



LIBASZ Renaud

ETSSR-2311

Technicien Supérieur Systèmes et Réseaux

RAPPORT DE PERIODE EN ENTREPRISE

Technicien informatique

ENI ECOLE INFORMATIQUE
NEUVILLY

Table des matières

1) Introduction.....	23
1.1. Mon parcours dans l'informatique	23
1.2. Pourquoi cette formation ?.....	23
1.3. L'entreprise : l'ENI.....	23
1.4. L'infrastructure.....	23
192.168.0.0/23 : Sous-réseau client :	24
192.168.2.0/25 : sous-réseau serveurs :	24
192.168.2.128/29 : DMZ :	24
2) Cadre de la période en entreprise.....	25
2.1. Objectifs	25
2.2. L'environnement.....	25
3) Serveurs Windows :	25
3.1. Active Directory.....	25
3.2. Deuxième contrôleur (tolérance de panne).....	26
3.3. Enregistrement DNS et serveur web en https	27
3.4. AD-CS sur le contrôleur de domaine 1.....	27
3.5. Installer IIS.....	28
3.6. Créer un certificat pour IIS	28
3.7. AGDLP.....	31
4) Système clients.....	32
5) Serveurs Linux	33
5.1. Serveur samba (partage de fichier).....	33
5.2. Création du dossier de partage.....	34
6) Unbound : Cache DNS et redirections.....	34
6.1. Installation et copie fichier de configuration	34
6.2. Modifier le fichier de configuration	35
6.3. Redirection Windows vers Unbound	35
7) Serveur Linux Apache Mariadb Php (LAMP) & Wordpress.....	36
7.1. Apache2/Php – Wordpress	36
7.2. Mariadb.....	37
7.3. Configuration de wordpress.....	38

8)	GLPI.....	38
8.1.	Fichier de configuration d'apache.....	39
8.2.	Base de données GLPI	39
8.3.	Installation GLPI	40
9)	Supervision : nagios	40
9.1.	Supervision.....	40
10)	Sauvegarde	42
	Debian11 vers Samba	42
	Windows 10 vers Samba	43
	GLPI	44
	Etude de sauvegarde des VM's	44
	Etude de sauvegarde des données en externe	45
11)	Conclusion	46
	Que vous a apporté, personnellement et techniquement, votre période en entreprise ?	46
	Avez-vous rencontré des difficultés et comment les avez-vous surmontées ?	46
	Confirme-t-il votre choix de parcours professionnel ?.....	47

1)INTRODUCTION

1.1. Mon parcours dans l'informatique

Extrêmement curieux du domaine avant la formation j'avais déjà vu quelques notions basiques de réseaux ainsi que de programmation. La formation m'a vraiment permis d'en apprendre encore plus sur l'informatique au travers des travaux pratiques et des mises en situations professionnelles.

1.2. Pourquoi cette formation ?

Je visais le métier de technicien informatique et le titre professionnel TSSR me semblait le plus adapté, et une école d'informatique est pour moi le meilleur choix pour une meilleure qualité de formation. Mes attentes en plus d'avoir un diplôme et de travailler dans le milieu de l'informatique, étaient de progresser dans l'informatique et d'augmenter mes compétences.

1.3. L'entreprise : l'ENI.

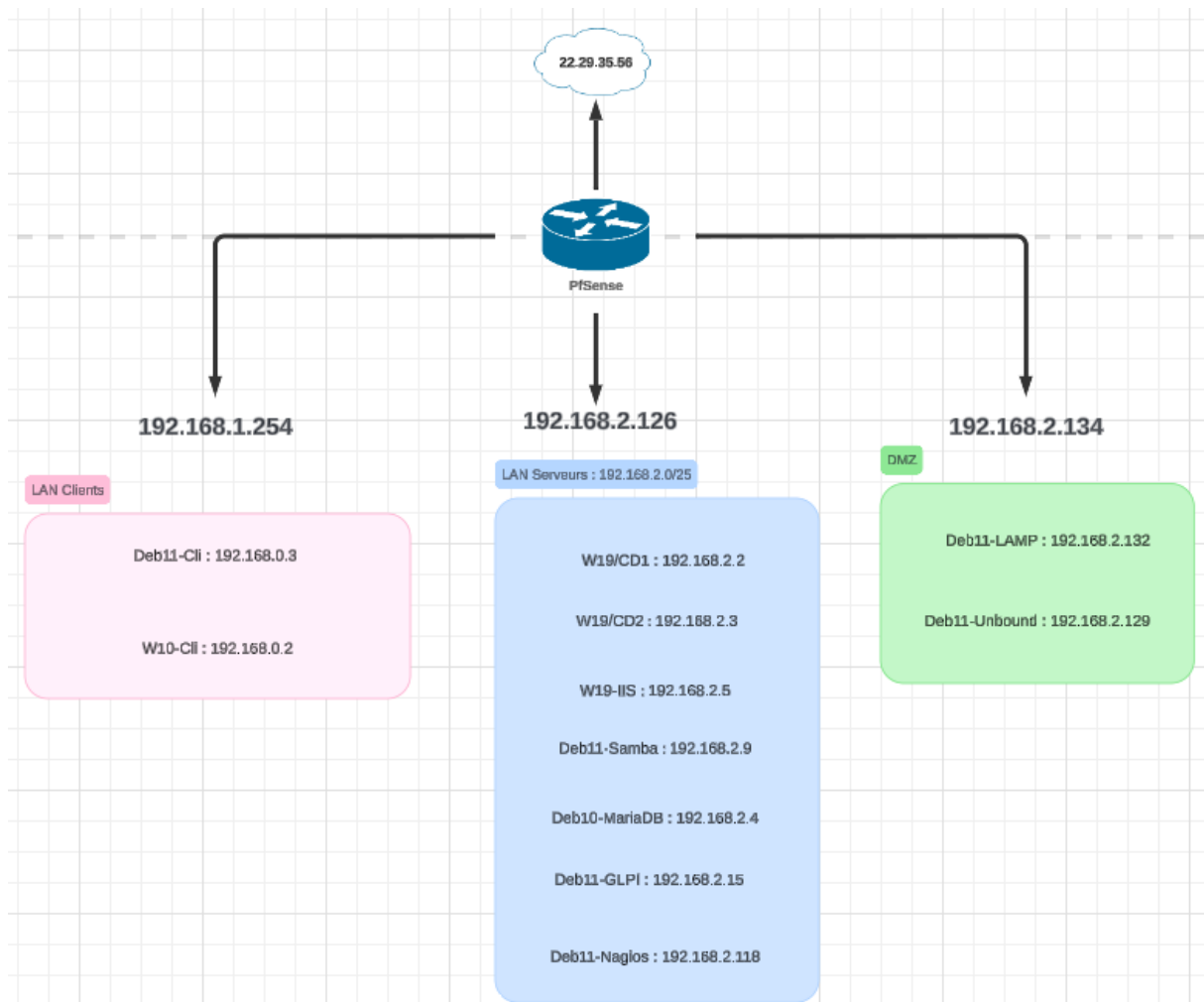
L'ENI école informatique est une école dédiée à l'informatique, qui dispense des formations reconnues par l'État de niveau Bac +2 à Bac +5. J'ai pour ma part choisi le campus en ligne de par ma situation géographique. L'ENI est présente depuis plus de 40 ans. Ses domaines d'expertise portent sur :

- **Développement – Test**
- **Système et Réseau – Cybersécurité – devOps**



1.4. L'infrastructure

Il était demandé ici, de créer une infrastructure comprenant trois sous-réseaux, un sous-réseau clients, un sous-réseau serveurs et une DMZ, en reliant le tout à un PfSense. Cette infrastructure est composée d'un Active Directory (deux CD), de deux serveurs web, IIS pour Windows et un serveur LAMP pour Linux. La résolution DNS est assurée par le CD1 qui interroge le serveur unbound qui lui-même interroge le DNS ENI. Il y a également un serveur Samba utilisé pour le partage de fichiers dans l'infrastructure et pour la sauvegarde des dossiers personnels des clients. Aussi un serveur de supervision Nagios, ainsi qu'un serveur base de données mariadb en Debian 10 hébergeant la base de données de notre serveur LAMP (WordPress) ainsi que de notre serveur GLPI. Ainsi qu'un VLAN Voix.



L'infrastructure comporte **3 sous réseaux** (Clients, Serveurs et DMZ).

L'adressage IP est le suivant :

Sous-réseau	Plage IP	Passerelle	Netmask
Clients	192.168.0.0 - 192.168.1.255	192.168.1.254	255.255.254.0 /23
Serveurs	192.168.2.0 - 192.168.2.127	192.168.2.126	255.255.255.128 /25
DMZ	192.168.2.128 – 192.168.2.135	192.168.2.134	255.255.255.248 /29

Ces sous réseaux font partie du réseau local : 192.168.0.0 /16

192.168.0.0/23 : SOUS-RESEAU CLIENT :

- ❖ 400 IP demander, ici, 510 IP disponible.

192.168.2.0/25 : SOUS-RESEAU SERVEURS :

- ❖ 100 IP demandé, ici, 126 IP disponible

192.168.2.128/29 : DMZ :

- ❖ 5 IP demandé, ici, 6 IP disponible

2) CADRE DE LA PERIODE EN ENTREPRISE

2.1. Objectifs

L'objectif de ce TP est la mise en place d'une infrastructure réseau avec notamment :

- Un active Directory
- Une second CD pour la tolérance de panne
- Un serveur web IIS sécurisé par le protocole HTTPS (création de certificat & PKI)
- Ajuster les réglages DNS de notre infrastructure
- Une partie client
- Un serveur Samba
- Un serveur Unbound cache DNS
- Une serveur base de données
- Un serveur LAMP
- Un serveur GLPI
- Un serveur Nagios
- Ainsi que de la sauvegarde et du scripting

2.2. L'environnement

Mon tuteur était Monsieur NICOLAS Cédric, Responsable Pédagogique chez ENI ECOLE.

