Mise en place d’une infrastructure pédagogique virtualisée et sécurisée :

BTS Services Informatiques aux Organisations
Option SISR – Solutions d’Infrastructure, Systèmes et Réseaux

Épreuve E6 – Administration des systèmes et des réseaux

Épreuve E5 – Support et mise à disposition de service Informatique

Candidat : Clovis Langlois
Formation : BTS SIO – Option SISR
Année scolaire : 2025 – 2026

Table des matières

1. Contexte du projet

Ce projet s'inscrit dans le cadre des épreuves **E5 – Support et mise à disposition de service Informatique et E6 – Administration des systèmes et des réseaux** du **BTS Services Informatiques aux Organisations (SIO), option SISR**.

L'objectif de ce travail est de concevoir, déployer et administrer une infrastructure informatique complète, virtualisée et sécurisée, en s'appuyant sur des technologies couramment utilisées en entreprise.
Le projet vise à mettre en pratique les compétences liées à l'administration des systèmes, à la gestion des réseaux, à la sécurité, à la supervision et à l'exploitation d'une infrastructure informatique.

L'environnement mis en place repose sur une architecture segmentée, intégrant des systèmes d'exploitation hétérogènes (Windows et Linux), des services d'annuaire, des outils de supervision, de gestion de parc, d'authentification centralisée ainsi que des services applicatifs.

2. Présentation du cas fictif : Langéo Education

Langéo Education est une filiale d'une holding familiale fictive spécialisée dans le conseil et l'apprentissage à destination des enfants et adolescents.
L'entreprise propose des cours généraux, notamment en **français** et en **mathématiques**, ainsi que des services d'accompagnement pédagogique.

Dans le cadre de son développement, Langéo Education souhaite disposer d'une **infrastructure informatique fiable, sécurisée et évolutive**, permettant :

- la gestion centralisée des utilisateurs et des ressources,
- la sécurisation des accès internes et externes,
- la supervision des serveurs et des services critiques,
- la gestion du parc informatique,
- la mise à disposition de services applicatifs internes,
- l'exposition contrôlée de services vers l'extérieur via une zone démilitarisée (DMZ).

L'infrastructure doit également servir de **support pédagogique**, simulant le système d'information d'une PME réelle, tout en respectant les bonnes pratiques d'administration systèmes et réseaux.

3. Objectifs du projet

L'objectif principal de ce projet est de concevoir et de mettre en œuvre une infrastructure informatique complète répondant aux besoins de l'organisation fictive **Langéo Education**, tout en respectant les bonnes pratiques d'administration des systèmes et des réseaux.

Les objectifs techniques et pédagogiques sont les suivants :

- Concevoir une architecture réseau segmentée et sécurisée à l'aide de VLAN.
- Déployer une infrastructure virtualisée permettant l'hébergement de plusieurs services.
- Mettre en place un service d'annuaire centralisé pour la gestion des utilisateurs et des ressources.
- Assurer la supervision des serveurs et des services critiques.
- Mettre en œuvre des services de gestion de parc et de gestion de projet.
- Déployer une solution d'authentification centralisée (SSO).
- Exposer des services applicatifs de manière sécurisée via une zone DMZ.
- Documenter l'ensemble des étapes d'installation, de configuration et d'exploitation.

Ce projet permet de mobiliser les compétences attendues dans le cadre des épreuves E5 et E6 du BTS SIO option SISR.

4. Périmètre technique

4.1 Environnement de virtualisation

- Hyperviseur : **Proxmox**
- Hébergement de l'ensemble des machines virtuelles du projet

4.2 Architecture réseau

- Pare-feu / Routeur : **pfSense**
- Segmentation réseau par VLAN :
    - VLAN 10 : Serveurs
    - VLAN 20 : Utilisateurs (DHCP)
    - VLAN 30 : DMZ
- Routage et filtrage inter-VLAN assurés par pfSense

4.3 Systèmes d'exploitation

- Windows Server 2025 : Active Directory, DNS
- Windows Server 2022 : Autorité de certification (AD CS)
- Debian : Zabbix, GLPI, Kanboard, Keycloak, Docker

4.4 Services déployés

- Annuaire : Active Directory (AD DS)
- Supervision : Zabbix
- Gestion de parc : GLPI
- Gestion de projet : Kanboard
- Authentification centralisée : Keycloak (OIDC / LDAP)
- Services Web : Docker (site vitrine en DMZ)

5. Présentation globale de l’architecture réseau

L’infrastructure informatique mise en place pour le projet **Langéo Education** repose sur une architecture virtualisée et segmentée, conçue afin de répondre aux exigences de sécurité, de performance et d’évolutivité d’une organisation de type PME.

L’ensemble des services est hébergé sur un hyperviseur **Proxmox**, permettant la centralisation et l’isolation des différentes machines virtuelles.
La gestion des flux réseau, du routage et de la sécurité est assurée par un pare-feu **pfSense**, positionné comme point central de l’architecture.

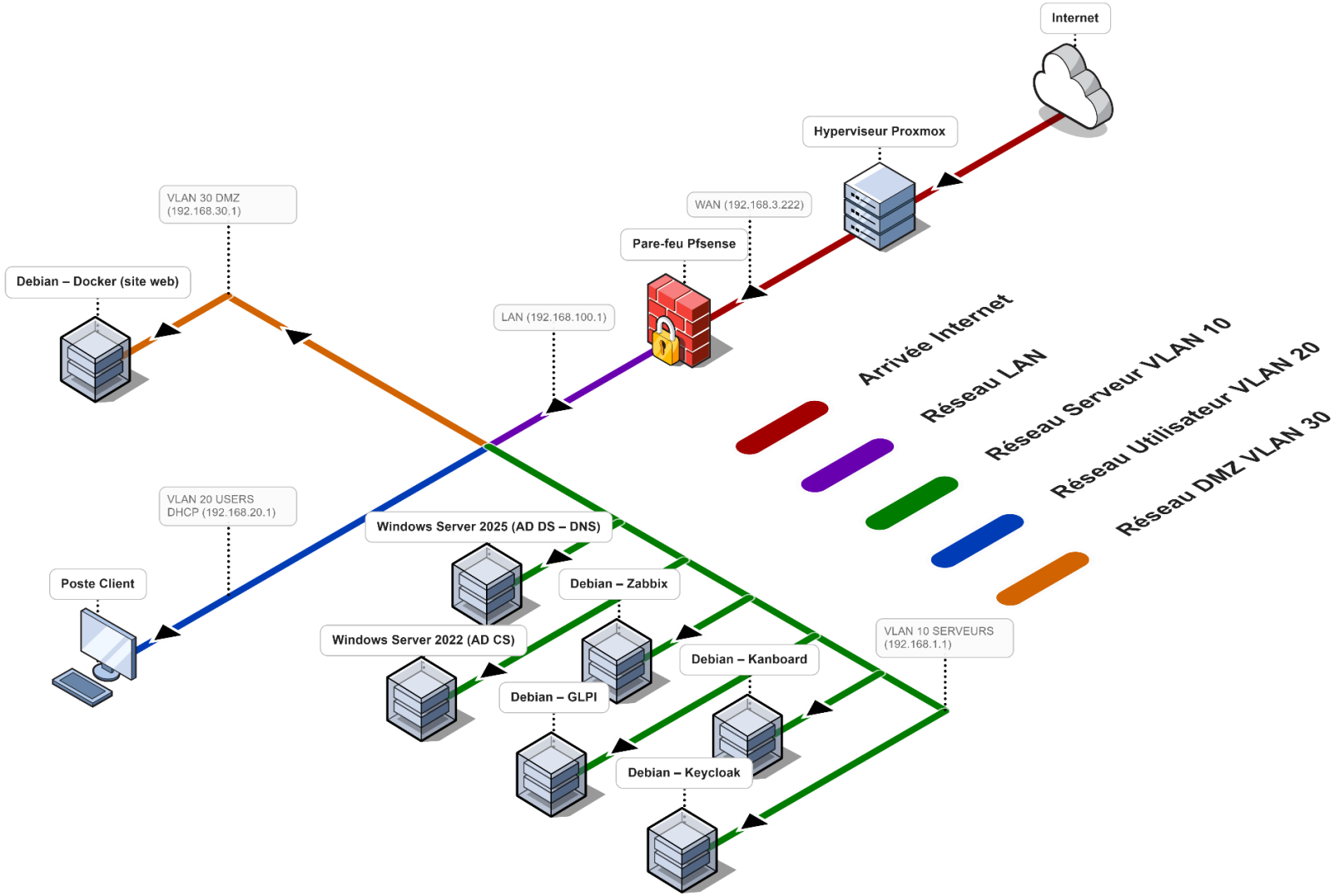
Le réseau interne est segmenté à l’aide de **VLAN**, afin de séparer les différents usages et de limiter les communications au strict nécessaire. Cette segmentation permet notamment :

- d’isoler les serveurs des postes utilisateurs,
- de sécuriser l’exposition de services vers l’extérieur,
- d’appliquer le principe du moindre privilège sur les flux inter-réseaux.

Une **zone démilitarisée (DMZ)** est dédiée à l’hébergement des services accessibles depuis l’extérieur, tandis que les services critiques internes (annuaire, supervision, gestion de parc) sont isolés dans un segment serveur dédié.

L’architecture a été conçue de manière évolutive afin de permettre l’ajout de nouveaux services ou de nouveaux utilisateurs sans remise en cause de la structure existante.

6. Schéma réseau global de l’infrastructure Langéo Education



7. Déploiement de l'infrastructure – Hyperviseur Proxmox

7.1 Rôle de l'hyperviseur

L'hyperviseur Proxmox Virtual Environment (PVE) constitue la base de l'infrastructure mise en place pour le projet Langéo Education.
Il permet l'hébergement et la gestion centralisée de l'ensemble des machines virtuelles nécessaires au fonctionnement des services de l'infrastructure.

L'utilisation d'un hyperviseur permet notamment :

- l'isolation des services entre eux,
- une meilleure gestion des ressources matérielles,
- une simplification des opérations d'administration,
- une meilleure évolutivité de l'infrastructure.

7.2 Justification du choix de Proxmox

Le choix de **Proxmox** s'explique par plusieurs critères techniques et pédagogiques :

- Solution **open source**, largement utilisée en environnement professionnel.
- Support de la virtualisation **KVM** et des conteneurs.
- Interface d'administration Web simple et complète.
- Gestion efficace des machines virtuelles (création, arrêt, sauvegarde).
- Compatibilité avec des environnements **Windows et Linux**.

Proxmox répond ainsi parfaitement aux besoins d'une infrastructure pédagogique simulant un système d'information de PME.

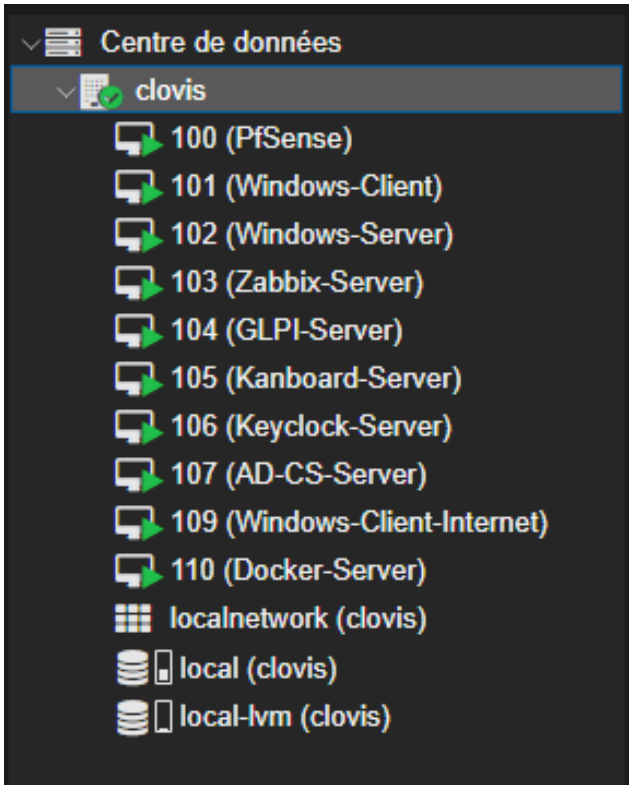
7.3 Organisation des machines virtuelles

L'ensemble des services du projet est déployé sous forme de machines virtuelles distinctes afin de garantir une séparation claire des rôles.

Les principales machines virtuelles hébergées sur Proxmox sont :

- un pare-feu **pfSense** assurant le routage et la sécurité réseau,
- des serveurs **Windows Server** pour les services d'annuaire et de certification,
- plusieurs serveurs **Debian** hébergeant les services applicatifs et d'exploitation.

Chaque machine virtuelle dispose de ressources adaptées à son rôle (CPU, mémoire, stockage) et est reliée au réseau correspondant via la segmentation par VLAN.



7.4 Intégration réseau

L'intégration réseau de l'hyperviseur **Proxmox** repose sur la création de **deux bridges Linux distincts**, permettant de séparer clairement le trafic réseau externe du réseau interne de l'infrastructure.

Deux interfaces de type *Linux Bridge* ont été configurées :

- **vmbr0** : bridge dédié au **réseau WAN**, relié à l'interface physique de l'hyperviseur connectée au réseau externe (Internet simulé).
  Ce bridge est utilisé exclusivement par l'interface WAN du pare-feu **pfSense**.
- **vmbr1** : bridge dédié au **réseau LAN interne**, servant de point de raccordement pour l'ensemble des machines virtuelles de l'infrastructure.
  Ce bridge transporte les différents **VLAN** configurés sur pfSense.

vmbr0	Linux Bridge	O...	Oui	Non	eno1	192.168.3.221/24	192.168.3.254	WAN – Réseau école / Internet
vmbr1	Linux Bridge	O...	Oui	Oui				LAN – Réseau interne utilisateurs

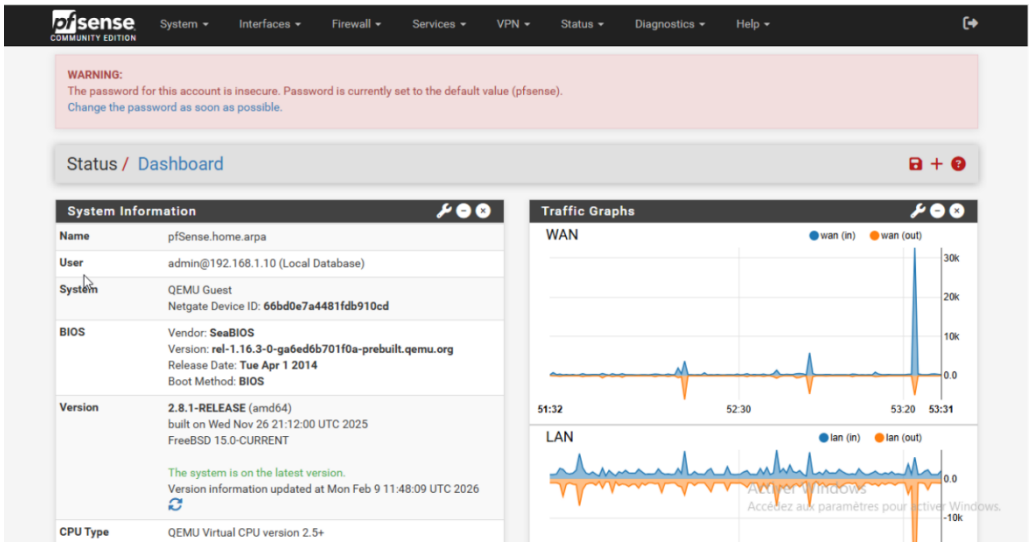
8. Pare-feu et routage – pfSense

8.1 Rôle du pare-feu

Le pare-feu pfSense constitue le point central de la gestion réseau de l'infrastructure Langéo Education. Il assure à la fois les fonctions de routage, de filtrage et de sécurisation des flux entre les différents réseaux.

pfSense est positionné entre le réseau externe (WAN) et les réseaux internes (LAN) de l'infrastructure, ce qui permet :

- de contrôler l'accès à Internet,
- de filtrer les communications inter-VLAN,
- de protéger les services internes contre les accès non autorisés.

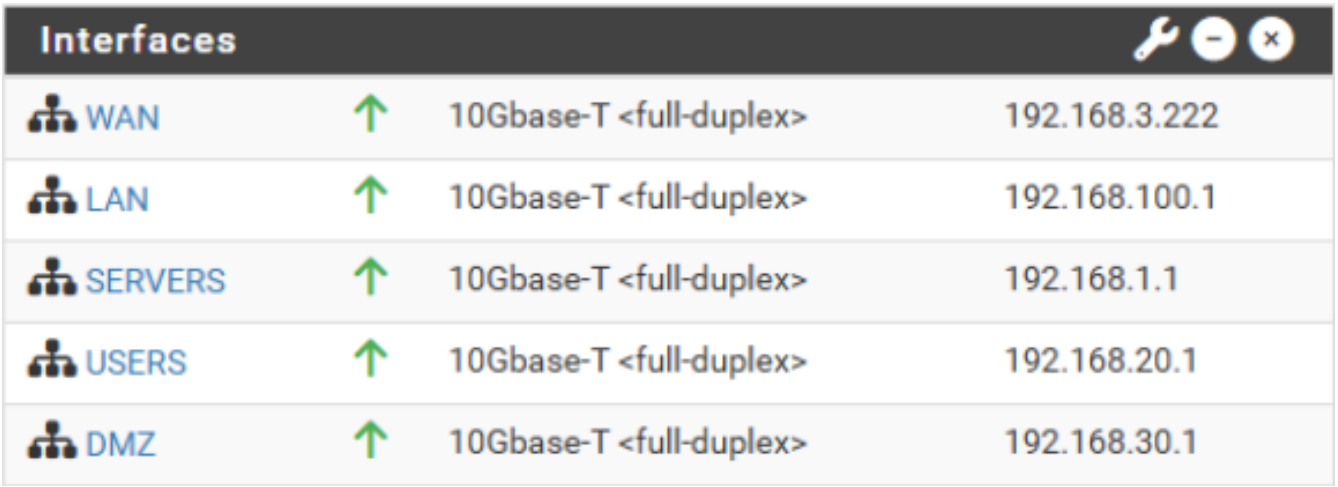


8.2 Segmentation par VLAN

Afin de renforcer la sécurité et d'organiser les flux réseau, plusieurs VLAN ont été mis en place sur pfSense :

- **VLAN 10 – Serveurs**
  Réseau dédié à l'hébergement des serveurs internes (annuaire, supervision, services applicatifs).
- **VLAN 20 – Utilisateurs**
  Réseau destiné aux postes clients, avec attribution automatique des adresses IP via le service DHCP.
- **VLAN 30 – DMZ**
  Réseau isolé permettant l'hébergement des services accessibles depuis l'extérieur, tels que le site web déployé via Docker.

Cette segmentation permet de limiter les communications au strict nécessaire et d'appliquer le **principe du moindre privilège**.



9. Services d'infrastructure – Active Directory (AD DS & DNS)

9.1 Objectif de la mise en place de l'Active Directory

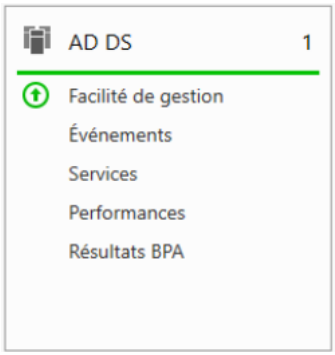
La mise en place d'un service Active Directory Domain Services (AD DS) a pour objectif de centraliser l'authentification, la gestion des utilisateurs, des ordinateurs et des ressources de l'infrastructure Langéo Education.

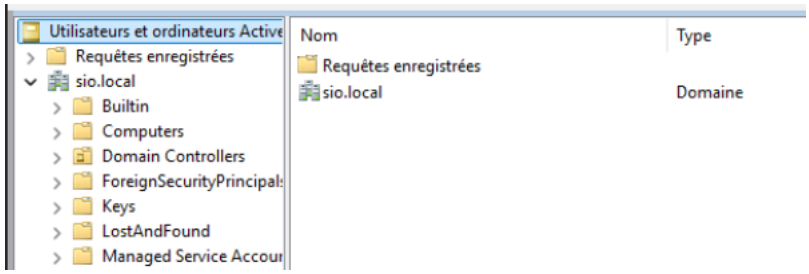
Active Directory constitue le socle de l'infrastructure, sur lequel reposent plusieurs services critiques tels que l'authentification des postes clients, la gestion des droits et l'intégration de services tiers nécessitant un annuaire LDAP.

