Administration du SI
&
sécurité IT
Livrable 3

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 3 - 18/12/2025

Sommaire

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 doit donc intégrer nativement les principes de confidentialité, d'intégrité, de disponibilité et de traçabilité des données.

XANADU exploite plusieurs services métiers essentiels, tels que la comptabilité, le service commercial, le juridique, les ressources humaines, le bureau d'étude et un laboratoire distant. Ces services s'appuient sur un ERP structuré en trois tiers comprenant une base PostgreSQL, un serveur applicatif et un serveur Web. L'infrastructure actuelle souffre de lacunes critiques, notamment un stockage non centralisé, une absence de contrôle des privilèges, des accès externes limités, des sauvegardes manuelles hétérogènes et des utilisateurs administrateurs de leurs postes. Pour pallier ces faiblesses, le nouveau système doit permettre la connexion sécurisée des itinérants, assurer une délégation d'administration par service, et proposer une architecture Active Directory cohérente entre les deux sites. Les objectifs de performance incluent un RTO de 4 heures pour les données critiques et une gestion rigoureuse des droits d'accès via des stratégies de groupe (GPO) et un cloisonnement réseau strict.

2. Objet du document

Le présent document constitue le Livrable 3 – Maquette du SI du projet CESITECH pour l'entreprise XANADU. Il vise à démontrer la mise en œuvre concrète des choix techniques et organisationnels définis dans les livrables précédents, à travers une infrastructure fonctionnelle et sécurisée. La maquette constitue également un support de démonstration lors de la soutenance et permet d'évaluer la cohérence globale du système, sa capacité d'administration ainsi que le respect des exigences de sécurité, de disponibilité et de traçabilité.

3. Présentation générale de la maquette

Cette section détaille l'architecture technique mise en œuvre pour répondre aux besoins du projet. La maquette a été conçue pour simuler un environnement d'entreprise (PME) réaliste, sécurisé et segmenté.

3.1 Périmètre fonctionnel

L'infrastructure déployée couvre l'ensemble des services informatiques essentiels à l'exploitation du réseau d'entreprise. La gestion des identités et des accès (IAM) est centralisée via Active Directory, incluant les rôles DNS et DHCP sous Windows Server 2022. La segmentation réseau est assurée par un commutateur de niveau 3 gérant les VLANs (10 à 100) et le routage inter-VLAN sécurisé par ACLs. La sécurité périmétrique repose sur un pare-feu pfSense qui filtre les flux et gère les accès distants via OpenVPN. Les services applicatifs comprennent une messagerie complète sous Poste.io, un serveur web NGINX et un proxy Squid pour le contrôle de la navigation. Enfin, la pérennité du système est garantie par une surveillance proactive via Zabbix et Wazuh, ainsi qu'une gestion centralisée des mises à jour par WSUS.

3.2 Environnement et composants maquetés

Le choix de l'environnement de virtualisation est un élément structurant de cette maquette. Pour répondre aux exigences de simulation réseau, nous avons opté pour une virtualisation de Type 2 (Hosted) via l'émulateur GNS3. Contrairement à une solution de virtualisation de Type 1 (Bare Metal) comme Proxmox VE, qui serait privilégiée pour la production réelle de XANADU en raison de ses performances brutes, GNS3 permet une émulation fidèle du matériel Cisco. Cette approche est indispensable pour tester les configurations de VLANs et de redondance HSRP sur des images IOS réelles, garantissant que les protocoles réseau réagiront de la même manière lors du déploiement physique.

L'infrastructure s'appuie sur une combinaison de systèmes robustes. Windows Server 2022 a été retenu pour sa gestion native des services d'annuaire et des stratégies de groupe, tandis qu'Ubuntu Server 24.04 LTS héberge les services open-source pour sa stabilité et sa faible consommation de ressources. Le pare-feu pfSense complète ce dispositif en offrant des fonctionnalités de sécurité avancées, telles que l'IDS/IPS et la gestion de certificats, indispensables pour sécuriser une infrastructure multi-sites connectée via des tunnels chiffrés.

3.3 Analyse comparative de la virtualisation

Le choix de l'environnement de virtualisation est déterminant pour la fidélité de la maquette. Il convient de distinguer deux catégories principales :

-Virtualisation de Type 1 (Bare Metal) : Des solutions comme Proxmox VE ou VMware ESXi s'installent directement sur le matériel. Elles sont optimales pour la production réelle de XANADU car elles offrent des performances maximales et une gestion robuste des serveurs. Cependant, Proxmox est limité pour simuler des architectures réseau complexes ; il traite le réseau de manière logicielle (Linux Bridges/OVS), ce qui ne permet pas d'émuler fidèlement le comportement spécifique d'équipements propriétaires.

-Virtualisation de Type 2 (Hosted) et Émulation : C'est le choix retenu pour cette maquette via GNS3. Contrairement à Proxmox, GNS3 ne se contente pas de faire tourner des

machines virtuelles ; il émule le matériel réseau (CPU/ASIC) des routeurs et commutateurs Cisco.

Justification du choix GNS3 pour le projet XANADU : Bien que Proxmox soit pressenti pour l'infrastructure cible en entreprise, GNS3 s'est imposé pour la phase de maquettage pour trois raisons majeures. D'abord, il permet d'exécuter de véritables images Cisco IOS, garantissant que les configurations de VLANs, de routage inter-VLAN et de redondance HSRP testées ici seront identiques lors du déploiement physique. Ensuite, GNS3 facilite la simulation de liens WAN (MPLS) entre les sites d'Atlantis et de Springfield, ce qui est complexe à reproduire sur un hyperviseur classique. Enfin, la capacité de capturer les flux en temps réel via Wireshark directement sur les liens virtuels offre une traçabilité indispensable pour valider la sécurité des flux Active Directory et VPN.

3.4 Contraintes et hypothèses

La réalisation de cette maquette a dû prendre en compte plusieurs contraintes inhérentes à un environnement de simulation, sensiblement différent d'un environnement de production physique.

Tout d'abord, la maquette étant exécutée localement sur une station de travail, les ressources matérielles disponibles ont constitué une contrainte majeure. Le nombre de machines virtuelles pouvant être déployées simultanément, ainsi que la puissance qui leur était allouée, dépendaient directement des capacités en mémoire vive et en processeur de l'hôte. Cette limitation a nécessité des arbitrages dans la répartition des ressources et le dimensionnement global de l'architecture simulée.

Par ailleurs, la connectivité WAN ne reposait pas sur une liaison opérateur réelle. L'accès Internet du pare-feu pfSense était simulé au moyen d'un mécanisme de NAT (Network Address Translation) s'appuyant sur le réseau physique de l'hôte. Cette configuration permettait de reproduire le comportement d'une connexion FAI standard, tout en restant tributaire des caractéristiques du réseau local de la machine utilisée pour la simulation.

Enfin, un comportement spécifique lié à l'émulateur GNS3 a mis en évidence une contrainte technique plus critique. À la suite d'une coupure électrique inopinée, l'intégrité de la maquette a été compromise, révélant une instabilité dans la gestion des protocoles de haute disponibilité reposant sur des adresses MAC virtuelles (VIP/HSRP). Contrairement à des équipements physiques qui auraient redémarré de manière nominale, l'environnement simulé a présenté des dysfonctionnements persistants au niveau de la couche ARP. La remise en service a alors nécessité un diagnostic approfondi, ainsi qu'une reconfiguration spécifique, incluant la désactivation temporaire de certaines mécanismes de redondance. Cet incident a permis de mettre en lumière les différences de résilience entre une maquette virtuelle et une infrastructure matérielle réelle.

