

# Livrable 2 : Projet système informatique et administration



Lisa ACHOUR,  
Enzo CADIERE,  
Maéva CHALLIES,  
Rayane OULDALI,  
Alejandro BAGLIVO

Année 2025-2026

## Table des matières

1) Table des figures	5
2) Équipe	6
3) Rappel du contexte et objectifs	7
4) Termes / Notions à définir	8
5) Attendus du livrable	9
6) Questionnaire de sécurité	10
a) Analyse de l'existant	10
b) Analyse du besoin	10
c) Le questionnaire	11
7) Mise en place des pare-feux	12
a) Rôle et Fonctionnement	12
b) Le Protocole CARP (Common Address Redundancy Protocol)	12
8) Politique de filtrage	13
a) Tableau d'autorisation des trafic inter-VLAN	14
b) Filtrage du site d'Atlantis	15
1. Filtrage VLAN 10 : Administration (10.0.10.0/24)	15
2. Filtrage VLAN 20 : Application (10.0.20.0/24)	16
3. Filtrage VLAN 30 : Postes Utilisateurs (172.16.0.0/16)	17
4. Filtrage VLAN 40 : Backup (10.0.40.0/24)	18
5. Filtrage VLAN 50 : DMZ / VPN (10.0.50.0/24)	18
6. Filtrage VLAN 60 : Imprimantes (10.0.60.0/24)	18
7. Filtrage VLAN 66 : Management (10.0.66.0/24)	19
c) Filtrage du site de Springfield	20
1. VLAN 110 : Supervision (10.1.10.0/24)	20
2. VLAN 120 : Postes Utilisateurs Labo (10.1.20.0/24)	20
3. VLAN 130 : Équipements Labo (10.1.30.0/24)	21
4. VLAN 140 : Imprimantes (10.1.40.0/24)	21
5. VLAN 150 : Active Directory (10.1.50.0/24)	21
6. VLAN 160 : Backup (10.1.60.0/24)	22
9) Exemples de scripts d'administration avec PowerShell	23
a) Création automatisée de l'arborescence de l'AD	23
b) Création automatique de tous les groupes (GG_/GA_/_)	24

c)	Création d'utilisateurs depuis un CSV, qui les placera dans la bonne OU plus groupe	25
d)	Désactivation automatique de comptes inactifs	26
e)	Inventaire AD (Utilisateurs + postes) exporté en CSV	26
f)	Sauvegarde toutes les GPO et les met dans un fichier horodate	27
g)	Contrôle quotidien de santé du domaine	27
h)	Mutation d'un utilisateur vers un autre service	28
i)	Alerte sur les mots de passe qui vont expirer	29
j)	Audit des comptes à priviléges	30
10)	Supervision	31
a)	Analyse de l'existant	31
b)	Analyse du besoin	32
1.	Besoins exprimés	32
2.	Contraintes	33
3.	Synthèse	33
c)	Solutions étudiées	33
1.	Zabbix	33
2.	Nagios / Nagios XI	34
3.	PRTG Network Monitor	34
4.	CheckMK	34
d)	Critères d'évaluation	35
1.	Coût total	35
2.	Facilité d'installation et maintenance	35
3.	Auto-découverte	35
4.	Support Windows / Linux	35
5.	Adaptabilité à une PME de 60 utilisateurs	35
6.	Courbe d'apprentissage	35
7.	Compatibilité multi-sites	35
8.	Scalabilité et volumétrie	35
e)	Histogramme d'évaluation des solutions de supervision	36
f)	Choix final	37
g)	Stratégie globale	37
1.	Système d'alerting	37
2.	Tableaux de bord	38

3.	Historisation et reporting	38
4.	Exemple d'évènements déclencheurs	38
h)	Schéma de l'architecture générale de la supervision	40

# 1) Table des figures

Figure 1 : Exemple type du questionnaire de sécurité	11
Figure 2 : Script de création automatique de l'arborescence de l'AD	23
Figure 3 : Script de la création automatique des groupes	24
Figure 4 : Script d'ajout des utilisateurs depuis CSV	25
Figure 5 : Script de désactivation automatique des comptes inactifs	26
Figure 6 : Script de l'inventaire automatique de l'AD	26
Figure 7 : Script de sauvegarde des GPO	27
Figure 8 : Script du contrôle de santé	27
Figure 9 : Script de mutation des utilisateurs vers d'autres services	28
Figure 10 : Script d'alerte des mots de passe qui vont expirer	29
Figure 11 : Script de l'audit des comptes à priviléges	30
Figure 12 : Histogramme d'évaluation des solutions de supervision	36
Figure 13 : Schéma de l'architecture générale de la surveillance	40

