

1. Active Directory	2
1.1) Hyperviseur de type 1 Proxmox	2
1.2) Domaine M2L3/DNS/DHCP	4
1.3) Script powershell importation des utilisateurs	7
1.4) Redondance active directory et serveur à basculement DHCP	8
1.5) Partages réseaux	15
2. Serveurs accessibles à distance	16
2.1) WS2019 accessibles via RDP	16
2.2) GLPI, Zabbix, Proxmox,HaProxy accessibles via SSH	17
3. GLPI	19
3.1) Installation de GLPI	19
3.2) Installation de GLPI Agent sur les postes utilisateurs	24
3.3) Intégration LDAP	25
3.4) Redondance Master-Master de la base de données	26
3.5) Test de la réplication	32
3.6) Modification du fichier 000-default.conf	33
4. Sécurité du système	33
4.1) Supervision via Zabbix	33
4.1.1) Modification du fichier zabbix_server.conf	35
4.1.2) On redémarre les services zabbix-server, zabbix-agent et apache2	36
4.1.3) Interface de Zabbix	36
4.1.4) Ajout d'un client Windows 10	37
4.1.5) Superviser notre infrastructure	39
4.1.6) Supervision du routeur	40
4.1.7) Réalisations des tests	41
4.2) Solution d'analyse de paquets	42
4.2.1) Installation de Wireshark	42
4.2.2) Installation de NpCap afin de réaliser des captures	42
4.2.3) Sélection de l'interface réseau	43
4.2.4) Analyse de paquets sur notre infrastructure	43
4.3) Mise en place d'un IDS	43
4.3.1) Installation du package Snort	43
4.3.2) Récupération d'un token sur le site officiel de Snort	44
4.3.3) Mise en place des règles	44
4.3.4) Activation de l'interface WAN	46
4.3.4) Détection des intrusions	46
4.4) Système de logs du SI	46
4.4.1) Installation de Visual Syslog Server	47
4.4.2) Récupération des logs sous Linux	48

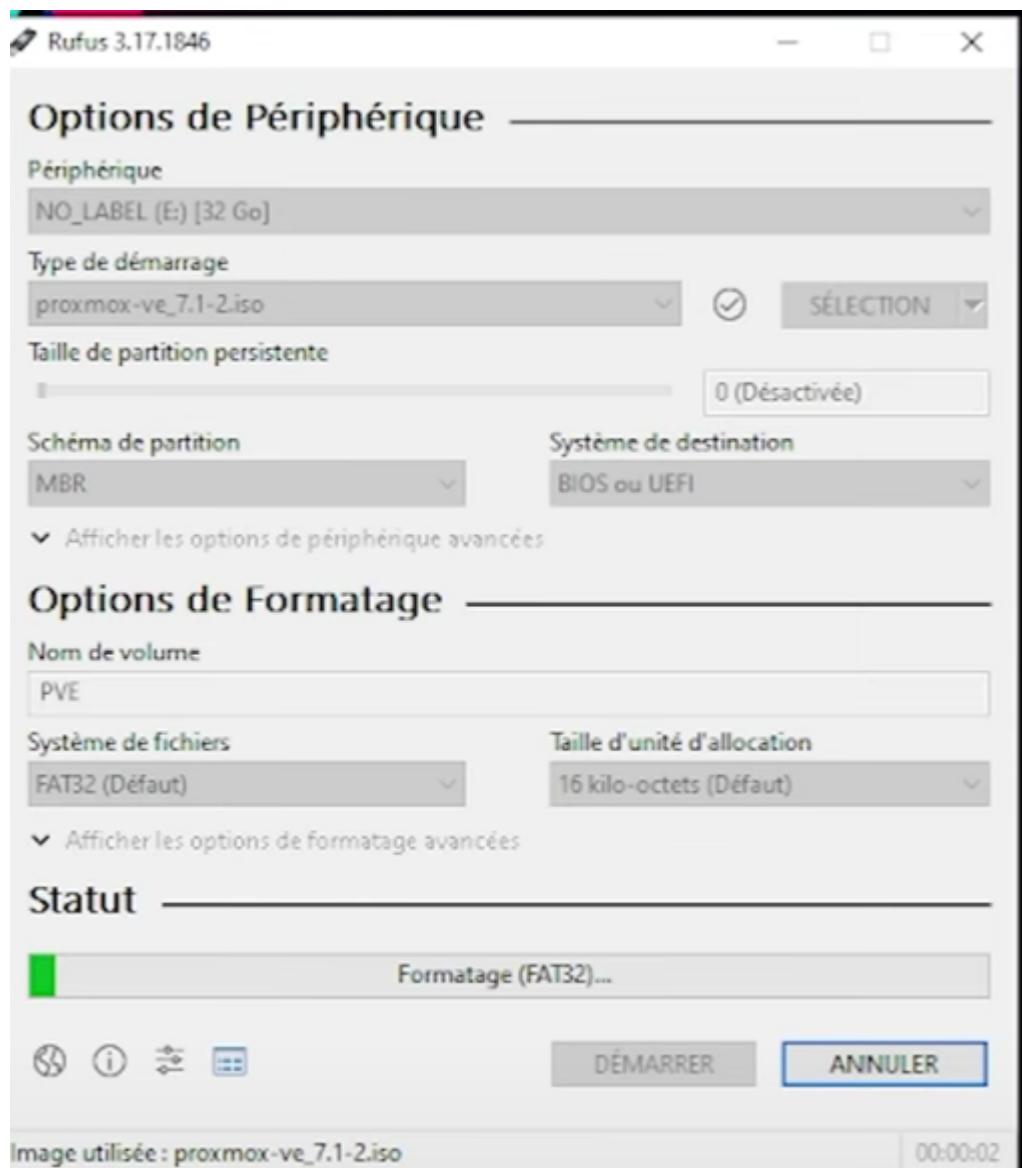
1. Active Directory

1.1) Hyperviseur de type 1 Proxmox

On sélectionne un ISO de Proxmox



On crée une clé bootable contenant Proxmox à l'aide du logiciel Rufus



On insère la clé USB qui contient Proxmox sur notre futur serveur.

Proxmox VE 7.1 (iso release 2) - <https://www.proxmox.com/>



Install Proxmox VE
Install Proxmox VE (Debug mode)
Rescue Boot
Test memory (Legacy BIOS)

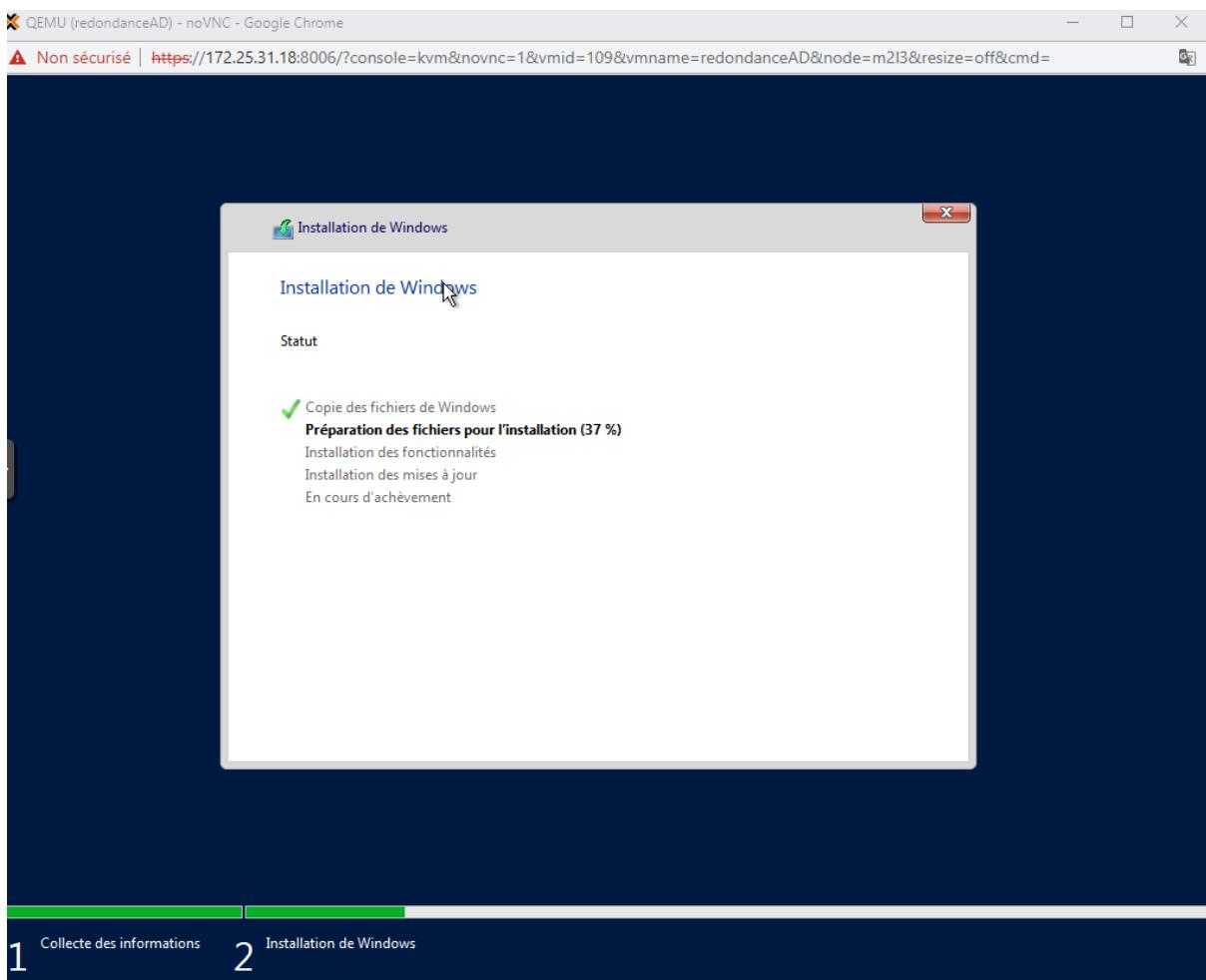
On sélectionne une adresse IP et on laisse l'installation se faire.

The screenshot shows the Proxmox VE interface. On the left, there's a sidebar titled "Server View" with a tree view of "Datacenter" and "Node 'm2i3'". Under "Node 'm2i3'", there are several entries: 100 (glpi1), 101 (AD), 102 (zabbix), 103 (HAProxy), 104 (PFSense), 105 (OwnCloud), 106 (glpi2clone), 107 (kali), 108 (cloneGlpi2), 111 (toip), local (m2i3), and local-lvm (m2i3). On the right, there's a table titled "Search" with columns: Type, Description, Disk usage..., Memory us..., CPU usage, Uptime, Host CPU ..., and Host Mem... . The table lists various VMs and their resource usage. At the top, there are tabs for "Documentation", "Create VM", and "Create CT".

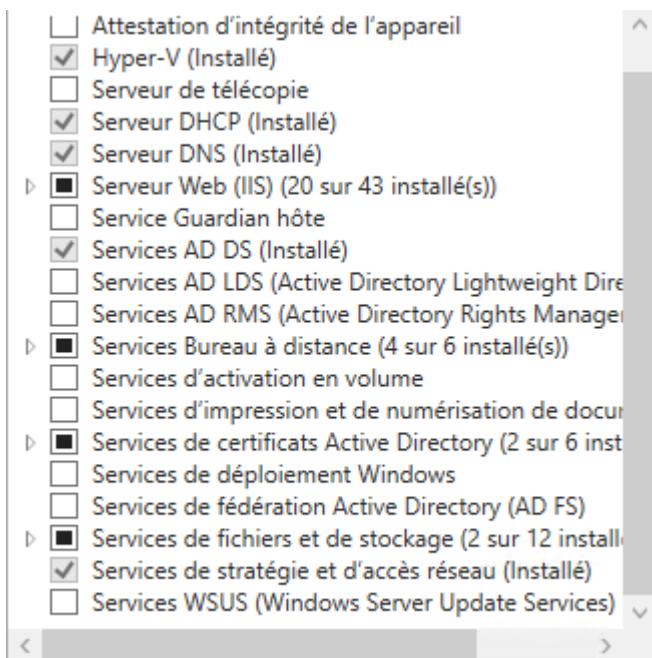
Une fois l'installation terminée, nous sommes prêts à créer des machines virtuelles.
Dorénavant, nous allons installer notre contrôleur de domaine.

1.2) Domaine M2L3/DNS/DHCP

Installation de Windows Serveur 2019



Installation des services AD/DNS/DHCP



Création du contrôleur de domaine

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
Principal-AD

Configuration de déploiement...

