Supervision Zabbix avec Active Directory et Authentification LDAP/LDAPS

Réalisé par : **SOULAIMAN Rayane**

Administrateur système, réseau et sécurité

Table des matières

Introduction

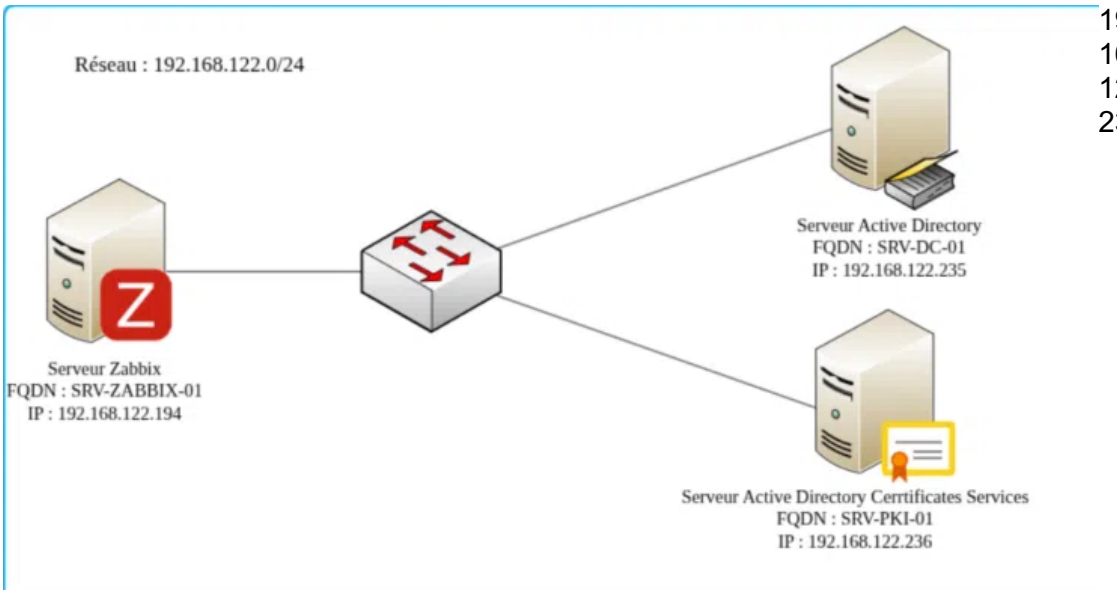
Ce document constitue le compte-rendu technique d'un travail pratique portant sur la mise en place d'une solution de supervision réseau Zabbix 7.4 intégrée à un annuaire Active Directory. Il s'inscrit dans le cadre de la formation BTS Services Informatiques aux Organisations (SIO) et illustre des compétences en administration système, en sécurité réseau et en gestion d'identités.

L'objectif de ce TP est triple :

- Déployer et configurer Zabbix 7.4 sur un serveur Debian 12 avec une base de données MariaDB et un serveur web Apache.
- Intégrer un agent Zabbix sur un serveur Windows Server membre d'un domaine Active Directory pour en assurer la supervision.
- Configurer l'authentification LDAP puis LDAPS (version chiffrée) afin que les comptes Active Directory puissent se connecter à l'interface web de Zabbix de manière sécurisée.

L'infrastructure mise en œuvre repose sur un environnement virtualisé composé des éléments suivants :

- Serveur Zabbix : VM Debian 12 — IP 192.168.122.194
- Contrôleur de domaine : VM Windows Server (SRV-DC-01) — IP 192.168.122.235
- Serveur PKI (Autorité de Certification) : VM Windows Server (SRV-PKI-01) — IP 192.168.122.236



Partie 1 — Installation de Zabbix sur Debian 12

Cette première partie décrit l'installation complète du serveur de supervision Zabbix 7.4, incluant la configuration de l'adresse IP statique, l'installation des paquets nécessaires, la création de la base de données et la finalisation via l'interface web.

1.1 Prérequis : configuration de l'adresse IP statique

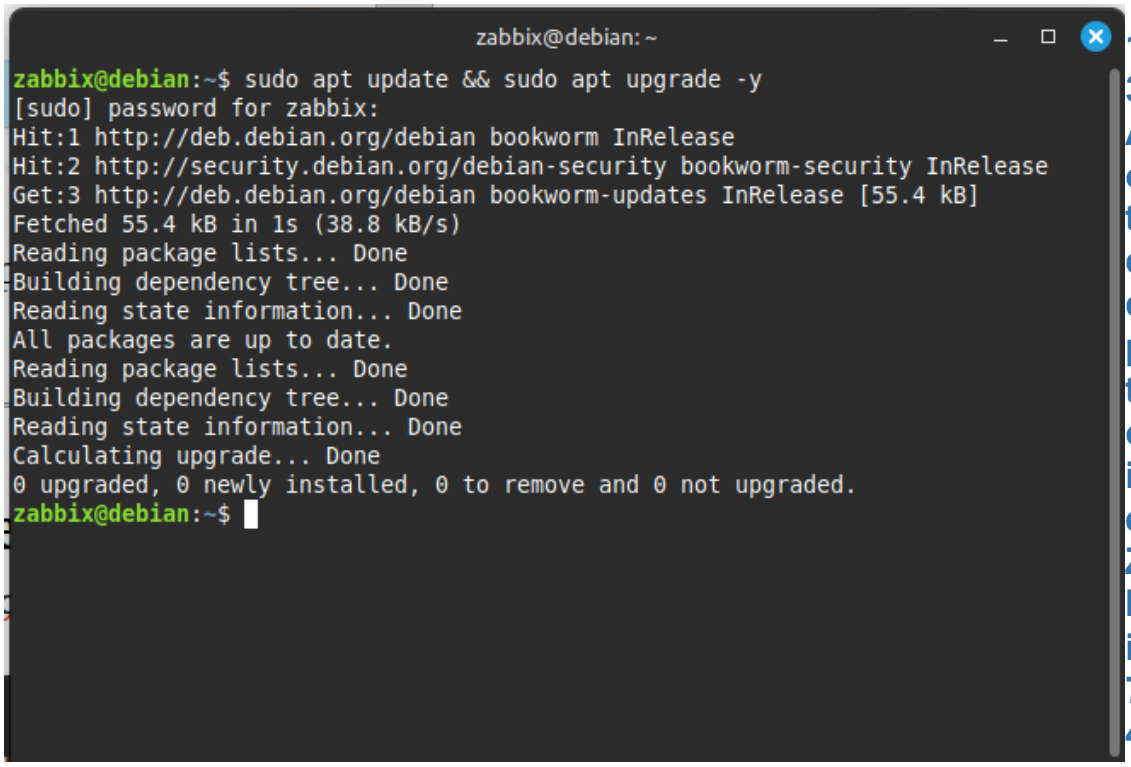
Avant toute installation de logiciel, il convient d'attribuer une adresse IP fixe au serveur afin de garantir la cohérence des communications réseau avec les autres machines de l'infrastructure.

Figure 1 — Configuration de l'adresse IP statique sur Debian 12

1.2 Mise à jour du système

La première opération consiste à s'assurer que le système dispose des dernières mises à jour de sécurité et de stabilité avant d'installer de nouveaux paquets.

```
sudo apt update && sudo apt upgrade -y
```



1.3 Ajout du dépôt officiel Zabbix 7.4

Zabbix ne figure pas dans les dépôts standard de Debian. Il est nécessaire d'ajouter le dépôt officiel du projet pour accéder à la version 7.4.

```
wget https://repo.zabbix.com/zabbix/7.4/release/debian/pool/main/z/zabbix-release/zabbix-release_latest_7.4+debian12_all.deb
sudo dpkg -i zabbix-release_latest_7.4+debian12_all.deb
sudo apt update
```

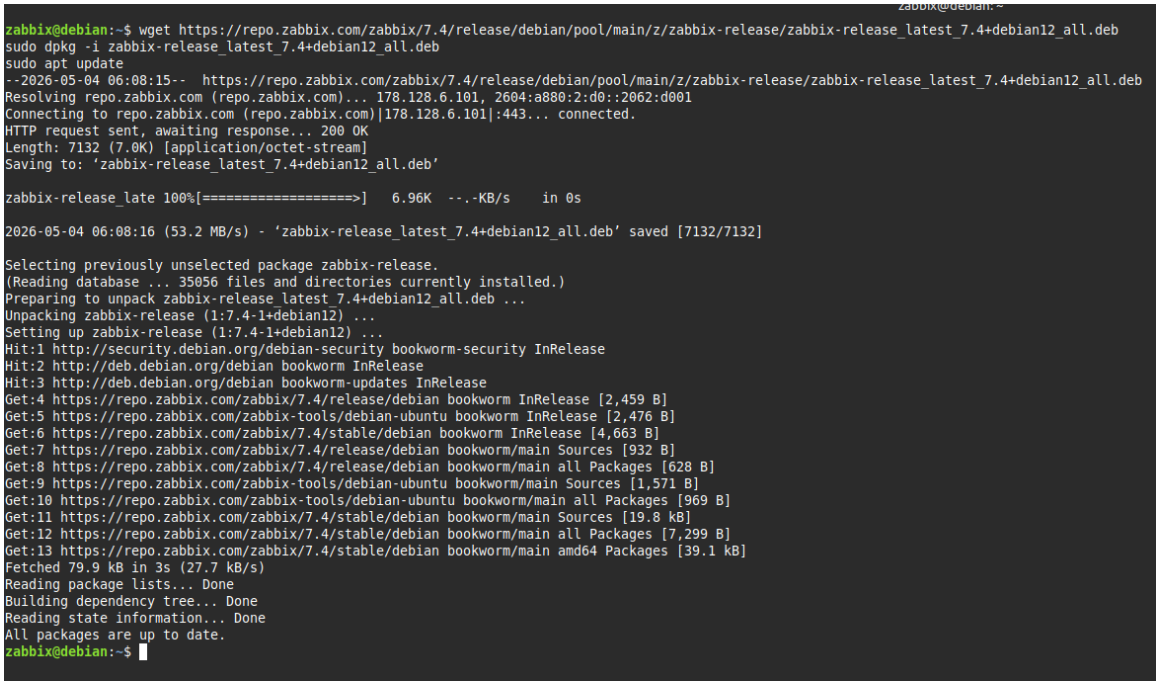


Figure 2 — Ajout et validation du dépôt officiel Zabbix

1.4 Installation des composants Zabbix

L'installation inclut le serveur Zabbix, le frontal web PHP, le module de configuration Apache, les scripts SQL d'initialisation et l'agent local.

```
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
zabbix-sql-scripts zabbix-agent -y
```

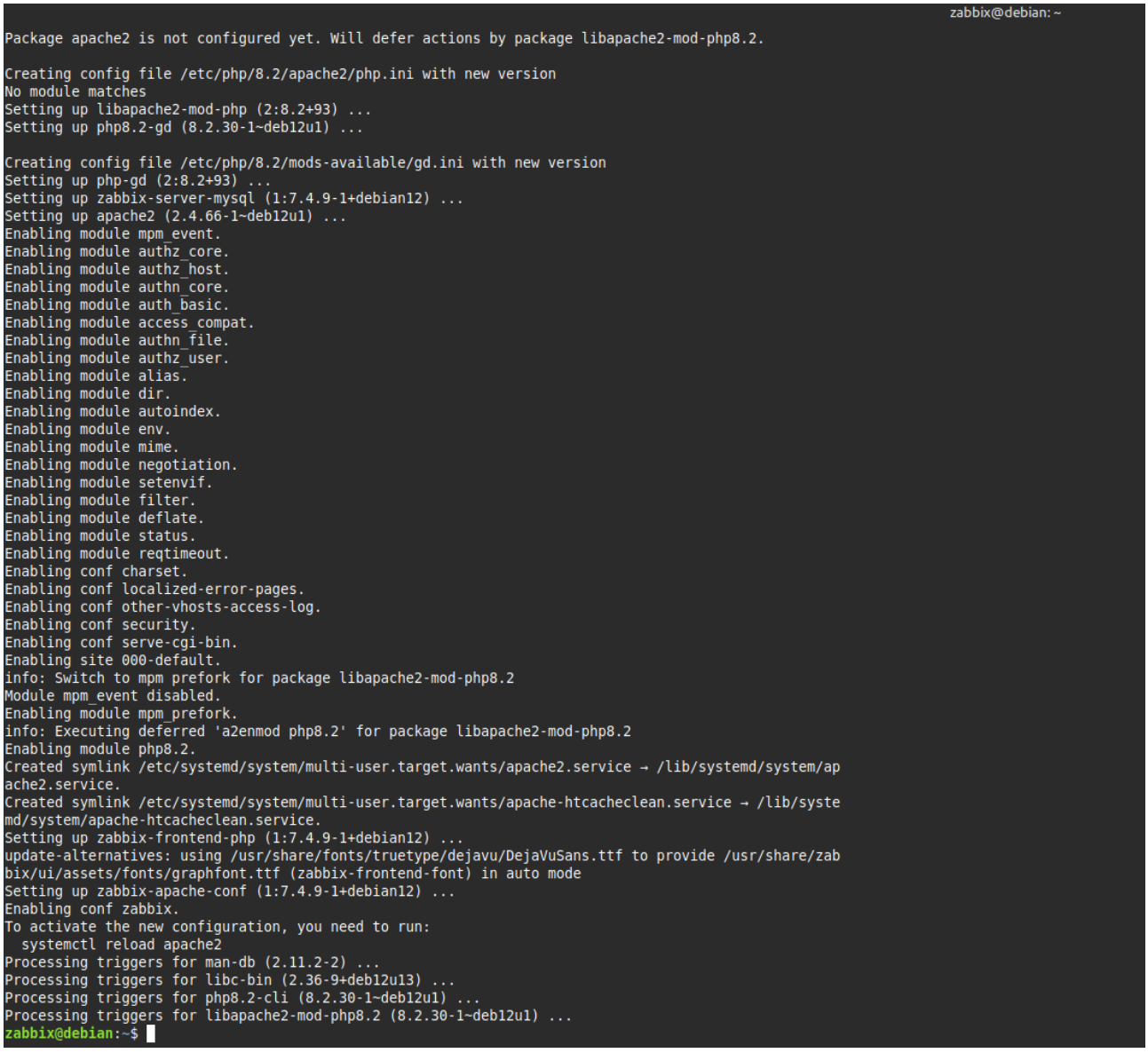


Figure 3 — Installation des paquets Zabbix

1.5 Installation et configuration de MariaDB

Zabbix utilise une base de données relationnelle pour stocker l'ensemble de ses données de supervision. MariaDB est ici utilisé comme SGBD.

```
sudo apt install mariadb-server -y
```

```
sudo systemctl start mariadb && sudo systemctl enable mariadb
```

Sécurisation de l'installation (répondre Y à toutes les questions et définir un mot de passe root robuste) :

```
sudo mysql_secure_installation
```

Création de la base de données dédiée à Zabbix et de son utilisateur :

```
sudo mysql -u root -p
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'MotDePasseForte';
GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
SET GLOBAL log_bin_trust_function_creators = 1;
FLUSH PRIVILEGES; EXIT;
```

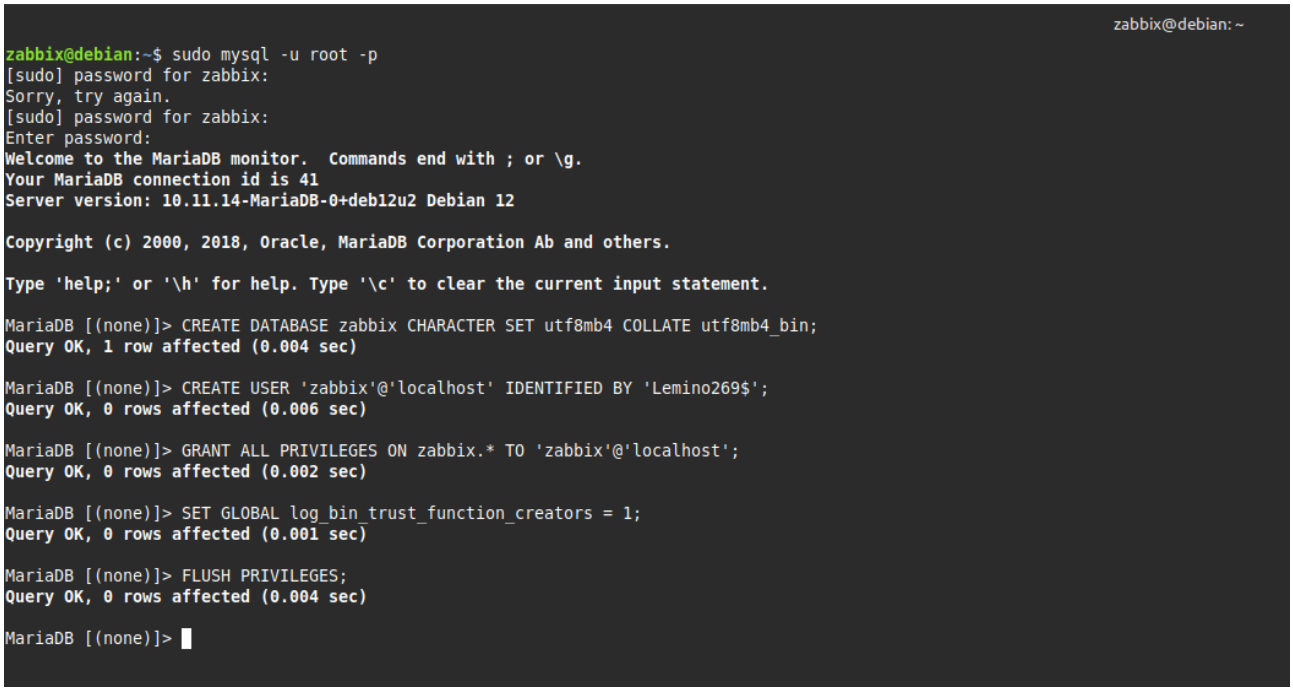


Figure 4 — Création de la base de données Zabbix dans MariaDB

1.6 Import du schéma de base de données

L'initialisation de la structure de la base de données s'effectue via le script SQL fourni par le paquet Zabbix.

```
sudo zcat /usr/share/zabbix/sql-scripts/mysql/server.sql.gz | mysql --
default-character-set=utf8mb4 -u zabbix -p zabbix
```

