flux : Site "SPRINGFIELD" (Distant).....25
4.4 Protection spécifique des services critiques.....25
4.4.1 Flux Active Directory et DNS (AD DS)..... 25
4.4.2 Accès aux bases de données et applicatifs métier..... 25
5. Automatisation et Scripts d'administration.....26
5.1 Stratégie d'automatisation et langage retenu (PowerShell/Bash).....26
5.2 Scripts de gestion des Identités et de l'Annuaire..... 27
5.2.1 Script 1 : user_functions.ps1 - Bibliothèque de fonctions communes..... 27
5.2.2 Script 2 : create_user.ps1 - Création et provisioning des utilisateurs.....27
5.2.3 Script 3 : create_user_info.ps1 - Création de comptes pour le département INFORMATIQUE..... 30
5.2.4 Script 4 : disable_user.ps1 - Désactivation et mise en quarantaine d'utilisateurs. 32
5.2.5 Script 5 : auto_quarentine.ps1 - Quarantaine automatique des comptes inactifs. 34
5.3 Scripts de gestion de sauvegarde.....38
5.3.1 Script de sauvegarde locale.....38
5.3.2 Script de restauration..... 41
5.3.3 Script d'externalisation des sauvegardes.....44
5.3.4 Script d'alerte..... 46
5.3.5 Script de planification des sauvegardes.....47
5.3.6 Script de purge / rétention des sauvegardes.....51
6. Supervision et Monitoring de sécurité.....54
6.1 Architecture de surveillance unifiée.....54
6.1.1 Rôle du SIEM (Wazuh) et du Monitoring (Zabbix).....54
6.2 Matrice des événements de sécurité surveillés.....55
6.2.1 Événements liés à l'authentification (Brute force, échecs).....55
6.2.2 Événements liés à l'intégrité système (Fichiers critiques).....56
6.2.3 Événements liés au réseau et aux menaces externes.....57
6.3 Gestion des alertes et déclencheurs (Triggers)..... 58
6.3.1 Niveaux de classification..... 58
6.3.2 Règles de déclenchement (Triggers)..... 59
6.3.3 Workflow de notification.....59
8. Table des figures.....61
8. Annexes..... 62
8.1 Audit de l'équipe technique et des employées.....62
8.2 Matrice de flux.....63

1. Contexte

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

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

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

Le nouveau système doit répondre aux besoins supplémentaires suivants :

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

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

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

2. Objet du document

Le présent document constitue le **Livrable 2 – Politiques & Questionnaires de sécurité** du projet CESITECH pour l'entreprise XANADU.

Il a pour objectif de définir les règles de gouvernance, les mesures de protection active et les outils d'exploitation nécessaires à la sécurisation de l'architecture présentée dans le Livrable 1.

2.1. Audit de sécurité et Politique de filtrage

Cette partie établit le diagnostic sécuritaire et les règles de protection périmétrique du système d'information.

Elle inclut un questionnaire de sécurité exhaustif permettant d'identifier les vulnérabilités potentielles (infrastructures, données, processus) et de mesurer le niveau de conformité aux normes actuelles. Chaque point audité est accompagné d'axes de remédiation et de recommandations de bonnes pratiques pour durcir le SI.

Elle détaille également la politique de filtrage déployée sur les équipements de sécurité (pare-feux* PfSense*). Cette politique est formalisée par des matrices de flux précisant, pour chaque interface, les sources, destinations, protocoles et actions (autoriser/bloquer).

Elle justifie les choix opérés pour garantir le cloisonnement strict des zones (VLANs*, DMZ*) et l'application du principe de moindre privilège, en cohérence avec les recommandations de l'ANSSI* sur la définition des règles de pare-feu.

2.2. Automatisation (Scripts) et Supervision

Ce livrable présente les outils techniques mis en œuvre pour assurer l'administration quotidienne et la surveillance du SI. Il propose une bibliothèque de **10 scripts d'administration** (PowerShell* ou Bash*), commentés et contextualisés.

Ces scripts répondent à des besoins fonctionnels précis (gestion des utilisateurs, sauvegardes, configuration) et respectent les bonnes pratiques de codage (lisibilité, gestion d'erreurs, sécurité). La stratégie de **supervision** est également décrite, incluant l'architecture de surveillance (Wazuh*, Zabbix*) et la méthodologie de collecte des données. Une liste de **10 événements déclencheurs** pertinents est définie (avec description, criticité, source et action), garantissant une réactivité immédiate face aux incidents de sécurité ou de performance.

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

Ce document est conçu comme un guide de référence opérationnel destiné à la direction de XANADU ainsi qu'aux équipes techniques chargées de l'exploitation.

Il complète l'architecture technique du Livrable 1 en apportant les garanties nécessaires en matière de **Confidentialité**, **Intégrité**, **Disponibilité** et **Traçabilité**.

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

De plus, l'architecture mentionnée au livrable 1 demande beaucoup de performances ; ainsi, elle ne peut être maquettée via un seul serveur de 32 Go de RAM.

C'est pourquoi nous avons adopté une nouvelle architecture, toujours aussi réaliste, mais qui correspond davantage à l'infrastructure actuelle de la PME XANADU.

Cette architecture dite « à trois pattes » constitue un socle solide qui pourra être développé à mesure que l'entreprise croît, pour tendre in fine vers une architecture « sandwich » plus complexe.

(**Voir annexe 8.3**)

Concrètement, nous rationalisons les équipements de sécurité en passant d'une double barrière de pare-feux à un dispositif central unique gérant trois zones de sécurité distinctes via des interfaces dédiées.

Dans cette configuration, le pare-feu central orchestre les flux entre trois pôles : l'interface LAN pour le réseau interne, l'interface DMZ connectée à un switch dédié pour isoler les services exposés, et l'interface WAN reliée directement au routeur de bordure (R1).

Cette topologie permet de maintenir une segmentation stricte et un filtrage efficace entre la zone interne, la zone démilitarisée et l'extérieur, tout en réduisant drastiquement la consommation de ressources matérielles nécessaires à la simulation.

Les équipements, adresses IP, matrice de flux et filtrage sont recensés dans les documents : **Inventaire_équipements.pdf, SW.pdf, Filtrage.pdf**

3. Questionnaire de sécurité et audit de l'existant

La sécurité d'un système d'information ne se limite pas à l'installation d'outils ; elle repose sur une analyse rigoureuse des risques et une connaissance parfaite du périmètre à protéger. Cette section détaille la méthode utilisée pour auditer la situation de XANADU et définir les axes d'amélioration.

3.1 Méthodologie d'audit et périmètre

Afin de répondre aux exigences du directeur (protection contre les rançongiciels, fiabilité, RTO de 4h) et de préparer la migration vers les sites d'Atlantis et Springfield, nous avons adopté une méthodologie d'audit structurée, inspirée des référentiels de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

3.1.1 Référentiels et approche

Notre démarche d'audit repose sur une analyse comparative rigoureuse entre l'état actuel ("Legacy"), tel que décrit dans le contexte, et les bonnes pratiques de sécurité ("Best Practices") intégrées à la nouvelle architecture.

Cette approche s'appuie sur plusieurs référentiels majeurs.

Nous suivons le Guide d'hygiène informatique de l'ANSSI pour établir les mesures concernant les postes de travail, l'authentification et les mises à jour.

En complément, nous nous inspirons des normes ISO/IEC 27001 et 27002 pour structurer la gouvernance, la gestion des accès et la continuité d'activité, tout en appliquant les CIS Benchmarks pour assurer le durcissement technique des systèmes d'exploitation Windows et Linux.

L'exécution de l'audit se déroule en trois phases successives.

La première étape consiste en une analyse de l'existant visant à identifier les failles critiques de l'infrastructure actuelle, telles que l'usage de comptes locaux, les sauvegardes sur supports USB, l'utilisation du protocole HTTP ou l'attribution de droits administrateurs excessifs.

Elle est suivie d'une évaluation des risques qui qualifie les menaces pesant sur XANADU, notamment l'exposition aux ransomwares, le vol de données et la perte d'exploitation.

La démarche aboutit à une proposition de remédiation définissant l'ensemble des mesures correctives, qu'elles soient techniques à travers l'architecture cible ou organisationnelles via l'établissement de nouvelles procédures.

Ainsi, un premier sondage Google Forms est proposé à l'équipe informatique afin de pouvoir collecter en profondeur la sécurité technique de l'infrastructure **(Voir annexe 8.1)** :

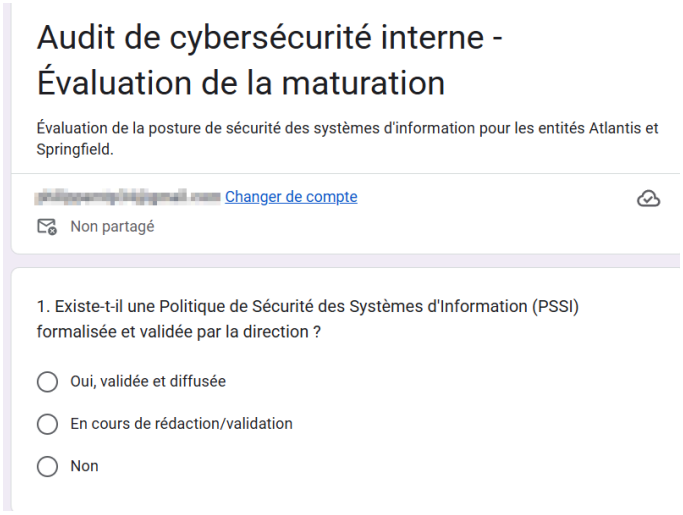


Figure 1 : Extrait du sondage de la cybersécurité

De plus, un questionnaire intéractif sur la plateforme Klaxoon est proposé, il est destiné aux employés de l'entreprise afin de jauger leur réflexes en cybersécurité :

(Voir annexe 8.1)

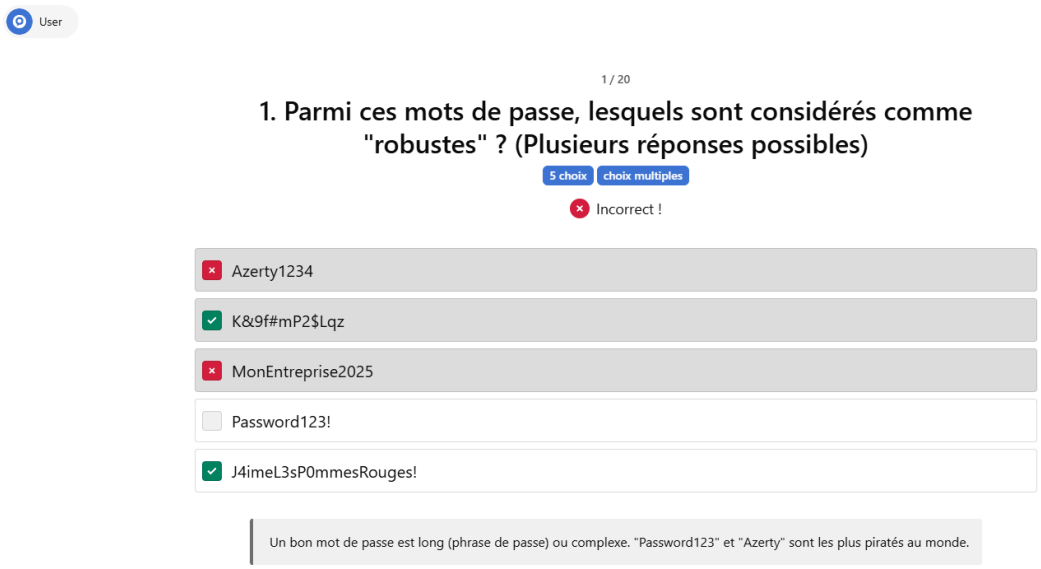


Figure 2 : Extrait du questionnaire utilisateur des réflexes cybersécurité

3.1.2 Périmètre de l'audit

Le périmètre de l'audit et du questionnaire de sécurité englobe l'intégralité du nouveau Système d'Information étendu de XANADU et se décompose en trois couches distinctes. Sur le plan physique et géographique, l'analyse couvre le site principal Atlantis, qui héberge le cœur de réseau, les serveurs critiques (AD, ERP, Fichiers) ainsi que 50 collaborateurs, et le site distant Springfield, accueillant le laboratoire, deux serveurs Linux de pilotage et 10 collaborateurs.

Le périmètre inclut également les utilisateurs nomades, tels que les commerciaux et les télétravailleurs, qui se connectent depuis l'extérieur via leur domicile, des hôtels ou des connexions 4G.

Concernant le volet logique et technique, l'audit examine l'infrastructure réseau, notamment la segmentation VLAN, le filtrage par pare-feu PfSense, les liaisons WAN (MPLS et VPN) ainsi que les accès Wi-Fi et filaires.

Il s'étend aux systèmes, incluant les contrôleurs de domaine Windows Server, les serveurs d'application Linux et le parc client sous Windows 10 et 11 Pro.

Les applications critiques sont également concernées, ciblant spécifiquement l'ERP basé sur PostgreSQL et Odoo, les services de fichiers SMB et la messagerie Office 365.

Enfin, le périmètre fonctionnel et organisationnel se concentre sur la gestion des identités, allant du cycle de vie des comptes utilisateurs (arrivées et départs) à la gestion des privilèges distinguant administrateurs et utilisateurs standard.

L'audit évalue aussi la continuité d'activité à travers les processus de sauvegarde (respect des RTO/RPO), les tests de restauration et la redondance des équipements.

La gouvernance globale est vérifiée par l'analyse des chartes informatiques, des actions de sensibilisation des utilisateurs et des procédures de mise à jour et de maintenance.

3.1.3 Objectifs de l'audit

L'objectif principal de cette démarche est de transformer le SI de XANADU, actuellement fragilisé par des vulnérabilités telles que les droits d'administration locaux, l'usage du protocole NTLM et des sauvegardes manuelles, en une architecture robuste.

Cette transformation vise à assurer la confidentialité en chiffrant les flux (VPN, HTTPS) et les données sensibles, ainsi que l'intégrité du système en empêchant les modifications non autorisées par la restriction des droits et la protection contre les ransomwares.

Elle doit également garantir la disponibilité des services, avec un objectif de temps de rétablissement (RTO) inférieur à 4 heures pour l'ERP grâce à la redondance et des sauvegardes fiables.

Enfin, la traçabilité est établie par la journalisation systématique des accès et des actions administratives afin de faciliter les audits futurs.

3.2 Gestion des accès et des identités (IAM)

La gestion des identités et des accès (IAM - Identity and Access Management) constitue la première ligne de défense logique du Système d'Information de XANADU.