L'environnement est virtualiser a l'aide de VMWare, le tout sur mon poste ENI. J'ai reçu le sujet car je n'ai pas trouvé de stage, j'ai fais ce sujet en télétravail, je me suis aidé de différentes IA, des cours, de mes notes, des recherches internet (forums, blog, tutoriel, ..) ainsi que des vidéos explicatives sur des sites tel que Youtube ou Dailymotion.

3) SERVEURS WINDOWS :

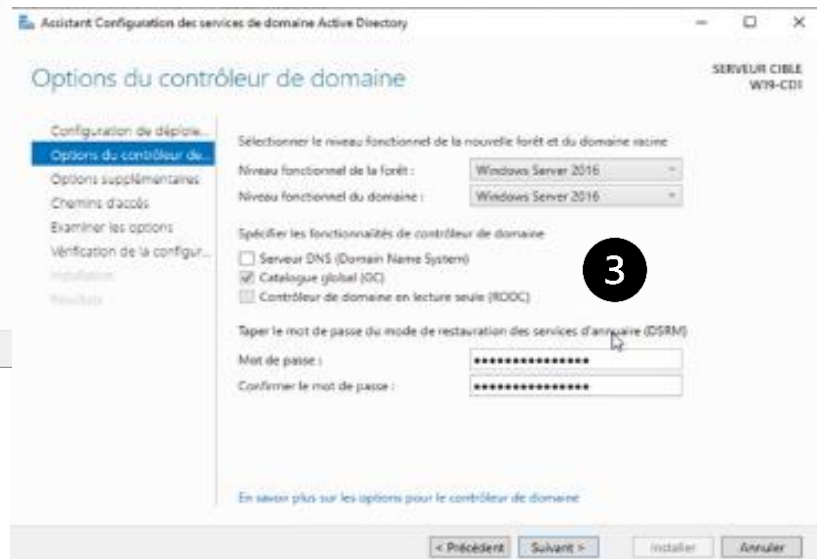
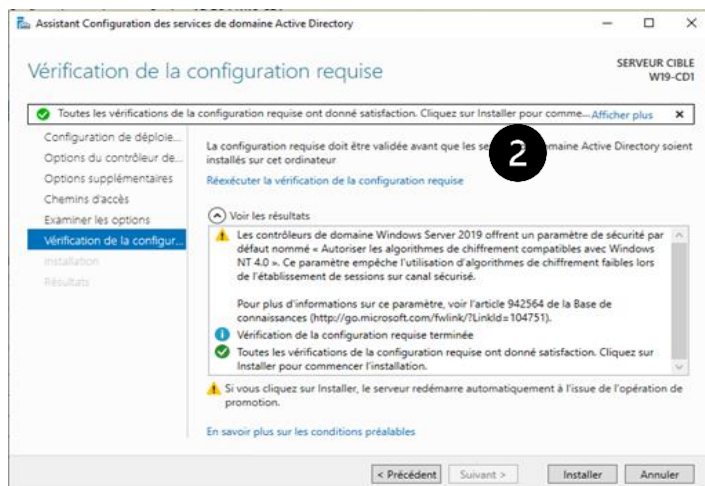
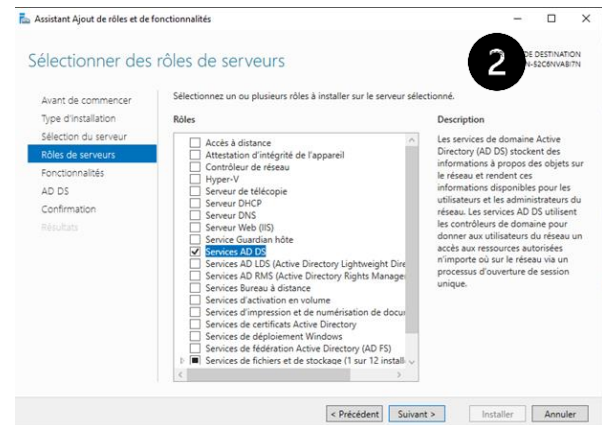
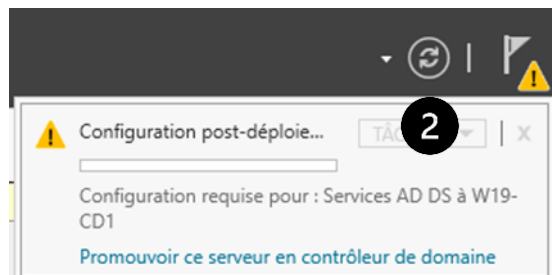
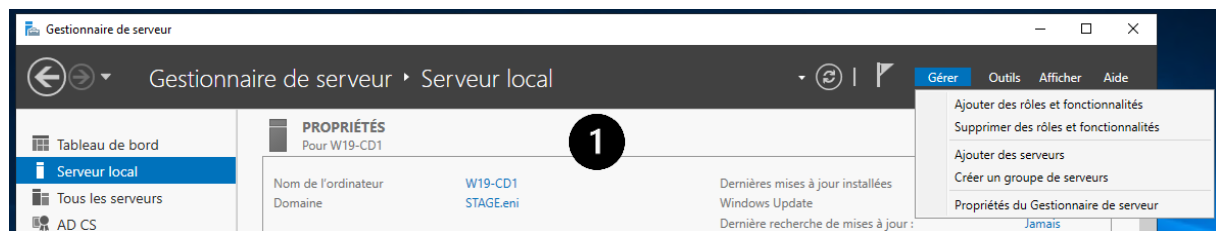
3.1. Active Directory

Pour mettre en place un active directory il faut comme pré-requis, entre autres un DNS, ici *localhost*, et une IP statique. Sur **W19-CD1** il faut installer le rôle *AD-DS*,

Ici, l'installation d'un AD sur un Windows Server 2016 (Vmware) :

- 1) Pour installer le rôle ADDS, il faut aller dans le **gestionnaire de serveur => Gérer => Ajouter des rôles et des fonctionnalités**
- 2) **Cocher** ensuite le service ADDS, finir l'installation et cliquer sur « Promouvoir ce serveur en contrôleur de domaine »
- 3) Remplir les différentes informations comme le nom de domaine, le DNS, le mot de passe, ... et installer après la confirmation

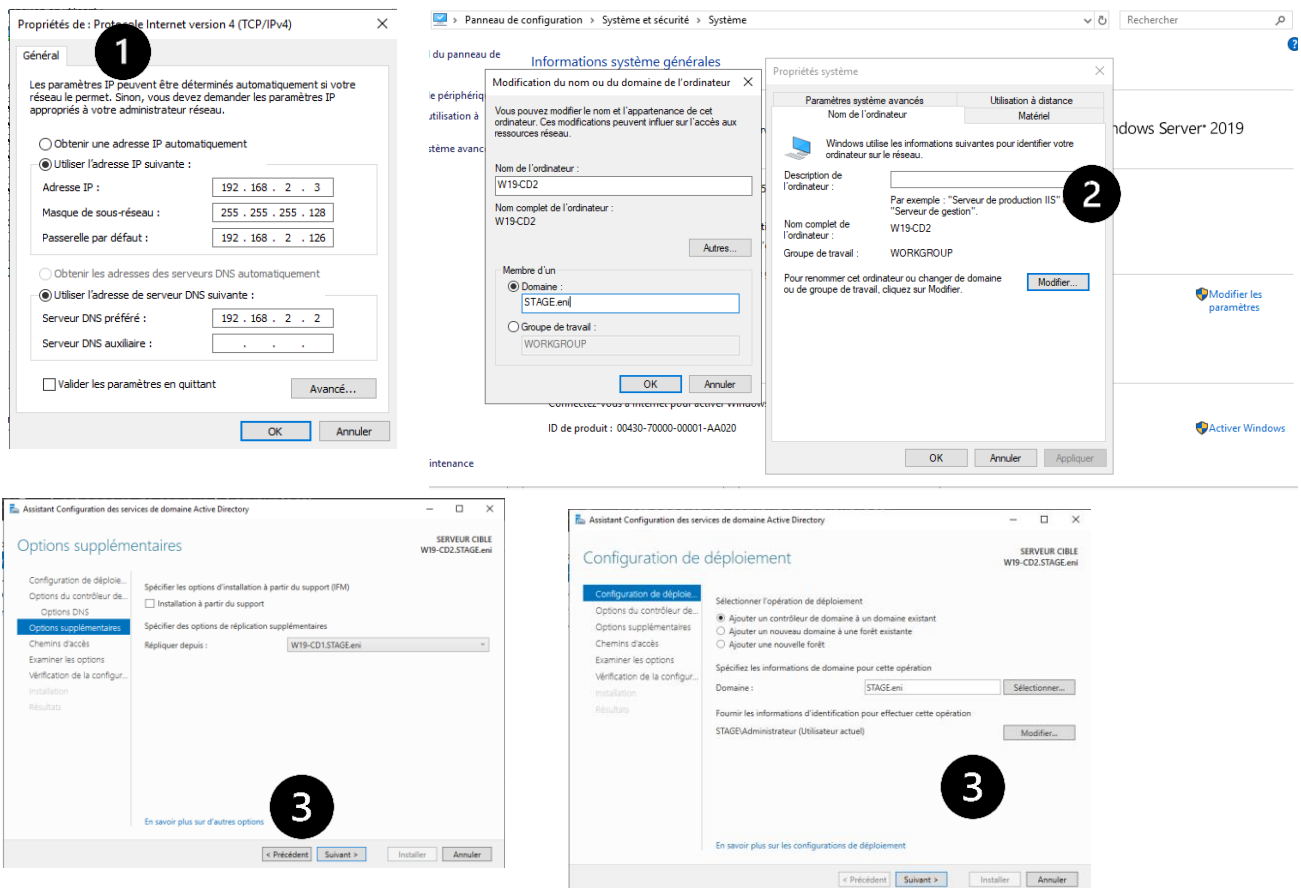
Et ensuite redémarrer l'ordinateur.