- Options du contrôleur de domaine
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la configuration
- Installation
- Résultats

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

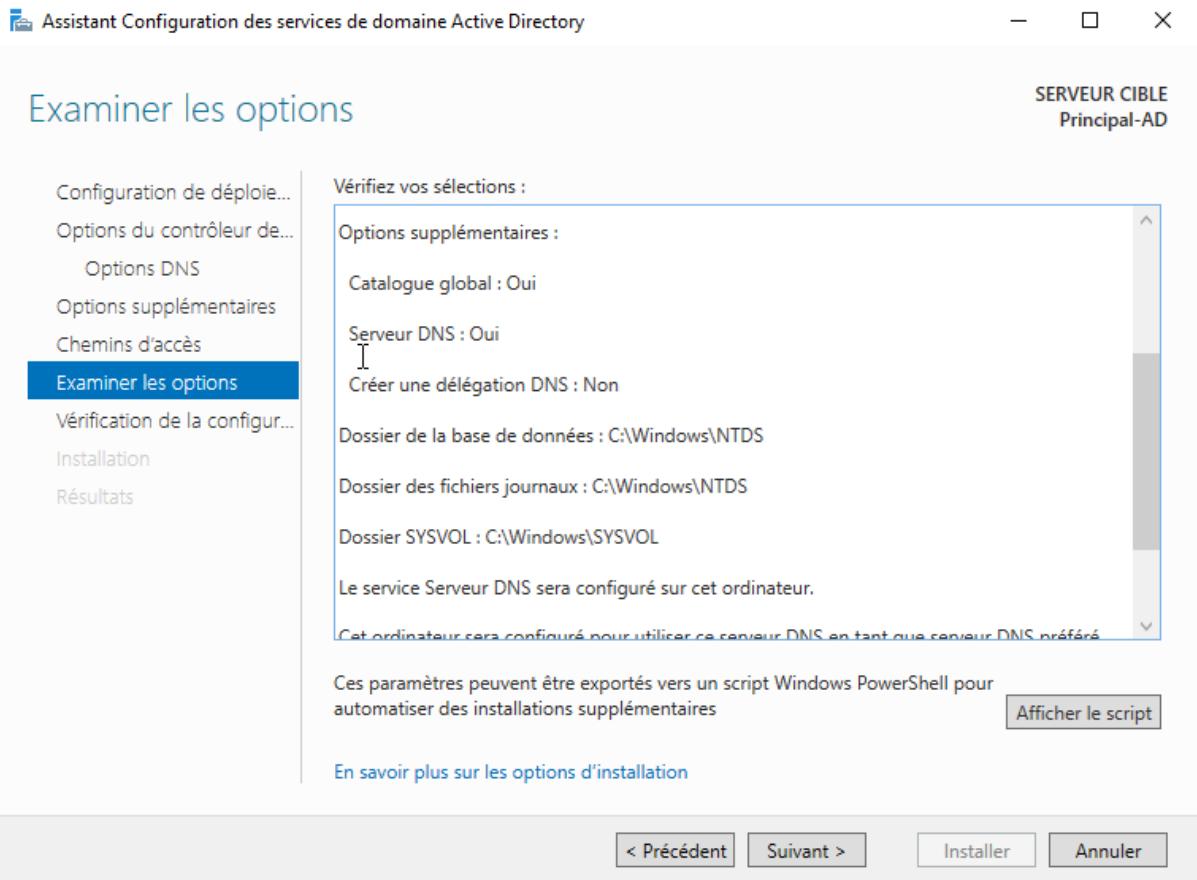
Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine : m2l3.lan

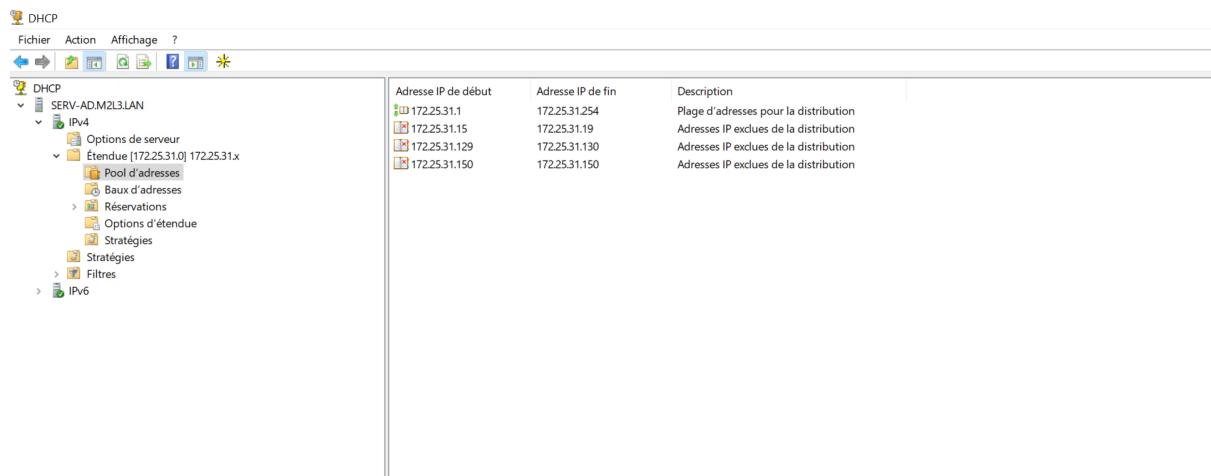
En savoir plus sur les configurations de déploiement

< Précédent Suivant > Installer Annuler



Création des utilisateurs

Étendue DHCP



Enregistrement DNS

The screenshot shows the Windows Server DNS management console. The left pane shows a tree structure with 'DNS', 'SERV-AD.M2L3.LAN', 'Zones de recherche directe', 'M2L3.LAN', 'Zones de recherche inversée', and 'Redirecteurs conditionnel'. The right pane displays a table of registered hosts:

Nom	Type	Données	Horodateur
_msdcs	Source de nom (SOA)	[651] serv-ad.m2l3.lan, hos...	statique
_sites	Serveur de noms (NS)	serv-ad.m2l3.lan.	statique
_tcp	Hôte (A)	172.25.31.129	04/05/2023 08:00:00
_udp	Hôte (A)	172.25.31.125	statique
DomainDnsZones	Hôte (A)	172.25.31.12	20/04/2023 06:00:00
ForestDnsZones	Hôte (A)	172.25.31.150	statique
(identique au dossier parent)	Hôte (A)	172.25.31.16	statique
asterisk	Hôte (A)	172.25.31.17	statique
DESKTOP-U7C1CR1	Hôte (A)	172.25.31.13	09/05/2023 11:00:00
glpi	Hôte (A)	172.25.31.10	statique
glpi1	Hôte (A)	172.25.31.11	statique
glpi2	Hôte (A)	172.25.31.12	statique
Hugo	Hôte (A)	172.25.31.13	04/05/2023 08:00:00
PC-CALVYN	Hôte (A)	172.25.31.14	statique
pfSense	Hôte (A)	172.25.31.15	10/05/2023 10:00:00
Redondance-AD	Hôte (A)	172.25.31.16	statique
serv-ad	Hôte (A)	172.25.31.17	statique
tplinkap	Hôte (A)	172.25.31.18	statique
zabbix	Hôte (A)	172.25.31.19	statique

1.3) Script powershell importation des utilisateurs

On importe les utilisateurs à partir d'un fichier CSV à l'aide du script suivant.

```

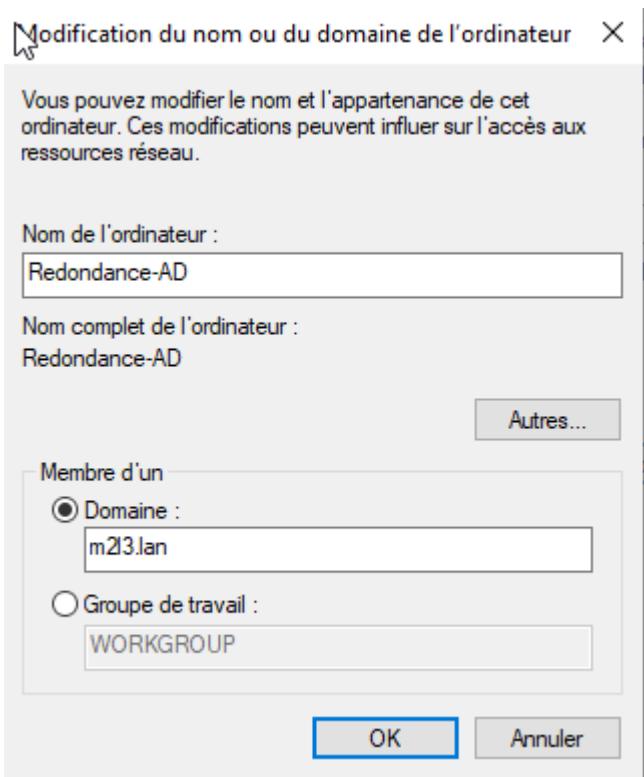
> MONSCRIPT.ps1 9+
G: > Mon Drive > BTS > AP > 2ème année > > MONSCRIPT.ps1 > ...
1  Install-Module -Name ImportExcel
2  $CSVFile="C:\Users\calvyn\Downloads\ListeUserPPE.xlsx"
3  $CSVData=Import-Excel -Path $CSVFile
4
5  foreach($Utilisateur in $CSVData){
6      $Domain = "M2L3"
7      $EXT = "LAN"
8      $Server = "SERV-AD.M2L3.LAN"
9      $UserID = $Utilisateur.ID
10     $UserDescription = $Utilisateur.IDescription
11     $UserNom= $Utilisateur.Nom
12     $UserPrenom=$Utilisateur.Prenom
13     $UserLogin = ($UserNom).Substring(0,1).ToLower() + $UserPrenom.ToLower()
14     $UserSecteur = $Utilisateur.Secteur
15     $UserType=$Utilisateur.Type
16     $UserDate_Fin=$Utilisateur.DateFin
17     $UserTel = $Utilisateur.Tel
18     $UserPays = $Utilisateur.Pays
19     $UserVille = $Utilisateur.Ville
20     $UserCP = $Utilisateur.CP
21     $UserRue = $Utilisateur.Rue
22     $UserMDP = "P@ssword3411!"
23
24 #Vérifier la présence de l'user dans l'AD
25 if(Get-AdUser -Filter {SamAccountName -eq $UserLogin})
26 {
27     Write-Warning "L'identifiant $UserLogin existe déjà dans l'AD"
28 }
29 else
30 [
31     New-ADUser -Name "$UserNom $UserPrenom" ` 
32             -DisplayName "$UserNom $UserPrenom" ` 
33             -GivenName $UserNom ` 
34             -Surname $UserPrenom ` 
35             -SamAccountName $UserLogin ` 
36             -UserPrincipalName "$UserLogin@m2l3.lan" ` 
37             -Title $UserSecteur ` 
38             -Path "OU=MesUtilisateurs, DC=M2L3, DC=LAN" ` 
39             -AccountPassword(ConvertTo-SecureString $UserMDP -AsPlainText -Force) ` 
40             -Enabled $true ` 
41             -ChangePasswordAtLogon $true
42
43
44
45     Write-Output "Création de l'user : $UserLogin ($UserPrenom $UserNom) avec l'ID $UserID"
46

```

1.4) Redondance active directory et serveur à basculement DHCP

Installation de Windows Serveur 2019

On joint le domaine M2L3 avec le serveur de redondance Redondance-AD



Modification du nom ou du domaine de l'ordinateur X



Bienvenue dans le domaine m2l3.lan.

OK

On ajoute un contrôleur de domaine au domaine existant : M2L3.

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
Redondance-AD.M2L3.LAN

Configuration de déploie...

- Options du contrôleur de...
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la config...

Installation

Résultats

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine : M2L3.LAN

Fournir les informations d'identification pour effectuer cette opération

M2L3\cmorin (Utilisateur actuel)

[En savoir plus sur les configurations de déploiement](#)

< Précédent Suivant > Installer Annuler

Assistant Configuration des services de domaine Active Directory

Options supplémentaires

SERVEUR CIBLE
Redondance-AD.M2L3.LAN

Configuration de déploie...

- Options du contrôleur de...
- Options DNS

Options supplémentaires

- Chemins d'accès
- Examiner les options
- Vérification de la config...

Installation

Résultats

Spécifier les options d'installation à partir du support (IFM)

Installation à partir du support

Spécifier des options de réplication supplémentaires

Répliquer depuis : SERV-AD.M2L3.LAN

[En savoir plus sur d'autres options](#)

< Précédent Suivant > Installer Annuler

Le contrôleur de domaine est répliqué.

