

BTS Services Informatiques aux Organisations
Option Solutions d'Infrastructure, Systèmes et Réseaux

Épreuve E6 - Administration des systèmes et Réseaux

Documentation Technique



Réalisation n°1: Monitoring Zabbix et configuration AD/DS

Table des matières

Table des matières	2
I. Contexte	3
II. Prérequis	3
III. Présentation Générale de l'Architecture Système	4
A. Schéma et logique	4
B. Rôles des machines	5
C. Objectifs de l'infrastructure	5
IV. Configuration et Réalisation	5
A. Configuration de la haute disponibilité Pfsense	5
1. Déclaration des adresses IP	5
2. Configuration de la synchronisation	7
B. Configuration des zones LAN.	10
Définition des sous-réseaux	10
C. Configuration des différents serveurs (fichiers, AD et Zabbix)	11
1. Serveur Active Directory	11
2. Serveur de fichiers	13
3. Serveur Zabbix	16
D. Monitoring des serveurs et routeurs	21
1. Installation de l'agent Zabbix sur les serveurs Windows	21
2. Activation du service SNMP sur Pfsense	22
3. Déclaration des machines sur Zabbix	23
E. Configuration des règles de Firewall.	24
F. Intégration de Zabbix à l'Active Directory.	24
Ajout de la machine Zabbix dans le contrôleur de domaine.	24
V. Tests	25
A. Failover PFSense	25
B. Connexion au domaine depuis le client	25
C. GPO appliquées (Lecteurs mappés) et accès aux fichiers partagés : droits respectés	27
D. Surveillance Zabbix : tous les équipements sont visibles et monitorer	29
VI. Conclusion et Préconisations	30
A. Conclusion	30
B. Préconisations	30

I. Contexte

La Maison des Ligues de Lorraine (M2L) a un besoin de centraliser les utilisateurs et les données, de sécuriser et segmenter le réseau, et d'assurer une haute disponibilité de l'accès à internet.

Ce projet vise à :

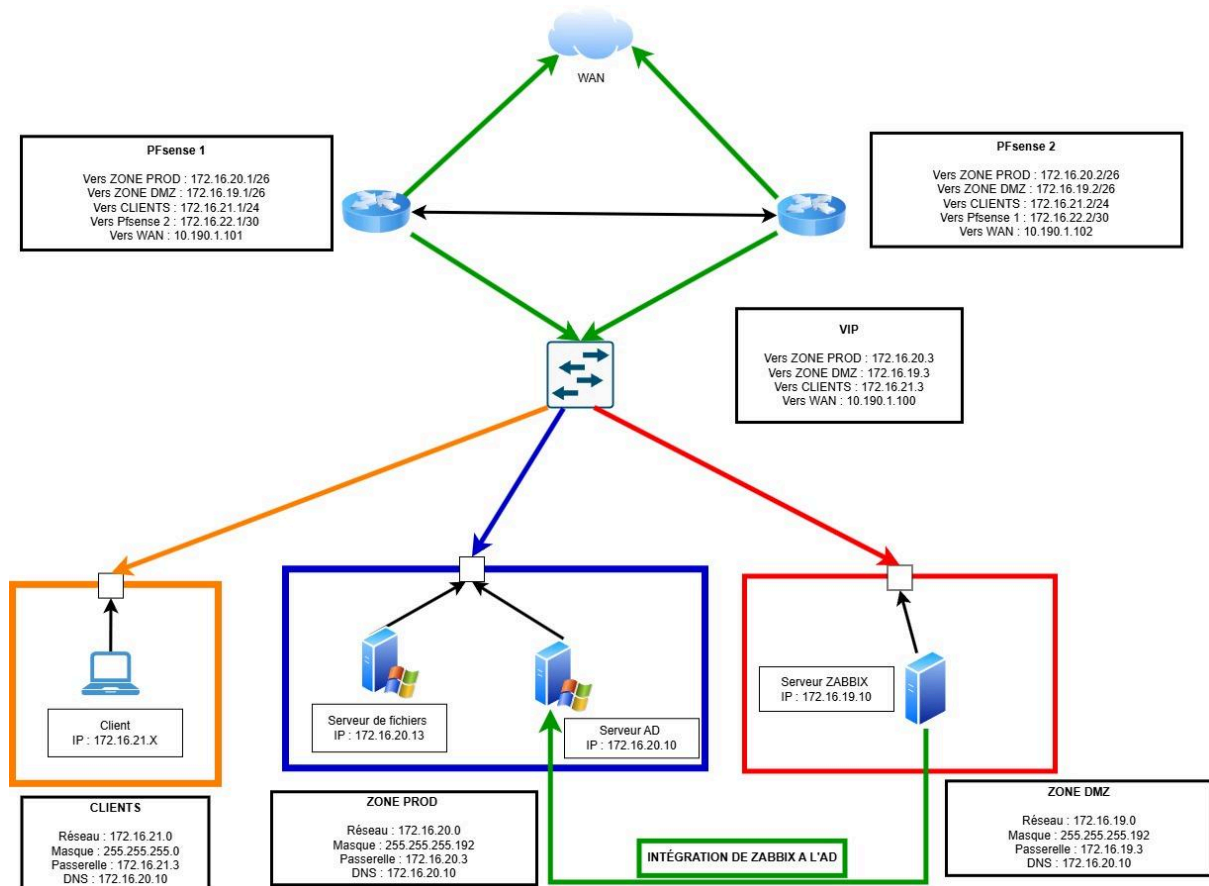
- Mettre en place deux routeurs Pfsense en haute disponibilité (failover) pour assurer une tolérance aux pannes.
- Créer plusieurs zones LAN segmentées pour mieux sécuriser les flux.
- Implémenter un serveur Zabbix pour surveiller l'état du réseau.
- Installer un serveur Active Directory / DNS et un serveur de fichiers pour centraliser les utilisateurs et les données.
- Déployer une stratégie de groupe GPO pour normaliser les configurations des postes clients.

II. Prérequis

- Matériel :
 - Deux routeurs Pfsense
 - Un serveur Zabbix
 - Deux serveurs Windows Server 2019 ou 2022 (AD/DNS, fichiers)
 - Un poste client en LAN
 - Environnement Proxmox
- Logiciels/Services
 - Pfsense, Zabbix, Windows Server, Console de management des GPO et console de gestion des utilisateurs et ordinateurs
 - Navigateur Web, client SSH/HTTPS, Active Directory Utilisateurs et Ordinateurs, Console Zabbix
 - Accès aux différents serveurs en tant qu'administrateur

III. Présentation Générale de l'Architecture Système

A. Schéma et logique



Le réseau est structuré en différentes zones pour la sécurité et la gestion.

- **Haute disponibilité PFsense:** Deux routeurs PFsense sont configurés pour assurer une haute disponibilité de l'accès internet, garantissant la connectivité même si un routeur tombe en panne.
- **Zones LAN:** Plusieurs zones LAN sont créées pour segmenter et sécuriser le réseau.
 - a. **Zone PROD :** Contient le serveur de fichiers et le serveur Active Directory pour la centralisation des données et utilisateurs.
 - b. **Zone DMZ :** Héberge le serveur Zabbix pour la surveillance du réseau.
 - c. **Zone CLIENTS :** Pour les différents utilisateurs.
- **Gestionnaire des stratégies de groupe :** Utilisé pour appliquer des configurations communes à un groupe ou à tous les utilisateurs.

- **Intégration de Zabbix à l'Active Directory**: la machine Zabbix est intégrée à l'Active Directory.

B. Rôles des machines

1. **Serveur de fichiers** : Centralise les données de la M2L.
2. **Serveur Active Directory** : Centralise les utilisateurs.
3. **Deux PfSense** : Fournissent une haute disponibilité aux réseaux internes.
4. **Serveur Zabbix** : Monitore le réseau.
5. **Poste Client** : Situé dans la zone CLIENTS pour les différents utilisateurs.
6. **Gestionnaire des stratégies de groupe** : Déploie et normalise les postes clients.

C. Objectifs de l'infrastructure

1. **Centralisation des utilisateurs et des données** : Utilisation d'un serveur de fichiers et d'un serveur Active Directory.
2. **Haute disponibilité de l'accès internet** : Mise en place de deux PfSense en haute disponibilité.
3. **Segmentation et sécurisation du réseau** : Création de plusieurs zones LAN (PROD, DMZ et CLIENTS) et utilisation du gestionnaire de stratégie de groupe pour normaliser les configurations.
4. **Monitoring du réseau** : Utilisation d'un serveur Zabbix.

IV. Configuration et Réalisation

A. Configuration de la haute disponibilité PfSense

1. Déclaration des adresses IP

Pour assurer le fonctionnement en haute disponibilité, chaque serveur pfSense nécessitera une adresse IP dédiée sur son interface physique. De plus, une adresse IP virtuelle (Firewall > Virtual IPs) unique sera configurée et partagée entre les deux serveurs. Ainsi, chaque réseau concerné nécessitera l'attribution de

trois adresses IP : une pour chaque serveur physique et une adresse virtuelle pour la redondance.









