DOCUMENTATION TECHNIQUE

Mise en place d'une infrastructure systeme virtualisee integrant Active Directory, GLPI et Zabbix

Element	Information
Etudiant	Alexandre PERZ
Etablissement	CFA ESTIAM
Diplome	BTS SIO - Option SISR
Session	2026
Projet	Infrastructure systeme, gestion de parc et supervision
Technologies	Proxmox VE, pfSense, Windows Server 2019, Active Directory, DNS, DHCP, Debian, GLPI, LDAP, Zabbix

Perimetre de cette documentation

Ce document correspond a la seconde partie du projet. La partie reseau et segmentation VLAN sous Proxmox/pfSense est traitee dans une documentation separee. Cette documentation presente la mise en place des services systeme : Active Directory, DNS, DHCP, GLPI, LDAP et Zabbix.

Sommaire

1. Presentation du projet et contexte technique

L'objectif de cette seconde partie du projet est de mettre en place les services systeme indispensables au fonctionnement d'une infrastructure d'entreprise. La premiere documentation a permis de creer l'architecture reseau virtualisee sous Proxmox, de segmenter les flux avec pfSense et de definir les VLAN. Cette documentation poursuit le projet avec la mise en place d'un controleur de domaine Active Directory, d'un serveur GLPI pour la gestion de parc et d'un serveur Zabbix pour la supervision.

- Centraliser l'authentification des utilisateurs avec Active Directory.
- Assurer la resolution DNS interne du domaine alex.local.
- Distribuer automatiquement les adresses IP des postes clients via DHCP depuis le serveur Windows.
- Mettre en place des GPO pour standardiser l'environnement utilisateur.
- Installer GLPI pour la gestion de parc informatique et le support.
- Connecter GLPI a Active Directory via LDAP pour eviter la gestion de comptes locaux separes.
- Installer Zabbix pour superviser la disponibilite et l'etat des serveurs.

Choix d architecture

Le service DHCP est volontairement heberge sur le controleur Active Directory, et non sur pfSense. pfSense conserve son role de routeur, de passerelle et de firewall. Le serveur Windows centralise les services d'annuaire, DNS et DHCP afin de garder une architecture coherente avec un environnement Microsoft.

2. Architecture cible et plan d adressage

L'infrastructure s'appuie sur trois segments reseau principaux : le VLAN utilisateurs, le VLAN serveurs et la DMZ. Les services internes sensibles sont places dans le VLAN serveurs, tandis que GLPI est positionne en DMZ afin de separer le service web du reseau interne.

Zone	Reseau	Passerelle	Role
VLAN10_USERS	192.168.10.0/24	192.168.10.1	Postes clients du domaine
VLAN20_SERVERS	192.168.20.0/24	192.168.20.1	Services internes : AD, DNS, DHCP, Zabbix
VLAN30_DMZ	192.168.30.0/24	192.168.30.1	Service web GLPI isole du LAN

Machine	Systeme	Adresse IP	Role
SRV-AD01	Windows Server 2019	192.168.20.10	Controleur de domaine, DNS, DHCP
SRV-GLPI01	Debian Linux	192.168.30.10	Gestion de parc et helpdesk
SRV-ZBX01	Debian Linux	192.168.20.20	Supervision Zabbix
pfSense	FreeBSD / pfSense	192.168.20.1 / 192.168.30.1 / 192.168.10.1	Routage, firewall, NAT, relais DHCP si besoin

Point important sur DHCP inter-VLAN

Le serveur DHCP se trouve dans le VLAN20_SERVERS alors que les postes clients sont dans le VLAN10_USERS. Pour que les clients puissent obtenir une adresse IP depuis l'AD, un relais DHCP doit etre configure sur pfSense ou les flux DHCP doivent etre autorises selon la topologie retenue. Le serveur DHCP reste cependant bien le serveur Windows.

3. Mise en place du controleur Active Directory

La partie Active Directory reprend le travail deja realise lors de la precedente mise en place, mais elle est reecrite avec les adresses IP de la nouvelle architecture. Les anciennes adresses en 192.168.72.0/24 ne sont plus utilisees. Le controleur de domaine est maintenant positionne dans le VLAN serveurs.