The screenshot shows the Windows Server Manager interface with the following components:

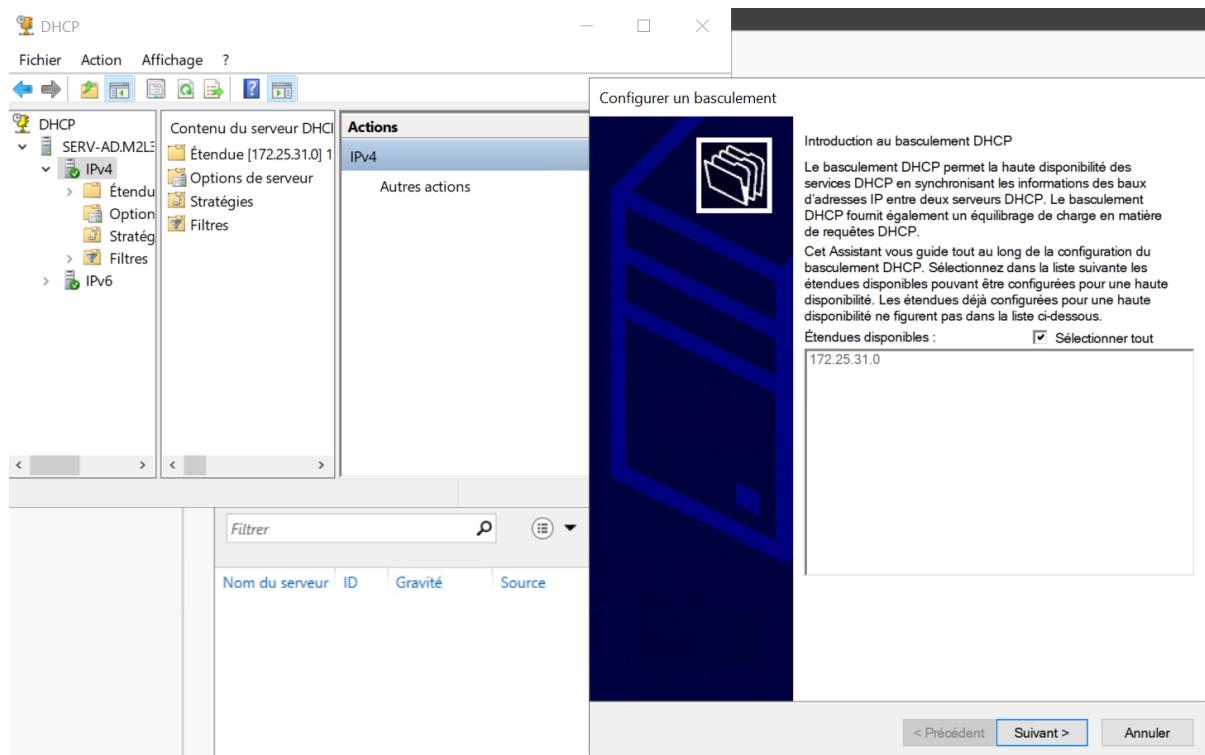
- Gestionnaire de serveur ▸ AD DS**: The main navigation pane on the left lists several services: Tableau de bord, Serveur local, Tous les serveurs, AD DS (selected), DHCP, DNS, and Services de fichiers et de dossiers.
- SERVEURS**: A list of servers under "Tous les serveurs". One server is listed: REDONDANCE-AD (172.25.31.130) - En ligne - Compteurs de performances non démarré (Last updated: 10/05/2023 11:30:31) - Activation de Windows Non activé.
- Utilisateurs et ordinateurs Active Directory**: A tree view of Active Directory structures: Utilisateurs et ordinateurs Active, Requêtes enregistrées, M2L3.LAN (selected), BuiltIn, Computers, connecteurLdap, Domain Controllers, ForeignSecurityPrincipal, Groups, Managed Service Account, MesUtilisateurs (selected), MonAD, and Users. A table lists users with columns: Nom (Name), Type (Type), and Description.

Nom	Type	Description
Aidan Abbot	Utilisateur	
Alan Carly	Utilisateur	
Allen Fallon	Utilisateur	
Alyssa Forrest	Utilisateur	
Angelica Re...	Utilisateur	
Aretha Illana	Utilisateur	
Ashton Alle...	Utilisateur	
Aurélien Gall...	Utilisateur	
Avram Arma...	Utilisateur	
Basia Calvin	Utilisateur	
Bradley Otto	Utilisateur	
Brendan Dris...	Utilisateur	
Brenden Ger...	Utilisateur	
Calvyn Morin	Utilisateur	
Cameron Ca...	Utilisateur	
Cameron Gary	Utilisateur	
Carly Addison	Utilisateur	
Carson Skyler	Utilisateur	
Cathleen Bre...	Utilisateur	
Chanda Jasper	Utilisateur	

- Gestionnaire DNS**: The DNS management console showing zones and records. The tree view includes: DNS, Redondance-AD.M2L3.LAN, Zones de recherche directe (_msdcs.M2L3.LAN, M2L3.LAN), Zones de recherche inversée, Points d'approbation, and Redirecteurs conditionnels. The table lists DNS records with columns: Nom (Name), Type (Type), Données (Data), and Horodatage (Last updated).

Nom	Type	Données	Horodatage
DomainDnsZones	Source de nom (SOA)	[665], redondance-ad.m2l3.lan.	statique
ForestDnsZones	Serveur de noms (NS)	redondance-ad.m2l3.lan.	statique
(identique au dossier parent)	Serveur de noms (NS)	serv-ad.m2l3.lan.	statique
(identique au dossier parent)	Hôte (A)	172.25.31.130	10/05/2023 11:30:31
(identique au dossier parent)	Hôte (A)	172.25.31.129	04/05/2023 11:30:31
asterisk	Hôte (A)	172.25.31.125	statique
DESKTOP-U7C1CR1	Hôte (A)	172.25.31.2	20/04/2023 11:30:31
glpi	Hôte (A)	172.25.31.150	statique
glpi1	Hôte (A)	172.25.31.16	statique
glpi2	Hôte (A)	172.25.31.17	statique
Hugo	Hôte (A)	172.25.31.3	09/05/2023 11:30:31
PC-CALVYN	Hôte (A)	172.25.31.5	04/05/2023 11:30:31
pfsense	Hôte (A)	172.25.31.10	statique
redondance-ad	Hôte (A)	172.25.31.130	statique
serv-ad	Hôte (A)	172.25.31.129	statique
tplinkap	Hôte (A)	172.25.31.1	statique
zabbix	Hôte (A)	172.25.31.99	statique

Serveur de basculement DHCP



Configurer un basculement

Créer une relation de basculement



Créer une relation de basculement avec le partenaire redondance-ad

Nom de la relation :

serv-ad.m2l3.lan-redondance-ad

Délai de transition maximal du client
(MCLT) :

1 heures 0 minutes

Mode :

Équilibrage de charge

Pourcentage d'équilibrage de charge

Serveur local :

50 %

Serveur partenaire :

50 %

Intervalle de basculement d'état :

60 minutes

Activer l'authentification du message

Secret partagé :

< Précédent

Suivant >

Annuler

Configurer un basculement

?

X

Progression de la configuration du basculement.

Le journal ci-dessous montre la progression des diverses tâches de configuration du basculement, ainsi que les erreurs rencontrées.

Ajouter des étendues sur le serveur partenaireRéussite
Désactiver des étendues sur le serveur partenaireRéussite
Création de la config. du basculement sur le serveur partenaireRéussite
Création de la configuration du basculement sur le serveur hôteRéussite
Activer des étendues sur le serveur partenaireRéussite
Réussite de la configuration du basculement.



Fermer

Le cluster DHCP est en place.

The screenshot shows the Windows Server Manager interface. On the left, there's a navigation pane with 'DHCP' selected. Under 'DHCP', there are two servers listed: 'redondance-ad' and 'SERV-AD.M2L3.LAN'. Each server has an 'IPv4' node expanded, showing various DHCP scopes and configurations. On the right, a detailed table lists all active DHCP leases. The table columns include: Adresse IP du client, Nom, Expiration du bail, Type, ID unique, Description, Protection d'accès réseau, and Expiration de la période. The leases shown are:

Adresse IP du client	Nom	Expiration du bail	Type	ID unique	Description	Protection d'accès réseau	Expiration de la période
172.25.31.1	asterisk.M2L3.LAN	17/05/2023 08:59:13	DHCP	2943d5550...	Accès complet	N/D	
172.25.31.2	Maks.M2L3.LAN	17/05/2023 09:19:15	DHCP	eaaeb423f...	Accès complet	N/D	
172.25.31.3	Hugo.M2L3.LAN	17/05/2023 11:25:53	DHCP	10b1fdf54...	Accès complet	N/D	
172.25.31.4		18/05/2023 07:57:03	DHCP	da186ccb2...	Accès complet	N/D	
172.25.31.5	BAD_ADDRESS	17/05/2023 13:37:01	DHCP	051f19ac...	Cette adresse...	Accès complet	N/D
172.25.31.6	S21-de-Aurelien.M2L3.LAN	17/05/2023 13:39:12	DHCP	3ef1c5e2b8...		Accès complet	N/D

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

[Ajouter un serveur](#)

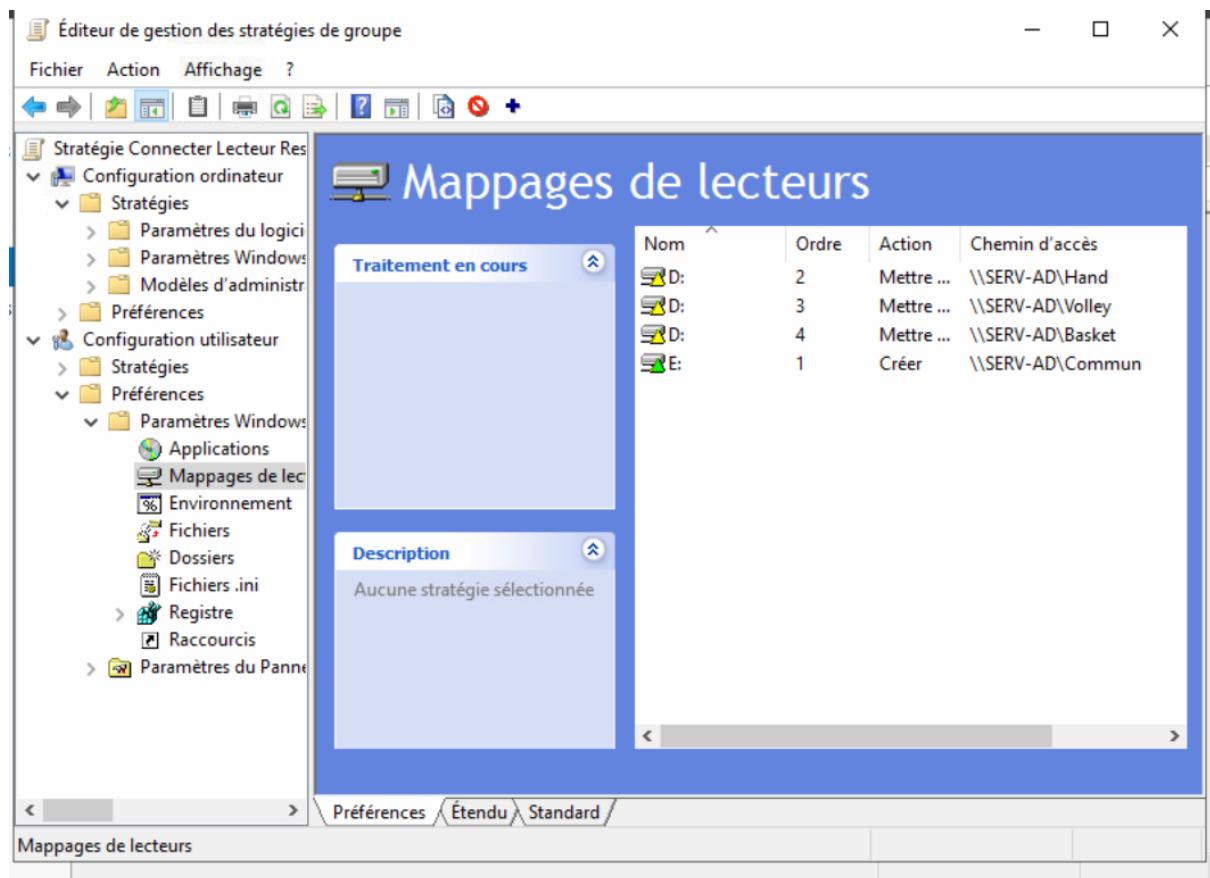
Réutiliser les relations de basculement existantes configurées avec ce serveur (je cas échéant).