9.2 Installation du rôle Active Directory Domain Services

Le rôle Active Directory Domain Services a été installé sur un serveur Windows Server 2025 (192.168.1.10), hébergé sur l'hyperviseur Proxmox et intégré au VLAN 10 – Serveurs.

À l'issue de l'installation du rôle, le serveur a été promu en contrôleur de domaine, permettant la création du domaine Active Directory.





9.3 Création du domaine Active Directory

Le domaine Active Directory créé pour l'infrastructure est nommé **sio.local**.

Ce choix permet d'identifier clairement le domaine interne de l'organisation fictive **Langéo Education**, tout en évitant toute confusion avec un nom de domaine public.

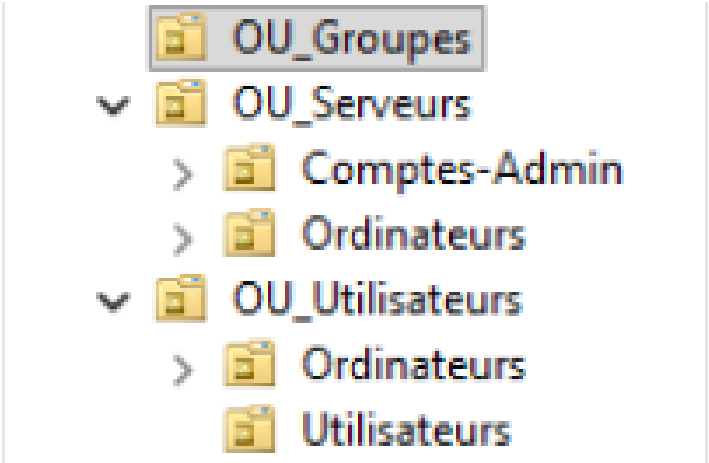
9.4 Mise en place de la structure organisationnelle (OU)

Afin de faciliter l'administration du domaine et d'appliquer des stratégies de sécurité adaptées, une structure organisationnelle basée sur des unités d'organisation (OU) a été mise en place.

Trois OU principales ont été créées :

- **OU_Groupes**
  Destinée à l'hébergement des **groupes de sécurité**, utilisés pour la gestion des droits et des accès aux ressources.
- **OU_Serveurs**
  Contient les **serveurs membres du domaine**, ainsi que les **comptes systèmes** nécessaires au fonctionnement des services (ex : comptes de service).
- **OU_Utilisateurs**
  Regroupe les **utilisateurs finaux** ainsi que les **postes clients** intégrés au domaine.

Cette organisation permet une gestion claire, évolutive et sécurisée du domaine Active Directory.

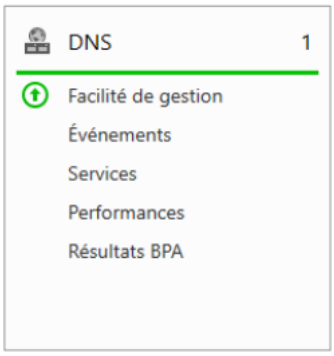


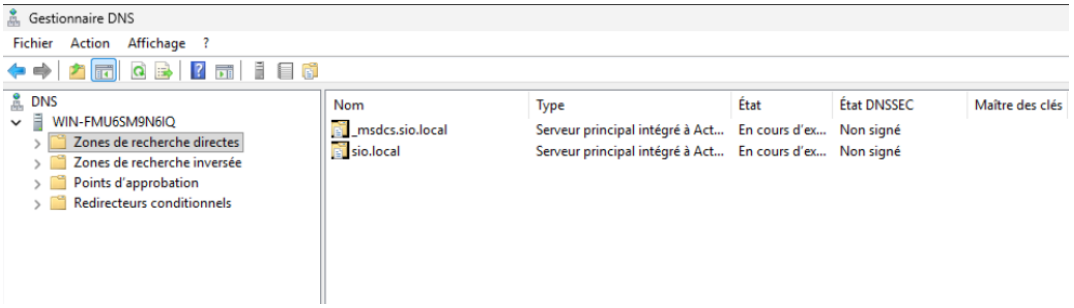
9.5 Mise en place du service DNS

Rôle du service DNS

Le service **DNS (Domain Name System)** est un composant indispensable au fonctionnement de l'Active Directory.
Il permet la résolution des noms de domaine et la localisation des services du domaine (contrôleurs de domaine, services LDAP, etc.).

Lors de l'installation du rôle **Active Directory Domain Services**, le rôle **DNS** a été installé automatiquement sur le contrôleur de domaine.





Intégration du DNS au domaine Active Directory

Le serveur DNS est configuré de manière intégrée à l'Active Directory.
Une **zone de recherche directe** correspondant au domaine **sio.local** a été créée automatiquement lors de la promotion du serveur en contrôleur de domaine.

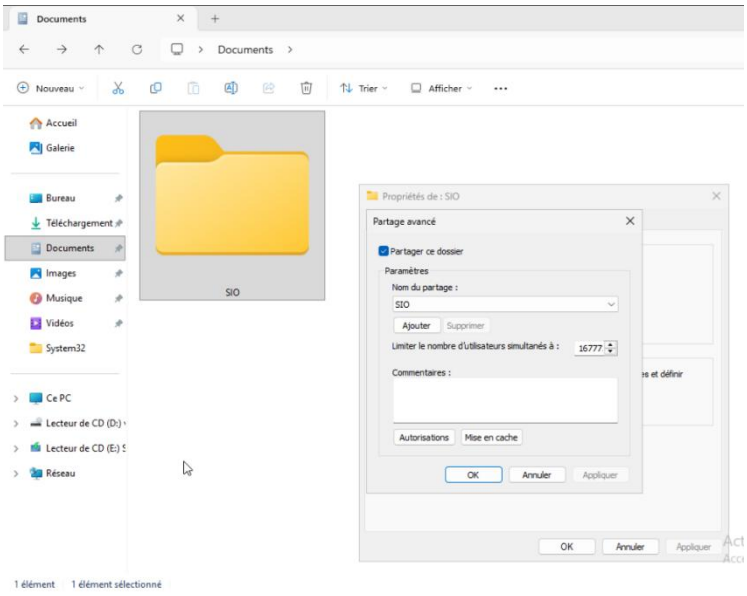
Cette intégration permet :

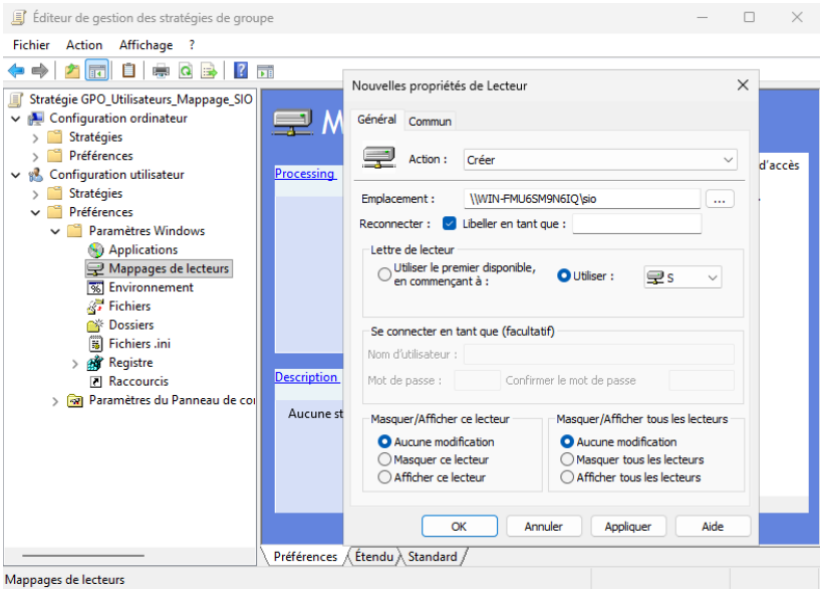
- la mise à jour automatique des enregistrements DNS,
- la résolution des noms des serveurs et postes clients du domaine,
- le bon fonctionnement des services dépendants de l'Active Directory.

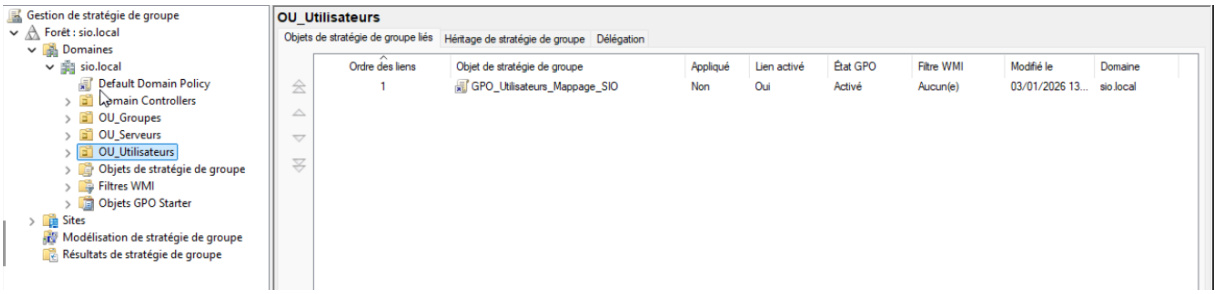
9.6 Mise en place d'une stratégie de groupe (GPO) – Lecteur réseau

Afin de mettre en pratique l'utilisation de l'Active Directory, une **stratégie de groupe (GPO)** a été mise en place pour automatiser le **mappage d'un lecteur réseau** destiné aux utilisateurs du domaine.

Ce lecteur réseau simule un **serveur de fichiers**, hébergé sur le contrôleur de domaine, et permet de centraliser l'accès aux ressources partagées de l'organisation **Langéo Education**.







9.7 Création des groupes de sécurité et gestion des accès

Afin de gérer de manière fine et sécurisée l'accès au serveur de fichiers, plusieurs **groupes de sécurité Active Directory** ont été créés.

Le partage réseau principal, nommé **SIO**, est hébergé sur le contrôleur de domaine et contient des sous-dossiers correspondant aux matières proposées par l'organisation fictive **Langéo Education**.

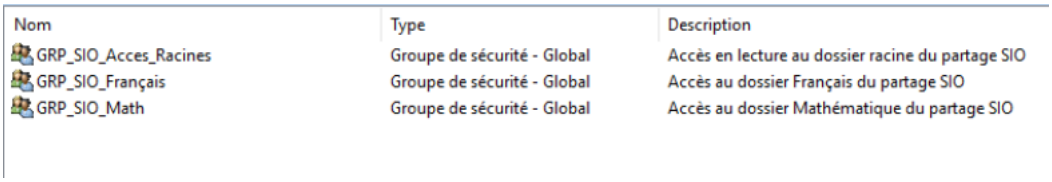
Dans ce cadre, les groupes de sécurité suivants ont été mis en place :

- **GS_SIO_Acces**
  Groupe principal permettant l'accès au partage réseau **SIO**.
  Ce groupe est utilisé pour autoriser le mappage du lecteur réseau via une stratégie de groupe (GPO).
- **GS_SIO_Francais**
  Groupe dédié aux utilisateurs autorisés à accéder au dossier **Français** du partage SIO.
- **GS_SIO_Mathematique**
  Groupe dédié aux utilisateurs autorisés à accéder au dossier **Mathématique** du partage SIO.

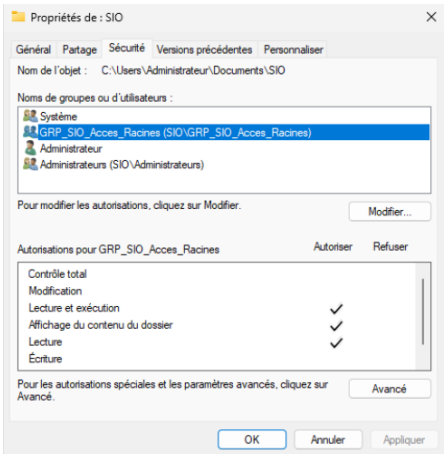
Les droits d'accès aux dossiers sont définis à l'aide des **permissions NTFS**, attribuées exclusivement aux groupes de sécurité, et non directement aux utilisateurs.
Les utilisateurs héritent ainsi automatiquement des droits correspondant aux groupes auxquels ils appartiennent.

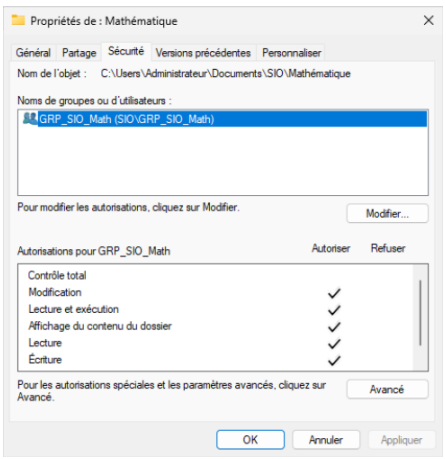
Cette approche permet :

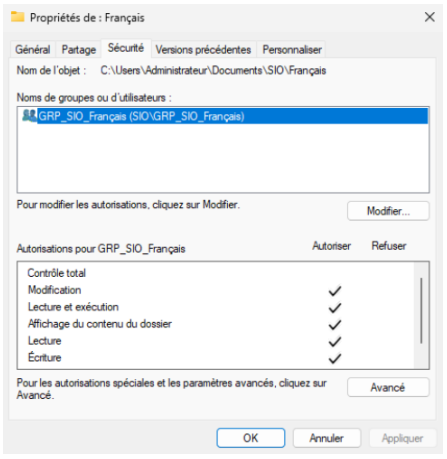
- une gestion centralisée et évolutive des autorisations,
- une séparation claire des accès par matière,
- une simplification de l'administration des droits.



Nom	Type	Description
GRP_SIO_Acces_Racines	Groupe de sécurité - Global	Accès en lecture au dossier racine du partage SIO
GRP_SIO_Français	Groupe de sécurité - Global	Accès au dossier Français du partage SIO
GRP_SIO_Math	Groupe de sécurité - Global	Accès au dossier Mathématique du partage SIO







9.8 Création des comptes utilisateurs du domaine

Dans le cadre de la mise en œuvre de l'infrastructure Active Directory de l'organisation fictive **Langéo Education**, deux comptes utilisateurs ont été créés afin de représenter les responsables des différentes matières proposées.

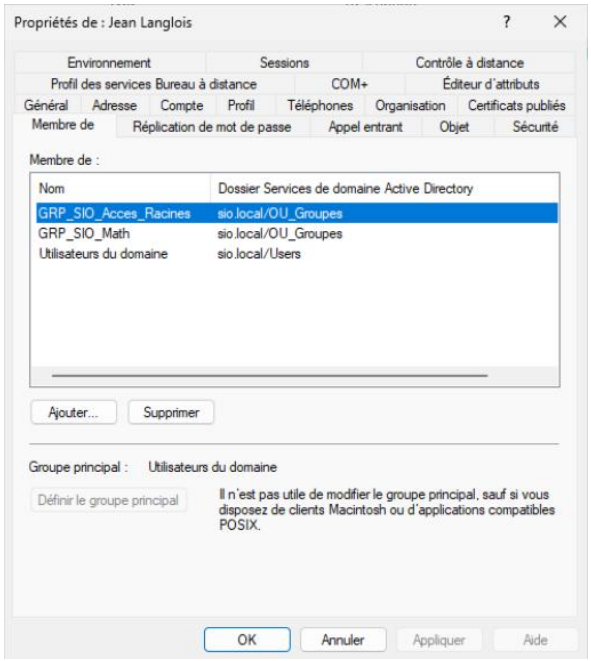
Les comptes suivants ont été mis en place dans l'unité d'organisation **OU_Utilisateurs** :

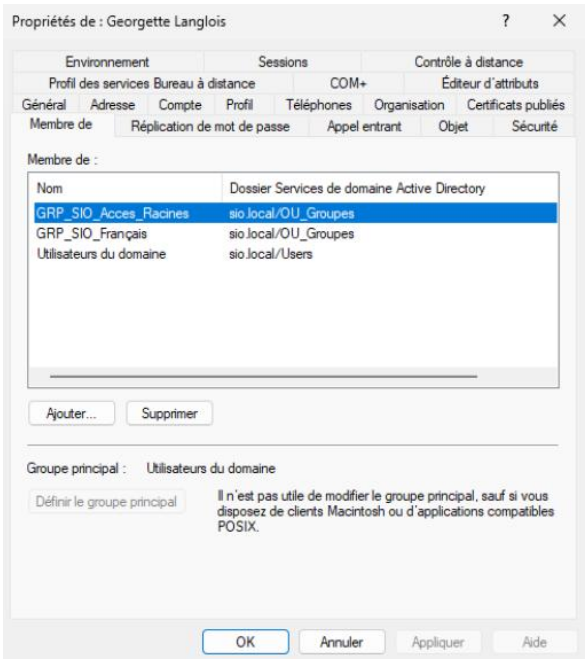
- **Jean Langlois**
  Responsable de la matière *Mathématique*.
- **Georgette Langlois**
  Responsable de la matière *Français*.

Chaque utilisateur est associé à un groupe de sécurité dédié, permettant une gestion centralisée et sécurisée des droits d'accès aux ressources partagées :

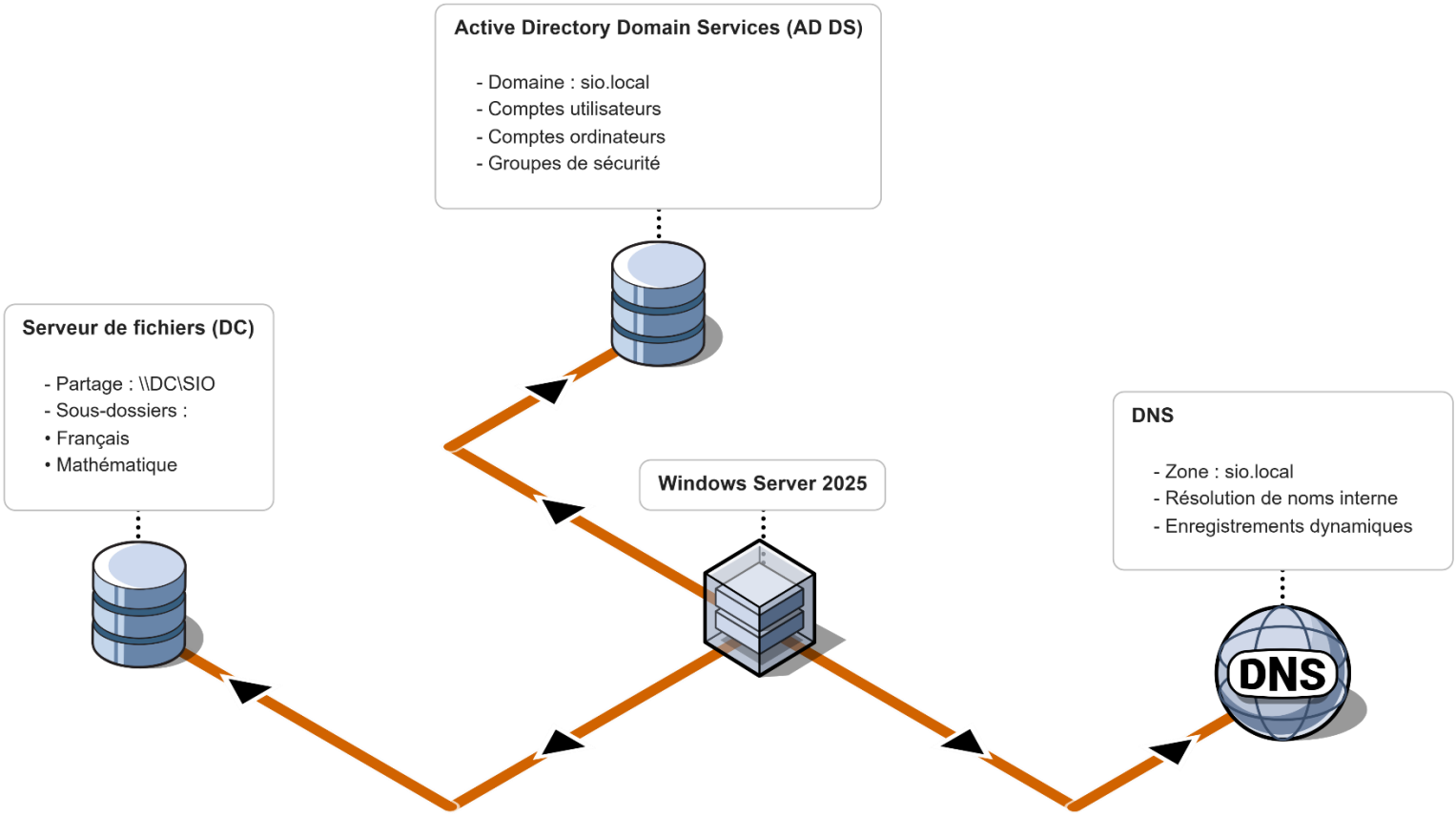
- **Jean Langlois** est membre du groupe **GS_SIO_Mathematique**, lui donnant accès au dossier *Mathématique* du partage réseau.
- **Georgette Langlois** est membre du groupe **GS_SIO_Francais**, lui donnant accès au dossier *Français* du partage réseau.