> *Remarque : après l'import, désactiver l'option temporaire log_bin_trust_function_creators :*
>
> ```
> sudo mysql -u root -p -e "SET GLOBAL log_bin_trust_function_creators = 0;"
> ```

Figure 5 — Import du schéma de base de données

1.7 Configuration du fichier de service Zabbix

Le fichier de configuration principal du serveur Zabbix doit être mis à jour avec le mot de passe de la base de données créée précédemment.

```
sudo nano /etc/zabbix/zabbix_server.conf
```

> *Modifier la ligne : DBPassword=<mot_de_passe_défini_précédemment>*

Figure 6 — Configuration du mot de passe de la base de données

1.8 Démarrage des services et vérification

Une fois la configuration terminée, les services sont démarrés et activés au démarrage du système.

```
sudo systemctl restart zabbix-server zabbix-agent apache2
sudo systemctl enable zabbix-server zabbix-agent apache2
sudo systemctl status zabbix-server
```

```
zabbix@debian:~$ sudo systemctl restart zabbix-server zabbix-agent apache2
sudo systemctl enable zabbix-server zabbix-agent apache2
[sudo] password for zabbix:
Synchronizing state of zabbix-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-server.service → /lib/systemd/system/zabbix-server.service.
zabbix@debian:~$
```

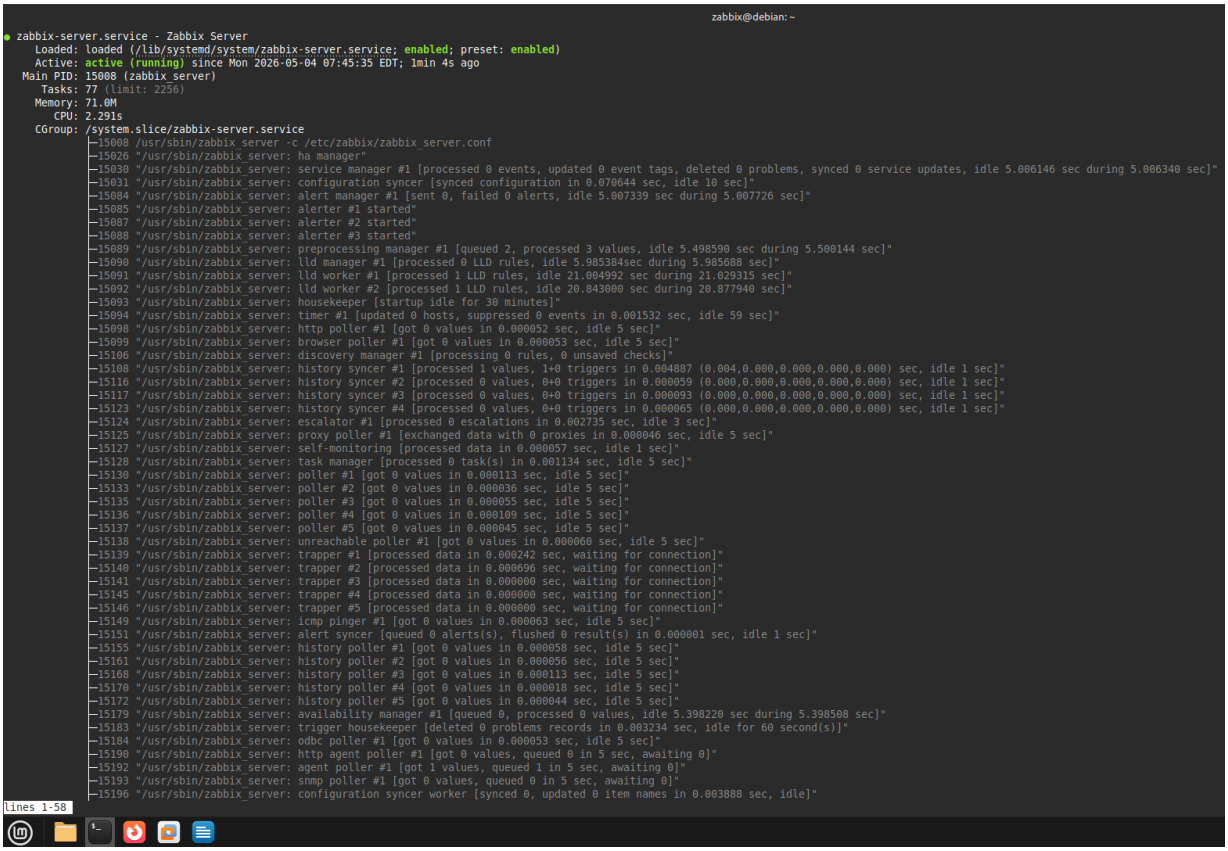


Figure 7 — Vérification du statut des services

1.9 Finalisation via l'interface web

L'assistant de configuration web est accessible à l'adresse http://192.168.122.194/zabbix. Il guide l'administrateur à travers les étapes suivantes :

- Vérification des prérequis PHP (toutes les cases doivent être validées en vert).
- Paramétrage de la connexion à la base de données (hôte : localhost, base : zabbix, utilisateur : zabbix).
- Attribution d'un nom au serveur et sélection du fuseau horaire (Europe/Paris).
- Connexion initiale avec les identifiants par défaut : Login Admin / Mot de passe zabbix.

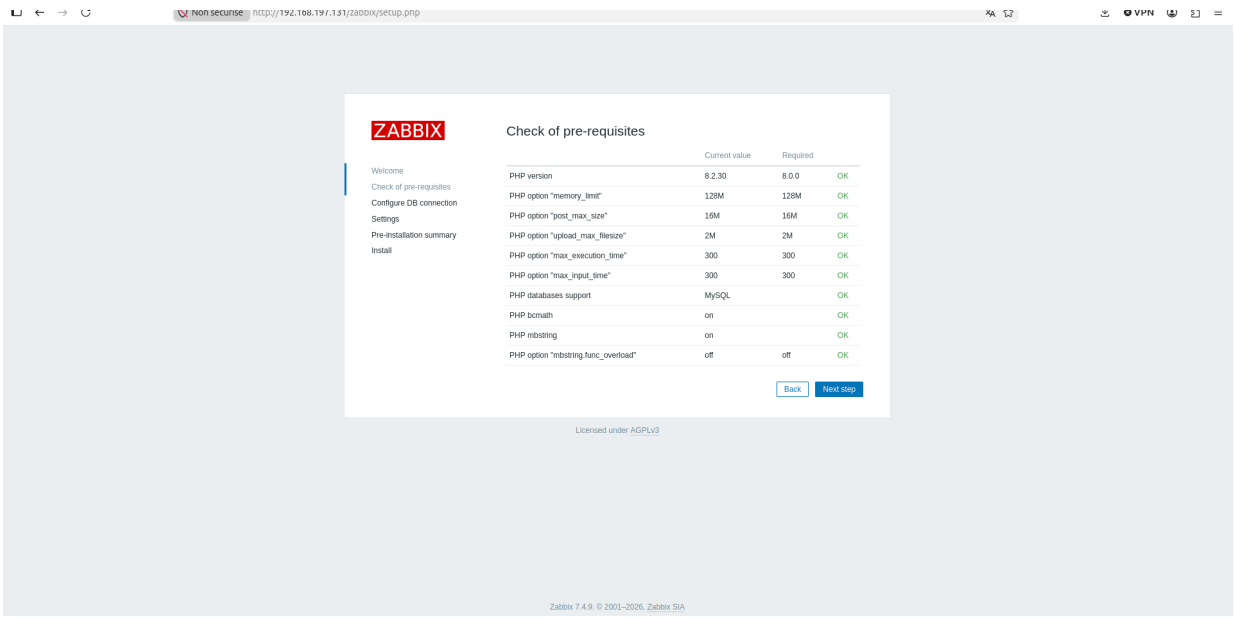


Figure 8 — Assistant de configuration web Zabbix

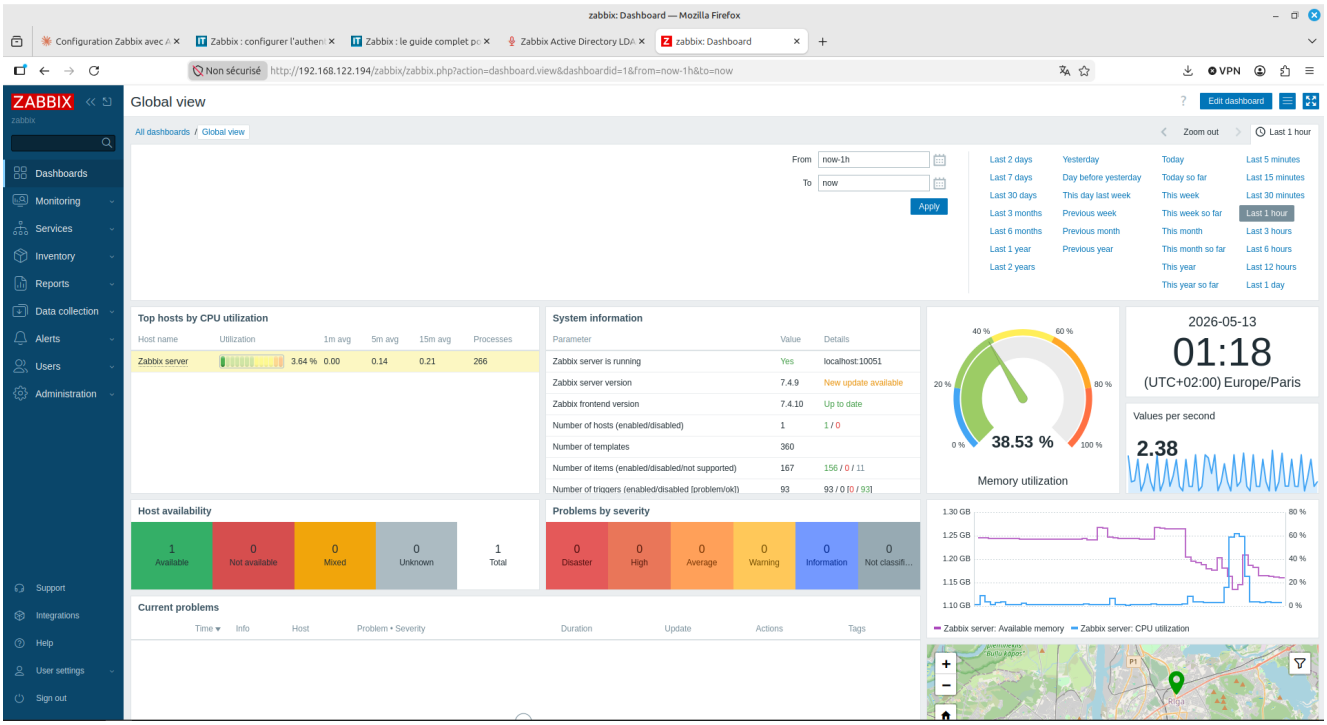


Figure 9 — Interface web Zabbix après connexion réussie

Partie 2 — Supervision du serveur Windows Server

Cette partie décrit l'installation de l'agent Zabbix sur le serveur Windows Server, sa déclaration dans l'interface de supervision et la configuration du pare-feu Windows pour permettre la communication.

2.1 Installation de l'agent Zabbix sur Windows Server

L'agent Zabbix Windows est disponible en téléchargement sur le site officiel du projet. Son installation nécessite de renseigner les informations suivantes lors de la procédure :

- Host name : nom exact du serveur Windows (SRV-DC-01 — respecter la casse).
- Zabbix server IP : adresse IP du serveur Zabbix (192.168.122.194).
- Listen port : laisser la valeur par défaut (10050).

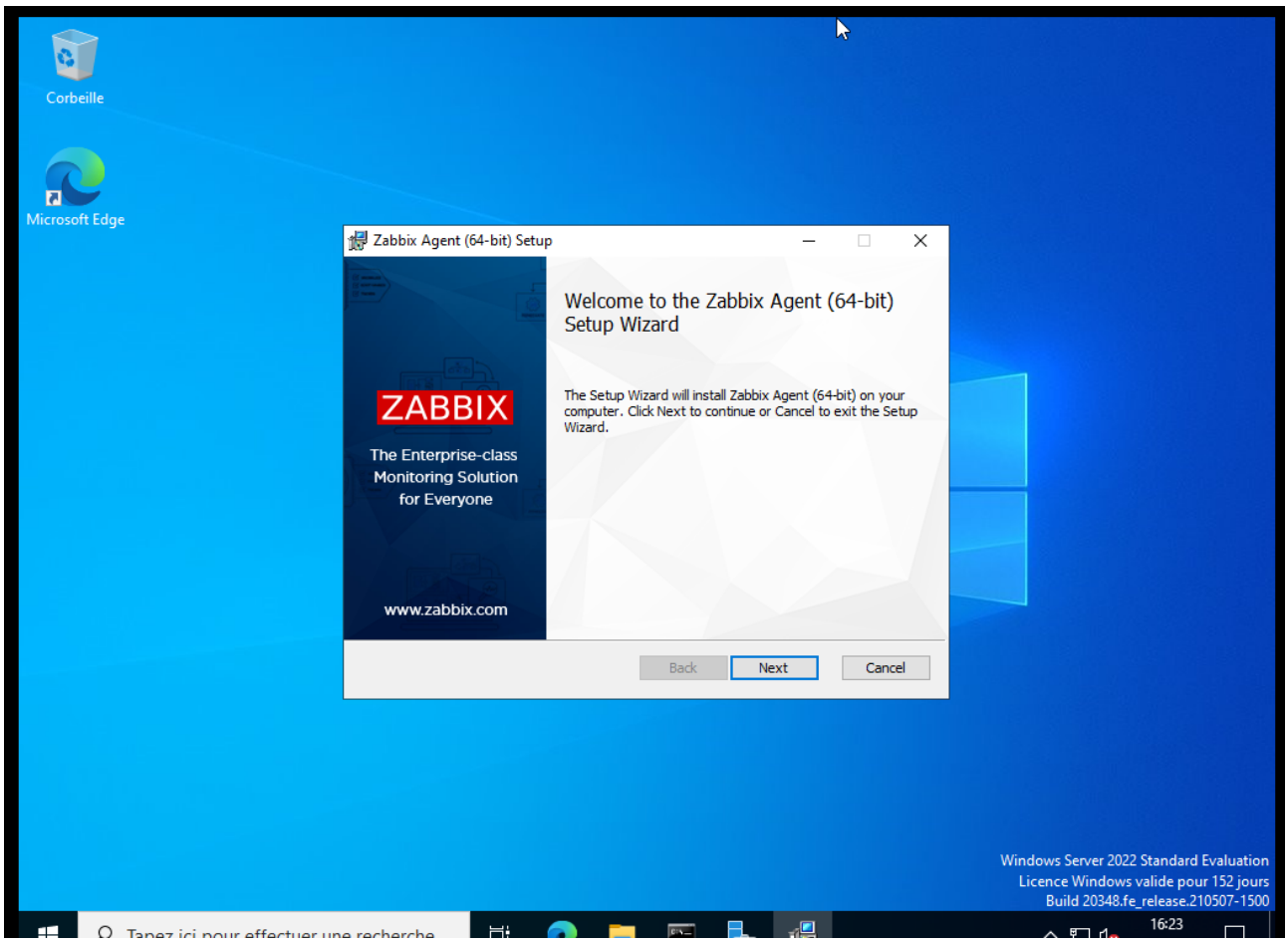


Figure 10 — Installation de l'agent Zabbix sur Windows Server

2.2 Autorisation de l'agent dans le pare-feu Windows

Windows bloque par défaut les connexions entrantes. Il est nécessaire d'ajouter une règle de pare-feu autorisant le trafic sur le port TCP 10050 utilisé par l'agent Zabbix.