[<< Précédent](#)

[<> Suivant >](#)

[Annuler](#)

1.5) Partages réseaux



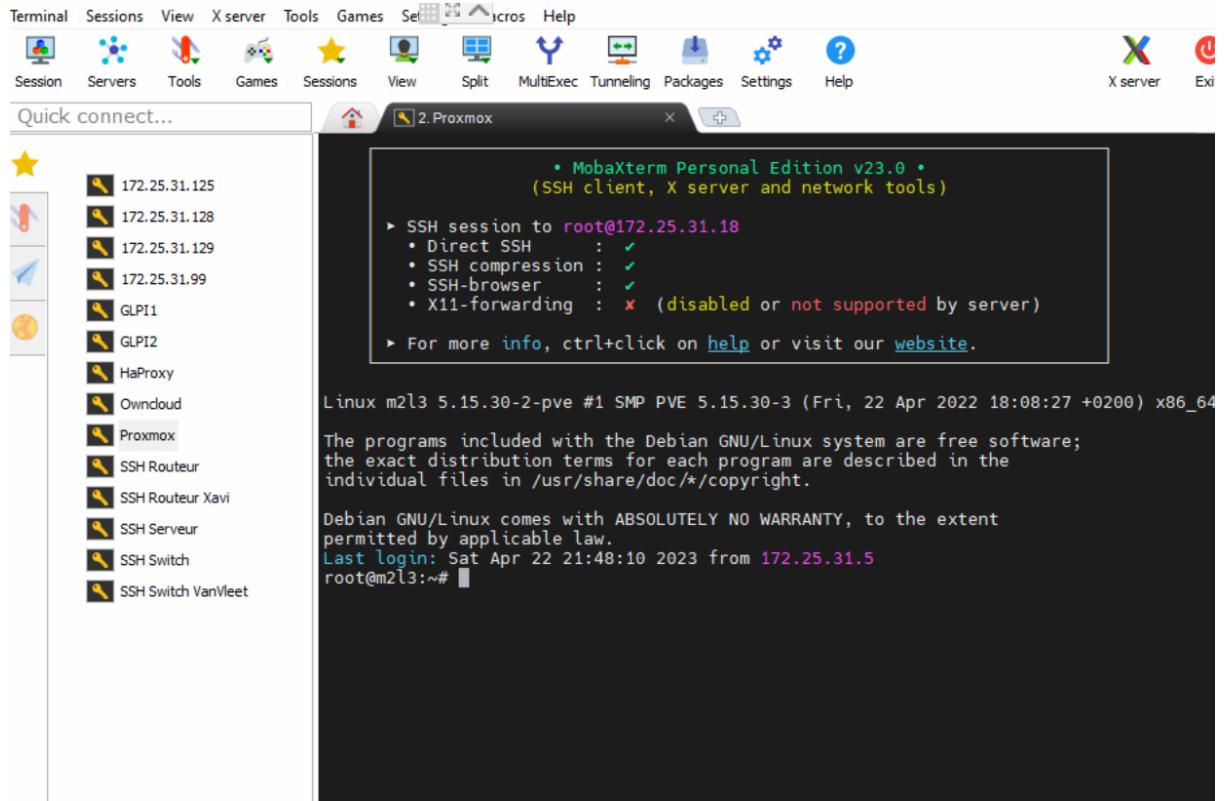
2. Serveurs accessibles à distance

2.1) WS2019 accessibles via RDP



2.2) GLPI, Zabbix, Proxmox, HaProxy accessibles via SSH

Proxmox :



HaProxy :

```
C:\Users\calvyn>ssh calvyn@172.25.31.150
calvyn@172.25.31.150's password:
Linux HaProxy 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May  9 14:36:31 2023 from 172.25.31.5
calvyn@HaProxy:~$
```

GLPI1 :

```
• MobaXterm Personal Edition v22.3 •
(SSH client, X server and network tools)

▶ SSH session to calvyn@172.25.31.16
• Direct SSH      : ✓
• SSH compression : ✓
• SSH-browser     : ✓
• X11-forwarding  : ✓ (remote display is forwarded through SSH)

▶ For more info, ctrl+click on help or visit our website.
```

Linux glpi1 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May 9 14:37:06 2023 from 172.25.31.5
calvyn@glpi1:~\$ █

GLPI2:

```
• MobaXterm Personal Edition v22.3 •
(SSH client, X server and network tools)

▶ SSH session to calvyn@172.25.31.17
• Direct SSH      : ✓
• SSH compression : ✓
• SSH-browser     : ✓
• X11-forwarding  : ✓ (remote display is forwarded through SSH)

▶ For more info, ctrl+click on help or visit our website.
```

Linux glpi2 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Tue May 9 14:37:04 2023 from 172.25.31.5
calvyn@glpi2:~\$ █

3. GLPI

3.1) Installation de GLPI

Fiche AP GLPI,  **INSTALLATION GLPI (DEBIAN 11 & GLPI 10.0.2)**

Installation de Perl

```
root@glpi1:~# apt install perl -y
```

Installation des dépendances PHP

```
root@glpi1:~# apt install php-ldap php-imap php-apcu php-xmlrpc php-cas php-mysqli php-mbstring php-curl php-gd php-simplexml php-xml php-intl php-zip php-bz2 -y
```

Installation d'Apache

```
root@glpi1:~# apt install apache2
```

On redémarre le service Apache

```
root@glpi1:~# systemctl reload apache2
```

On télécharge les paquets de GLPI

```
root@glpi1:/tmp# wget https://github.com/glpi-project/glpi/releases/download/10.0.7/glpi-10.0.7.tgz
```

On les décomprime

```
root@glpi1:/tmp# tar xzf glpi-10.0.7.tgz -C /var/www/html
```

On accorde les droits aux fichiers de GLPI

```
root@glpi1:/tmp# chown -R www-data:www-data /var/www/html/glpi
root@glpi1:/tmp# chmod -R 775 /var/www/html/glpi
```

On installe MariaDB

```
root@glpi1:/tmp# apt install mariadb-server
```

Création de la BDD glpidb

```
root@glpi1:/tmp# mysql -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.19-MariaDB-0+deb11u2 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database glpidb;
```

Création de l'utilisateur glpiuser

```
MariaDB [(none)]> create user glpiuser@localhost identified by '1234';
Query OK, 0 rows affected (0,004 sec)
```

On accorde tous les priviléges à l'utilisateur glpiuser sur la BDD glpidb

```
MariaDB [(none)]> grant all privileges on glpidb.* to glpiuser@localhost;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0,000 sec)
```

Installation de GLPI



A screenshot of the "Début de l'installation" (Initial Installation) step of the GLPI Setup process. The title "GLPI SETUP" is at the top. A callout box on the left contains an information icon and the text: "Installation ou mise à jour de GLPI. Choisissez 'Installation' pour une nouvelle installation de GLPI. Choisissez 'Mise à jour' pour lancer la mise à jour de votre version de GLPI à partir d'une version antérieure." Below the callout are two yellow buttons: "Installer" with a download icon and "Mettre à jour" with an update icon.

A screenshot of the "Étape 1 Configuration de la connexion à la base de données" (Step 1: Database connection configuration) step. The title "GLPI SETUP" is at the top. It asks for "Serveur SQL (MariaDB ou MySQL)" and shows the input field "localhost". It also asks for "Utilisateur SQL" and shows the input field "glpiuser". It asks for "Mot de passe SQL" and shows the input field with four dots ("****"). At the bottom is a yellow "Continuer >" button.

glpi

GLPI SETUP

Étape 2

Test de connexion à la base de données

Connexion à la base de données réussie

Veuillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

glpidb

Continuer >



Installation du GLPI sur le second serveur Web, avec la mise en place de la redondance de BDD

← → C Non sécurisé | 172.25.31.17/install/install.php

Raccourci serveurs

glpi

GLPI SETUP

Étape 2

Test de connexion à la base de données

Connexion à la base de données réussie

Veuillez sélectionner une base de données :

Créer une nouvelle base ou utiliser une base existante :

glpi

Continuer >



Non sécurisé | 172.25.31.16/front/central.php

Raccourci serveurs

GLPI

Accueil

Tableau de bord

- Pour des raisons de sécurité, veuillez changer le mot de passe par défaut pour le(s) utilisateur(s) : glpi post-only tech normal
- Pour des raisons de sécurité, veuillez supprimer le fichier : install/install.php
- La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à la documentation d'installation pour plus de détails.

Central

Logiciel (0), Ordinateur (0), Matériel réseau (0), Téléphone (0), Licence (0), Moniteur (0), Balle (0), Imprimante (0)

Aucune donnée trouvée

Ordinateurs par Fabricant, Moniteurs par Modèle, Matériels réseau par Type

Utilisateurs (4), Groupe (0), Fournisseur (0), Document (0), Entité (1), Profils (8), Base de connaissance (0), Projet (0)

Statuts des tickets par mois

Ticket (0), Tickets en retard (0), Problème (0), Changement (0)

Aucune donnée trouvée

Aucune donnée trouvée

Aucune donnée trouvée

Aucune donnée trouvée

Non sécurisé | 172.25.31.16/front/ticket.php

Raccourci serveurs

GLPI

Accueil / Assistance / Tickets / + Ajouter / Rechercher / Listes / Gabarits / Kanban global / Tickets attendant votre validation

Rechercher / Super-Admin

Ticket	Tickets entrants	Tickets en attente	Tickets assignés	Tickets planifiés	Tickets résolus	Tickets fermés
1	0	0	1	0	0	0

Caractéristiques - Statut : est / Non résolu

Actions

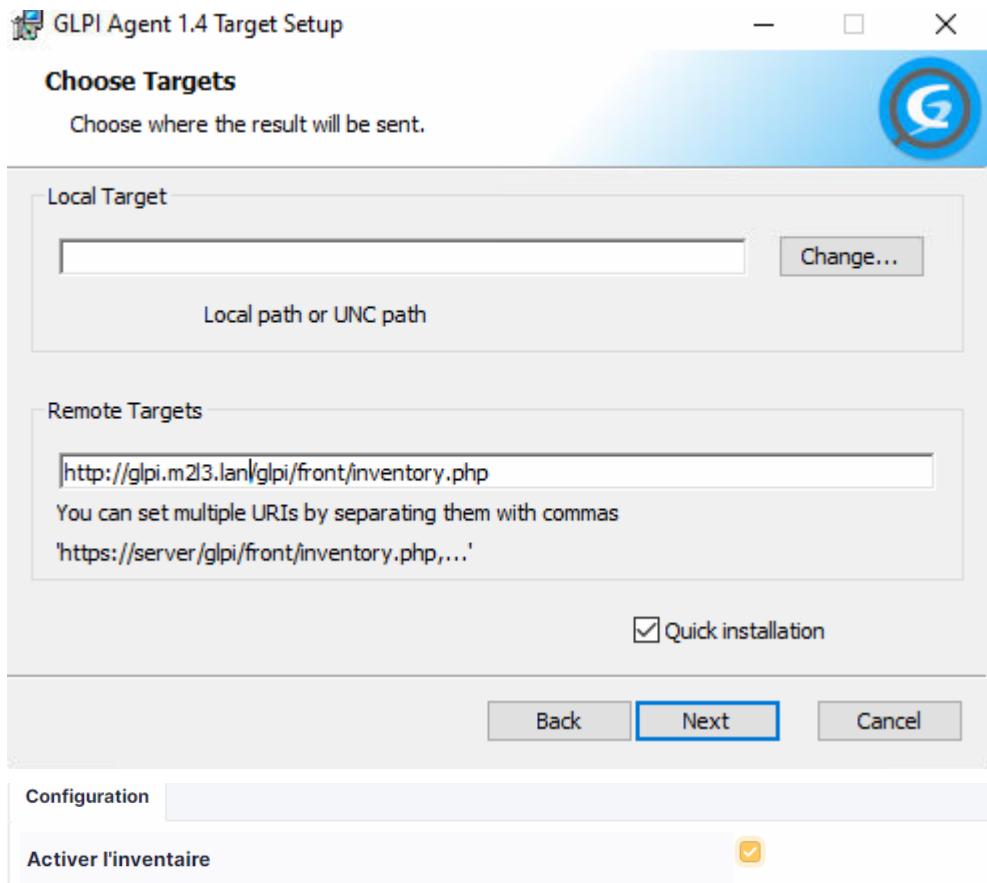
ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE	PRIORITÉ	DEMANDEUR - DEMANDEUR	ATTRIBUÉ À - TECHNICIEN	CATÉGORIE	TTR
1	sallut	En cours (Attribué)	2023-05-17 11:11	2023-05-17 11:11	Moyenne	glpi i	glpi i		

20 lignes / page

The screenshot shows the GLPI ticket management interface. On the left is a sidebar with a navigation menu. The main area has a dashboard with six colored boxes showing ticket counts: 1 Ticket (yellow), 0 Tickets entrants (green), 0 Tickets en attente (orange), 1 Tickets assignés (light blue), 0 Tickets planifiés (dark blue), and 0 Tickets résolus (grey). Below the dashboard is a search bar and a table of tickets. The table has columns: ID, TITRE, STATUT, DERNIÈRE MODIFICATION, DATE D'OUVERTURE, PRIORITÉ, DEMANDEUR - DEMANDEUR, and ATTRIBUÉ À - TECH. One ticket is listed: ID 1, TITRE 'salut', STATUT 'En cours (Attribué)', DERNIÈRE MODIFICATION '2023-05-17 11:11', DATE D'OUVERTURE '2023-05-17 11:11', PRIORITÉ 'Moyenne', DEMANDEUR 'glpi i', and ATTRIBUÉ À 'glpi i'. The table also shows '20 lignes / page' and 'De 1 à 1 sur 1 lignes'.

3.2) Installation de GLPI Agent sur les postes utilisateurs





3.3) Intégration LDAP

On entre l'adresse IP du serveur Active Directory ou son nom DNS(SERV-AD.M2L3.LAN).Le port utilisé est le port par défaut du LDAP, le port 389.La baseDN correspond à l'arborescence de l'annuaire LDAP de l'Active Directory.On utilise un compte administrateur pour se connecter à l'annuaire LDAP.

Annuaire LDAP		Annuaire LDAP - SERV-AD.M2L3.LAN		
Tester				
Utilisateurs	Nom	SERV-AD.M2L3.LAN	Dernière modification	2023-05-10 14:30
Groupes	Serveur par défaut	Oui	Actif	Oui
Informations avancées	Serveur	172.25.31.129	Port (par défaut 389)	389
Réplicats	Filtre de connexion			
Historique	BaseDN	OU=MesUtilisateurs,DC=M2L3,DC=LAN		
Tous	Utilisez un compte (pour les connexions non anonymes)	Oui		
	i			
	DN du compte (pour les connexions non anonymes)	Administrateur@m2l3.lan		
	Mot de passe du compte (pour les connexions non anonymes)	<input type="password"/>		
	<input type="checkbox"/> Effacer			
	Champ de l'identifiant	samaccountname	Commentaires	
	Champ de synchronisation			
		<input type="button" value="Supprimer définitivement"/>		<input type="button" value="Sauvegarder"/>

3.4) Redondance Master-Master de la base de données

Fiche AP GLPI, [How to Configure MySQL Master-Slave Replication on Ubuntu | Debinan](#)
[Commande GitHub](#)

Ne pas oublier de créer les fichiers log !