Pfsense 1 :

```
WAN (wan)      -> vtnet0      -> v4: 10.190.1.101/22
PROD (lan)     -> vtnet1      -> v4: 172.16.20.1/26
DMZ (opt1)    -> vtnet2      -> v4: 172.16.19.1/26
CLIENTS (opt2) -> vtnet3      -> v4: 172.16.21.1/24
PTP (opt3)    -> vtnet4      -> v4: 172.16.22.1/30
```

Pfsense 2 :

```
WAN (wan)      -> vtnet0      -> v4: 10.190.1.102/22
PROD (lan)     -> vtnet1      -> v4: 172.16.20.2/26
DMZ (opt1)    -> vtnet2      -> v4: 172.16.19.2/26
CLIENTS (opt2) -> vtnet3      -> v4: 172.16.21.2/24
PTP (opt3)    -> vtnet4      -> v4: 172.16.22.2/30
```

Virtual IP :

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
172.16.20.3/26 (vhid: 2)	PROD	CARP	CARP PROD	 
172.16.19.3/26 (vhid: 3)	DMZ	CARP	CARP DMZ	 
172.16.21.3/24 (vhid: 4)	CLIENTS	CARP	CARP CLIENTS	 
10.190.1.100/22 (vhid: 5)	WAN	CARP	VIP WAN	 

Exemple :

Edit Virtual IP

Type
☐ IP Alias
☒ CARP
☐ Proxy ARP
☐ Other

Interface
PROD

Address type
Single address

Address(es)
172.16.20.3 / 26

The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password

Enter the VHID group password.

Confirm

VHID Group
2

Enter the VHID group that the machines will share.

Advertising frequency

Base
1

Skew
0

The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description
CARP PROD

A description may be entered here for administrative reference (not parsed).

- **Interface** : l'interface sur laquelle la VIP doit être configurée. Ici, on configure la VIP sur l'interface PROD.

- **Adresse(s) :** Nous utiliserons l'adresse VIP 172.16.20.3 avec un masque de sous-réseau /26 pour l'interface.
- **Virtual IP Password :** Un mot de passe de sécurité sera défini pour authentifier les communications entre les deux serveurs pfSense partageant la VIP. Ce même mot de passe devra être configuré sur le serveur pfSense secondaire.
- **VHID Group :** Nous changeons l'identifiant de groupe virtuel (VHID) par défaut et nous mettons l'ID "2" pour identifier ce groupe de VIP.
- **Advertising Frequency :** Pour déterminer le rôle des serveurs, le champ "Skew" sera réglé à 0 sur le serveur primaire (master), et une valeur supérieure sur le serveur secondaire (backup). La valeur "Base", qui définit le délai en secondes avant de considérer un hôte comme inactif, sera laissée à sa valeur par défaut de 1 seconde.

Pour finaliser la configuration de la haute disponibilité, nous allons répliquer les mêmes étapes sur l'interface PROD (et les autres interfaces) du serveur pfSense secondaire (pfSense 2). Une attention particulière sera portée au champ "Skew", dont la valeur devra être impérativement supérieure à 0 sur ce serveur. Une fois cette configuration terminée, l'état de l'adresse IP virtuelle et le statut du basculement (CARP) pourront être consultés et vérifiés à tout moment via le menu "Status" puis "CARP (failover)" de l'interface web de pfSense.

Dans le cas présent, les adresses VIP créée ont bien le statut "master" sur le pfSense 1 :

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
PROD@2	172.16.20.3/26	CARP PROD	MASTER
DMZ@3	172.16.19.3/26	CARP DMZ	MASTER
CLIENTS@4	172.16.21.3/24	CARP CLIENTS	MASTER
WAN@5	10.190.1.100/22	VIP WAN	MASTER

2. Configuration de la synchronisation

Il reste à configurer la haute-disponibilité. Pour cela, se rendre dans "System" > "High Avail. Sync".

State Synchronization Settings (pfsync)

- **Synchronize States :** Cochoons cette case sur les deux serveurs (primaire et secondaire) pour activer pfsync.
- **Synchronize Interface :** Nous sélectionnons l'interface à utiliser pour la synchronisation. Ici, "PTP"

- **pfsync Synchronize Peer IP :**

- Sur le serveur pfSense primaire, nous entrons l'adresse IP de l'interface de synchronisation du serveur secondaire (172.16.22.2)
- Sur le serveur pfSense secondaire, nous indiquons l'adresse IP de l'interface de synchronisation du serveur primaire (172.16.22.1).
- Si aucun IP n'est spécifié, pfSense utilisera le multicast sur l'interface sélectionnée.

Configuration de la synchronisation de la configuration (XMLRPC Sync) :

- **Synchronize Config to IP :**

- Sur le serveur pfSense primaire (10.75.19.1), nous entrons l'adresse IP de l'interface de synchronisation du serveur secondaire (la même adresse que celle renseignée dans "pfsync Synchronize Peer IP").
- Laissons ce champ vide sur le serveur pfSense secondaire.

- **Remote System Username :** Sur le serveur pfSense primaire, nous indiquons le nom d'utilisateur pour accéder à l'interface web du pfSense secondaire ("admin" par défaut). Laissons ce champ vide sur le serveur secondaire.

- **Remote System Password :** Sur le serveur pfSense primaire, nous entrons le mot de passe de l'utilisateur spécifié ci-dessus. Nous laissons ce champ vide sur le serveur secondaire.

- **Synchronize Admin :** cette case est à cocher sur les deux pfsense

Enfin, nous sélectionnons les services à synchroniser en cochant les cases correspondantes. Il est généralement recommandé de tout cocher ("Toggle All"). Il est important de noter que cette manipulation n'est à faire que sur le master.

Résultat attendu sur le master :

State Synchronization Settings (pfsync)	
Synchronize states	<input checked="" type="checkbox"/> pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table. This setting should be enabled on all members of a failover group. Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)
Synchronize interface	<div>PTP</div> <div>If Synchronize States is enabled this interface will be used for communication. It is recommended to set this to an interface other than LAN! A dedicated interface works the best. An IP must be defined on each machine participating in this failover group. An IP must be assigned to the interface on any participating sync nodes.</div>
Filter Host ID	<div>9e36b0f7</div> <div>Custom pf host identifier carried in state data to uniquely identify which host created a firewall state. Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01). Each node participating in state synchronization must have a different ID.</div>
pfsync Synchronize Peer IP	<div>172.16.22.2</div> <div>Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.</div>

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username
Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password
Enter the webConfigurator password of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and password option on backup cluster members!

Synchronize admin ☒ synchronize admin accounts and autoupdate sync password.
By default, the admin account does not synchronize, and each node may have a different admin password.
This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Select options to sync

- ☒ User manager users and groups
- ☒ Authentication servers (e.g. LDAP, RADIUS)
- ☒ Certificate Authorities, Certificates, and Certificate Revocation Lists
- ☒ Firewall rules
- ☒ Firewall schedules
- ☒ Firewall aliases
- ☒ NAT configuration
- ☒ IPsec configuration
- ☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)
- ☒ DHCP Server settings
- ☒ DHCP Relay settings
- ☒ DHCPv6 Relay settings
- ☒ WoL Server settings
- ☒ Static Route configuration
- ☒ Virtual IPs
- ☒ Traffic Shaper configuration
- ☒ Traffic Shaper Limiters configuration
- ☒ DNS Forwarder and DNS Resolver configurations
- ☒ Captive Portal

☒ Toggle All

Autoriser les flux de réplication au niveau des règles du firewall

Il reste à autoriser les flux de répliquions sur les firewall. La configuration se passe dans "Firewall" > "Rules".

Il y a deux flux réseau à autoriser :

- le flux pour la synchronisation XML-RPC qui s'effectue via le port 443
- le flux pour la synchronisation du protocole pfsync

Sur le firewall primaire, nous créons les deux règles citées précédemment :

XML-RPC :

- **Action** : Nous sélectionnons "Pass"
- **Interface** : Nous choisissons l'interface dédiée à la synchronisation, ici, "PTP".
- **Address Family** : Nous laissons "IPv4"
- **Protocol** : Nous choisissons "TCP"

- **Source :** Nous indiquons l'adresse IP de l'interface de synchronisation (pour le primaire 172.16.22.2).
- **Destination :** Nous choisissons "This firewall (self)"
- **Destination port range :** Nous choisissons "HTTPS (443)" car la synchronisation XMLRPC utilise ce port.