4. Infrastructure Active Directory

4.1 Architecture AD

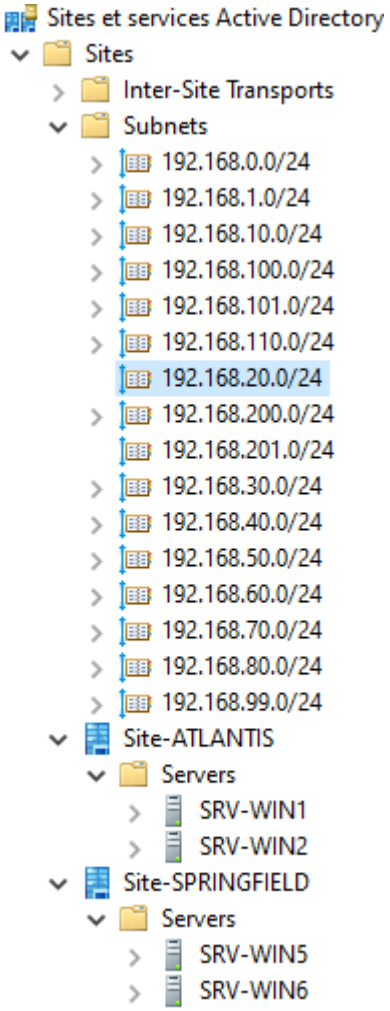

Figure 1 : console Sites et services Active Directory

La topologie Active Directory a été segmentée en deux sites logiques correspondant aux implantations physiques de XANADU. Cette configuration permet d'optimiser la réplication de l'annuaire entre le siège et le laboratoire distant via le lien MPLS, garantissant ainsi une authentification locale rapide pour les utilisateurs de Springfield.

4.2 DNS / DHCP

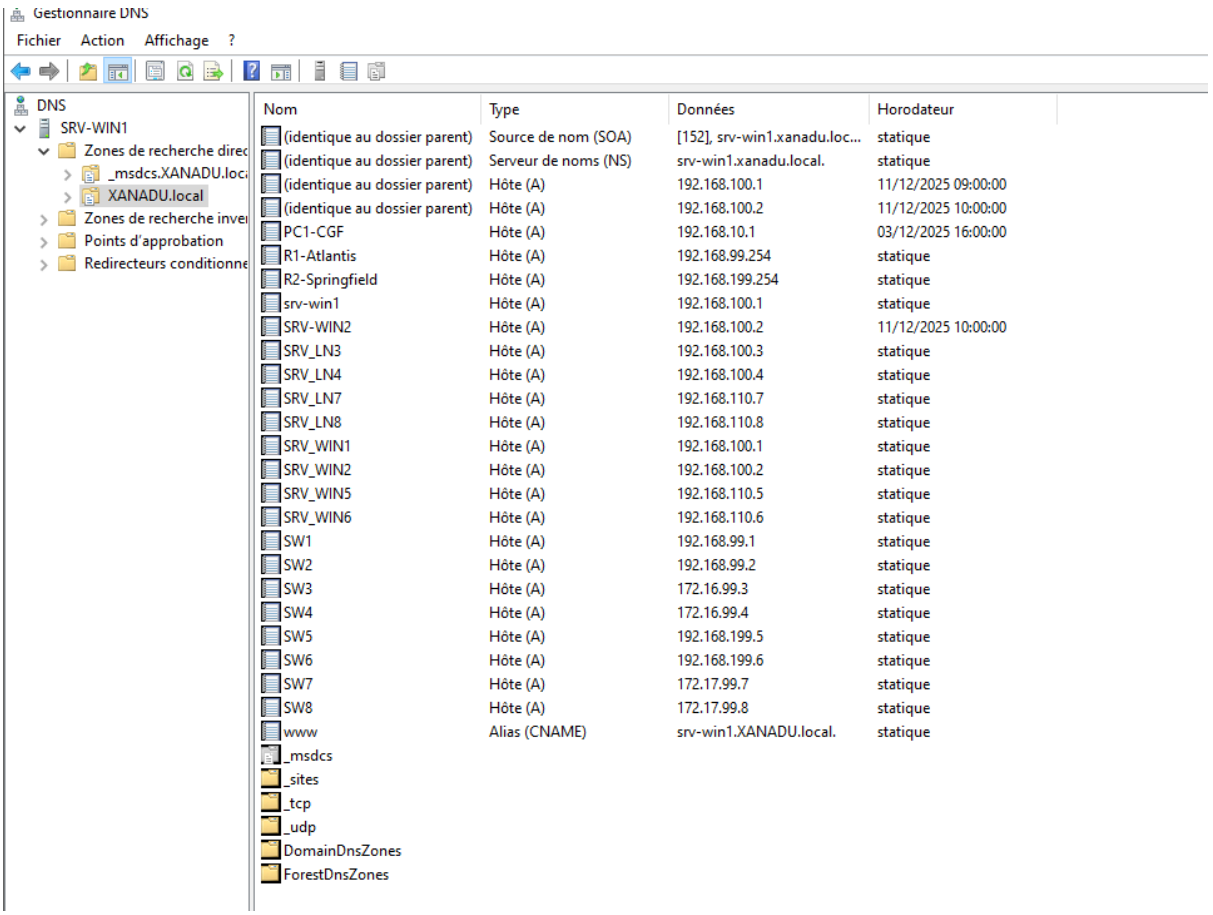

Figure 2 : Console DNS montrant la zone `XANADU.local`

Le service DNS assure la résolution de noms critiques pour les services métiers (ERP, Web). Le DHCP est configuré en haute disponibilité entre SRV-WIN1 et SRV-WIN2, avec des options configurées pour diriger automatiquement les clients vers la passerelle de leur VLAN respectif.