Cette organisation basée sur des groupes de sécurité Active Directory permet de dissocier les utilisateurs des permissions, facilitant ainsi l'administration des droits d'accès et garantissant une gestion évolutive et sécurisée du serveur de fichiers.





9.9 Architecture logique des services Active Directory et DNS



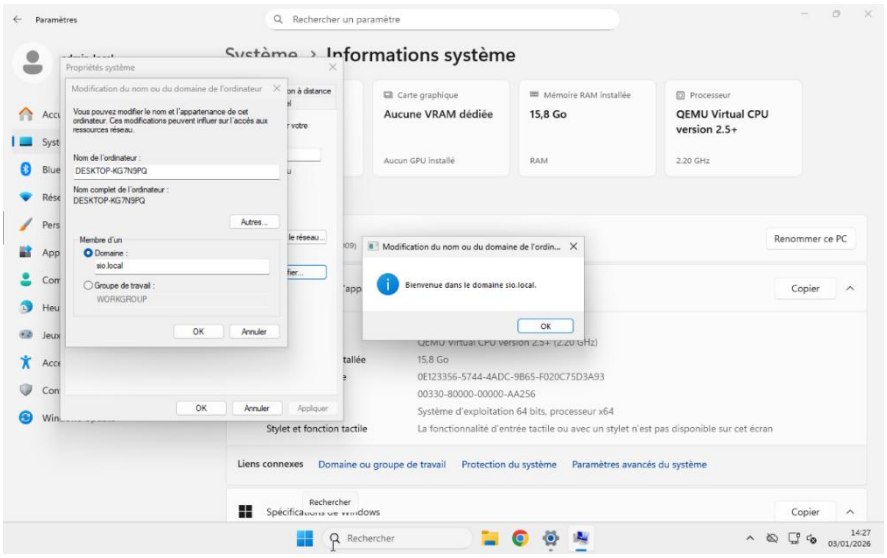
10. Enrôlement d’une machine cliente dans le domaine Active Directory

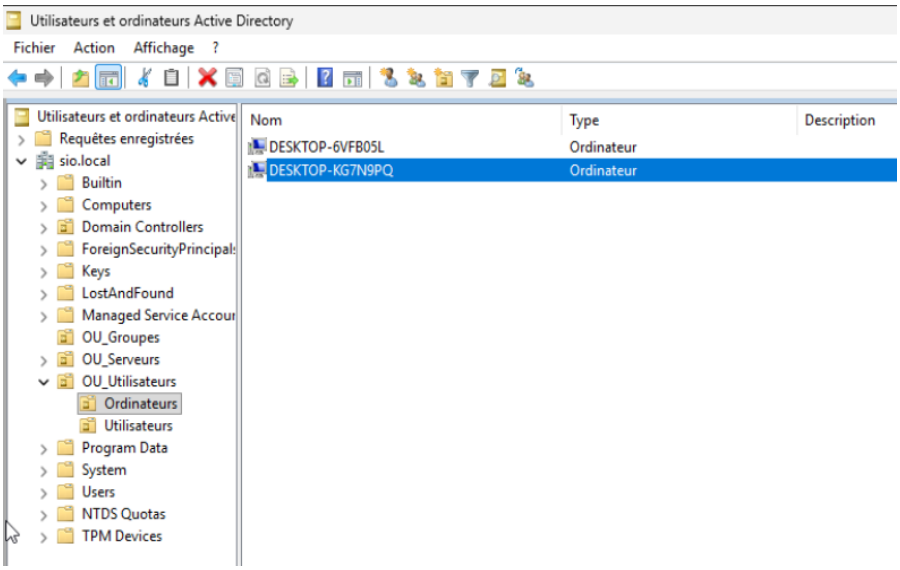
Afin de valider le bon fonctionnement des services Active Directory et DNS, un test a été réalisé à partir d’une machine cliente Windows intégrée à l’infrastructure.

La machine cliente est déployée dans le VLAN 20 – Réseau utilisateurs, configuré en DHCP.
L’adressage IP, la passerelle par défaut ainsi que le serveur DNS sont fournis automatiquement par le pare-feu pfSense, permettant à la machine de communiquer avec le contrôleur de domaine.

L’ordinateur a ensuite été enrôlé dans le domaine Active Directory ***sio.local*** via les paramètres système de Windows.
L’opération s’est déroulée avec succès, confirmée par le message de bienvenue dans le domaine, attestant de la bonne résolution DNS et de la communication avec le contrôleur de domaine.

Après redémarrage, la machine apparaît correctement dans l’Active Directory, au sein de l’unité d’organisation dédiée aux postes clients, conformément à la structure organisationnelle définie.





10.1 Test de connexion utilisateur et mappage du lecteur réseau

Une connexion utilisateur a ensuite été réalisée avec le compte **Jean Langlois**, utilisateur du domaine et membre des groupes de sécurité associés à la matière **Mathématique**.

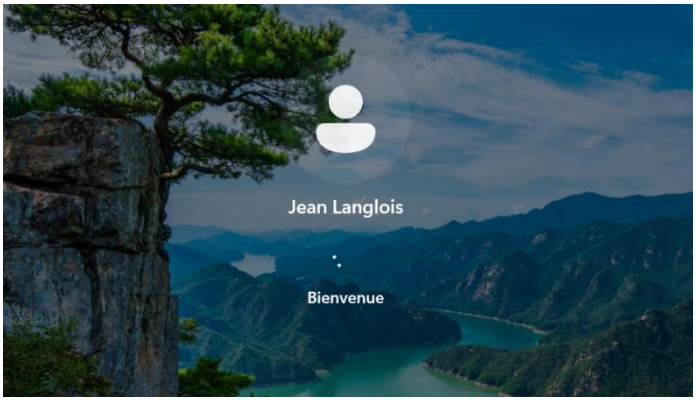
Lors de l'ouverture de session, **la stratégie de groupe (GPO)** précédemment mise en place s'applique automatiquement.
Celle-ci permet le **mappage du lecteur réseau** hébergé sur le contrôleur de domaine, simulant un serveur de fichiers centralisé.

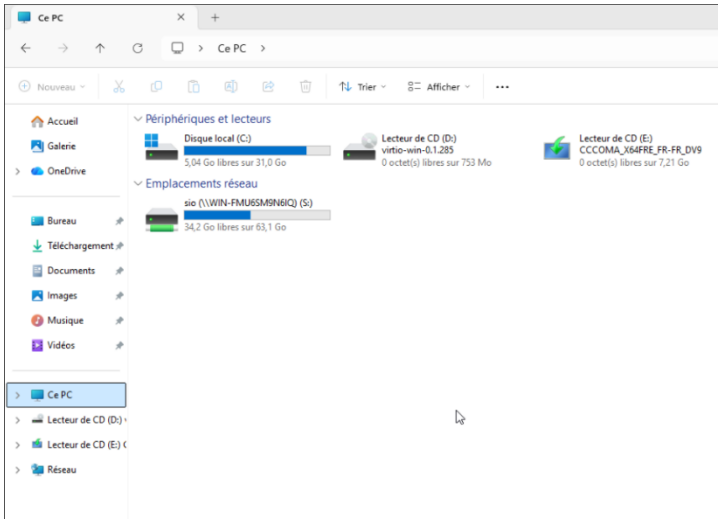
Le lecteur réseau apparaît correctement dans l'explorateur de fichiers, avec une lettre de lecteur dédiée.
L'utilisateur dispose uniquement des droits correspondant à son groupe de sécurité :

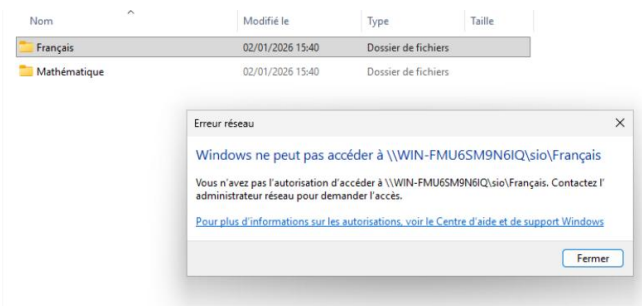
- accès autorisé au dossier **Mathématique**,
- absence d'accès au dossier **Français**, conformément aux permissions NTFS définies.

Ce test valide :

- le bon fonctionnement de l'authentification Active Directory,
- l'application des stratégies de groupe (GPO),
- la gestion des accès par groupes de sécurité,
- et la centralisation des ressources utilisateurs.







11. Services applicatifs – Gestion des identités (Keycloak)

11.1 Objectif de la mise en place de Keycloak

Le service **Keycloak** a été déployé afin de mettre en place une **gestion centralisée des identités** et de permettre l'utilisation d'un **Single Sign-On (SSO)** pour les services applicatifs de l'organisation fictive **Langéo Education**.

Keycloak agit comme un **fournisseur d'identité (IdP)**, chargé de :

- centraliser l'authentification des utilisateurs,
- déléguer l'authentification à Active Directory,
- fournir des mécanismes d'authentification modernes (OIDC / SAML),
- simplifier l'accès aux applications internes.

11.2 Déploiement de la machine virtuelle Keycloak

Le service Keycloak est hébergé sur :

- une **machine virtuelle Debian**,
- intégrée au **VLAN 10 – Serveurs**,
- déployée sur l'hyperviseur **Proxmox**.

Cette machine est dédiée exclusivement au service d'authentification afin de garantir :

- une meilleure isolation,
- une sécurité renforcée,
- une maintenance simplifiée.

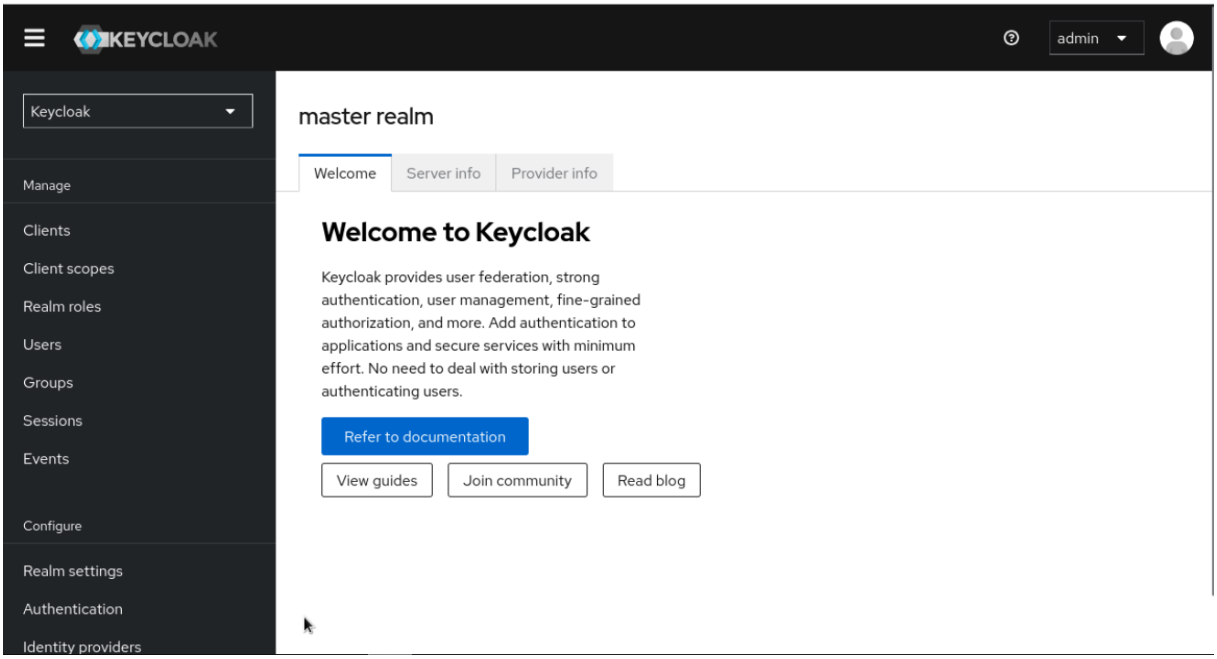
11.3 Installation du service Keycloak

Keycloak a été installé sur le serveur Debian à l'aide d'un environnement adapté à un usage serveur.

L'installation comprend :

- le déploiement du service Keycloak,
- la configuration d'un compte administrateur,
- l'accès à l'interface d'administration web.

À ce stade, le service Keycloak est fonctionnel mais **non encore intégré à Active Directory**.



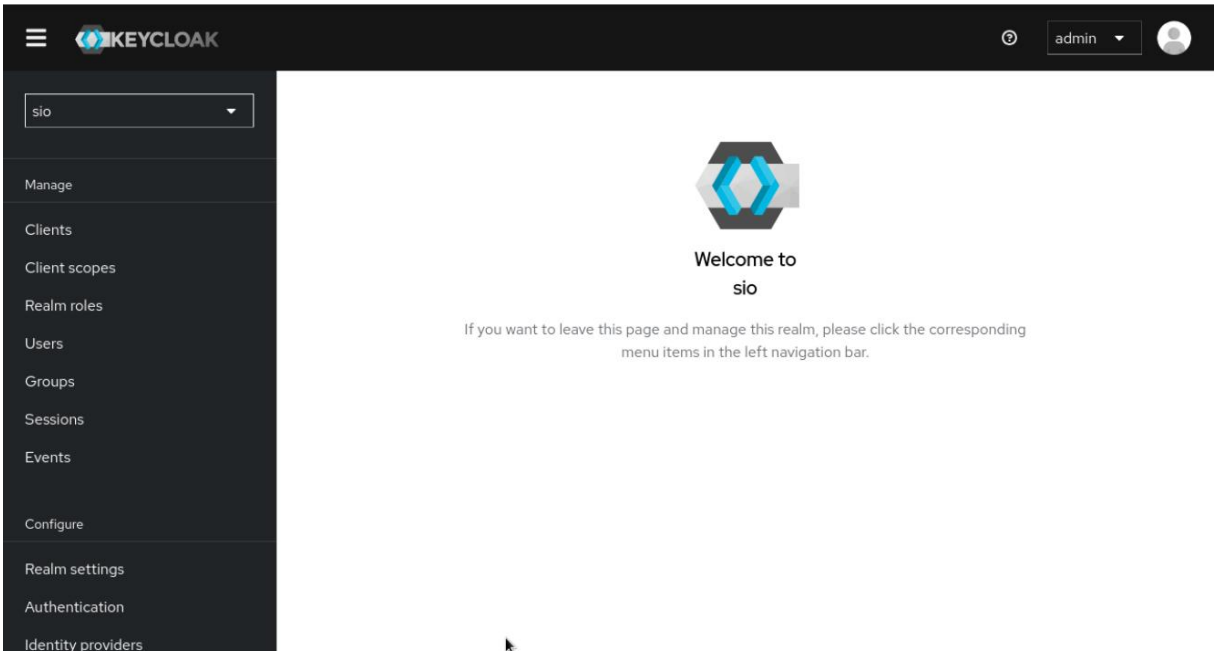
11.4 Configuration initiale de Keycloak

Une configuration de base a été réalisée, comprenant :

- la création d'un **realm dédié** à l'organisation (SIO)
- la préparation des paramètres d'authentification,
- la vérification de l'accessibilité du service via le navigateur.

À cette étape :

- l'authentification est encore locale,
- aucun certificat n'est utilisé,
- aucune connexion à Active Directory n'est encore active.



Une fois le service Keycloak installé et fonctionnel, il a été nécessaire de sécuriser les échanges et de préparer l'intégration avec l'Active Directory.

12. Services d'infrastructure – Autorité de certification (AD CS)

12.1 Objectif de la mise en place d'AD CS

L'objectif de la mise en place d'une **autorité de certification (AD CS)** est de fournir une infrastructure de certificats permettant :

- l'émission de certificats numériques internes,
- la sécurisation des communications entre services,
- l'authentification basée sur des certificats,
- et l'intégration d'un **SSO (Single Sign-On)** entre **Active Directory** et **Keycloak**.

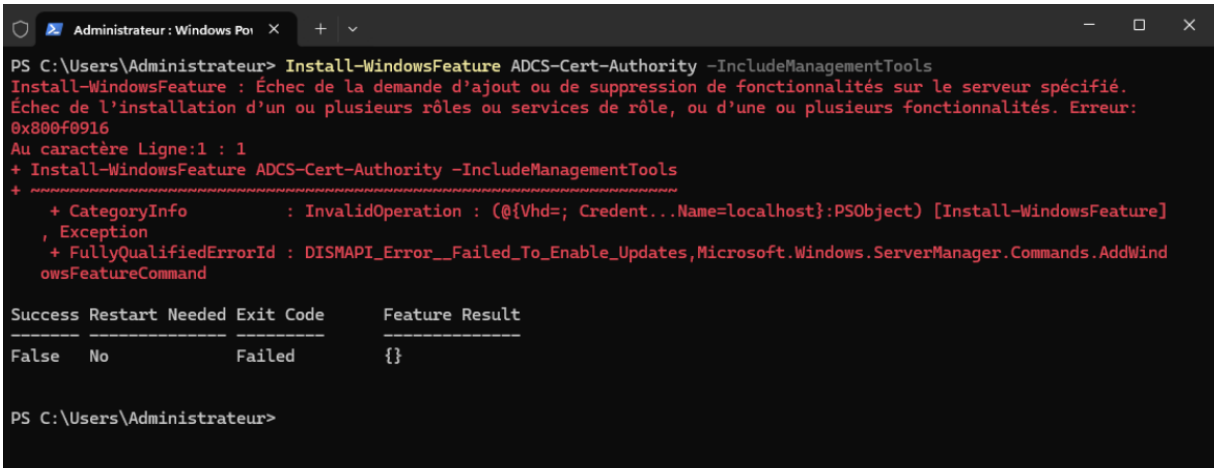
Cette infrastructure est un prérequis pour la mise en place d'une authentification centralisée et sécurisée des services applicatifs de l'organisation fictive **Langéo Education**.

12.2 Difficulté rencontrée sur Windows Server 2025

Lors de la conception de l'infrastructure, une tentative d'installation du rôle **Active Directory Certificate Services (AD CS)** a été réalisée sur le contrôleur de domaine principal sous **Windows Server 2025**.

Cependant, l'installation du rôle a échoué en raison d'une **erreur liée au magasin de services Windows**, empêchant le bon déploiement de l'autorité de certification.
Cette erreur rendait l'environnement instable et non exploitable pour une infrastructure de certificats fiable.

Choix technique assumé :
Plutôt que de contourner le problème de manière risquée, il a été décidé de **changer de version de système d'exploitation** afin de garantir la stabilité et la pérennité de l'infrastructure.



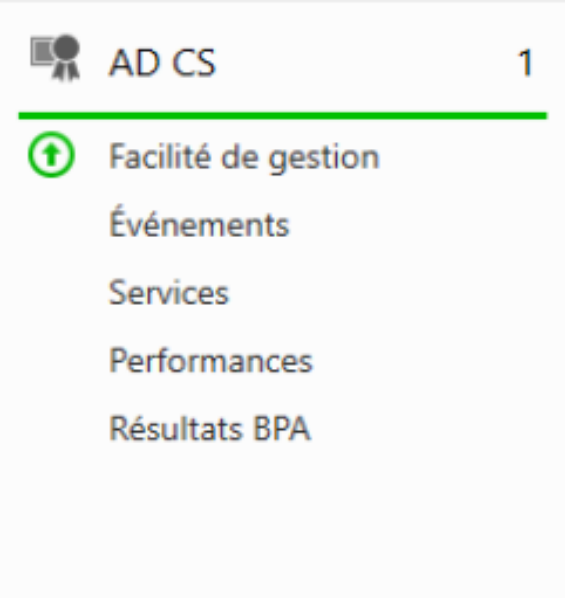
12.3 Mise en place d'un serveur AD CS dédié sous Windows Server 2022

Une **machine virtuelle dédiée sous Windows Server 2022** a été déployée sur l'hyperviseur Proxmox. Cette version a été choisie pour sa **stabilité éprouvée** et sa **compatibilité totale avec Active Directory et AD CS**.