Pfsync :

- **Action :** Nous sélectionnons "Pass"
- **Interface :** Nous choisissons l'interface dédiée à la synchronisation, ici, "PTP".
- **Address Family :** Nous laissons "IPv4"
- **Protocol :** Nous choisissons "PFSYNC"
- **Source :** Nous indiquons l'adresse IP de l'interface de synchronisation (pour le primaire 172.16.22.2).
- **Destination :** Nous choisissons "This firewall (self)"

B. Configuration des zones LAN.

La segmentation du réseau en différentes zones LAN est vise à améliorer la sécurité, la gestion et la performance. Chaque zone est définie par un sous-réseau IP distinct et isolé logiquement des autres.

Définition des sous-réseaux

- Zone PROD :
 - Objectif : Héberger les serveurs critiques de l'organisation (serveur de fichiers, contrôleur de domaine Active Directory).
 - Plage d'adresses IP : 172.16.20.0/26 (.3 pour la passerelle en VIP, .10 pour le serveur AD, .13 pour le serveur de fichiers).
 - Services Hôtes : Active Directory (authentification, gestion des utilisateurs et des ordinateurs), Serveur de fichiers (partages réseau, stockage centralisé des données).
- Zone DMZ (Demilitarized Zone) :
 - Objectif : Isoler les serveurs accessibles depuis l'extérieur ou nécessitant une sécurité renforcée, ici le serveur de monitoring Zabbix. La DMZ permet de protéger le réseau interne des attaques potentielles ciblant ces services.
 - Plage d'adresses IP : 172.16.19.0/29 (.3 pour la passerelle PfSense en VIP, .10 pour le serveur Zabbix).
 - Services Hôtes : Serveur Zabbix (collecte des métriques, alertes, supervision).
- Zone CLIENTS :

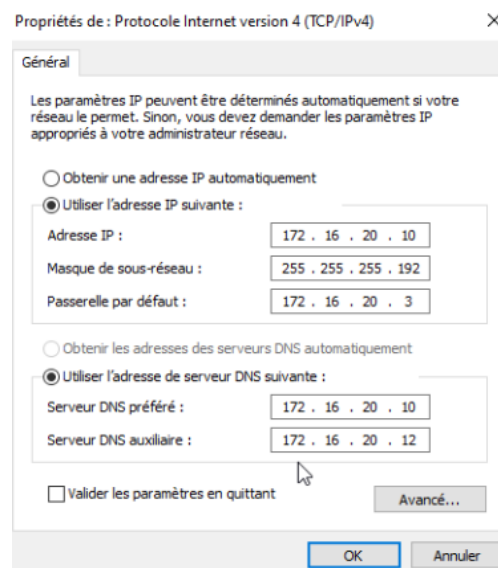
- Objectif : Accueillir les postes de travail des utilisateurs finaux de la M2L. Cette zone est la plus exposée et nécessite des règles de sécurité strictes pour contrôler les accès aux autres zones.
- Plage d'adresses IP : 172.16.21.0/24 (.3 pour la passerelle PfSense, postes clients IP .X).
- Services Hôtes : Postes utilisateurs (accès aux applications métiers, internet, serveur de fichiers via les règles de pare-feu).

C. Configuration des différents serveurs (fichiers, AD et Zabbix)

1. Serveur Active Directory

Étape 1 : Configuration de base du serveur

- Renommer la machine, ici, "M2L-DC1"
- Attribuer une adresse IP statique



Étape 2 : Installer le rôle "Services de domaine Active Directory"

- Ouvrir le Gestionnaire de serveur.
- Cliquer sur "Gérer" puis "Ajouter des rôles et fonctionnalités".
- Avancer jusqu'à l'étape des rôles, et cocher "Services de domaine Active Directory".
- L'assistant ajoutera automatiquement le rôle DNS et les outils de gestion.
- Cliquer sur "Suivant" jusqu'à "Installer", puis attendre la fin de l'installation.

Étape 3 : Promouvoir le serveur en contrôleur de domaine

Cliquer sur la notification dans le Gestionnaire de serveur disant "Promouvoir ce serveur en contrôleur de domaine"

- a. Ajouter une nouvelle forêt
 - Nom du domaine racine : m2l.lan
- b. Cliquer sur Suivant et choisir :
 - Niveau fonctionnel de la forêt et du domaine (par défaut : Windows Server 2016/2019).
 - Définir un mot de passe pour le mode de restauration des services d'annuaire (DSRM).
- c. Laisser les options DNS et GC (Catalogue global) cochées.
- d. Laisser les options de NetBIOS par défaut (généralement le système propose automatiquement un nom).
- e. Le chemin des bases de données AD, des logs et SYSVOL peuvent rester par défaut.
- f. Vérifier le résumé de configuration, puis cliquer sur "Installer".
- g. Redémarrer le serveur

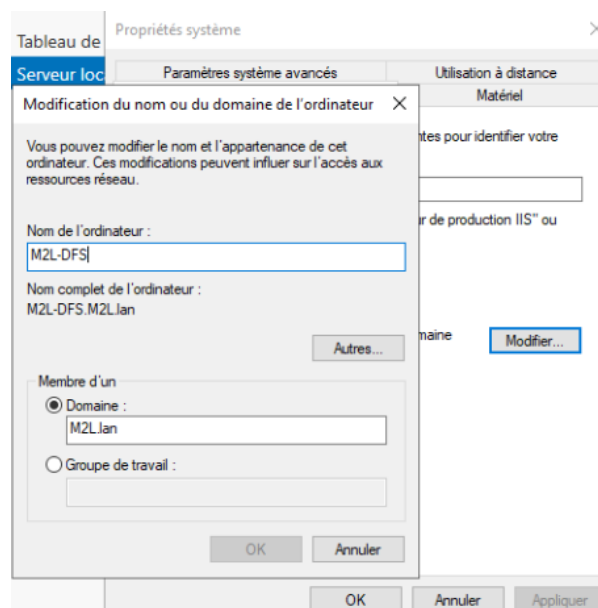
2. Serveur de fichiers

Étape 1 : Configuration de base du serveur

1. Renommer la machine, ici, "M2L-DFS"
2. Attribuer une adresse IP statique





3. Joindre le serveur au domaine



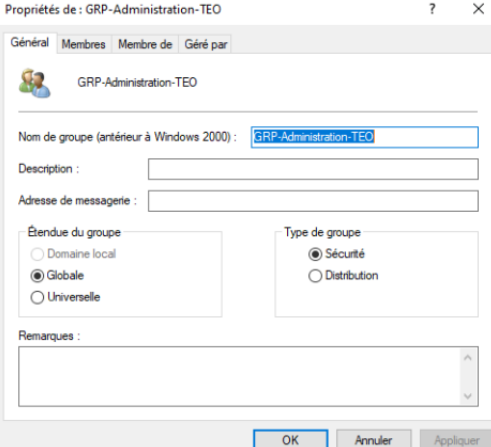
4. Redémarrer le serveur

Étape 2 : Création des groupes de sécurité et des utilisateurs sur l'Active Directory

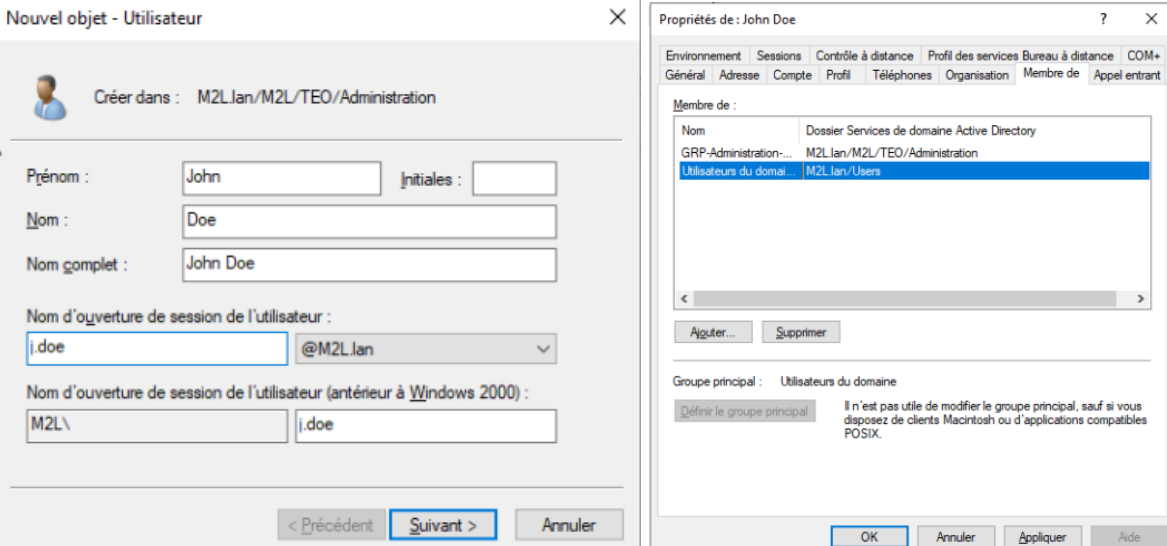
Exemple :