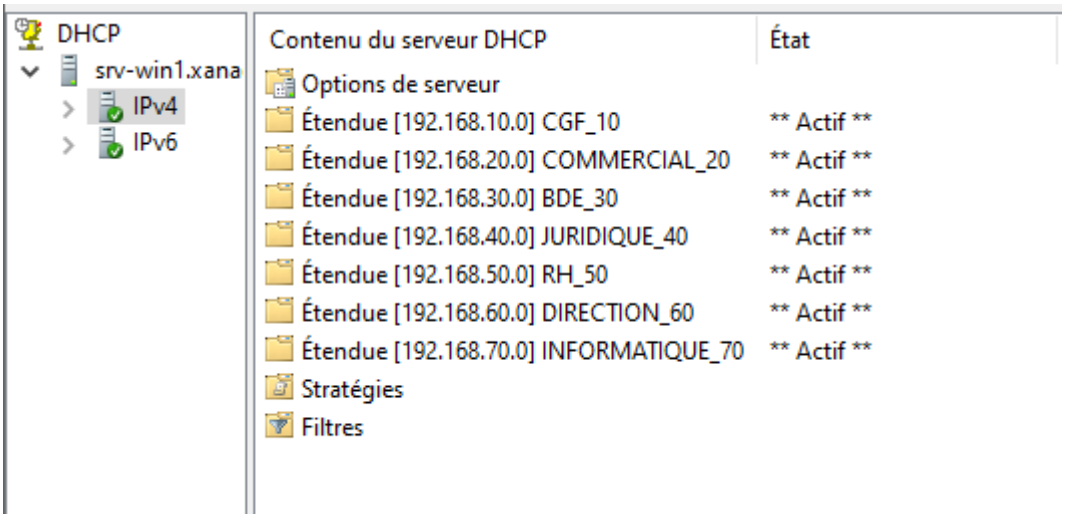

Figure 3 : Console DHCP

4.3 OU, groupes et droits

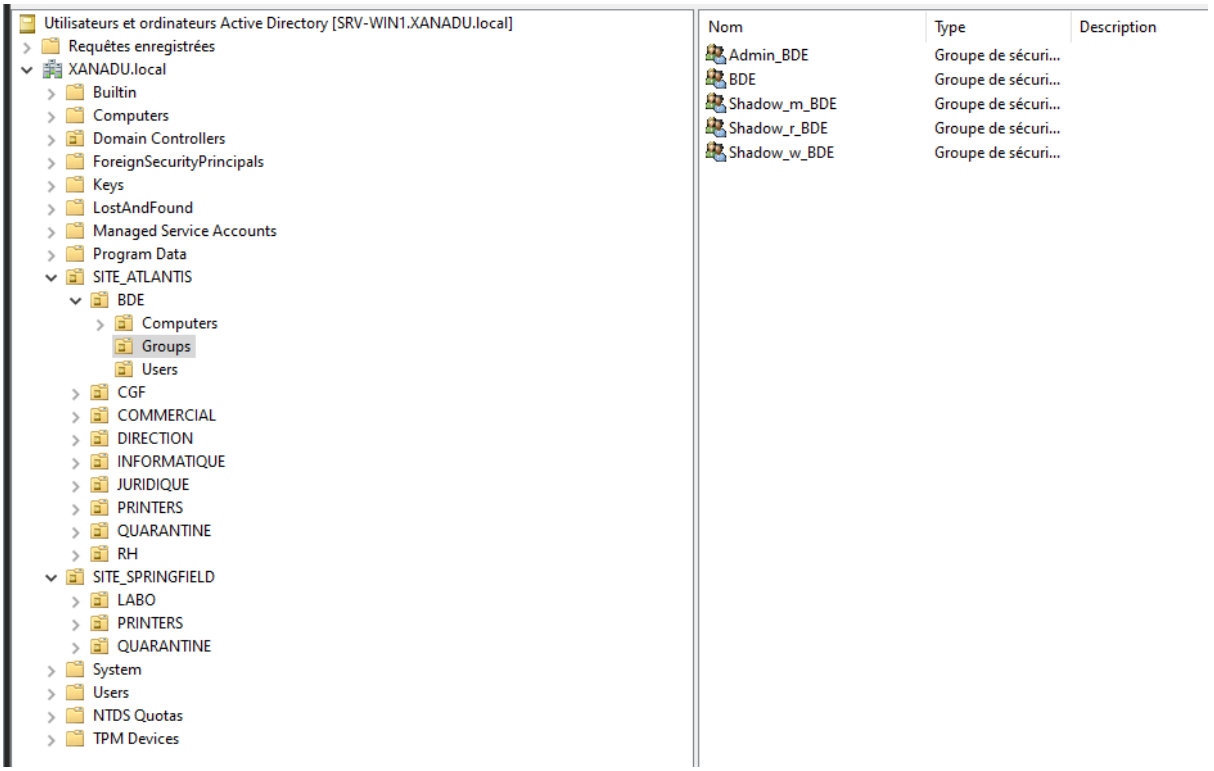

Figure 4 : Console Utilisateurs et ordinateurs Active Directory

L'arborescence LDAP respecte une logique géographique puis fonctionnelle. L'implémentation du modèle AGDLP simplifié via les 'Shadow Groups' permet d'isoler strictement les accès aux dossiers partagés (Lecture, Écriture, Modification) sans complexifier la gestion des comptes individuels.

4.4 Délégation d'administration

Afin de décentraliser la gestion quotidienne sans compromettre la sécurité globale, nous avons mis en œuvre la délégation de contrôle. Le groupe `Admin_RH` dispose désormais des droits de réinitialisation de mots de passe et de gestion des comptes uniquement sur son périmètre (OU RH), illustrant l'application du principe de moindre privilège.

4.5 GPO mises en œuvre

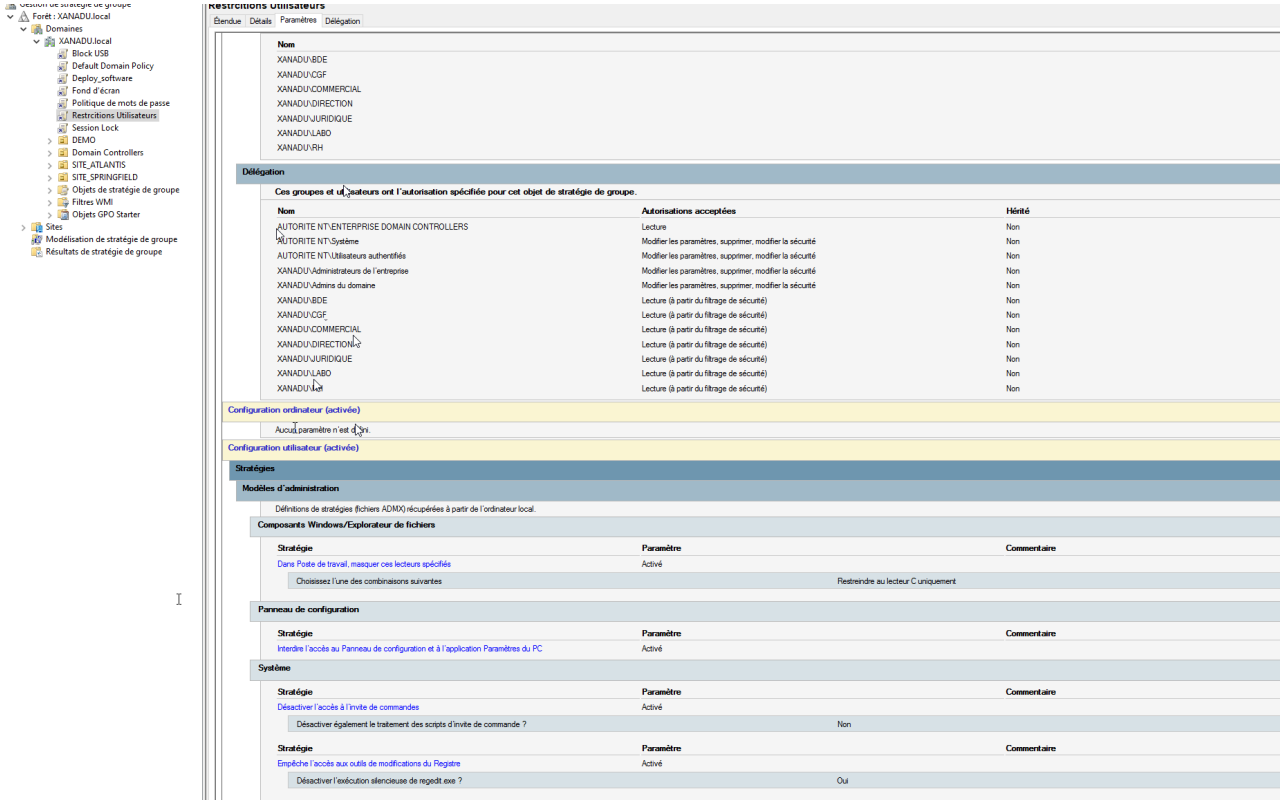

Figure 5 : Extrait de gpo de restrictions utilisateur

Le parc est piloté par des Group Policy Objects (GPO) hiérarchisées. Nous distinguons les stratégies de 'Durcissement' (blocage USB, CMD, Panneau de configuration) des stratégies de 'Confort' (montage de lecteurs réseau, déploiement d'imprimantes par site). Ce déploiement automatisé garantit l'homogénéité de la configuration des 60 postes clients.