L'objectif est de garantir que seules les personnes autorisées peuvent accéder aux ressources nécessaires à leur fonction, selon le principe du **"Moindre Privilège"**.

Cette section analyse les mécanismes d'authentification, la gestion du cycle de vie des comptes utilisateurs et la traçabilité des actions au sein de l'infrastructure (Active Directory, ERP, Équipements réseaux).

3.2.1 Analyse des comptes, privilèges et authentification

L'audit initial ayant mis en lumière des vulnérabilités critiques telles que l'usage de comptes partagés et des droits d'administration excessifs, la nouvelle politique de sécurité restructure en profondeur la gestion des identités pour corriger ces failles.

Concernant le cycle de vie des comptes (JML), une convention de nommage stricte, de type p.nom, est désormais appliquée pour garantir l'unicité et l'identification immédiate de chaque utilisateur.

L'imputabilité des actions est renforcée par l'interdiction formelle des comptes génériques pour les sessions interactives, rendant les comptes nominatifs obligatoires.

De plus, pour éviter la persistance de comptes orphelins, une procédure de départ automatisée via script assure la désactivation immédiate des accès AD, VPN et ERP dès la sortie d'un collaborateur.

La gestion des privilèges repose désormais sur le principe du moindre privilège et la séparation des pouvoirs.

Concrètement, les utilisateurs standard ne disposent plus des droits d'administrateur local sur leur poste, une mesure essentielle pour bloquer l'installation de logiciels non autorisés et freiner la propagation des ransomwares.

Les administrateurs du système d'information doivent quant à eux utiliser deux comptes distincts : un compte standard pour la bureautique courante et un compte dédié (préfixe adm_) exclusivement réservé aux tâches de maintenance serveur.

En complément, la solution LAPS a été déployée pour centraliser la gestion des mots de passe des administrateurs locaux de secours, rendant chaque mot de passe unique pour empêcher les mouvements latéraux en cas de compromission.

Enfin, le durcissement de l'authentification est assuré par une stratégie de groupe (GPO) imposant des mots de passe complexes d'au moins 12 caractères, incluant majuscules, minuscules, chiffres et caractères spéciaux, avec un verrouillage automatique du compte après cinq tentatives échouées pour contrer les attaques par force brute.

Sur le plan des protocoles, la sécurité est renforcée par la désactivation de NTLMv1 au profit de Kerberos pour l'authentification interne, ainsi que par l'obligation de signature LDAP ou l'usage de LDAPS sur le port 636 pour sécuriser les flux des applications tierces connectées à l'Active Directory.

3.2.2 Journalisation des accès

Afin de satisfaire aux exigences de traçabilité et de permettre des investigations numériques (Forensic) efficaces en cas d'incident, avec un objectif de temps de rétablissement (RTO) inférieur à 4 heures, un système centralisé de journalisation a été déployé.

Les journaux d'événements ne sont plus stockés uniquement en local, où ils restaient vulnérables à une suppression par un attaquant, mais sont transmis en temps réel vers un serveur centralisé de type Wazuh ou un serveur Syslog sécurisé.

La politique d'audit, configurée par GPO et sur les équipements réseaux tels que Cisco ou PfSense, surveille des événements ciblés.

Cela inclut les authentifications (succès et échecs, notamment hors heures ouvrées), la gestion des comptes (création, suppression ou modification de groupes sensibles comme les administrateurs du domaine), ainsi que l'accès et la modification de fichiers dans les dossiers critiques des services RH, Direction ou Code Source ERP.

La traçabilité s'étend également aux commandes administratives exécutées via sudo sur les serveurs Linux et aux changements de configuration sur les équipements réseaux.

Pour garantir la cohérence temporelle indispensable à l'analyse de ces logs entre les différents systèmes (Atlantis, Springfield, Cloud), l'ensemble des équipements, incluant serveurs, switchs et postes de travail, est synchronisé sur une source de temps unique.

Ce serveur NTP interne, hébergé sur le contrôleur de domaine PDC, se synchronise lui-même sur une strate externe fiable pour assurer une exactitude totale des horodatages.

3.3 Sécurisation des réseaux et des flux

3.3.1 Cloisonnement, VPN et Monitoring réseau

Segmentation et contrôle des accès Pour prévenir la propagation latérale de menaces, l'ancien réseau plat a été remplacé par une segmentation stricte en VLANs.

Ce découpage isole les Utilisateurs (par métier), les Serveurs critiques (AD, ERP), l'Administration et les Invités. Le contrôle des flux est assuré par le cœur de réseau Cisco (Niveau 3) via des ACLs rigoureuses appliquées aux interfaces virtuelles (SVI).

Ce principe de moindre privilège garantit que seuls les flux légitimes sont autorisés (ex. : accès spécifique Compta vers ERP), bloquant tout trafic inter-services non justifié.

Interconnexion et mobilité sécurisée L'architecture WAN distingue les flux inter-sites des accès nomades. La liaison Atlantis-Springfield transite exclusivement par le lien MPLS grâce à un routage statique, sécurisant nativement les réplications Active Directory et les données métiers. Pour le télétravail, OpenVPN a été déployé sur les pare-feux pfSense.

Sécurisés en AES-256, les tunnels sont conditionnés à une authentification centralisée via Active Directory, permettant une gestion dynamique des droits d'accès et une révocation immédiate en cas de risque.

Monitoring proactif La supervision de l'infrastructure repose sur le couple Zabbix et Wazuh. La collecte des métriques réseau utilise le protocole SNMP v3 pour garantir l'authentification et le chiffrement des échanges, tandis que des agents dédiés surveillent les ressources des serveurs (CPU, RAM, Disque). Une politique d'alerting en temps réel a été configurée sur les services vitaux, assurant une réactivité immédiate des équipes techniques avant tout impact sur la production.

3.4 Sécurité des terminaux (Postes et Serveurs)

La sécurité périmétrique (Pare-feu) ne suffit plus. Dans une stratégie de "Défense en Profondeur", chaque terminal (Endpoint) doit être une forteresse capable de résister à une infection, même si elle parvient à traverser le réseau. Cette section détaille le durcissement des postes de travail Windows 11 et des Serveurs.

3.4.1 Protection virale (Malwares et Ransomwares)

Conformément à la stratégie établie, XANADU déploie une protection multicouche associant Antivirus, EDR et XDR pour contrer les menaces modernes telles que les rançongiciels. Le socle de sécurité repose sur Microsoft Defender, durci via GPO sur l'ensemble du parc, garantissant une protection temps réel indésactivable et une détection Cloud des menaces émergentes.

En complément, l'agent OpenEDR équipe les postes critiques et serveurs pour pallier les limites de l'antivirus traditionnel par une surveillance comportementale capable de tuer instantanément un processus de chiffrement massif et d'isoler la machine infectée. L'ensemble est supervisé par la solution XDR Wazuh qui centralise les alertes de sécurité et surveille l'intégrité des fichiers sensibles de l'ERP et du système via son module FIM.

3.4.2 Durcissement et verrouillage des postes

Pour réduire la surface d'attaque, nous appliquons le principe du "Moindre Privilège" et restreignons les capacités de l'OS via des GPO restrictives (Livrable 1 §3.5).

Afin de réduire drastiquement la surface d'attaque, XANADU applique le principe du moindre privilège en supprimant les droits d'administration locale pour les utilisateurs standards, empêchant ainsi l'installation de logiciels non approuvés et l'ancrage profond de malwares. En complément, la stratégie de groupe `GPO_USB_Block` restreint l'usage des ports USB par un blocage en écriture généralisé et une interdiction totale pour les services sensibles, prévenant l'exfiltration de données et les attaques physiques.

Enfin, le système est verrouillé via les règles ASR (Attack Surface Reduction) qui bloquent l'exécution de scripts obfusqués, les processus enfants issus de macros Office ainsi que l'accès à PowerShell et à l'invite de commande pour les utilisateurs non privilégiés.

3.4.3 Verrouillage du BIOS et chiffrement des disques

Pour garantir la sécurité physique des équipements mobiles exposés au vol, le BIOS/UEFI de chaque poste est protégé par un mot de passe superviseur et le Secure Boot est activé, tandis que la séquence de démarrage est verrouillée sur le disque interne pour empêcher tout contournement via un média externe.

En parallèle, la confidentialité des données est assurée par le chiffrement intégral BitLocker (AES-256) couplé à la puce TPM 2.0 sur tous les ordinateurs portables et serveurs critiques, avec une sauvegarde automatique des clés de récupération dans l'Active Directory pour garantir la maintenance.

3.5 Gouvernance et Maintenance

3.5.1 Politiques et réglementation

Nous avons proposé plusieurs politiques et réglementations vis-à-vis de la cybersécurité de XANADU, afin de formaliser et uniformiser l'ensemble du personnel, des documents ont été rédigés (PSSI, charte informatique, gestion d'incidents, charte IA).

Voir PSSI.pdf, Charte_informatique.pdf, Charte_IA.pdf, INCIDENT_CYBER.pdf dans le dossier "documents".

3.5.2 Gestion des mises à jour et correctifs

Afin de combler les vulnérabilités logicielles dès leur découverte, XANADU centralise le déploiement des correctifs via le rôle WSUS installé sur les contrôleurs de domaine principaux. Cette gestion centralisée permet au service informatique de tester et d'approuver les mises à jour critiques avant leur diffusion massive, garantissant ainsi la stabilité de la

production tout en imposant une installation sous 7 jours pour réduire l'exposition aux failles connues.

3.5.3 Politique de sauvegarde et tests de restauration

La pérennité des données repose sur l'application stricte de la règle 3-2-1, combinant stockage local haute performance sur RAID 10 pour un RTO inférieur à 4 heures et réplication chiffrée vers le site distant de Springfield pour contrer les sinistres majeurs. La fiabilité de ce dispositif est assurée par l'immuabilité des sauvegardes critiques, protégeant contre l'effacement par rançongiciel, et validée par des tests de restauration automatisés hebdomadaires garantissant l'intégrité des archives.

3.5.4 Formation et sensibilisation des utilisateurs

Considérant l'humain comme le premier rempart de la sécurité, XANADU instaure un programme continu de sensibilisation incluant des campagnes de faux phishing et des ateliers sur les bonnes pratiques numériques. L'adhésion formelle à la charte informatique est rendue obligatoire pour tout collaborateur, définissant clairement les responsabilités et les interdictions, notamment concernant l'ouverture de pièces jointes suspectes ou l'usage de supports amovibles personnels.

3.6 Continuité et Sécurité physique

3.6.1 Plan de continuité et de reprise après sinistre (PCA/PRA)

L'architecture a été conçue pour la résilience grâce à la redondance systématique des équipements critiques, incluant le cluster de pare-feux, la haute disponibilité des cœurs de réseau et la réplication des services Active Directory. En cas d'incident majeur, une procédure de réponse formalisée dicte les étapes d'isolation et de bascule vers les infrastructures de secours, permettant le maintien des fonctions vitales de l'entreprise et la restauration des services prioritaires dans les délais contractuels définis.

3.6.2 Redondance

Une redondance de tous les services importants a été proposée.

En effet, les équipements réseaux tels que les firewalls, les serveurs ont été dédoublés et se répliquent entre eux.

Ainsi, un serveur Windows / Linux possède 2 cartes réseaux branchées sur 2 switchs différents et dont les switchs sont redondants également.

Ces switchs sont également branchés à des firewalls qui sont redondants, et ceux via le protocole CARP (permettant la mise en place d'un réseau privé entre les équipements) permettant de reprendre la configuration des différents équipements.

De plus, les équipements ont chacun une adresse IP physique différente SW1 : 192.168.200.253/24 et SW2 : 192.168.200.252/24 mais continuent à répondre sous une adresse virtuelle, SW1 et SW2 répondent à 192.168.200.254/24 mais SW1 est prioritaire, et si SW1 ne répond pas à SW2 via le réseau privé SW1-SW2 192.168.199.0/24 dans une durée donnée comme 10 secondes, alors SW2 prend le relais et répond sous 192.168.200.254/24.

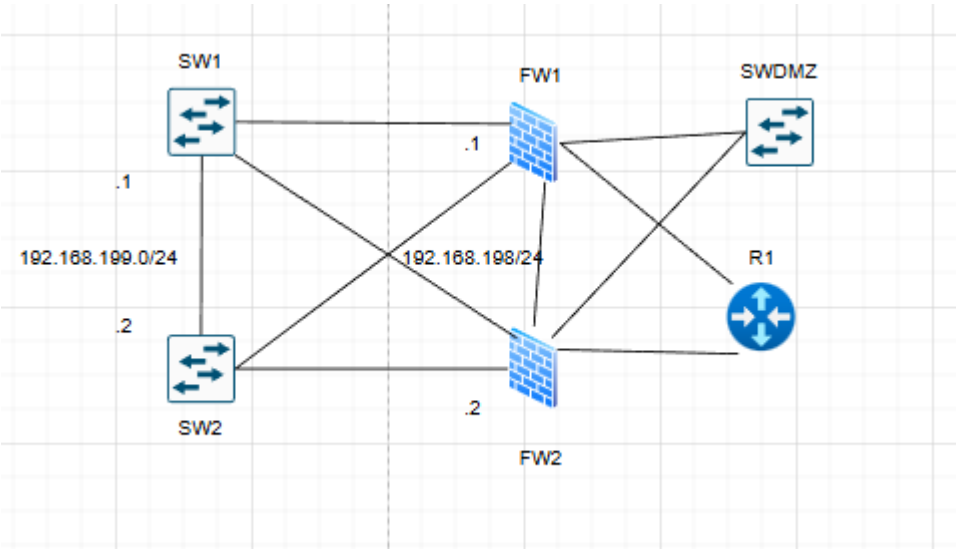


Figure 3 : Schéma explicatif de la redondance des équipements

Le même fonctionnement s'applique pour les serveurs qui ont 2 interfaces réseau mais qui sont "logiquement fusionnée" afin de répondre sous la même adresse IP

Cela permet dans un cas de coupure, de panne ou de cyberattaque sur un des équipements importants, de pouvoir assurer la continuité de la production.

3.6.3 Protection physique des locaux et équipements

L'accès aux infrastructures sensibles est strictement contrôlé par un verrouillage physique des salles serveurs et des baies de brassage, réservé au seul personnel autorisé.

La disponibilité électrique est sécurisée par des onduleurs pilotés permettant une extinction propre en cas de coupure prolongée, tandis que les prises réseaux des zones publiques sont désactivées ou sécurisées pour empêcher toute connexion illégitime au réseau interne.

3.7 Synthèse des risques et Plan de remédiation (Bonnes pratiques)

L'audit initial a mis en évidence une exposition critique liée à l'absence de cloisonnement, des droits administrateurs excessifs et une gestion obsolète des mots de passe.