3.1 Creation de la machine virtuelle Windows Server

Objectif

Deployer une machine Windows Server 2019 qui portera les roles Active Directory, DNS et DHCP.

Procedure realisee

- Depuis Proxmox, creer une nouvelle machine virtuelle nommee SRV-AD01.
- Associer la carte reseau de la VM au bridge correspondant au VLAN20_SERVERS.
- Monter l ISO Windows Server 2019.
- Allouer des ressources suffisantes : 2 vCPU, 4 Go de RAM minimum et un disque de 60 Go.
- Lancer l installation de Windows Server en edition Desktop Experience afin de disposer de l interface graphique.

Validation

- La VM demarre correctement.
- Le serveur est joignable depuis le VLAN serveurs.
- Le nom de la machine est configure en SRV-AD01.

3.2 Configuration IP statique du serveur

Objectif

Attribuer une adresse IP fixe au controleur de domaine pour garantir la stabilite des services AD, DNS et DHCP.

Procedure realisee

- Ouvrir les parametres de la carte reseau Windows.
- Desactiver l adressage automatique DHCP sur le serveur.
- Configurer manuellement l adresse IP, le masque, la passerelle et le DNS.
- Verifier que le serveur peut joindre la passerelle pfSense.

Validation

- ping 192.168.20.1 repond.
- La commande ipconfig /all affiche bien les parametres attendus.

Parametre	Valeur
Adresse IP	192.168.20.10

Parametre	Valeur
Masque	255.255.255.0
Passerelle	192.168.20.1
DNS prefere	192.168.20.10

3.3 Installation des roles AD DS, DNS et DHCP

Objectif

Installer les roles serveur necessaires a la centralisation de l administration du domaine.

Procedure realisee

- Ouvrir le Gestionnaire de serveur.
- Cliquer sur Gerer puis Ajouter des roles et fonctionnalites.
- Selectionner Installation basee sur un role ou une fonctionnalite.
- Selectionner le serveur local SRV-AD01.
- Cocher Active Directory Domain Services, DNS Server et DHCP Server.
- Valider les fonctionnalites supplementaires proposees par Windows.
- Lancer l installation puis attendre la fin du processus.

Validation

- Les roles apparaissent dans le Gestionnaire de serveur.
- Une notification demande de promouvoir le serveur en controleur de domaine.

3.4 Promotion du serveur en controleur de domaine

Objectif

Transformer le serveur Windows en controleur de domaine Active Directory.

Procedure realisee

- Dans le Gestionnaire de serveur, cliquer sur le drapeau de notification.
- Choisir Promouvoir ce serveur en controleur de domaine.
- Selectionner Ajouter une nouvelle foret.
- Renseigner le nom de domaine racine : alex.local.
- Definir le mot de passe DSRM.
- Conserver l installation DNS integree.
- Verifier le nom NetBIOS propose : ALEX.
- Conserver les chemins par defaut pour NTDS, SYSVOL et les journaux.
- Lancer l installation puis laisser le serveur redemarrer.

Validation

- Apres redemarrage, l ouverture de session se fait avec le domaine ALEX.
- La console Utilisateurs et ordinateurs Active Directory est disponible.
- La zone DNS alex.local est creee automatiquement.

Nom de domaine retenu

Le domaine utilise dans la documentation est alex.local. Il permet de simuler un domaine interne d entreprise. En production, il serait preferable d utiliser un sous-domaine d un domaine public maitrise, par exemple ad.entreprise.fr.

4. Configuration DNS et DHCP

Le controleur de domaine assure a la fois le service DNS interne et le service DHCP. Cette centralisation permet aux postes clients d'obtenir automatiquement les bons parametres reseau pour rejoindre le domaine et appliquer les GPO.

4.1 Verification de la zone DNS directe

Objectif

Verifier que le domaine alex.local dispose bien d une zone DNS interne.

Procedure realisee

- Ouvrir Gestionnaire de serveur - Outils - DNS.
- Developper le serveur SRV-AD01.
- Ouvrir Zones de recherche directes.
- Verifier la presence de la zone alex.local.
- Verifier la presence des enregistrements SRV necessaires a Active Directory.

Validation

- nslookup alex.local retourne le serveur DNS.
- Les postes du domaine peuvent resoudre le nom SRV-AD01.alex.local.