3.2. Deuxième contrôleur (tolérance de panne)

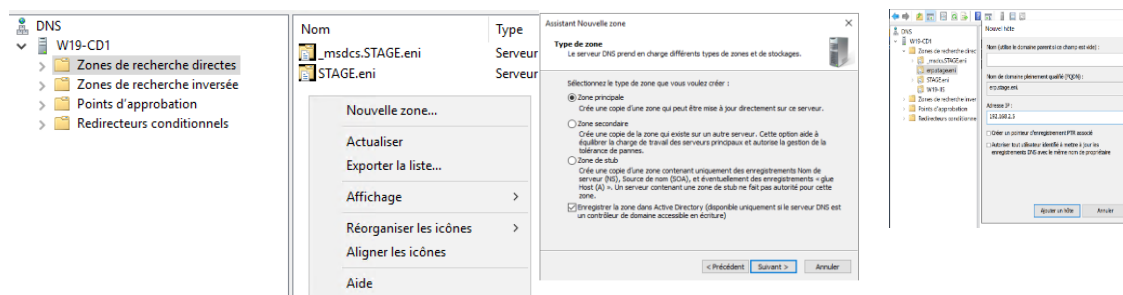
Pour ajouter un second contrôleur de domaine pour la tolérance de panne il faut :

- 1) Une ip fixe, le DNS est CD1.
- 2) Joindre le serveur Windows 2019 a notre domaine
- 3) Installer le rôle ADDS, choisir « Ajouter un controleur de domaine a un domaine existant » et l'option répliquer depuis CD1



3.3. Enregistrement DNS et serveur web en https

Pour que notre serveur Windows 2019 puisse répondre à l'adresse 'erp.stage.eni' nous allons devoir ajouter un enregistrement DNS.



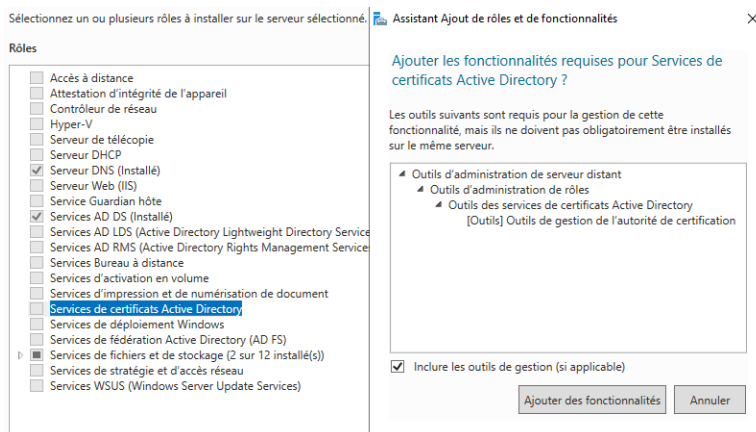
Il faut d'abord créer une **nouvelle zone** « erp.stage.eni » et ajouter un enregistrements A pointant vers notre serveur Windows 2019.

DNS	Nom	Type	Données	Horodateur
W19-CD1	(identique au dossier parent)	Source de nom (SOA)	[2], w19-cd1.stage.eni, ho...	statique
W19-CD1	(identique au dossier parent)	Seurver de noms (NS)	w19-cd2.stage.eni.	statique
W19-CD1	(identique au dossier parent)	Seurver de noms (NS)	w19-cd1.stage.eni.	statique
W19-CD1	(identique au dossier parent)	Hôte (A)	192.168.2.5	

3.4. AD-CS sur le Controleur de domaine 1

Une PKI est une infrastructure à clé publique ici cela se traduit par le fait d'installer le rôle **ADCS** et

ainsi pouvoir **valider** le certificat et agir en tant qu'autorité de certification.



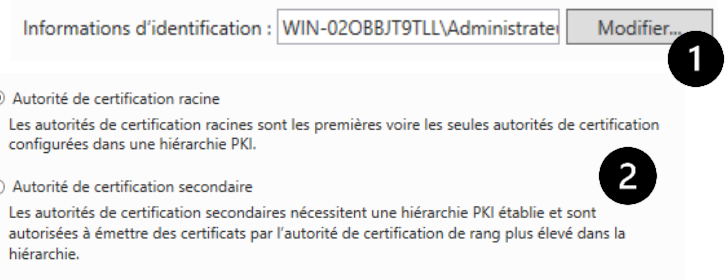
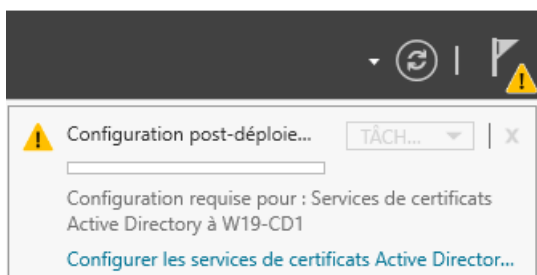
Il faut donc ajouter un rôle et ajouter le « services de certificats Active Directory »

Cliquer sur le drapeau, il faut ensuite créer notre propre clé :

1 – Mettre les informations d'identification au compte administrateur.

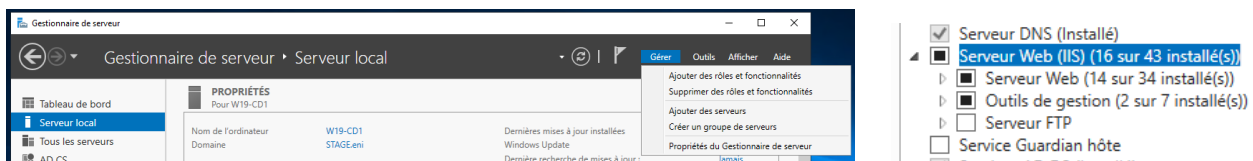
2 – Cocher autorité de certificat racine.

Ensuite créer la clé.



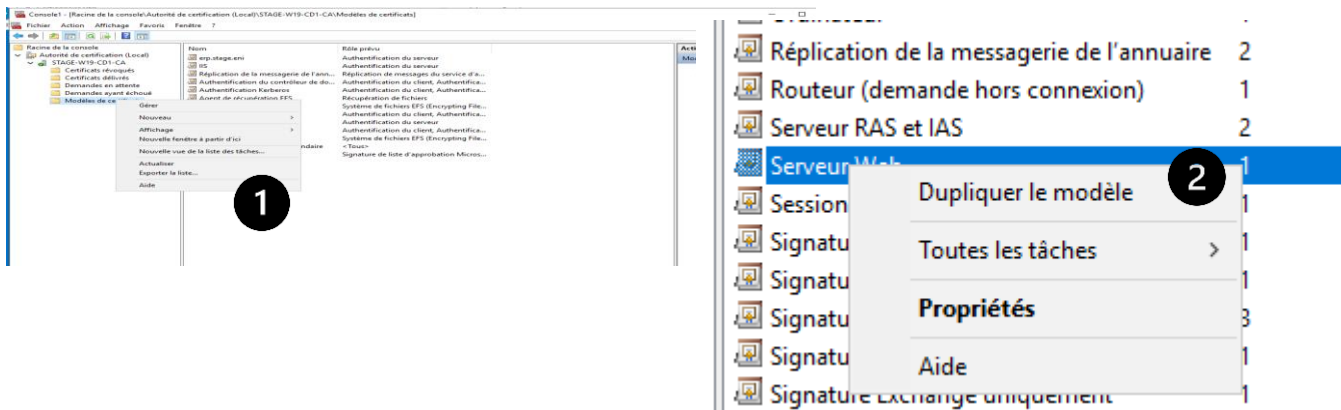
3.5. Installer IIS

Sur notre serveur web il faut installer le rôle IIS et installer le rôle Serveur Web (IIS).