5. Sécurité réseau et accès distants

5.1 Pare-feu et filtrage

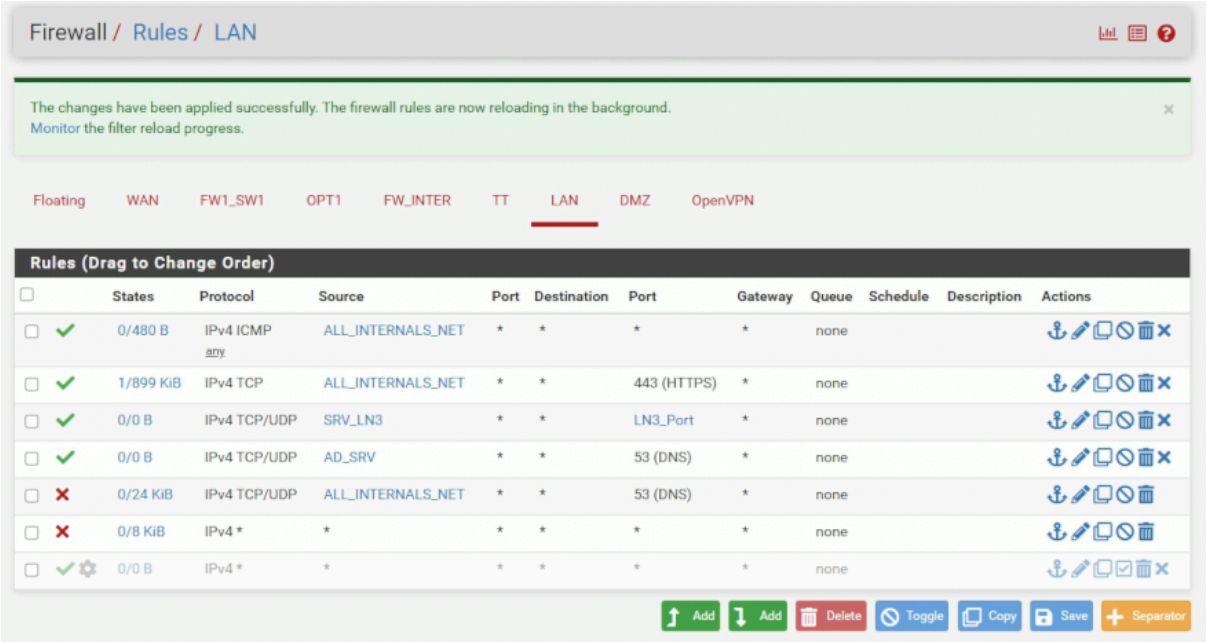

Figure 6 : Interface Web de pfSense dans Firewall > Rules

La sécurité périmétrique repose sur pfSense avec une politique de filtrage 'Default Deny'. Seuls les flux explicitement documentés dans la matrice de flux (en annexe) sont autorisés, limitant ainsi la surface d'attaque en cas de compromission d'un poste.

5.2 VPN

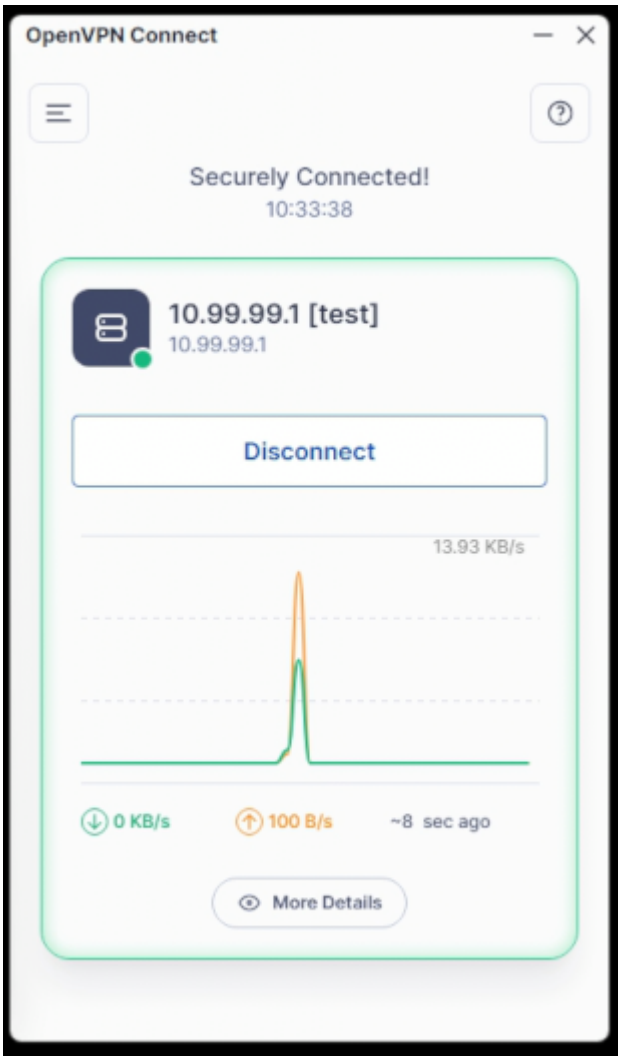

Figure 7 : Le client OpenVPN GUI connecté sur un poste "Télétravail"

L'accès distant pour les itinérants est sécurisé par un tunnel OpenVPN (AES-256). L'authentification est couplée à l'Active Directory via le service NPS/RADIUS, permettant une révocation immédiate des accès en cas de départ d'un collaborateur.
La sécurisation des accès repose sur une relation d'approbation entre le serveur NPS (Active Directory) et le pare-feu pfSense via le protocole RADIUS.