## 2) Équipe

Lisa ACHOUR : **Secrétaire**

Maéva CHALLIES : **Cheffe de projet / Scribe**

Enzo CADIÈRE : **Directeur technique**

Rayane OULDALI : **Groupe**

Alejandro BAGLIVO : **Gestionnaire du temps**

### 3) Rappel du contexte et objectifs

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

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

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

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

## 4) Termes / Notions à définir

Termes/ Notions	Définition
<b>Protocole CARP</b>	Partage d'une IP virtuelle entre plusieurs machines pour assurer la haute disponibilité.
<b>Pare-feu</b>	Filtre le trafic réseau selon des règles.
<b>Monitoring</b>	Surveillance continue d'un système ou réseau.
<b>Filtrage</b>	Action de bloquer/autoriser du trafic selon des critères.
<b>MPLS (Multiprotocol label)</b>	Acheminement réseau basé sur des labels, rapide et utilisé par les opérateurs.
<b>ACL (Access control list )</b>	Liste définissant qui peut accéder à quoi.
<b>DMZ (Demilitarized Zone)</b>	Zone réseau isolée pour les services exposés à Internet.
<b>OU (Organizational Unit )</b>	Dossier AD pour organiser utilisateurs et machines.
<b>Groupe AD</b>	Ensemble d'utilisateurs pour gérer des permissions.
<b>DC (Domain controller)</b>	Serveur qui authentifie les utilisateurs AD.
<b>GPO (Group policy object)</b>	Règle appliquée à des utilisateurs/ordinateurs dans AD.
<b>RPO (Recovery point objective )</b>	Perte de données maximale acceptable après un incident.
<b>RTO (Recovery time objective )</b>	Durée maximale pour rétablir un service après incident.
<b>NAS (Network attached storage )</b>	Stockage réseau accessible par plusieurs utilisateurs.
<b>ERP (Entreprise Ressource planning)</b>	Logiciel de gestion intégrée (production, finances, RH...).
<b>DLP (Data loss prevention)</b>	Protection contre la fuite de données sensibles.
<b>SLA (Service level agreement)</b>	Engagement de niveau de service entre client et fournisseur.
<b>EDR (Endpoint Detection and Response )</b>	Protection avancée des postes contre malwares et comportements suspects.
<b>MFA (Multi Facto Authentication )</b>	Authentification avec plusieurs facteurs (ex : mot de passe + SMS).
<b>IAM (Identity and Acess management)</b>	Gestion centralisée des identités et accès.
<b>Moindre privilège</b>	Donner seulement les accès strictement nécessaires.
<b>Audit Sécurité</b>	Analyse d'un système pour identifier failles et risques.
<b>VPN (Virtual Private Network)</b>	Connexion chiffrée pour accéder au réseau à distance.

## 5) Attendus du livrable

Dans le cadre de ce livrable, nous allons présenter les aspects suivants :

1. **Le questionnaire de sécurité avec les axes de remédiation**, les objectifs sont les suivants :
  - Identifier les vulnérabilités
  - Mesurer le niveau de sécurité :
    - o Des infrastructures
    - o Des données
    - o Des processus
  - Respecter les normes
  - Indiquer les axes de remédiation et les bonnes pratiques
2. **La politique de filtrage pare-feu** : décrire clairement la politique de filtrage à prévoir, justifier les choix et détailler les éléments suivants :
  - Équipement
  - Interface
  - Source
  - Destination
  - Protocole
  - Action
  - Description
  - Ordre d'application
3. **10 exemples de scripts d'administration avec PowerShell**, qui doivent être :
  - Fonctionnels
  - Commentés
  - Contextualisés dans le système mis en place
  - Respectueux des bonnes pratiques de codage :
    - o Structure et lisibilité
    - o Nommage
    - o Sécurité
    - o Robustesse
    - o Paramétrage
4. **Le dispositif de supervision + 10 événements déclencheurs.** Intégrer :
  - Description de la solution dont :
    - o Outils utilisés
    - o Méthodologie de collecte des données
    - o Schéma de l'architecture générale de la surveillance
  - Donner 10 exemples d'événements déclencheurs avec :
    - o Description de l'évènement
    - o Criticité
    - o Source
    - o Action déclenchée
    - o Justification de la pertinence de cet événement pour la sécurité

## 6) Questionnaire de sécurité

### a) Analyse de l'existant

Après avoir répondu à l'appel d'offre nous avons pu identifier l'organisation de l'équipe ainsi que les données critiques de l'ERP. Nous savons qu'il existe 7 départements différents.

- Service comptabilité et gestion financière
- Service commercial
- Bureau d'étude
- Service juridique
- Service RH
- Laboratoire sur site distant
- Direction de l'agence

Chaque département possède des utilisateurs ainsi que des techniciens qui possèdent les droits d'administration. À partir de cet instant, nous pouvons mettre en liste une série de questions pour mieux comprendre l'infrastructure actuelle de XANADU.

- Les utilisateurs disposent-t-il des droits administrateurs sur leur pc ?
- Les sauvegardes sont-elles manuelles ?
- Quel est l'accessibilité de l'ERP ?
- Comment s'organise l'utilisation des antivirus homogènes/hétérogènes ?
- Le NAS est-il ouvert à tous ?
- Comment s'organise la segmentation réseaux ?
- Quel est la gestion des documents importants ?

Cette liste de questions type audit est un avant-goût du questionnaire de sécurité qui est consultable via un document Excel séparé. De cette façon nous pouvons donner à XANADU un moyen de nous informer quant à l'organisation actuel de leur SI.

### b) Analyse du besoin

Nous avons été notifiés de données critiques. Les bases de données de l'ERP contiennent des informations sensibles :

- Informations personnelles
- Documents des services clients
- Conseil et commerce
- Les courriels professionnels : correspondances internes et externes importantes.

Voici les notions de sécurités importantes à rappeler :

- Gestion des identités
- Protection des postes de travail
- Sécurité du réseau
- Sécurité des serveurs
- Protection des données

- Continuité d'activité
- Sécurité applicative
- Sensibilisation et gouvernance

### c) Le questionnaire

Le questionnaire de sécurité s'organise autour de huit grands thèmes, qui reprennent l'ensemble des piliers essentiels de la cybersécurité au sein d'un système d'information. Il aide à faire le point sur le niveau de sécurité de l'entreprise, à mettre en lumière les atouts, mais aussi à cibler les zones de vulnérabilité.

L'objectif ? Permettre de définir clairement les priorités d'action. Chaque catégorie rassemble des questions concrètes, conçues pour fournir un diagnostic solide et directement utilisable.

Pour chaque question, un tableau Excel s'organisera sous trois colonnes. Question booléen, état de la SI actuelle, Point de remédiation et bonne pratique, c'est-à-dire les solutions à mettre en place.