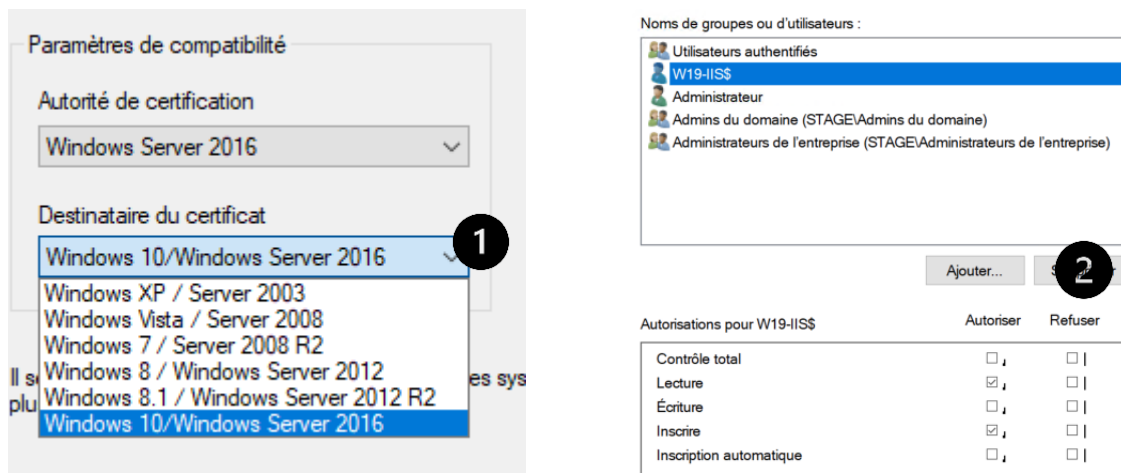


3.6. Créer un certificat pour IIS

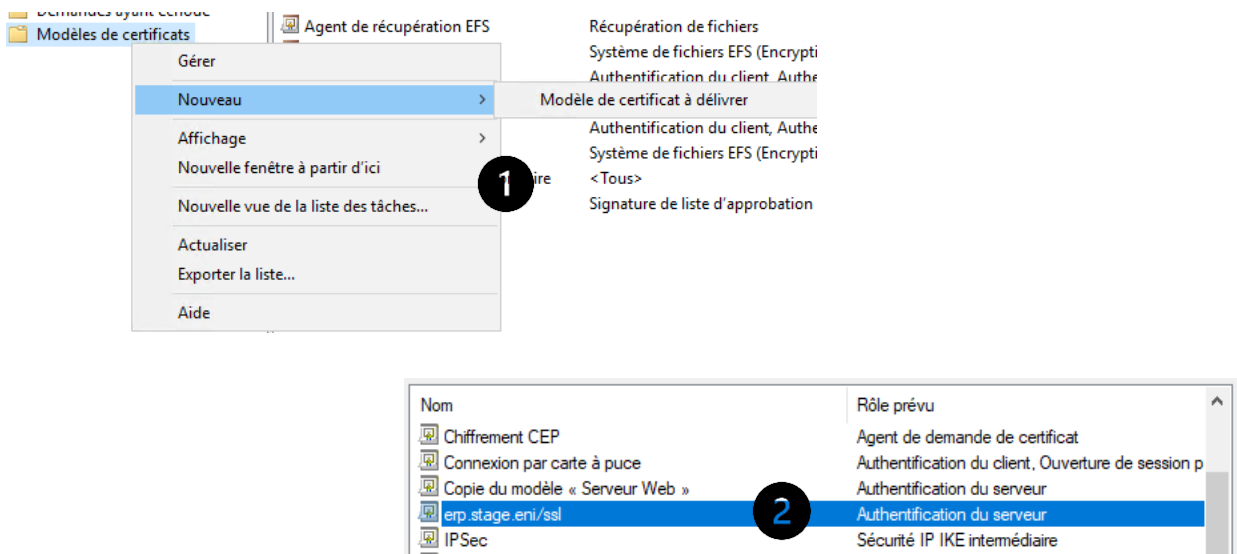
Pour créer un certificat il faut lancer une console mmc sur notre DC1, ajouter un composant/logiciel enfichable et choisir **autorité de certification**. Déroulé le menu, sur modèles de certificats choisir Gérer(1). Choisir Serveur web et dupliquer le modèles(2).



Ici les choses importantes sont les paramètres de comptabilité(1) et d'ajouter le serveur WEB dans liste des autorisations en *Lecture* et *Inscrire*(2).



Ensuite il faut aller sur modèles de certificats > nouveau > Modèle de certificats(1) a délivrer et choisir le modèle dernièrement créer(2).

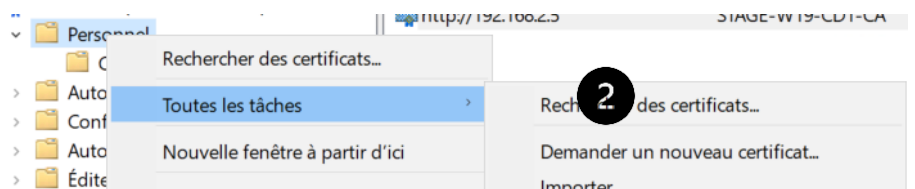
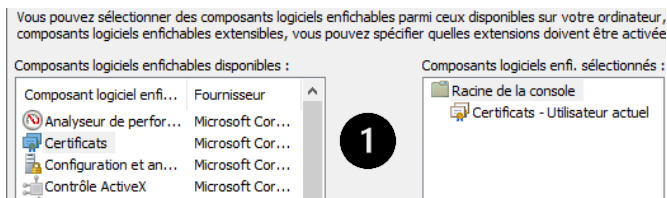


Validation du certificat :

Ensuite revenir sur le **serveur web IIS** et lancer une console mmc et ajouter le composant Certificats.

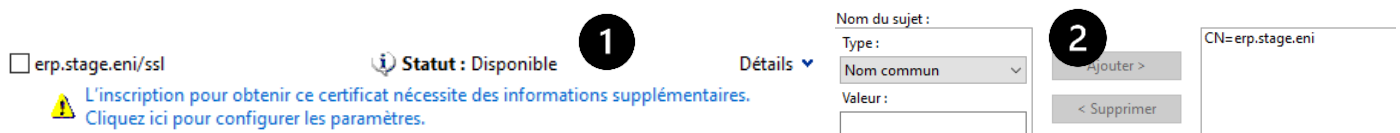
Sélectionner compte d'ordinateur.(1)

Clique droit sur Personnel, Toutes les tâches > Demander un nouveau certificat.(2)

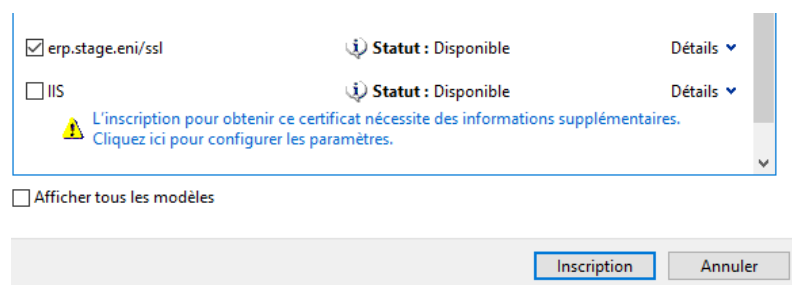


Sélectionner le certificats(1).

Ajouter comme Nom commun erp.stage.eni.(2)

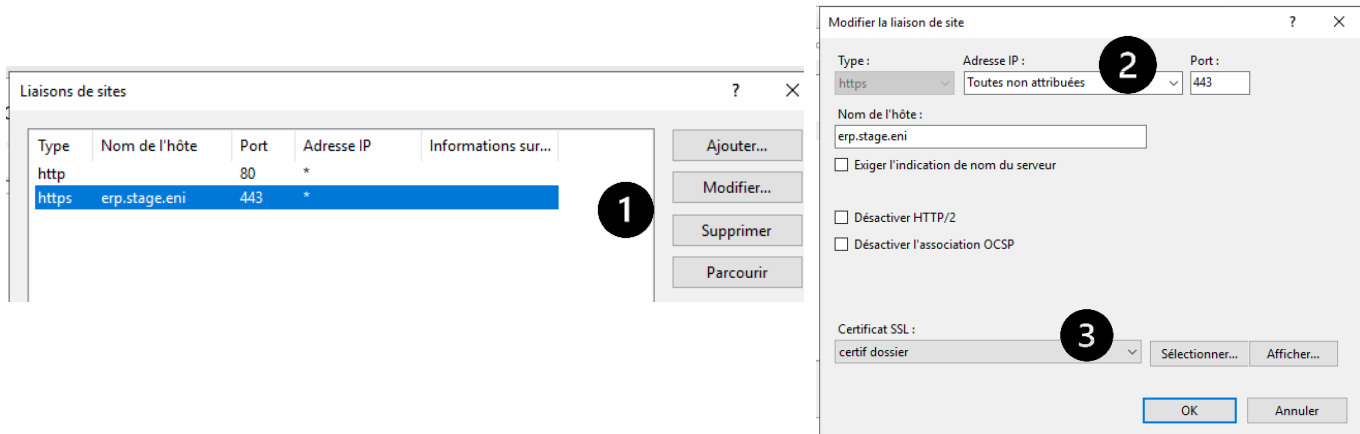


Et cliquer sur Inscription.



Ensuite il faut aller dans le gestionnaire IIS, liaisons et créer une liaison https (1), modifier.

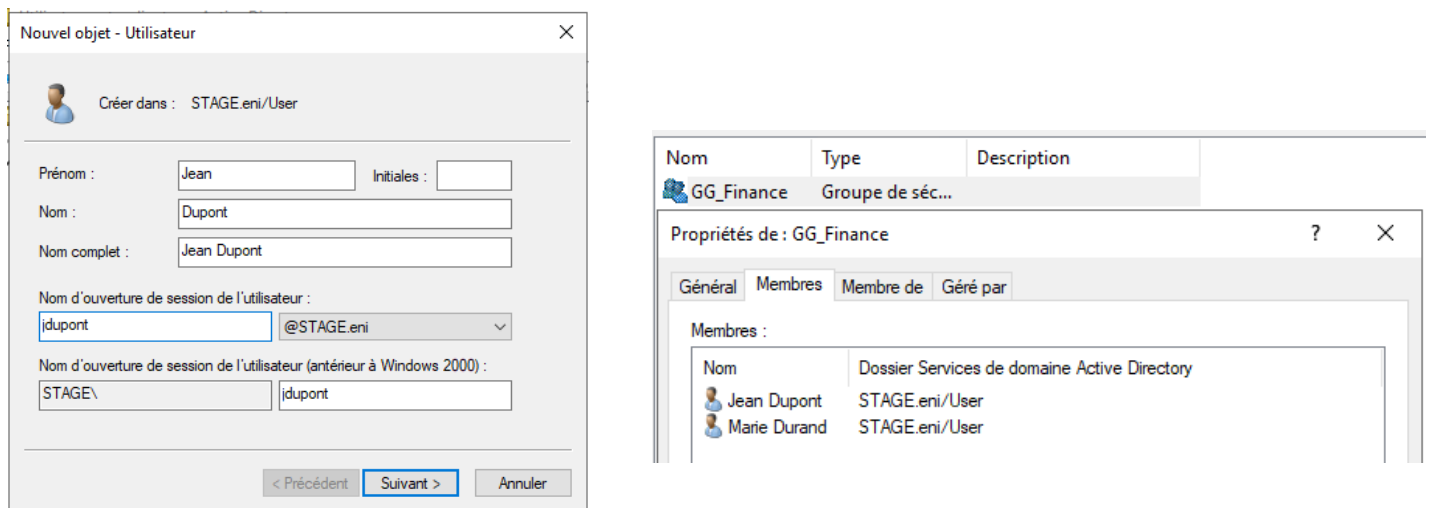
Ici(2), bien choisir le port 443 le nom de l'hôte et le bon certificat SSL (3).