4.2 Creation des zones DNS inversees

Objectif

Permettre la resolution inverse IP vers nom, utile pour le diagnostic et certaines integrations.

Procedure realisee

- Dans la console DNS, faire un clic droit sur Zones de recherche inversees.
- Cliquer sur Nouvelle zone.
- Selectionner Zone principale integree a Active Directory.
- Choisir une zone IPv4.
- Creer une zone pour le reseau 192.168.20.0/24.
- Creer si necessaire une zone pour le reseau 192.168.10.0/24.
- Autoriser uniquement les mises a jour dynamiques securisees.

Validation

- La zone inverse 20.168.192.in-addr.arpa est presente.
- La commande nslookup 192.168.20.10 retourne SRV-AD01.

4.3 Autorisation du serveur DHCP dans Active Directory

Objectif

Autoriser le serveur DHCP afin qu il puisse distribuer des baux dans le domaine.

Procedure realisee

- Dans le Gestionnaire de serveur, cliquer sur le drapeau de notification DHCP.
- Choisir Terminer la configuration DHCP.
- Utiliser le compte administrateur du domaine pour autoriser le serveur.
- Fermer l assistant lorsque la configuration est terminee.

Validation

- La console DHCP affiche le serveur comme autorise.
- Aucune alerte DHCP n est presente dans le Gestionnaire de serveur.

4.4 Creation de l etendue DHCP pour les postes clients

Objectif

Distribuer automatiquement les adresses IP aux postes du VLAN utilisateurs.

Procedure realisee

- Ouvrir Gestionnaire de serveur - Outils - DHCP.
- Developper SRV-AD01 puis IPv4.
- Clic droit sur IPv4 puis Nouvelle etendue.
- Nommer l etendue VLAN10_USERS.
- Configurer la plage 192.168.10.100 a 192.168.10.200.
- Configurer le masque en /24.
- Ajouter une plage d exclusion pour les adresses reservees si necessaire.
- Definir une duree de bail de 5 jours.
- Configurer les options DHCP.
- Activer l etendue.

Validation

- Un client du VLAN10 recoit une adresse en 192.168.10.100-200.
- Le client recoit la passerelle 192.168.10.1 et le DNS 192.168.20.10.

Option DHCP	Valeur	Role
Plage	192.168.10.100 - 192.168.10.200	Adresses distribuees aux postes clients
Option 003 - Routeur	192.168.10.1	Passerelle pfSense du VLAN utilisateurs
Option 006 - DNS	192.168.20.10	Resolution DNS via Active Directory

Option DHCP	Valeur	Role
Option 015 - Nom de domaine	alex.local	Suffixe DNS du domaine
Duree du bail	5 jours	Renouvellement regulier des adresses

4.5 Configuration du relais DHCP sur pfSense

Objectif

Permettre aux clients du VLAN10_USERS de joindre le serveur DHCP situe dans le VLAN20_SERVERS.

Procedure realisee

- Dans pfSense, aller dans Services - DHCP Relay.
- Activer le relais DHCP.
- Selectionner l interface VLAN10_USERS.
- Renseigner le serveur DHCP cible : 192.168.20.10.
- Sauvegarder puis appliquer.
- Verifier que les regles firewall autorisent les flux DHCP necessaires.

Validation

- Un poste client en VLAN10 obtient un bail depuis le serveur Windows.
- La console DHCP Windows affiche le bail attribue.

5. Organisation de l annuaire et GPO

Une fois Active Directory operationnel, l'annuaire a ete structure afin de faciliter l'administration. Les utilisateurs, groupes et ressources sont organises dans des unites d'organisation. Des GPO permettent ensuite d'appliquer automatiquement des parametres aux postes et utilisateurs du domaine.

5.1 Creation des unites d organisation

Objectif

Structurer l annuaire pour separer les services et faciliter l application des GPO.

Procedure realisee

- Ouvrir Utilisateurs et ordinateurs Active Directory.
- Clic droit sur le domaine alex.local.
- Creer une unite d organisation nommee Services.
- Creer les sous-Ou Administration, Service IT et Telephonie IP.
- Creer une Ou Utilisateurs si elle n existe pas.
- Activer la protection contre la suppression accidentelle pour les Ou importantes.

Validation

- Les Ou sont visibles dans la console Active Directory.
- Les objets sont ranges dans l Ou correspondant a leur role.