Nom	Type	Description
 GRP-Administration-TEO	Groupe de sécurité - Global	
 John Doe	Utilisateur	

Groupe de sécurité :

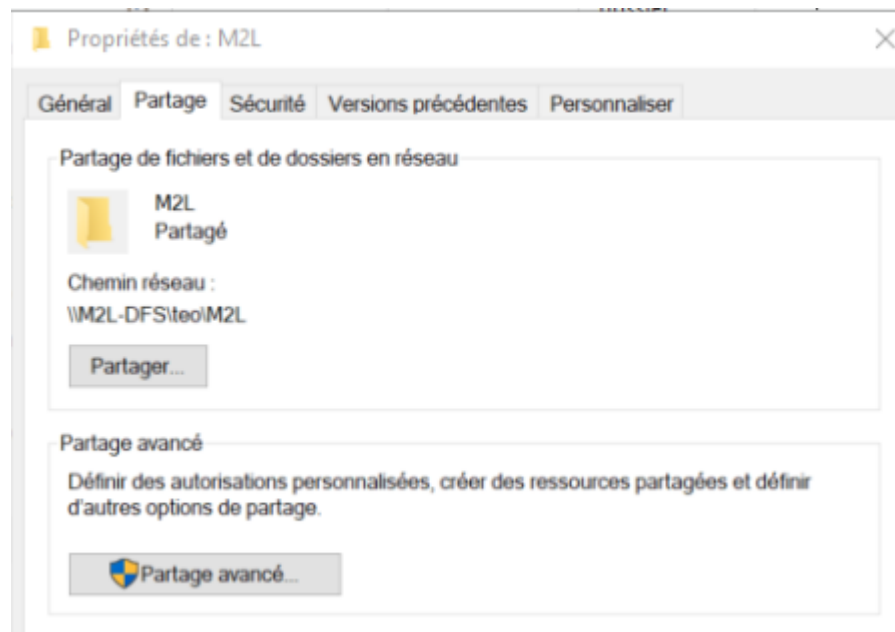


Utilisateur membre du groupe de sécurité Administration :



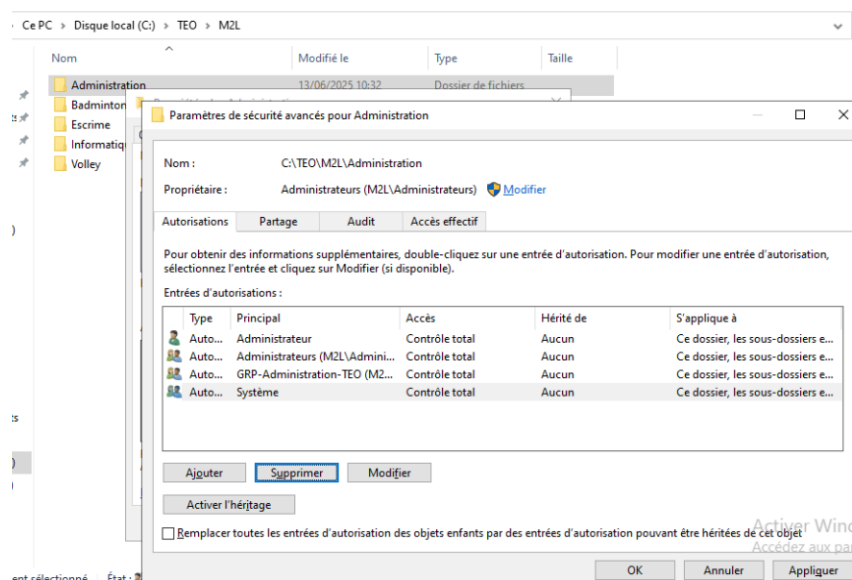
La création de groupe de sécurité permettra de limiter les accès aux dossiers se trouvant sur le serveur de fichiers, afin de garantir une sécurité supplémentaire des données.

Étape 3 : Création du partage et des sous-dossiers



Après avoir partagé le dossier, nous pouvons voir le chemin UNC du répertoire.

Il faut ensuite désactiver l'héritage des sous-dossiers dans le but de donner les accès aux répertoires uniquement aux groupes légitimes



Pour finir, il faut répéter l'opération pour tous les sous-dossiers.

3. Serveur Zabbix

Zabbix est une solution de supervision puissante et flexible conçue pour surveiller les performances des systèmes, des réseaux et des applications.

Étape 1 : Configuration de la machine Debian

- a. Donner un nom à la machine (/etc/hostname)

```
GNU nano 7.2 /etc/hostname
sio-zabbix
```

- b. Attribuer une IP statique dans le réseau DMZ (/etc/network/interfaces)

```
GNU nano 7.2 /etc/network/interfaces
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 172.16.19.10/26
    gateway 172.16.19.3
    dns-nameservers 172.16.20.10 172.16.20.12 8.8.8.8
```

Étape 2 : Mise à jour du système, installation et configuration des outils nécessaires

1. Mise à jour du système :
 - a. `sudo apt -y update && sudo apt upgrade`

2. Installer le serveur de la base de données MariaDB et le configurer
La base de données est un composant essentiel pour Zabbix, car elle stocke toutes les données de supervision.

- a. `sudo apt install mariadb-server mariadb-client -y`
- b. `sudo systemctl start mariadb`
- c. `sudo systemctl enable mariadb`
- d. `sudo mysql_secure_installation`

Effectuer la sécurisation de base à l'aide du script "mysql_secure_installation". Lors de l'exécution de "mysql_secure_installation", appuyer sur 'y' à toutes les étapes sauf lorsque vous devez définir un mot de passe.

3. Ajouter le dépôt Zabbix
 - a. `wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest+debian12_all.deb`

- b. `sudo dpkg -i zabbix-release_latest+debian12_all.deb`
 - c. `sudo apt update`
- 4. Installer Zabbix et ses dépendances
`sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y`
- 5. Configurer la base de données pour Zabbix
 - a. Connexion à MariaDB
`sudo mysql -u root -p`
 - b. Créer une base de données dédiée pour Zabbix et configurer un utilisateur spécifique avec les commandes suivantes :
 - i. `CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;`
 - ii. `CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'VotreMotDePasseZabbix';`
 - iii. `GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';`
 - iv. `SET GLOBAL log_bin_trust_function_creators = 1;`
 - v. `EXIT;`
 - c. Importer le schéma initial de Zabbix en utilisant le mot de passe de votre utilisateur "zabbix"
 - i. `zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix`
 - d. Désactiver l'option `log_bin_trust_function_creators` :
 - i. `sudo mysql -u root -p -e "SET GLOBAL log_bin_trust_function_creators = 0;"`
- 6. Configurer Zabbix Server
 - a. Modifier le fichier de configuration de Zabbix Server pour inclure les informations d'accès à la base de données :
 - i. `sudo nano /etc/zabbix/zabbix_server.conf`
 - ii. Trouver et modifier les lignes :
`DBPassword=VotreMotDePasseZabbix`
`EnableGlobalScripts=1`
- 7. Configurer Apache et PHP

Pour assurer le bon fonctionnement de l'interface web de Zabbix, il est nécessaire de configurer correctement PHP qui est géré par Apache.

 - a. Modifier les paramètres de configuration de PHP :
 - i. `sudo nano /etc/zabbix/apache.conf`
 - b. Indiquer le bon fuseau horaire
 - i. `php_value date.timezone Europe/Paris`
 - c. Redémarrer Apache pour appliquer les modifications
 - i. `sudo a2enmod php8.2`

- ii. `sudo systemctl restart apache2`
- iii. `sudo systemctl enable apache2`

8. Configurer le Pare-feu

Pour sécuriser le serveur, il faut configurer le pare-feu pour n'autoriser que les ports nécessaires à Zabbix.

- a. `sudo apt install -y iptables`
- b. `sudo iptables -A INPUT -p tcp --dport 10051 -j ACCEPT`
- c. `sudo iptables -A INPUT -p tcp --dport 10050 -j ACCEPT`
- d. `sudo mkdir -p /etc/iptables`
- e. `sudo sh -c "iptables-save > /etc/iptables/rules.v4"`
- f. `sudo iptables-restore < /etc/iptables/rules.v4`

9. Démarrer les services Zabbix

- a. `sudo systemctl restart zabbix-server zabbix-agent apache2`
- b. `sudo systemctl enable zabbix-server zabbix-agent apache2`

10. Accéder à l'interface web de Zabbix pour finaliser la configuration

- a. Dans la barre d'adresse du navigateur
 - i. <http://172.16.19.10/zabbix>



Vérifier que tous les prérequis sont "OK".