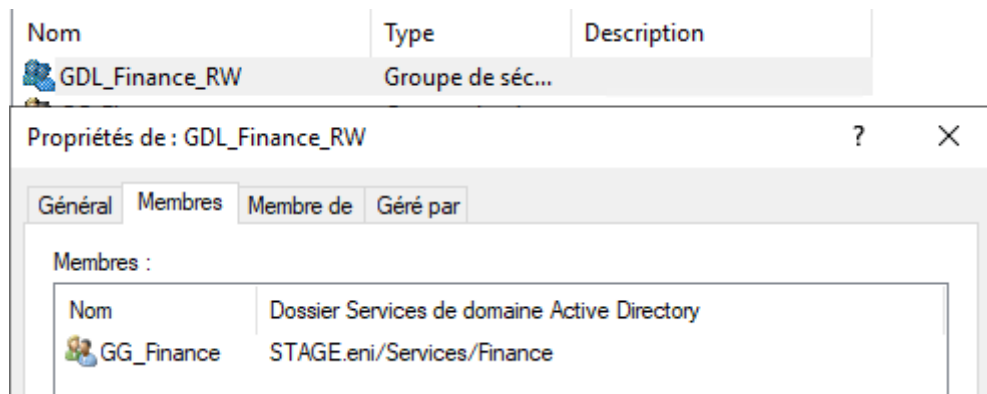
3.7. AGDLP

La méthode **AGDLP** (**A**ccount **G**lobal **D**omain **L**ocal **P**ermissions) est une méthode de gestion des groupes et des permissions. Cela fonctionne comme ça : les **utilisateurs** sont membre d'un **groupe global** (qui à une portée dans plusieurs domaines AD) et ces **groupes global** sont eux membre d'un **groupe local** (avec une portée dans le même domaine AD), et c'est ce **groupe local** que l'on va ajouter aux permissions NTFS.

Il faut aller dans l'ADUC, créer des utilisateurs, il faut ensuite créer un **groupe global** (avec par exemple le nom du service), et ajouter ces utilisateurs au **groupe globale** :

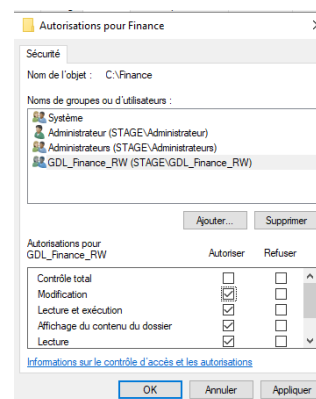


Une fois fait, il faut créer un **groupe local** avec comme nomenclature : GDL_NomDuPartage_Droits, et ajouter le **groupe global** à ce **groupe local** :

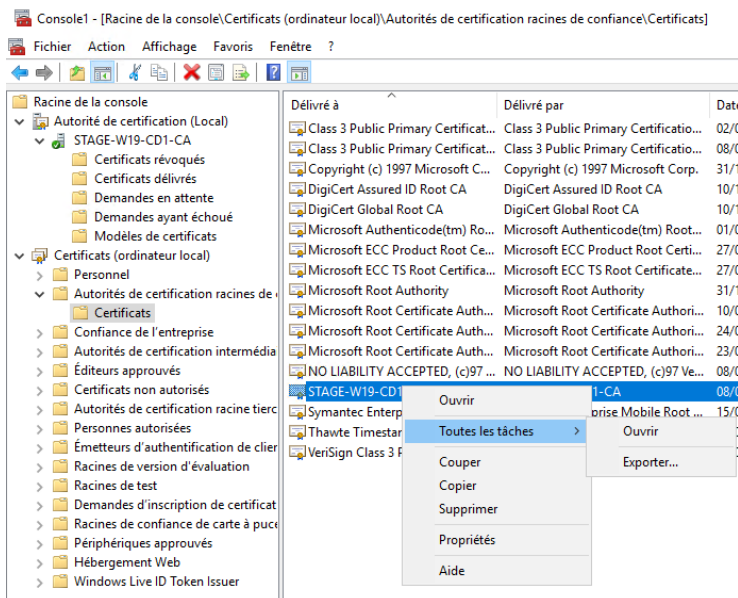


Et ensuite il faut ajouter **ce groupe local** aux permissions NTFS du partage.

Le but ici est que les groupes ayant les autorisations ne puisse intervenir que dans un seul domaine AD, cela renforce la sécurité et fais gagner en lisibilité.



4) SYSTEME CLIENTS



Pour installer le certificats sur notre clients il faut d'abord l'exporter de notre DC1 vers notre serveur web IIS (SSH) :

```
C:\Users\Administrateur>scp C:\Users\Administrateur\Desktop\W19-CD1.cer renaud@192.168.0.3:/tmp
renaud@192.168.0.3's password:
W19-CD1.cer 100% 901 0.9KB/s 00:00
```

Ensuite, le faut copier le certificats au bon emplacement et mettre a jours les certificats :

```
sudo cp /tmp/W19-CD1.cer /usr/local/share/ca-certificates/
```

```
update-ca-certification
```

Et nous avons l'accès a erp.stage.eni en HTTPS depuis nos clients :



5) SERVEURS LINUX

5.1. Serveur samba (partage de fichier)

Pour pouvoir avoir un serveur de partage de fichier sur Windows et sur Linux, j'ai choisi d'utiliser **Samba**.

Pour installer samba :

```
apt-get update & apt install samba
```

Ensuite active le démarrage automatique de samba :

```
systemctl enable samba
```

Après copier le fichier de configuration pour en avoir un vierge sous la main

```
root@debian11-ServerData:/etc/samba# cp smb.conf smb.conf.orig
root@debian11-ServerData:/etc/samba# ls
gdbcommands  smb.conf  smb.conf.orig  tls
```

Après il faut ajouter ces lignes au fichier de configuration :

```
[Partage]
comment = Partage serveur
path = /serveur/samba/partage
browsable = yes
guest ok = no
read only = no
valid users = @GrpPartage
```

Explications des options :

[Partage] = nom du partage

Browsable = Rendre le partage visible ou masqué

Comment = description

valid users = Liste des utilisateurs ou groupes

Guest ok = autorise ou non l'accès invité

autorise sur le partage

Path = localisation du partage

Ensuite **redémarrer** le service Samba avec : `systemctl restart smbd` et ensuite `adduser partagelinux` pour ajouter un utilisateur nommé *partagelinux* .

`smbpasswd -a partagelinux` pour ajouter l'utilisateur à Samba et donc lui autoriser l'accès a partir de Samba. Lui définir un mot de passe Samba.

Ensuite je crée le groupe défini (autorisé) dans le fichier de configuration smb.conf avec `groupadd GrpPartage` le groupe GrpPartage est donc créer.

Et ajouter l'utilisateur partagelinux au groupe GrpPartage.

```
root@deb11-serverdata2:~# gpasswd -a partagelinux GrpPartage
Adding user partagelinux to group GrpPartage
```

5.2. Création du dossier de partage

Il faut créer le dossier que l'on va partager. Pour cela il faut que ce soit le même que dans le fichier de configuration (smb.conf).

```
root@deb11-serverdata2:~# mkdir -p /serveur/samba/partage
```

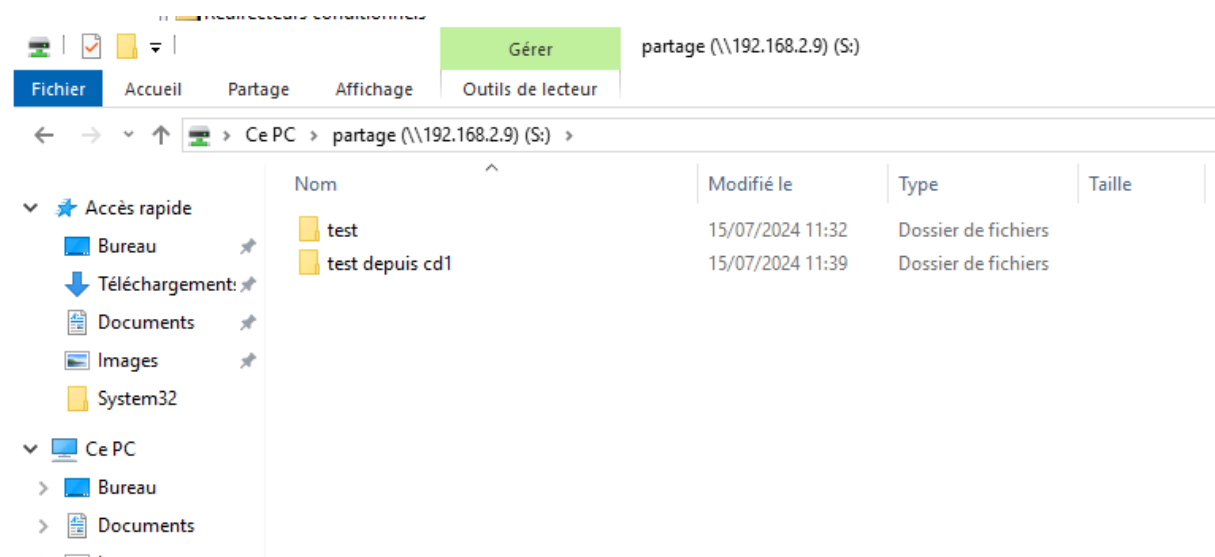
Il faut ensuite changer le groupe propriétaires de notre partage par le groupe défini dans le fichier de configuration.