5.3 Protection postes / serveurs

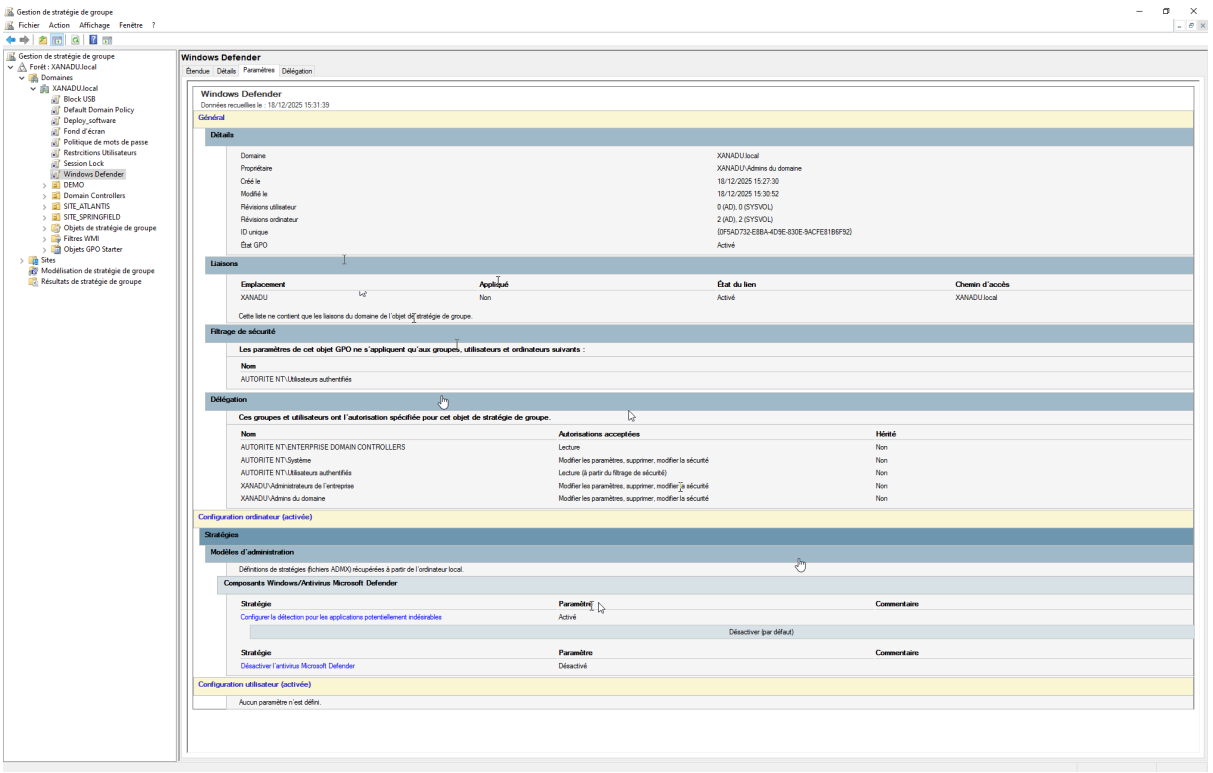

Figure 8 : Durcissement de Microsoft Defender via GPO

Plutôt que d'utiliser Windows Defender dans sa configuration par défaut, nous avons implémenté des politiques de durcissement via GPO. En activant les règles ASR (Attack Surface Reduction), nous dotons l'antivirus de capacités de détection comportementale proches d'un EDR. Ces règles interdisent notamment l'exécution de scripts malveillants par les logiciels de bureautique et protègent le processus LSASS contre le vol d'identifiants en mémoire.

Il permet en plus, de ne pas surcharger les performances d'un poste client à la manière d'un antivirus (Kaspersky, Avast) étant donné que Windows Defender assure ces fonctions.

Il est aussi couplé à Wazuh et son XDR, car il permet de remonter les logs Windows et de les corréler avec du trafic réseau suspect.

6. Intégration de la sauvegarde dans la maquette

6.1 Exécution et preuves

```
PS C:\Users\Administrateur\Documents\script> .\scheduler_backup.ps1 -List
Aucune tache planifiee associee au systeme XANADU.
PS C:\Users\Administrateur\Documents\script>
PS C:\Users\Administrateur\Documents\script>
PS C:\Users\Administrateur\Documents\script> .\scheduler_backup.ps1

=== CONFIGURATION DE LA TACHE PLANIFIEE ===

Type de sauvegarde (full/dif/inc) [default: full]:
Chemin fichier includes.txt [default: C:\Users\Administrateur\Documents\script\includes.txt]:
Criticite (Critical/Important/Standard) [default: Standard]:
Nom complet de la tache planifiee [default: XANADU_Standard_full]:

Saisir une expression CRON-like (ex : */30 * * * *)
Expression CRON: */1 * * * *+

TaskPath                                 TaskName                       State
--------                                 --------                       -----
\                                        XANADU_Standard_full           Ready
Tache planifiee creee avec succes : XANADU_Standard_full


PS C:\Users\Administrateur\Documents\script> .\scheduler_backup.ps1 -List

=== TACHES PLANIFIEES XANADU ===

[1] XANADU_Standard_full
    Next Run : 12/17/2025 10:55:55
    Last Run : 11/30/1999 00:00:00
    State    :
--------------------------------

Choisir une action : D = Delete une tache, M = Modify CRON, Q = Quitter
Action:
```

Figure 9 : Exécution du script scheduler_backup.ps1

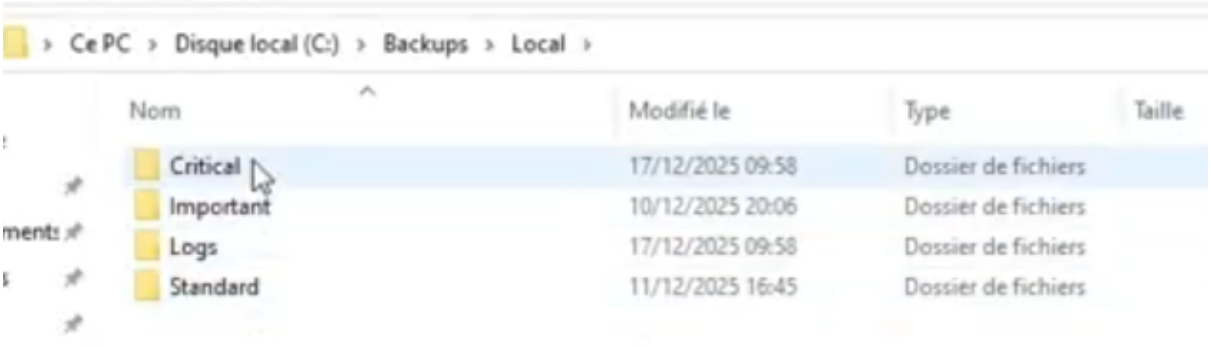

Figure 10 : Dossier des sauvegardes rangées par criticité.

```
.\backup_file.ps1 -Policy Critical -Type full -IncludesFile
C:\Users\Administrateur\Documents\script\includes.txt
```

Figure 11 : Exécution du script de sauvegarde

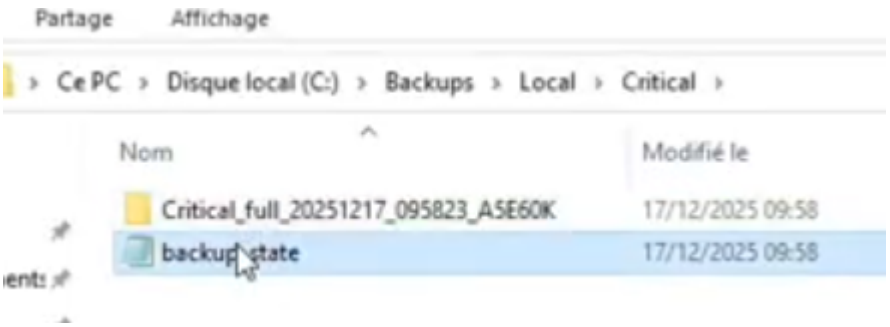

Figure 12 : Exemple de dossier de sauvegarde

La sauvegarde est intégrée à la maquette via un script exécuté automatiquement à l'aide d'une tâche planifiée.