Le plan de remédiation déployé transforme cette posture réactive en une défense proactive par la mise en œuvre de la segmentation VLAN, du principe de moindre privilège et d'une surveillance centralisée, alignant ainsi le système d'information de XANADU sur les standards de l'ANSSI et garantissant la confidentialité, l'intégrité et la disponibilité des données.

4. Filtrage

4.1 Principes directeurs de la sécurité périmétrique

4.1.1 Principe du "Block All" et moindre privilège

La sécurité périmétrique de XANADU repose sur une politique de refus par défaut stricte appliquée sur l'ensemble des interfaces des pare-feux PfSense.

Contrairement à une approche permissive, tout flux réseau qui n'est pas explicitement autorisé par une règle est silencieusement bloqué et journalisé.

Cette logique de "Block All" s'applique aussi bien aux connexions entrantes depuis Internet qu'aux communications transversales entre les VLANs internes, garantissant ainsi que seule la communication strictement nécessaire au métier est possible.

4.1.2 Gestion des objets et groupes d'adresses

Afin de garantir la maintenabilité de la configuration et de réduire les erreurs humaines lors des modifications futures, aucune adresse IP brute n'est utilisée directement dans les règles de filtrage.

L'ensemble des hôtes, réseaux et ports sont définis sous forme d'Alias (Objets) dans PfSense.

Cette abstraction permet de modifier l'adresse IP d'un serveur critique comme le contrôleur de domaine sans avoir à réécrire la centaine de règles de sécurité qui y font référence.

4.2 Matrice de flux : Site "ATLANTIS" (Siège)

Voir annexe 8.2

Les matrices de flux concernent les firewalls PfSense, mais une 1ère restriction de flux est faite via les ACLs des switchs afin de pouvoir alléger la charge des firewalls contre les communications du LAN (ex: VLAN 10 vers VLAN 100 n'a pas besoin d'aller jusqu'au firewall pour être filtré).

Les règles autorisées par le firewall sont également autorisées pour le switch afin que ces derniers puissent passer par le PfSense.

4.2.1 Filtrage Inter-VLANs (Segmentation interne)

Le cœur de la politique de sécurité interne réside dans le cloisonnement des services.

Les règles ci-dessous illustrent la logique appliquée : les utilisateurs peuvent accéder aux services d'infrastructure (DNS, AD) et aux applicatifs métiers (ERP Web), mais toute communication directe entre deux postes de travail de VLANs différents est interdite pour bloquer la propagation latérale des vers et ransomwares.

4.2.2 Règles d'accès vers la DMZ

L'architecture impose une vérification de la validation des flux. Le trafic venant d'Internet traverse le pare-feu frontal pour atteindre la DMZ, mais ne peut pas rebondir vers le réseau interne (LAN) sauf exceptions strictes.

Actuellement, la DMZ héberge les points de terminaison VPN, isolant ainsi le processus d'authentification externe du cœur du réseau.

Le pare-feu interne refuse par défaut toute initiation de connexion venant de la DMZ vers le LAN.

4.2.3 Protection des interfaces WAN (Publiques)

L'interface WAN connectée au routeur R1 est la zone la plus exposée. La configuration applique un blocage total des flux entrants non sollicités.

Seuls les protocoles de tunnels sécurisés nécessaires à l'interconnexion des sites et au télétravail sont autorisés à franchir cette barrière.

Ainsi, la politique “Block All” protège correctement les interfaces exposées au public.

4.3 Matrice de flux : Site "SPRINGFIELD" (Distant)

La politique de sécurité du site distant est un miroir de celle du siège, adaptée aux spécificités locales du Laboratoire.

Le VLAN LABO (80) est soumis à des restrictions supplémentaires, interdisant tout accès vers les réseaux administratifs locaux.

Les flux inter-sites transitant par le tunnel MPLS sont filtrés à l'entrée et à la sortie du tunnel, garantissant que seule la réplication Active Directory et les sauvegardes traversent le lien WAN.

4.4 Protection spécifique des services critiques

4.4.1 Flux Active Directory et DNS (AD DS)

La sécurisation de l'Active Directory est prioritaire.

Les règles de pare-feu interdisent aux postes clients d'interroger directement des serveurs DNS publics (tels que 8.8.8.8), forçant ainsi l'utilisation du serveur DNS interne pour la résolution de noms et le filtrage des requêtes malveillantes.

De même, l'accès aux contrôleurs de domaine est restreint aux seuls ports nécessaires à l'authentification et aux GPO, bloquant systématiquement les tentatives de connexion administrative (RDP, WinRM) provenant des VLANs utilisateurs.

4.4.2 Accès aux bases de données et applicatifs métier

L'architecture 3-tiers de l'ERP impose un cloisonnement strict de la base de données PostgreSQL.

Le port TCP 5432 du serveur SRV-LN3 n'est accessible que depuis le serveur applicatif local ou le VLAN de management.

Aucune connexion directe à la base de données n'est permise depuis les postes utilisateurs ou depuis le VPN, obligeant les flux à passer par l'interface Web HTTPS dûment sécurisée et journalisée.

5. Automatisation et Scripts d'administration

5.1 Stratégie d'automatisation et langage retenu (PowerShell/Bash)

Dans le cadre de la modernisation du système d'information de XANADU, l'automatisation des tâches d'administration s'impose comme un pilier fondamental pour assurer la cohérence, la traçabilité et l'efficacité opérationnelle des processus de gestion.

Cette stratégie repose sur une approche rigoureuse guidée par plusieurs principes directeurs essentiels. Tout d'abord, la modularité est privilégiée à travers la création de fonctions réutilisables, ce qui permet d'optimiser le code et d'en faciliter la maintenance.

La sécurité constitue également un prérequis absolu, matérialisé par la validation systématique des privilèges administrateur avant l'exécution de tout script afin de prévenir les actions non autorisées.

Par ailleurs, la robustesse des développements est garantie par une gestion structurée des erreurs, utilisant des blocs de type try/catch associés à des messages explicites pour gérer les exceptions sans interrompre brutalement les services.

La traçabilité est assurée par la journalisation des opérations critiques, offrant ainsi une piste d'audit fiable. L'ensemble des scripts est conçu dans le strict respect de la conformité organisationnelle et de l'architecture multi-sites spécifique aux entités ATLANTIS et SPRINGFIELD.

Enfin, une attention particulière est portée à la documentation intégrée ; chaque script est abondamment commenté et accompagné d'une documentation technique détaillée pour en expliquer le fonctionnement et simplifier la maintenance future.

Les scripts et les documentations de chaque script sont tous disponible sur le github dans le dossier Scripts.

5.2 Scripts de gestion des Identités et de l'Annuaire

5.2.1 Script 1 : user_functions.ps1 - Bibliothèque de fonctions communes

Objectif : Centraliser les fonctions réutilisables pour éviter la duplication de code et garantir la cohérence des opérations.

Fonctions principales :

Fonction	Description
Get-UniqueUsername	Génère un nom d'utilisateur unique en ajoutant un compteur si nécessaire (ex : j.dupont, j.dupont2, j.dupont3)
Get-UniqueFullName	Génère un nom complet unique dans une OU spécifique pour éviter les conflits
New-GenericPassword	Génère un mot de passe temporaire selon le format : Première_lettre_majuscule + nom_utilisateur + année + ! (ex : Jdupont2025!)

Justification technique : Cette approche modulaire permet de maintenir une cohérence dans la génération des identifiants et mots de passe tout en facilitant les évolutions futures. La fonction de génération de mot de passe respecte les exigences de complexité tout en restant mémorisable pour les utilisateurs lors de leur première connexion.

5.2.2 Script 2 : create_user.ps1 - Création et provisioning des utilisateurs

L'objectif principal du script create_user.ps1 est d'automatiser intégralement le processus de provisioning des comptes utilisateurs au sein de l'annuaire Active Directory, en assurant une gestion rigoureuse des sites géographiques et une attribution des droits fondée sur le modèle RBAC.

Le fonctionnement du programme débute par une interface interactive invitant l'opérateur à sélectionner le site de rattachement, tel qu'ATLANTIS ou SPRINGFIELD, ainsi que le service concerné.

Afin de garantir l'intégrité des données de l'annuaire, le script intègre un mécanisme de validation des entrées qui restreint la saisie des noms et prénoms aux seuls caractères alphabétiques. Une fois ces informations validées, l'outil génère automatiquement les identifiants de connexion selon un format standardisé combinant l'initiale du prénom et le nom complet, tout en configurant l'adresse de messagerie sur le domaine @xanadu.com.

L'objet utilisateur est ensuite instancié précisément dans l'Unité d'Organisation adéquate, en respectant l'arborescence hiérarchique définie par le service et la localisation au sein du domaine xanadu.local.

Outre le placement structurel, le script assure une distinction des niveaux de privilèges entre les utilisateurs standards et les administrateurs.

Enfin, le processus se conclut par l'attribution interactive des permissions d'accès aux ressources fichiers, telles que la lecture, l'écriture ou la modification, en s'appuyant sur l'ajout de l'utilisateur aux groupes Shadow correspondants.

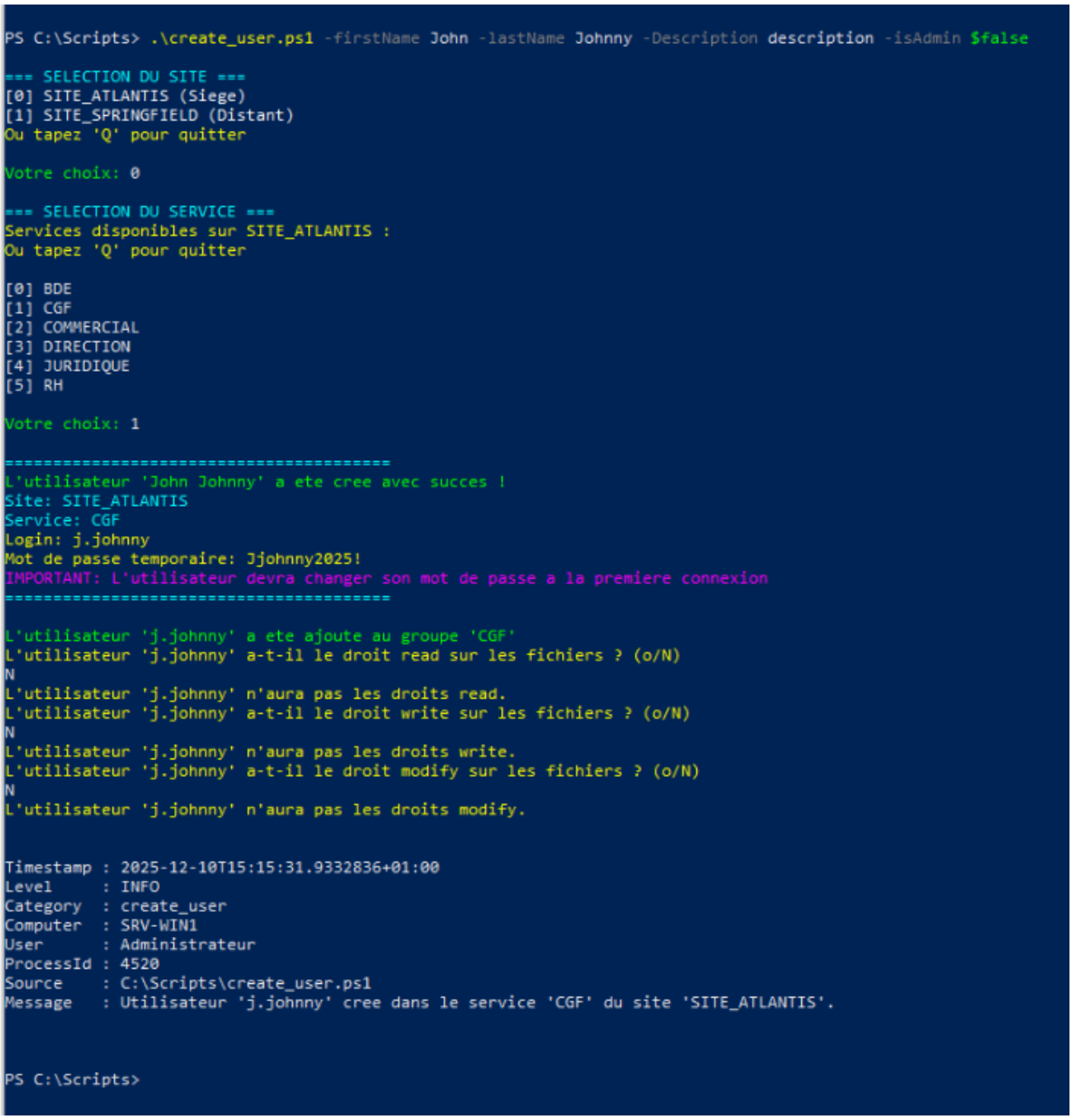


Figure X : Création d'un utilisateur

Architecture des groupes de sécurité

Le script implémente une stratégie de groupes Shadow pour la gestion granulaire des permissions :

Groupe	Permissions NTFS
Shadow_r_SERVICE	Lecture seule (Read & Execute, List folder contents, Read)
Shadow_w_SERVICE	Écriture (création de fichiers uniquement, pas de suppression)
Shadow_m_SERVICE	Modification complète (Read, Write, Modify, Delete)
Admin_SERVICE	Possède les 3 rôles Shadow

Exemple d'utilisation :

.\create_user.ps1 -FirstName "Marie" -LastName "Martin" -Description "Responsable Comptabilité" -isAdmin $false

Justification technique : L'approche basée sur les groupes Shadow permet de respecter le principe de moindre privilège tout en facilitant l'administration. La séparation entre comptes utilisateurs et comptes administrateurs (via le paramètre isAdmin) renforce la sécurité en limitant l'utilisation de privilèges élevés aux seules tâches d'administration.

5.2.3 Script 3 : create_user_info.ps1 - Création de comptes pour le département INFORMATIQUE

Objectif : Créer automatiquement une paire de comptes (utilisateur standard + compte administrateur) pour les membres du département informatique, conformément aux bonnes pratiques de séparation des privilèges.

Fonctionnalités principales

- Création duale automatisée : génère simultanément un compte utilisateur (prénom.nom) et un compte administrateur (adm_prénom.nom)

- Placement automatique dans l'OU dédiée : OU=Users,OU=INFO,OU=SITE_ATLANTIS
- Attribution des groupes appropriés : INFO pour les deux comptes, et Admins pour le compte administrateur
- Génération de mots de passe distincts pour chaque compte selon la politique définie
- Affichage structuré des informations de connexion pour transmission sécurisée

Exemple d'utilisation :

.\create_user_info.ps1 -FirstName "Thomas" -LastName "Dubois" -Description "Administrateur Système"

Résultat attendu :

- Compte utilisateur : t.dubois@xanadu.com avec mot de passe Tdubois2025!
- Compte admin : adm_t.dubois@xanadu.com avec mot de passe Admtdubois2025!