Vérification des prérequis

	Valeur actuelle	Requis	
Version de PHP	8.2.24	8.0.0	OK
Option PHP "memory_limit"	128M	128M	OK
Option PHP "post_max_size"	16M	16M	OK
Option PHP "upload_max_filesize"	2M	2M	OK
Option PHP "max_execution_time"	300	300	OK
Option PHP "max_input_time"	300	300	OK
soutien de bases de données par PHP	MySQL		OK
bcmath pour PHP	actif		OK
mbstring pour PHP	actif		OK
Option PHP "mbstring.func_overload"	inatif	inatif	OK

[Retour](#)[Prochaine étape](#)

Par la suite, renseigner le nom de votre base de donnée, votre utilisateur et son mot de passe, ici :

- Nom de la base de données : zabbix
- Utilisateur : zabbix
- Mot de passe : VotreMotDePasseZabbix

Configurer la connexion à la base de données

Veuillez créer la base de données manuellement et configurer les paramètres de connexion. Appuyez sur le bouton "Prochaine étape" quand c'est fait.

Type de base de données

Hôte base de données

Port de la base de données 0 - utiliser le port par défaut

Nom de la base de données

Stocker les informations d'identification dans ☒ Texte brut ☐ Coffre HashiCorp ☐ Coffre CyberArk

Utilisateur

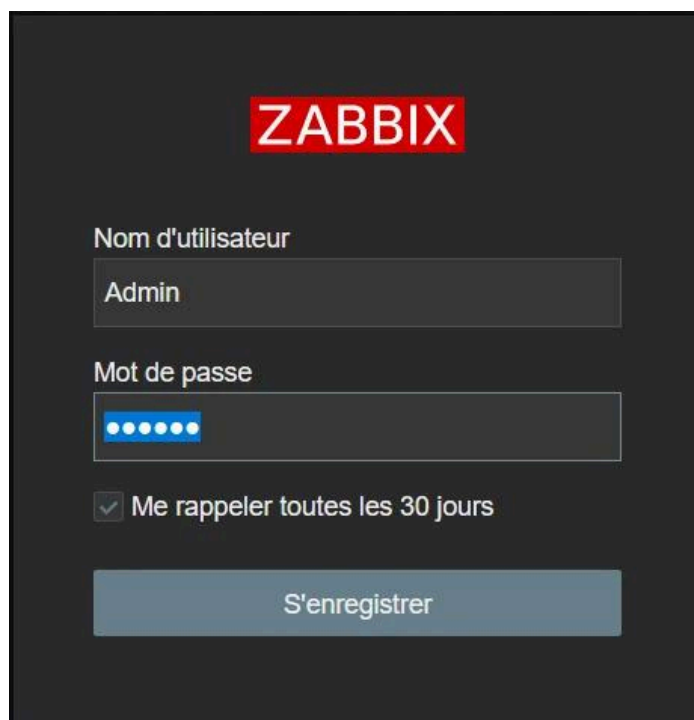
Mot de passe

Chiffrement TLS de la base de données La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix) ou de la mémoire partagée (Windows).

[Retour](#)[Prochaine étape](#)

Pour finir, nommer le serveur et accéder à l'interface Zabbix avec les identifiants :

- Login : Admin
- Mot de passe : zabbix



ZABBIX

Nom d'utilisateur

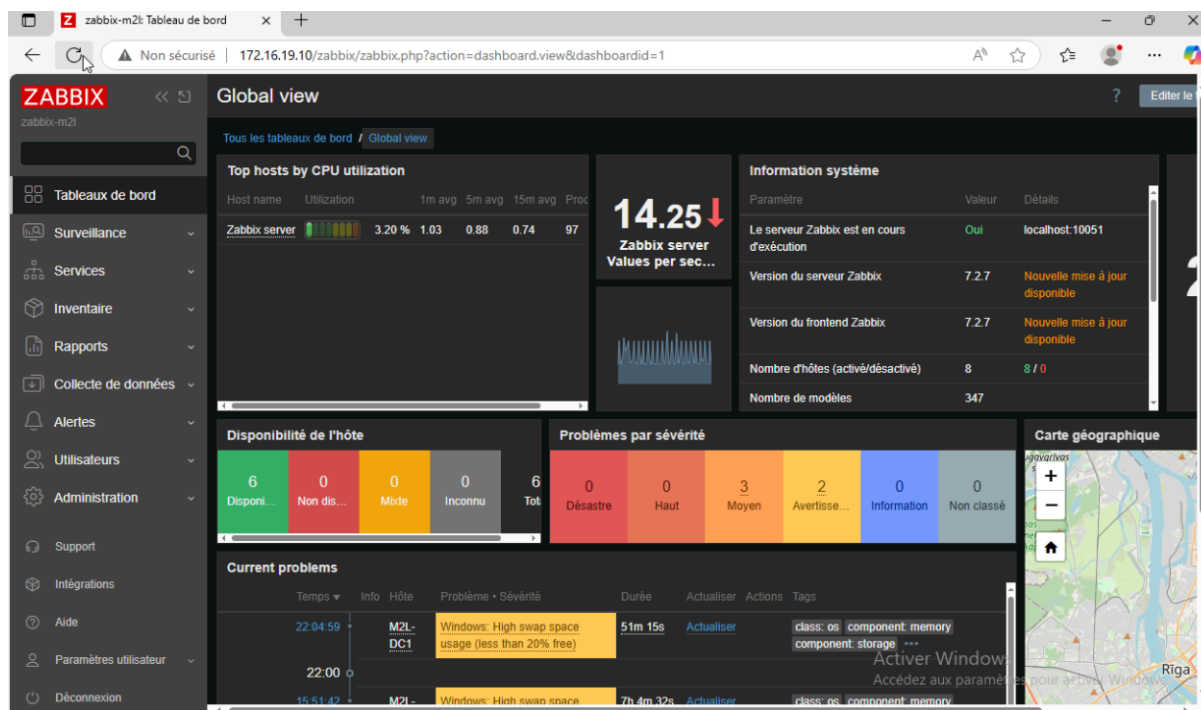
Admin

Mot de passe

Me rappeler toutes les 30 jours

S'enregistrer

Étape 3 : Accéder à l'interface Zabbix



ZABBIX Global view

Tous les tableaux de bord / Global view

Top hosts by CPU utilization

Host name	Utilization	1m avg	5m avg	15m avg	Proc
Zabbix server	3.20 %	1.03	0.88	0.74	97

14.25
Zabbix server
Values per sec...

Information système

Paramètre	Valeur	Détails
Le serveur Zabbix est en cours d'exécution	Oui	localhost:10051
Version du serveur Zabbix	7.2.7	Nouvelle mise à jour disponible
Version du frontend Zabbix	7.2.7	Nouvelle mise à jour disponible
Nombre d'hôtes (activé/désactivé)	8 / 0	
Nombre de modèles	347	

Disponibilité de l'hôte

Disponi...	Non dis...	Mixte	Inconnu	Tot
6	0	0	0	6

Problèmes par sévérité

Désastre	Haut	Moyen	Avertisse...	Information	Non classé
0	0	3	2	0	0

Current problems

Temps	Info	Hôte	Problème • Sévérité	Durée	Actualiser	Actions	Tags
22:04:59		M2L-DC1	Windows: High swap space usage (less than 20% free)	51m 15s	Actualiser		class: os component: memory component: storage ...
22:00		M2L-	Windows: High swap space	7h 4m 32s	Actualiser		class: os component: memory