Applique récursivement les permissions de lecture et d'écriture au groupe propriétaire sur le partage.

```
root@deb11-serverdata2:~# chgrp -R GrpPartage /serveur/samba/partage
root@deb11-serverdata2:~# chmod -R g+rw /serveur/samba/partage
```

Ensuite on redemarre avec : `systemctl restart smbd`.

On peut ensuite le monter dans CD1 par exemple pour y avoir accès depuis l'explorateur de fichier.



6) UNBOUND : CACHE DNS ET REDIRECTIONS

6.1. Installation et copie fichier de configuration

Pour **mettre en place** un serveur cache DNS, comme demandé, **Unbound** est un logiciel permettant de gérer les DNS.

`Apt install unbound` pour **installer** les paquets.

Ensuite **naviguer** jusqu'au fichier de configuration et faire une **copie** avec :

`cp unbound.conf unbound.conf.orig` pour avoir un fichier par défaut sous la main.

```
root@deb11-DNS:~# cd /etc/unbound# ls
unbound.conf  unbound.conf.d  unbound.conf.orig  unbound_control.key  unbound_control.pem  unbound_server.key  unbound_server.pem
root@deb11-DNS:~# cd /etc/unbound# cp unbound.conf.orig
```

`Unbound.conf.d` sert à **enregistrer séparément** des options, pour plus de lisibilité.

6.2. Modifier le fichier de configuration

Pour **modifier** le fichier de configuration, j'utilise nano, donc `nano unbound.conf`.

```
root@deb11-DNS:~# cd /etc/unbound
root@deb11-DNS:~# cd /etc/unbound# ls
unbound.conf  unbound.conf.d  unbound.conf.orig  unbound_control.key  unbound_control.pem  unbound_server.key  unbound_server.pem
root@deb11-DNS:~# cd /etc/unbound# nano unbound.conf
root@deb11-DNS:~# cd /etc/unbound# nano unbound.conf
```

Notre fichier de configuration :

```
include-toplevel: "/etc/unbound/unbound.conf.d/*.conf"

server:
  interface: 192.168.2.129
  access-control: 192.168.0.0/16 allow
  access-control: 127.0.0.1/8 allow
  #access-control: ::1 allow
  verbosity: 1
  log-queries: yes
  logfile: "/var/log/unbound/unbound.log"
  username: "unbound"
forward-zone:
  name: "."
  forward-addr: 10.0.0.3
#include: "/etc/unbound/unbound.conf.d/forward.conf"
```

La section server contient les configurations du serveur :

Interface : interface sur laquelle le serveur écoute

Access-control : liste des clients/réseau autoriser à requêter notre serveur unbound (ici **tout** notre réseau)

Verbosity : niveau de verbosité des logs

Log-queries : journalisation des requêtes DNS

Logfile : ou sont stockés les logs

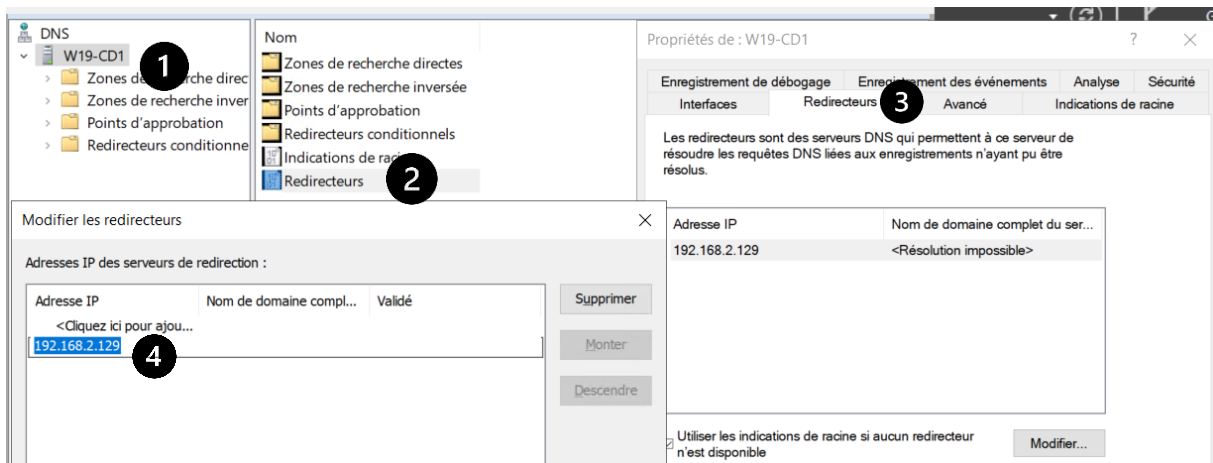
Username : définit l'utilisateur sous lequel le processus unbound doit s'exécuter

La section forward-zone est utilisée pour rediriger les requêtes :

Indique à unbound de rediriger toutes les requêtes ("."), vers l'IP 10.0.0.3.

6.3. Redirection Windows vers Unbound

Pour ajouter un redacteur sur les DNS windows, il faut sur le DC1 ajouter un redacteur pointant vers notre serveur Unbound :



Pour ajouter un redirecteur DNS pour les serveurs windows pointant vers le debian11 Unbound il faut aller dans les outils d'administration et sur le services DNS. Une fois dans le gestionnaire de DNS, cliquer sur le serveur(1), cliquer sur redirecteurs(2), et dans l'onglet redirecteurs (3) ajouter l'ip(4) du serveur Unbound. Une redirection, si le serveur DNS sur DC1 ne peut pas résoudre la requête, il l'envoie vers le debian11 Unbound qui interroge le DNS ENI ou son propre cache.

7) SERVEUR LINUX APACHE MARIADB PHP (LAMP) & WORDPRESS

7.1. Apache2/Php – Wordpress

Pour installer un serveur **LAMP** nous allons installer apache2, php ainsi que d'autre paquet tel que php-mysql.

```
apt-get install -y php php-pdo php-mysql php-zip php-gd php-mbstring php-curl php-xml php-pear php-bcmath  
systemctl restart apache2
```

Ensuite créer la page de test php et l'envoyer à la racine de notre serveur web :

```
echo "<?php phpinfo(); ?>" | tee /var/www/html/index.php
```

Ensuite mettre www-data en propriétaire et groupe sur nos fichiers :

```
root@debian11apachephp2:~# chown -R www-data:www-data /var/www/html  
root@debian11apachephp2:~# ls -l /var/www/html  
total 16  
-rw-r--r-- 1 www-data www-data 10701 30 juil. 09:56 index.html  
-rw-r--r-- 1 www-data www-data 20 30 juil. 10:35 index.php
```

Après il faut télécharger wordpress, l'extraire, le mettre dans notre apache et lui accorder les bon droits et propriétaire. J'ai télécharger wordpress sur mon poste eni et je me le suis envoyer en ssh sur ma machine virtuelle.

```
PS C:\Users\rlibasz2023> scp C:\Users\rlibasz2023\Desktop\wordpress-6.6.1.tar.gz renaud@10.3.200.39:/tmp  
renaud@10.3.200.39's password:  
wordpress-6.6.1.tar.gz 100% 23MB 74.8MB/s 00:00  
PS C:\Users\rlibasz2023>
```

Une fois le dossier dans /tmp, il faut l'extraire et l'envoyer a notre site web :

```
tar -xzf wordpress-6.6.1.tar.gz  
ls  
mv wordpress /var/www/html/
```

Ensuite mettre www-data en propriétaire pour permettre au serveur web d'écrire et de lire des fichiers.

Ensuite gérer les droits des répertoires.

Et créer le fichier de configuration de wordpress pour apache.

```
root@debian11apachephp2:/var/www/html# chown -R www-data:www-data /var/www/html/wordpress  
root@debian11apachephp2:/var/www/html# chmod -R 755 /var/www/html/wordpress  
root@debian11apachephp2:/var/www/html# nano /etc/apache2/sites-available/wordpress.conf
```

Pour plus de sécurité il faut mettre des droits différents au **fichiers** au sein de wordpress pour que seul son auteur puisse le modifier :

```
|_root@debian11apachephp2:/var/www/html# find wordpress -type f -exec chmod 644{} \;
```

Cette commande **cherche** tout les **fichiers** dans le repertoire wordpress, et execute un **chmod 644** pour restreindre les permissions de modification aux fichiers.

Ensuite activer les modules apache nécessaire et restart :

```
|_root@debian11apachephp2:/var/www/html# a2ensite wordpress
Enabling site wordpress.
To activate the new configuration, you need to run:
    systemctl reload apache2
|_root@debian11apachephp2:/var/www/html# a2enmod rewrite
Module rewrite already enabled
|_root@debian11apachephp2:/var/www/html# systemctl restart apache2
|_root@debian11apachephp2:/var/www/html#
```

7.2. Mariadb

Pour installer mariadb :

apt-get install -y mariadb-server mariadb-client

Pour démarrer et activer le démarrage automatique de mariadb :

systemctl start mariadb

systemctl enable mariadb

Ensuite il faut lancer le **mysql_secure_installation** pour définir quelques options de bases ainsi qu'un mot de passe pour le compte root.