Justification technique : Cette séparation des comptes suit les recommandations de l'ANSSI pour les comptes à privilèges. L'administrateur utilisera son compte standard pour les tâches quotidiennes et son compte administrateur uniquement pour les opérations nécessitant des privilèges élevés, réduisant ainsi la surface d'attaque en cas de compromission.

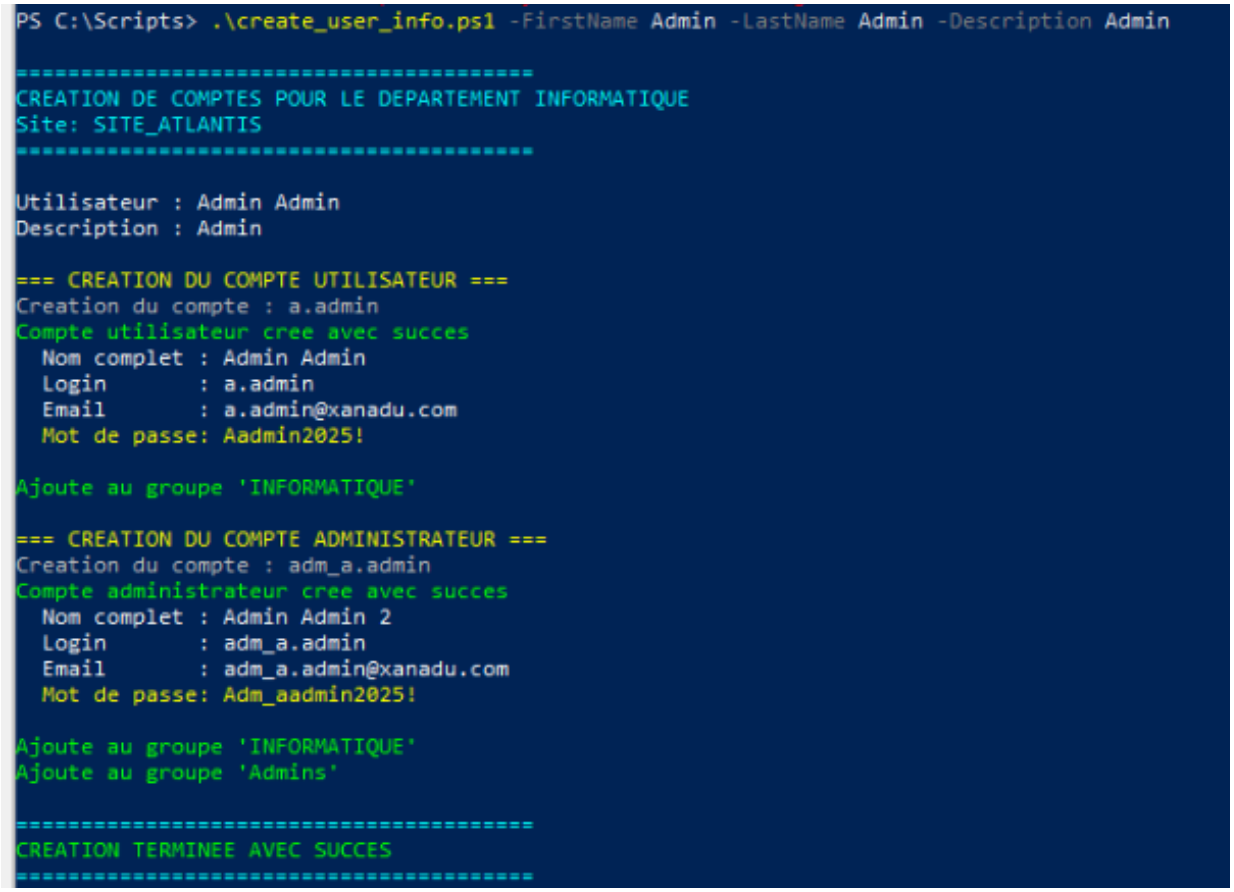


Figure 4 : Création des comptes utilisateurs informatique

5.2.4 Script 4 : disable_user.ps1 - Désactivation et mise en quarantaine d'utilisateurs

Objectif : Désactiver un compte utilisateur et le déplacer vers l'OU de quarantaine appropriée selon son site d'origine, conformément aux procédures de départ ou de suspension.

Fonctionnalités principales

• Détection automatique du site d'origine (ATLANTIS ou SPRINGFIELD) à partir du Distinguished Name

•Vérifications de sécurité multiples : existence du compte, détection de doublons, état actuel

•Gestion des conflits avec proposition de renommage automatique (timestamp) en cas d'utilisateur existant dans la quarantaine

•Confirmations interactives avant opérations critiques pour éviter les erreurs

•Désactivation du compte et déplacement vers l'OU QUARANTINE du site concerné

•Affichage détaillé des informations avant/après pour traçabilité

Exemple d'utilisation :

.\disable_user.ps1 -UserLogin "m.martin"

Justification technique : La mise en quarantaine permet de conserver les comptes désactivés pendant une période définie sans polluer les OU actives, tout en facilitant une éventuelle réactivation. Le système de détection de site garantit que les comptes restent dans leur périmètre administratif d'origine, respectant ainsi l'architecture multi-sites de XANADU.

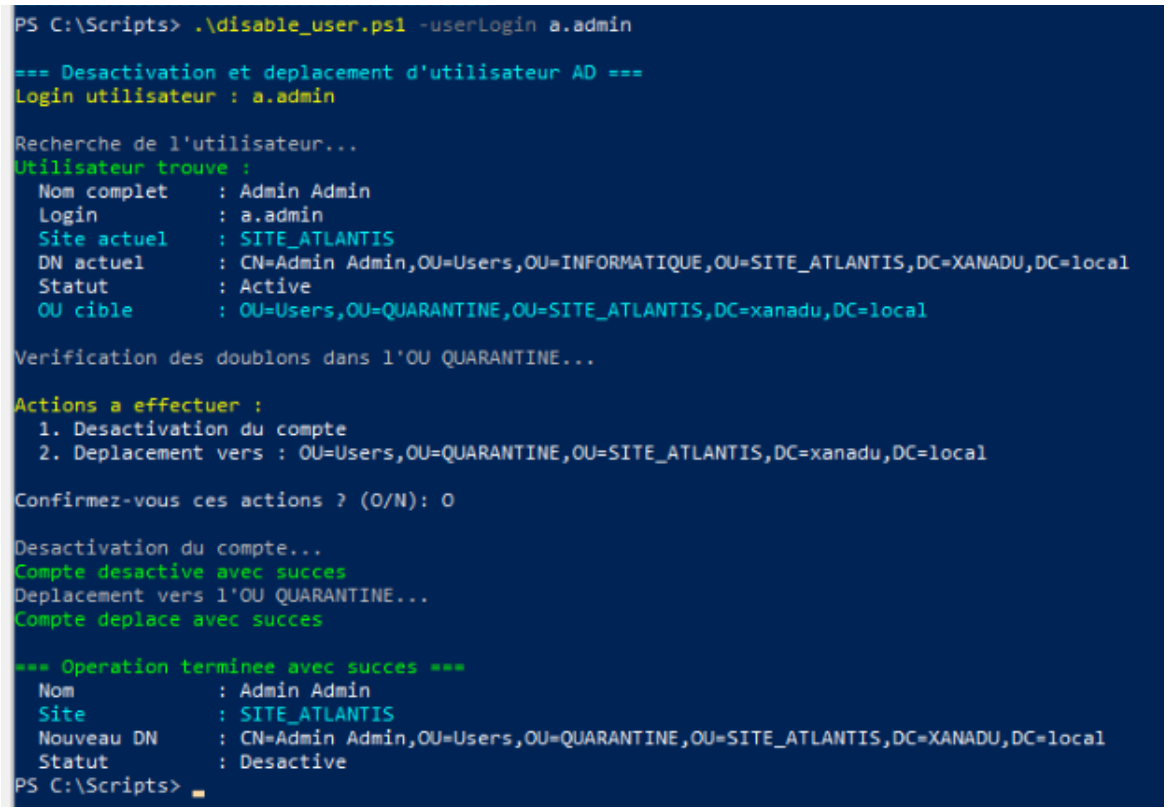


Figure 5 : Désactivation d'un utilisateur

5.2.5 Script 5 : auto_quarentine.ps1 - Quarantaine automatique des comptes inactifs

Objectif : Identifier et traiter automatiquement les comptes utilisateurs inactifs depuis plus de 60 jours pour maintenir l'hygiène de l'annuaire et réduire la surface d'attaque.

Fonctionnalités principales

- Détection automatique des comptes inactifs basée sur le LastLogonDate (seuil : 60 jours)
- Exclusions intelligentes des comptes système (Administrator, Guest, krbtgt) et des comptes de service

- Exclusion des OU sensibles pour éviter de traiter des comptes déjà en quarantaine ou ayant un statut particulier
- Traitement par lot avec rapport détaillé (nombre de succès/échecs)
- Désactivation et déplacement automatiques sans intervention manuelle
- Affichage d'un tableau récapitulatif avant traitement pour visibilité

Configuration du script

Paramètre	**Valeur par défaut**
InactiveDays	60 jours (configurable selon la politique de sécurité)
targetOU	OU=Users,OU=Quarentine,DC=xanadu,DC=local
excludedUsers	Administrator, Guest, krbtgt
excludedOUs	OU Quarentine et OU ServiceAccounts

Planification :

Ce script doit être planifié via le Planificateur de tâches Windows pour s'exécuter automatiquement :

- Fréquence : Hebdomadaire (chaque lundi à 2h00 par exemple)
- Privilèges : Compte de service avec droits d'administration AD

L'automatisation de la quarantaine des comptes inactifs répond aux exigences de conformité et de sécurité en réduisant le nombre de comptes actifs non utilisés qui pourraient être compromis.

Le seuil de 60 jours représente un équilibre entre sécurité et tolérance pour les absences prolongées (congés, arrêts maladie).

Le système d'exclusion garantit qu'aucun compte critique n'est affecté par erreur.

```
QUARANTAINE AUTOMATIQUE MULTI-SITES
Seuil d'inactivite: 60 jours

SITE: SITE_ATLANTIS
 OU Quarantaine validee
Utilisateurs actifs analyses: 23
Utilisateurs inactifs detectes: 23

Name                SamAccountName LastLogonDate InactiveDays
----                -------------- ------------- ------------
Fatima Benali       f.benali       Jamais        Jamais connecté
Mateo Garcia        m.garcia       Jamais        Jamais connecté
Wei Chen            w.chen         Jamais        Jamais connecté
Elena Popov         e.popov        Jamais        Jamais connecté
Aisha Traore        a.traore       Jamais        Jamais connecté
Lucas Dubois        l.dubois       Jamais        Jamais connecté
Priya Patel         p.patel        Jamais        Jamais connecté
John Smith          j.smith        Jamais        Jamais connecté
Sofia Rossi         s.rossi        Jamais        Jamais connecté
Amir Haddad         a.haddad       Jamais        Jamais connecté
Hiroki Sato         h.sato         Jamais        Jamais connecté
Sarah Connor        s.connor       Jamais        Jamais connecté
Sven Jensen         s.jensen       Jamais        Jamais connecté
ADMIN Sven Jensen   adm_s.jensen   Jamais        Jamais connecté
Kenza Diop          k.diop         Jamais        Jamais connecté
ADMIN Kenza Diop    adm_k.diop     Jamais        Jamais connecté
youcef afane        y.afane        Jamais        Jamais connecté
youcef afane        y.afane2       Jamais        Jamais connecté
Antonin AR. Rabatel anto           Jamais        Jamais connecté
matheo fafa         m.fafa         Jamais        Jamais connecté
jojo jiji           j.jiji         Jamais        Jamais connecté
John Johnny         j.johnny       Jamais        Jamais connecté
Admin Admin 2       adm_a.admin    Jamais        Jamais connecté

Traitement: Fatima Benali...
   Compte desactive: Fatima Benali
   Compte deplace en quarantaine: Fatima Benali
Traitement: Mateo Garcia...
   Compte desactive: Mateo Garcia
   Compte deplace en quarantaine: Mateo Garcia
Traitement: Wei Chen...
   Compte desactive: Wei Chen
   Compte deplace en quarantaine: Wei Chen
Traitement: Elena Popov...
   Compte desactive: Elena Popov
   Compte deplace en quarantaine: Elena Popov
Traitement: Aisha Traore...
   Compte desactive: Aisha Traore
   Compte deplace en quarantaine: Aisha Traore
Traitement: Lucas Dubois...
   Compte desactive: Lucas Dubois
   Compte deplace en quarantaine: Lucas Dubois
Traitement: Priya Patel...
   Compte desactive: Priya Patel
   Compte deplace en quarantaine: Priya Patel
Traitement: John Smith...
   Compte desactive: John Smith
   Compte deplace en quarantaine: John Smith
Traitement: Sofia Rossi...
   Compte desactive: Sofia Rossi
   Compte deplace en quarantaine: Sofia Rossi
Traitement: Amir Haddad...
   Compte desactive: Amir Haddad
   Compte deplace en quarantaine: Amir Haddad
Traitement: Hiroki Sato...
   Compte desactive: Hiroki Sato
   Compte deplace en quarantaine: Hiroki Sato
Traitement: Sarah Connor...
   Compte desactive: Sarah Connor
   Compte deplace en quarantaine: Sarah Connor
Traitement: Sven Jensen...
   Compte desactive: Sven Jensen
   Compte deplace en quarantaine: Sven Jensen
Traitement: ADMIN Sven Jensen...
   Compte desactive: ADMIN Sven Jensen
   Compte deplace en quarantaine: ADMIN Sven Jensen
Traitement: Kenza Diop...
   Compte desactive: Kenza Diop
```