Le serveur a été :

- joint au domaine **sio.local**,
- positionné dans le **VLAN 10 – Serveurs (192.168.1.15)**
- puis configuré avec le rôle **Active Directory Certificate Services**.

Le rôle installé correspond à une **autorité de certification d'entreprise**, intégrée à Active Directory, permettant l'émission automatique de certificats pour les services du domaine.



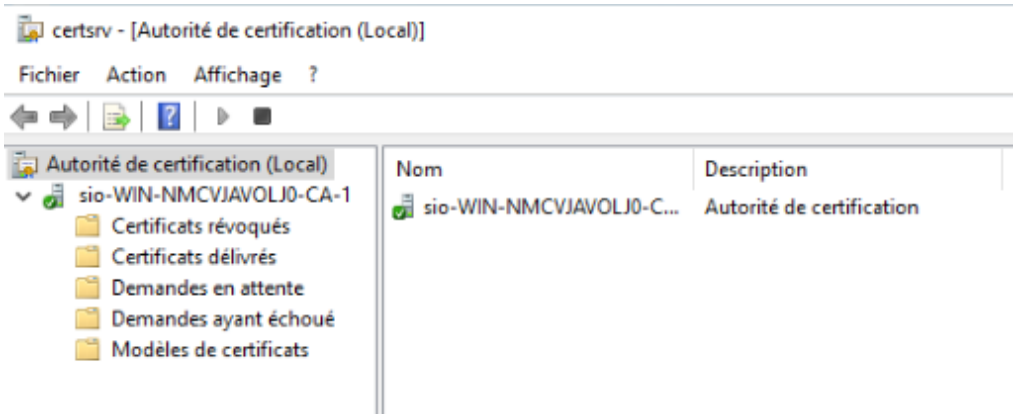
12.4 Configuration initiale de l’autorité de certification

Une fois le rôle **Active Directory Certificate Services** installé, l’autorité de certification a été configurée afin de permettre l’émission de certificats numériques internes.

L’autorité mise en place correspond à une **autorité de certification d’entreprise**, intégrée à l’Active Directory, permettant :

- l’émission centralisée de certificats,
- la gestion du cycle de vie des certificats,
- l’intégration automatique avec les services du domaine.

À l’issue de cette configuration, l’autorité de certification est opérationnelle et prête à délivrer des certificats pour les services internes.



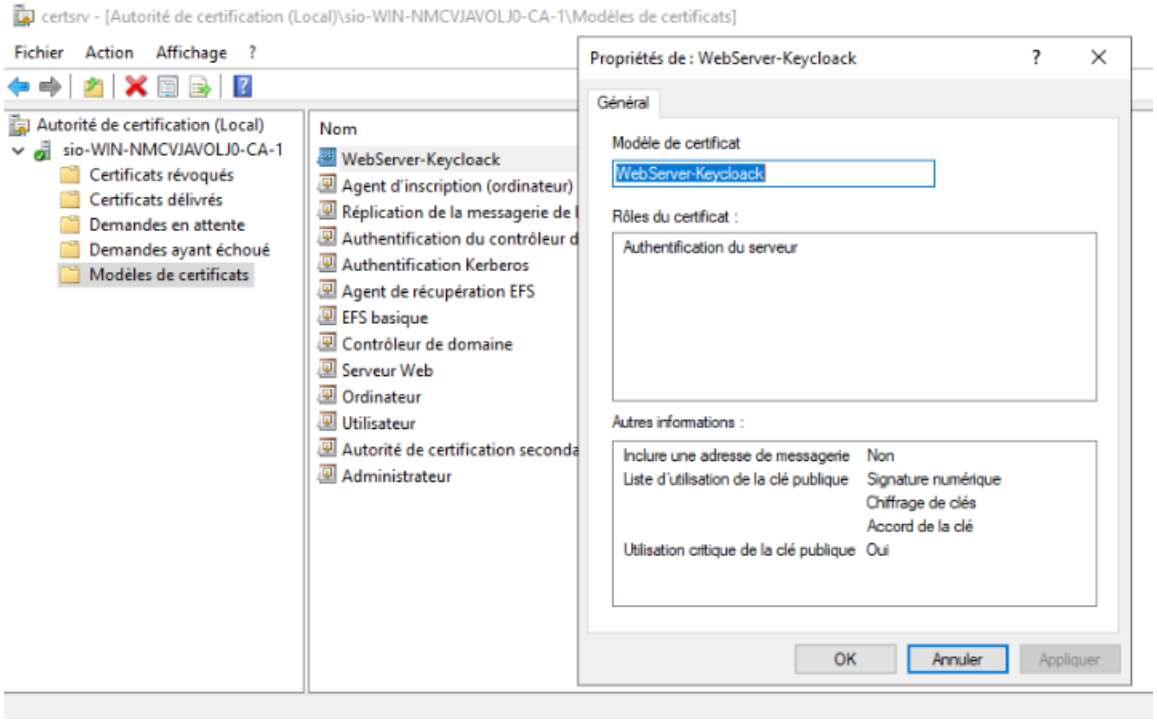
12.5 Mise en place des modèles de certificats

Afin de répondre aux besoins de sécurisation des services applicatifs, des **modèles de certificats** ont été utilisés au sein de l'autorité de certification.

Un modèle de certificat spécifique nommé **WebServer-Keycloak** a été configuré.
Ce modèle est basé sur un usage de type **serveur web**, permettant :

- l'authentification du service,
- la sécurisation des communications via HTTP,
- l'utilisation de certificats pour des services applicatifs internes.

Ce modèle de certificat est destiné au service **Keycloak**, afin de permettre l'établissement d'une relation de confiance sécurisée avec l'Active Directory et de préparer la mise en place d'une authentification centralisée (SSO).



12.6 Émission d’un certificat pour le service Keycloak

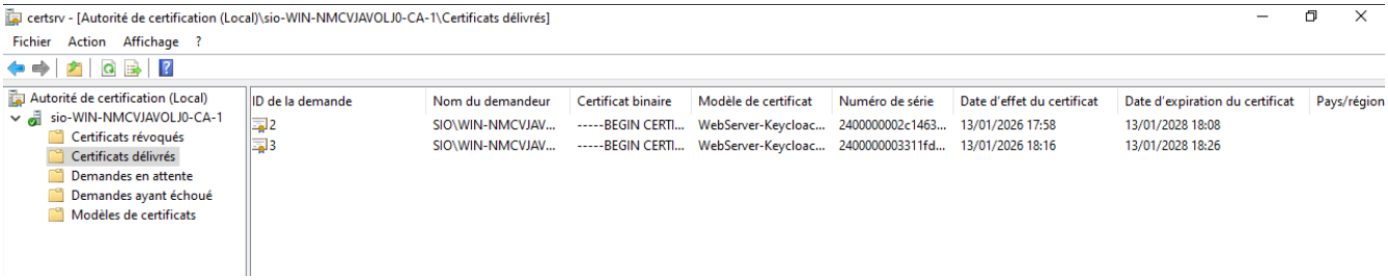
Une fois l’autorité de certification opérationnelle et le modèle de certificat **WebServer-Keycloak** configuré, un certificat numérique a été émis pour le service **Keycloak**.

Ce certificat est destiné à sécuriser les communications du service Keycloak via le protocole HTTPS et à établir une relation de confiance avec l’infrastructure Active Directory.

Le certificat a été délivré par l’autorité de certification d’entreprise **sio-WIN-NMCVJAVOLJO-CA-1** et est associé au nom de service **keycloak.sio.local**.

Cette étape permet :

- l’authentification sécurisée du service Keycloak,
- le chiffrement des communications entre les services,
- la préparation de l’intégration avec Active Directory via des mécanismes sécurisés (LDAPS / SSO).



12.7 Déploiement du certificat sur le service Keycloak

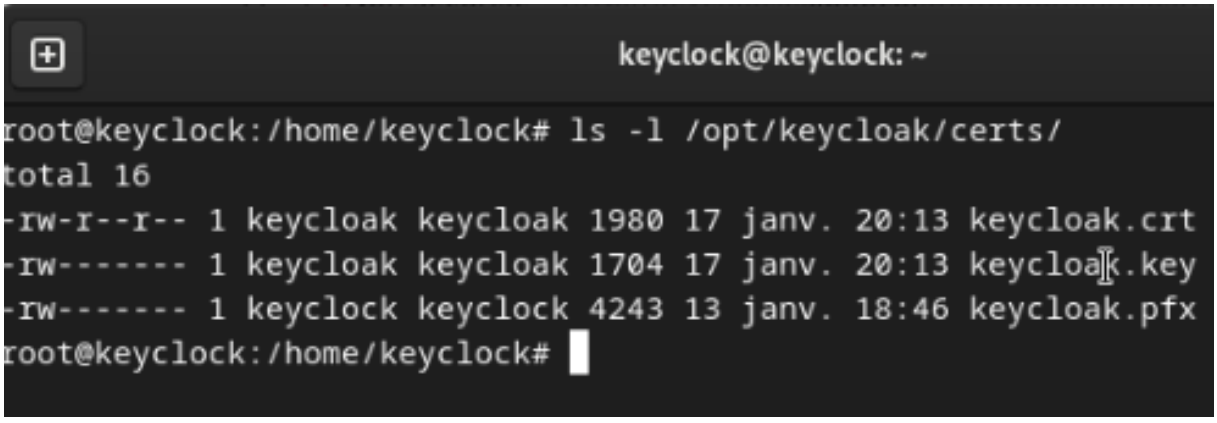
Afin de sécuriser les échanges entre le service Keycloak et l'infrastructure Active Directory, le certificat numérique précédemment émis par l'autorité de certification d'entreprise a été déployé sur le serveur Keycloak.

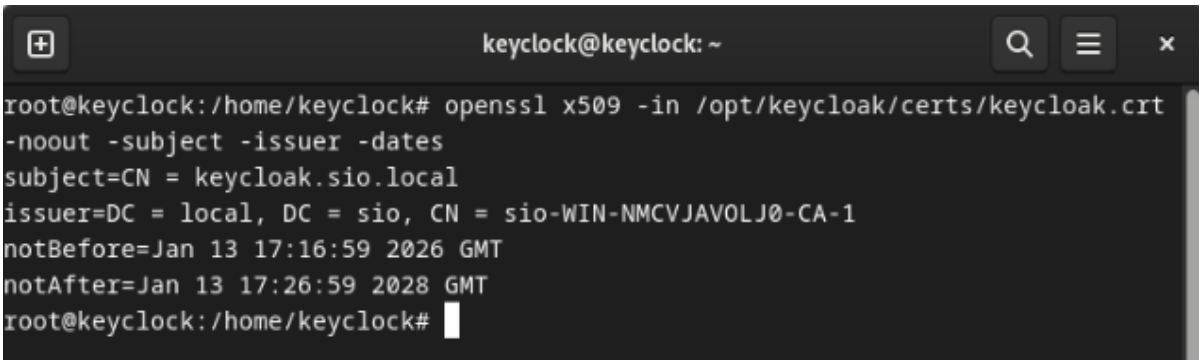
Le certificat est installé sur la machine virtuelle Debian hébergeant Keycloak, dans un répertoire dédié aux certificats applicatifs.

Les fichiers suivants sont présents sur le serveur Keycloak :

- un certificat public (keycloak.crt),
- une clé privée associée (keycloak.key),
- un fichier de type PKCS#12 (keycloak.pfx) permettant l'import du certificat depuis l'autorité de certification.

Cette organisation permet une gestion claire et sécurisée des éléments cryptographiques nécessaires au fonctionnement du service.





13. Intégration d'Active Directory avec Keycloak (LDAP / LDAPS)

13.1 Objectif de l'intégration

L'objectif de cette étape est de permettre à **Keycloak** d'utiliser les comptes utilisateurs gérés dans **Active Directory**, afin de centraliser l'authentification et de préparer la mise en place d'un **Single Sign-On (SSO)** pour les services applicatifs de l'organisation fictive *Langéo Education*.

Keycloak agit comme **fournisseur d'identité (IdP)**, tandis qu'Active Directory reste l'annuaire de référence pour la gestion des utilisateurs et des groupes.

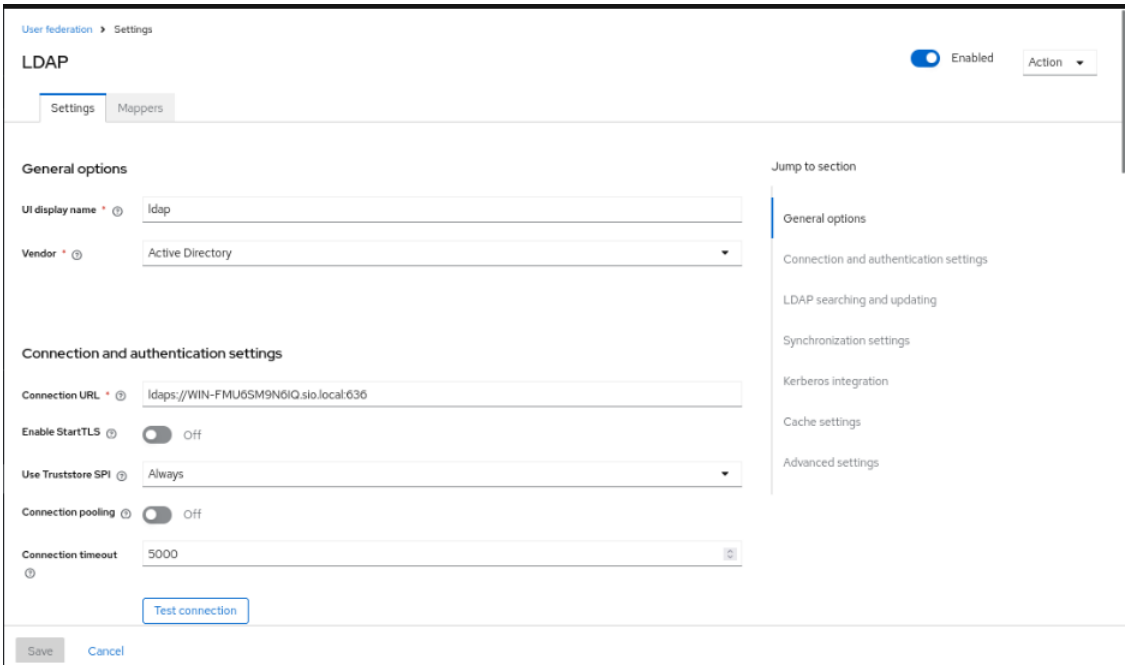
13.2 Mise en place du fournisseur LDAP dans Keycloak

L'intégration a été réalisée via la fonctionnalité **User Federation** de Keycloak, en configurant un fournisseur de type **LDAP** avec un annuaire **Active Directory**.

Les paramètres principaux configurés sont :

- **Type de fournisseur** : LDAP
- **Vendor** : Active Directory
- **URL de connexion** :
  ldaps://WIN-FMU6SM9N6IQ.sio.local:636
- **Base DN** :
  DC=sio,DC=local

La communication est établie via le protocole **LDAPS**, s'appuyant sur l'infrastructure de certificats mise en place précédemment.



13.3 Compte de service Active Directory

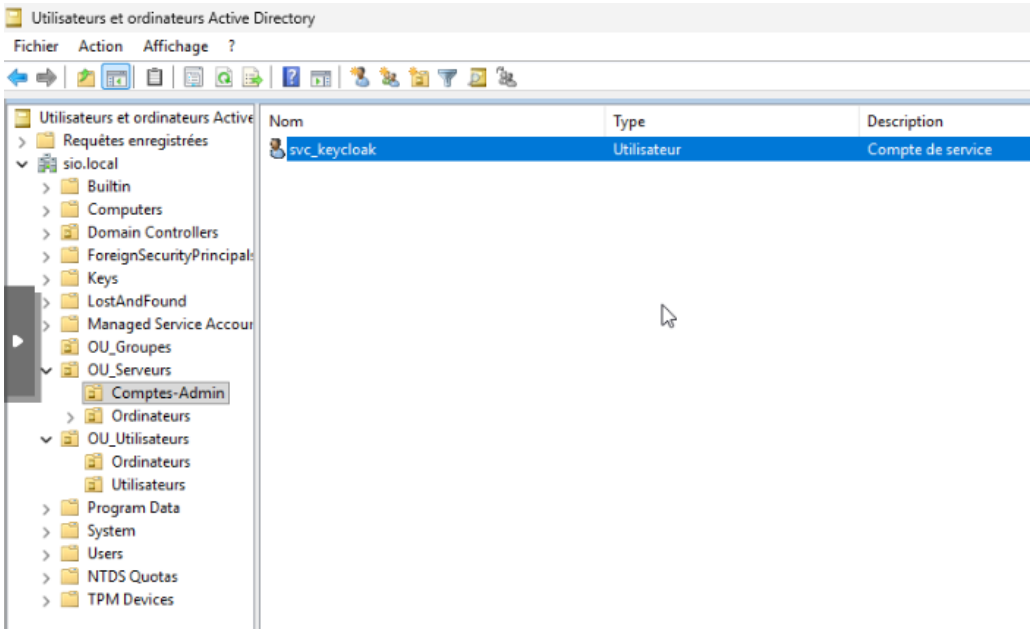
Un compte de service dédié nommé **svc_keycloak** a été créé dans Active Directory afin de permettre à Keycloak d'interroger l'annuaire.

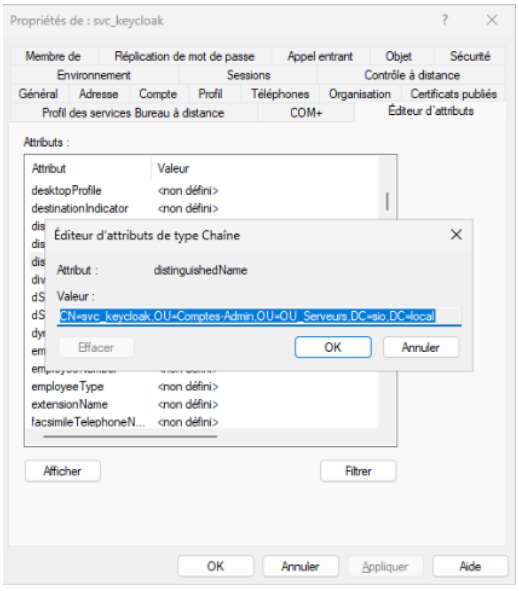
Ce compte est positionné dans l'unité d'organisation suivante :

OU=Comptes-Admin,OU=OU_Serveurs,DC=sio,DC=local

L'utilisation d'un compte de service dédié permet :

- une meilleure traçabilité,
- une séparation claire des rôles,
- une sécurisation accrue de l'accès à l'annuaire.





13.4 Validation de la connexion et de l'authentification

Une fois les paramètres configurés, des tests ont été réalisés depuis l'interface Keycloak :

- **Test de connexion LDAP** : réussi,
- **Test d'authentification via le compte de service** : réussi.

Ces tests confirment :

- la bonne communication entre Keycloak et Active Directory,
- la validité des paramètres LDAP,
- la préparation effective de l'authentification centralisée.

13.5 Résultat

À l'issue de cette configuration :

- Keycloak est correctement intégré à Active Directory,
- les utilisateurs du domaine peuvent être authentifiés via Keycloak,
- l'infrastructure est prête pour les tests d'authentification et de SSO applicatif.

14. Services applicatifs – Gestion de projet (Kanboard)

14.1 Objectif de la mise en place de Kanboard

Le service **Kanboard** a été déployé afin de fournir un outil de gestion de projet adapté au suivi pédagogique des élèves de l'organisation fictive *Langéo Education*.

Cet outil permet notamment :

- le suivi des activités par élève,
- la gestion des tâches pédagogiques,
- l'organisation du travail par matière ou par projet.