Question booléenne	Etat actuel	Solution/Bonne pratique
--------------------	-------------	-------------------------

Exemple type :

Questionnaire Sécurité Livarble	Etat actuel	Solution/bonne pratique à mettre en place
<b>3 Gestion des identités et accès(IAM)</b>		
Une politique de mots de passe est elle actuellement appliquée ?		ajouter l'usage de gestionnaires de mots de passe, vérifier la conformité avec les standards NIST, imposer la rotation uniquement pour comptes sensibles.
Les comptes génériques sont-ils limités et documentés ?		mise en place de comptes nominatifs + traçabilité, journalisation des accès, suppression progressive des comptes partagés.
La séparation des priviléges est-elle effective ?		adoption du principe du moindre privilège, comptes administrateurs distincts des comptes utilisateurs, PAM (Privileged Access Management).
Une authentification multi-facteurs est-elle déployée pour les accès sensibles ?		étendre MFA à toutes les applications critiques, privilégier des méthodes modernes
Quelle est la gestion des départs ? Si oui comment est elle effectuer (% de comptes désactivés à temps)		automatiser la désactivation des comptes via RH/IT, audits réguliers des comptes inactifs.

Figure 1 : Exemple type du questionnaire de sécurité

Le questionnaire est créé pour XANADU. Ils doivent répondre de façon à nous en apprendre plus sur leur infrastructure. L'ensemble des questions sont posées de façon à recevoir une sortie booléenne en réponse. La partie Solution & bonne pratique est déjà préremplie par précaution.

L'ensemble du questionnaire est disponible sous forme de fichier Excel en document séparé sous le nom « Questionnaire\_de\_Sécurité ».

## 7) Mise en place des pares-feux

Nous avons configuré de la haute disponibilité (H1), qui est configuré en actif/passif (ou Active/Standby), garantit qu'en cas de panne, le service de filtrage et de routage n'est pas interrompu.

### a) Rôle et Fonctionnement

Pare-feu Actif (Primary) : C'est l'équipement qui traite activement tout le trafic réseau. Il répond aux requêtes, effectue le filtrage, le NAT (Network Address Translation), et gère les sessions en cours.

Pare-feu Passif/Secours (Standby), cet équipement est en veille. Il est synchronisé en permanence avec le pare-feu actif pour recevoir l'état des sessions et la table de configuration. Il ne traite aucun trafic utilisateur directement. Si le pare-feu actif tombe en panne (matériel, logiciel, alimentation, etc.), le pare-feu passif prend immédiatement le relais et devient le nouvel actif. Ce processus s'appelle le Failover.

### b) Le Protocole CARP (Common Address Redundancy Protocol)

CARP est le protocole qui permet aux deux pares-feux de partager les mêmes adresses IP (virtuelles) et d'assurer le basculement rapide.

## 8) Politique de filtrage

Une politique de filtrage permet d'autoriser ou d'interdire les utilisations et accès de certains services selon le cas d'utilisation, elle permet également de limiter la diffusion de services illicites (virus ...). Elle est mise en place dans la périphérie du réseau afin de filtrer l'utilisation du réseau par les utilisateurs.

Dans le respect de notre cartographie du système informatique, chaque VLAN devra posséder ses propres règles de filtrage. Certaines machines internes à certains VLANs peuvent avoir des règles de filtrage supplémentaire.

Nous allons nous concentrer sur la politique de filtrage des pare-feux principaux du site d'Atlantis (FIREWALL 1 et 2, fonctionnant en haute disponibilité) ainsi que ceux du site de Springfield, car ce sont eux qui gèrent l'accès Internet, le VPN, la liaison inter-sites (MPLS) et le routage inter-VLAN.

#### a) Tableau d'autorisation des trafic inter-VLAN

## b) Filtrage du site d'Atlantis

### 1. Filtrage VLAN 10 : Administration (10.0.10.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
210	WSUS-01	Internet	HTTPS(443), TCP/8530- 8531	Autoriser	Téléchargement des mises à jour.	<b>Justification :</b> Nécessaire pour la sécurité des postes (MAJ centralisées). <b>Ordre :</b> Dans la section MCO (200), priorité sur les flux métiers.
230	DC-01/02	Internet	DNS (UDP 53), TCP/88, TCP/389, TCP/636	Autoriser	Résolution DNS publique.	<b>Justification :</b> Essentiel pour le bon fonctionnement d'AD, même si les requêtes des clients sont résolues en interne. <b>Ordre :</b> Dans la section MCO, nécessaire avant les accès métiers.
310	VLAN 30/VPN	FS-01	SMB (445)	Autoriser	Accès aux partages de fichiers.	<b>Justification :</b> Flux métier principal vers le serveur de fichiers (partages et dossiers personnels). <b>Ordre :</b> Section des flux métiers (300).
400	DC-01/02	VLAN 150 (RODC)	AD Ports	Autoriser	RéPLICATION Active Directory.	<b>Justification :</b> Assurer la cohérence AD inter-sites via MPLS. <b>Ordre :</b> Section inter-sites (400).
420	VLAN 120 (Labo)	FS-01 (Bureau d'étude)	SMB (445)	Autoriser	Accès Lecture Seule aux dossiers du Bureau d'étude.	<b>Justification :</b> Exigence métier spécifique pour le laboratoire. <b>Ordre :</b> Section inter-sites (400), après la réPLICATION AD.

999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	<b>Justification :</b> Sécurité par défaut : interdire tout ce qui n'est pas explicitement autorisé. <b>Ordre :</b> Toujours la dernière règle.
-----	-----	-----	-----	---------------------	---------------------------	--

## 2. Filtrage VLAN 20 : Application (10.0.20.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
320	VLAN 30/VPN	ERP-APP	HTTPS (443)	Autoriser	Accès des utilisateurs à l'interface de l'ERP.	Justification : Flux métier vers l'application, sécurisé en HTTPS. Ordre : Section flux métiers (300).
330	ERP-APP	ERP-DB	PostgreSQL (5432)	Autoriser	Communication Applicative interne ERP.	Justification : Essentiel au fonctionnement de l'ERP (Application $\rightarrow$ Base de données). Ordre : Immédiatement après l'accès à l'application.
410	VLAN 120 (Labo)	ERP-APP	HTTPS (443)	Autoriser	Accès des utilisateurs Labo à l'ERP.	Justification : Exigence métier spécifique. Ordre : Section inter-sites (400).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut. Ordre : Toujours la dernière règle.