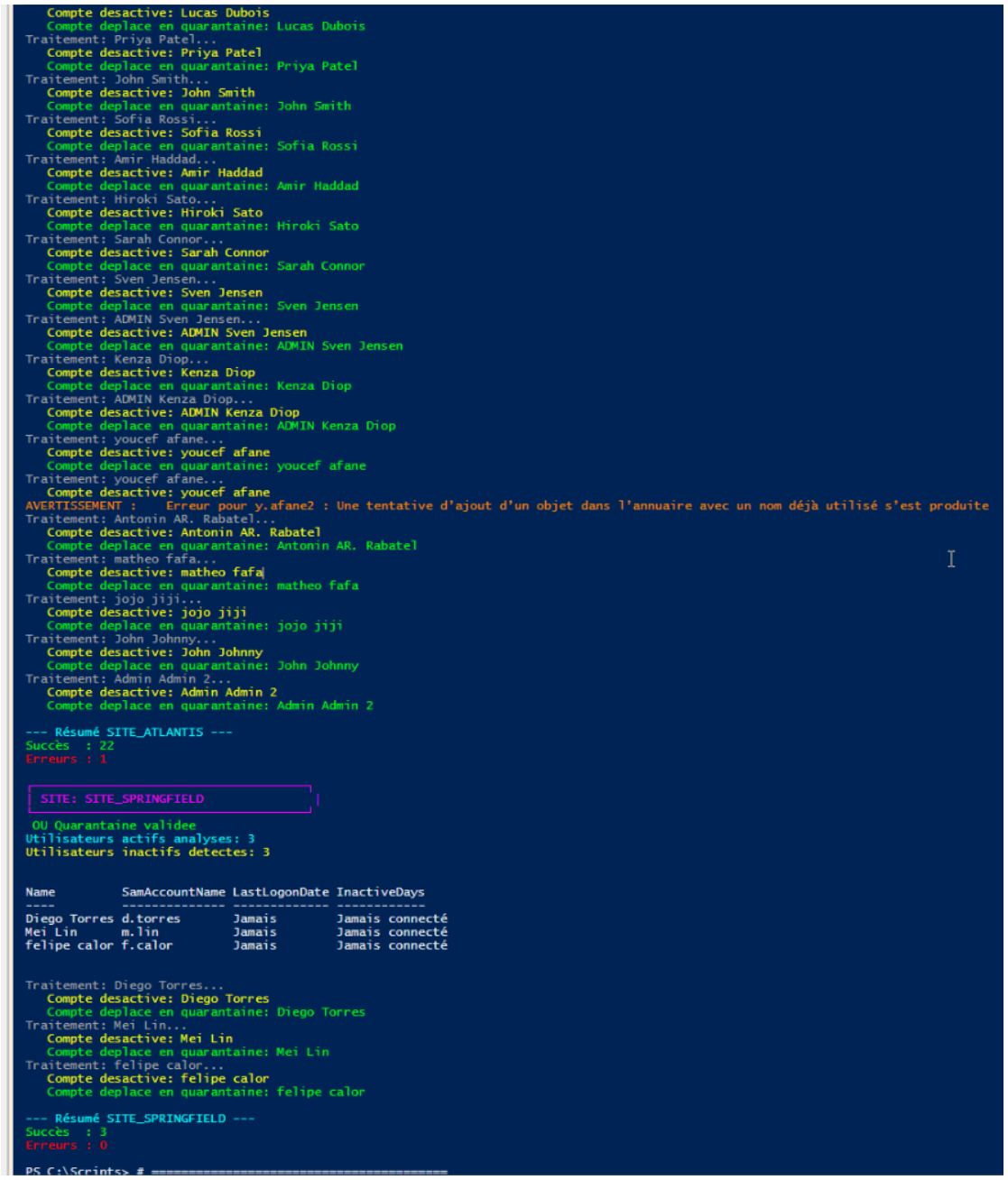


Figure 6 : Désactivation automatique des utilisateurs inactifs

5.3 Scripts de gestion de sauvegarde

Ces six scripts suivants constituent ensemble un plan de sauvegarde complet et cohérent : backup_file est le cœur du dispositif, il réalise les sauvegardes locales selon les politiques définies; scheduler_backup automatise leur exécution (type, fréquence, criticité) pour garantir la régularité sans dépendre d'une action humaine; externalize_backups envoie les sauvegardes vers un site distant, ce qui protège contre la perte de données en cas de sinistre sur le site principal; purge_backups applique les règles de rétention (locales / externalisées, RGPD, criticité) pour éviter la saturation du stockage tout en conservant l'historique nécessaire; restore_file permet, en cas d'incident, de restaurer rapidement un backup complet ou des fichiers ciblés, ce qui est la finalité même de la sauvegarde; enfin alert_backup surveille les logs de ces opérations et remonte automatiquement les erreurs par mail, ce qui assure la supervision et la réactivité en cas de problème.

5.3.1 Script de sauvegarde locale

Le script backup_file.ps1 effectue des sauvegardes locales de répertoires de données vers C:\Backups\Local avec 3 types de sauvegarde :

- Sauvegarde complète (full) : copie tous les fichiers des sources.
- Sauvegarde différentielle (dif) : copie uniquement les fichiers modifiés depuis la dernière sauvegarde complète.
- Sauvegarde incrémentielle (inc) : copie uniquement les fichiers modifiés depuis la dernière sauvegarde (full/dif/inc).

Fonctionnalités principales :

- Gestion par policy (Critical / Important / Standard) : séparation des sauvegardes et des métadonnées par criticité.
- Préservation de l'arborescence des dossiers sources.
- Fichier de métadonnées JSON par policy pour suivre la dernière sauvegarde complète et la dernière sauvegarde tout court.
- Logs dédiés par policy et type de sauvegarde.

- Force automatiquement une sauvegarde complète si aucune sauvegarde de référence n'existe encore.

Nom	Type	Obligatoire	Valeurs Possibles	Description
Type	String	Oui	full, dif, inc	Type de sauvegarde à exécuter (complète, différentielle ou incrémentielle).
IncludesFile	String	Oui	Chemin vers un fichier texte existant	Fichier listant les chemins sources à sauvegarder (un chemin absolu par ligne).
Policy	String	Oui	Critical, Important, Standard	Niveau de criticité. Sert à isoler la sauvegarde dans un sous-dossier dédié et le log associé.

Chemins nécessaires / générés du script de sauvegarde

Les sauvegardes locales sont centralisées sous *C:\Backups\Local*. Pour chaque policy (Critical, Important, Standard), le script utilise un sous-dossier dédié, par exemple *C:\Backups\Local\Critical*. À chaque exécution, il crée un nouveau dossier de sauvegarde dans ce répertoire, nommé selon le format *{Policy}_{Type}_{Horodatage}_{ID}* (par exemple *Critical_full_20250206_143000_AB12CD*), dans lequel il recrée l'arborescence des différentes sources listées dans le fichier IncludesFile.

Le script s'appuie sur un fichier texte externe (paramètre IncludesFile) qui contient, ligne par ligne, les chemins sources à sauvegarder (par exemple *C:\Users\Alexandre\Documents* ou *D:\Projects*). Ces chemins doivent exister et être accessibles en lecture.

Pour le suivi de l'historique, un fichier de métadonnées backup_state.json est maintenu par policy dans le dossier correspondant, par exemple *C:\Backups\Local\Critical\backup_state.json*. Ce fichier enregistre notamment la date de la dernière sauvegarde complète et de la dernière sauvegarde tout type confondu. Enfin, la journalisation est centralisée dans *C:\Backups\Local\Logs*, où le script écrit un fichier de log par combinaison policy / type de sauvegarde, par exemple Backup_Critical_full.log.

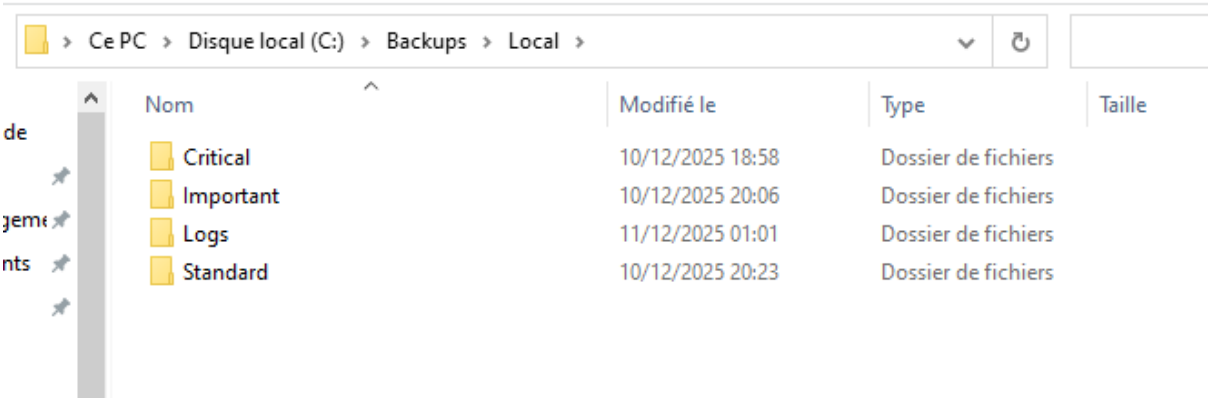


Figure 7 : Path des sauvegardes locales

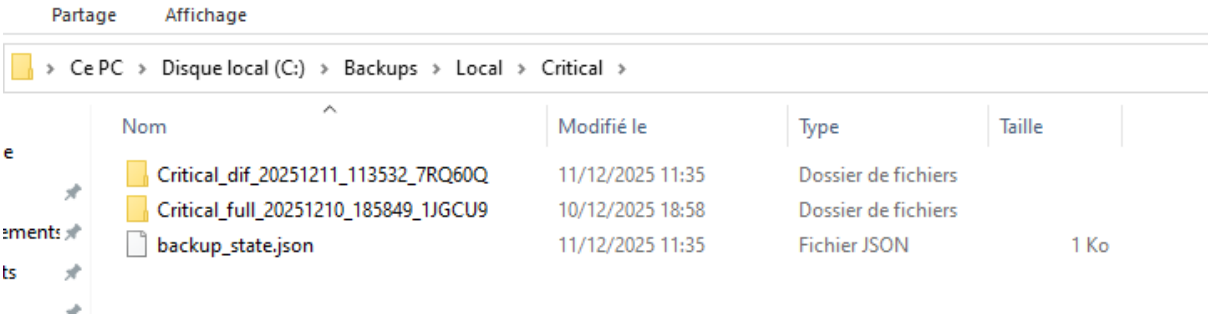


Figure 8 : Sauvegardes critiques

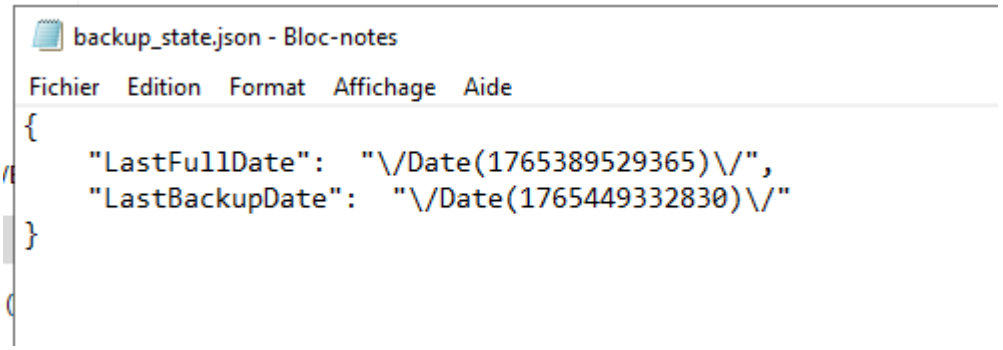


Figure 9 : Fichier backup_state.json

5.3.2 Script de restauration

Le script restore_file.ps1 permet de restaurer des sauvegardes produites par le système XANADU à partir du dépôt de backups local ou externalisé.

Il propose plusieurs usages :

- Restauration complète d'un backup
- Restauration ciblée de certains fichiers en fonction d'un terme de recherche,
- Simple affichage du contenu d'un backup
- Sélection interactive d'un backup lorsque aucun nom n'est fourni. Il reconstruit l'arborescence d'origine dans le répertoire de destination, ne remplace jamais un fichier existant (il renomme en ajoutant un suffixe horodaté) et journalise l'ensemble des opérations dans un fichier de log de restauration.

Tableau des paramètres

Nom	Type	Obligatoire	Valeurs possibles	Description
BackupRoot	String	Non	Chemin vers la racine des sauvegardes	Racine des backups XANADU. Par défaut C:\Backups, contenant les sous-dossiers Local/External.
Location	String	Non	Local, External	Emplacement de stockage à cibler. Si omis, le script recherche les backups dans les deux emplacements.
BackupLabel	String	Non	Nom du backup (ex. full_20241204_135954_A7X9Q2)	Identifiant du backup à restaurer. Si omis, le script liste tous les backups trouvés et propose un choix interactif.

TargetPath	String	Non	Chemin de destination	Répertoire de restauration des fichiers. Par défaut C:\Restore. Créé automatiquement s'il n'existe pas.
FileToRestore	String	Non	Terme de recherche	Filtre de restauration ciblée : seuls les fichiers dont le nom contient ce terme sont restaurés.
List	Switch	Non	—	Active le mode "liste uniquement" : affiche le contenu du backup sans rien restaurer.

Chemins nécessaires / générés

Le script suppose que les sauvegardes sont organisées sous une racine de type BackupRoot, par défaut *C:\Backups*. Sous cette racine, il s'attend à trouver au moins un répertoire d'emplacement (Local ou External), puis les sous-dossiers de politique (par exemple Critical, Important, Standard), à l'intérieur desquels se trouvent les dossiers de backup créés par le script de sauvegarde (backup_file.ps1). Concrètement, un backup typique se trouve donc sous un chemin du type *C:\Backups\Local\Critical\Critical_full_20241204_135954_A7X9Q2*, et c'est ce répertoire que le script parcourt pour lire les fichiers à restaurer.

Le seul répertoire qu'il crée de lui-même est le répertoire de destination TargetPath (par défaut C:\Restore) ainsi que son sous-dossier de logs. Lors d'une restauration, tous les fichiers du backup sont recopiés vers ce TargetPath en recréant l'arborescence relative d'origine. Si un fichier existe déjà à l'emplacement de destination, il est renommé automatiquement en ajoutant un suffixe horodaté pour éviter tout écrasement.