Exécuter la commande suivante dans PowerShell (en tant qu'Administrateur) :

```
netsh advfirewall firewall add rule name="Zabbix" dir=in action=allow
protocol=TCP localport=10050
```

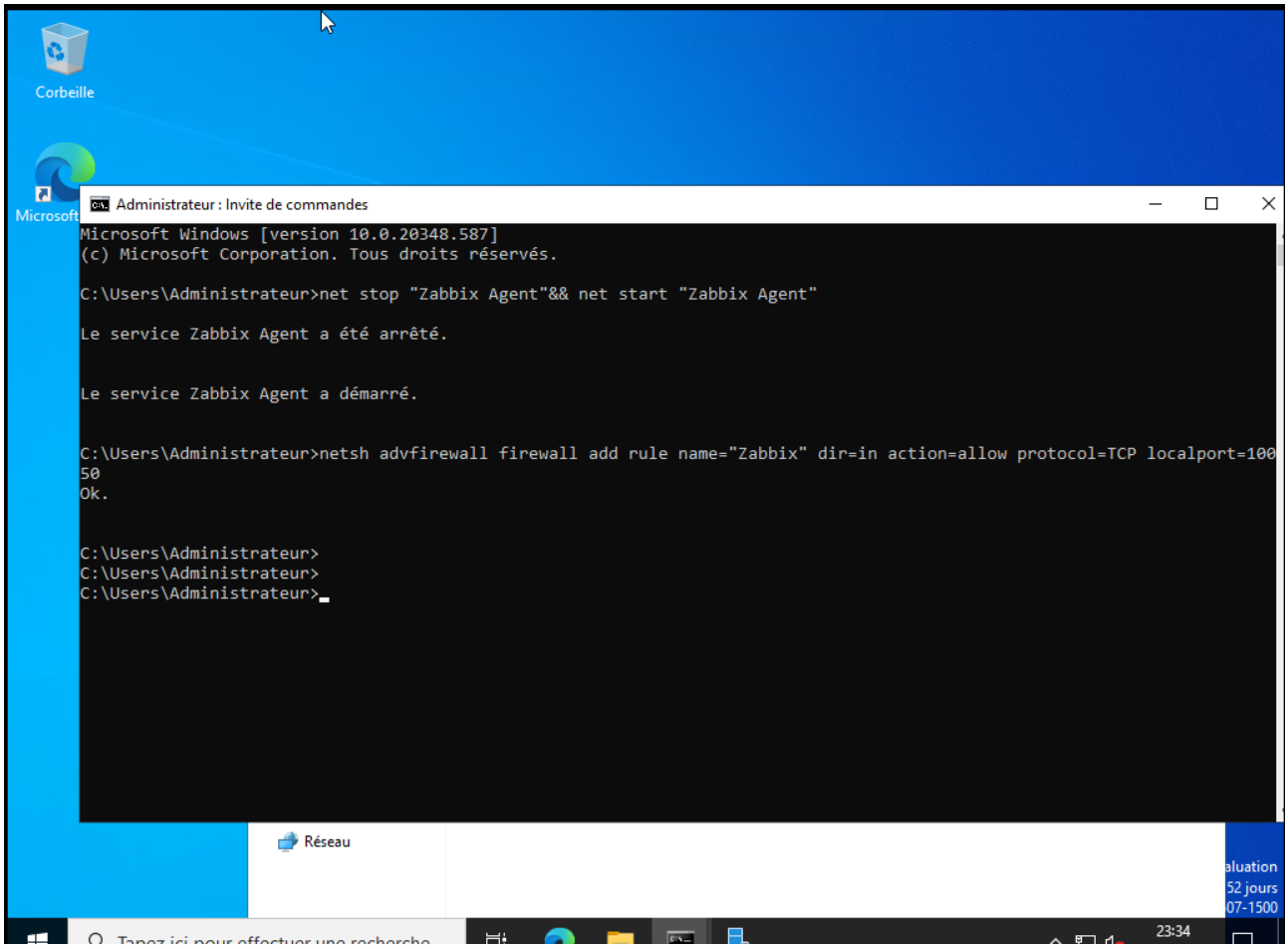


Figure 11 — Règle de pare-feu Windows pour l'agent Zabbix

2.3 Déclaration de l'hôte Windows dans Zabbix

Depuis l'interface web Zabbix, la déclaration de l'hôte s'effectue via le menu Data Collection > Hosts > Create host.

Paramètres de l'hôte

- Host name : SRV-DC-01 (respecter exactement la casse).
- Templates : Windows by Zabbix agent (ce modèle définit automatiquement les métriques à surveiller).
- Host groups : sélectionner un groupe existant ou créer un nouveau groupe (ex. : Serveurs Windows).
- Interfaces : ajouter une interface de type Agent avec l'IP 192.168.122.235 et le port 10050.

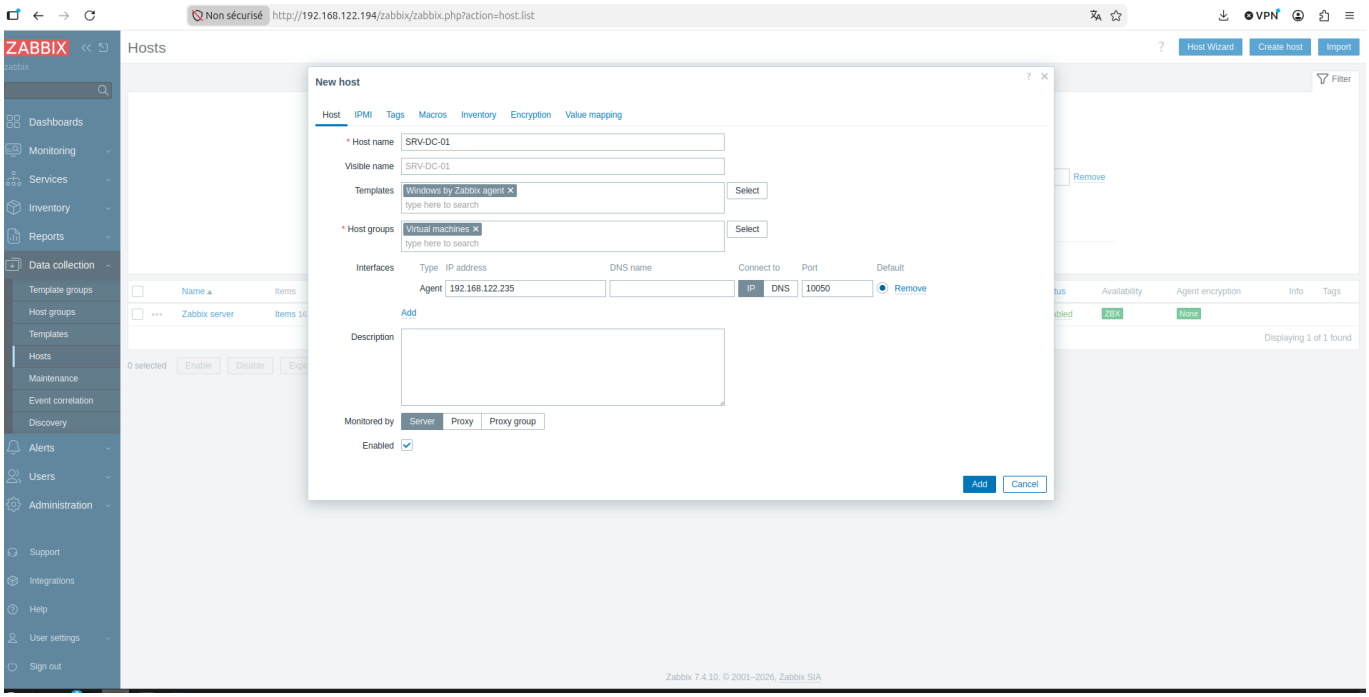


Figure 12 — Déclaration de l'hôte SRV-DC-01 dans Zabbix

Validation de la connexion

Après l'ajout, patienter une à deux minutes puis actualiser la page. L'icône ZBX verte indique que la communication entre le serveur Zabbix et l'agent Windows est opérationnelle et que la supervision a démarré.

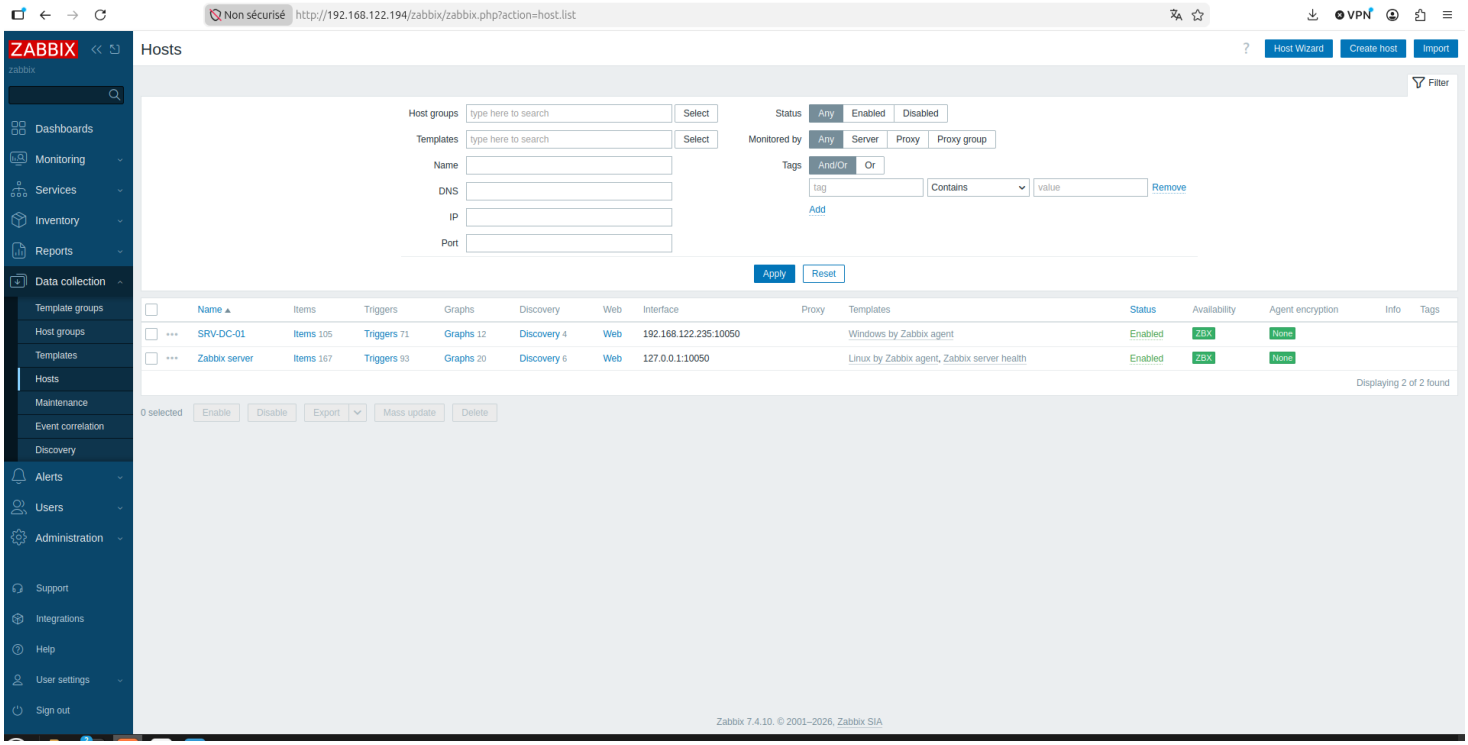


Figure 14 — Icône ZBX verte confirmant la supervision active

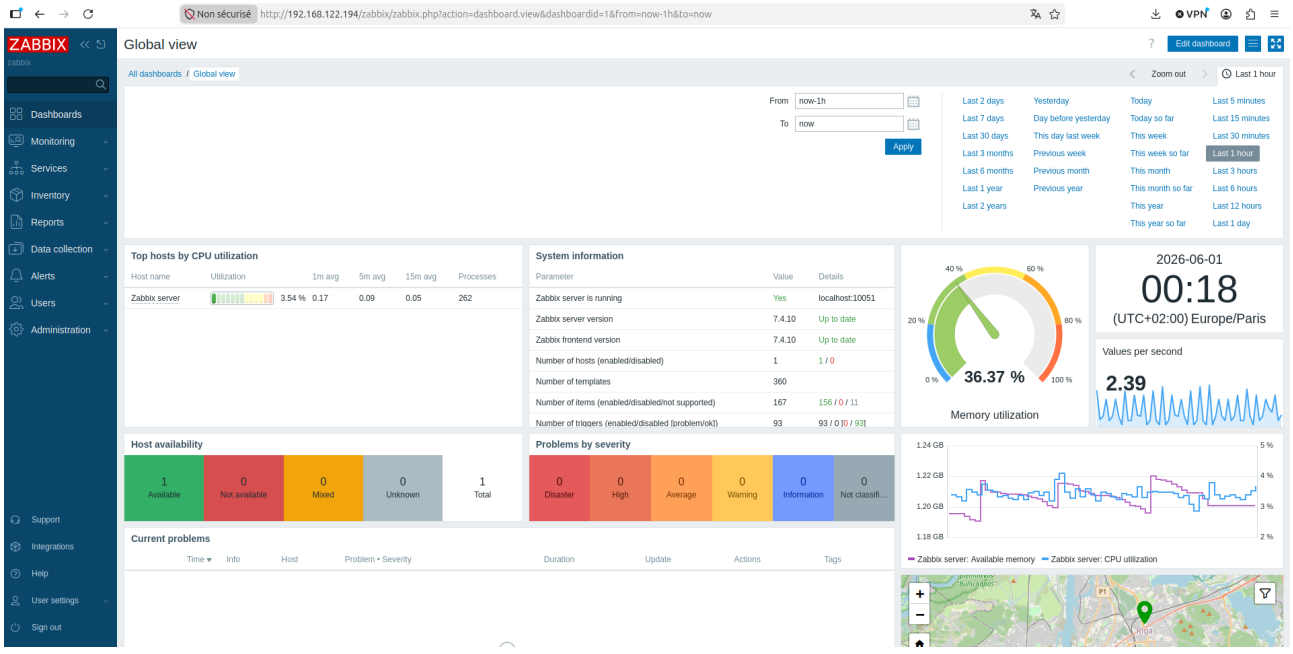
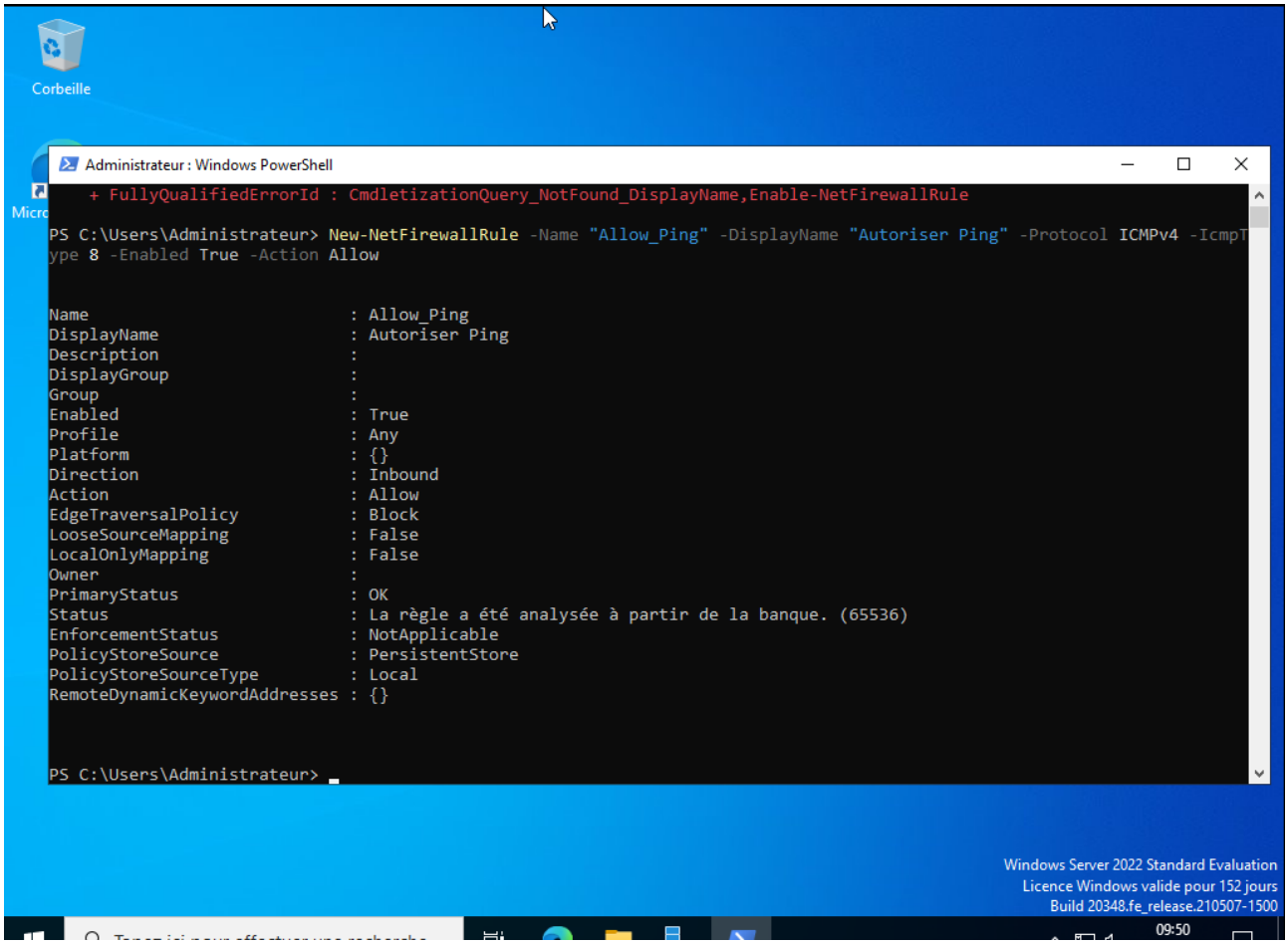
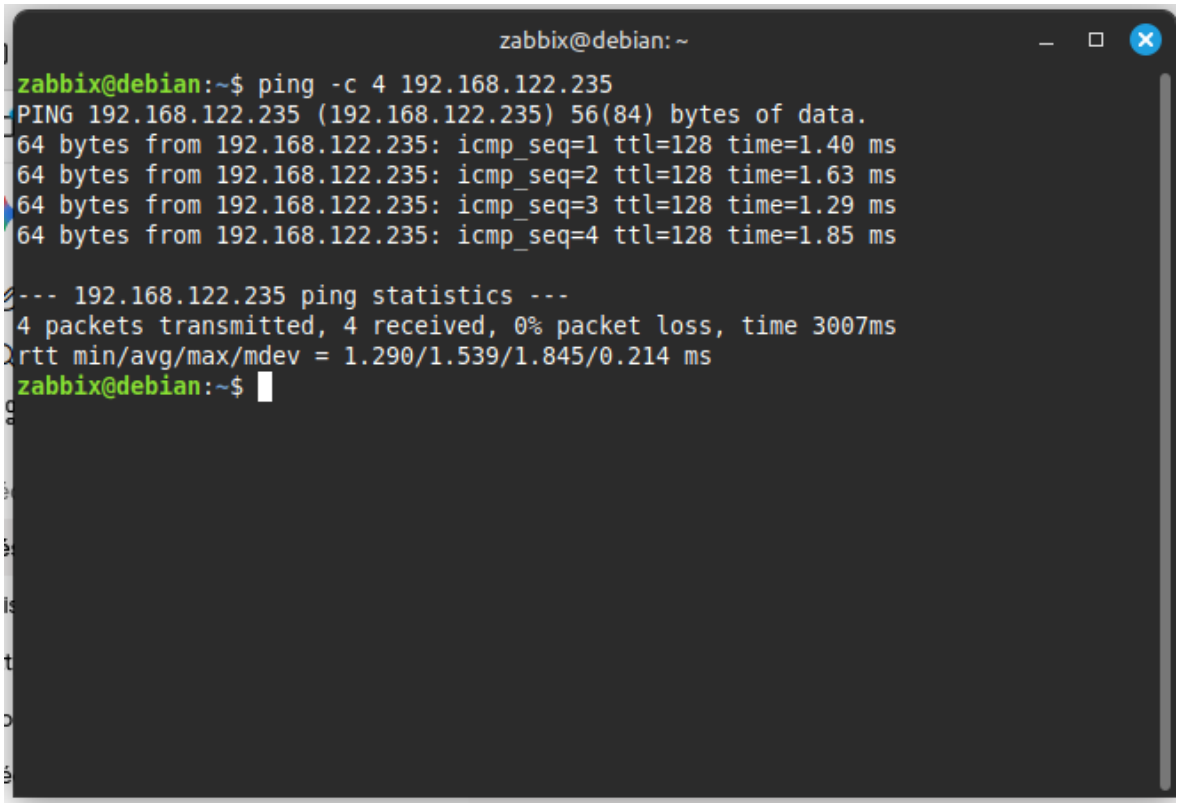