OU	Contenu	Interet
Administration	Comptes et groupes administratifs	Separer les comptes privilegies des comptes standards
Service IT	Utilisateurs et ressources IT	Appliquer des GPO specifiques au service informatique
Utilisateurs	Comptes utilisateurs standards	Centraliser les utilisateurs du domaine
Telephonie IP	Objets lies a la telephonie	Preparer une organisation par metier ou service

5.2 Creation d un compte administrateur dedie

Objectif

Eviter d utiliser le compte Administrateur integre pour les operations quotidiennes.

Procedure realisee

- Dans l Ou Administration, creer un nouvel utilisateur administrateur.
- Definir un mot de passe fort.
- Decocher si necessaire l obligation de changement au prochain demarrage pour un compte de service.
- Ajouter le compte aux groupes d administration necessaires.
- Utiliser ce compte pour les actions d administration du domaine.

Validation

- Le compte peut ouvrir une session d administration.
- Le compte dispose des droits necessaires sans utiliser le compte Administrateur integre.

5.3 GPO de deploiement du fond d ecran

Objectif

Standardiser l environnement utilisateur en appliquant un fond d ecran commun aux postes du domaine.

Procedure realisee

- Placer le fichier fond.jpg dans le partage SYSVOL du domaine.
- Ouvrir Gestion de strategie de groupe.
- Creer une GPO nommee Deploiement fond d ecran.
- Configurer une preference Fichiers pour copier l image localement dans C:\Windows\Web\Wallpaper.
- Configurer le parametre Papier peint du Bureau dans Configuration utilisateur.
- Lier la GPO a l Ou contenant les utilisateurs cibles.

Validation

- La commande gpupdate /force applique la GPO.
- Le fond d ecran apparait sur le poste client apres ouverture de session.

5.4 GPO de mappage de lecteur reseau

Objectif

Fournir automatiquement un lecteur reseau aux utilisateurs autorises.

Procedure realisee

- Creer un dossier partage sur le serveur.
- Attribuer les droits NTFS et partage au groupe de securite concerne.
- Creer une GPO de mappage de lecteur.
- Aller dans Configuration utilisateur - Preferences - Parametres Windows - Mappages de lecteurs.
- Creer un lecteur mappe vers le chemin reseau du partage.
- Choisir une lettre de lecteur, par exemple Z:.
- Utiliser le ciblage par groupe de securite si necessaire.

Validation

- Le lecteur reseau apparait automatiquement sur le poste client.
- Les droits d acces correspondent aux groupes de securite Active Directory.

6. Installation et configuration de GLPI

GLPI est une solution de gestion de parc informatique et de gestion des tickets. Dans cette architecture, le serveur GLPI est place dans la DMZ afin d'isoler le service web du reseau interne. Les communications vers Active Directory sont limitees aux flux necessaires pour l'authentification LDAP et la resolution DNS.

Parametre	Valeur
Nom serveur	SRV-GLPI01
Systeme	Debian Linux
Adresse IP	192.168.30.10
Passerelle	192.168.30.1
DNS	192.168.20.10
Zone	VLAN30_DMZ

6.1 Preparation du serveur Debian

Objectif

Installer un serveur Linux propre et lui attribuer une configuration reseau statique.

Procedure realisee

- Creer une VM Debian dans Proxmox.
- Connecter la carte reseau au bridge correspondant a la DMZ.
- Installer Debian en mode serveur.
- Configurer le nom d hote SRV-GLPI01.
- Configurer l adresse IP statique 192.168.30.10.
- Verifier la connectivite avec la passerelle pfSense et le serveur DNS AD.

Validation

- ping 192.168.30.1 fonctionne.
- ping 192.168.20.10 fonctionne si les regles firewall l autorisent.
- La resolution DNS interne fonctionne via 192.168.20.10.

```
ip a
ip route
ping 192.168.30.1
ping 192.168.20.10
```

6.2 Installation de la pile web LAMP

Objectif

Installer les composants necessaires au fonctionnement de GLPI : serveur web, PHP et base de donnees.

Procedure realisee

- Mettre a jour les depots Debian.
- Installer Apache2.
- Installer MariaDB Server.
- Installer PHP et les extensions requises par GLPI.
- Activer les modules Apache necessaires.
- Verifier que le service Apache repond depuis un navigateur.