### 3. Filtrage VLAN 30 : Postes Utilisateurs (172.16.0.0/16)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
300	VLAN 30	Internet	DNS (53), HTTP(80), HTTPS (443)	Autoriser	Accès Internet et Office 365 des postes.	Justification : Nécessité de navigation et de communication (O365). Ordre : Flux métier prioritaire.
310	VLAN 30	FS-01 (VLAN 10)	SMB (445)	Autoriser	Accès aux dossiers partagés.	Justification : Flux métier vers le serveur de fichiers. Ordre : Section flux métiers (300).
320	VLAN 30	ERP-APP (VLAN 20)	HTTPS (443)	Autoriser	Accès à l'ERP.	Justification : Flux métier vers l'ERP. Ordre : Section flux métiers (300).
340	VLAN 30	VLAN 60 (Imprimantes)	TCP 9100, SNMP	Autoriser	Impression.	Justification : Nécessité d'impression. Ordre : Section flux métiers (300).
430	VLAN 30 (Bureau d'étude)	Equipements Labo (VLAN 130)	Spécifique	Autoriser	Accès aux données et pilotage Labo.	Justification : Exigence métier spécifique inter-sites. Ordre : Section inter-sites (400).
999	Any	Anye	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut. Ordre : Toujours la dernière règle.

#### 4. Filtrage VLAN 40 : Backup (10.0.40.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
220	TRUENAS-01	VLAN 10/20/130/150	SMB/SSH/etc, TCP/8007 Proxmox Backup	Autoriser	Flux de sauvegarde initiés par le serveur de backup.	Justification : Essentiel pour la reprise d'activité (PCA/PRA). Le flux est initié uniquement par le VLAN de sauvegarde pour l'isoler des menaces. Ordre : Section MCO (200), très critique.
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut : interdire tout accès au VLAN de sauvegarde non lié à la sauvegarde elle-même. Ordre : Toujours la dernière règle.

#### 5. Filtrage VLAN 50 : DMZ / VPN (10.0.50.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
440	VPN WireGuard	VLAN 10/20/30	Services Autorisés	Autoriser	Accès des télétravailleurs aux ressources internes.	<b>Justification</b> : Répond au besoin de connexion à distance. <b>Ordre</b> : Section intersites et distants (400).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	<b>Justification</b> : Sécurité par défaut. <b>Ordre</b> : Toujours la dernière règle.

#### 6. Filtrage VLAN 60 : Imprimantes (10.0.60.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
340	VLAN 60	VLAN 30	TCP 9100	Autoriser	Réponse à la demande d'impression.	Justification : Permettre le retour du flux d'impression. Ordre : Section flux métiers (300).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut : limiter les communications des périphériques d'impression. Ordre : Toujours la dernière règle.

## 7. Filtrage VLAN 66 : Management (10.0.66.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
100	VLAN 66	FIREWALL 1/2	SSH (22), HTTPS (443)	Autoriser	Accès à l'administration du Pare-feu.	Justification : Essentiel pour la gestion et l'auto-protection du pare-feu (ANSSI R1). Ordre : Section d'auto-protection (100), la plus haute priorité.
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut. Ordre : Toujours la dernière règle.

## c) Filtrage du site de Springfield

### 1. VLAN 110 : Supervision (10.1.10.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
200	Any (VLAN 120/130/140)	LAB-01/02	Syslog	Autoriser	Collecte des logs sur les serveurs Linux du laboratoire.	Justification : Traçabilité locale des événements. Ordre : Section MCO (200).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut. Ordre : Toujours la dernière règle.

### 2. VLAN 120 : Postes Utilisateurs Labo (10.1.20.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
410	VLAN 120	ERP-APP (VLAN 20)	HTTPS (443)	Autoriser	Accès à l'ERP du site principal.	Justification : Exigence métier via MPLS. Ordre : Section inter-sites (400).
420	VLAN 120	FS-01 (VLAN 10)	SMB (445)	Autoriser	Accès Lecture Seule aux dossiers du Bureau d'étude.	Justification : Exigence métier via MPLS. Ordre : Section inter-sites (400).
450	VLAN 120	VLAN 140 (Imprimantes)	TCP 9100, SNMP	Autoriser	Impression.	Justification : Nécessité d'impression. Ordre : Section inter-sites (400).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut. Ordre : Toujours la dernière règle.

### 3. VLAN 130 : Équipements Labo (10.1.30.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
430	VLAN 30 (Bureau d'étude)	VLAN 130	Spécifique	Autoriser	Accès aux équipements de Labo pour le Bureau d'étude.	Justification : Exigence métier via MPLS. Ordre : Section inter-sites (400).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut : isoler les équipements sensibles du labo. Ordre : Toujours la dernière règle.

### 4. VLAN 140 : Imprimantes (10.1.40.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
450	VLAN 140	VLAN 120	TCP 9100	Autoriser	Réponse à la demande d'impression.	Justification : Permettre le retour du flux d'impression. Ordre : Section flux métiers (400).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut. Ordre : Toujours la dernière règle.

### 5. VLAN 150 : Active Directory (10.1.50.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
400	DC-03 (RODC)	VLAN 10 (Atlantis DC)	AD Ports	Autoriser	RéPLICATION Active Directory (flux initié par le RODC).	Justification : Essentiel pour la connexion des utilisateurs de Springfield. Ordre : Section inter-sites (400).
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut : isoler le contrôleur de domaine. Ordre : Toujours la dernière règle.