Figure 15 — Vue de la liste des hôtes supervisés


Corbeille
Administrateur : Windows PowerShell
+ FullyQualifiedErrorId : CmdletizationQuery_NotFound_DisplayName,Enable-NetFirewallRule
PS C:\Users\Administrateur> New-NetFirewallRule -Name "Allow_Ping" -DisplayName "Autoriser Ping" -Protocol ICMPv4 -IcmpType 8 -Enabled True -Action Allow
Name : Allow_Ping
DisplayName : Autoriser Ping
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : La règle a été analysée à partir de la banque. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PS C:\Users\Administrateur>
Windows Server 2022 Standard Evaluation
Licence Windows valide pour 152 jours
Build 20348.fe_release.210507-1500
09:50


zabbix@debian: ~
zabbix@debian:~$ ping -c 4 192.168.122.235
PING 192.168.122.235 (192.168.122.235) 56(84) bytes of data.
64 bytes from 192.168.122.235: icmp_seq=1 ttl=128 time=1.40 ms
64 bytes from 192.168.122.235: icmp_seq=2 ttl=128 time=1.63 ms
64 bytes from 192.168.122.235: icmp_seq=3 ttl=128 time=1.29 ms
64 bytes from 192.168.122.235: icmp_seq=4 ttl=128 time=1.85 ms
--- 192.168.122.235 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.290/1.539/1.845/0.214 ms
zabbix@debian:~$

Partie 3 — Déploiement de l'Active Directory

Avant de configurer l'authentification LDAP dans Zabbix, il est nécessaire de disposer d'un domaine Active Directory opérationnel. Cette partie décrit la promotion du serveur Windows en contrôleur de domaine et la création des objets nécessaires.

3.1 Installation du rôle AD DS

Le rôle Active Directory Domain Services (AD DS) est installé via PowerShell (en tant qu'Administrateur) :

```
Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
```

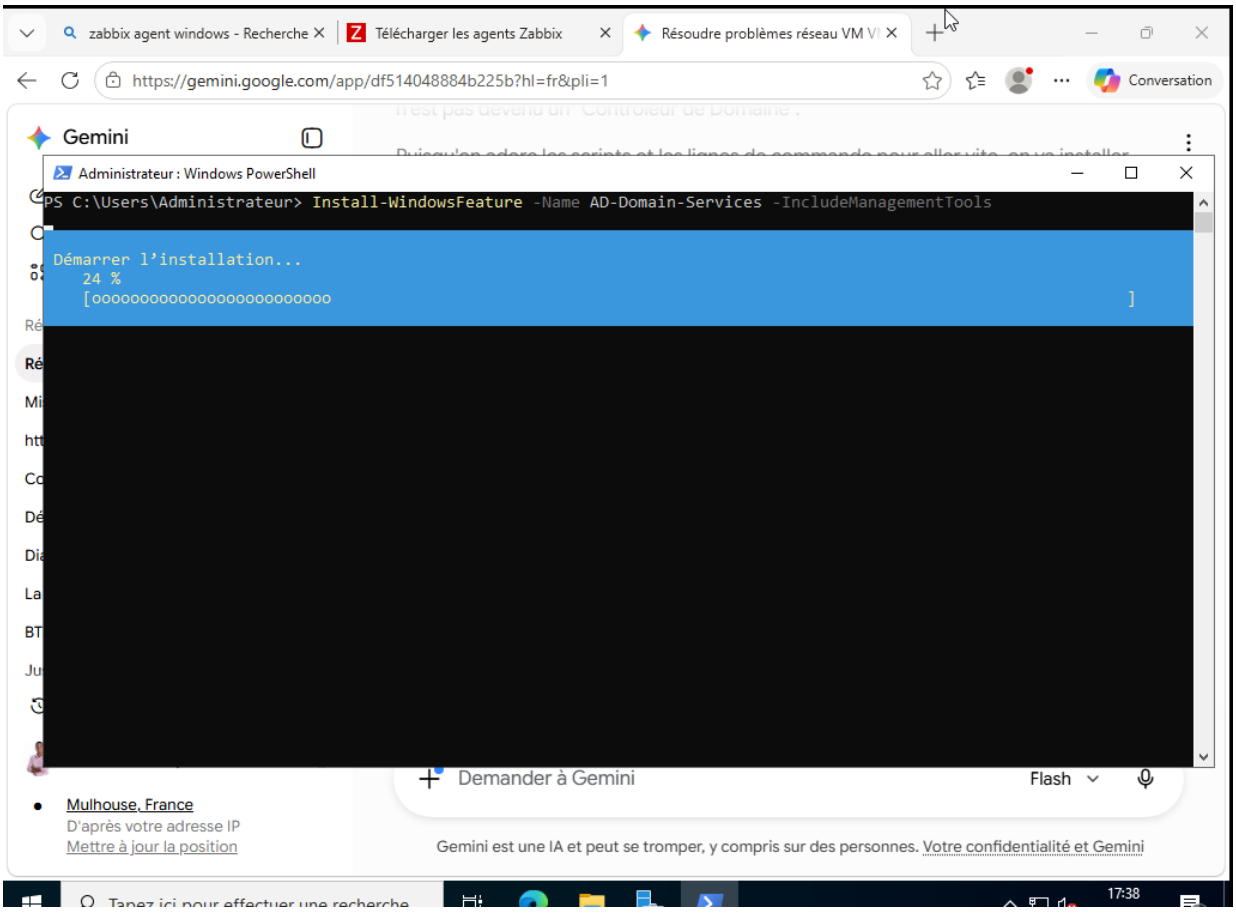


Figure 16 — Installation du rôle AD DS via PowerShell

3.2 Création du domaine rayane.local

Une fois le rôle installé, la commande suivante crée la forêt Active Directory et promeut le serveur en contrôleur de domaine. Le serveur redémarre automatiquement à l'issue de l'opération.

```
Install-ADDSForest -DomainName "rayane.local" -SafeModeAdministratorPassword
(ConvertTo-SecureString "P@ssword2026!" -AsPlainText -Force) -Force
```

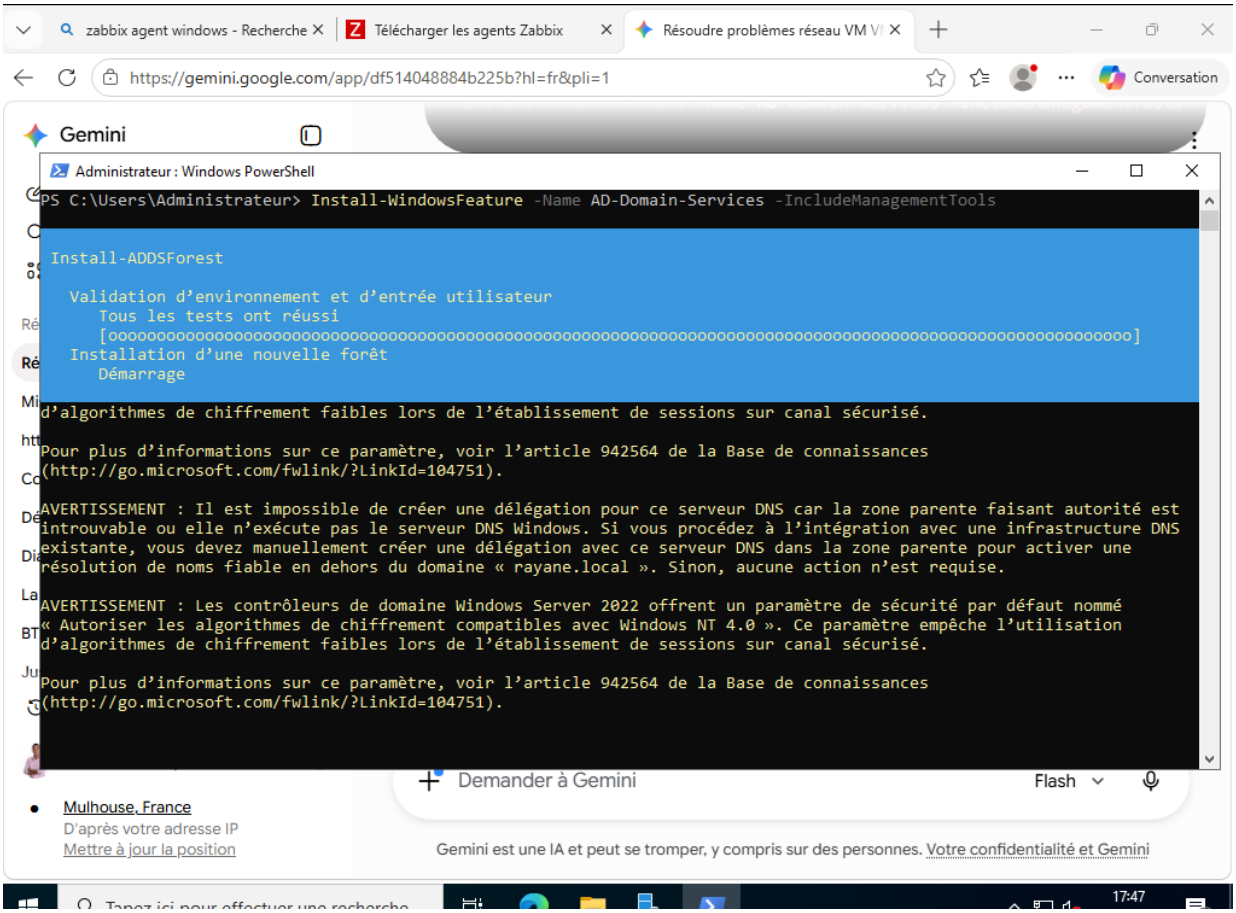


Figure 17 — Promotion du serveur en contrôleur de domaine

3.3 Création du compte de liaison Zabbix

Après le redémarrage du serveur (l'identifiant devient Rayane\Administrateur), un compte de service dédié est créé dans l'annuaire. Ce compte sera utilisé par Zabbix pour interroger l'annuaire LDAP.

```
New-ADOrganizationalUnit -Name "Supervision"
New-ADUser -Name "zabbix-auth" -SamAccountName "zabbix-auth" -Path "OU=Supervision,DC=rayane,DC=local" -AccountPassword (ConvertTo-SecureString "P@ssword2026!" -AsPlainText -Force) -Enabled $true
Set-ADUser -Identity "zabbix-auth" -PasswordNeverExpires $true
```