Validation

- La page par defaut Apache est accessible.
- Les services apache2 et mariadb sont actifs.

```
apt update && apt upgrade -y
apt install apache2 mariadb-server -y
apt install php php-mysql php-curl php-gd php-intl php-ldap php-xml php-mbstring
php-zip php-bz2 unzip -y
systemctl enable --now apache2 mariadb
```

6.3 Securisation initiale de MariaDB

Objectif

Securiser le serveur de base de donnees avant la creation de la base GLPI.

Procedure realisee

- Lancer l assistant mysql_secure_installation.
- Definir ou confirmer le mot de passe root MariaDB selon la configuration.
- Supprimer les utilisateurs anonymes.
- Desactiver les connexions root distantes.
- Supprimer la base de test.
- Recharger les privileges.

Validation

- MariaDB est accessible localement.
- Les comptes inutiles sont supprimes.

```
mysql_secure_installation
```

6.4 Creation de la base de donnees GLPI

Objectif

Creer une base et un utilisateur dedie pour GLPI.

Procedure realisee

- Se connecter a MariaDB.
- Creer la base de donnees glpi.
- Creer un utilisateur glpiuser avec un mot de passe fort.
- Donner les privileges uniquement sur la base glpi.
- Recharger les privileges.

Validation

- La base glpi est visible dans MariaDB.
- L utilisateur glpiuser peut se connecter a la base.

```
mysql -u root -p
CREATE DATABASE glpi CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
CREATE USER 'glpiuser'@'localhost' IDENTIFIED BY 'MotDePasseFort';
GRANT ALL PRIVILEGES ON glpi.* TO 'glpiuser'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

6.5 Deploiement des fichiers GLPI

Objectif

Installer GLPI dans le repertoire web du serveur.

Procedure realisee

- Telecharger l archive de la version stable de GLPI.
- Extraire l archive.
- Deplacer le dossier glpi dans /var/www/html/.
- Attribuer les droits au compte www-data.
- Verifier que le dossier est accessible par Apache.

Validation

- Le repertoire /var/www/html/glpi existe.
- Les permissions appartiennent a www-data.

```
cd /tmp
# Telecharger puis extraire l archive GLPI utilisee pour le projet
tar -xvzf glpi-*.tgz
mv glpi /var/www/html/glpi
chown -R www-data:www-data /var/www/html/glpi
chmod -R 755 /var/www/html/glpi
```

6.6 Configuration du site Apache pour GLPI

Objectif

Declarer un VirtualHost Apache dedie a GLPI.

Procedure realisee

- Creer un fichier /etc/apache2/sites-available/glpi.conf.
- Declarer le DocumentRoot vers /var/www/html/glpi/public si la version GLPI l exige.
- Autoriser les overrides necessaires.
- Activer le site GLPI.
- Recharger Apache.

Validation

- Apache redemarre sans erreur.
- GLPI est accessible depuis un navigateur.