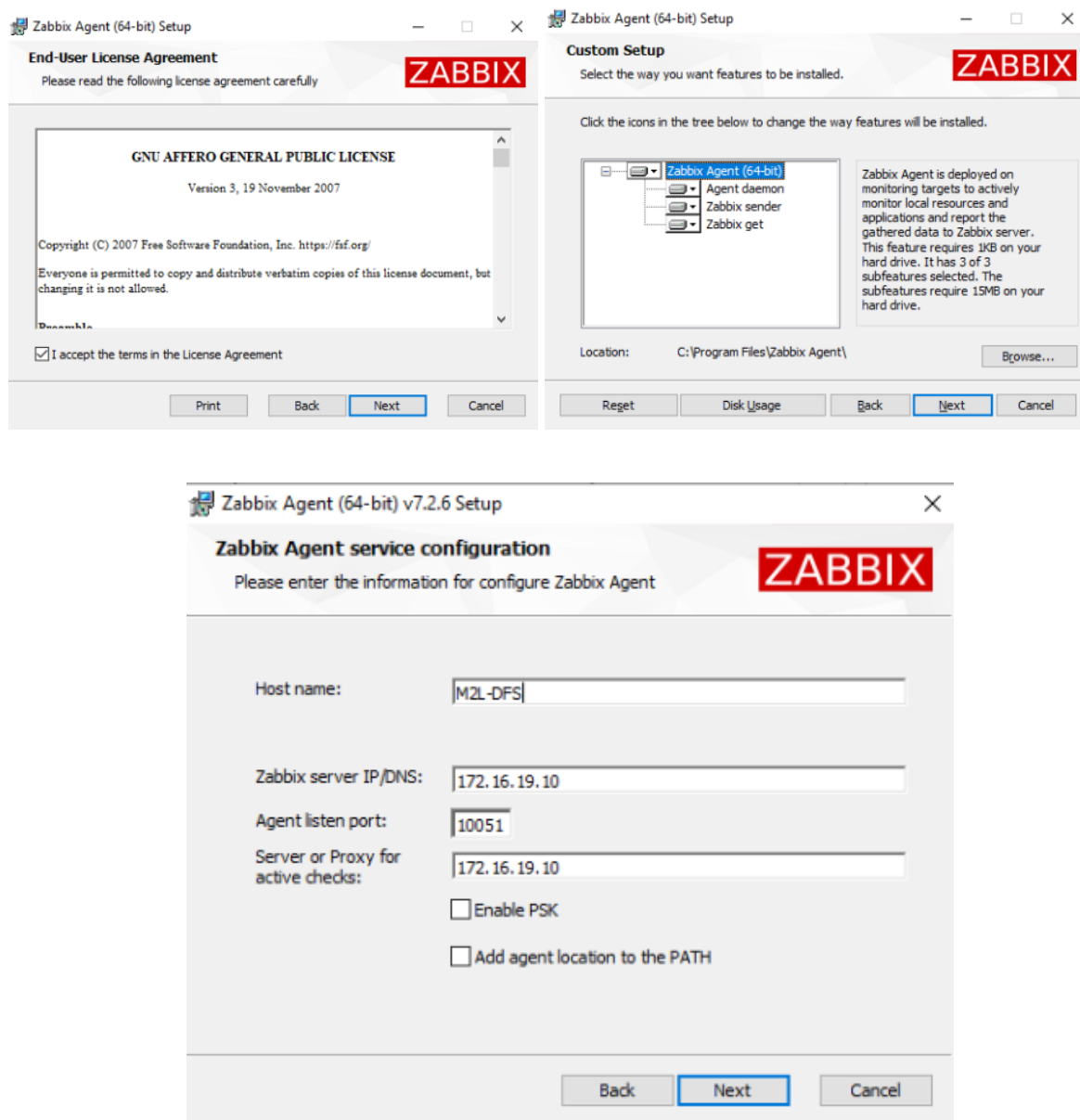
Carte géographique

Rīga

D. Monitoring des serveurs et routeurs

1. Installation de l'agent Zabbix sur les serveurs Windows

Exemple d'installation d'agent Zabbix sur le serveur de fichiers :



Lors de l'installation de l'agent zabbix, il faut renseigner :

- Le nom de la machine sur laquelle est installé l'agent
- L'adresse IP du serveur Zabbix
- Le port sur lequel communique les machines

2. Activation du service SNMP sur Pfsense

Il n'est pas possible d'installer l'agent Zabbix sur les Pfsense, alors pour communiquer, le serveur Zabbix et les Pfsense utilisent le protocole SNMP qui écoute sur les ports 161 et 162.

Il est possible d'activer le protocole sur Pfsense sur "Service > SNMP"

The screenshot displays the Pfsense web interface for the 'Services > SNMP' configuration page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into several sections:

- SNMP Daemon:** A toggle switch is set to 'Enable', with a checkbox 'Enable the SNMP Daemon and its controls' checked.
- SNMP Daemon Settings:**
 - Polling Port:** Set to '161'. A note states: 'Enter the port to accept polling events on (default 161).'.
 - System Location:** An empty text field.
 - System Contact:** An empty text field.
 - Read Community String:** Set to 'public'. A note states: 'The community string is like a password, restricting access to querying SNMP to hosts knowing the community string. Use a strong value here to protect from unauthorized information disclosure.'
- SNMP Traps Enable:** A toggle switch is set to 'Enable', with a checkbox 'Enable the SNMP Trap and its controls' unchecked.
- SNMP Modules:**
 - SNMP modules:** A list of modules with checkboxes: MibII (checked), Netnranh (unchecked), and others.
- Interface Binding:**
 - Internet Protocol:** Set to 'IPv4'.
 - Bind Interfaces:** A dropdown menu showing 'All', 'WAN', 'PROD', and 'DMZ'.

At the bottom of the page, there is a 'Save' button and a watermark for 'Activer Windows'.

Une fois l'agent installé sur les serveurs Windows (AD et fichiers) et sur les routeurs Pfsense, il est nécessaire de déclarer les machines sur l'interface Zabbix.

3. Déclaration des machines sur Zabbix

a. Déclaration du routeur Pfsense 1

The screenshot shows the Zabbix 'Host' configuration page for a host named 'PfSense1'. The 'Nom de l'hôte' field is set to 'PfSense1' and 'Nom visible' is also 'PfSense1'. Under 'Modèles', the 'PFSense by SNMP' template is selected. In the 'Groupes d'hôtes' section, the 'Routeurs' group is selected. The 'Interfaces' table shows one interface named 'SNMP' with IP address '172.16.19.1', connected to 'IP' and 'DNS' on port '161'. The 'Description' field is empty. At the bottom, there are buttons for 'Actualiser', 'Clone', 'Supprimer', and 'Annuler'.

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
SNMP	172.16.19.1		IP DNS	161	<input checked="" type="radio"/> Supprimer

- Déclaration du nom de l'hôte
- Utilisation du template de surveillance déjà existant sur Zabbix (PFSense by SNMP)
- Ajout au groupe d'hôte "Routeurs"
- Création de l'interface par SNMP avec adresse IP du routeur et le port 161.

b. Déclaration du serveur de fichiers

The screenshot shows the Zabbix 'Host' configuration page for a host named 'M2L-DFS'. The 'Nom de l'hôte' field is set to 'M2L-DFS' and 'Nom visible' is also 'M2L-DFS'. Under 'Modèles', the 'Windows by Zabbix agent' template is selected. In the 'Groupes d'hôtes' section, the 'Serveurs' group is selected. The 'Interfaces' table shows one interface named 'Agent' with IP address '172.16.20.13', connected to 'IP' and 'DNS' on port '10051'. The 'Description' field is empty. At the bottom, there are buttons for 'Actualiser', 'Clone', 'Supprimer', and 'Annuler'.

Type	adresse IP	Nom DNS	Connexion à	Port	Défaut
Agent	172.16.20.13		IP DNS	10051	<input checked="" type="radio"/> Supprimer

- Déclaration du nom de la machine
- Ajout du template déjà existant pour Windows (Windows by Zabbix Agent)
- Ajout au groupe d'hôtes "Serveurs"
- Création de l'interface de communication avec le modèle Agent, l'adresse IP du serveur de fichiers et le port 10051

c. Résultat

Une fois que la disponibilité des serveurs et routeurs passent au vert, cela signifie que la connexion est établie.

E. Configuration des règles de Firewall.

F. Intégration de Zabbix à l'Active Directory.

Ajout de la machine Zabbix dans le contrôleur de domaine.

Commandes :

1. apt install realmd
Installe l'outil realmd, qui permet de découvrir et de joindre un domaine Active Directory de manière simplifiée.
2. realm discover M2L.lan
Recherche les informations sur le domaine M2L.lan (nom DNS du domaine AD) pour vérifier sa disponibilité et les méthodes d'intégration possibles.
3. apt-get install sssd-tools sssd libnss-sss libpam-sss adcli
samba-common-bin -y
Installe les dépendances nécessaires à l'authentification via AD, notamment :

- sssd : gestion des identités et de l'authentification,
 - libnss-sss et libpam-sss : intégration avec NSS et PAM,
 - adcli : outil en ligne de commande pour interagir avec AD,
 - samba-common-bin : outils Samba requis pour la communication avec le domaine.
4. `realm join --client-software=sssd 172.16.20.10 -U Administrateur`
Rejoint le domaine Active Directory via l'IP du contrôleur de domaine 172.16.20.10 en utilisant l'utilisateur Administrateur. Le logiciel client sssd est utilisé pour gérer l'authentification.

V. Tests

A. Failover PFSense

PFSense 1 :

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
PROD@2	172.16.20.3/26	CARP PROD	▶ MASTER
DMZ@3	172.16.19.3/26	CARP DMZ	▶ MASTER
CLIENTS@4	172.16.21.3/24	CARP CLIENTS	▶ MASTER
WAN@5	10.190.1.100/22	VIP WAN	▶ MASTER

PFSense 2 :

CARP Status			
Interface and VHID	Virtual IP Address	Description	Status
PROD@2	172.16.20.3/26	CARP PROD	⏸ BACKUP
DMZ@3	172.16.19.3/26	CARP DMZ	⏸ BACKUP
CLIENTS@4	172.16.21.3/24	CARP CLIENTS	⏸ BACKUP
WAN@5	10.190.1.100/22	VIP WAN	⏸ BACKUP

Pour tester le basculement de la PFSense 1 vers la PFSense 2, il est possible soit :

- Eteindre la PFSense master
- Désactiver CARP temporairement sur la PFSense 1

Lorsque ce test est effectué, on peut voir que la PFSense 2 passe en master.