Chaque serveur doit posséder sa propre base de données.

```
root@glpi1:/etc/mysql/mariadb.conf.d# systemctl status mysql
● mariadb.service - MariaDB 10.5.19 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2023-05-17 09:47:06 CEST; 9min ago
    Docs: man:mariadb(8)
          https://mariadb.com/kb/en/library/systemd/
   Process: 19301 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/ mysql
   Process: 19302 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION
   Process: 19304 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] & VAR= _WSREP_START_POSITION
   Process: 19362 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION
   Process: 19364 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
 Main PID: 19348 (mariadb)
   Status: "Taking your SQL requests now ... "
     Tasks: 16 (limit: 1099)
    Memory: 164.1M
      CPU: 3.725s
     CGroup: /system.slice/mariadb.service
             └─19348 /usr/sbin/mariadb

mai 17 09:47:06 glpi1 systemd[1]: Started MariaDB 10.5.19 database server.
mai 17 09:47:06 glpi1 /etc/mysql/debian-start[19366]: Upgrading MySQL tables if necessary...
mai 17 09:47:06 glpi1 /etc/mysql/debian-start[19369]: Looking for 'mariadb' as: /usr/libexec/mysql
mai 17 09:47:06 glpi1 /etc/mysql/debian-start[19369]: Looking for 'mariadb-check' as: /usr/libexec/mysql
mai 17 09:47:06 glpi1 /etc/mysql/debian-start[19369]: This installation of MariaDB is...
mai 17 09:47:06 glpi1 /etc/mysql/debian-start[19369]: There is no need to run mysql_upgrade
mai 17 09:47:06 glpi1 /etc/mysql/debian-start[19369]: You can use --force if you still...
mai 17 09:47:06 glpi1 /etc/mysql/debian-start[19381]: Triggering myisam-recover for a...
mai 17 09:47:19 glpi1 mariadb[19348]: 2023-05-17 9:47:19 30 [Warning] Aborted connection ...
mai 17 09:47:29 glpi1 mariadb[19348]: 2023-05-17 9:47:29 31 [Warning] Aborted connection ...
lines 1-28/28 (END)
```

```
root@glpi2:/etc/apache2/sites-available# systemctl status mariadb
● mariadb.service - MariaDB 10.5.19 database server
  Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: ena
  Active: active (running) since Wed 2023-05-17 09:54:36 CEST; 1min 24s ago
    Docs: man:mariadb(8)
          https://mariadb.com/kb/en/library/systemd/
 Process: 16919 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/
 Process: 16920 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_P
 Process: 16924 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR=
 Process: 16987 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_
 Process: 16990 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCE
 Main PID: 16973 (mariadb)
   Status: "Taking your SQL requests now ... "
     Tasks: 9 (limit: 1099)
    Memory: 77.2M
      CPU: 335ms
     CGroup: /system.slice/mariadb.service
             └─16973 /usr/sbin/mariadb

mai 17 09:54:36 glpi2 mariadb[16973]: Version: '10.5.19-MariaDB-0+deb11u2'  socket:
mai 17 09:54:36 glpi2 systemd[1]: Started MariaDB 10.5.19 database server.
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[16992]: Upgrading MySQL tables if neces
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[16995]: Looking for 'mariadb' as: /usr/
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[16995]: Looking for 'mariadb-check' as:
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[16995]: This installation of MariaDB is
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[16995]: There is no need to run mysql_u
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[16995]: You can use --force if you stil
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[17004]: Checking for insecure root acco
mai 17 09:54:36 glpi2 /etc/mysql/debian-start[17009]: Triggering myisam-recover for a
[lines 1-28/28 (END)]
```

On configure la base de données du serveur maître

On commente la ligne bind-address

```
GNU nano 5.4                               50-server.cnf
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see
#
# this is read by the standalone daemon and embedded servers
[server]
#
# this is only for the mysqld standalone daemon
[mysqld]
#
# * Basic Settings
#
user                      = mysql
pid-file                 = /run/mysqld/mysqld.pid
basedir                  = /usr
datadir                  = /var/lib/mysql
tmpdir                   = /tmp
lc-messages-dir          = /usr/share/mysql
lc-messages              = en_US
skip-external-locking

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address            = 127.0.0.1

#
# * Fine Tuning
#
#key_buffer_size          = 128M
#max_allowed_packet       = 1G
#thread_stack             = 192K
#thread_cache_size        = 8
# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
#myisam_recover_options = BACKUP
#max_connections          = 100
#table_cache               = 64
```

On ajoute ces lignes sur le serveur maître 1

```
[mysqld]

#
# * Basic Settings
#
bind-address = 172.25.31.16
server-id=1
report_host=glpi1
#
log_bin=/var/log/mysql/mariadb-bin
log_bin_index=/var/log/mysql/mariadb-bin.index
#
relay_log=/var/log/mysql/relay-bin
relay_log_index=/var/log/mysql/relay-bin.index
user = mysql
pid-file = /run/mysqld/mysqld.pid
basedir = /usr
datadir = /var/lib/mysql
tmpdir = /tmp
lc-messages-dir = /usr/share/mysql
lc-messages = en_US
skip-external-locking
```

Même chose sur le serveur maître 2

```
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#
bind-address = 172.25.31.17
server-id = 2
report_host = glpi2
log_bin = /var/log/mysql/mariadb-bin
log_bin_index = /var/log/mysql/mariadb-bin.index
relay_log = /var/log/mysql/relay-bin
relay_log_index = /var/log/mysql/relay-bin.index

user = mysql
pid-file = /run/mysqld/mysqld.pid
basedir = /usr
datadir = /var/lib/mysql
tmpdir = /tmp
lc-messages-dir = /usr/share/mysql
lc-messages = en_US
skip-external-locking

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address = 127.0.0.1

#
# * Fine Tuning
#
#key_buffer_size = 128M
```

On crée un utilisateur dédié à la synchronisation des bases de données. On effectue les mêmes commandes sur les 2 serveurs maîtres.

```
MariaDB [(none)]> CREATE USER 'rep_user'@'%' IDENTIFIED BY '1234';
Query OK, 0 rows affected (0,002 sec)

MariaDB [(none)]> GRANT REPLICATION SLAVE ON *.* TO 'rep_user'@'%';
Query OK, 0 rows affected (0,004 sec)
```

On vérifie le statut du serveur maître 1

```
MariaDB [(none)]> show master status;
+-----+-----+-----+
| File | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+-----+-----+-----+
| mariadb-bin.000001 |      772 |           |           |
+-----+-----+-----+
1 row in set (0,000 sec)
```

On vérifie le statut du serveur maître 2

```
MariaDB [(none)]> show master status;
+-----+-----+-----+
| File | Position | Binlog_Do_DB | Binlog_Ignore_DB |
+-----+-----+-----+
| mariadb-bin.000001 |      772 |           |           |
+-----+-----+-----+
1 row in set (0,000 sec)
```

Les positions sont similaires.

On arrête le service slave sur le serveur maître 1.

```
MariaDB [(none)]> stop slave;
Query OK, 0 rows affected, 1 warning (0,000 sec)
```

Sur le premier serveur maître, on implémente la réplication de base de données

```
MariaDB [(none)]> CHANGE MASTER TO
    → MASTER_HOST='172.25.31.16',
    → MASTER_USER='rep_user',
    → MASTER_PASSWORD='1234',
    → MASTER_LOG_FILE='mariadb-bin.000001',
    → MASTER_LOG_POS=772;
Query OK, 0 rows affected (0,037 sec)
```

On relance le service slave

```
MariaDB [(none)]> start slave;
Query OK, 0 rows affected (0,001 sec)
```

La réplication est donc active sur le premier serveur maître.

```

MariaDB [(none)]> start slave;
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> show slave status\G;
***** 1. row *****
    Slave_IO_State: Waiting for master to send event
        Master_Host: 172.25.31.17
        Master_User: rep_user
        Master_Port: 3306
        Connect_Retry: 60
        Master_Log_File: mariadb-bin.000001
    Read_Master_Log_Pos: 772
        Relay_Log_File: relay-bin.000002
        Relay_Log_Pos: 557
    Relay_Master_Log_File: mariadb-bin.000001
        Slave_IO_Running: Yes
        Slave_SQL_Running: Yes

```

On fait la même chose sur le serveur maître 2.

```

MariaDB [(none)]> show slave status\G;
***** 1. row *****
    Slave_IO_State: Waiting for master to send event
        Master_Host: 172.25.31.16
        Master_User: rep_user
        Master_Port: 3306
        Connect_Retry: 60
        Master_Log_File: mariadb-bin.000001
    Read_Master_Log_Pos: 772
        Relay_Log_File: relay-bin.000002
        Relay_Log_Pos: 557
    Relay_Master_Log_File: mariadb-bin.000001
        Slave_IO_Running: Yes
        Slave_SQL_Running: Yes
        Replicate_Do_DB:

```

On ouvre les ports 3306, 4567, 4568 et 4444 pour permettre la communication entre les deux serveurs.

To	Action	From
--	-----	-----
3306	ALLOW	Anywhere
22	ALLOW	Anywhere
80	ALLOW	Anywhere
443	ALLOW	Anywhere
4564	ALLOW	Anywhere
4568	ALLOW	Anywhere
4444	ALLOW	Anywhere
3306 (v6)	ALLOW	Anywhere (v6)
22 (v6)	ALLOW	Anywhere (v6)
80 (v6)	ALLOW	Anywhere (v6)
443 (v6)	ALLOW	Anywhere (v6)
4564 (v6)	ALLOW	Anywhere (v6)
4568 (v6)	ALLOW	Anywhere (v6)
4444 (v6)	ALLOW	Anywhere (v6)

3.5) Test de la réPLICATION

```
MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| glpi          |
| information_schema |
| mysql          |
| performance_schema |
+-----+
4 rows in set (0,000 sec)

MariaDB [(none)]> show slave status\G
***** 1. row *****
Slave_IO_State: Waiting for master to send event
    Master_Host: 172.25.31.16
    Master_User: rep_user
    Master_Port: 3306
    Connect_Retry: 60
    Master_Log_File: mariadb-bin.000002
    Read_Master_Log_Pos: 475
    Relay_Log_File: mysql-relay-bin.000002
    Relay_Log_Pos: 557
    Relay_Master_Log_File: mariadb-bin.000002
    Slave_IO_Running: Yes
    Slave_SQL_Running: Yes
    Replicate_Do_DBI:
    Replicate_Ignore_DBI:
    Replicate_Do_Table:
    Replicate_Ignore_Table:
    Replicate_Wild_Do_Table:
    Replicate_Wild_Ignore_Table:
        Last_Error:
        Skip_Counter: 0
    Exec_Master_Log_Pos: 475
    Relay_Log_Space: 867
    Until_Condition: None
    Until_Log_File:
    Until_Log_Pos: 0
    Master_SSL_Allowed: No
    Master_SSL_CA_File:
    Master_SSL_CA_Path:
        Master_SSL_Cert:
        Master_SSL_Cipher:
        Master_SSL_Key:
    Seconds_Behind_Master: 0
Master_SSL_Verify_Server_Cert: No
    Last_IO_Errno: 0
    Last_IO_Error:
    Last_SQL_Errno: 0
    Last_SQL_Error:
Replicate_Ignore_Server_Ids:
    Master_Server_Id: 1
        Master_SSL_Crl:
        Master_SSL_Crlpath:
            Using_Gtid: No
            Gtid_IO_Pos:
Replicate_Do_Domain_Ids:
Replicate_Ignore_Domain_Ids:
    Parallel_Mode: optimistic
    SQL_Delay: 0
    SQL_Remaining_Delay: NULL
    Slave_SQL_Running_State: Slave has read all relay log; waiting for more updates
    Slave_DDL_Groups: 5
Slave_Non_Transactional_Groups: 1
Slave_Transactional_Groups: 0
1 row in set (0,000 sec)

MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| glpi          |
| information_schema |
| mysql          |
| performance_schema |
+-----+
4 rows in set (0,000 sec)
```

3.6) Modification du fichier 000-default.conf

```
GNU nano 5.4                               000-default.conf
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/glpi

    # Available loglevels: trace8, ... , trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
root@glpi1:/etc/apache2/sites-available# sudo a2ensite 000-default.conf
Site 000-default already enabled
```

En tapant le nom de domaine du site, on atterrit directement sur le GLPI.

4. Sécurité du système

 COMMENT SURVEILLER SON RESEAU INFORMATIQUE ? ZABBIX !