## 6. VLAN 160 : Backup (10.1.60.0/24)

Ordre	Source	Destination	Protocole	Action	Description	Justification et Ordre
220	TRUENAS-02	VLAN 110/120/130/150	SMB/SSH/etc.	Autoriser	Flux de sauvegarde initiés par le serveur de backup.	Justification : Essentiel pour la continuité d'activité du laboratoire. Ordre : Section MCO (200), très critique.
999	Any	Any	Any	Interdire (Drop)	Règle implicite de refus.	Justification : Sécurité par défaut : isoler le réseau de Backup. Ordre : Toujours la dernière règle.

---

## 9) Exemples de scripts d'administration avec PowerShell

### a) Création automatisée de l'arborescence de l'AD

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

Figure 2 : Script de création automatique de l'arborescence de l'AD

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

## b) Création automatique de tous les groupes (GG\_ /GA\_ /)

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

Figure 3 : Script de la création automatique des groupes

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

## c) Création d'utilisateurs depuis un CSV, qui les placera dans la bonne OU plus groupe

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

Figure 4 : Script d'ajout des utilisateurs depuis CSV

Ce script génère les comptes utilisateurs à partir d'un fichier CSV et les place directement dans les bonnes OUs et groupes, ce qui accélère l'onboarding, supprime les manipulations répétitives et assure une configuration correcte dès la création du compte.

#### d) Désactivation automatique de comptes inactifs

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

Figure 5 : Script de désactivation automatique des comptes inactifs

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

#### e) Inventaire AD (Utilisateurs + postes) exporté en CSV

```
1 Script-inventaire-utilisateurs.ps1
2
3 Import-Module ActiveDirectory
4
5 # Inventaire des utilisateurs
6 Get-ADUser -Filter * -Properties Enabled,LastLogonDate,Department |
7 Select-Object SamAccountName,Name,Enabled,Department,LastLogonDate |
8 Export-Csv "C:\Admin\inventaire_utilisateurs.csv" -NoTypeInformation -Delimiter ';'
9
10 # Inventaire des ordinateurs
11 Get-ADComputer -Filter * -Properties OperatingSystem,IPv4Address,LastLogonDate |
12 Select-Object Name,OperatingSystem,IPv4Address,LastLogonDate |
13 Export-Csv "C:\Admin\inventaire_ordis.csv" -NoTypeInformation -Delimiter ';'
14
15 Write-Host "Inventaires générés."
```

Figure 6 : Script de l'inventaire automatique de l'AD

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

## f) Sauvegarde toutes les GPO et les met dans un fichier horodate

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

Figure 7 : Script de sauvegarde des GPO

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

## g) Contrôle quotidien de santé du domaine

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

Figure 8 : Script du contrôle de santé

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

## h) Mutation d'un utilisateur vers un autre service

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

Figure 9 : Script de mutation des utilisateurs vers d'autres services

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

## i) Alerte sur les mots de passe qui vont expirer

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

Figure 10 : Script d'alerte des mots de passe qui vont expire

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

## j) Audit des comptes à privilèges

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

Figure 11 : Script de l'audit des comptes à privilèges

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

## 10) Supervision

### a) Analyse de l'existant

XANADU ne dispose d'aucun système de supervision digne de ce nom. Actuellement, la détection des problèmes se fait uniquement après coup.

#### L'existant chez XANADU :

- Quelques scripts PowerShell tournent pour gérer les sauvegardes, mais sans aucun contrôle pour vérifier qu'elles se sont bien déroulées
- De temps à autre, quelqu'un va consulter manuellement les interfaces d'administration (ESXi, NAS, etc.)
- Aucun système d'alerte automatique quand un problème survient
- Pas de traçabilité ni d'historique des événements système

#### Les impacts concrets de cette situation :

- Les pannes sont détectées beaucoup trop tard (parfois plusieurs heures, voire plusieurs jours après leur survenue)
- Le RTO de 4 heures exigé par la direction devient totalement irréaliste dans ces conditions
- Aucune visibilité sur l'évolution des ressources critiques (par exemple, des disques qui saturent progressivement sans que personne ne s'en aperçoive)
- Des sauvegardes peuvent échouer pendant plusieurs semaines sans que l'équipe en soit informée
- L'équipe IT fonctionne en permanence dans l'urgence au lieu de pouvoir anticiper les incidents

#### Les manques identifiés :

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

## b) Analyse du besoin

### 1. Besoins exprimés

Être capable de repérer les problèmes avant que les utilisateurs ne s'en plaignent, garantir les délais de remise en route annoncés (pas plus de 4 heures pour ce qui est vital, maximum 24 heures pour le reste), avoir accès à un tableau de bord compréhensible d'un coup d'œil, et récupérer des chiffres concrets pour défendre les demandes de matériel ou de budget.

Les éléments à mettre sous surveillance sont donc les suivants :

#### **Côté serveurs :**

- Le contrôleur de domaine : vérifier qu'il reste de la place sur les disques, que l'Active Directory tourne correctement avec le DNS et le DHCP, que la réPLICATION fonctionne bien, et que les authENTIFICATIONS passent sans accroc
- L'hyperviseur ESXi : s'assurer que la machine physique va bien, surveiller l'état des VMs qui tournent dessus, garder un œil sur comment le stockage est utilisé
- Le serveur qui héberge l'ERP : voir si l'application répond normalement, contrôler que la base de données n'est pas à la ramasse
- Le NAS : surveiller le remplissage des disques, regarder les indicateurs SMART pour anticiper les pannes de disques, vérifier que le partage de fichiers SMB est opérationnel

#### **Infrastructure réseau :**

- La ligne MPLS qui relie à Springfield : s'assurer que les engagements du prestataire sont tenus (temps de réponse qui ne dépasse pas 50ms, stabilité avec moins de 10ms de variation, perte de paquets quasi inexistante à moins de 0,1%)
- Le routeur et le pare-feu
- Tous les switchs répartis sur le réseau