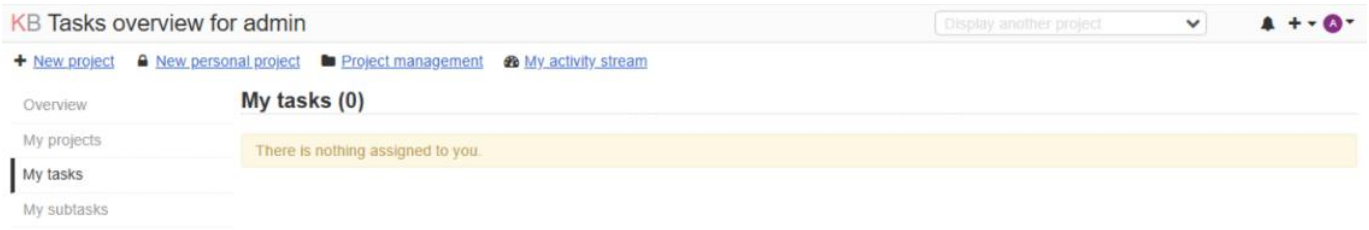
Dans une logique de centralisation des identités et de simplification des accès, l'authentification à Kanboard a été intégrée au service **Keycloak**, permettant une connexion unique (**Single Sign-On – SSO**) basée sur les comptes Active Directory.

14.2 Déploiement du service Kanboard

Le service Kanboard est hébergé sur une machine virtuelle dédiée sous **Debian**, intégrée au **VLAN 10 – Serveurs (192.168.1.13)** et déployée sur l'hyperviseur Proxmox.

Ce choix permet :

- une isolation claire du service applicatif,
- une meilleure sécurité,
- une administration simplifiée.



14.3 Configuration DNS des services applicatifs

Afin de permettre un accès simplifié aux services applicatifs et d'assurer la cohérence de l'architecture, des enregistrements DNS de type **A** ont été créés dans la zone sio.local.

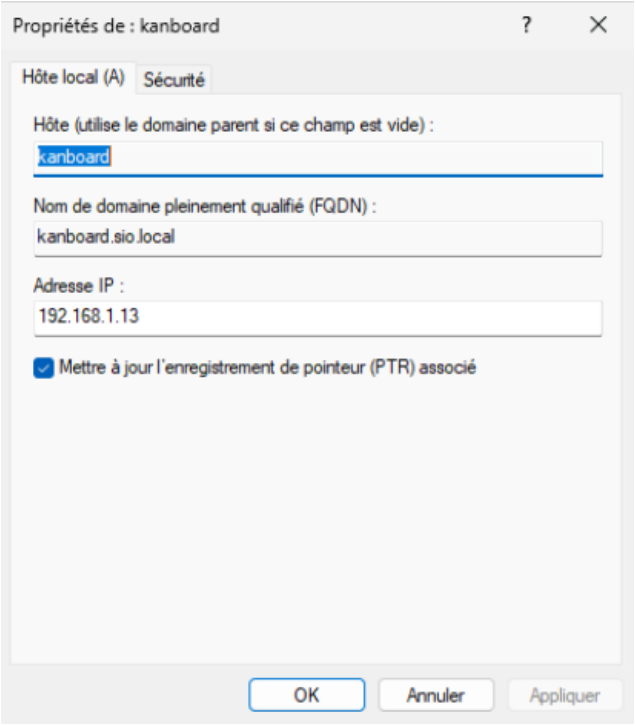
Les enregistrements suivants ont été ajoutés :

- **keycloak.sio.local** → 192.168.1.14
- **kanboard.sio.local** → 192.168.1.13

Cette configuration permet :

- l'utilisation de noms de domaine lisibles au lieu d'adresses IP,
- le bon fonctionnement des redirections OAuth2 / OpenID Connect,
- une meilleure intégration avec les certificats (CN / FQDN),
- une architecture plus professionnelle et maintenable.

Ces enregistrements sont configurés dans le gestionnaire DNS d'Active Directory.



14.4 Principe de l'authentification centralisée avec Keycloak

L'authentification des utilisateurs sur Kanboard repose sur le service **Keycloak**, configuré comme fournisseur d'identité centralisé.

Lorsqu'un utilisateur accède à Kanboard :

- il est redirigé vers Keycloak pour l'authentification,
- Keycloak délègue la vérification des identifiants à Active Directory,
- une fois authentifié, l'utilisateur est automatiquement reconnecté à Kanboard sans création de compte local.

14.5 Mise en place de l'authentification SSO avec OAuth2-Proxy et Nginx

Afin de mettre en place une authentification centralisée (SSO) entre Kanboard et Keycloak, un mécanisme intermédiaire basé sur **OAuth2-Proxy** et **Nginx** a été déployé.

Cette solution permet de sécuriser l'accès à Kanboard tout en déléguant l'authentification à Keycloak, sans gestion locale des mots de passe.

Rôle des composants

- **Keycloak** : fournisseur d'identité (IdP), authentifie les utilisateurs via Active Directory.
- **OAuth2-Proxy** : composant intermédiaire chargé de gérer le flux OAuth2 / OpenID Connect.
- **Nginx** : reverse proxy qui protège l'accès à Kanboard et interroge OAuth2-Proxy avant d'autoriser l'accès.

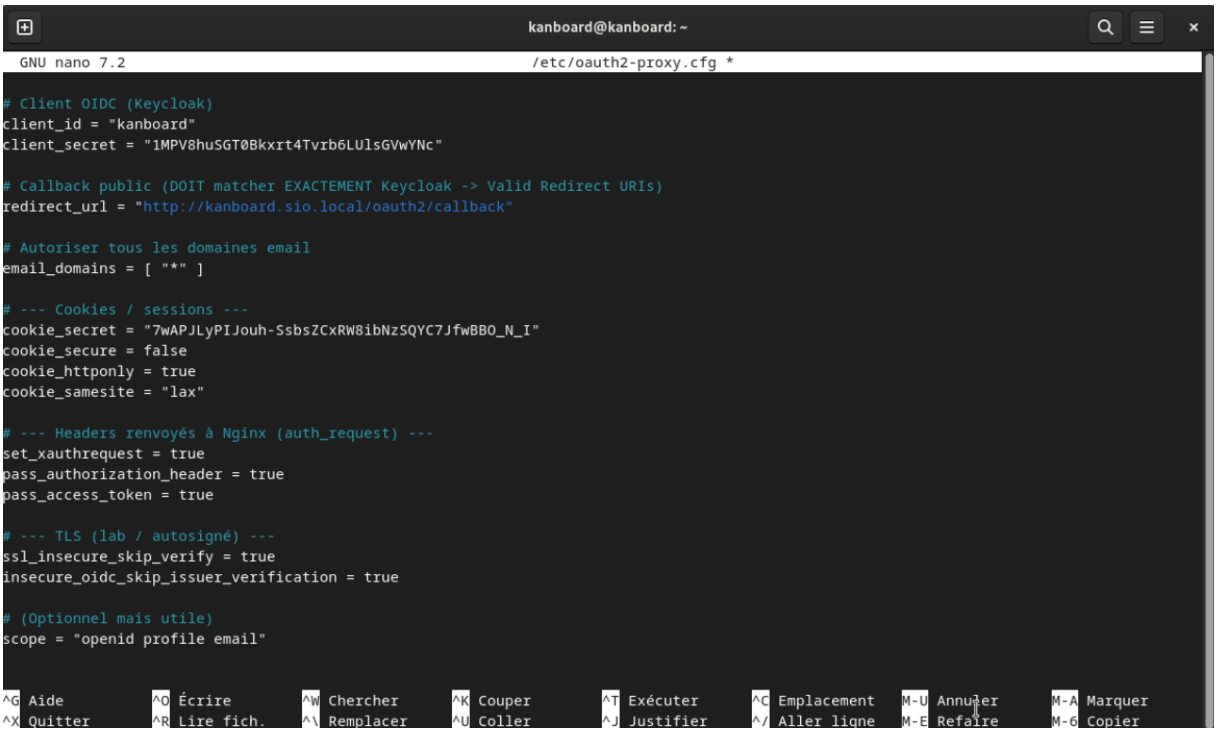
Principe de fonctionnement

1. L'utilisateur accède à l'URL de Kanboard.
2. Nginx intercepte la requête et déclenche une vérification d'authentification.
3. OAuth2-Proxy redirige l'utilisateur vers Keycloak.
4. Après authentification réussie :
    - OAuth2-Proxy valide le jeton,
    - l'accès à Kanboard est autorisé,
    - l'utilisateur est automatiquement connecté.

14.6 Configuration OAuth2-Proxy

Le fichier de configuration d'OAuth2-Proxy définit les paramètres de connexion au client OIDC déclaré dans Keycloak, notamment :

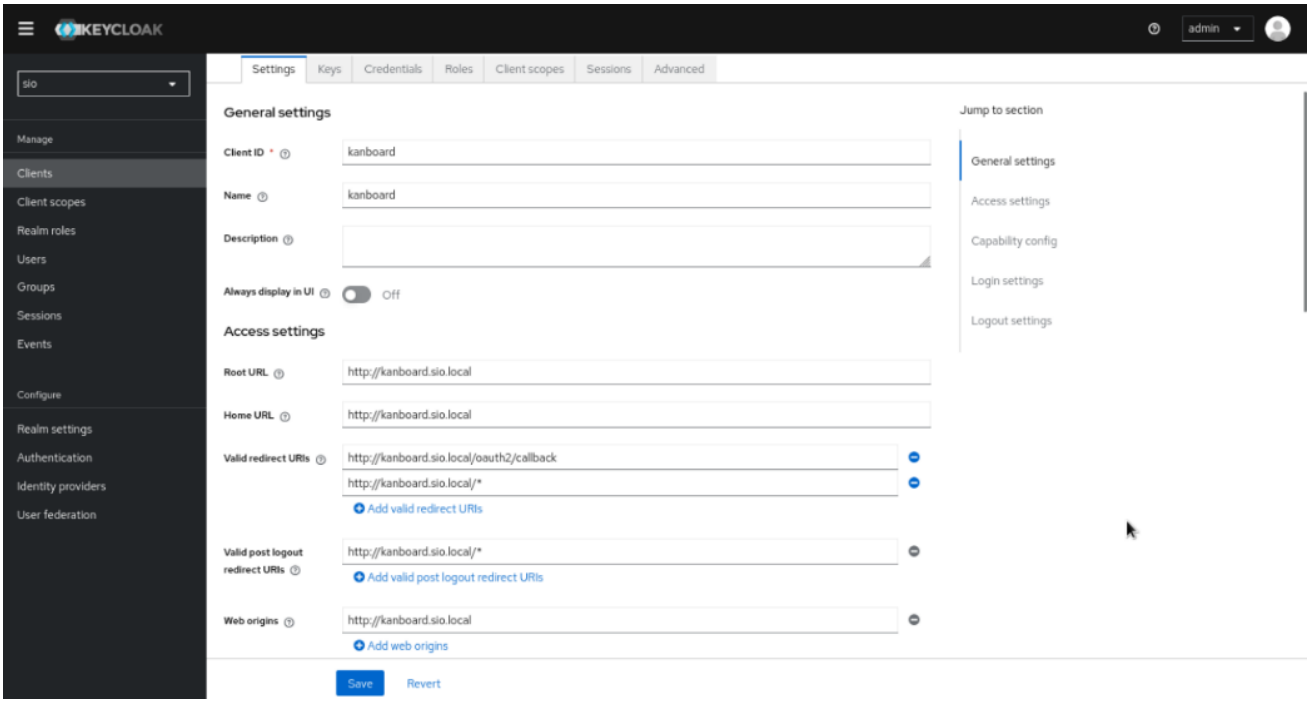
- l'identifiant du client (client_id),
- l'URL de redirection (redirect_url),
- les paramètres de session et de sécurité,
- l'activation du mode auth_request pour l'intégration avec Nginx.



Le client OIDC *kanboard* a été déclaré dans Keycloak afin de permettre l'authentification centralisée des utilisateurs.

Les URL de redirection configurées correspondent au service OAuth2-Proxy, qui assure l'intermédiation entre Keycloak et l'application Kanboard.

Cette configuration permet à Kanboard de déléguer l'authentification à Keycloak sans gérer directement les identifiants utilisateurs.



Le service Nginx est utilisé comme reverse proxy pour l'application Kanboard.

Il constitue le point d'entrée HTTP du service et intercepte toutes les requêtes utilisateurs avant l'accès à l'application.

Grâce au mécanisme auth_request, Nginx délègue l'authentification à OAuth2-Proxy, lequel s'appuie sur Keycloak pour vérifier l'identité des utilisateurs via Active Directory.

L'accès à Kanboard est autorisé uniquement si l'authentification est validée par Keycloak, garantissant ainsi une connexion centralisée et sécurisée (SSO).

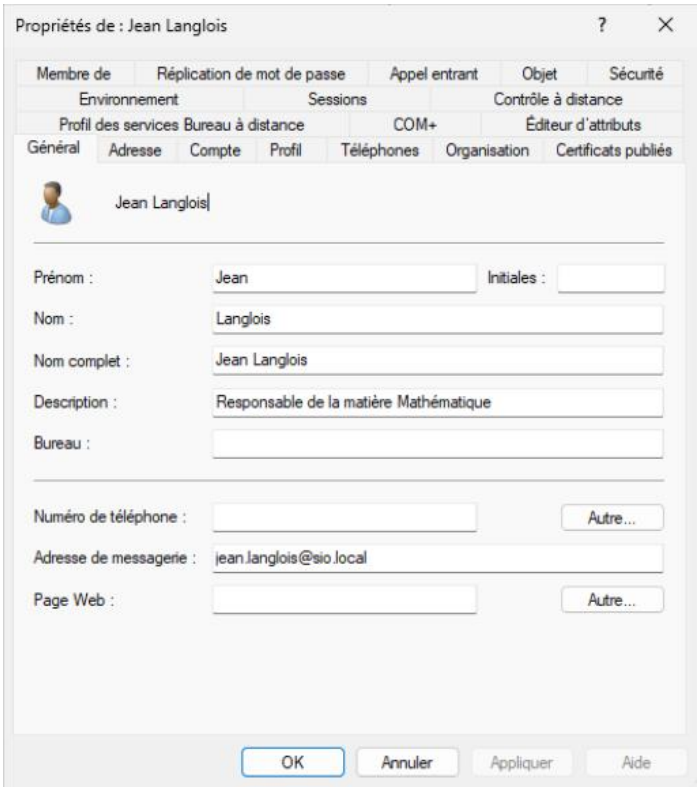
15. Validation du SSO – Keycloak & Kanboard

15.1 Objectif

Valider le bon fonctionnement de l'authentification centralisée (Single Sign-On – SSO) entre :

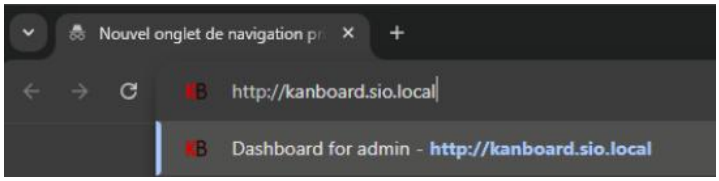
- Active Directory
- Keycloak
- OAuth2-Proxy / Nginx
- Kanboard

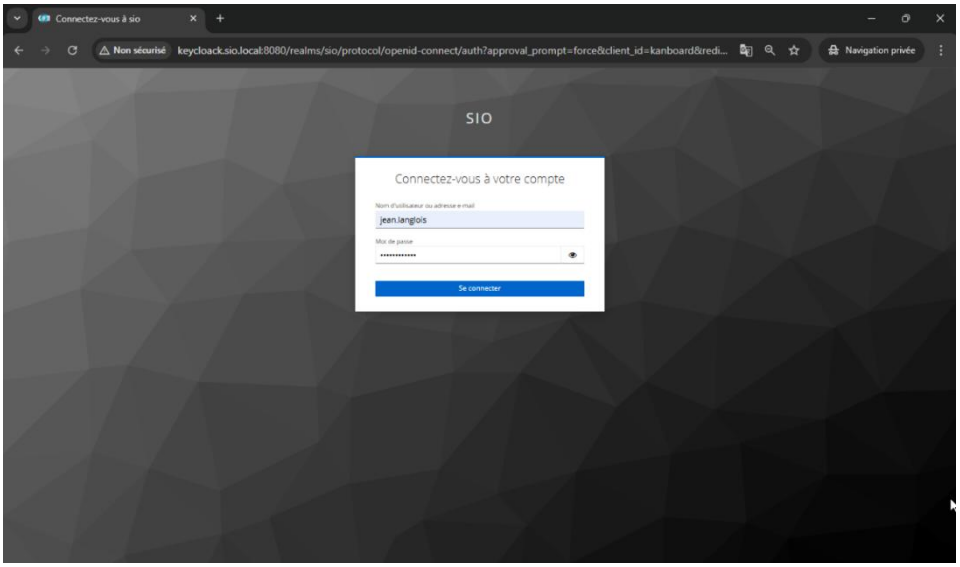
Le test est réalisé avec l'utilisateur **Jean Langlois**, compte du domaine sio.local.

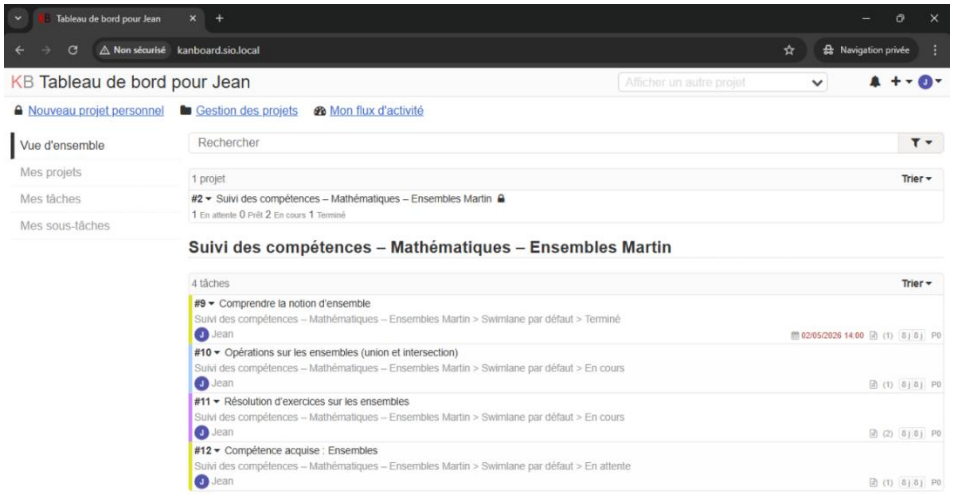


15.2 Déroulement du test

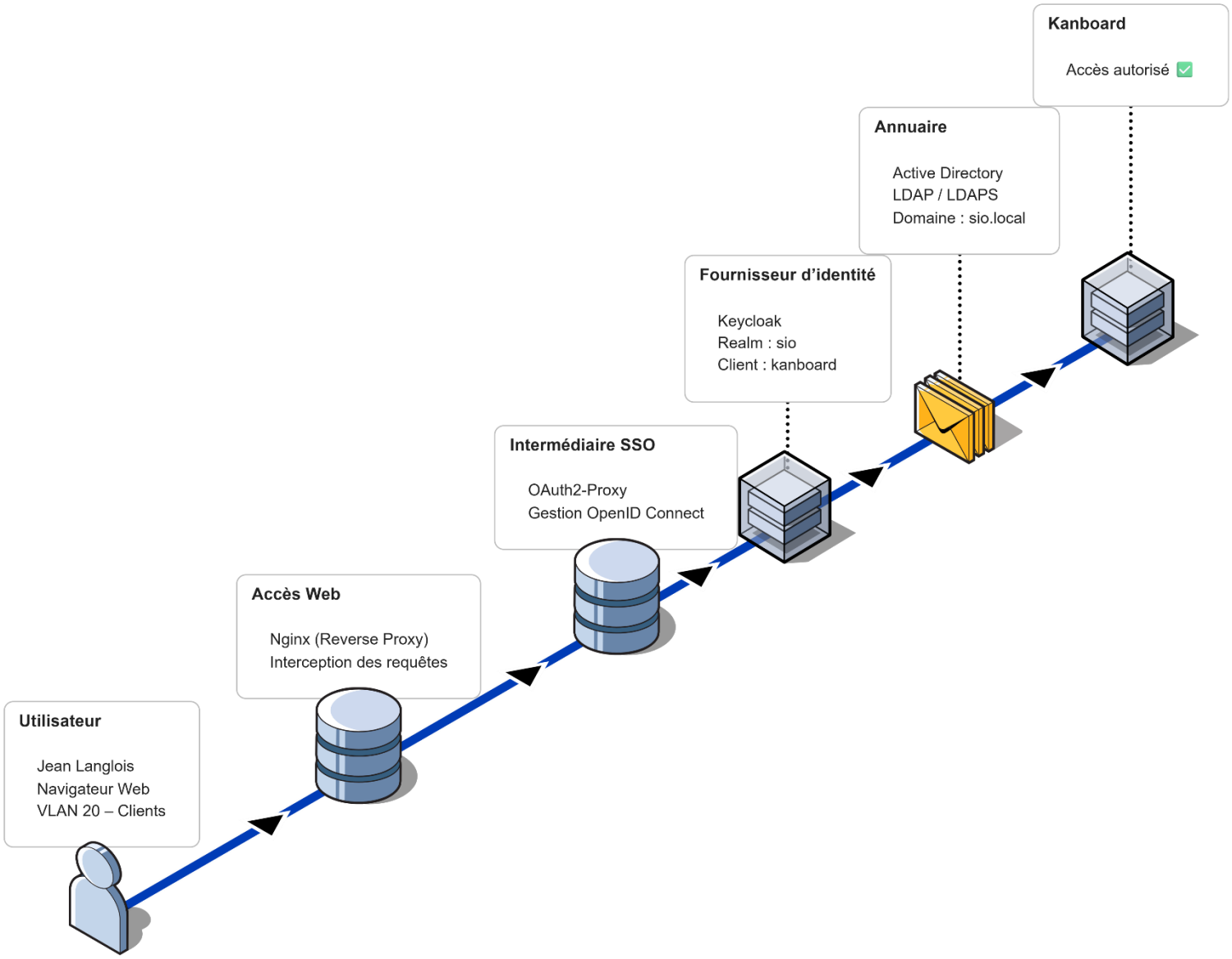
1. L'utilisateur accède à l'URL **http://kanboard.sio.local**
2. Nginx intercepte la requête et déclenche une vérification via OAuth2-Proxy.
3. L'utilisateur est redirigé vers l'interface de connexion Keycloak.
4. Les identifiants Active Directory sont saisis.
5. Après validation par Active Directory (via LDAP), l'utilisateur est automatiquement redirigé vers Kanboard.