```
a2ensite glpi.conf
a2enmod rewrite
systemctl reload apache2
```

6.7 Installation via l interface web

Objectif

Finaliser la configuration GLPI depuis un navigateur.

Procedure realisee

- Ouvrir http://192.168.30.10/glpi ou le VirtualHost configure.
- Choisir la langue francaise.
- Accepter la licence.
- Lancer l installation.
- Renseigner le serveur MariaDB localhost.
- Indiquer l utilisateur glpiuser et son mot de passe.
- Selectionner la base glpi.
- Finaliser l installation.
- Se connecter avec le compte administrateur GLPI.

Validation

- L interface GLPI est accessible.
- La connexion administrateur fonctionne.
- Les tables GLPI sont creees dans MariaDB.

6.8 Actions post-installation GLPI

Objectif
Securiser et nettoyer l installation apres le premier demarrage.

Procedure realisee

- Supprimer le fichier install/install.php si GLPI le demande.
- Changer les mots de passe des comptes par defaut.
- Verifier les droits sur les dossiers files, config et marketplace.
- Configurer le fuseau horaire PHP si necessaire.
- Configurer le cron GLPI pour les actions automatiques.
- Limiter les acces firewall a l interface GLPI selon le besoin.

Validation

- GLPI ne signale plus d alertes critiques post-installation.
- Les comptes par defaut ne conservent pas leur mot de passe initial.

7. Integration LDAP de GLPI avec Active Directory

L'integration LDAP permet a GLPI d'utiliser les comptes presents dans Active Directory. Les utilisateurs n'ont donc pas besoin d'un compte local separe dans GLPI. Cette integration ameliore la centralisation, la tracabilite et la coherence de l'administration.

Parametre LDAP	Valeur
Serveur LDAP	192.168.20.10
Port	389
BaseDN	DC=alex,DC=local
Domaine	alex.local
Compte de liaison	Compte AD dedie a la lecture LDAP
Filtre utilisateur	(&(objectClass=user)(objectCategory=person))

7.1 Preparation cote Active Directory

Objectif

Creer un compte de service permettant a GLPI de lire l annuaire.

Procedure realisee

- Dans Active Directory, creer un utilisateur de service, par exemple svc_glpi_ldap.
- Placer ce compte dans une Ou dediee aux comptes de service.
- Definir un mot de passe fort.
- Desactiver le changement obligatoire de mot de passe a la prochaine connexion.
- Limiter les droits au strict necessaire : lecture de l annuaire.

Validation

- Le compte peut s authentifier sur le domaine.
- Le compte n est pas administrateur du domaine.

7.2 Configuration LDAP dans GLPI

Objectif

Declarer le serveur Active Directory comme source d authentification externe.

Procedure realisee

- Dans GLPI, aller dans Configuration - Authentification - Annuaires LDAP.
- Ajouter un nouvel annuaire.
- Renseigner le nom : AD alex.local.
- Indiquer l hote LDAP : 192.168.20.10.
- Indiquer le port : 389.
- Renseigner la base DN : DC=alex,DC=local.
- Renseigner le compte de liaison et son mot de passe.
- Tester la connexion LDAP.
- Sauvegarder la configuration.

Validation

- Le test de connexion LDAP est reussi.
- GLPI peut rechercher les utilisateurs Active Directory.

7.3 Import des utilisateurs AD dans GLPI

Objectif

Importer les utilisateurs du domaine afin qu ils puissent se connecter a GLPI.

Procedure realisee

- Dans GLPI, aller dans Administration - Utilisateurs.
- Choisir Liaison annuaire LDAP.
- Rechercher les utilisateurs presents dans Active Directory.
- Selectionner les comptes a importer.
- Importer les utilisateurs.
- Verifier les champs recuperes : nom, prenom, identifiant, adresse mail.

Validation

- Les utilisateurs AD apparaissent dans GLPI.
- Un utilisateur importe peut ouvrir une session GLPI avec son compte domaine.

7.4 Regles firewall necessaires pour LDAP

Objectif

Autoriser uniquement les flux utiles entre GLPI en DMZ et le serveur Active Directory.

Procedure realisee

- Autoriser depuis 192.168.30.10 vers 192.168.20.10 le port TCP 389 pour LDAP.
- Autoriser le DNS depuis 192.168.30.10 vers 192.168.20.10 sur TCP/UDP 53.
- Bloquer les autres flux DMZ vers le VLAN serveurs par defaut.
- Documenter les regles dans pfSense.

Validation

- GLPI peut joindre LDAP et DNS.
- La DMZ ne peut pas acceder librement au VLAN serveurs.

8. Installation et configuration de Zabbix

Zabbix est utilise pour superviser la disponibilite et l'etat des equipements de l'infrastructure. Il permet de visualiser les incidents, de suivre les ressources systeme et de detecter rapidement les interruptions de service.

Parametre	Valeur
Nom serveur	SRV-ZBX01
Systeme	Debian Linux
Adresse IP	192.168.20.20
Passerelle	192.168.20.1
DNS	192.168.20.10
Zone	VLAN20_SERVERS

8.1 Preparation du serveur Debian Zabbix

Objectif

Installer une machine Debian dediee a la supervision.

Procedure realisee

- Creer une VM Debian dans Proxmox.
- Connecter la VM au bridge du VLAN20_SERVERS.
- Configurer le nom d hote SRV-ZBX01.
- Configurer l adresse IP statique 192.168.20.20.
- Verifier la resolution DNS et l acces Internet pour l installation des paquets.

Validation

- Le serveur repond au ping sur 192.168.20.20.
- Le serveur peut resoudre les noms DNS internes et externes.