Ensuite pour se connecter a mariadb on utilise cette commande : **mysql -u root -p**, nous sommes invité à entrer notre mot de passe précédemment créer avec **mysql_secure_installation**.

```
|_MariaDB [(none)]> CREATE DATABASE wordpress;
Query OK, 1 row affected (0,000 sec)

|_MariaDB [(none)]> CREATE USER 'wordpressuser'@'192.168.2.132' IDENTIFIED BY '[REDACTED]';
Query OK, 0 rows affected (0,000 sec)

|_MariaDB [(none)]> GRANT ALL PRIVILEGES ON wordpress.* TO 'wordpressuser'@'192.168.2.132';
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your
ntax to use near 'PRIVILEGES ON wordpress.* TO 'wordpressuser'@'192.168.2.132'' at line 1
|_MariaDB [(none)]> GRANT ALL PRIVILEGES ON wordpress.* TO 'wordpressuser'@'192.168.2.132';
Query OK, 0 rows affected (0,001 sec)

|_MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,001 sec)

|_MariaDB [(none)]> EXIT
```

- 1- On créer une base de données appeler « wordpress »
- 2- On créer l'utilisateur wordpressuser, qui peut se connecter depuis 192.168.2.132 et on définit son mot de passe.

- 3- On accorde tout les privilèges sur la base de donnée « wordpress » à l'utilisateur « wordpressuser » qui se connecte depuis 192.168.2.132 .
- 4- Recharge les tables pour prise en compte des modifications.

Ensuite modifier le fichier de configuration de mariadb pour autoriser toutes les connexions.

```
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
```

7.3. Configuration de wordpress

Retour sur la vm apache/php, se rendre dans le répertoire de wordpress et modifier le fichier de configuration, après l'avoir copier :

```
152 mv wp-config-sample.php wp-config.php
153 ls
154 nano wp-config.php
155 systemctl restart apache2
```

Modifier ces lignes pour se connecter a la base de données :

```
// ** Database settings - You can get this info from your web host
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wordpressuser' );

/** Database password */
define( 'DB_PASSWORD', 'XXXXXXXXXX' );

/** Database hostname */
define( 'DB_HOST', '192.168.2.4' );
```

Et se rendre à <http://192.168.2.132/wordpress> pour finir l'installation.

8) GLPI

Ensuite j'installe un debian 11 GLPI, je clone ma debian modèle, ajuste les dépôts, et MAJ avec *apt-get update* et *apt-get full-upgrade -y*.

Ensuite il faut installer apache, PHP et les extensions PHP nécessaires :

```
apt install apache2 libapache2-mod-php php php-cli php-mysql php-xml php-mbstring php-curl php-gd php-intl
php-zip php-bz2 php-json php-ldap unzip wget -y
```

Ensuite je dois activer SSH donc on l'installe avec la commande : ***apt install openssh-server*** .

Et on transfère le dossier glpi de l'hôte ENI vers la debian 11, avec scp : ***C:/Users/rlibasz2023/Desktop/glpi-10.0.16.tgz renaud@10.3.200.58:/tmp***

Après il faut extraire l'archive avec : ***tar -xvzf glpi-10.0.16.tgz***, ensuite on déplace le dossier a la racine de notre serveur web, on attribue les bons propriétaires et les bon droits a notre dossier.

```

root@debian11apachephp2:/tmp# mv glpi /var/www/html
root@debian11apachephp2:/tmp# chown -R www-data:www-data /var/www/html/glpi
root@debian11apachephp2:/tmp# chmod -R 755 /var/www/html/glpi

```

8.1. Fichier de configuration d'apache

Ensuite il faut créer un fichier de configuration pour GLPI dans apache, on le crée à */etc/apache2/sites-available*.

```

root@debian11apachephp2:/tmp# nano /etc/apache2/sites-available/glpi.conf
root@debian11apachephp2:/tmp# cat /etc/apache2/sites-available/glpi.conf
<VirtualHost *:80>
    ServerAdmin admin@example.com
    DocumentRoot /var/www/html/glpi
    ServerName glpi.example.com
    ServerAlias www.glpi.example.com

    <Directory /var/www/html/glpi>
        Options FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/glpi_error.log
    CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
</VirtualHost>

```

<VirtualHost * :80> : S'applique à toutes les IP sur le serveur pour le port 80.

DocumentRoot /var/www/html/glpi : Définit le répertoire racine du site.

ServerName glpi.example.com : Spécifie le nom de domaine principal associé à ce site web. Laisser tel quel car l'infrastructure est un laboratoire.

<Directory /var/www/html/glpi> : Ce bloc s'applique au répertoire */var/www/html/glpi*.

Options FollowSymLinks : Permet l'utilisation de liens symboliques dans ce répertoire.

Activer le site et les modules apache nécessaires et redémarrer le service apache :

```

root@debian11apachephp2:/etc/apache2/sites-available# a2ensite glpi.conf
Enabling site glpi.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@debian11apachephp2:/etc/apache2/sites-available# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@debian11apachephp2:/etc/apache2/sites-available# systemctl restart apache2
root@debian11apachephp2:/etc/apache2/sites-available#

```

8.2. Base de données GLPI

Il faut ensuite créer une base de données pour notre GLPI, sur notre serveur mariadb on se connecte à nos bases de données avec : *mariadb -u root -p*

```
renaud@deb10-mariadb2:
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
MariaDB [(none)]> CREATE DATABASE glpi;
Query OK, 1 row affected (0,002 sec)

MariaDB [(none)]> CREATE USER 'glpi_user'@'%' IDENTIFIED BY '[REDACTED]';
Query OK, 0 rows affected (0,012 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON glpi.* TO 'glpi_user'@'%';
Query OK, 0 rows affected (0,007 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,007 sec)
```

CREATE DATABASE glpi; => On créer une base de donnée nommé glpi.

CREATE USER 'glpi_user'@'%' IDENTIFIED BY 'your_password'; => On créer un utilisateur mariadb nommé glpi_user, on l'autorise a se connecter depuis tout adresse IP avec '%', et définit le mot de passe de cette utilisateur.

GRANT ALL PRIVILEGES ON glpi.* TO 'glpi_user'@'%'; => Accorde tout les privilèges sur la base de donnée glpi, tout les tables avec '.', à l'utilisateur 'glpi_user' qui peut se connecter depuis n'importe quelle adresse IP.

FLUSH PRIVILEGES; => Rechargement pour prise en compte des privilèges.

Ensuite on redemarre mariadb avec : `systemctl restart mariadb`

8.3. Installation GLPI



Se rendre a <http://192.168.2.15/glpi>, pour finir l'installation de GLPI.

Ici, rempli l'IP de notre mariadb, et l'utilisateur et le password de notre utilisateur MariaDB.

9) SUPERVISION : NAGIOS

9.1. Supervision

Pour ajouter des hotes a superviser il faut installer l'agent NRPE, avec la commande **apt install nagios-nrpe-server**.

Il faut ensuite modifier le fichier de configuration : **nano /etc/nagios.nrpe.cfg**, il faut modifier cette ligne en ajouter l'IP de notre Nagios :

```
allowed_hosts=127.0.0.1,:::1,192.168.2.118
```

Ensuite il faut ajouter ces commande pour créer des sondes supplémentaire que celle présente par défaut sur notre hôte à superviser :

```
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -r -w .15,.10,.05 -c .30,.25,.20
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hda1
command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200

command[check_disk_root]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /
command[check_swap]=/usr/lib/nagios/plugins/check_swap -w 50 -c 20
command[check_uptime]=/usr/lib/nagios/plugins/check_uptime
command[check_cpu]=/usr/lib/nagios/plugins/check_cpu -w 85% -c 95%
command[check_memory]=/usr/lib/nagios/plugins/check_memory check_memory -vmstats -w 80% -c 90%
```

Il faut ensuite redémarrer le service avec **systemctl restart nagios-nrpe-server**.

Il faut aussi modifier les fichiers *commands.cfg* (définir des commandes personnalisées) et *linuxservices.cfg* (définir quels éléments doivent être surveillés (pour les hôtes Linux), et *windowsservices.cfg* pour les hôtes Windows) dans le dossier */etc/nagios4/objects/*.

Ensuite redémarrer le service Nagios avec **systemctl restart nagios4**.




















```
# Definitions for monitoring the Linux host
cfg_file=/etc/nagios4/objects/localhost.cfg
cfg_file=/etc/nagios4/objects/linuxhosts.cfg
cfg_file=/etc/nagios4/objects/linuxservices.cfg

# Definitions for monitoring a Windows machine
cfg_file=/etc/nagios4/objects/windowshosts.cfg
cfg_file=/etc/nagios4/objects/windowsservices.cfg
```

Il faut ajouter ces lignes pour dire à Nagios où se trouvent les différents fichiers contenant nos hôtes et nos commandes : Windows et Linux.

ubuntu-mariadb	CPU	UNKNOWN	08-18-2024 15:59:10	0d 0h 55m 28s	3/3
	Load	OK	08-18-2024 15:56:14	0d 0h 58m 24s	1/3
	Nombre de processus	WARNING	08-18-2024 16:01:17	0d 0h 53m 21s	3/3
	Nombre de processus zombies	OK	08-18-2024 15:58:20	0d 0h 56m 18s	1/3
	Root Partition	OK	08-18-2024 15:59:24	0d 0h 55m 14s	1/3
	Swap	OK	08-18-2024 16:00:27	0d 0h 54m 11s	1/3
	Uptime	UNKNOWN	08-18-2024 15:55:30	0d 0h 49m 8s	3/3
	Utilisateurs connectés	OK	08-18-2024 16:02:43	0d 0h 52m 4s	1/3
	memoire	UNKNOWN	08-18-2024 15:57:22	0d 0h 47m 16s	3/3

Voici les services et matériel supervisé ainsi que l'ensemble de l'infrastructure.