15.3 Schéma d’architecture de l’authentification centralisée (SSO)



16. Mise en place du serveur GLPI

16.1 Objectif

Le service GLPI a été déployé afin de mettre en place une solution de gestion du parc informatique et de gestion des tickets d'incident pour l'organisation Langéo Education.

Cette solution permet :

- l'inventaire automatique des postes et logiciels,
- le suivi des incidents et demandes,
- la gestion des utilisateurs et des équipements.

16.2 Déploiement de la machine virtuelle GLPI

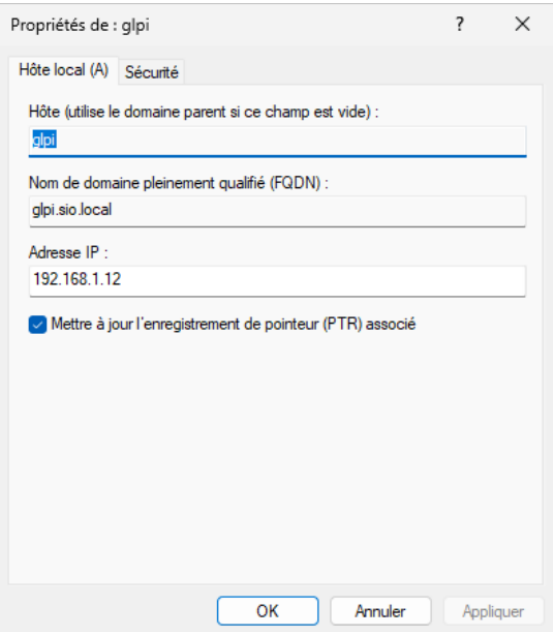
Le service GLPI est hébergé sur :

- une machine virtuelle Debian,
- intégrée au VLAN 10 – Serveurs,
- déployée sur l'hyperviseur Proxmox.

Cette machine est dédiée exclusivement à la gestion du parc informatique et des tickets afin de garantir :

- une meilleure isolation du service,
- une centralisation des données d'inventaire,
- une maintenance simplifiée et évolutive.

L'application est accessible via le nom de domaine **glpi.sio.local**, configuré dans le serveur DNS Active Directory.



16.3 Installation et configuration de la base de données

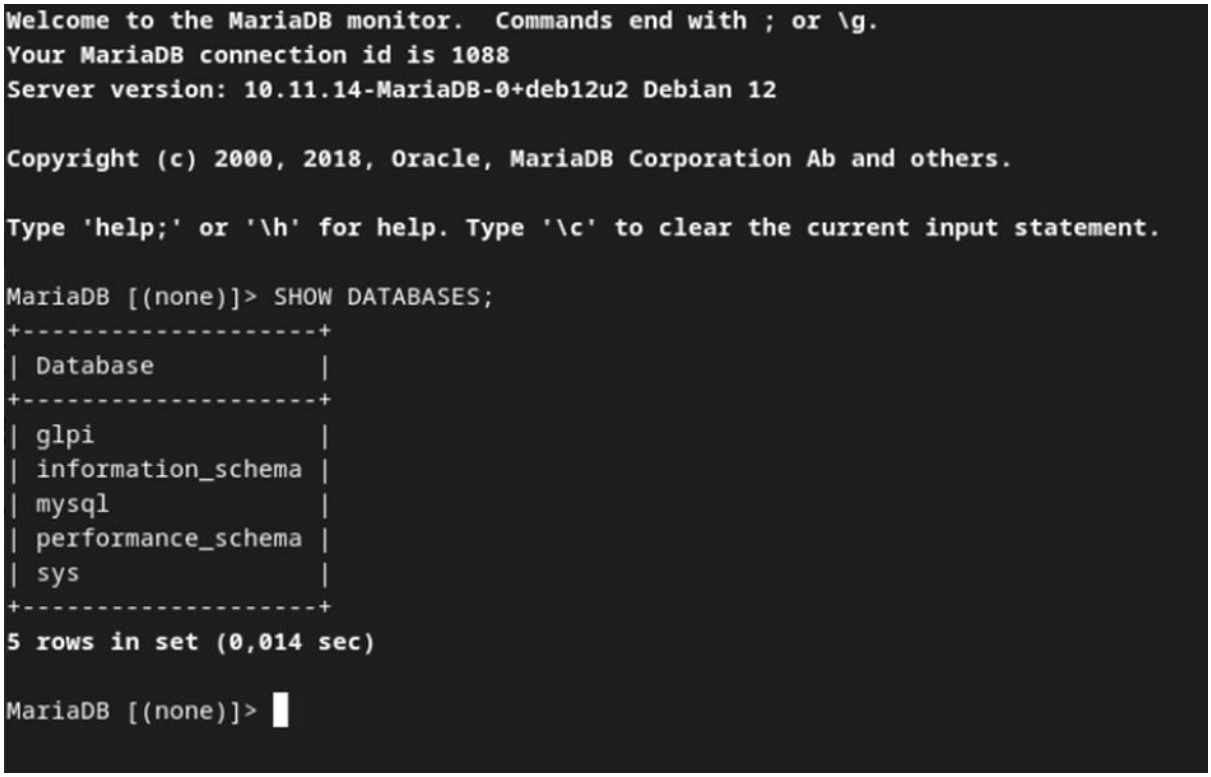
Afin d'assurer le fonctionnement de l'application GLPI, une base de données MariaDB a été installée et configurée sur la machine virtuelle dédiée.

La configuration comprend :

- l'installation du serveur MariaDB,
- la création d'une base de données dédiée à GLPI,
- la création d'un utilisateur spécifique avec des droits restreints,
- l'association de cet utilisateur à la base GLPI.

Cette séparation permet :

- une meilleure sécurisation des accès,
- une gestion maîtrisée des privilèges,
- une architecture plus professionnelle et maintenable.



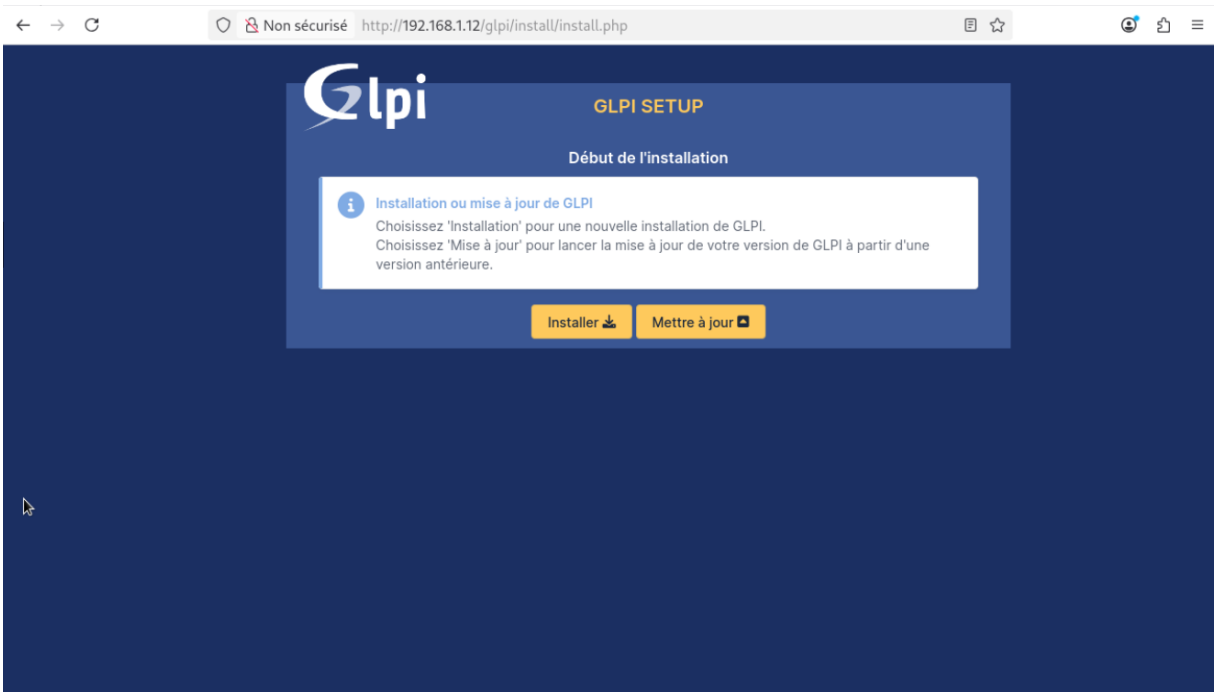
16.4 Installation et mise en service de GLPI

Une fois la base de données MariaDB opérationnelle, l'installation de GLPI a été réalisée via son interface web.

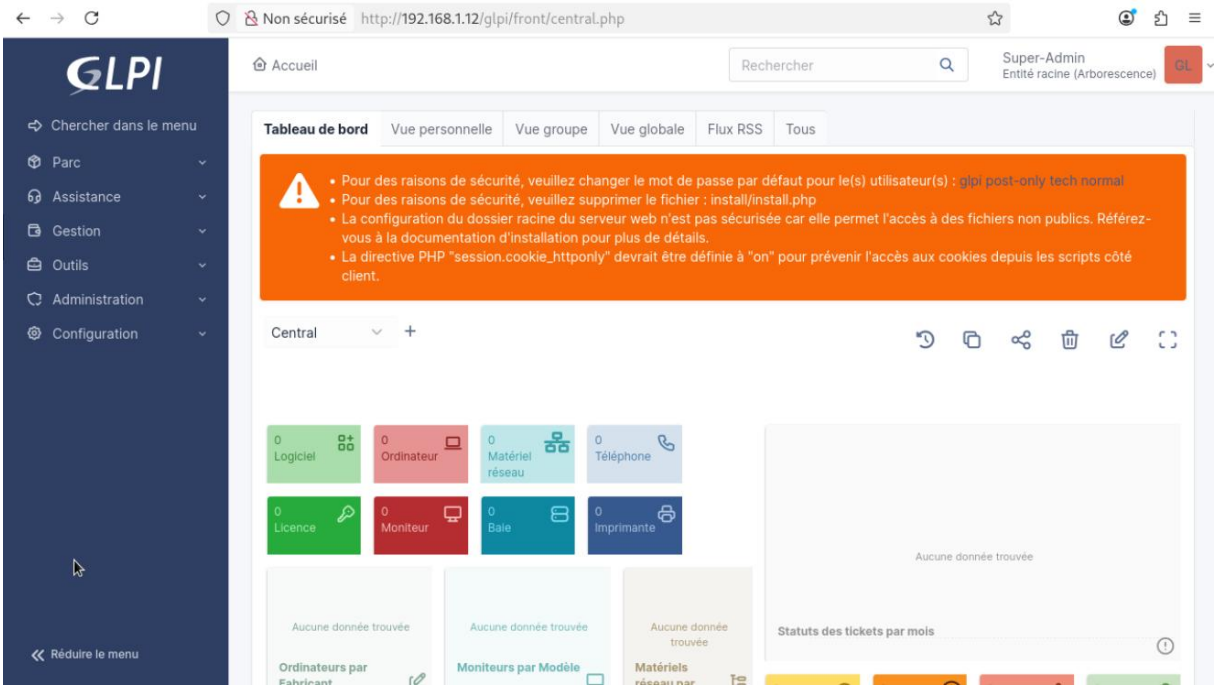
La configuration repose sur :

- un serveur MariaDB local,
- une base dédiée nommée glpi,
- un utilisateur SQL spécifique disposant de droits restreints.

Cette étape permet de finaliser le déploiement de l'application et de rendre l'interface accessible aux administrateurs.



Une fois l'installation terminée, l'accès au tableau de bord confirme la bonne initialisation du service et la disponibilité de l'environnement de gestion.



Conformément aux bonnes pratiques de sécurité, les paramètres par défaut ont été modifiés et les éléments d'installation supprimés.

16.5 Déploiement de l'agent GLPI et remontée d'inventaire

Afin d'automatiser la gestion du parc informatique de l'organisation fictive *Langéo Education*, l'agent GLPI a été déployé sur les postes clients du VLAN 20.

L'agent permet de :

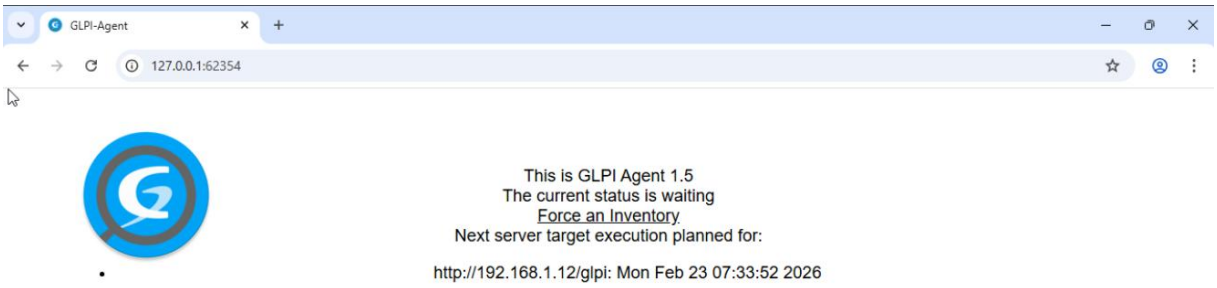
- remonter automatiquement les informations matérielles (processeur, mémoire, stockage),
- inventorier les logiciels installés,
- identifier le système d'exploitation,
- transmettre les données vers le serveur GLPI.

Les postes configurés communiquent directement avec le serveur GLPI via son adresse interne **http://glpi.sio.local**

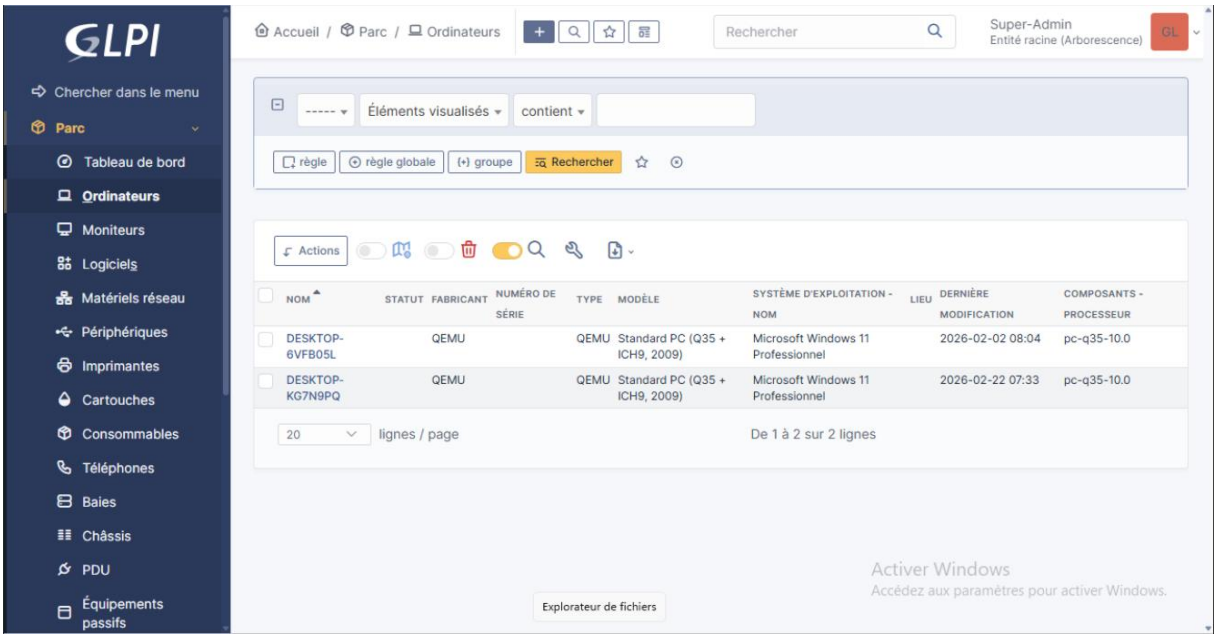
Chaque machine envoie périodiquement ses informations, permettant à l'administrateur de disposer d'une vision centralisée et actualisée du parc informatique.

Une interface locale accessible sur chaque poste via **127.0.0.1:62354**, permet de vérifier l'état de l'agent et de déclencher manuellement un inventaire à l'aide de la fonctionnalité **"Force an Inventory"**.

Cette action a été utilisée afin de valider immédiatement la remontée des informations vers le serveur GLPI.



La présence des postes, de leurs composants matériels et de leurs logiciels dans l'interface GLPI confirme le bon fonctionnement du mécanisme d'inventaire.



16.6 Création des comptes utilisateurs et administrateurs GLPI

Une fois l'application GLPI opérationnelle, la gestion des comptes utilisateurs a été configurée afin de structurer les accès au service.