Le premier élément présenté correspond à la configuration et à la présence de la tâche planifiée associée au système XANADU, garantissant l'exécution régulière des sauvegardes sans intervention manuelle.

Les écrans suivants illustrent l'exécution du script de sauvegarde ainsi que le résultat obtenu, avec une arborescence organisée par niveau de criticité (Critical, Important, Standard).

Chaque exécution génère un dossier de sauvegarde horodaté ainsi qu'un fichier d'état permettant de suivre les sauvegardes précédentes, attestant du bon fonctionnement opérationnel du mécanisme au sein de la maquette.

6.2 Logs et supervision

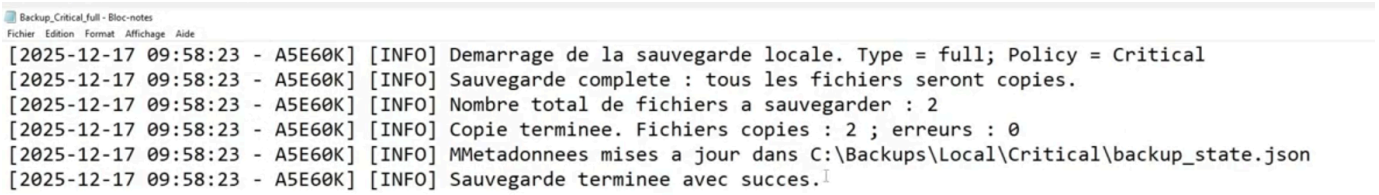

Figure 13 : Logs généré par l'exécution du script de sauvegarde

Chaque exécution de la sauvegarde génère un journal détaillé consignant les différentes étapes du processus, incluant le type de sauvegarde, le volume de données traité et l'état final de l'opération.

Ces journaux constituent un élément essentiel de la traçabilité et peuvent être exploités par l'outil de supervision afin de détecter rapidement les anomalies ou échecs lors des sauvegardes.

6.3 Test de restauration

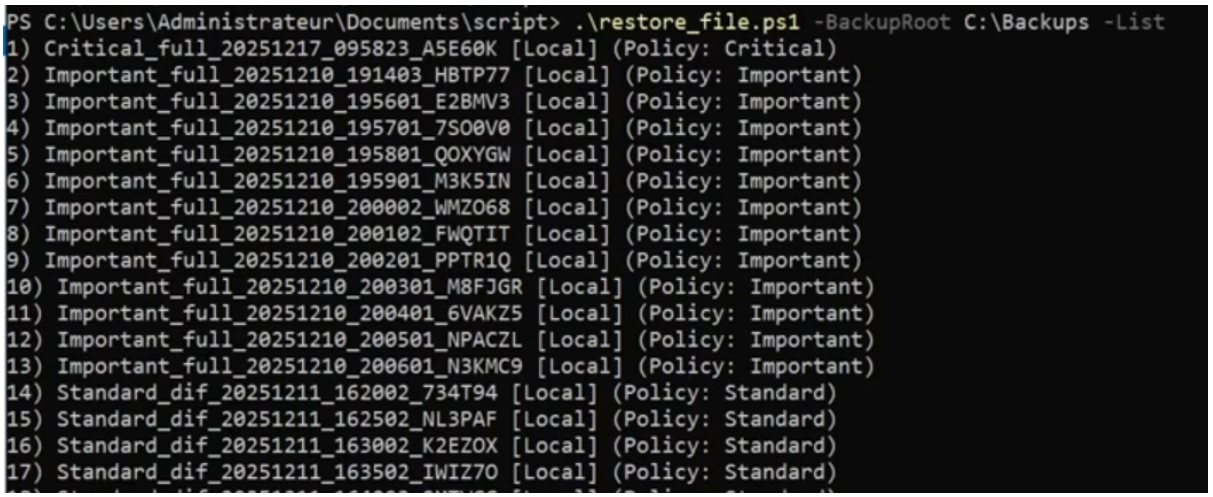

Figure 14 : Listing des sauvegardes effectuées

```
.\restore_file.ps1 -BackupRoot C:\Backups -BackupLabel
Critical_full_202251217_095823_A5E60K
```

Figure 15 : Exécution du script de restauration

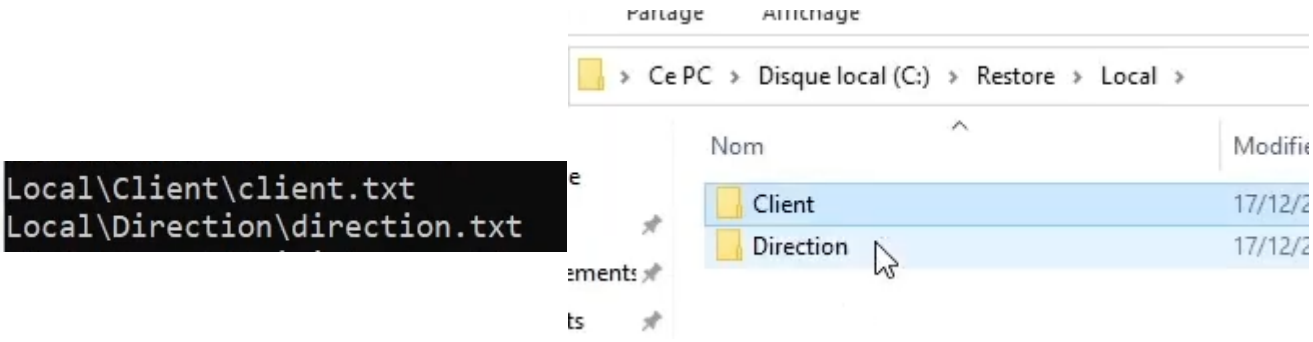

Figure 16 : Preuve de restauration d'un jeu de fichiers depuis une sauvegarde locale

Un test de restauration a été réalisé afin de valider l'exploitabilité des sauvegardes produites par le système.

Le premier écran présente la liste des sauvegardes disponibles, permettant de sélectionner précisément le jeu de données à restaurer. La restauration est ensuite déclenchée via un script dédié, comme illustré sur le second écran.

Le dernier écran confirme la restauration effective des fichiers dans un répertoire de test distinct, démontrant la capacité du système à restaurer des données de manière fiable dans le cadre de la maquette.