```
hostnamectl set-hostname SRV-ZBX01
ip a
ping 192.168.20.1
ping 192.168.20.10
```

8.2 Installation des paquets Zabbix

Objectif

Installer le serveur Zabbix, son interface web, sa base de donnees et son agent.

Procedure realisee

- Ajouter le depot Zabbix correspondant a la version utilisee.
- Mettre a jour les depots apt.
- Installer zabbix-server-mysql.
- Installer l interface web Zabbix.
- Installer zabbix-agent.
- Installer MariaDB si elle n est pas presente.
- Activer les services necessaires.

Validation

- Les paquets Zabbix sont installes.
- Les services Apache, MariaDB et Zabbix sont presents.

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

8.3 Creation de la base de donnees Zabbix

Objectif

Preparer la base de donnees utilisee par le serveur Zabbix.

Procedure realisee

- Se connecter a MariaDB.
- Creer la base zabbix avec l encodage recommande.
- Creer l utilisateur zabbix.
- Attribuer les droits sur la base zabbix.
- Importer le schema initial fourni par Zabbix.

Validation

- La base zabbix existe.
- L import du schema se termine sans erreur.

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

# Import du schema selon le chemin fourni par la version installee
```

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```

8.4 Configuration du serveur Zabbix

Objectif

Renseigner les parametres de connexion a la base de donnees.

Procedure realisee

- Editer le fichier /etc/zabbix/zabbix_server.conf.
- Renseigner DBName=zabbix.
- Renseigner DBUser=zabbix.
- Renseigner DBPassword avec le mot de passe defini.
- Configurer le fuseau horaire PHP dans la configuration Apache de Zabbix.
- Redemarrer les services.

Validation

- Le service zabbix-server demarre correctement.
- L interface web Zabbix est accessible.

```
nano /etc/zabbix/zabbix_server.conf
# DBName=zabbix
# DBUser=zabbix
# DBPassword=MotDePasseFort

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

8.5 Finalisation via l interface web Zabbix

Objectif

Terminer l installation de Zabbix depuis le navigateur.

Procedure realisee

- Ouvrir http://192.168.20.20/zabbix.
- Verifier les pre-requis PHP.
- Renseigner les informations de base de donnees.
- Definir le nom du serveur Zabbix.
- Finaliser l assistant.
- Se connecter avec le compte administrateur initial.
- Changer le mot de passe par defaut.

Validation

- Le tableau de bord Zabbix est accessible.
- Le serveur Zabbix indique que le backend fonctionne.

9. Supervision de l infrastructure

Une fois Zabbix installe, les differents serveurs et equipements sont ajoutes comme hotes. La supervision permet de verifier l'etat des services, la disponibilite reseau et les ressources systeme.

9.1 Installation de l agent Zabbix sur Debian

Objectif

Permettre a Zabbix de recuperer des informations detaillees sur les serveurs Linux.

Procedure realisee

- Installer le paquet zabbix-agent sur SRV-GLPI01.
- Editer le fichier de configuration de l agent.
- Renseigner Server=192.168.20.20.
- Renseigner ServerActive=192.168.20.20 si l agent actif est utilise.
- Renseigner Hostname=SRV-GLPI01.
- Redemarrer l agent.

Validation

- Le port agent est joignable depuis Zabbix si autorise.
- L hote SRV-GLPI01 remonte des donnees dans Zabbix.