4.1) Supervision via Zabbix

Installation des paquets nécessaires au fonctionnement de Zabbix :

```
root@zabbix:/home/calvyn# apt install apache2 php php-{mysql,mysqlnd,ldap,bcmath,mbstring,gd,pdo,xml} libapache2-mod-php mariadb-server mariadb-client
```

Installation du paquet Zabbix :

```
root@zabbix:/# wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
--2023-04-22 16:09:51--  https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-release_6.4-1+debian11_all.deb
Résolution de repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connexion à repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 3740 (3,7K) [application/octet-stream]
Sauvegarde en : « zabbix-release_6.4-1+debian11_all.deb »

  % Total    Speed     Time   Time     Time Current
                                 Dload  Upload   Lost%  Retries
2023-04-22 16:09:52 (164 MB/s) - « zabbix-release_6.4-1+debian11_all.deb » sauvegardé [3740/3740]
```

On décomprime l'archive :

```
root@zabbix:/# sudo dpkg -i zabbix-release_6.4-1+debian11_all.deb
Selection du paquet zabbix-release précédemment désélectionné.
(Lecture de la base de données... 146255 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de zabbix-release_6.4-1+debian11_all.deb ...
Dépaquetage de zabbix-release (1:6.4-1+debian11) ...
Paramétrage de zabbix-release (1:6.4-1+debian11) ...
```

Installation de Zabbix Server, Frontend,Agent

```
root@zabbix:/# apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent
```

On crée la base de données initiale

```
MariaDB [(none)]> create database zabbix character set utf8 collate utf8_bin;
Query OK, 1 row affected (0,021 sec)

MariaDB [(none)]> create user zabbix@localhost identified by '1234';
Query OK, 0 rows affected (0,017 sec)

MariaDB [(none)]> grant all privileges on zabbix.* to zabbix@localhost;
Query OK, 0 rows affected (0,003 sec)

MariaDB [(none)]> quit;
Bye
root@zabbix:/#
```

4.1.1) Modification du fichier zabbix_server.conf



```
calvyn@zabbix: ~
GNU nano 5.4          /etc/zabbix/zabbix_server.conf

#      empty string.
#
# Mandatory: yes
# Default:
# DBName=

DBName=zabbix

### Option: DBSchema
#      Schema name. Used for PostgreSQL.
#
# Mandatory: no
# Default:
# DBSchema=


### Option: DBUser
#      Database user.
#
# Mandatory: no
# Default:
# DBUser=


DBUser=zabbix

### Option: DBPassword
#      Database password.
#      Comment this line if no password is used.
#
# Mandatory: no
# Default:
# DBPassword=1234

### Option: DBSocket
#      Path to MySQL socket.

^G Aide      ^O Écrire      ^W Chercher      ^K Couper      ^T Exécuter      ^C Emplacement      M-U Annuler
^X Quitter    ^R Lire fich.   ^\ Remplacer    ^U Coller       ^J Justifier     ^  Aller ligne    M-E Refaire
```

4.1.2) On redémarre les services zabbix-server, zabbix-agent et apache2

```
● zabbix-server.service - Zabbix Server
  Loaded: loaded (/lib/systemd/system/zabbix-server.service; enabled; vendor preset: enabled)
  Active: active (running) since Sat 2023-04-22 16:32:58 CEST; 6s ago
    Process: 17225 ExecStart=/usr/sbin/zabbix_server -c $CONFFILE (code=exited, status=0/SUCCESS)
   Main PID: 17227 (zabbix_server)
     Tasks: 1 (limit: 2321)
    Memory: 2.8M
      CPU: 15ms
     CGroup: /system.slice/zabbix-server.service
             └─17227 /usr/sbin/zabbix_server -c /etc/zabbix/zabbix_server.conf

avril 22 16:32:58 zabbix systemd[1]: Starting Zabbix Server...
avril 22 16:32:58 zabbix systemd[1]: Started Zabbix Server.

● zabbix-agent.service - Zabbix Agent
  Loaded: loaded (/lib/systemd/system/zabbix-agent.service; enabled; vendor preset: enabled)
  Active: active (running) since Sat 2023-04-22 16:31:26 CEST; 1min 38s ago
    Process: 17168 ExecStart=/usr/sbin/zabbix_agentd -c $CONFFILE (code=exited, status=0/SUCCESS)
   Main PID: 17173 (zabbix_agentd)
     Tasks: 6 (limit: 2321)
    Memory: 3.8M
      CPU: 24ms
     CGroup: /system.slice/zabbix-agent.service
             ├─17173 /usr/sbin/zabbix_agentd -c /etc/zabbix/zabbix_agentd.conf
             ├─17174 /usr/sbin/zabbix_agentd: collector [idle 1 sec]
             ├─17175 /usr/sbin/zabbix_agentd: listener #1 [waiting for connection]
             ├─17176 /usr/sbin/zabbix_agentd: listener #2 [waiting for connection]
             ├─17177 /usr/sbin/zabbix_agentd: listener #3 [waiting for connection]
             └─17178 /usr/sbin/zabbix_agentd: active checks #1 [idle 1 sec]

avril 22 16:31:26 zabbix systemd[1]: Starting Zabbix Agent...
avril 22 16:31:26 zabbix systemd[1]: Started Zabbix Agent.
```

4.1.3) Interface de Zabbix

ZABBIX

Bienvenue

Vérification des prérequis

Configurer la connexion à la base de données

Paramètres

Résumé pré-installation

Installer

Bienvenue dans

Zabbix 6.4

Langage par défaut **Français (fr_FR)**

Licencié sous GPL v2

Retour Prochaine étape

Global view

Tous les tableaux de bord / Global view

Page 1 ...

Top hosts by CPU utilization

Utilisation	1m avg	5m avg	15m avg	Processes
Zabbix server	159 %	0.00	0.08	233.00

1.45 ↓
Zabbix server
Values per second

Information système

Paramètre	Valeur	Détails
Le serveur Zabbix est en cours d'exécution.	Oui	localhost:10051
Nombre d'éléments (activés/désactivés)	1	1 / 1
Nombre de modules	279	
Nombre d'éléments (actifs/désactivés) [problème(s)]	110	99 / 0 / 11
Nombre de déclencheurs (actifs/désactivés) [problème(s)]	64	64 / 0 / 64
Nombre d'utilisateurs (en ligne)	2	1

15:18
Paris

Disponibilité de l'hôte

1 Disponible	0 Non disponible	0 Incertain	1 Total
--------------	------------------	-------------	---------

Problems by severity

0 Désastre	0 Haut	0 Moyen	0 Avertissement	0 Information	0 Non classé
------------	--------	---------	-----------------	---------------	--------------

Current problems

Temps ▾ Info Hôte Problème ▾ Sévérité Date Actualiser Actions Tags

Aucune donnée trouvée.

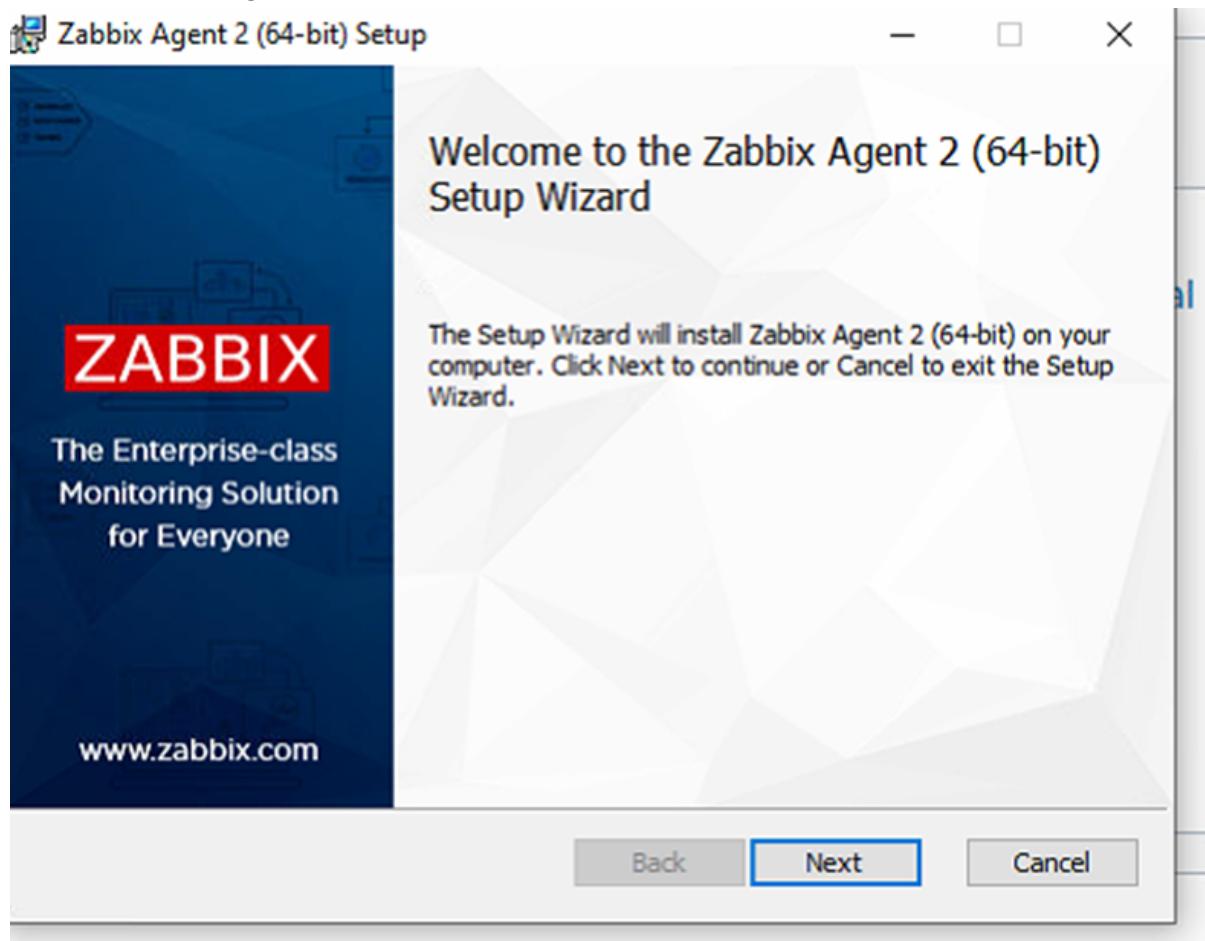
Carte géographique

Support Integrations Aide Paramètres utilisateur Déconnexion

Taper ici pour rechercher:

4.1.4) Ajout d'un client Windows 10

Installation de l'agent Zabbix



Création d'un groupe d'hôtes sur le superviseur

A screenshot of the Zabbix web interface. The URL is "172.25.31.99/zabbix/zabbix.php?action=hostgroup.list". The left sidebar shows navigation categories like Tableaux de bord, Surveillance, Inventaire, Rapports, Collecte de données, Groupes d'hôtes, Modèles, Hôtes, Maintenance, Corrélation d'événement, Découvertes, Alertes, Utilisateurs, Administration, and Support. The main content area is titled "Groupes d'hôtes" and shows a list of host groups. A search bar at the top right has "Windows" typed into it. Below the search bar are two buttons: "Appliquer" and "Réinitialiser". The list table has columns for "Nom" (Name), "Hôtes" (Hosts), and "Info". One row is selected, indicated by a blue border. At the bottom of the list, there are buttons for "Activer les filtres" (Enable filters), "Désactiver les filtres" (Disable filters), and "Supprimer" (Delete). A status bar at the bottom right says "Affichage de 7 sur 7 trouvés" (Displaying 7 of 7 found).

Création d'un hôte

Nouvel hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte	PC-CALVYN				
Nom visible	PC-CALVYN				
Modèles	taper ici pour rechercher	Sélectionner			
* Groupes d'hôtes	Windows <input checked="" type="checkbox"/>	Sélectionner			
Interfaces	Type adresse IP	Nom DNS	Connexion à	Port	Défaut
	Agent 172.25.31.5		IP	DNS	10050
			<input checked="" type="radio"/>	Supprimer	
Ajouter					
Description	<div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>				
Surveillé via le proxy	(pas de proxy) <input type="button" value="▼"/>				
Activé	<input checked="" type="checkbox"/>				
Ajouter Annuler					

Ajout d'un modèle à l'hôte

Hôte

Hôte IPMI Tags Macros Inventaire Chiffrement Table de correspondance

* Nom de l'hôte	PC-CALVYN				
Nom visible	PC-CALVYN				
Modèles	Nom	Action			
	Windows by Zabbix agent	Supprimer lien Supprimer lien et nettoyer			
	taper ici pour rechercher	Sélectionner			
* Groupes d'hôtes	Windows <input checked="" type="checkbox"/>	Sélectionner			
Interfaces	Type adresse IP	Nom DNS	Connexion à	Port	Défaut
	Agent 172.25.31.5		IP	DNS	10050
			<input checked="" type="radio"/>	Supprimer	

4.1.5) Superviser notre infrastructure

Création d'un graphique



Envoi de mail

<input type="checkbox"/> Email	Courriel	Activé	serveur SMTP: "smtp.gmail.com", courriel: "calvyn.morin@gmail.com"	Test
<input type="checkbox"/> Email (HTML)	Courriel	Désactivé	serveur SMTP: "mail.example.com", SMTP helo: "example.com", courriel: "zabbix@example.com"	Test
<input type="checkbox"/> Express.ms	Webhook	Désactivé		Test
<input type="checkbox"/> GitHub	Webhook	Désactivé		Test
<input type="checkbox"/> GLPI	Webhook	Désactivé		Test
<input type="checkbox"/> Gmail	Courriel	Activé	serveur SMTP: "smtp.gmail.com", courriel: "calvyn.morin@gmail.com"	Test

Action

Action Opérations 2

* Nom

Type de calcul A and B

Conditions

Étiquette	Nom	Action
A	Sévérité du déclencheur est supérieur ou égal à Non classé	Supprimer
B	Hôte égal PC-CALVYN	Supprimer
Ajouter		