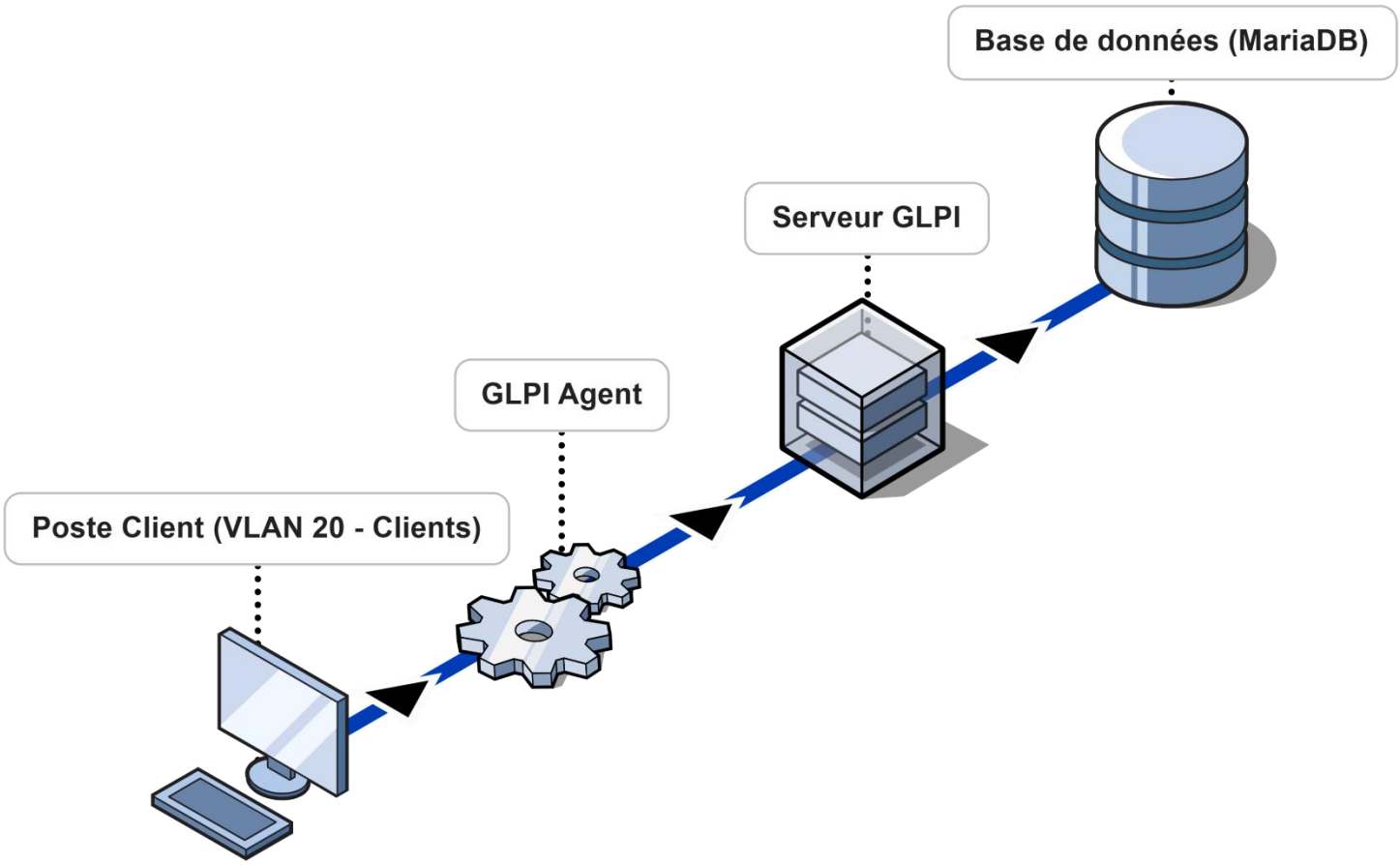
Deux types de comptes ont été mis en place :

- des comptes utilisateurs standards destinés aux collaborateurs pour la création et le suivi des tickets,
- un compte administrateur dédié à la gestion technique de la plateforme.

Cette séparation des rôles permet :

- une meilleure organisation des accès,
- une traçabilité des actions,
- une sécurisation accrue de l'environnement.

16.7 Architecture logique du service GLPI



17. Mise en place du serveur de supervision Zabbix

17.1 Objectif

Le service **Zabbix** a été déployé afin d'assurer la supervision centralisée de l'infrastructure mise en place pour le projet *Langéo Education*.

Il permet de surveiller en temps réel :

- le serveur **GLPI**,
- le serveur **Keycloak**,
- le serveur **Kanboard**,
- le serveur **Docker (DMZ)**,
- le contrôleur de domaine **Active Directory / DNS**,
- ainsi que le pare-feu **pfSense**.

Cette supervision permet :

- la détection proactive des incidents,
- le suivi des ressources système (CPU, RAM, stockage),
- la vérification de la disponibilité des services,
- une meilleure réactivité en cas de panne.

17.2 Déploiement du serveur Zabbix

Le service Zabbix est hébergé sur :

- une machine virtuelle Debian,
- intégrée au **VLAN 10 – Serveurs**,
- déployée sur l'hyperviseur **Proxmox**.

La solution repose sur :

- un serveur Zabbix,
- une base de données MariaDB,
- une interface Web accessible aux administrateurs.

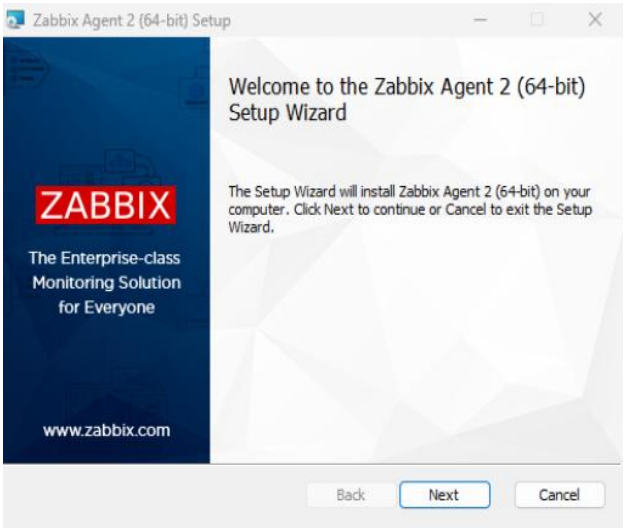
17.3 Fonctionnement de la supervision

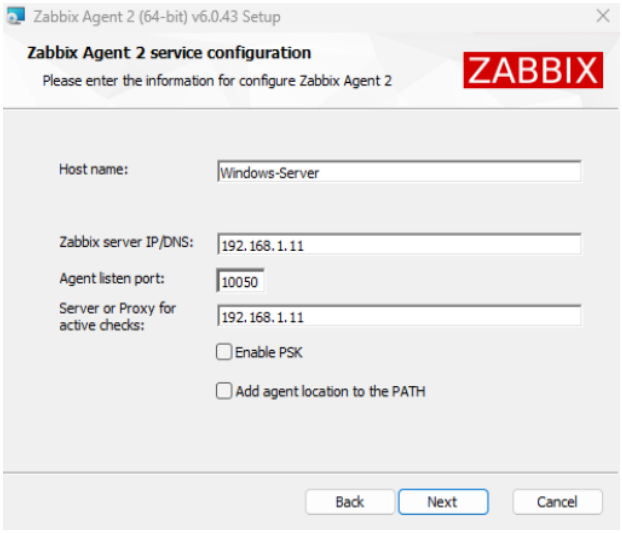
La collecte des données s'effectue via l'installation d'un agent Zabbix sur chaque serveur supervisé.

L'agent :

- collecte les informations système (CPU, RAM, disque, uptime),
- surveille l'état des services,
- transmet les données au serveur Zabbix.

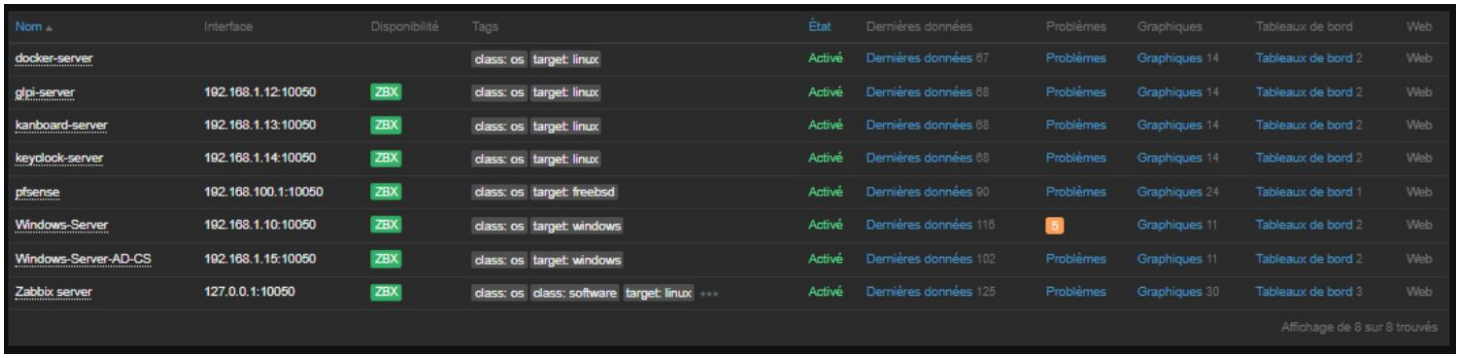
La communication s'effectue via le port 10050/TCP





Une vue centralisée des hôtes supervisés permet de vérifier en temps réel la disponibilité des serveurs, la réception des données et l'absence d'incidents critiques.

Tous les serveurs critiques affichent un statut actif, confirmant la bonne communication des agents avec le serveur Zabbix via le port 10050/TCP.



17.4 Tableaux de bord personnalisés

Des tableaux de bord spécifiques ont été créés pour chaque serveur critique.

L'exemple ci-dessous présente le dashboard du pare-feu pfSense, affichant :

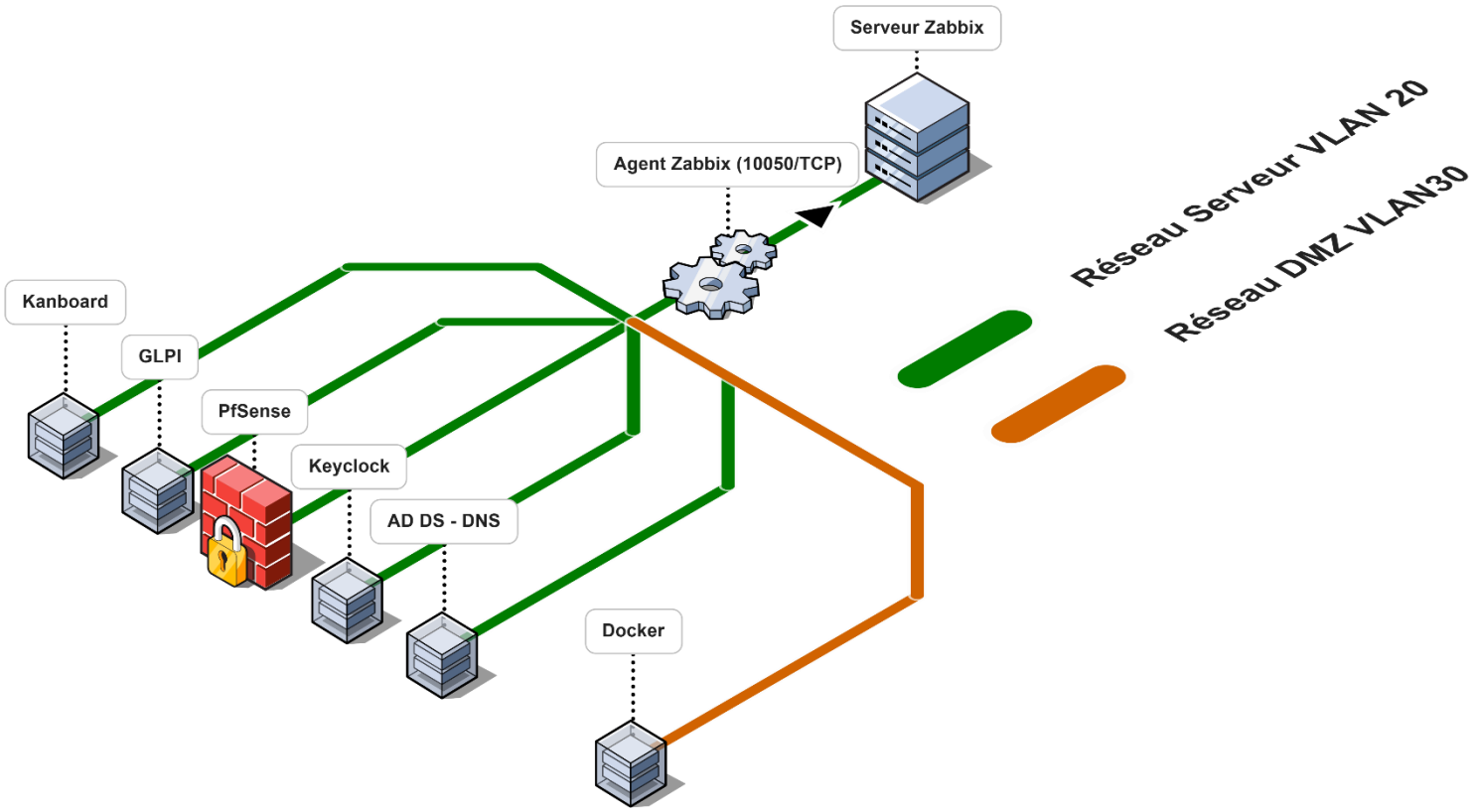
- l'utilisation mémoire,
- la charge CPU,
- le trafic WAN et LAN,
- l'activité des VLAN 10, 20 & 30.

Ces dashboards permettent une analyse rapide de l'état d'un service sans avoir à naviguer dans les menus techniques.

Ils constituent un outil essentiel pour :

- détecter une surcharge,
- anticiper une panne,
- démontrer la stabilité de l'infrastructure.

17.5 Architecture logique du service de supervision Zabbix



18. Mise en place du serveur Web en DMZ (Docker)

18.1 Objectif

Un serveur Web a été déployé en **DMZ (VLAN 30)** afin de simuler la mise en ligne du site Internet de l'organisation fictive *Langéo Education*.

L'objectif est de reproduire un scénario réaliste dans lequel :

- l'établissement dispose d'un site institutionnel accessible depuis Internet,
- le service Web est isolé du réseau interne,
- les flux sont strictement contrôlés par le pare-feu pfSense,
- l'architecture respecte les bonnes pratiques de sécurité.

Cette mise en situation permet d'illustrer concrètement l'exposition d'un service vers l'extérieur tout en garantissant la protection de l'infrastructure interne.

18.2 Déploiement de la machine virtuelle DMZ

Le service Web public de *Langéo Education* est hébergé sur une machine virtuelle Debian dédiée, positionnée dans le **VLAN 30 – DMZ**.

Sur cette machine :

- le moteur **Docker** a été installé,
- l'outil de gestion **Portainer** a été déployé,
- un conteneur Web simule le site institutionnel.

L'utilisation d'une machine dédiée en DMZ permet :

- d'isoler le service exposé du réseau interne,
- de cloisonner les flux via pfSense,
- de limiter les risques en cas de compromission.

18.3 Mise en place de Docker et Portainer

Docker a été installé sur la VM Debian afin de permettre la conteneurisation des services.

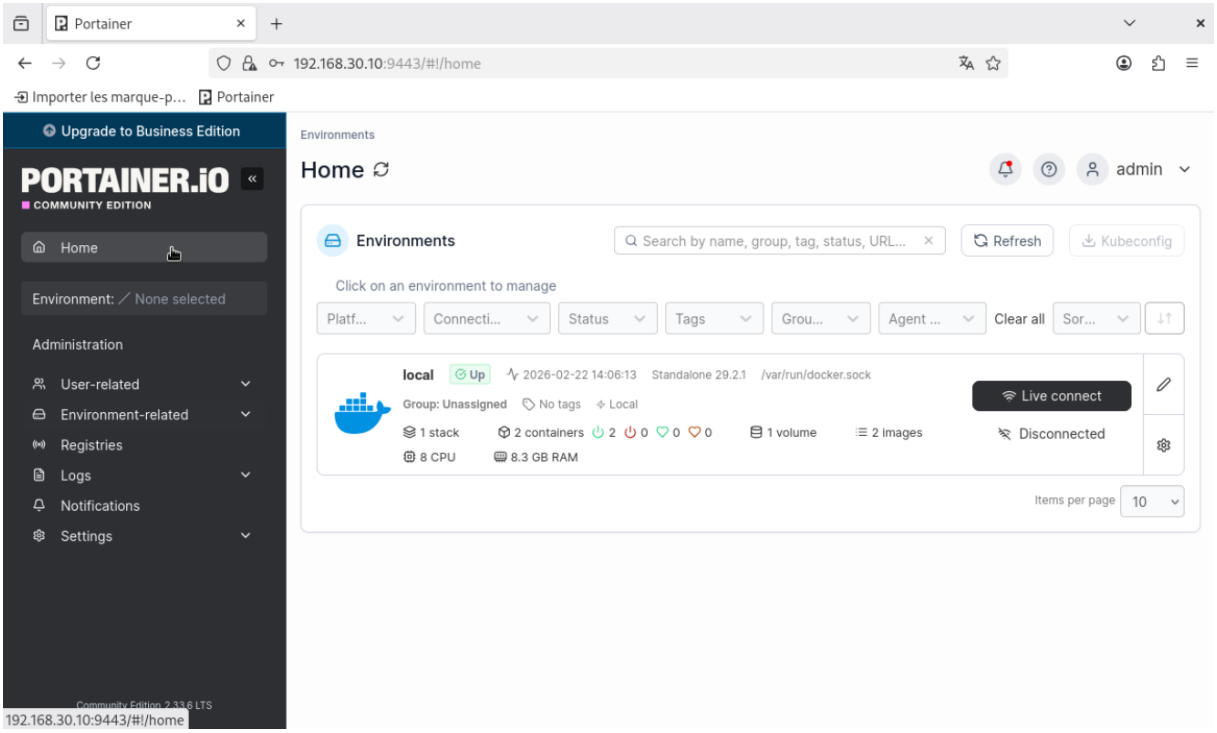
L'interface **Portainer** a été déployée pour :

- administrer les conteneurs,
- superviser leur état,
- simplifier la gestion et le redéploiement.

Un conteneur Web a ensuite été lancé pour simuler le site public de Langéo Education, exposé sur le port 80 du serveur DMZ.

Cette approche permet une architecture :

- modulaire,
- facilement maintenable,
- évolutive.



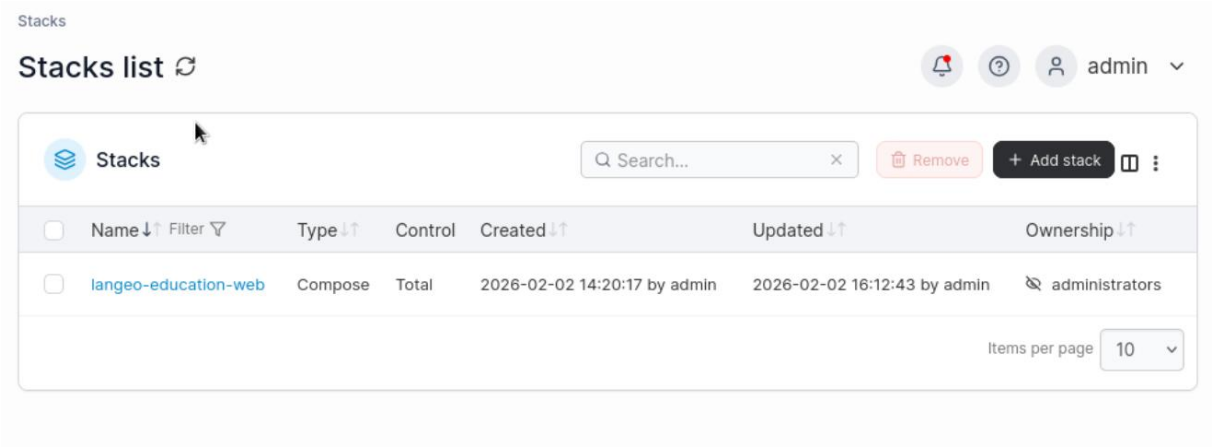
18.4 Stack du service Web exposé

Le site public de *Langéo Education* repose sur un conteneur Web exécuté via Docker sur la machine DMZ.

Le conteneur :

- écoute sur le port 80,
- est administré via Portainer,
- est isolé du réseau interne.

Le port 80 du serveur DMZ sera ensuite publié via une règle NAT sur pfSense afin de permettre l'accès depuis Internet.



18.5 Publication du service Web via pfSense

Afin de rendre le site Web de *Langéo Education* accessible depuis l'extérieur, une règle de redirection NAT a été configurée sur le pare-feu pfSense.

Le principe retenu est le suivant :

- le port **8081** de l'interface WAN est exposé,
- ce port est redirigé vers le serveur Web situé en **DMZ (192.168.30.10)**,
- le trafic est ensuite transmis vers le port **80 (HTTP)** du conteneur Docker.

Cette configuration permet :

- d'exposer uniquement le service Web,
- de ne pas divulguer directement le port interne 80,
- de contrôler précisément les flux entrants.