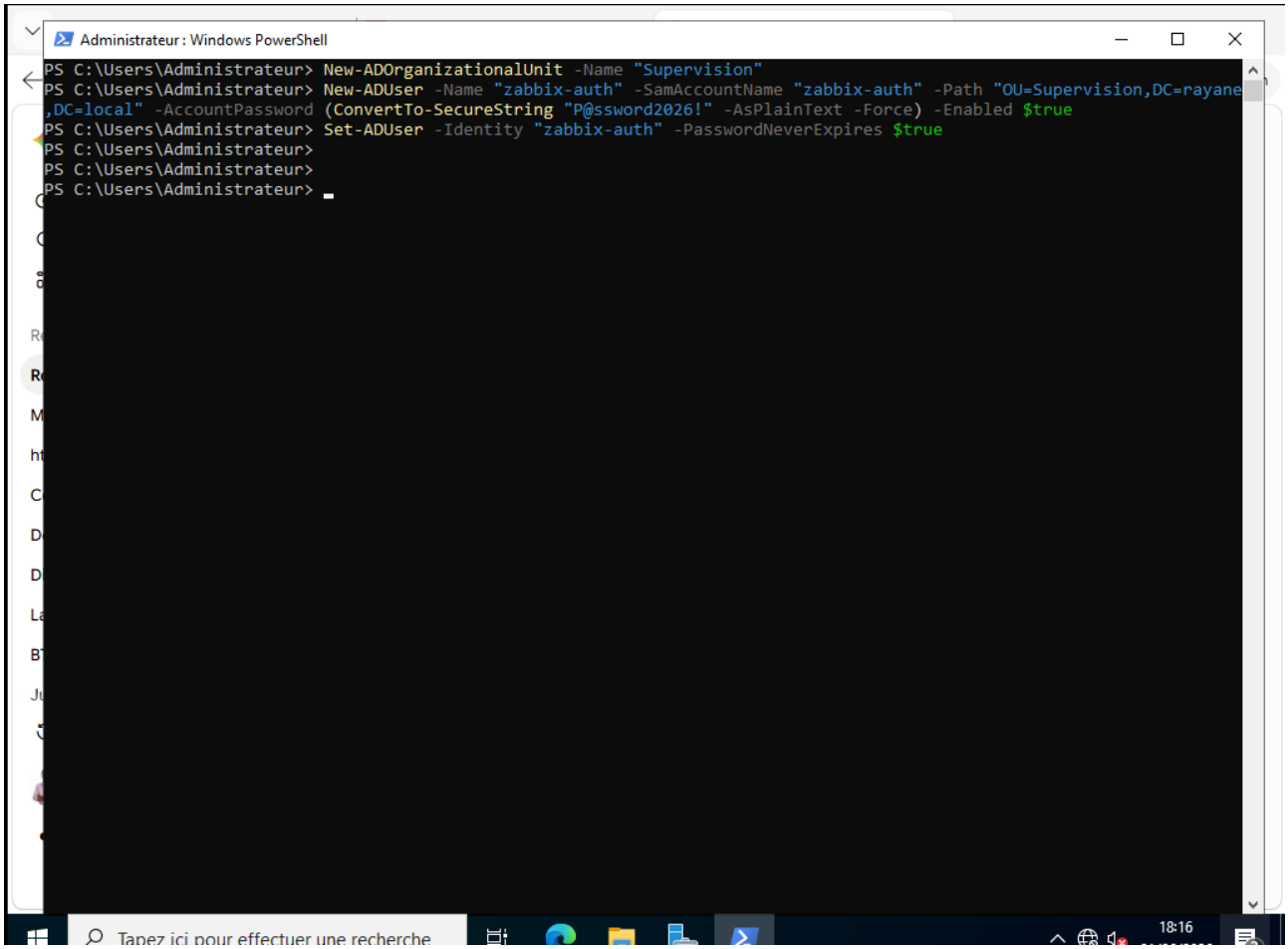


Figure 18 — Création du compte de liaison zabbix-auth dans l'OU Supervision

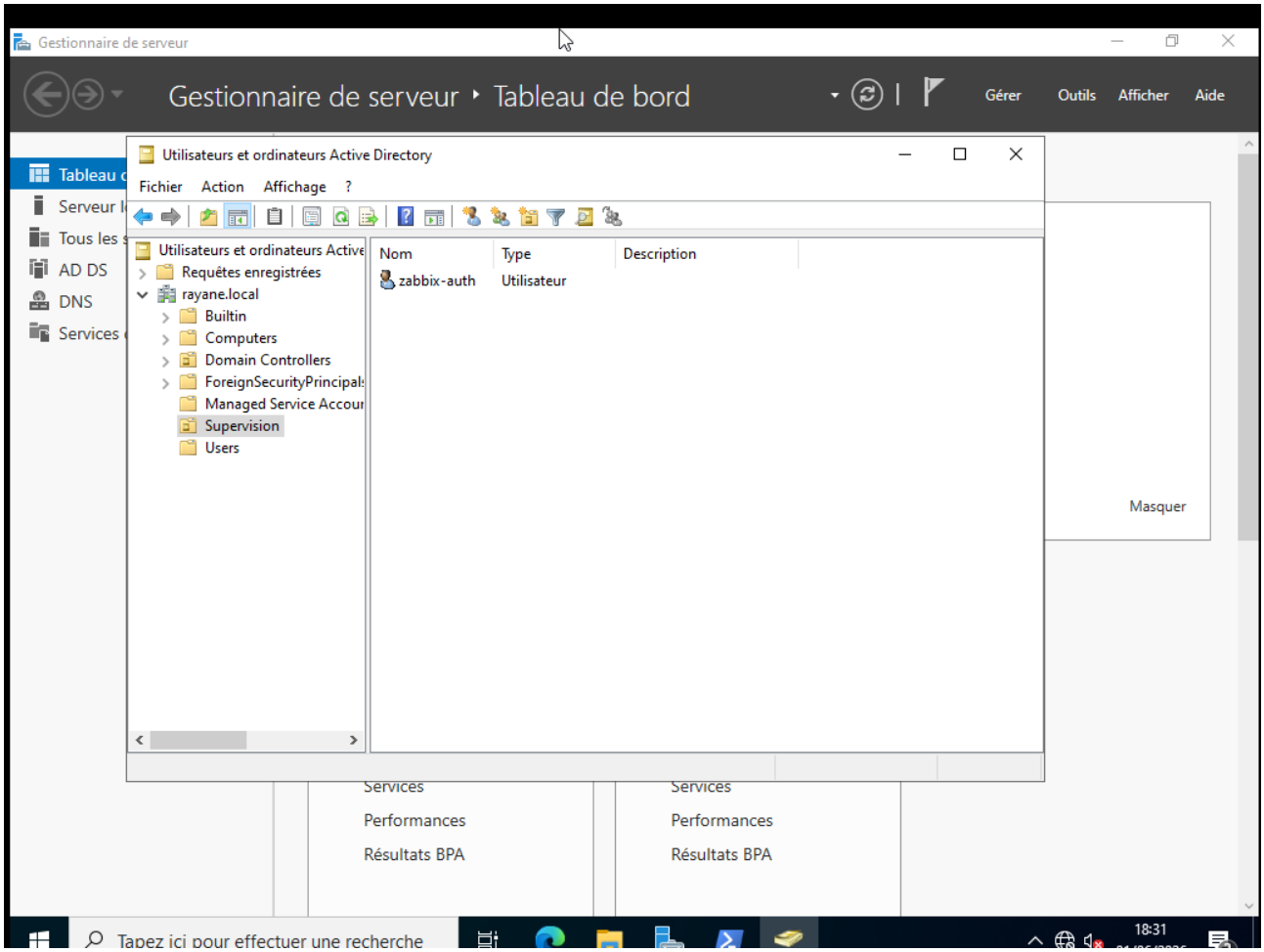


Figure 19 — Vérification de la création du compte dans l'annuaire

Partie 4 — Configuration de l'authentification LDAP

Cette partie décrit la configuration de l'authentification LDAP dans Zabbix, permettant aux utilisateurs du domaine Active Directory de se connecter à l'interface web de supervision.

4.1 Accès aux paramètres d'authentification

Dans l'interface web Zabbix, accéder au menu Administration (ou Users selon la version) > Authentication, puis sélectionner l'onglet LDAP settings et activer la case Enable LDAP authentication.

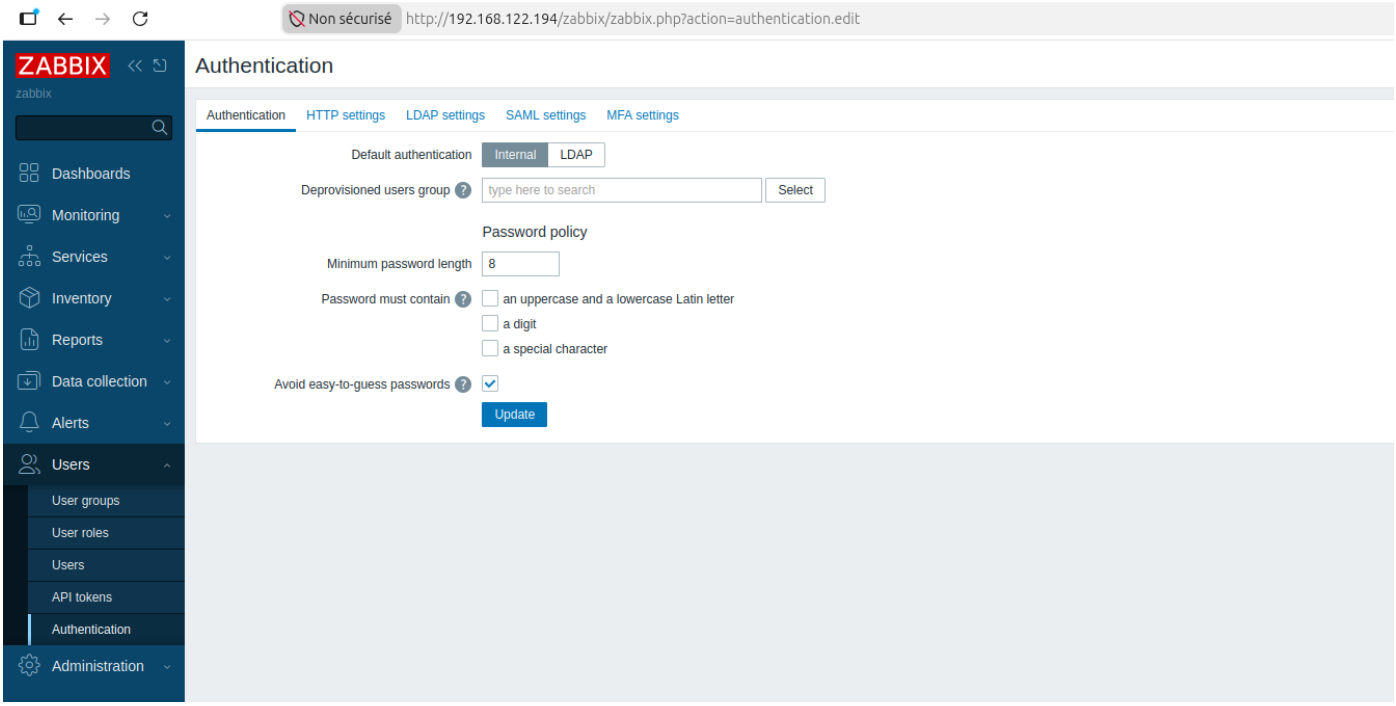


Figure 20 — Activation de l'authentification LDAP dans Zabbix

4.2 Configuration du serveur Active Directory

Cliquer sur le bouton Add et renseigner les paramètres de connexion à l'annuaire :

- Name : Active Directory Rayane
- Host : 192.168.122.235 (adresse IP du contrôleur de domaine)
- Port : 389 (port LDAP standard)
- Base DN : dc=rayane,dc=local
- Search attribute : sAMAccountName (identifiant Windows — respecter la casse)
- Bind DN : zabbix-auth@rayane.local (compte de liaison créé précédemment)
- Bind password : mot de passe du compte de liaison

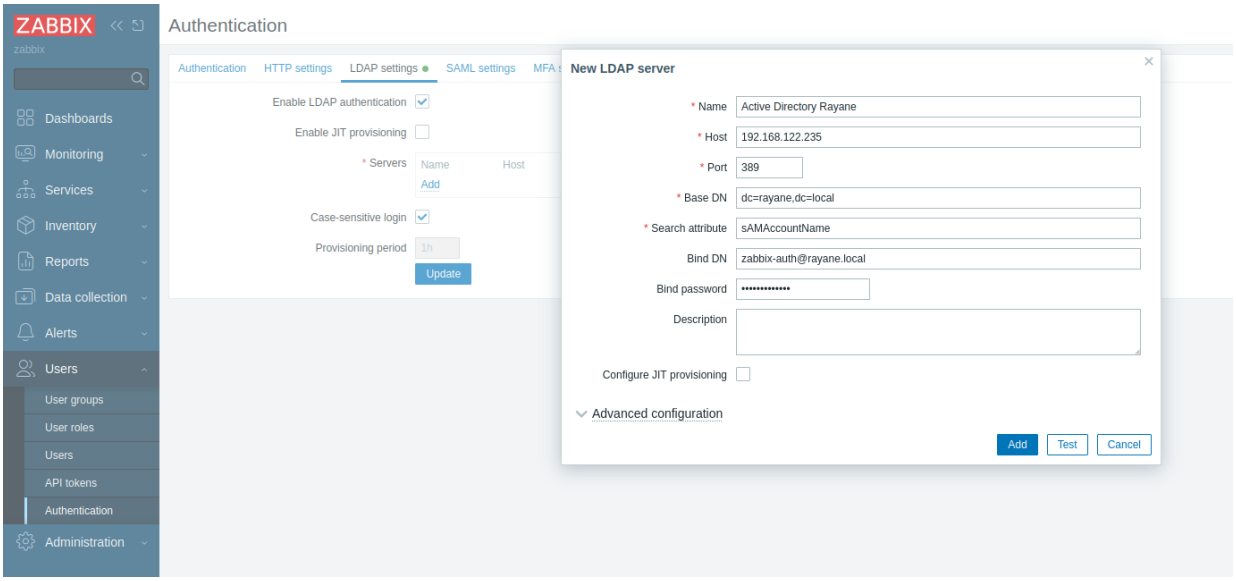


Figure 21 — Paramètres de connexion LDAP au serveur Active Directory

4.3 Test et validation de la connexion LDAP

La section Test authentication en bas du formulaire permet de valider la configuration en testant une authentification avec un compte du domaine. Un bandeau vert confirme le succès de la connexion. Cliquer sur Add pour enregistrer la configuration.

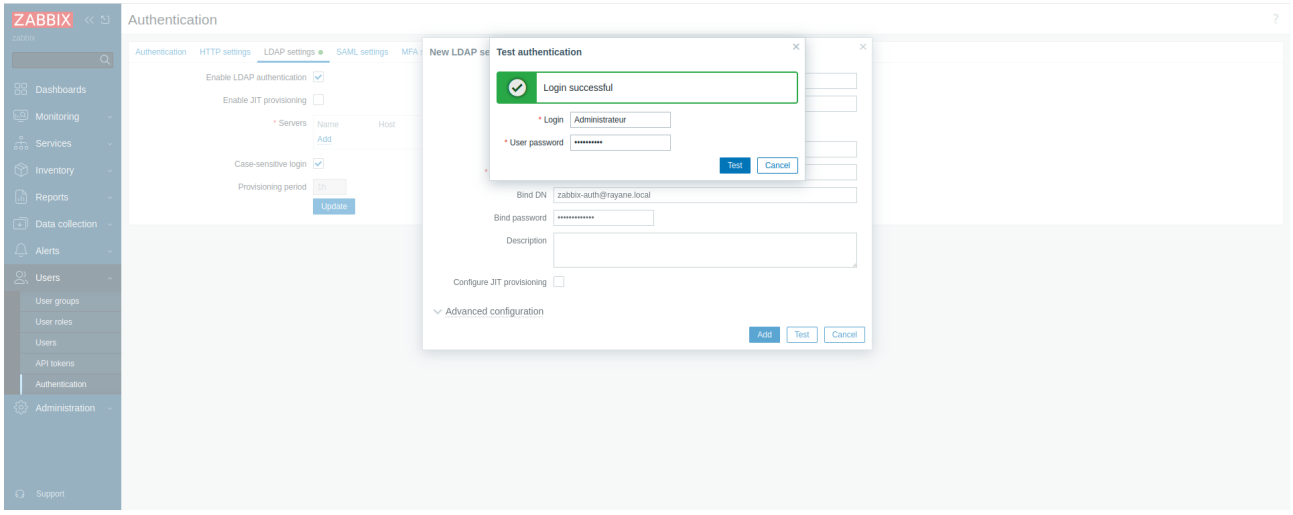


Figure 22 — Test de l'authentification LDAP réussi

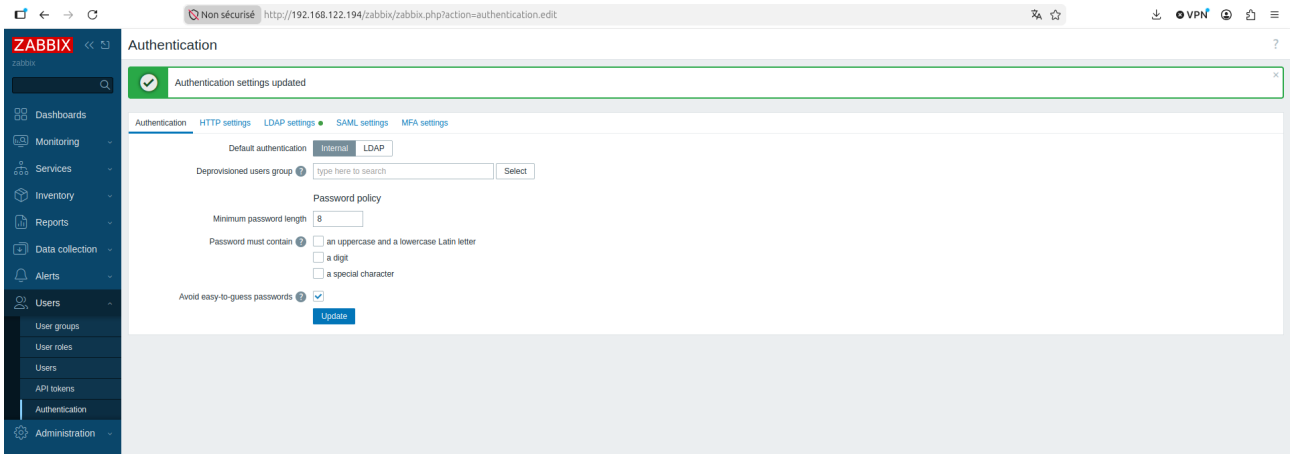


Figure 23 — Connexion LDAP validée

Partie 5 — Sécurisation avec LDAPS et Autorité de Certification

LDAP standard transmet les données, y compris les mots de passe, en clair sur le réseau. La mise en place de LDAPS (LDAP over SSL/TLS) chiffre ces échanges et garantit la confidentialité des authentifications. Cette partie décrit le déploiement d'une Autorité de Certification interne (PKI) et la configuration de LDAPS.

5.1 Préparation du serveur SRV-PKI-01

Configuration IP

Le serveur SRV-PKI-01 doit être configuré avec une adresse IP statique et pointer vers le contrôleur de domaine pour la résolution DNS, condition obligatoire pour rejoindre le domaine.