#### **Applications et services utilisés :**

- L'interface web pour accéder à l'ERP
- Les dossiers partagés sur le réseau
- La suite Office 365

#### **Gestion des sauvegardes :**

- Savoir si chaque sauvegarde s'est bien passée ou a planté
- Vérifier qu'on a bien une copie récente (idéalement de moins d'une journée)
- Contrôler la taille de ce qui est sauvegardé
- Voir combien d'espace il reste pour les prochaines sauvegardes

#### **L'agence de Springfield :**

- Le contrôleur de domaine qui fait backup
- Les machines qui tournent sous Linux là-bas
- Tout le matériel réseau sur place

## 2. Contraintes

- Budget limité : XANADU n'a pas énormément de marge financière, donc il vaut mieux partir sur une solution gratuite (CheckMK Raw plutôt qu'une version payante)
- Délai court : La présentation est calée semaine 51, il faut donc pouvoir déployer rapidement sans passer des semaines à tout configurer
- Compétences : L'interface doit rester accessible, pas besoin d'être un expert pour s'en servir, avec une courbe d'apprentissage qui reste raisonnable
- Scalabilité : La solution doit pouvoir évoluer avec les besoins sans avoir à tout recommencer dans quelques années
- Pérennité : Privilégier un outil qui a une communauté active derrière et qui continue d'avoir des mises à jour régulières

## 3. Synthèse

### *Écart existant/besoin*

Aspect	Existant	Besoin	Écart
Détection	Manuelle, posteriori	a Automatique, temps réel	CRITIQUE
Alertes	Aucune	Email/SMS selon criticité	CRITIQUE
Visibilité	Nulle	Dashboards multi- profils	MAJEUR
Historique	Inexistant	90 jours + tendances	MAJEUR
Multi-sites	N/A	Supervision Atlantis + Springfield	NÉCESSAIRE
Traçabilité	Aucune	Logs 90j + rapports RTO	IMPORTANT

### *Priorités de supervision*

P1 (impact immédiat) : Services ERP, DC, espace disque serveurs, lien MPLS, sauvegardes

P2 (dégradation rapide) : Performances serveurs (CPU/RAM), ESXi, NAS/partages, santé matérielle

P3 (optimisation) : Imprimantes, métriques réseau avancées, métriques applicatives

## c) Solutions étudiées

Nous avons étudié les principales solutions disponibles sur le marché

### 1. Zabbix

#### *Points forts :*

- Solution open source
- Communauté d'utilisateur et documentation importante
- Très flexible et personnalisable
- Supporte nativement la plupart des protocoles (SNMP, ICMP, IPMI, etc...)

**Points faibles :**

- Courbe d'apprentissage abrupte
- Configuration initiale relativement complexe
- L'installation et la maintenance demande des bases solides
- Les templates peuvent demander des ajustements importants

## 2. Nagios / Nagios XI

**Points forts :**

- Très stable et éprouvé
- Beaucoup de plugins disponibles
- Version Core gratuite et open source

**Points faibles :**

- Interface graphique très vieillissante
- Configuration à l'aide de fichiers textes uniquement pour la version Core
- Pas d'auto-découverte des matériels réseau
- Nécessite beaucoup de configuration pour atteindre un niveau fonctionnel

## 3. PRTG Network Monitor

**Points forts :**

- Interface web très moderne et agréable
- Installation simple et rapide sous Windows
- Autoconfiguration efficace qui configure automatiquement les différents capteurs
- Support technique commercial réactif

**Points faibles :**

- Solution commercial propriétaire avec coûts par capteur
- Moins adapté au environnements Linux (Springfield)
- Historisation des données faibles pour la version de base

## 4. CheckMK

**Points forts :**

- Interface moderne et intuitive
- Auto-découverte automatique des services avec configuration automatique des seuils
- Version RAW (Gratuite) très complète
- Bonne gestion des enivrements hétérogènes
- Documentation claire et en Français
- Historisation native sur plusieurs mois

**Points faibles :**

- Moins connu que Zabbix ou Nagios donc moins de ressources communautaires
- Nécessite un serveur Linux pour l'installation