7. Supervision et exploitation

7.1 Outil de supervision

7.1.1 Zabbix

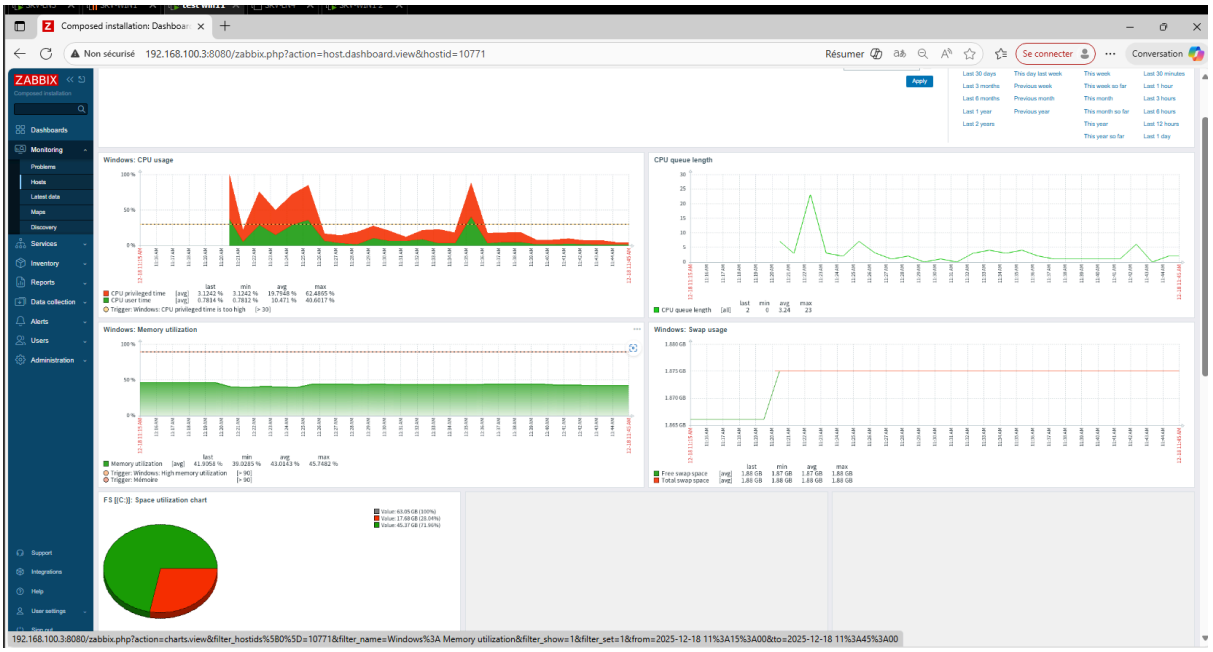

Figure 17 : Tableau de bord Zabbix

Zabbix est utilisé pour la supervision de la performance et de la disponibilité (Health Check). Grâce au protocole SNMP et aux agents Zabbix, nous suivons en temps réel l'état des services critiques (DNS, DHCP) et la charge des équipements réseau entre Atlantis et Springfield

7.1.2 Wazuh

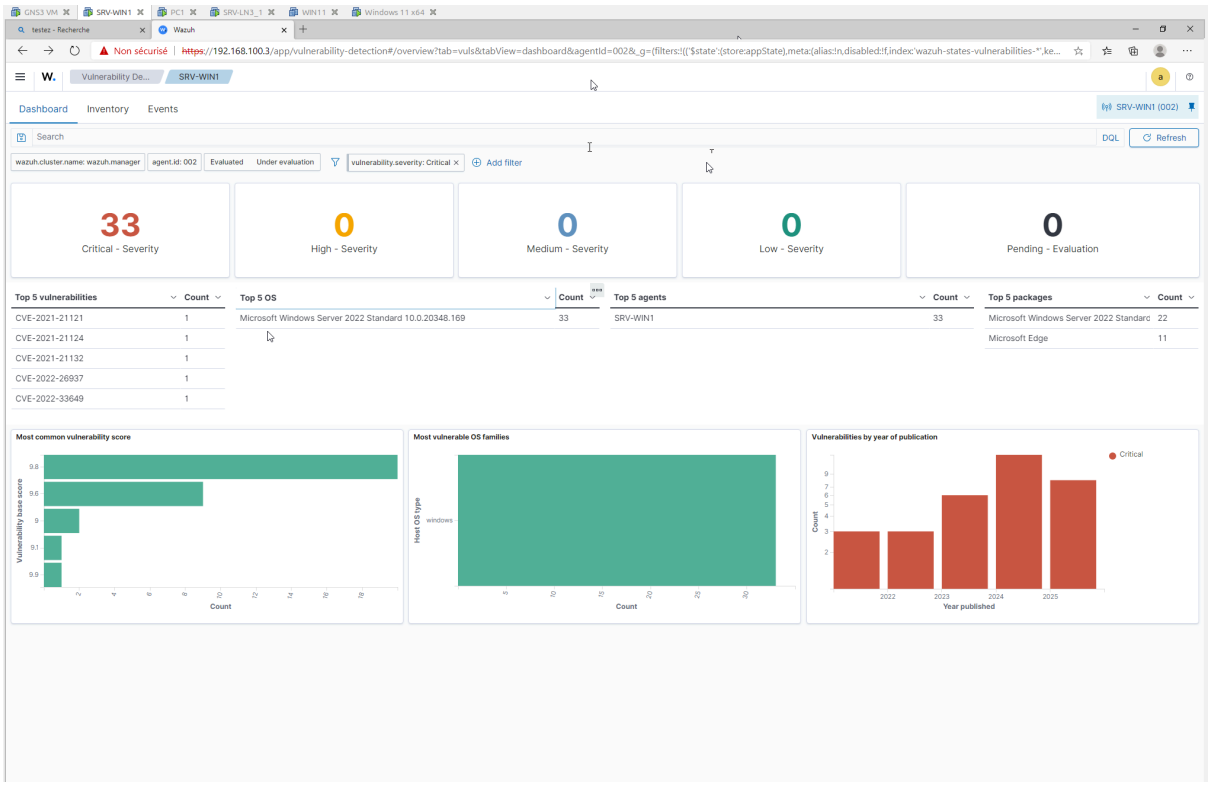

Figure 18 : Tableau de bord Wazuh

Wazuh complète la supervision en apportant une dimension SIEM/XDR. Il centralise les logs de sécurité, détecte les tentatives de connexion suspectes et analyse en continu les vulnérabilités des systèmes. C'est notre outil principal pour la traçabilité et la réponse aux incidents cyber.

7.2 Éléments supervisés

La supervision s'étend au-delà des serveurs : les équipements réseau (switchs, pare-feu) sont interrogés via SNMP pour surveiller la charge des liens MPLS et la température des équipements critiques