Parallèlement, le script consigne toutes ses actions dans un fichier de log unique situé sous TargetPath\Logs\Restore.log, qui est créé au besoin à la première exécution.

```
PS C:\Users\Administrateur\Documents\script> .\backup_file.ps1 -Type dif
PS C:\Users\Administrateur\Documents\script> .\restore_file.ps1
1) Critical_dif_20251211_113532_7RQ60Q [Local] (Policy: Critical)
2) Critical_full_20251210_185849_1JGCU9 [Local] (Policy: Critical)
3) Important_full_20251210_191403_HBTP77 [Local] (Policy: Important)
4) Important_full_20251210_195601_E2BMV3 [Local] (Policy: Important)
5) Important_full_20251210_195701_7SO0V0 [Local] (Policy: Important)
6) Important_full_20251210_195801_QOXYGW [Local] (Policy: Important)
7) Important_full_20251210_195901_M3K5IN [Local] (Policy: Important)
8) Important_full_20251210_200002_WMZO68 [Local] (Policy: Important)
9) Important_full_20251210_200102_FWQTIT [Local] (Policy: Important)
10) Important_full_20251210_200201_PPTR1Q [Local] (Policy: Important)
11) Important_full_20251210_200301_M8FJGR [Local] (Policy: Important)
12) Important_full_20251210_200401_6VAKZ5 [Local] (Policy: Important)
13) Important_full_20251210_200501_NPACZL [Local] (Policy: Important)
14) Important_full_20251210_200601_N3KMC9 [Local] (Policy: Important)
15) Standard_full_20251210_185900_5ORS14 [Local] (Policy: Standard)
16) Standard_full_20251210_201402_NDEE5G [Local] (Policy: Standard)
17) Standard_full_20251210_201502_116DKO [Local] (Policy: Standard)
18) Standard_full_20251210_202101_UJCCCA [Local] (Policy: Standard)
19) Standard_full_20251210_202201_GG1HQU [Local] (Policy: Standard)
20) Standard_full_20251210_202301_39WVU7 [Local] (Policy: Standard)
SÃ©lectionner un numÃ©ro: 6
PS C:\Users\Administrateur\Documents\script>
```

Figure 10 : Sélection interactive d'un backup

```
  .\restore_file.ps1  -BackupLabel  Important_full_20251210_195801_QOXYGW
-List
```

```
PS C:\Users\Administrateur\Document
Local\Client\client.txt
Local\Direction\direction.txt
PS C:\Users\Administrateur\Document
```

Figure 11 : Listing d'une sauvegarde

```
.\restore_file.ps1   -BackupLabel   Important_full_20251210_195801_QOXYGW
-FileToRestore direction.txt
```

```
[2025-12-11 11:57:12 - 161600] [INFO] Liste du backup affichée.
[2025-12-11 12:01:24 - BP0UNN] [INFO] Backup spécifié : Important_full_20251210_195801_QOXYGW (Policy : Important)
[2025-12-11 12:01:24 - BP0UNN] [INFO] Début de la restauration depuis Important_full_20251210_195801_QOXYGW
[2025-12-11 12:01:24 - BP0UNN] [INFO] Mode : restauration ciblée du fichier 'direction.txt'
[2025-12-11 12:01:24 - BP0UNN] [INFO] Fichier restauré : C:\Restore\Local\Direction\direction_2025-12-11_12-01-24_restore.txt
[2025-12-11 12:01:24 - BP0UNN] [INFO] Restauration ciblée terminée.
```

Figure 12 : Commande et Logs d'un fichier unique

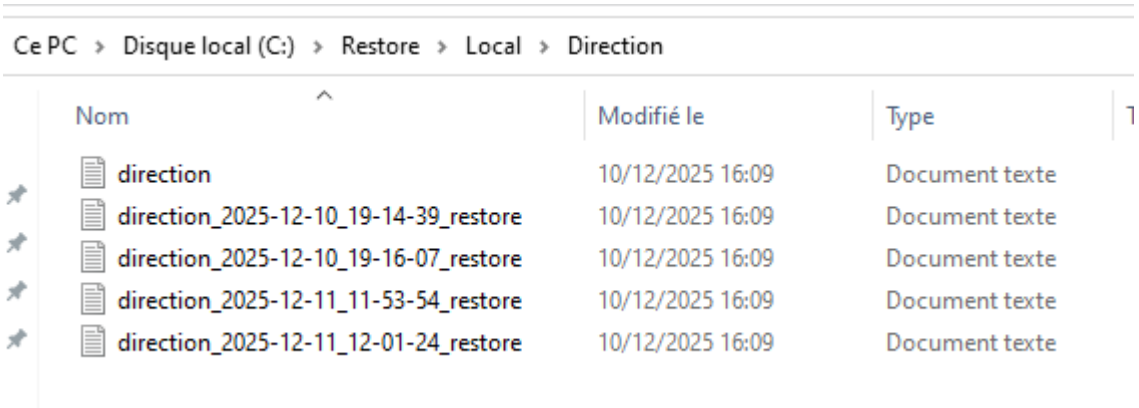


Figure 13 : Dossier de restauration du fichier unique

5.3.3 Script d'externalisation des sauvegardes

Le script externalize_backups.ps1 externalise automatiquement les sauvegardes locales XANADU vers un serveur distant via SFTP, en s'appuyant sur la bibliothèque WinSCP .NET. Il parcourt les dossiers de sauvegarde locaux, détecte les backups par type (full, dif, inc), ne sélectionne que ceux qui n'ont pas encore été externalisés (grâce à un fichier d'état JSON), puis les transfère récursivement vers un répertoire racine sur le serveur distant. Il ajoute un suffixe *_external* au nom du backup côté distant, maintient un historique détaillé des transferts (dates, statut, chemin distant) et produit des logs complets, avec la possibilité de fonctionner en mode simulation (DryRun) sans aucun transfert réel.

Tableau des paramètres

Nom	Type	Obligatoire	Valeurs possibles	Description
Type	String	Non	full, dif, inc, all	Filtre sur le type de sauvegarde à externaliser. all (par défaut) traite tous les types.
BackupRoot	String	Non	Chemin vers les sauvegardes locales	Racine des sauvegardes locales à externaliser. Par défaut C:\Backups\Local.
DryRun	Switch	Non	—	Active le mode simulation : aucune connexion SFTP ni transfert, le script indique seulement ce qu'il ferait.

Chemins nécessaires / générés

Le script considère comme source un répertoire racine de sauvegardes locales, BackupRoot, qui pointe par défaut sur C:\Backups\Local. Sous ce dossier se trouvent les répertoires de backups générés par le script de sauvegarde (de type full_*, dif_*, inc_*), que le script parcourt pour identifier ceux qui doivent être externalisés. Il maintient à ce niveau un fichier d'état external_state.json, également stocké sous BackupRoot, qui mémorise pour chaque backup déjà transféré sa première date d'envoi, sa dernière date d'envoi, son statut et le chemin distant associé, ce qui permet de ne plus renvoyer les mêmes données.

La journalisation locale est réalisée dans un sous-dossier Logs situé sous BackupRoot (par exemple C:\Backups\Local\Logs) avec un fichier principal Externalize.log et, en complément, un log détaillé de la bibliothèque WinSCP (Externalize_WinSCP.log) utilisé pour le diagnostic réseau. Côté distant, tous les backups sont envoyés sous un répertoire racine SFTP configuré dans la variable $RemoteBase (par défaut C:\Backups\External dans le script, à

adapter), chaque sauvegarde locale NomBackup étant recopiée dans un dossier de même nom suffixé par *_external* (par exemple *Critical_full_20241211_143022_A7X9Q2_external*). Le chemin vers la bibliothèque WinSCPnet.dll doit enfin correspondre à l'installation WinSCP sur le serveur d'exécution, tel que configuré dans $WinScpDllPath.

5.3.4 Script d'alerte

Le script alert_backup.ps1 analyse les journaux produits par les scripts de sauvegarde, d'externalisation et de restauration XANADU afin de détecter automatiquement des anomalies (erreurs explicites, messages de fin "terminée avec erreurs", mots-clés d'échec ou logs vides). Pour chaque log jugé problématique, il extrait les métadonnées (policy, type de sauvegarde, statut local/externalisé), construit un rapport synthétique (dont les dernières lignes du log concerné) et envoie une alerte par email via le serveur SMTP interne (Poste.io) aux administrateurs. Toutes les analyses et envois sont eux-mêmes tracés dans un fichier Alert.log.

Tableau des paramètres

Nom	Type	Obligatoire	Valeurs possibles	Description
LogsRoot	String	Non	Chemin vers le dossier de logs	Répertoire racine des fichiers de log à analyser. Par défaut *C:\Backups\Local\Logs*.

Chemins nécessaires / générés

Le script s'appuie sur un répertoire de logs centralisé, LogsRoot, qui pointe par défaut sur C:\Backups\Local\Logs. Dans ce dossier se trouvent les fichiers de journalisation produits par les autres scripts de la solution : logs de sauvegarde (*Backup_<Policy>_<Type>.log*), logs d'externalisation (*Backup_<Policy>_<Type>_external.log*), ainsi que le fichier Alert.log dans lequel le script consigne ses propres messages (début d'analyse, anomalies détectées, envois d'emails, éventuels échecs SMTP). Le chemin des logs est le seul paramètre technique requis ; la configuration SMTP (adresse du serveur Poste.io, port, compte d'envoi, mot de passe, liste des destinataires) est définie directement dans les variables globales du

script et doit être adaptée à l'infrastructure de messagerie de l'entreprise avant mise en production.

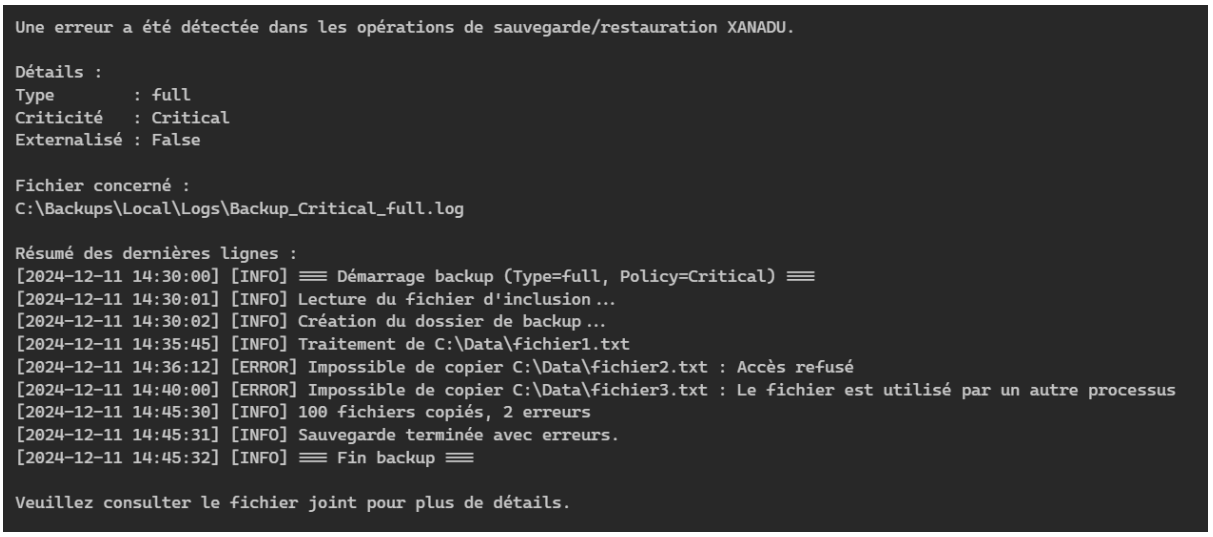


Figure 14 : Exemple de mail d'alerte envoyé

5.3.5 Script de planification des sauvegardes

Le script scheduler_backup.ps1 sert à créer, modifier et gérer des tâches planifiées Windows qui exécutent automatiquement le script de sauvegarde backup_file.ps1. Il traduit une expression CRON simplifiée en déclencheurs Windows (quotidien, hebdomadaire, mensuel ou répétition toutes les X minutes), passe au script de sauvegarde les paramètres nécessaires (-Type, -IncludesFile, -Policy), et applique un préfixe standard XANADU_ à toutes les tâches pour les identifier facilement. Il propose un mode interactif (question/réponse) lorsqu'aucun paramètre n'est fourni et un mode "liste" permettant d'afficher, supprimer ou replanifier les tâches XANADU existantes.

Tableau des paramètres

Nom	Type	Obligatoire	Valeurs possibles	Description
Cron	String	Non	Expression M H DOM MON DOW (CRON simplifiée)	Planification de la tâche (minutes, heures, jour du mois, mois, jour de semaine).
Type	String	Non	full, dif, inc	Type de sauvegarde transmis à backup_file.ps1 via le paramètre -Type.
Includes	String	Non	Chemin de fichier	Fichier liste des sources, transmis à backup_file.ps1 via -IncludesFile.
Policy	String	Non	Critical, Important, Standard, Logs	Criticité transmise à backup_file.ps1 via -Policy. Par défaut Standard.
TaskName	String	Non	Nom logique sans préfixe	Nom "fonctionnel" de la tâche ; le nom réel sera XANADU_{TaskName}. Par défaut backup_file.
List	Switch	Non	—	Active le mode gestion : liste les tâches XANADU_* et permet suppression ou modification du CRON.

Chemins nécessaires / générés

Le script suppose l'existence du script de sauvegarde à un emplacement fixe, configuré dans la variable $BackupScriptPath (par défaut *C:\Users\Administrateur\Documents\script\backup_file.ps1*) ainsi que d'un fichier includes.txt pointé par $DefaultIncludesFile. Ces chemins sont validés avant la création de la tâche et transmis ensuite au planificateur Windows comme arguments de la commande powershell.exe. Toutes les opérations du scheduler (création, suppression, erreurs de validation, conversions CRON) sont journalisées dans le fichier Scheduler.log, stocké dans

le répertoire C:\Backups\Local\Logs, qui est créé automatiquement si nécessaire. Côté système, les tâches planifiées sont enregistrées dans le Planificateur de tâches Windows avec un nom construit à partir du préfixe XANADU_ suivi du nom logique fourni (par exemple XANADU_backup_daily_full), ce qui permet de les retrouver et de les gérer facilement via le paramètre -List ou directement dans la console de planification.

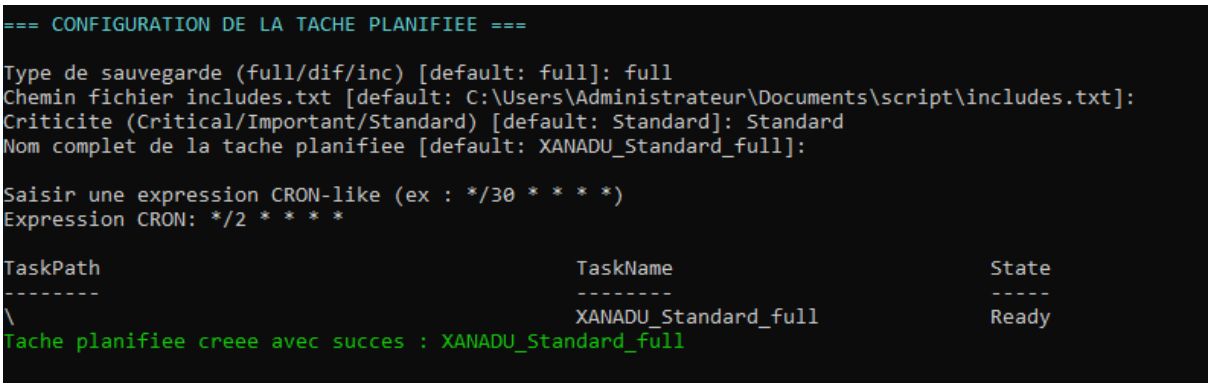


Figure 15 : Configuration d'une sauvegarde planifiée

On peut donc voir qu'on peut faire la configuration de la sauvegarde planifiée de manière interactive.