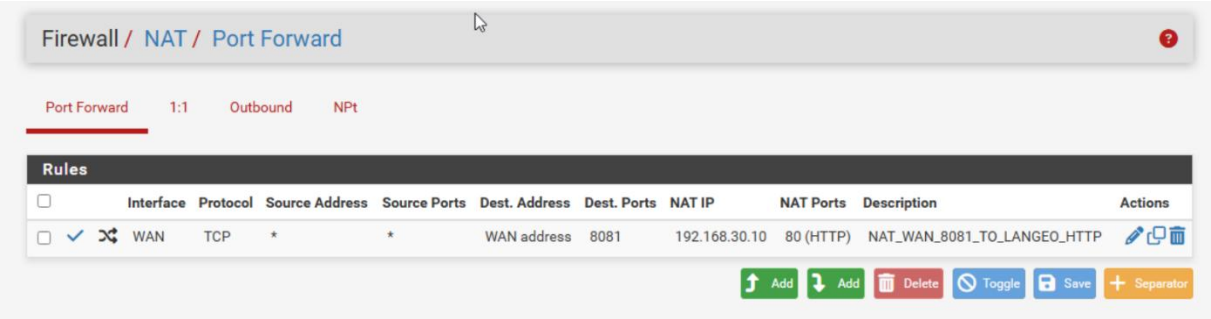
La règle NAT est complétée par une règle firewall associée autorisant le trafic TCP entrant sur le port 8081.

En parallèle, des règles spécifiques ont été mises en place sur le VLAN 30 (DMZ) afin de :

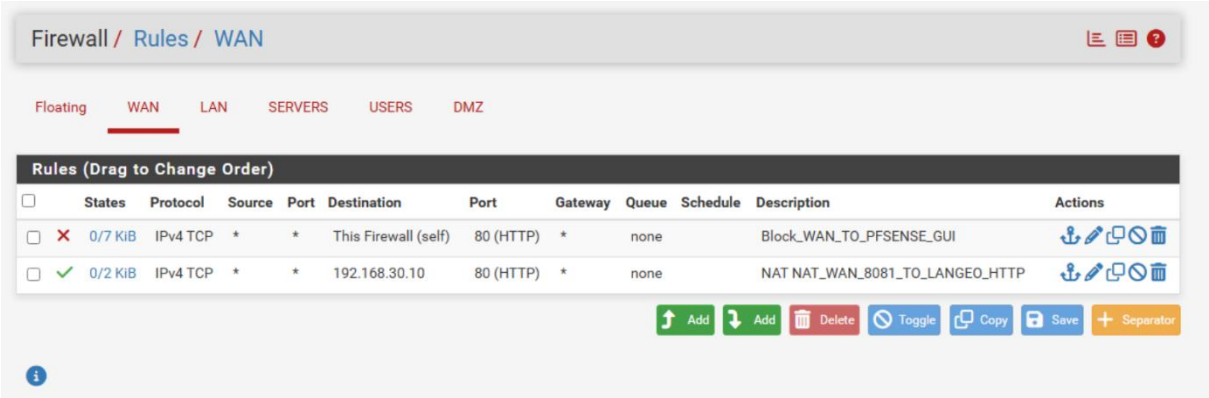
- autoriser uniquement les flux nécessaires (HTTP et supervision Zabbix),
- permettre la résolution DNS vers Internet,
- bloquer tout accès vers les réseaux internes (LAN, USERS),
- interdire l'accès direct au pare-feu.

Cette architecture reproduit un scénario réel d'exposition d'un service Internet tout en respectant les bonnes pratiques de sécurité réseau.

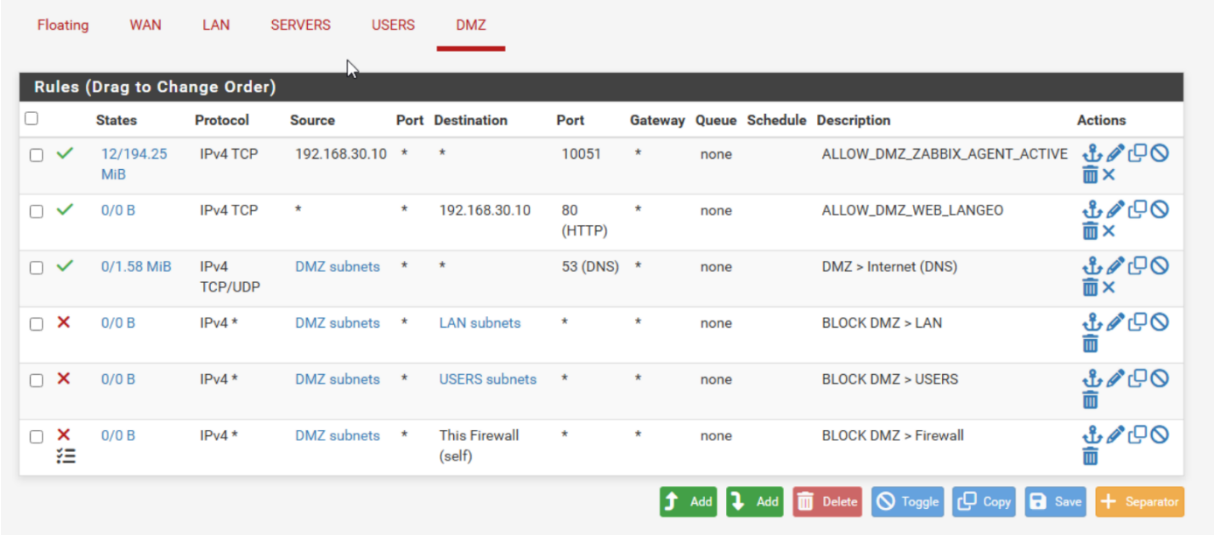
Règle NAT WAN :



Règles Firewall WAN :



Règles VLAN 30 (DMZ) :



** Les statistiques de trafic visibles sur les règles confirment le bon fonctionnement de la publication du service.*

18.6 Test d'accessibilité externe du service Web

Afin de valider la publication du site Web de *Langéo Education*, un test d'accès a été réalisé depuis un poste situé en dehors du réseau interne.

Dans le cadre de cette maquette, le réseau « WAN » ne correspond pas à Internet réel mais au réseau externe du routeur pfSense.
Ce choix permet de simuler un accès extérieur tout en restant dans un environnement contrôlé.

Le poste de test a été placé sur le réseau WAN et configuré avec les paramètres suivants :

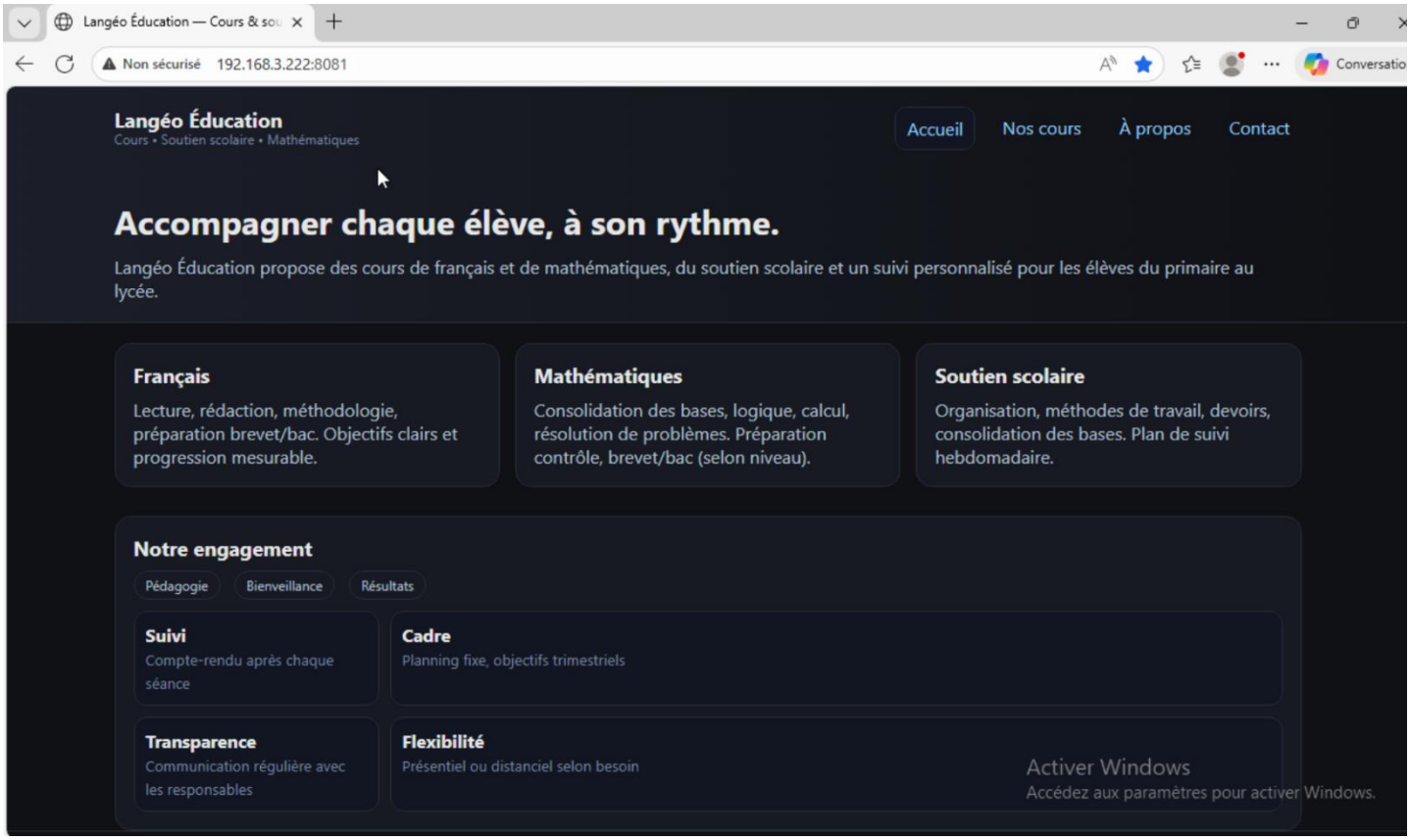
- Adresse IP : 192.168.3.230
- Passerelle : 192.168.3.254 (Routeur du centre de formation)

Une connexion a ensuite été effectuée vers l'adresse **192.168.3.222:8081**

La page du site Web institutionnel s'affiche correctement, confirmant :

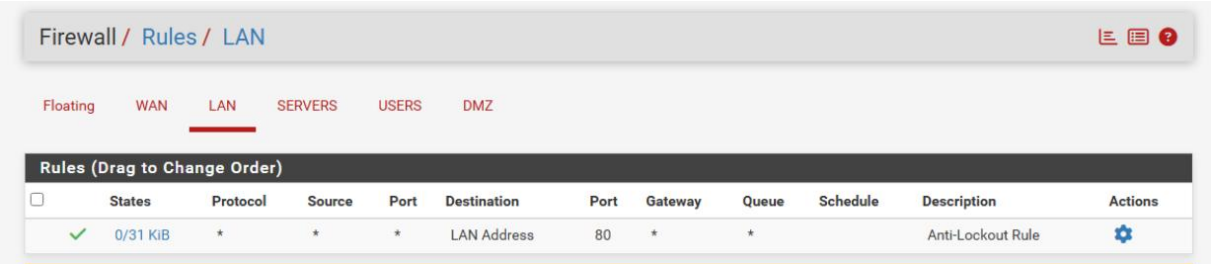
- le bon fonctionnement de la règle NAT,
- l'autorisation du flux WAN,
- l'accessibilité du serveur Web situé en DMZ.

Ce test valide le bon cloisonnement de l'infrastructure ainsi que l'exposition maîtrisée du service vers l'extérieur.



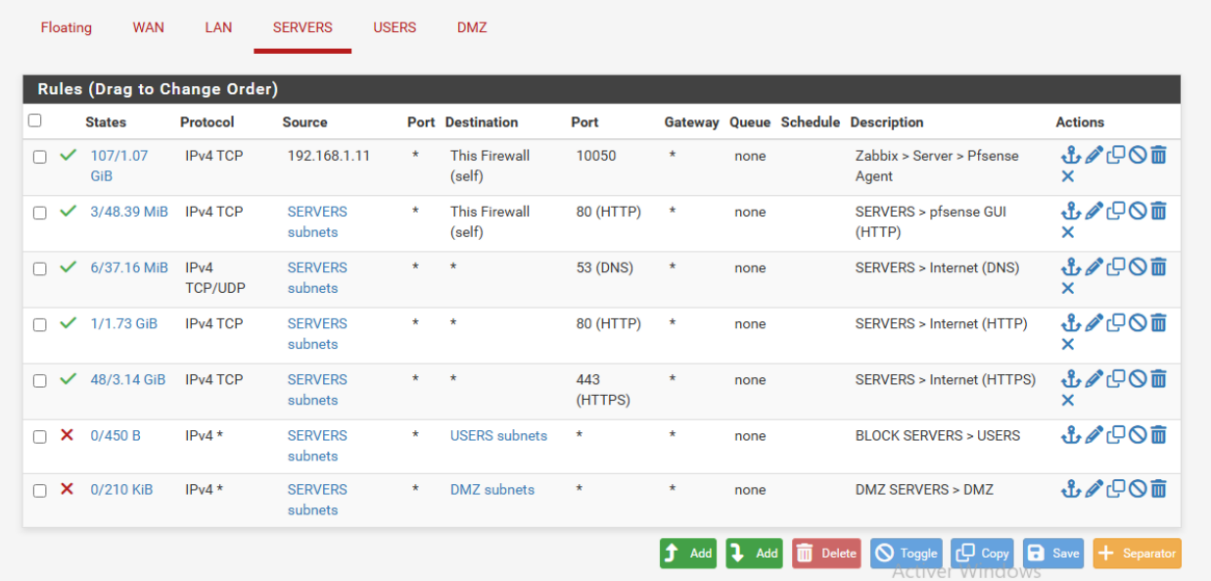
19. Sécurisation et gestion des flux inter-VLAN

Interface LAN :



L'interface LAN conserve la règle Anti-Lockout par défaut permettant l'accès sécurisé à l'interface d'administration du pare-feu.

VLAN 10 – Serveurs :



Le VLAN 10 regroupe les serveurs applicatifs et d'infrastructure (GLPI, Keycloak, Kanboard, Zabbix, Active Directory / DNS).

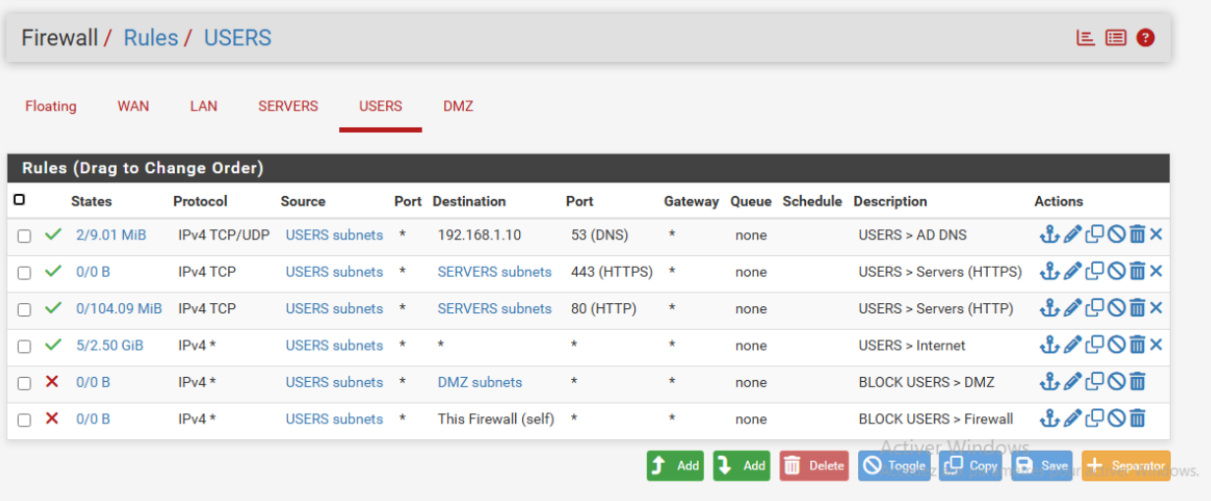
Les règles configurées permettent :

- la supervision du pare-feu par le serveur Zabbix,
- l'accès à l'interface pfSense depuis le réseau serveurs,
- la résolution DNS ainsi que les mises à jour via Internet (HTTP/HTTPS).

Les flux vers le VLAN 20 (Utilisateurs) et le VLAN 30 (DMZ) sont bloqués afin d'éviter tout mouvement latéral non nécessaire.

Cette configuration limite la surface d'attaque et protège les postes utilisateurs en cas de compromission d'un serveur.

VLAN 20 – Utilisateurs :



Le VLAN 20 regroupe les postes clients de l'infrastructure.

Les règles permettent :

- la résolution DNS via le contrôleur de domaine,
- l'accès aux services internes hébergés dans le VLAN 10 (HTTP/HTTPS),
- l'accès à Internet pour les usages courants.

Les communications vers la DMZ ainsi que vers le pare-feu sont bloquées afin de garantir le cloisonnement réseau.

Cette approche applique le principe du moindre privilège en autorisant uniquement les flux nécessaires au fonctionnement des services.

20. Conclusion

Le projet *Langéo Education* avait pour objectif de concevoir et déployer une infrastructure réseau virtualisée intégrant plusieurs services essentiels : gestion de parc (GLPI), supervision (Zabbix), authentification centralisée (Keycloak), gestion de projets (Kanboard), ainsi qu'un service Web exposé en DMZ.

L'architecture mise en place repose sur :

- une segmentation logique via plusieurs VLANs,
- un pare-feu pfSense assurant le filtrage et la gestion des flux,
- une isolation des services critiques,
- une supervision active de l'ensemble des composants.

La mise en œuvre d'une DMZ dédiée à l'exposition du service Web illustre concrètement la maîtrise des mécanismes de publication sécurisée via NAT et règles de filtrage.
Les règles inter-VLAN appliquent le principe du moindre privilège en autorisant uniquement les communications strictement nécessaires au fonctionnement des services.

La supervision via Zabbix permet une surveillance proactive des serveurs et équipements, garantissant la disponibilité et la stabilité de l'infrastructure.

Ce projet m'a permis de mobiliser et d'approfondir mes compétences en :

- conception d'architecture réseau,
- segmentation et sécurisation des flux,
- administration de serveurs Linux et Windows,
- gestion des services applicatifs,
- mise en œuvre de solutions de supervision,
- publication contrôlée d'un service vers l'extérieur.

Au-delà de l'aspect technique, cette réalisation m'a permis d'adopter une démarche professionnelle : analyse des besoins, structuration de l'infrastructure, validation des flux et contrôle de la sécurité.

L'infrastructure obtenue est cohérente, cloisonnée et conforme aux bonnes pratiques d'administration système et réseau.

21. Glossaire

1. VLAN (Virtual Local Area Network)

Un VLAN permet de segmenter logiquement un réseau physique en plusieurs réseaux distincts afin d'isoler les flux et améliorer la sécurité.

2. DMZ (Demilitarized Zone)

Zone réseau intermédiaire destinée à héberger des services exposés vers l'extérieur tout en protégeant le réseau interne.

3. NAT (Network Address Translation)

Mécanisme permettant de traduire une adresse IP ou un port vers une autre adresse interne, utilisé pour publier un service.

4. Pare-feu (Firewall)

Équipement ou logiciel permettant de filtrer les communications réseau selon des règles définies.

5. Principe du moindre privilège

Concept de sécurité consistant à autoriser uniquement les accès strictement nécessaires.

6. Supervision

Surveillance en temps réel des ressources et services d'une infrastructure afin de détecter les incidents.

7. Agent de supervision

Logiciel installé sur une machine permettant de collecter et transmettre des informations au serveur de supervision.

8. Conteneurisation

Méthode permettant d'exécuter des applications dans des environnements isolés et portables (ex : Docker).

9. Hyperviseur

Logiciel permettant de créer et gérer des machines virtuelles (ex : Proxmox).

10. Segmentation réseau

Découpage d'un réseau en plusieurs zones afin de limiter la propagation d'une attaque.

**Le présent glossaire reprend les principaux termes techniques utilisés dans ce dossier. Il vise à faciliter la compréhension des notions clés mobilisées dans le cadre du projet.*