## d) Critères d'évaluation

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

### 1. Coût total

**Pourquoi ?**

PME de 60 personnes, budget limité

### 2. Facilité d'installation et maintenance

**Pourquoi ?**

Pas d'équipe IT dédiée, correspondants informatiques par service

### 3. Auto-découverte

**Pourquoi ?**

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

### 4. Support Windows / Linux

**Pourquoi ?**

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

### 5. Adaptabilité à une PME de 60 utilisateurs

**Pourquoi ?**

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

### 6. Courbe d'apprentissage

**Pourquoi ?**

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

### 7. Compatibilité multi-sites

**Pourquoi ?**

Architecture à 2 sites distants avec liaison MPLS

### 8. Scalabilité et volumétrie

**Pourquoi ?**

Croissance prévue de l'entreprise

## e) Histogramme d'évaluation des solutions de supervision

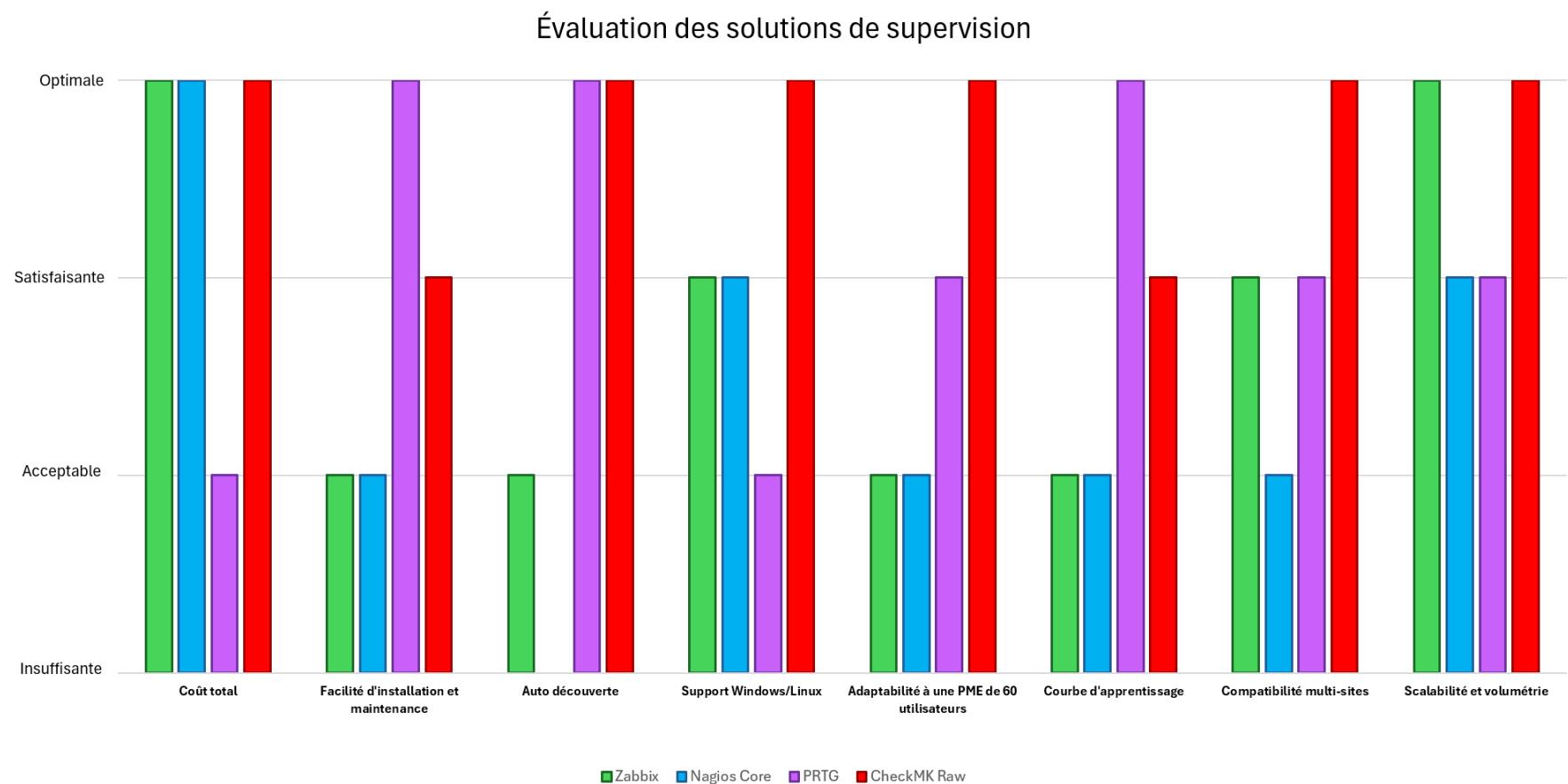


Figure 12 : Histogramme d'évaluation des solutions de supervision

## f) Choix final

Après analyse des différentes solutions, CheckMK nous semble être le meilleur choix pour XANADU.

### **Répond parfaitement à vos besoins**

CheckMK permet de configurer des alertes qui distinguent les services critiques (ERP, RTO 4h) des services standards (RTO 24h). Les tableaux de bord donnent à la direction une vision claire du SI sans compétences techniques particulières.

### **Économique**

La version gratuite offre toutes les fonctionnalités nécessaires sans limite d'équipements. Contrairement à PRTG qui facture par capteur, CheckMK quant à lui surveille toute l'infrastructure.

### **Compatible multi-sites**

Les agents consomment peu de bande passante et la latence garantie assure des remontées temps réel. CheckMK gère nativement la supervision multi-sites avec filtrage par localisation.

### **Évolutif et simple d'utilisation**

L'ajout de nouveaux serveurs se fait en quelques clics. Si besoin, la migration vers la version Enterprise est transparente.

### **Sécurité intégrée**

CheckMK conserve les logs 90 jours et trace les notifications envoyées ce qui est parfait pour des audits.

## g) Stratégie globale

### 1. Système d'alerting

Niveau	Déclencheurs	Notification
CRITIQUE	ERP/DC, MPLS coupé, disque > 95%, backup > 24h	Email + SMS 24/7
ÉLEVÉ	CPU > 85%, disque > 85%, tentative authentification, erreurs matérielles	Email immédiat (heures ouvrées)
MOYEN	CPU > 70%, certificat < 30j, dégradations	Email quotidien/hebdo
INFO	Backup OK, redémarrages planifiés	

**Destinataires** : L'admin reçoit tout ce qui est critique et important, la direction uniquement les alertes vraiment critiques, et les correspondants ne voient que ce qui concerne leur service.

**Anti-saturation** : On met un délai entre deux alertes similaires pour éviter le spam, on regroupe les alertes qui tombent en même temps, on évite de spam en dehors des heures de bureau quand c'est possible, et on demande un accusé de réception.

## 2. Tableaux de bord

- Direction : Des indicateurs simples en vert/orange/rouge, le taux de disponibilité du mois, les 3 incidents principaux, et quelques courbes pour voir les tendances
- Technique : Une vue détaillée avec tous les paramètres, des graphiques sur les 7 derniers jours, les alertes qui sont actives en ce moment, et l'accès aux logs
- Correspondants : Une vue qui filtre juste leur service, leurs postes de travail, et leurs quotas de stockage

## 3. Historisation et reporting

- Rétention : On garde les données détaillées pendant 90 jours, puis on passe à des données agrégées conservées 1 an
- Rapports : Un point hebdo pour l'admin, un bilan mensuel pour la direction, et un récap trimestriel lors des revues

## 4. Exemple d'évènements déclencheurs

### **Disque du DC presque plein**

L'espace disque du contrôleur de domaine est critique : seulement 5 % restant. Des notifications critiques ont été envoyées par mail et SMS.