- Adresse IP : 192.168.122.236
- Masque de sous-réseau : 255.255.255.0
- Serveur DNS préféré : 192.168.122.235 (SRV-DC-01)

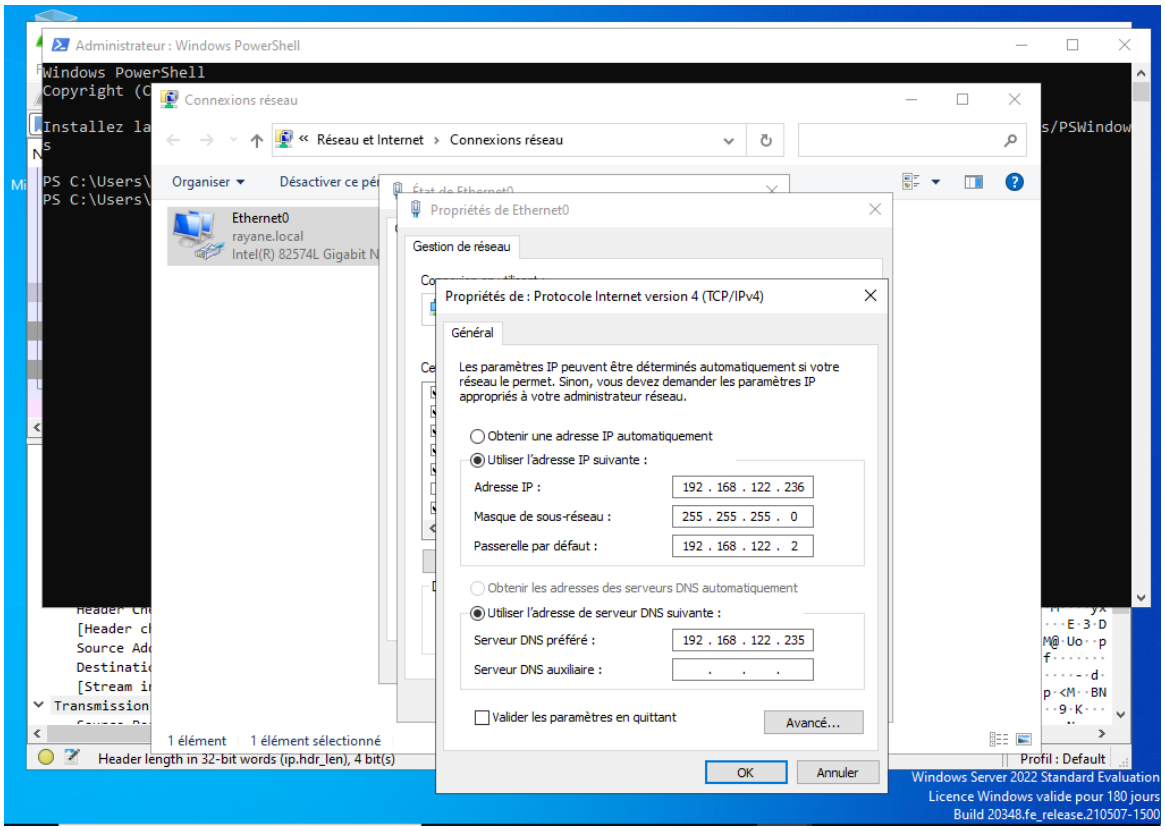


Figure 24 — Configuration IP du serveur SRV-PKI-01

Jonction au domaine

Depuis le Gestionnaire de serveur, dans Serveur local > Groupe de travail, cliquer sur Modifier, cocher Domaine et saisir rayane.local. Renseigner les identifiants de l'administrateur du domaine. Le serveur redémarre après jonction.

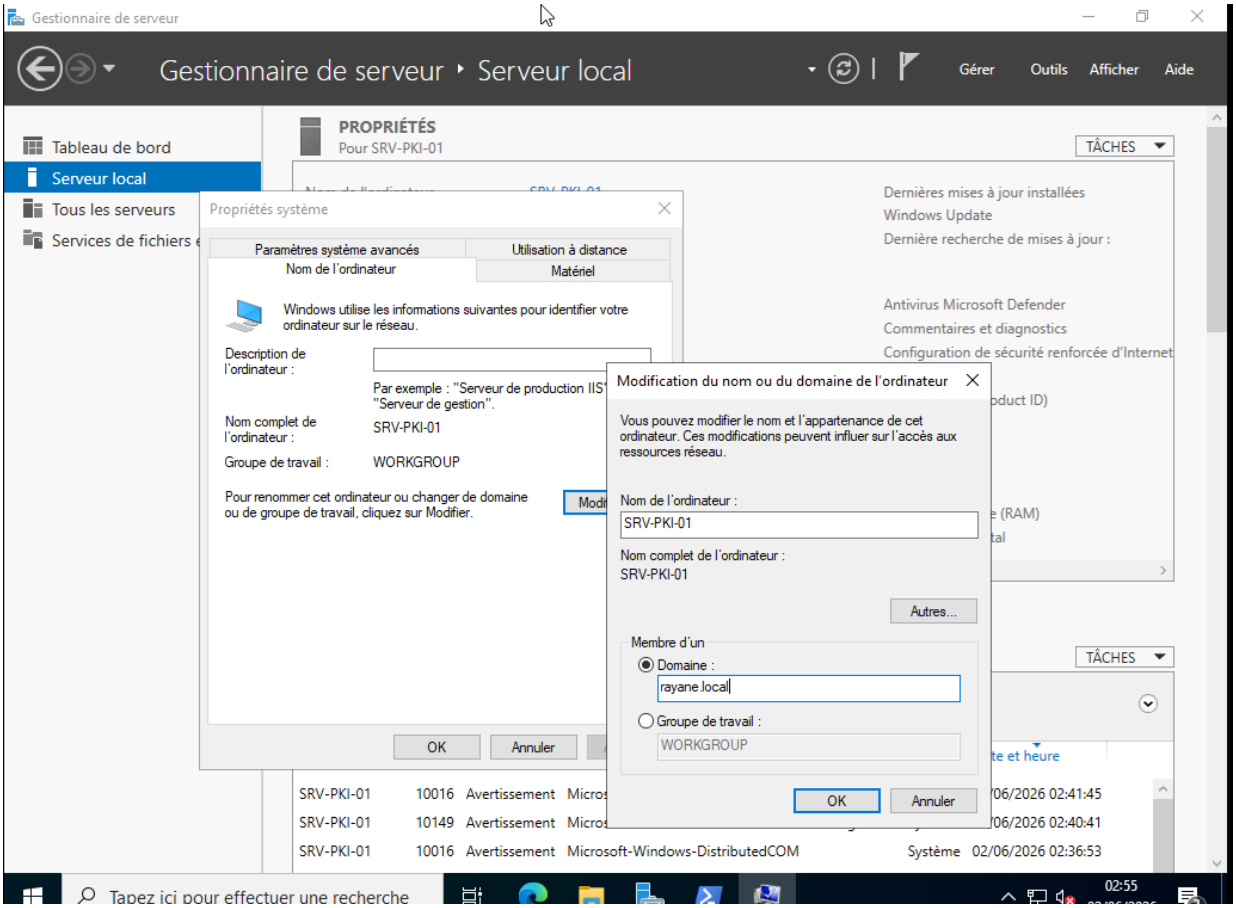


Figure 25 — Jonction du serveur SRV-PKI-01 au domaine rayane.local

5.2 Installation du rôle ADCS

L'installation des Services de certificats Active Directory (AD CS) s'effectue depuis le Gestionnaire de serveur via Gérer > Ajouter des rôles et fonctionnalités. Sélectionner Services de certificats Active Directory puis valider l'ajout des fonctionnalités.

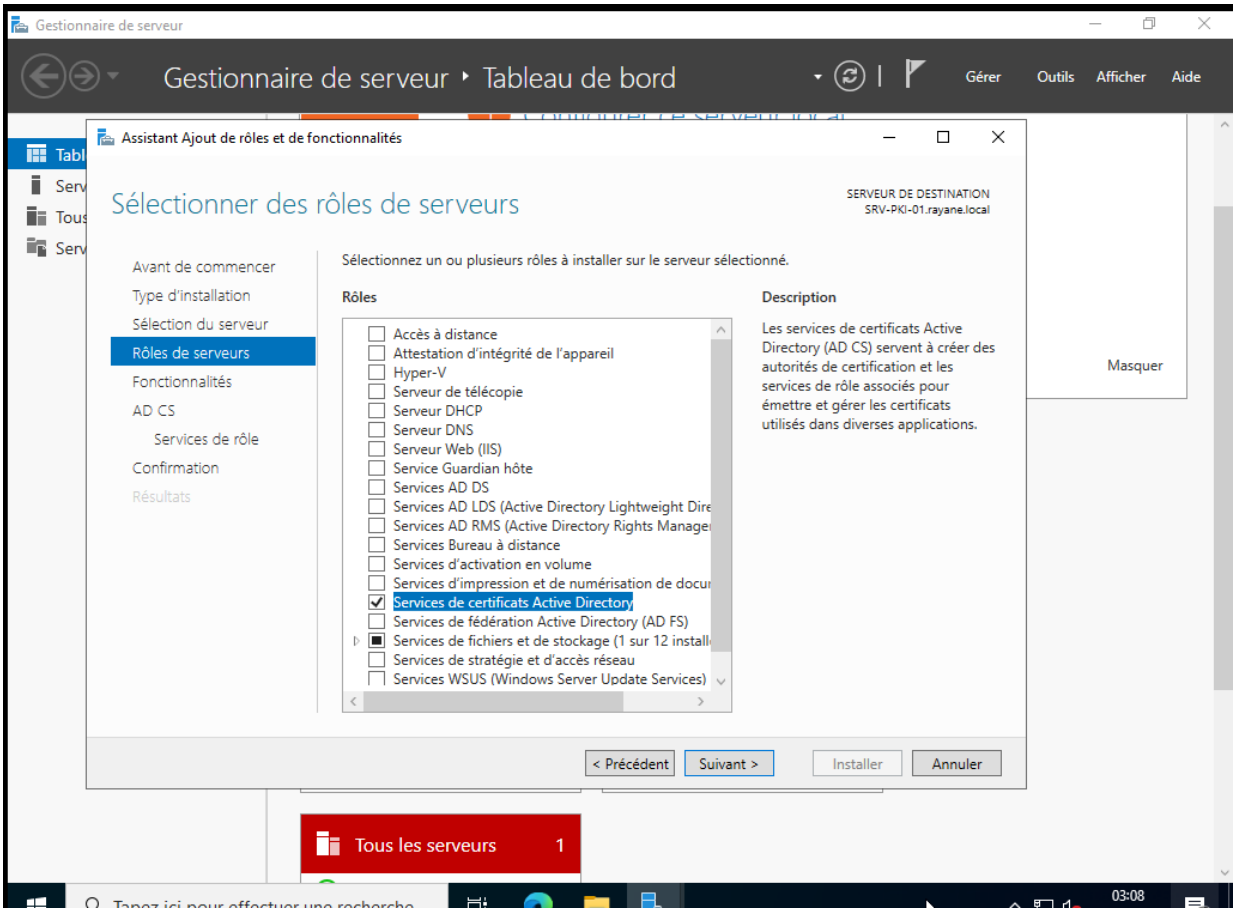


Figure 26 — Installation du rôle AD CS

5.3 Configuration de l'Autorité de Certification

À l'issue de l'installation, une notification apparaît dans le Gestionnaire de serveur pour finaliser la configuration. Renseigner les paramètres suivants :

- Type d'autorité : Autorité de certification d'entreprise (Enterprise CA)
- Type de CA : Autorité de certification racine (Root CA)
- Clé privée : Créer une nouvelle clé privée
- Chiffrement : SHA256 / 2048 bits (valeurs par défaut)
- Nom de la CA : rayane-SRV-PKI-01-CA (généré automatiquement)
- Période de validité : 5 ans

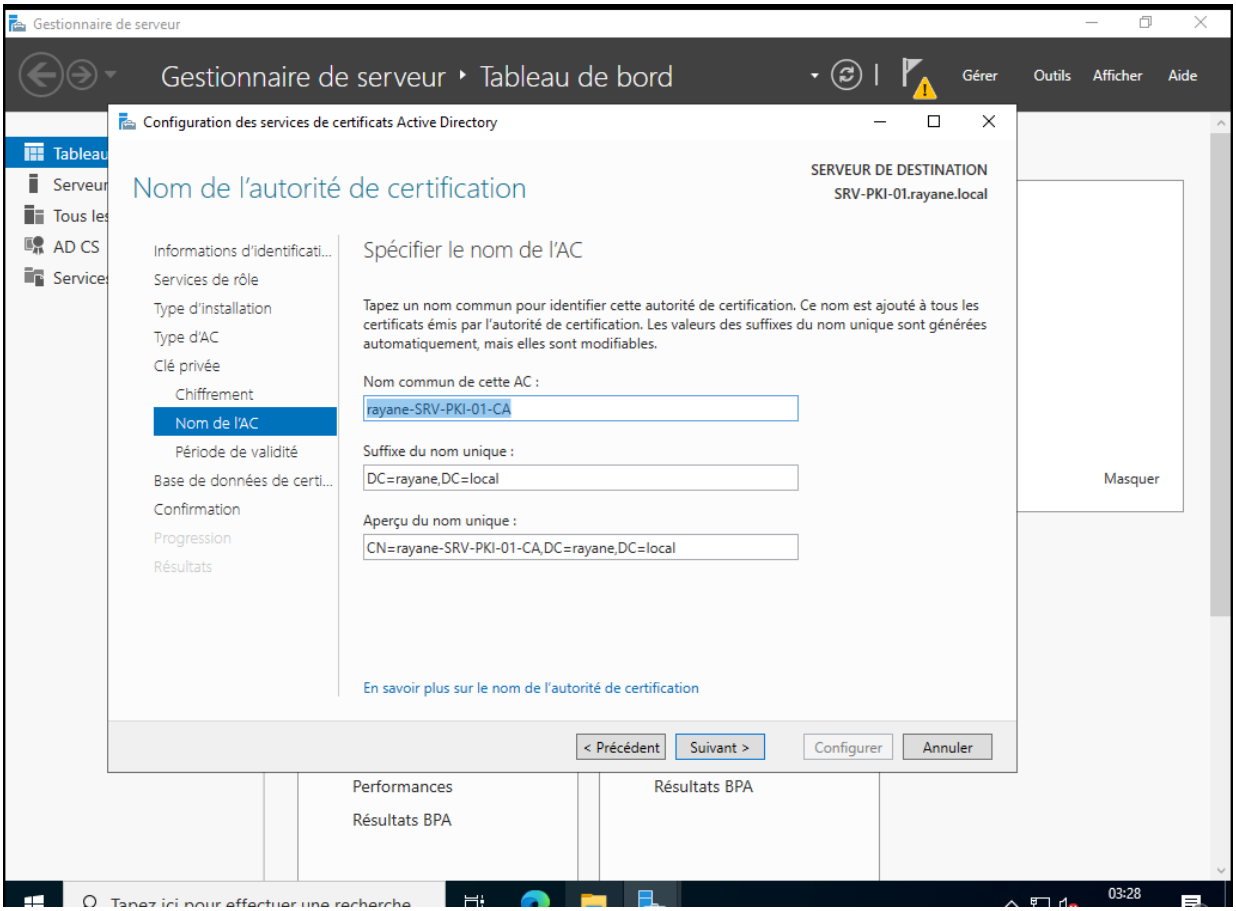


Figure 27 — Configuration de l'Autorité de Certification racine

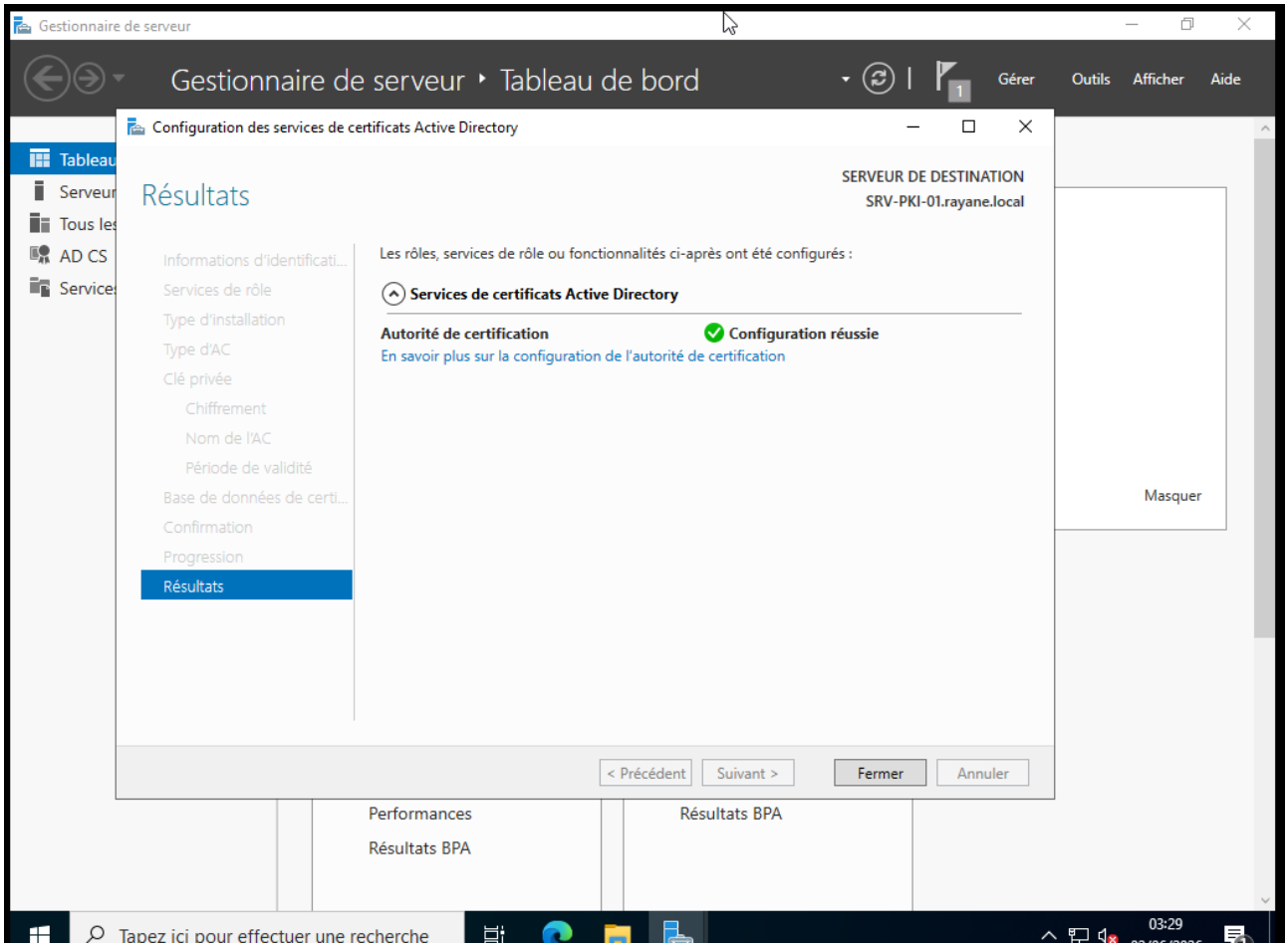


Figure 28 — Finalisation de la configuration ADCS

5.4 Export du certificat depuis SRV-PKI-01

Le certificat racine de l'autorité doit être exporté pour être installé sur le serveur Zabbix, lui permettant de valider les connexions SSL.