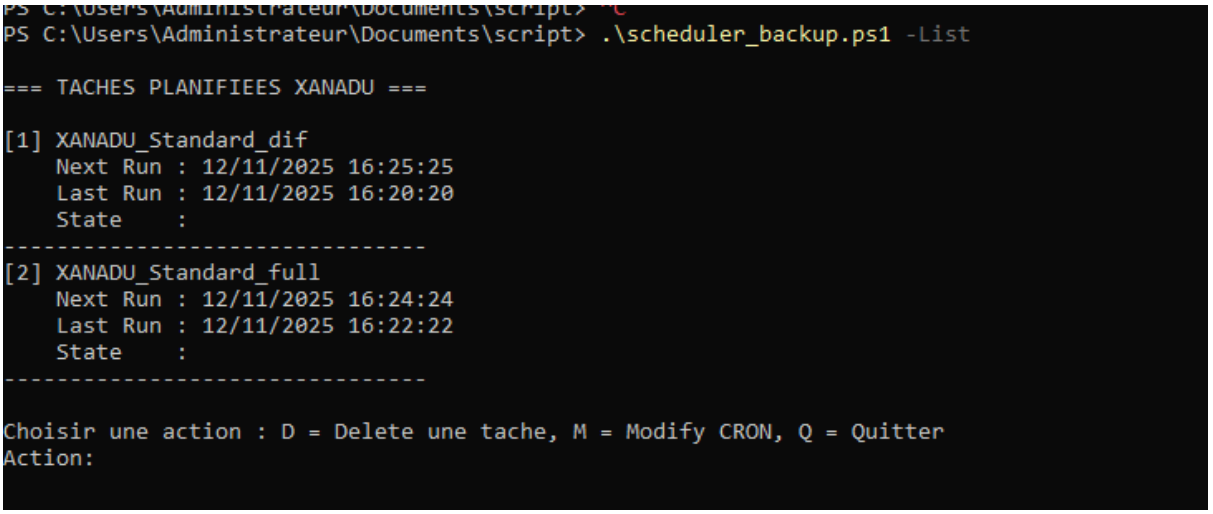


Figure 16 : Listing des sauvegardes planifiées

On peut voir que je peux supprimer ou modifier n'importe quelle sauvegarde planifiée en utilisant l'index.

```
=== TACHES PLANIFIEES XANADU ===

[1] XANADU_Standard_dif
    Next Run : 12/11/2025 16:50:50
    Last Run : 12/11/2025 16:45:45
    State    :
--------------------------------
[2] XANADU_Standard_full
    Next Run : 12/11/2025 16:46:46
    Last Run : 12/11/2025 16:44:44
    State    :
--------------------------------

Choisir une action : D = Delete une tache, M = Modify CRON, Q = Quitter
Action: D
Numero de la tache a supprimer: 1
Suppression de : XANADU_Standard_dif...
Tache supprimee.
PS C:\Users\Administrateur\Documents\script> .\scheduler_backup.ps1 -List

=== TACHES PLANIFIEES XANADU ===

[1] XANADU_Standard_full
    Next Run : 12/11/2025 16:46:46
    Last Run : 12/11/2025 16:44:44
    State    :
--------------------------------
```

Figure 17 : Suppression d'une sauvegarde planifiés

On peut voir que la sauvegarde planifiée a bien été supprimée.

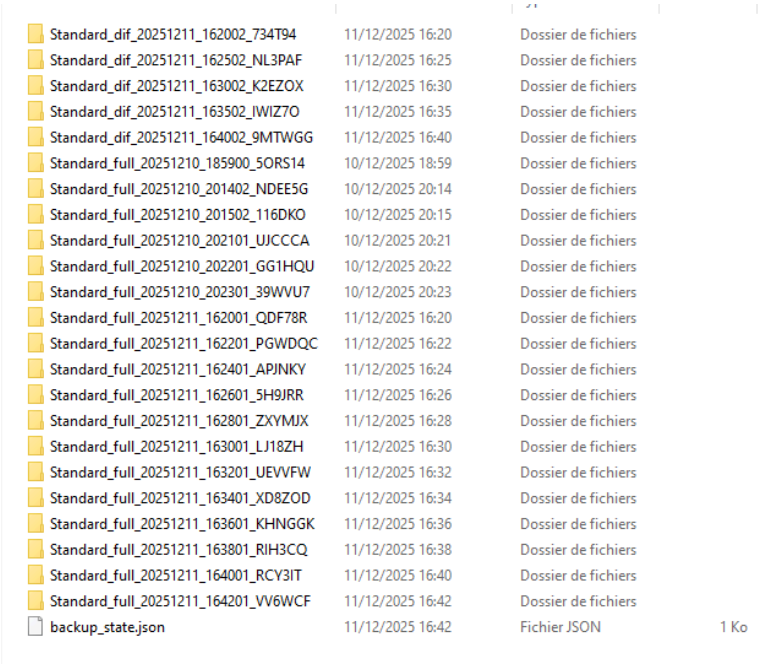


Figure 18 : Exemple des sauvegardes générés en 20 minutes

On peut voir ici que les sauvegardes complètes se sont bien lancées toutes les 2 minutes et les sauvegardes différentielles toutes les 5 minutes.

5.3.6 Script de purge / rétention des sauvegardes

Le script purge_backups.ps1 applique les règles de rétention des sauvegardes XANADU, à la fois sur le stockage local et sur le stockage externalisé. Il lit une configuration JSON par niveau de criticité (Critical, Important, Standard) pour savoir combien de sauvegardes complètes conserver et quelles durées de rétention appliquer aux sauvegardes locales et externalisées. Il supprime en priorité les sauvegardes trop anciennes au regard d'un seuil RGPD global, nettoie les sauvegardes différentielles et incrémentielles devenues inutiles par rapport à la dernière sauvegarde complète, et garantit dans la mesure du possible qu'au moins une sauvegarde complète récente reste disponible par policy. Toutes les décisions (conserver / supprimer) sont tracées dans un log dédié, avec un mode simulation permettant de tester les règles sans suppression réelle.

Tableau des paramètres

Nom	Type	Obligatoire	Valeurs possibles	Description
BackupRoot	String	Non	Chemin vers la racine de backup	Racine des sauvegardes XANADU (local + external). Par défaut C:\Backups.
RetentionConfigPath	String	Non	Chemin de fichier JSON	Fichier retention.json décrivant les règles de rétention par policy. Par défaut C:\Backups\retention.json.
MaxAgeDays	Int	Non	Nombre de jours	Âge maximal avant suppression forcée (règle RGPD globale). Par défaut 150 jours.
DryRun	Switch	Non	—	Mode simulation : aucune suppression effective, le script ne fait que journaliser ce qu'il ferait.

Chemins nécessaires / générés

Le script considère comme point d'entrée une racine de sauvegarde, BackupRoot, qui par défaut est *C:\Backups*. Sous cette racine, il s'attend à trouver les sous-dossiers Local et External, chacun organisé par criticité (Critical, Important, Standard) contenant les répertoires de backup nommés selon le format standard (par exemple *Critical_full_20251210_162032_444LDH*). Les règles de rétention sont lues dans un fichier JSON centralisé, retention.json, stocké par défaut directement à la racine de BackupRoot (C:\Backups\retention.json) ou à un emplacement explicitement fourni via -RetentionConfigPath. La journalisation de la purge est réalisée dans un fichier Purge.log placé dans le sous-dossier Logs de BackupRoot (par exemple *C:\Backups\Logs\Purge.log*), ce dossier étant créé automatiquement si nécessaire. Lorsqu'il n'est pas en mode DryRun, le script supprime physiquement les dossiers de backup ciblés (locaux et/ou externalisés) dans l'arborescence sous BackupRoot, en s'appuyant uniquement sur ces chemins et sur les informations extraites des noms de répertoire.

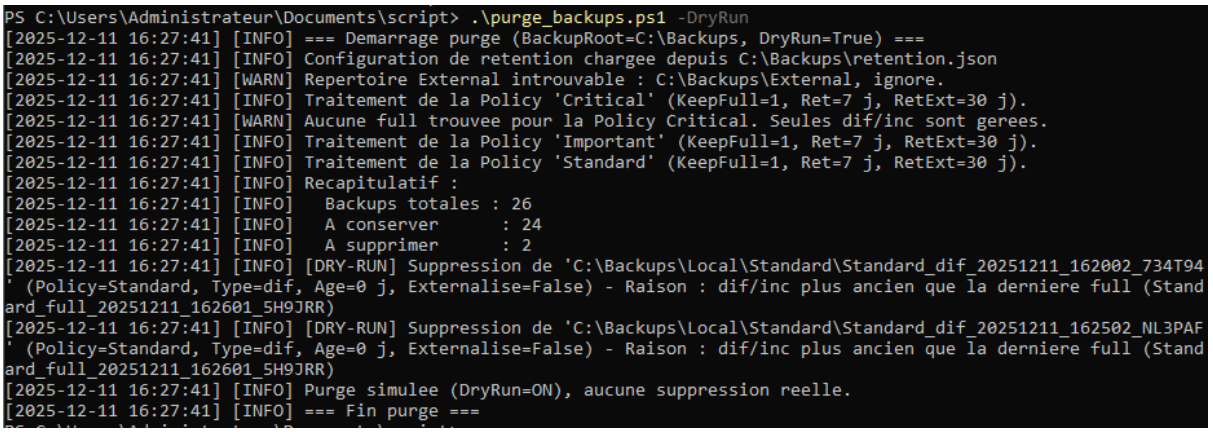


Figure 19 : Utilisation du script en mode DryRun

On peut voir que le script a repéré des sauvegardes différentielles plus anciennes que des complètes et donc peut les supprimer (ces sauvegardes sont d'ailleurs les sauvegardes générées par le script scheduler_backup.ps1) .

6. Supervision et Monitoring de sécurité

6.1 Architecture de surveillance unifiée

6.1.1 Rôle du SIEM (Wazuh) et du Monitoring (Zabbix)

L'écosystème de surveillance s'articule autour de deux solutions complémentaires hébergées sur les serveurs Linux dédiés de chaque site.

D'une part, Zabbix assure le maintien en condition opérationnelle en surveillant la disponibilité et la performance des équipements.

Il remonte les métriques techniques telles que la charge système, la latence réseau ou l'espace disque, garantissant une réactivité immédiate en cas de panne ou de dégradation de service.

D'autre part, Wazuh agit comme le centre névralgique de la sécurité (SIEM/XDR). Sa mission est de centraliser et d'analyser les journaux d'événements pour détecter les menaces actives.

Il surveille l'intégrité des fichiers critiques, identifie les vulnérabilités logicielles sur le parc et repère les comportements suspects, comme les tentatives d'intrusion ou les élévations de privilèges, complétant ainsi la vision technique par une analyse sécuritaire approfondie.

6.1.2 Méthodologie de collecte (Agents, Syslog, SNMP)
La remontée des informations vers les serveurs de supervision s'effectue via des canaux sécurisés, adaptés à la nature de chaque équipement. Pour l'ensemble des serveurs et des postes de travail, l'utilisation d'agents logiciels chiffrés a été privilégiée. Cette méthode permet une collecte granulaire des données système tout en autorisant l'exécution de réponses actives, telles que le blocage automatique d'un processus malveillant.

Concernant l'infrastructure réseau active, le protocole SNMP v3 a été configuré sur les commutateurs et routeurs. Ce choix garantit l'authentification et le chiffrement des échanges

lors de l'interrogation des sondes, protégeant ainsi la topologie du réseau contre les écoutes passives. Enfin, les pare-feux pfSense transmettent leurs journaux d'activité via le protocole Syslog vers les collecteurs, permettant au SIEM d'analyser les flux périmétriques et de corréler le trafic réseau avec les événements internes.

6.2 Matrice des événements de sécurité surveillés

Cette section définit l'ensemble des événements capturés et analysés par notre solution de supervision (SIEM/IDS).

L'objectif est de transformer les logs bruts en indicateurs de sécurité exploitables. Nous avons classé ces événements en trois catégories critiques.

6.2.1 Événements liés à l'authentification (Brute force, échecs)

La surveillance de l'authentification est la première ligne de défense pour détecter les tentatives d'intrusion et les compromissions de comptes.

Type d'événement	**Description**	**Signature / ID (Exemples)**	**Sévérité**
Échec d'authentification	Tentative de connexion avec un mot de passe incorrect ou un utilisateur inconnu.	Win: 4625 Linux: Failed password	Faible (si isolé)
Attaque Brute Force	Multiples échecs d'authentification provenant de la même IP ou ciblant le même utilisateur dans un court laps de temps.	Règle: > 5 échecs en 60 sec	**Critique**

		Win: 4625 (fréquence élevée)	
Succès hors horaires	Connexion réussie à une heure anormale (nuit/week-end) pour un compte standard.	Win: 4624 Linux: Accepted password	Moyenne
Élévation de privilèges	Utilisation de commandes administratives (root/sudo) ou changement de groupe utilisateur.	Linux: sudo usage, su Win: 4672 (Special Privileges)	Haute
Nettoyage des logs	Suppression des journaux d'événements pour masquer des traces.	Win: 1102 (Log Clear) Linux: rm /var/log/*	**Critique**

6.2.2 Événements liés à l'intégrité système (Fichiers critiques)

Nous utilisons le FIM (File Integrity Monitoring) pour détecter toute modification non autorisée sur les fichiers vitaux du système d'exploitation et les configurations services.

Cible surveillée	Type de modification	Impact potentiel	Sévérité
Registres Windows	Clés Run, RunOnce, Services.	Persistance d'un malware au redémarrage.	Haute
Fichiers Linux sensibles	/etc/passwd, /etc/shadow, /etc/sudoers.	Création de backdoor ou modification de droits.	**Critique**
Configuration SSH	~/.ssh/authorized_keys, sshd_config.	Ajout d'une clé publique attaquante pour accès distant.	Haute
Binaires système	/bin/*, /sbin/*, System32.	Remplacement de commandes légitimes par des chevaux de Troie (Trojan).	**Critique**
Contenu Web	/var/www/html.	Défaçage de site ou injection de code (Webshell).	Moyenne

6.2.3 Événements liés au réseau et aux menaces externes

Cette catégorie regroupe les anomalies de trafic détectées par les pare-feux et les sondes réseaux positionnés dans la topologie GNS3.