7.3 Alertes

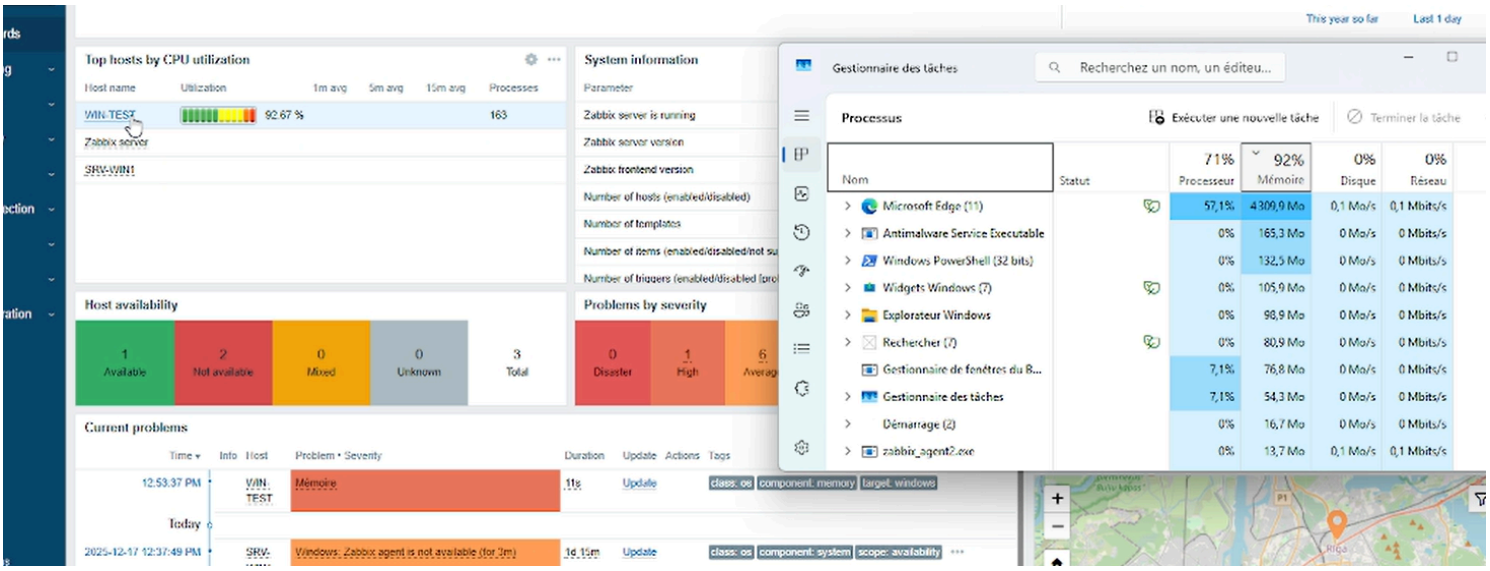

Figure 19 : Alertes sur Zabbix

Le système d'alerting est configuré avec des seuils critiques. En cas de dépassement (ex: disque rempli à 90% ou arrêt d'un service AD), une notification visuelle et mail est générée pour garantir un RTO minimal.

8. Mise en œuvre et automatisation (Scripts)

8.1 Panorama des outils d'automatisation

Cinq scripts principaux ont été développés pour couvrir le cycle de vie des utilisateurs :

- **user_functions.ps1** : Bibliothèque de fonctions mutualisées (journalisation, vérification d'existence).
- **create_user.ps1** : Script principal de provisioning des collaborateurs.
- **create_user_info.ps1** : Script spécialisé pour les privilèges élevés du service informatique.
- **disable_user.ps1** : Procédure de départ d'un collaborateur (désactivation et déplacement en OU "Quarantaine").
- **auto_quarantine.ps1** : Tâche planifiée pour sécuriser les comptes inactifs depuis plus de 90 jours.

8.2 Focus : Provisioning des utilisateurs (create_user.ps1)

```
PS C:\Scripts> .\create_user.ps1 -firstName John -lastName Johnny -Description description -isAdmin $false

=== SELECTION DU SITE ===
[0] SITE_ATLANTIS (Siege)
[1] SITE_SPRINGFIELD (Distant)
Ou tapez 'Q' pour quitter

Votre choix: 0

=== SELECTION DU SERVICE ===
Services disponibles sur SITE_ATLANTIS :
Ou tapez 'Q' pour quitter

[0] BDE
[1] CGF
[2] COMMERCIAL
[3] DIRECTION
[4] JURIDIQUE
[5] RH

Votre choix: 1

=======================================
L'utilisateur 'John Johnny' a ete cree avec succes !
Site: SITE_ATLANTIS
Service: CGF
Login: j.johnny
Mot de passe temporaire: Jjohnny2025!
IMPORTANT: L'utilisateur devra changer son mot de passe a la premiere connexion
=======================================

L'utilisateur 'j.johnny' a ete ajoute au groupe 'CGF'
L'utilisateur 'j.johnny' a-t-il le droit read sur les fichiers ? (o/N)
N
L'utilisateur 'j.johnny' n'aura pas les droits read.
L'utilisateur 'j.johnny' a-t-il le droit write sur les fichiers ? (o/N)
N
L'utilisateur 'j.johnny' n'aura pas les droits write.
L'utilisateur 'j.johnny' a-t-il le droit modify sur les fichiers ? (o/N)
N
L'utilisateur 'j.johnny' n'aura pas les droits modify.


Timestamp : 2025-12-10T15:15:31.9332836+01:00
Level     : INFO
Category  : create_user
Computer  : SRV-WIN1
User      : Administrateur
ProcessId : 4520
Source    : C:\Scripts\create_user.ps1
Message   : Utilisateur 'j.johnny' cree dans le service 'CGF' du site 'SITE_ATLANTIS'.


PS C:\Scripts>
```

Figure 20 : create_user.ps1

Le script **create_user.ps1** constitue la pièce maîtresse de cette automatisation. Lors de son exécution, il réalise plusieurs actions critiques de manière séquentielle. Il génère d'abord l'identifiant unique selon la convention définie, puis assure la création de l'arborescence des dossiers personnels sur le serveur

de fichiers. Enfin, il positionne les droits NTFS via les groupes Shadow et renseigne l'intégralité des attributs Active Directory. Cette méthode élimine tout risque d'erreur humaine et assure que chaque nouvel employé, qu'il soit rattaché au siège d'Atlantis ou au laboratoire de Springfield, bénéficie d'un environnement numérique prêt à l'emploi et sécurisé dès sa première connexion.

9. Analyse critique et améliorations

La réalisation de cette maquette a permis de valider la viabilité de l'architecture proposée pour XANADU, tout en nous confrontant à des réalités techniques formatrices. Si l'interconnexion des services et la sécurisation des flux sont aujourd'hui fonctionnelles, le processus de déploiement a révélé des limites inhérentes à l'environnement de simulation.

L'une des principales difficultés a concerné l'instabilité des protocoles de haute disponibilité, tels que le HSRP, au sein de l'émulateur GNS3. Suite à un incident électrique, nous avons constaté une rupture de l'intégrité de la couche ARP, rendant les adresses virtuelles (VIP) inopérantes. Cette contrainte nous a obligés à adapter notre stratégie en stabilisant le routage via des passerelles fixes pour la démonstration. Cet obstacle, bien que spécifique à la virtualisation, nous a permis de mieux appréhender les mécanismes de bascule réseau et l'importance de la persistance des tables d'adresses MAC dans un environnement de production réel.

Parallèlement, nous avons dû composer avec les limitations matérielles de la station de travail hôte. La puissance de calcul disponible s'est avérée juste pour supporter simultanément l'ensemble des contrôleurs de domaine et les serveurs de supervision gourmands en ressources comme Wazuh. Pour pallier ces ralentissements, nous avons optimisé l'allocation des ressources en privilégiant des versions "Core" pour certains services et en affinant le séquençage du démarrage des machines.

En guise de perspectives, l'infrastructure pourrait être encore renforcée par l'implémentation d'une authentification multi-facteurs (MFA) pour les accès VPN et par une automatisation plus poussée de la configuration réseau via des outils d'Infrastructure as Code (IaC) comme Ansible.

10. Conclusion

Le projet de modernisation du système d'information de l'entreprise XANADU aboutit à une infrastructure robuste, capable de répondre aux défis sécuritaires actuels. L'architecture déployée assure une segmentation réseau efficace, une gestion centralisée des identités et une protection proactive des terminaux grâce au durcissement des politiques Microsoft Defender.

La mise en œuvre de la règle de sauvegarde 3-2-1 et la centralisation de la supervision garantissent à la direction de XANADU une continuité d'activité conforme à leurs exigences métiers les plus strictes. Cette maquette démontre qu'en combinant des standards industriels comme Active Directory avec des solutions de sécurité avancées, il est possible d'offrir à une PME un environnement numérique aussi agile que sécurisé.

11. Table des figures