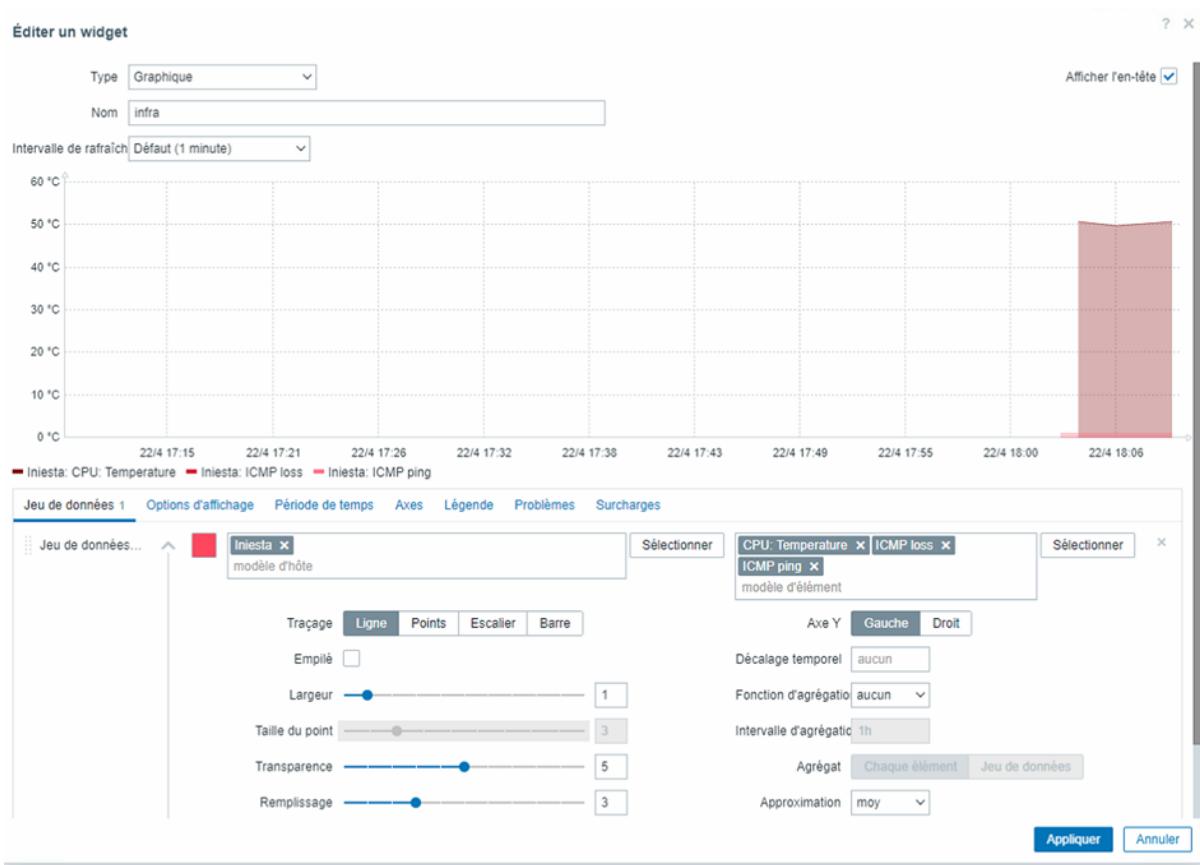
Activé

* Au moins une opération doit exister.

[Actualiser](#) [Clone](#) [Supprimer](#) [Annuler](#)

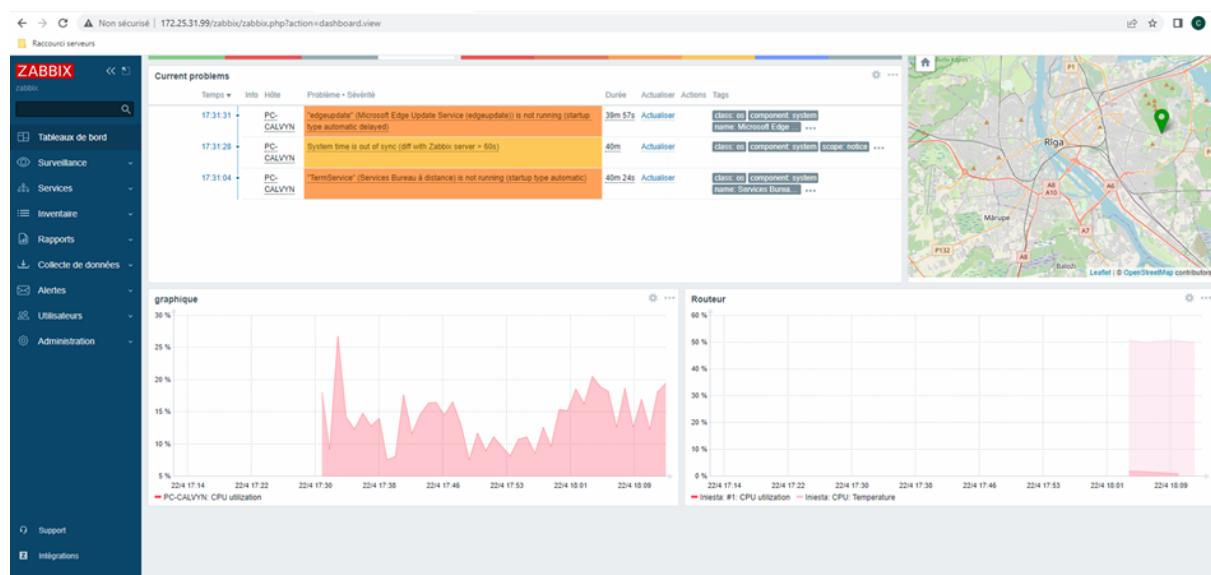
4.1.6) Supervision du routeur

```
Iniesta(config)#snmp-server community public R0
Iniesta(config)#snmp-server enable traps
NHRP MIB is not enabled: Trap generation suppressed
However, configuration changes effective
Iniesta(config)#snmp-server enable traps config
Iniesta(config)#
snmp-server host 172.25.31.99 version 2c R0
```



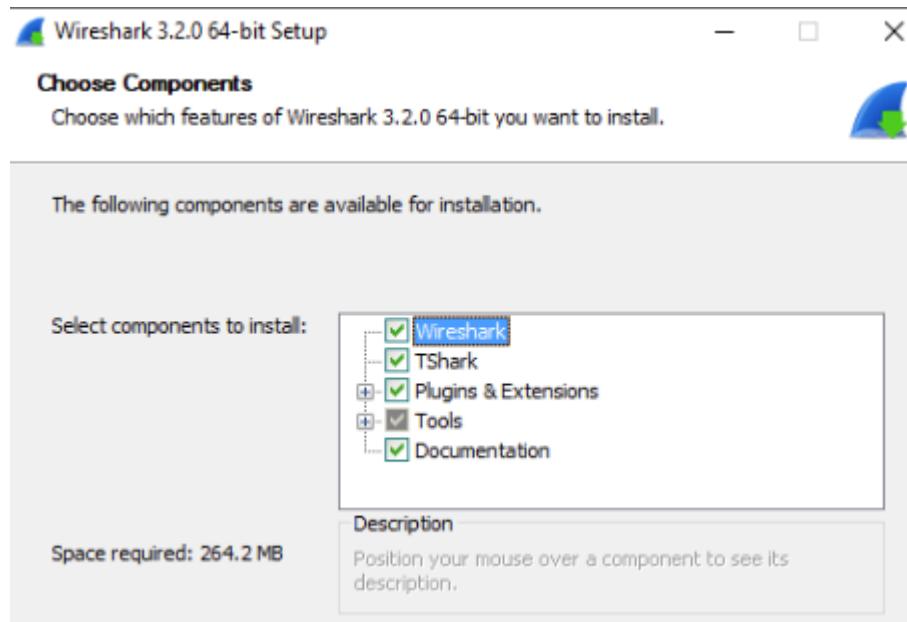
4.1.7) Réalisations des tests

Notre PC ainsi que notre routeur sont bien remontés sur notre serveur de supervision Zabbix.

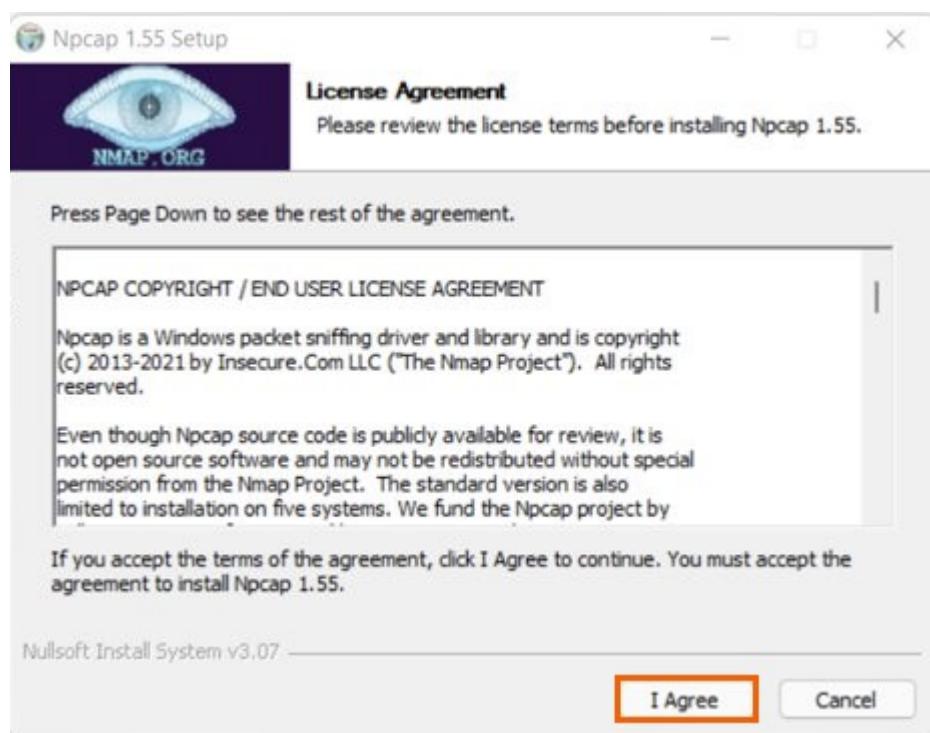


4.2) Solution d'analyse de paquets

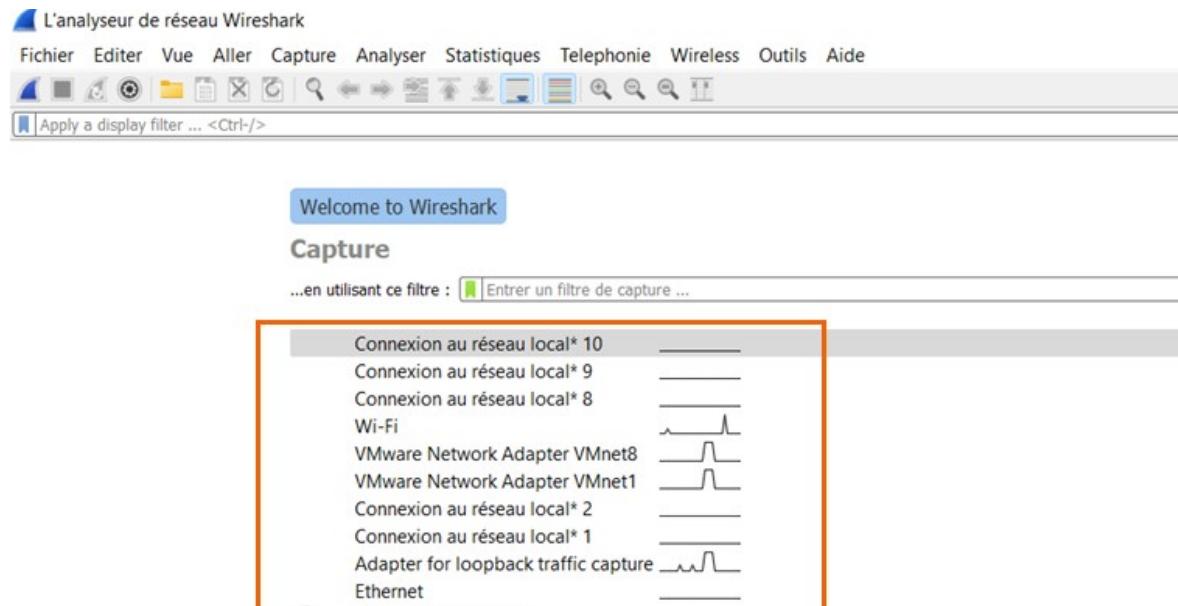
4.2.1) Installation de Wireshark



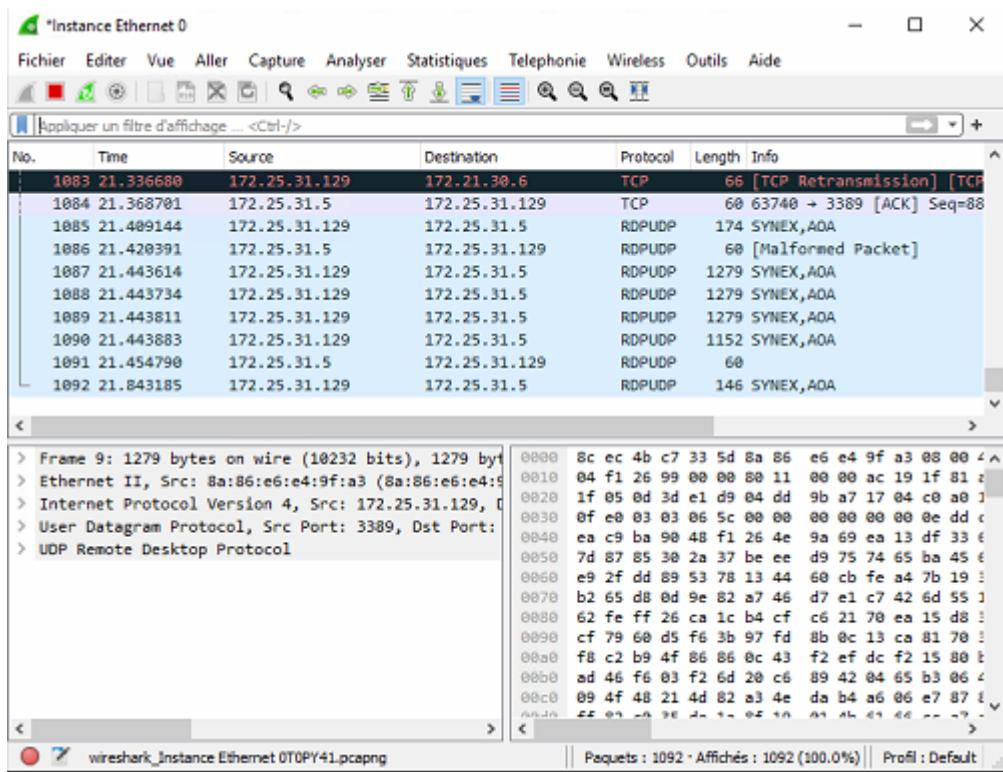
4.2.2) Installation de NpCap afin de réaliser des captures