- Ouvrir MMC (Windows + R > mmc) et ajouter le composant Certificats (compte d'ordinateur, ordinateur local).
- Dans l'arborescence : Autorités de certification racines de confiance > Certificats.
- Effectuer un clic droit sur le certificat rayane-SRV-PKI-01-CA > Toutes les tâches > Exporter.
- Sélectionner le format DER encodé binaire (.CER) et enregistrer sous le nom rayane-CA.cer.

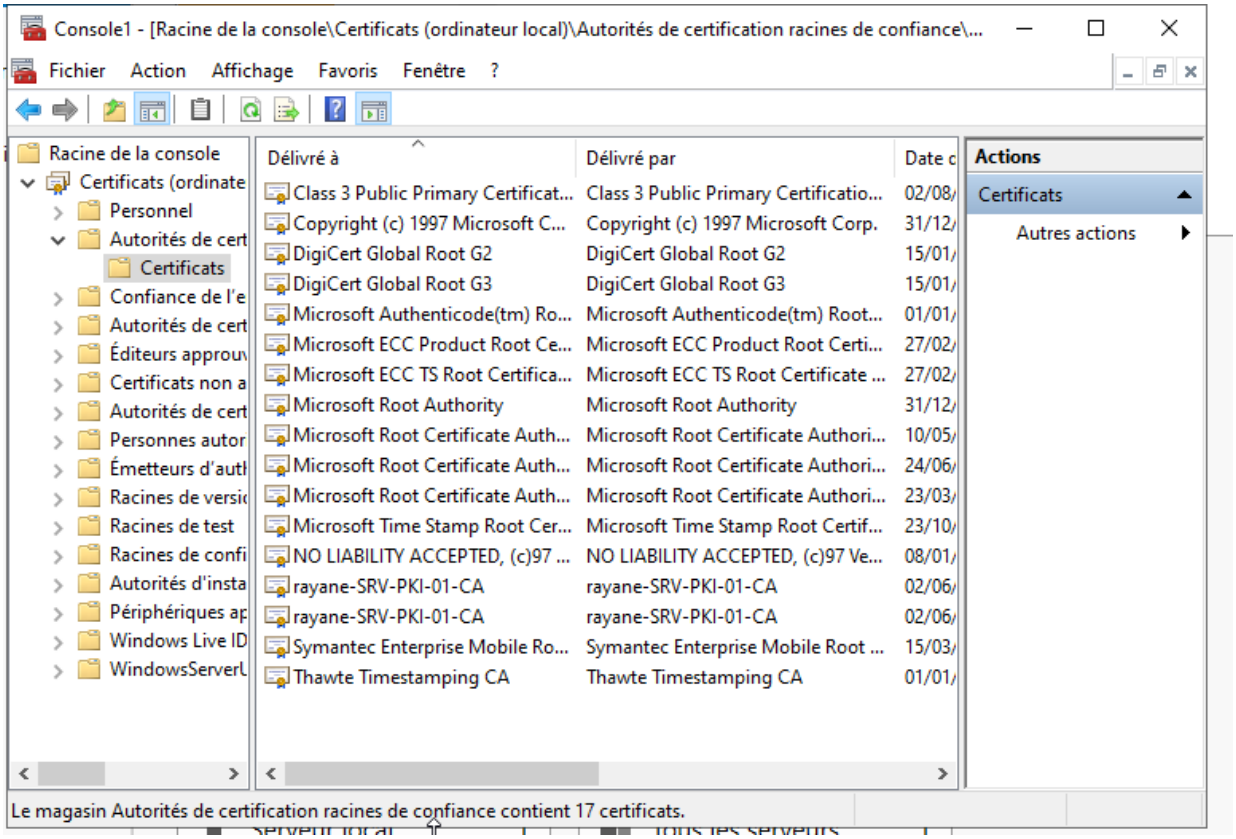


Figure 29 — Export du certificat de l'Autorité de Certification

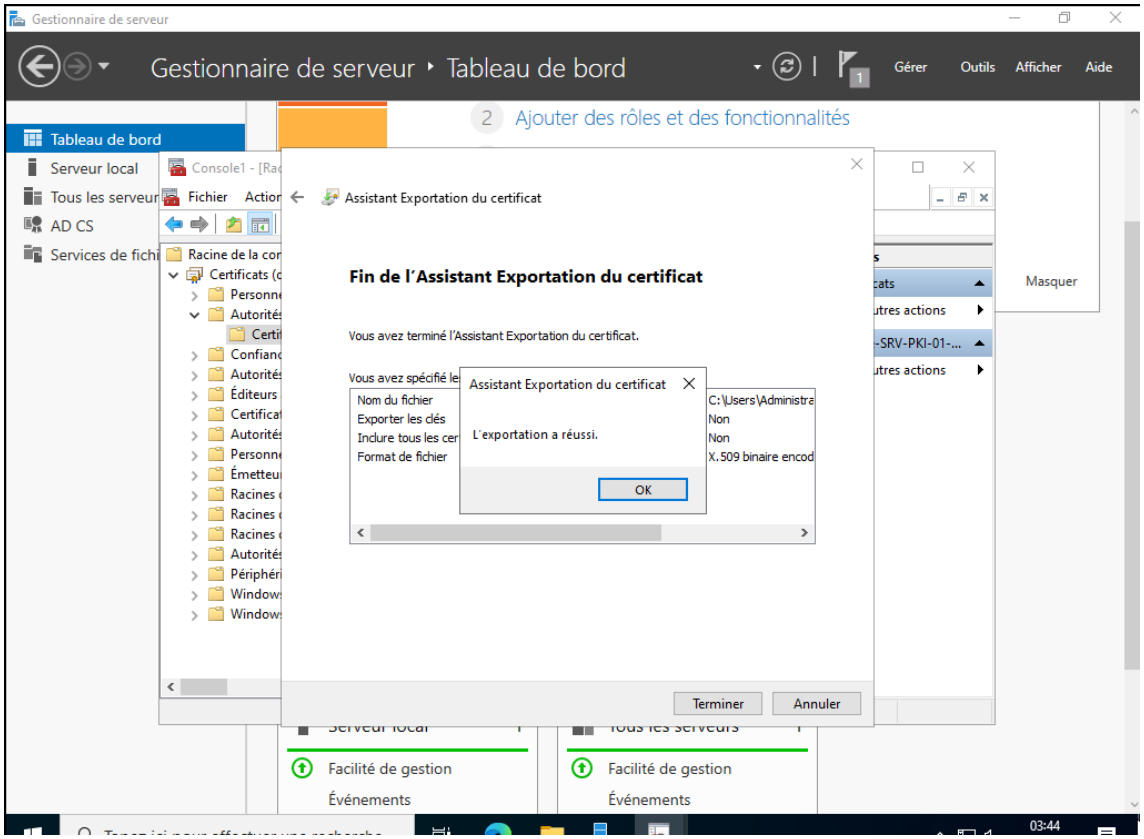
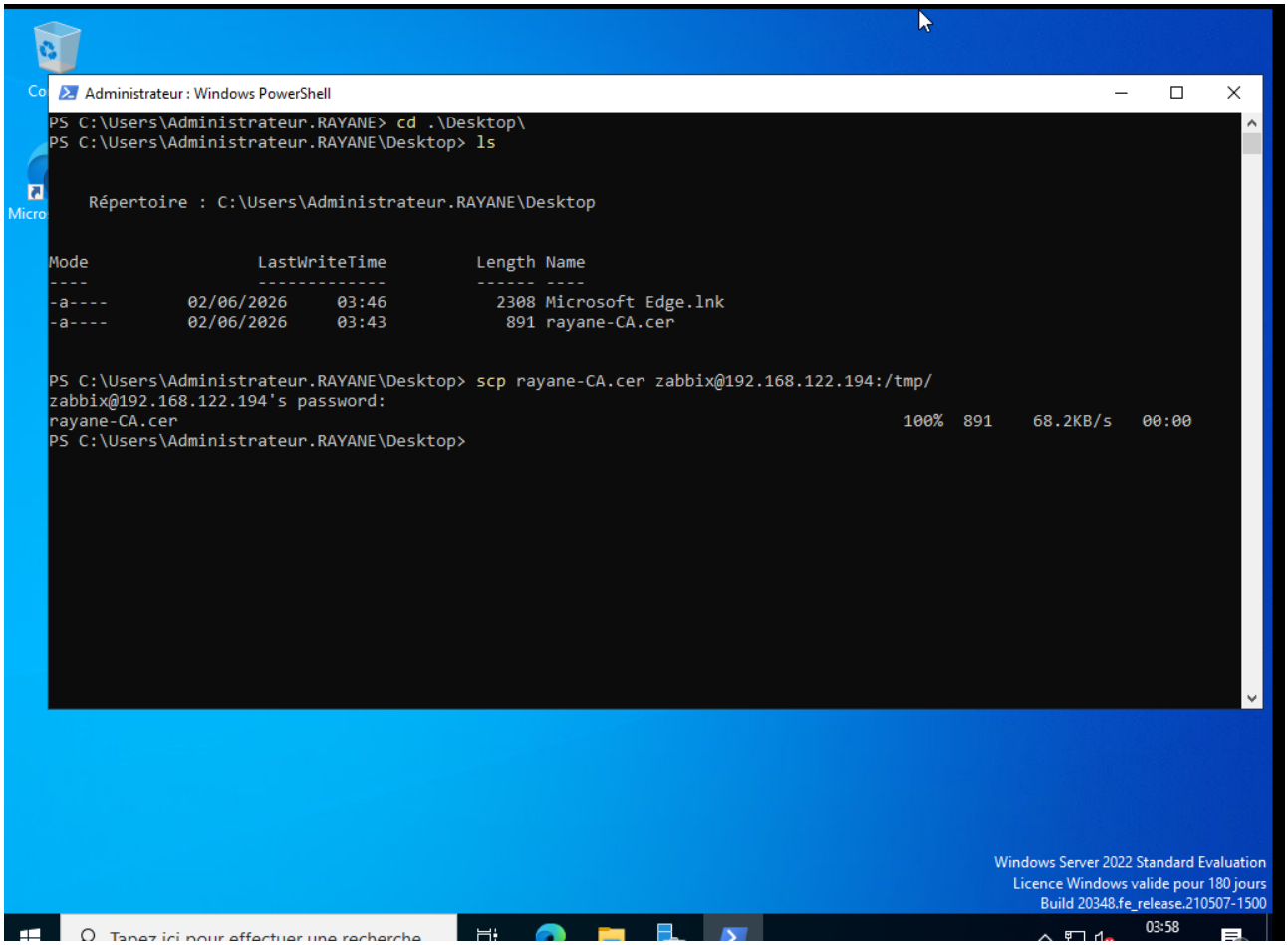


Figure 30 — Certificat exporté au format DER

5.5 Transfert et installation du certificat sur Zabbix

Le certificat est transféré vers le serveur Zabbix via SCP, puis installé dans le magasin de confiance du système Linux.

```
scp C:\Users\Administrateur\Desktop\rayane-CA.cer
zabbix@192.168.122.194:/tmp/
```



Sur le serveur Zabbix (connexion SSH) :

```
cd /tmp
openssl x509 -inform der -in rayane-CA.cer -out rayane-CA.crt
sudo mv rayane-CA.crt /usr/local/share/ca-certificates/
sudo update-ca-certificates
```

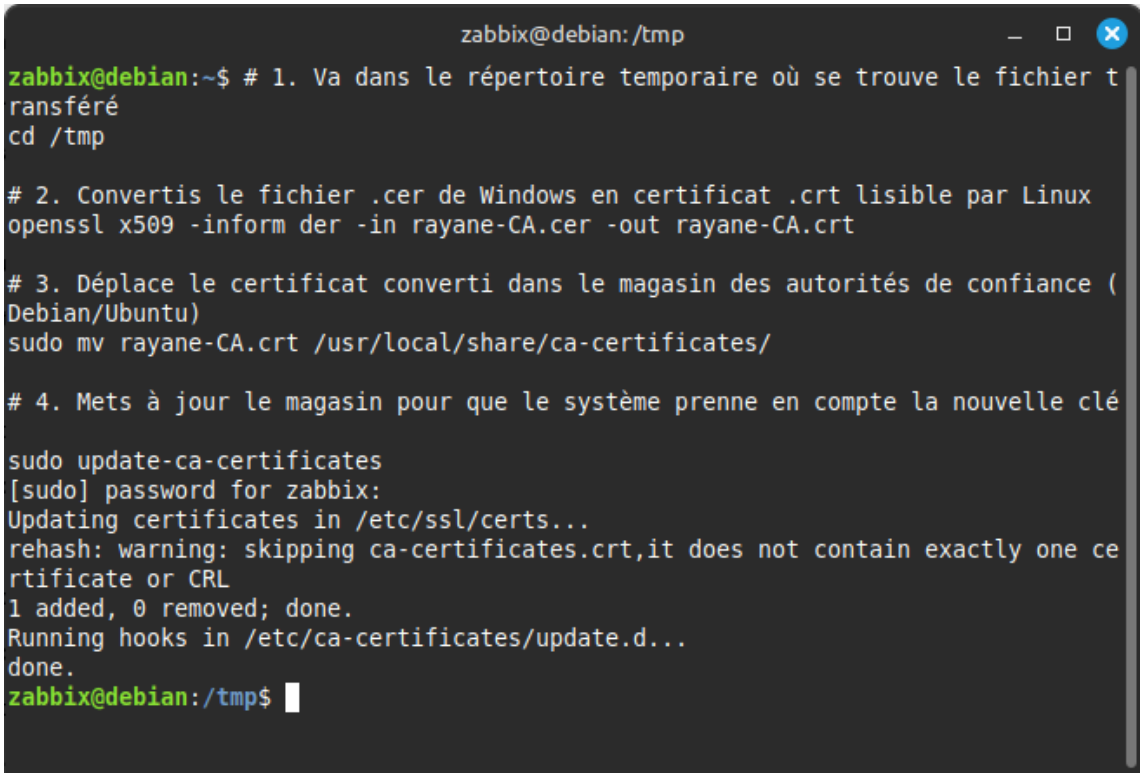


Figure 31 — Installation du certificat sur le serveur Zabbix

5.6 Test du canal LDAPS

La commande suivante permet de vérifier que la connexion chiffrée sur le port 636 fonctionne correctement entre le serveur Zabbix et le contrôleur de domaine.

```
openssl s_client -connect 192.168.122.235:636
```

> *Un retour « Verification: OK » confirme que le chiffrement TLS est opérationnel.*