B. Connexion au domaine depuis le client

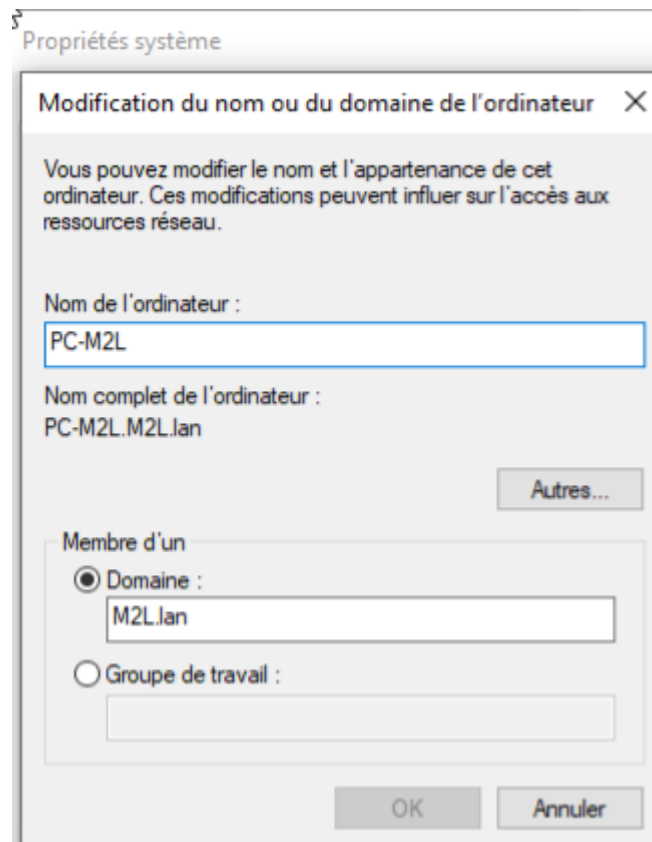
- Vérifier que la machine est dans le bon réseau
- S'assurer qu'elle possède le bon DNS

```
Carte Ethernet Ethernet :  
  
Suffixe DNS propre à la connexion. . . : M2L.lan  
Description. . . . . : Red Hat VirtIO Ethernet Adapter  
Adresse physique . . . . . : 00-11-22-C8-D5-37  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . : Oui  
Adresse IPv6 de liaison locale. . . . : fe80::b28e:82b7:f4c6:aaa1%14(préfééré)  
Adresse IPv4. . . . . : 172.16.21.53(préfééré)  
Masque de sous-réseau. . . . . : 255.255.255.0  
Bail obtenu. . . . . : vendredi 20 juin 2025 14:05:17  
Bail expirant. . . . . : mardi 24 juin 2025 02:05:23  
Passerelle par défaut. . . . . : 172.16.21.3  
Serveur DHCP . . . . . : 172.16.20.10  
IAID DHCPv6 . . . . . : 335548706  
DUID de client DHCPv6. . . . . : 00-01-00-01-2F-E1-E8-21-00-11-22-C8-D5-37  
Serveurs DNS. . . . . : 172.16.20.10  
172.16.20.12  
NetBIOS sur Tcpip. . . . . : Activé
```