4.2.3) Sélection de l'interface réseau



4.2.4) Analyse de paquets sur notre infrastructure



4.3) Mise en place d'un IDS

4.3.1) Installation du package Snort

System / Package Manager / Installed Packages

Installed Packages Available Packages

Installed Packages

Name	Category	Version	Description	Actions
✓ snort	security	4.1.6	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	

Package Dependencies:

- snort-2.9.20

4.3.2) Récupération d'un token sur le site officiel de Snort

Oinkcode

2149a7abdd82b0ff28a1799a07e0e2c7f78968ff

Regenerate

4.3.3) Mise en place des règles

Update Your Rule Set

Last Update	May-10 2023 08:17	Result: Success
Update Rules	<input checked="" type="button"/> Update Rules	Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Block Settings

Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	Legacy Mode
Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.	
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgb, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.	
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	BOTH
Select which IP extracted from the packet you wish to block. Default is BOTH.	

Detection Performance Settings

Search Method	AC-BNFA
Choose a fast pattern matcher algorithm. Default is AC-BNFA.	
Split ANY-ANY	<input type="checkbox"/> Enable splitting of ANY-ANY port group. Default is Not Checked.
Search Optimize	<input type="checkbox"/> Enable search optimization. Default is Not Checked.
Stream Inserts	<input type="checkbox"/> Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.
Checksum Check Disable	<input type="checkbox"/> Disable checksum checking within Snort to improve performance. Default is Not Checked.

Block Settings

Block Offenders Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.
Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnx, cc, cxgb, cxl, em, ena, ice, igb, igc, ix, ixgb, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performance Settings

Search Method Choose a fast pattern matcher algorithm. Default is AC-BNFA.

Split ANY-ANY Enable splitting of ANY-ANY port group. Default is Not Checked.

Search Optimize Enable search optimization. Default is Not Checked.

Stream Inserts Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.

Checksum Check Disable Disable checksum checking within Snort to improve performance. Default is Not Checked.

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

WAN Settings WAN Categories WAN Rules WAN Variables WAN Preprocs WAN IP Rep WAN Logs

Automatic Flowbit Resolution

Resolve Flowbits If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Auto-Flowbit Rules Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.

Snort Subscriber IPS Policy Selection

Use IPS Policy If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.
Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

Select the rulesets (Categories) Snort will load at startup

(- Category is auto-enabled by SID Mgmt conf files
(- Category is auto-disabled by SID Mgmt conf files)

Enable	Ruleset: Snort GPLv2 Community Rules				
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)				
Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	
<input checked="" type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules
<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_browser-ie.so.rules

4.3.4) Activation de l'interface WAN

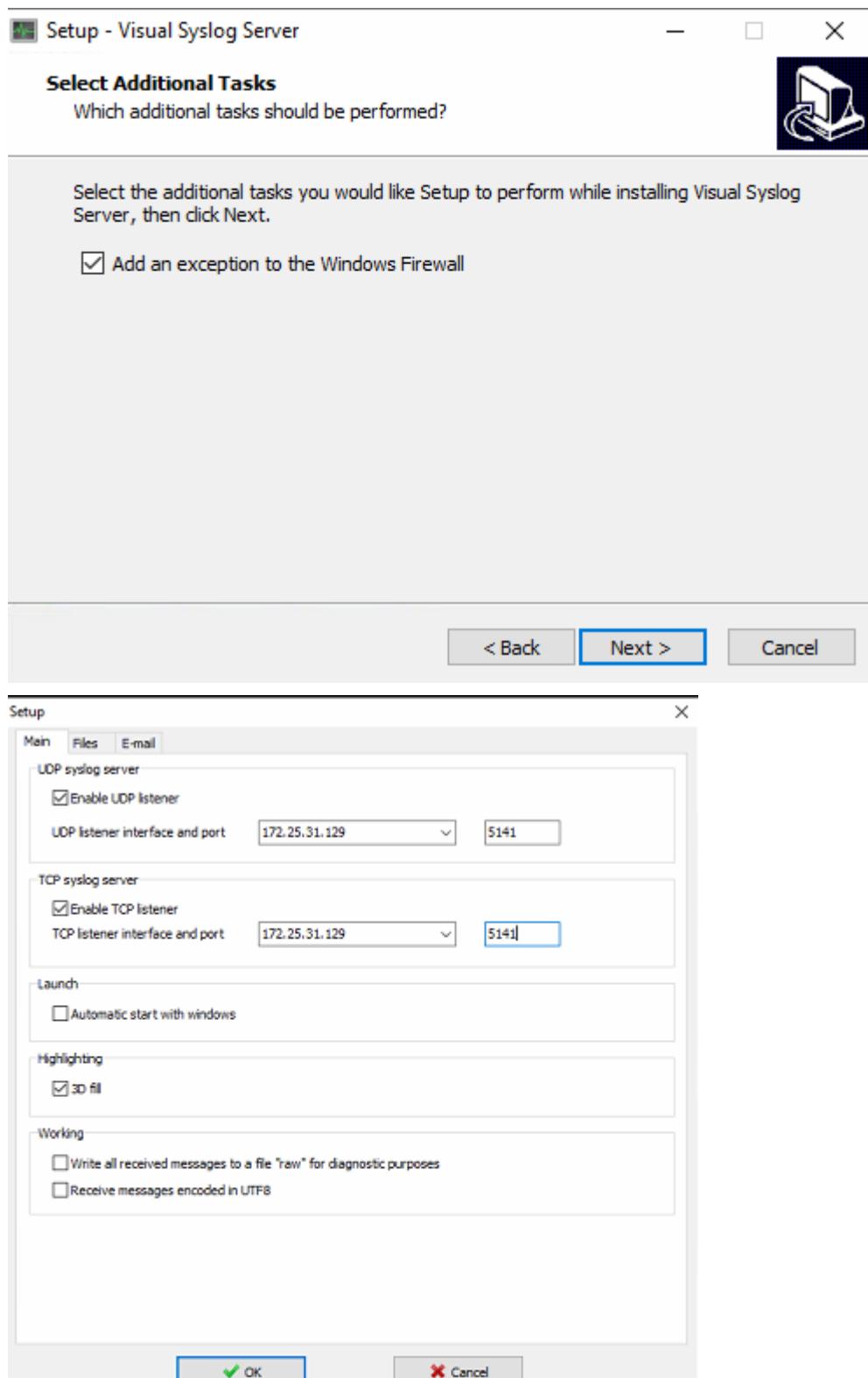
The screenshot shows the 'Snort / Snort / Interfaces' section of a web-based interface. The top navigation bar includes links for Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The 'Snort Interfaces' tab is selected. Below the navigation is a table titled 'Interface Settings Overview' with columns: Interface, Snort Status, Pattern Match, Blocking Mode, Description, and Actions. A single row is present for 'WAN (vtnet0)', showing a gear icon for status, 'AC-BNFA' for pattern match, 'LEGACY MODE' for blocking mode, and 'WAN' for description. The 'Actions' column contains icons for edit, copy, and delete. At the bottom right of the table are 'Add' and 'Delete' buttons.

4.3.4) Détection des intrusions

The screenshot shows the pfSense Community Edition dashboard. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message at the top states: 'WARNING: The admin account password is set to the default value. Change the password in the User Manager.' The main content area has two sections: 'System Information' on the left and 'Interfaces' and 'Snort Alerts' on the right. The 'System Information' table includes rows for Name (pfSense.m23.lan), User (admin@172.25.31.5), System (KVM Guest), BIOS (Seabios, version r01-1.15.0-0-g2dd4b9b3f840-prebuilt.qemu.org), Version (2.6.0-RELEASE (amd64)), CPU Type (Common KVM processor, AES-NI CPU Crypto: No, QAT Crypto: No), Hardware crypto (Enabled), MDS Mitigation (Inactive), Uptime (03 Hours 47 Minutes 14 Seconds), Current date/time (Wed May 17 17:24:26 UTC 2023), DNS server(s) (127.0.0.1, 172.25.31.129, 8.8.8), Last config change (Wed May 17 16:56:57 UTC 2023), and State table size (0% (11/198000)). The 'Interfaces' table lists three interfaces: WAN (10Gbase-T <full-duplex>, 192.168.28.198), LAN (10Gbase-T <full-duplex>, 172.25.31.10), and OPT1 (10Gbase-T <full-duplex>, 172.25.33.1). The 'Snort Alerts' table lists several ET POLICY HSRP Active Router Changed events over time, with source and destination addresses like 172.25.33.1 and 224.0.0.2:1985.

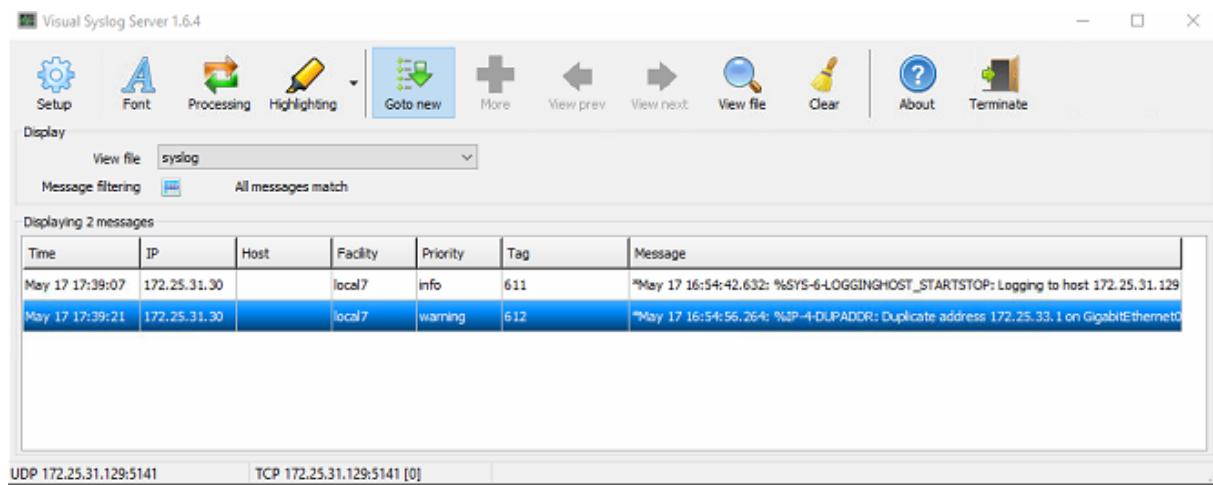
4.4) Système de logs du SI

4.4.1) Installation de Visual Syslog Server



On envoie le trafic vers notre serveur centralisant les logs.

```
Iniesta(config)#log
Iniesta(config)#logging on
Iniesta(config)#logging 172.25.31.129
Iniesta(config)#logging trap 6
```



4.4.2) Récupération des logs sous Linux

On modifie le fichier rsyslog.conf

```
# provides UDP syslog reception
module(load="imudp")

```

Enfin, on modifie le fichier /etc/rsyslog.d/50-default.conf

```
GNU nano 5.4                               50-default.conf
auth,authpriv.* @172.25.31.129:514
```

On envoie les informations de connexion vers notre serveur de centralisation de log.

May 17 23:39:01	172.25.31.16	gpi1	authpriv	info	CRON[25406]	pam_unix(cron:session): session opened for user
May 17 23:39:01	172.25.31.16	gpi1	authpriv	info	CRON[25406]	pam_unix(cron:session): session closed for user

Solution de Supervision(Zabbix):

COMMENT SURVEILLER SON RESEAU INFORMATIQUE ? ZABBIX !