```
apt install zabbix-agent -y
nano /etc/zabbix/zabbix_agentd.conf
# Server=192.168.20.20
# Hostname=SRV-GLPI01
systemctl restart zabbix-agent
systemctl enable zabbix-agent
```

9.2 Supervision du serveur Active Directory

Objectif

Superviser le controleur de domaine Windows.

Procedure realisee

- Installer l agent Zabbix Windows sur SRV-AD01.
- Configurer le serveur Zabbix : 192.168.20.20.
- Configurer le nom de l hote : SRV-AD01.
- Ouvrir les flux firewall necessaires entre Zabbix et le serveur Windows.
- Ajouter l hote dans Zabbix avec un template Windows.
- Verifier la remontee CPU, RAM et disque.

Validation

- SRV-AD01 apparait disponible dans Zabbix.
- Les metriques systeme remontent correctement.

9.3 Supervision de pfSense

Objectif

Verifier la disponibilite du firewall et des passerelles reseau.

Procedure realisee

- Ajouter pfSense dans Zabbix comme hote.
- Configurer une supervision ICMP simple sur les passerelles 192.168.10.1, 192.168.20.1 et 192.168.30.1.
- Optionnellement, activer SNMP sur pfSense pour remonter plus de metriques.
- Associer un template ICMP ou SNMP selon la configuration retenue.

Validation

- Zabbix detecte si une passerelle devient indisponible.
- Les temps de reponse ICMP sont visibles dans les graphiques.

Element supervise	Methode	Informations surveillees
SRV-AD01	Agent Zabbix Windows + ICMP	Disponibilite, CPU, RAM, disque, services Windows
SRV-GLPI01	Agent Zabbix Linux + HTTP	Disponibilite, charge, espace disque, service web Apache
SRV-ZBX01	Agent local Zabbix	Etat du serveur de supervision
pfSense	ICMP / SNMP optionnel	Disponibilite des passerelles et latence

10. Tests de validation

La validation de l'infrastructure a ete realisee en plusieurs etapes afin de confirmer le bon fonctionnement du domaine, du DNS, du DHCP, de GLPI, de LDAP et de Zabbix.

Test	Commande ou action	Resultat attendu
Connectivite AD	ping 192.168.20.10	Le controleur de domaine repond
Resolution DNS	nslookup alex.local	Le DNS retourne le serveur AD
DHCP client	ipconfig /renew	Le poste obtient une IP en 192.168.10.x
Jonction domaine	Joindre le domaine alex.local	Le poste rejoint le domaine
Application GPO	gpupdate /force	Fond d ecran et lecteur reseau appliques
Acces GLPI	http://192.168.30.10/glpi	L interface GLPI s affiche
LDAP GLPI	Test connexion LDAP	La connexion a l AD est reussie
Zabbix	Tableau de bord Zabbix	Les hotes supervises sont disponibles

```
ipconfig /all
ipconfig /renew
nslookup alex.local
gpupdate /force
gpresult /r
ping 192.168.20.10
ping 192.168.30.10
ping 192.168.20.20
```

11. Difficultes rencontrees et resolutions

Difficulte	Cause possible	Resolution appliquee
Le client ne recoit pas d adresse DHCP	Serveur DHCP dans un autre VLAN	Activation du relais DHCP sur pfSense vers 192.168.20.10
Impossible de joindre le domaine	DNS client incorrect	Configuration du DNS client vers 192.168.20.10
GLPI ne se connecte pas a LDAP	Flux bloque entre DMZ et VLAN serveurs	Autorisation TCP 389 et DNS vers le controleur de domaine
GPO non appliquee	Utilisateur dans mauvaise OU ou replication lente	Verification du lien GPO et gpupdate /force
Agent Zabbix indisponible	Firewall ou mauvais Hostname	Verification de la configuration agent et des regles firewall
Apache ne charge pas GLPI	Permissions incorrectes	Correction des droits www-data sur le dossier GLPI

Ces difficultes ont ete resolues par des tests progressifs : verification IP, ping, resolution DNS, journaux Windows, logs Apache, logs GLPI et etat des services Linux.

12. Conclusion

Cette seconde partie du projet complete l'infrastructure reseau mise en place precedemment. Active Directory centralise l'authentification, le DNS et le DHCP. GLPI apporte une solution de gestion de parc et de support, connectee a l'annuaire via LDAP. Zabbix permet de superviser les serveurs et les equipements critiques afin d'ameliorer la disponibilite de l'infrastructure.

L'ensemble forme une architecture coherente et professionnelle : segmentation reseau, services systeme centralises, gestion de parc, authentification LDAP et supervision. Cette solution est evolutive et peut etre enrichie par des sauvegardes, des certificats TLS, une supervision SNMP plus complete et une politique de durcissement des serveurs.

Synthese des competences mobilisees

Administration systeme Windows Server, services reseau DNS/DHCP, gestion Active Directory, GPO, administration Linux, deploiement web, base de donnees, integration LDAP, supervision, securisation des flux inter-VLAN et validation technique.