- S'assurer que le client peut contacter le serveur Active Directory (+ résolution DNS)

```
C:\Users\t.basol>ping M2L-DC1  
  
Envoi d'une requête 'ping' sur M2L-DC1.M2L.lan [172.16.20.10] avec 32 octets de données :  
Réponse de 172.16.20.10 : octets=32 temps<1ms TTL=127  
Réponse de 172.16.20.10 : octets=32 temps<1ms TTL=127  
Réponse de 172.16.20.10 : octets=32 temps<1ms TTL=127  
Réponse de 172.16.20.10 : octets=32 temps<1ms TTL=127  
  
Statistiques Ping pour 172.16.20.10:  
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
Durée approximative des boucles en millisecondes :  
Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

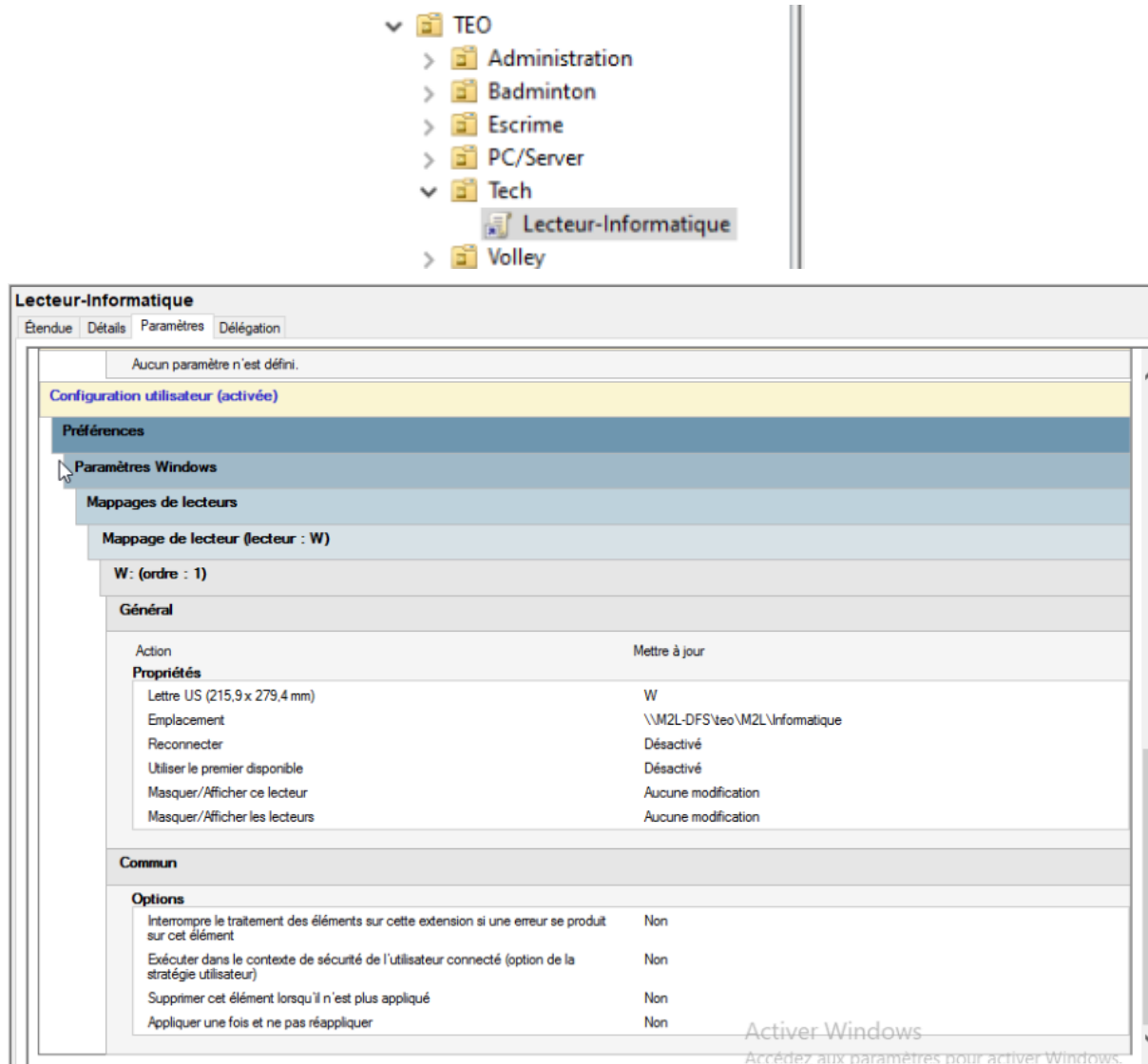
- Joindre la machine au domaine



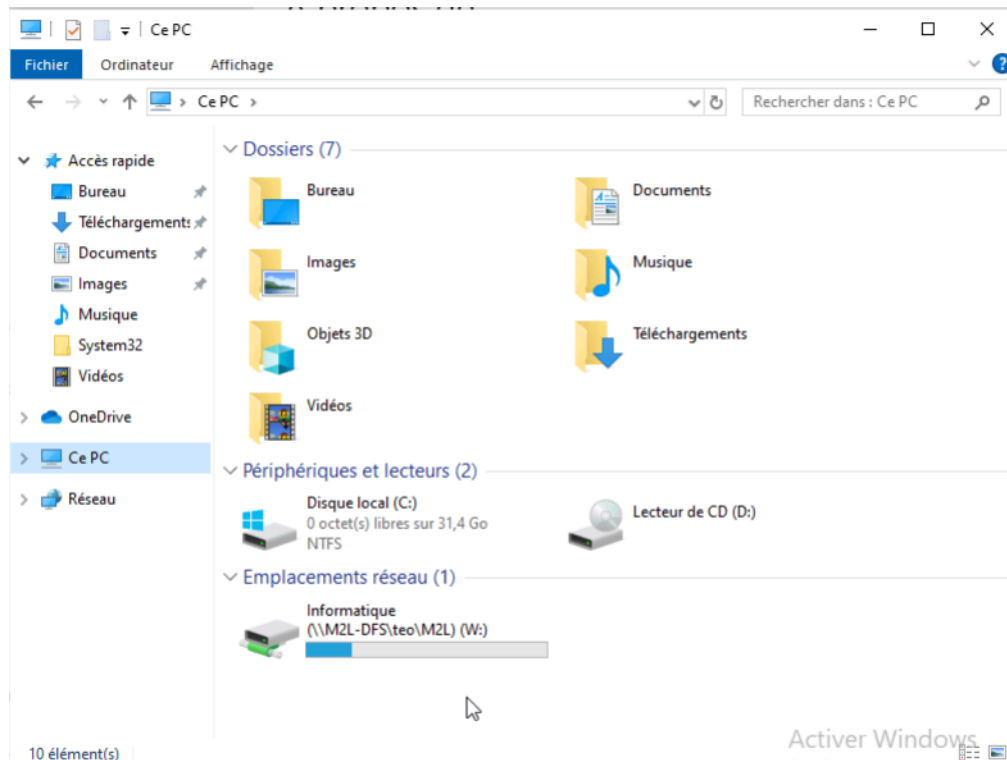
- Se connecter à un utilisateur de l'Active Directory

C. GPO appliquées (Lecteurs mappés) et accès aux fichiers partagés : droits respectés

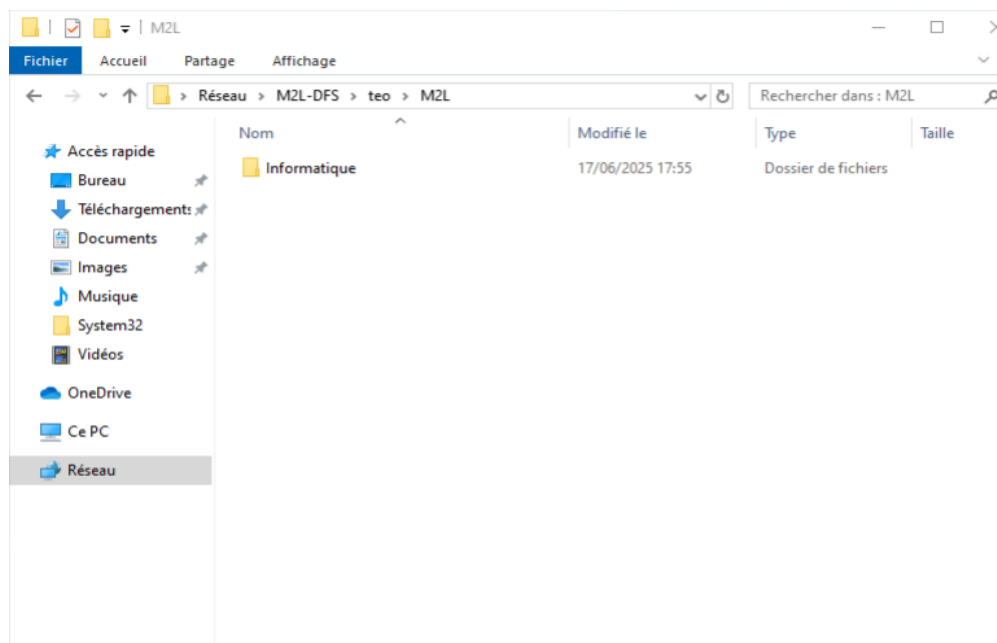
Exemple de GPO pour un lecteur mappé pour le serveur de fichiers



Connexion au client avec un compte technicien pour vérifier si le lecteur informatique s'affiche :



Vérification que les utilisateurs n'ont accès qu'à leurs partages, exemple avec un profil technicien



D.Surveillance Zabbix : tous les équipements sont visibles et monitorer

Vérifier la disponibilité et la communication des machines :

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques
glpi	172.16.19.11:10050	ZBX	class: os target: linux	Activé	Dernières données 58	1	Graphiques 11
M2L-DC1	172.16.20.10:10051	ZBX	class: os target: windows	Activé	Dernières données 126	1	Graphiques 18
M2L-DC2	172.16.20.12:10051	ZBX	class: network class: os target: icmp	Activé	Dernières données 130	1	Graphiques 18
M2L-DFS	172.16.20.13:10051	ZBX	class: os target: windows	Activé	Dernières données 103	1	Graphiques 12
M2L-WDS	172.16.20.11:10051	ZBX	class: os target: windows	Activé	Dernières données 105	1	Graphiques 12
PfSense1	172.16.19.1:161	SNMP	class: software target: pfsense	Activé	Dernières données 174	1	Graphiques 19
PfSense2	172.16.19.2:161	SNMP	class: software target: pfsense	Activé	Dernières données 174	1	Graphiques 19
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux	Activé	Dernières données 131	1	Graphiques 12

On peut voir que tous les équipements sont disponibles, grâce aux icônes verts.

Vérifier si les problèmes remontent sur l'interface (Surveillance > Problèmes) :

	Temps	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Actualiser	Actions	Tags
	10:20:34	Moyen	10:21:33	RÉSOLU		glpi	Linux: Load average is too high (per CPU load over 1.5 for 5m)	59s	Actualiser	2	class: os scope: capac
	10:20:17	Moyen	10:21:09	RÉSOLU		Zabbix server	Linux: Load average is too high (per CPU load over 1.5 for 5m)	52s	Actualiser	2	class: os scope: capac
Aujourd'hui											
	22/06/2025 15:51:42	Avertissement		PROBLÈME		M2L-WDS	Windows: High swap space usage (less than 20% free)	18h 32m 28s	Actualiser		class: os component: s
Hier											
	19/06/2025 11:07:36	Moyen		PROBLÈME		PfSense 1	PfSense: DHCP server is not running	3j 23h 16m	Actualiser	1	class: software scope: availa
	17/06/2025 15:26:34	Moyen		PROBLÈME		glpi	Linux: High memory utilization (>90% for 5m)	5j 18h 57m	Actualiser		class: os scope: capac
	06/06/2025 17:20:04	Moyen		PROBLÈME		Zabbix server	Linux: High memory utilization (>90% for 5m)	16j 17h 4m	Actualiser		class: os scope: capac

VI. Conclusion et Préconisations

A. Conclusion

Ce projet a permis de bâtir une infrastructure réseau fiable et sécurisée pour la M2L, parfaitement adaptée à une organisation moderne. Chaque élément a été conçu pour être robuste, facile à gérer et réactif en cas de problème.

Les points clés du projet sont :

- **Haute disponibilité avec Pfsense (CARP) :** Deux pare-feux Pfsense garantissent un accès internet constant, même en cas de panne. Le basculement est automatique et transparent pour les utilisateurs.
- **Sécurité renforcée par segmentation réseau (CLIENTS / PROD / DMZ) :** Le réseau est découpé en zones isolées, permettant un filtrage précis et une meilleure protection des services critiques (PROD), des services exposés (DMZ) et des utilisateurs finaux (CLIENTS).
- **Gestion centralisée des utilisateurs avec Active Directory :** Un serveur Active Directory simplifie la gestion des comptes, des droits d'accès et des politiques de sécurité (GPO), permettant un déploiement rapide des règles communes.
- **Supervision proactive avec Zabbix en DMZ :** Zabbix surveille en temps réel l'état des équipements. Les alertes aident à détecter et résoudre rapidement les dysfonctionnements, réduisant ainsi les temps d'arrêt.

En résumé, cette infrastructure est désormais prête à supporter les activités de la M2L de manière fiable, avec une bonne capacité d'évolution.

B. Préconisations

Pour maintenir et améliorer cette infrastructure, voici quelques axes d'amélioration :

- **Ajouter un serveur de sauvegarde dédié :** Mettre en place une solution de sauvegarde automatique vers un NAS ou un serveur distant pour protéger les données critiques du serveur de fichiers.
- **Étendre la supervision :** Intégrer d'autres équipements (imprimantes, NAS, points d'accès Wi-Fi, onduleurs, caméras IP) à la supervision Zabbix via des protocoles comme SNMP pour une vision complète du réseau.
- **Maintenir une documentation technique à jour :** Conserver une documentation complète et sécurisée (topologie, adresses IP, mots de passe, règles firewall, procédures) pour faciliter la gestion, les audits et le dépannage.

- **Mettre en place un Plan de Reprise d'Activité et un Plan de Continuité d'Activité :** Préparer des plans structurés pour anticiper les pannes majeures, définir les étapes de redémarrage des services et, si nécessaire, prévoir un basculement vers une infrastructure secondaire.