### **Liaison MPLS Springfield**

Le lien MPLS est actuellement indisponible, bloquant l'activité du laboratoire. L'équipe IT a été alertée immédiatement.

### **Sauvegarde ERP échouée**

Aucune sauvegarde valide de l'ERP n'a été effectué depuis plus de 24 heures. Cela représente un risque en cas de défaillance. Une alerte critique a été déclenchée.

### **Charge CPU sur ESXi élevée**

Le processeur d'un serveur ESXi dépasse 85 % d'utilisation depuis plus de 15 minutes. Une alerte de niveau élevé a été transmise.

### ***ERP inaccessible***

L'interface web de l'ERP est indisponible, ce qui bloque les processus métiers. Une notification de niveau élevé est donc transmise.

### ***Disque NAS à risque***

Les indicateurs SMART signalent un risque imminent de panne des disques du NAS. Une alerte élevée a été activée.

### ***Suspicion d'intrusion sur Active Directory***

Plusieurs échecs d'authentification ont été détectés. L'alerte a été classée comme élevée afin de lancer un audit de sécurité.

### ***Stockage en augmentation***

Les partages atteignent 87 % de leur capacité et continuent de se remplir. Une alerte de niveau moyen est en place pour anticiper la saturation.

### ***Certificat SSL bientôt expiré***

Le certificat SSL du serveur web expirera dans 25 jours. Une alerte de niveau moyen est donc transmise

### ***Sauvegarde quotidienne réussie***

La sauvegarde du jour a été réalisée avec succès. Une notification a été envoyée pour information et suivi d'audit.

## h) Schéma de l'architecture générale de la supervision

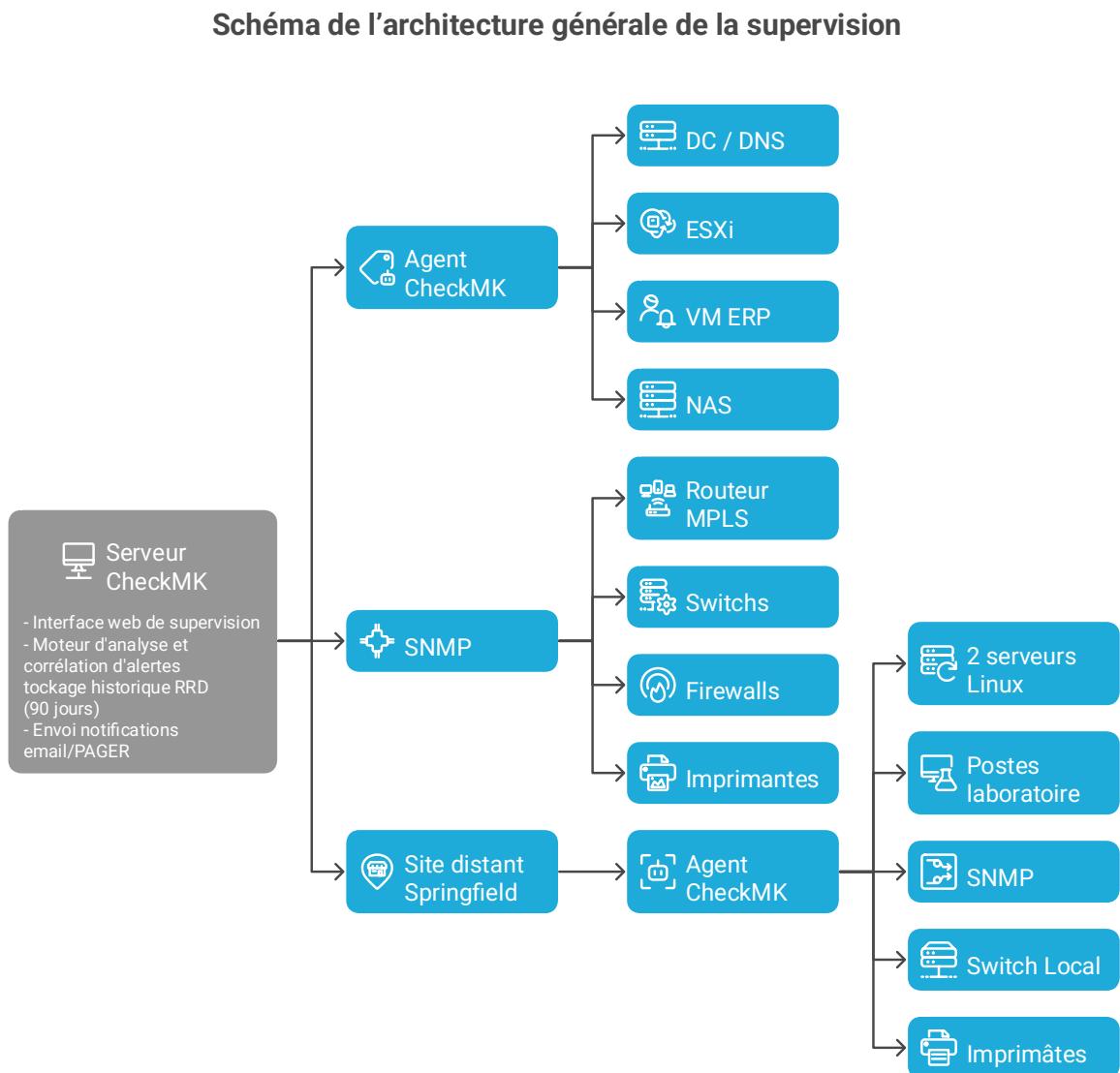


Figure 13 : Schéma de l'architecture générale de la surveillance