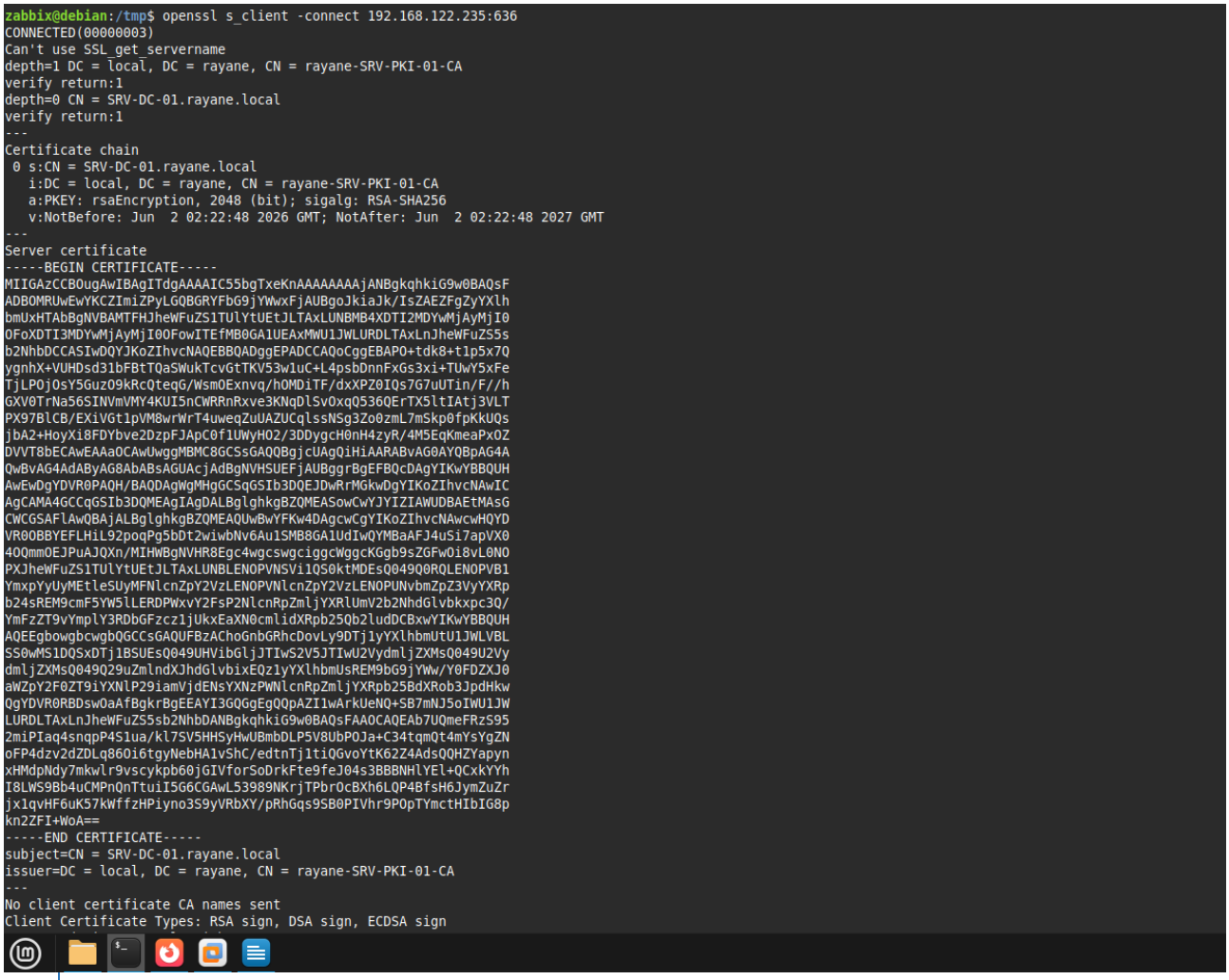


Figure 32 — Test de la connexion LDAPS avec OpenSSL

5.7 Activation de LDAPS dans l'interface Zabbix

Dans l'interface web Zabbix (Administration > Authentication > LDAP settings), modifier les paramètres du serveur Active Directory Rayane comme suit :

- Hôte : ldaps://192.168.122.235 (préfixe ldaps:// obligatoire)
- Port : 636 (port LDAPS standard, remplace le port 389)
- Bind password : resaisir le mot de passe du compte de liaison zabbix-auth

Cliquer sur Test pour vérifier la connexion, puis sur Update pour sauvegarder la configuration.

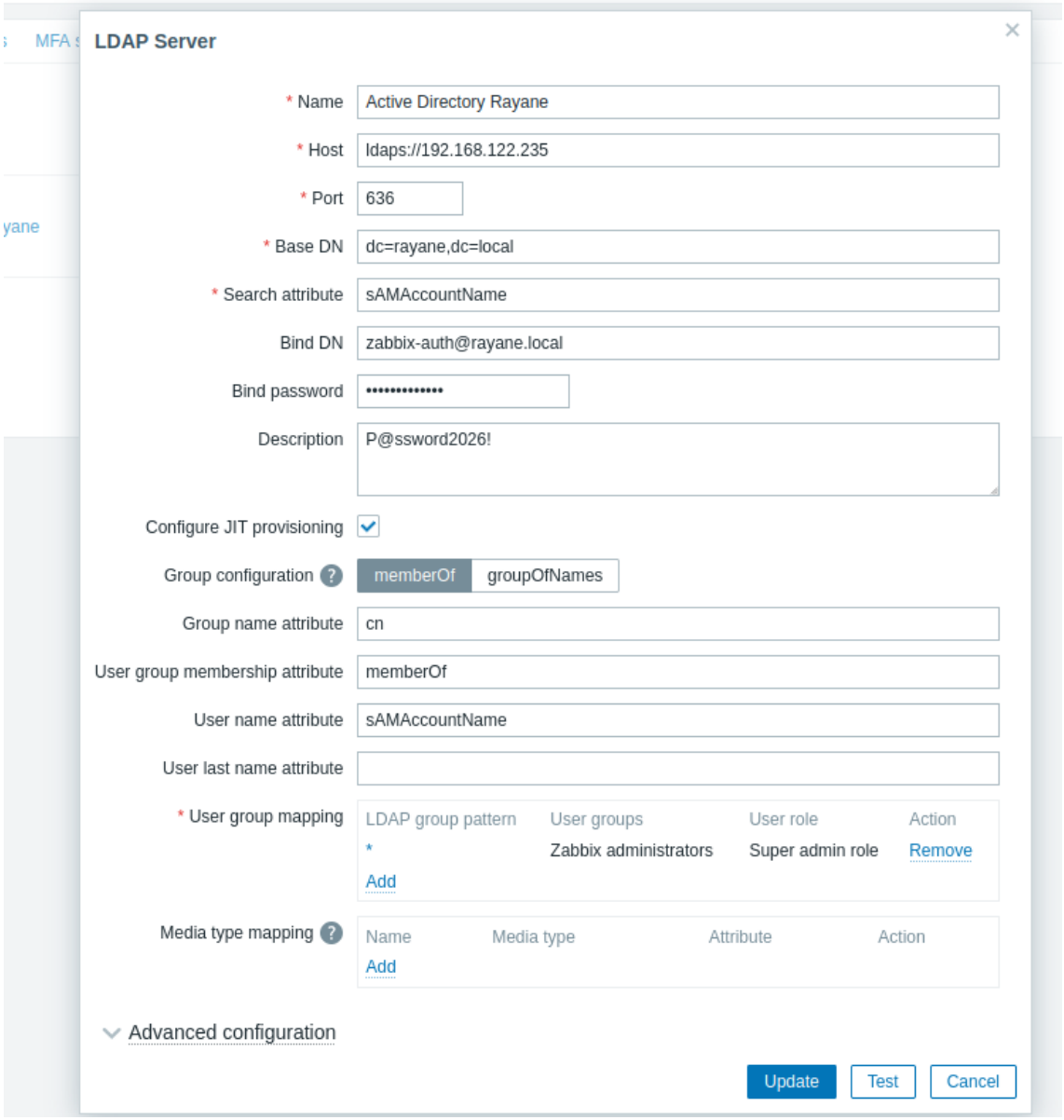


Figure 33 — Configuration LDAPS dans l'interface Zabbix

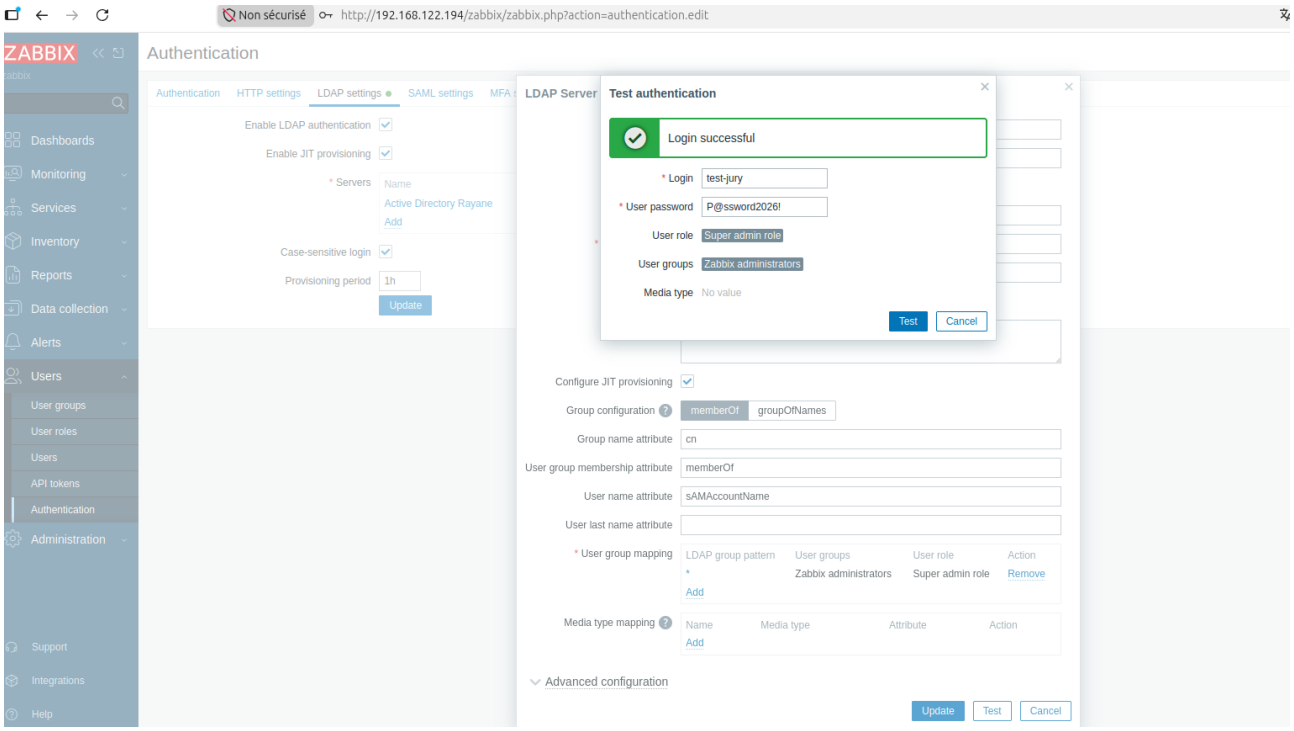


Figure 34 — Connexion LDAPS validée avec succès

Partie 6 — Analyse de sécurité avec Wireshark

Cette dernière partie illustre, à travers une capture réseau Wireshark, l'intérêt concret du passage de LDAP à LDAPS du point de vue de la sécurité.

6.1 Comparaison LDAP vs LDAPS

Les comptes qui se connectent à l'interface de Zabbix sont généralement des membres de l'équipe informatique disposant de privilèges élevés au sein du système d'information. La sécurisation de leurs authentifications est donc critique.

Avec une connexion LDAP non chiffrée (port 389), l'intégralité du trafic transite en clair sur le réseau. Un attaquant capable de capturer le trafic peut obtenir sans difficulté les identifiants et mots de passe des comptes de l'annuaire, y compris le mot de passe du compte connecteur (zabbix-auth).

L'activation de LDAPS (port 636) chiffre l'ensemble de ces échanges via TLS, rendant toute interception inexploitable.

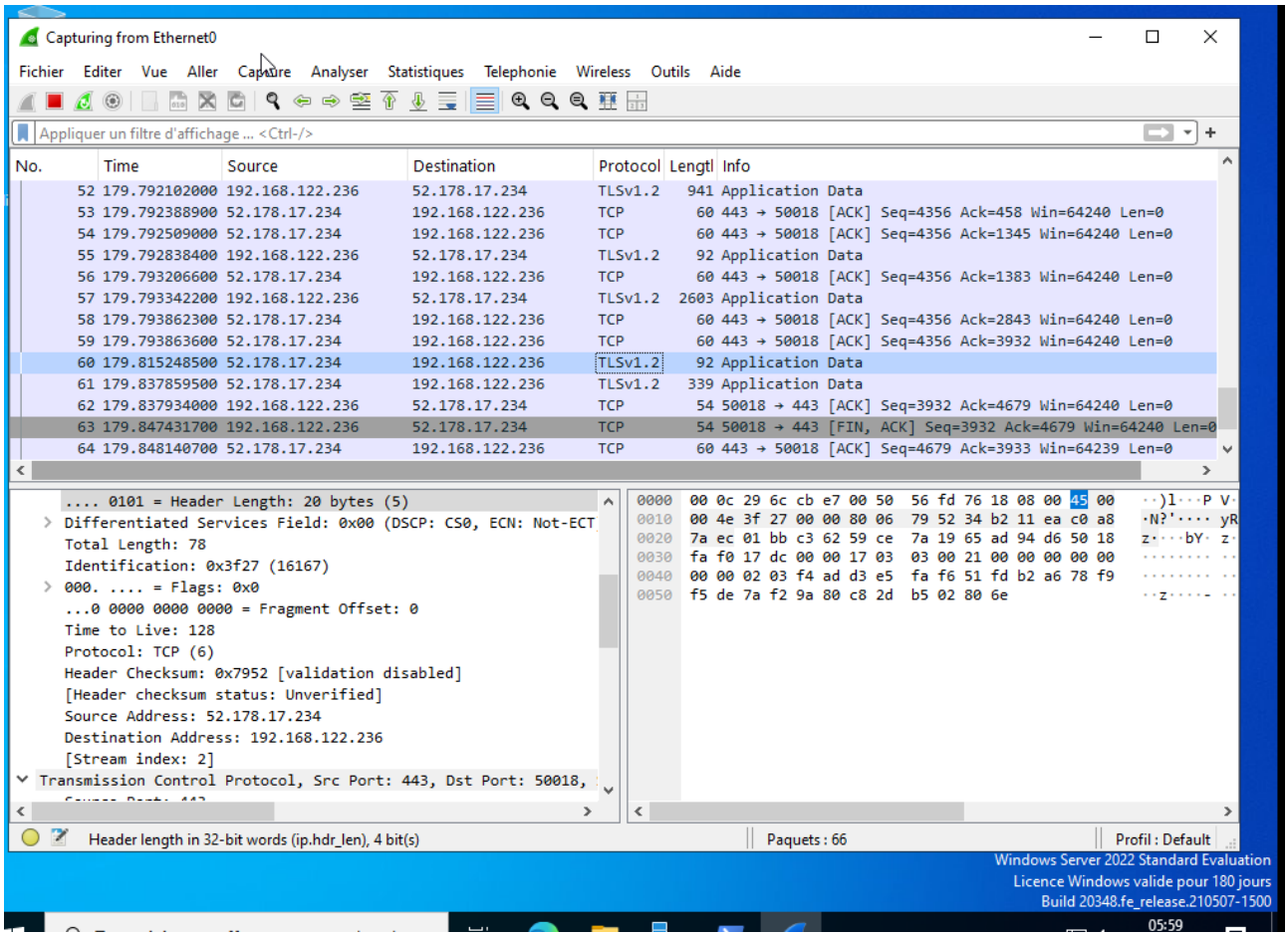


Figure 35 — Capture Wireshark

6.2 Conclusion de l'analyse

La mise en place de LDAPS représente une mesure de sécurité essentielle dans tout environnement de production. Elle protège les identifiants d'authentification contre les attaques de type Man-in-the-Middle (MitM) et garantit la confidentialité des échanges entre Zabbix et l'annuaire Active Directory.

Conclusion

Ce travail pratique a permis de mettre en œuvre une solution de supervision complète et sécurisée, illustrant plusieurs compétences fondamentales du BTS SIO :

- Administration système Linux : installation, configuration de services (Zabbix, MariaDB, Apache).
- Administration Windows Server : promotion en contrôleur de domaine, gestion des objets Active Directory, installation d'une PKI.
- Sécurité réseau : passage de l'authentification en clair (LDAP) à une authentification chiffrée (LDAPS) avec gestion des certificats.
- Supervision informatique : déploiement d'agents, déclaration d'hôtes, utilisation de modèles de supervision.
- Analyse réseau : utilisation de Wireshark pour comparer et valider les niveaux de sécurité.

L'ensemble de la chaîne de l'installation du serveur de supervision à la sécurisation des authentifications constitue une infrastructure cohérente et documentée, directement transposable en environnement professionnel.