Type d'événement	Description	Indicateur technique	Sévérité

Scan de ports	Tentative d'énumération des services ouverts sur une machine cible.	Connexions multiples sur ports distincts (TCP Connect/SYN).	Moyenne
Trafic vers IP malveillante	Communication sortante vers une IP réputée dangereuse (C&C, Botnet).	Comparaison avec liste de "Threat Intelligence".	Haute
Refus de service (DoS)	Augmentation anormale du volume de paquets ou du nombre de connexions.	Saturation de la bande passante ou des sessions TCP.	Haute
Mouvement latéral	Tentative de connexion RDP ou SSH entre postes de travail (non-serveurs).	Flux interne inhabituel (Workstation à Workstation).	Moyenne

6.3 Gestion des alertes et déclencheurs (Triggers)

Pour éviter la "fatigue de l'alerte" (trop de notifications inutiles), nous avons défini des règles de déclenchement précises basées sur des seuils et des corrélations.

6.3.1 Niveaux de classification

Chaque alerte générée est classée selon une échelle de gravité standardisée :

Niveau 1 - Info (Log Only) : Événement normal (ex: connexion réussie, mise à jour système). Stocké pour audit, aucune notification.

Niveau 2 - Warning (Avertissement) : Événement suspect mais non bloquant (ex: scan de port lent, erreur 404 massive). Nécessite une revue hebdomadaire.

Niveau 3 - High (Alerte de Sécurité) : Menace probable (ex: modification fichier critique, malware détecté mais nettoyé). Notification immédiate par email.

Niveau 4 - Critical (Incident Majeur) : Compromission avérée ou attaque en cours (ex: Brute force réussi, exfiltration de données). Notification multicanal (SMS/Slack + Email) et isolement automatique si possible.

6.3.2 Règles de déclenchement (Triggers)

Les déclencheurs sont configurés pour corréler plusieurs événements avant de lever une alerte.

Tableau des règles de déclenchement principales :

Scénario d'attaque	**Condition de déclenchement (Trigger)**	**Action automatisée**
Attaque par dictionnaire	Si Échec Auth > 5 fois en 60 secondes DEPUIS Même IP.	Générer Alerte **Critique** + Bloquer IP (Firewall).
Changement Configuration	Si modification détectée sur /etc/sudoers SANS ticket de maintenance associé.	Générer Alerte **Haute** + Snapshot système.
Scan Réseau	Si connexion sur > 10 ports différents en < 10 secondes.	Générer Alerte **Moyenne** (Warning).
Détection Malware	Si détection AV/EDR confirmée sur un hôte.	Générer Alerte **Haute** + Isoler l'hôte du réseau virtuel.

6.3.3 Workflow de notification

Lorsqu'un déclencheur s'active, le système engage immédiatement un processus structuré débutant par une phase d'enrichissement.

Cette étape vise à compléter l'alerte brute en y agrégeant automatiquement le contexte technique nécessaire à l'analyse, tel que le nom de l'hôte, l'adresse IP source et l'identité de l'utilisateur concerné.

Une fois ces données consolidées, la notification est transmise vers les canaux de communication prédéfinis, qu'il s'agisse d'un affichage en temps réel sur le tableau de bord du SIEM, d'une alerte par email à l'administrateur ou de la création d'un ticket dans l'outil de gestion.

Enfin, le cycle se conclut par l'acquittement, une action obligatoire où l'analyste doit qualifier l'alerte en la marquant comme "Prise en compte" ou comme "Faux positif" afin de clore formellement l'incident de sécurité.

8. Table des figures

Figure 1 : Extrait du sondage de la cybersécurité 11
Figure 2 : Extrait du questionnaire utilisateur des réflexes cybersécurité 12
Figure 3 : Schéma explicatif de la redondance des équipements 22
Figure 4 : Création des comptes utilisateurs informatique 32
Figure 5 : Désactivation d'un utilisateur 34
Figure 6 : Désactivation automatique des utilisateurs inactifs 37
Figure 7 : Path des sauvegardes locales 40
Figure 8 : Sauvegardes critiques 40
Figure 9 : Fichier backup_state.json 40
Figure 10 : Sélection interactive d'un backup 43
Figure 11 : Listing d'une sauvegarde 43
Figure 12 : Commande et Logs d'un fichier unique 44
Figure 13 : Dossier de restauration du fichier unique 44
Figure 14 : Exemple de mail d'alerte envoyé 47
Figure 15 : Configuration d'une sauvegarde planifiée 49
Figure 16 : Listing des sauvegardes planifiées 50
Figure 17 : Suppression d'une sauvegarde planifiés 50
Figure 18 : Exemple des sauvegardes générés en 20 minutes 51
Figure 19 : Utilisation du script en mode DryRun 53

8. Annexes

8.1 Audit de l'équipe technique et des employées

Le lien menant au Google Forms afin de sonder la maturité de l'équipe cybersécurité (mode éditeur)

https://docs.google.com/forms/d/1NF8ZgL8ekte6LElvKyPQNyEoLKfrr8RUS91UnCECBfM/edit

Le lien menant au Google Forms afin de sonder la maturité de l'équipe cybersécurité (mode répondant)

https://docs.google.com/forms/d/e/1FAIpQLSd6mOtZ2pPEh6d1U5U8DP2FYIzQI3h4wgNmFw2JemfoZ1k-ow/viewform?usp=publish-editor

Le lien vers le Klaxoon pour le questionnaire utilisateurs :

https://go.klaxoon.com/4XB77KX

8.2 Matrice de flux

La matrice de flux des sites Atlantis et Springfield au niveau du firewall PfSense :

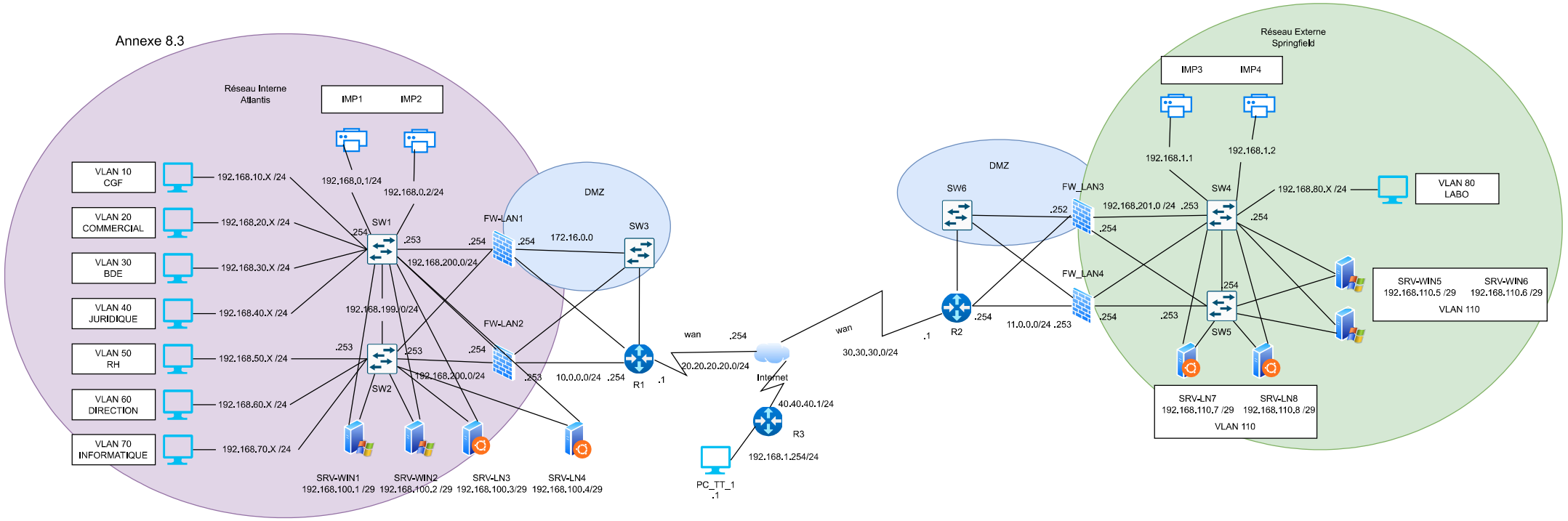
Equipements / Services	VLAN 10 (CGF)	VLAN 20 (Comm)	VLAN 30 (BDE)	VLAN 40 (JURIDIQUE)	VLAN 50 (RH)	VLAN 60 (DIRECTION)	VLAN 70 (INFORMATIQUE)	VLAN 80 (LABO)	VLAN 99 (MGMT)	VLAN 101 (MGMT)	VLAN 100 (SRV)	VLAN 110 (SRV)	IMP 1	IMP 2	Internet
VLAN 10 (CGF)	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	(443),Proxy(8080), SM	~~~~~~~~~~	Oui	Oui	HTTPS (443), DNS (53)
VLAN 20 (Comm)	~~~~~~~~~~	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	(443),Proxy(8080), SM	~~~~~~~~~~	Oui	Oui	HTTPS (443), DNS (53)
VLAN 30 (BDE)	~~~~~~~~~~	~~~~~~~~~~	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	(443),Proxy(8080), SM	~~~~~~~~~~	Oui	Oui	HTTPS (443), DNS (53)
VLAN 40 (JURIDIQUE)	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	(443),Proxy(8080), SM	~~~~~~~~~~	Oui	Oui	HTTPS (443), DNS (53)
VLAN 50 (RH)	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	(443),Proxy(8080), SM	~~~~~~~~~~	Oui	Oui	HTTPS (443), DNS (53)
VLAN 60 (DIRECTION)	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	(443),Proxy(8080), SM	~~~~~~~~~~	Oui	Oui	HTTPS (443), DNS (53)
LAN 70 (INFORMATIQUE)	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	(443),Proxy(8080), SM	~~~~~~~~~~	Oui	Oui	HTTPS (443), DNS (53)
VLAN 80 (LABO)	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	ICMP	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~~~~~~~	443),Proxy(8080), SMT	Oui	Oui	HTTPS (443), DNS (53)
VLAN 99 (MGMT)	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	ICMP		RDP (3389), SSH (22)	~~~~~~~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~
VLAN 101 (MGMT)	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	RDP (3389), SSH (22)	~~~~~~~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~~~~~~~
VLAN 100 (SRV)	DNS(53),LDAPS(636)	DNS(53),LDAPS(636)	DNS(53),LDAPS(636)	DNS(53),LDAPS(636)	DNS(53),LDAPS(636)	DNS(53),LDAPS(636)	RDP (3389), SSH (22)	~~~~~~~~~~~~~~~~	DNS(53),LDAPS(636)		LDAPS(636)	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~	Oui
VLAN 110 (SRV)	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	RDP (3389), SSH (22)	DNS(53),LDAPS(636)	~~~~~~~~~~~~~~~~		~~~~~~~~~~~~~~~~	LDAPS(636)			
IMP 1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	~~~~~~~~~~~~~~~~		~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~
IMP 2	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	~~~~~~~~~~~~~~~~		~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~
Internet	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	~~~~~~~~~~		~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~~~~~~~	~~~~~~~~~~	~~~~~~~~~~

La matrice de flux traduite en règles :

N° Règle	Equipement	Interface	Source	Objet Source	Destination	Objet Destinatior	Protocole / Port	Action	Description
1	SW1-SW2	e0-8/0-3	192.168.VLAN.X/24 (Sauf VLAN 100,99)	VLAN (10-100)	192.168.100.1-2/24	DC1 - DC2	DHCP (67-68), Proxy (8080), SMTP (25), IMAP (14	Allow	Trafic user
2	SW1-SW2	e0-8/0-3	192.168.VLAN.X/24 (Sauf VLAN 100,99)	VLAN (10-100)	192.168.VLAN.254/2	Passerelle VLAN	HTTPS(443), DNS (53)	Allow	Trafic user
3	FW-LAN1 - FW-LAN2	LAN	192.168.VLAN.X/24 (Sauf VLAN 100,99)	VLAN (10-100)	Internet	Internet	HTTPS (443)	Allow	Internet
4	SW1-SW2	e6/0-6/3	192.168.70.0/24	VLAN Informatique	192.168.100.X/29	VLAN Serveur ATL	RDP (3389), SSH (22)	Allow	ADMIN
5	SW1-SW2	e6/0-6/3	192.168.70.0/24	VLAN Informatique	192.168.110.X/29	VLAN Serveur SPR	RDP (3389), SSH (22)	Allow	ADMIN
8	Default	Default	Any	Any	Any		Any	Block	Block All Policy

Les protocoles et ports autorisées sont : DNS(53),LDAPS(636),DHCP(68/67),HTTPS(443),Proxy(8080), SMTP(25),IMAP(143),WSUS (3451), ZABBIX (10050), WAZUH (8432)

Annexe 8.3


Réseau Interne
Atlantis
IMP1
IMP2
192.168.0.1/24
192.168.0.2/24
VLAN 10
CGF
192.168.10.X /24
VLAN 20
COMMERCIAL
192.168.20.X /24
VLAN 30
BDE
192.168.30.X /24
VLAN 40
JURIDIQUE
192.168.40.X /24
VLAN 50
RH
192.168.50.X /24
VLAN 60
DIRECTION
192.168.60.X /24
VLAN 70
INFORMATIQUE
192.168.70.X /24
SW1
SW2
.254
.253
192.168.200.0/24
192.168.199.0/24
FW-LAN1
FW-LAN2
172.16.0.0
DMZ
SW3
10.0.0.0/24
R1
.1
wan
20.20.20.20.0/24
Internet
40.40.40.1/24
R3
192.168.1.254/24
PC_TT_1
.1
SRV-WIN1
192.168.100.1 /29
SRV-WIN2
192.168.100.2 /29
SRV-LN3
192.168.100.3/29
SRV-LN4
192.168.100.4/29
30.30.30.0/24
R2
11.0.0.0/24
SW6
DMZ
FW_LAN3
FW_LAN4
192.168.201.0 /24
Réseau Externe
Springfield
IMP3
IMP4
192.168.1.1
192.168.1.2
SW4
SW5
192.168.80.X /24
VLAN 80
LABO
SRV-WIN5
192.168.110.5 /29
SRV-WIN6
192.168.110.6 /29
VLAN 110
SRV-LN7
192.168.110.7 /29
SRV-LN8
192.168.110.8 /29
VLAN 110