Host  	Status  	Last Check  	Duration  
localhost 	UP	08-18-2024 16:03:59	0d 10h 58m 3s
ubuntu-GLPI 	DOWN	08-18-2024 16:03:03	0d 1h 2m 47s
ubuntu-Samba 	UP	08-18-2024 16:03:01	0d 1h 2m 15s
ubuntu-Unbound 	DOWN	08-18-2024 16:05:27	0d 1h 1m 32s
ubuntu-apache/php 	UP	08-18-2024 16:03:19	0d 1h 2m 16s
ubuntu-clients 	DOWN	08-18-2024 16:01:42	0d 1h 0m 17s
ubuntu-mariadb 	UP	08-18-2024 16:03:22	0d 1h 1m 9s
w19-CD1 	UP	08-18-2024 16:04:53	0d 0h 2m 2s
w19-CD2 	DOWN	08-18-2024 16:04:49	0d 0h 3m 36s
w19-CLI 	DOWN	08-18-2024 16:04:40	0d 0h 3m 9s
w19-IIS 	DOWN	08-18-2024 16:05:54	0d 0h 2m 32s

10) SAUVEGARDE

Avant tout il faut que sur les clients le paquet **smbclient** soit installer avec **apt-get install smbclient**, mais aussi le paquets **cifs-utils** lorsqu'il faut monter le partage Samba.

DEBIAN11 VERS SAMBA

Pour sauvegarder le dossier personnel de l'utilisateur et le stocker sur notre serveur de fichier samba, j'ai tout d'abord installer quelque paquets :

```
Apt-get install smbclient cifs-utils
```

J'ai ensuite vérifier sur les deux machines que le protocole SSH était bien opérationnel.

Ensuite j'ai écrit le script sur le client permettant la sauvegarde :

```
1 #!/bin/bash
2
3 # Variables
4 REMOTE_USER="partagelinux"
5 REMOTE_HOST="192.168.2.9"
6 REMOTE_DIR="/serveur/samba/partage/backup-server/debian11"
7 LOCAL_DIR="/home"
8 DATE=$(date +%Y-%m-%d_%H-%M-%S)
9 BACKUP_FILE="backup_${DATE}.tar.gz"
10
11 # Création de l'archive locale
12 tar -czf /tmp/$BACKUP_FILE -C $LOCAL_DIR .
13
14 # Vérification de la création de l'archive
15 if [ $? -eq 0 ]; then
16     echo "Archive créée avec succès : /tmp/$BACKUP_FILE"
17 else
18     echo "Erreur lors de la création de l'archive."
19     exit 1
20 fi
21
22 # Transfert de l'archive vers le serveur distant
23 scp /tmp/$BACKUP_FILE ${REMOTE_USER}@${REMOTE_HOST}:${REMOTE_DIR}/
24
25 # Vérification du transfert
26 if [ $? -eq 0 ]; then
27     echo "Transfert réussi : ${REMOTE_DIR}/${BACKUP_FILE}"
28 else
29     echo "Échec du transfert."
30 fi
31
32 # Nettoyage de l'archive locale
33 rm /tmp/$BACKUP_FILE
34 ..
```

En premier lieu on créer les variables : serveur samba, user samba, repertoire ou sera stocker la sauvegarde, le repertoire a sauvegarder, la date.

On créer l'archive local avec tar.

On vérifie ensuite que l'archive s'est bien créer.

On l'envoie avec scp sur le serveur Samba.

On vérifie si le transfert c'est bien passez avec la variable d'environnement \$?, si code erreur 0 alors succès.

Sauvegarde :

```
root@deb11-samba:/serveur/samba/partage/backup-server/debian11# ls
backup_2024-08-14_17-06-05.tar.gz
```

Pour automatiser la sauvegarde on va utiliser la commande crontab : `crontab -e`

```
0 2 * * * /home/renaud/Bureau/backup2.sh
```

Windows 10 vers Samba

Ici tout comme la sauvegarde du Debian 11, le point important est que sur le serveur de fichiers les dossiers de destination doivent avoir le bon utilisateur propriétaire et le bon groupe propriétaire, pour cela on utilise la commande : `chown GrpPartage:partagelinux Windows10`

```
root@deb11-samba:/serveur/samba/partage/backup-server# ls -l
total 8
drwxr-xr-x 2 partagelinux GrpPartage 4096 14 août 17:06 debian11
drwxr-xr-x 2 partagelinux GrpPartage 4096 15 août 12:38 Windows10
```

Le script :

```
# Répertoire source
$source = "C:\Users"

# Répertoire de sauvegarde temporaire
$tempBackupPath = "C:\Temp\Backup"

# Créer le répertoire temporaire s'il n'existe pas
if (-not (Test-Path $tempBackupPath)) {
    New-Item -Path $tempBackupPath -ItemType Directory | Out-Null
}

# Date pour nommer le fichier de sauvegarde
$date = Get-Date -Format "yyyy-MM-dd_HH-mm-ss"
$backupFile = "backup_$date.zip"
$localBackupPath = Join-Path -Path $tempBackupPath -ChildPath $backupFile

# Créer l'archive ZIP localement
Compress-Archive -Path $source -DestinationPath $localBackupPath

# Vérifier si la création de l'archive a réussi
if ($?) {
    Write-Output "Archive créée avec succès : $localBackupPath"
} else {
    Write-Output "Erreur lors de la création de l'archive."
    exit 1
}

# Définir le chemin du partage réseau
$destination = "\\192.168.2.9\Partage\backup-server\Windows10"

# Vérifier que le partage réseau est accessible
if (-not (Test-Path $destination)) {
    Write-Output "Le partage réseau n'est pas accessible : $destination"
    exit 1
}

# Copier l'archive vers le partage réseau
try {
    Copy-Item -Path $localBackupPath -Destination "$destination\$backupFile" -ErrorAction Stop
    Write-Output "Transfert réussi : $destination\$backupFile"
} catch {
    Write-Error "Erreur lors du transfert de l'archive : $_"
    exit 1
}

# Nettoyage de l'archive locale
Remove-Item -Path $localBackupPath
```

```
root@deb11-samba:/serveur/samba/partage/backup-server/Windows10# ls
backup_2024-08-15_12-38-22.zip
```

Pour automatiser la sauvegarde chaque nuit, on peut utiliser le planificateur de tâche, d'abord **Windows+R** et tapez '**taskschd.msc**'.

Nouveau déclencheur

Lancer la tâche : À l'heure programmée

Paramètres

☐ Une fois
☒ Chaque jour
☐ Chaque semaine
☐ Chaque mois

Démarrer : 15/08/2024 02:00:00 ☐ Synch. fuseaux horaires

Répéter tous les : 1 jours

Paramètres avancés

☐ Report maximal de la tâche (aléatoire) : 1 heure
☐ Répéter la tâche toutes les : 1 heure pour une durée de : 1 jour
☐ Arrêter toutes les tâches à l'issue de la durée de répétition
☐ Arrêter la tâche si elle s'exécute plus de : 3 jours
☐ Expiration : 15/08/2025 14:10:44 ☐ Synch. fuseaux horaires
☒ Activée

OK Annuler

Action	Détails
Démarrer un progr...	C:\Users\Administrateur\Desktop\Sauvegarde\script\sauvegarde.ps1

GLPI

```
root@debian11apachephp2:/home/renaud/Bureau# ./backup_glpi2.sh
Sauvegarde de la base de données réussie : /var/backups/glpi/glpi_backup_2024-08-16.sql.gz
sending incremental file list
glpi_backup_2024-08-16.sql.gz
```

```
sent 92,273 bytes received 35 bytes 184,616.00 bytes/sec
total size is 92,129 speedup is 1.00
Transfert de la sauvegarde réussi sur le serveur Samba.
Sauvegarde terminée avec succès.
root@debian11apachephp2:/home/renaud/Bureau# █
```

ETUDE DE SAUVEGARDE DES VM'S

1) Objectifs :

La sauvegarde de machine virtuelles sert à garantir la continuité des activités, la protection contre les pannes matérielles, les erreurs humaines et les cyberattaques.

2) Analyse des besoins :

Combien de VM sont à sauvegarder ?

Quelles sont les VMs critiques pour l'activité ?

Quel est le volume des données à sauvegarder ?

Sauvegarde quotidienne, hebdomadaire, ou en continu (sauvegarde incrémentielle) ?

3) Options de sauvegarde :

Type de sauvegarde	Sur site (on-premise)	Hybride (on-premise et cloud)	100% cloud
Avantages	Contrôle total Latence faible Récupération rapide	Combinaison de rapidité locale et de sécurité en cloud Meilleure résilience	Évolutivité Réduction des coûts d'infrastructure sur site Résilience géographique.

Inconvénients	Risques liés aux pannes matérielles Coût d'infrastructure élevé	Complexité de gestion Coût potentiellement élevé	Dépendance à la connexion internet Coût lié à la bande passante et aux ressources cloud
----------------------	--	---	--

4) Plan de mise en œuvre :

- 1 - Audit de l'existant (quantité, criticité, taille des VMs).
- 2 - Sélection de la solution logicielle et matérielle en fonction des besoins.
- 3 - Définition de la politique de sauvegarde (fréquence, rétention, chiffrement des données).
- 4 - Tests de récupération (pour valider les temps de restauration et l'intégrité des sauvegardes).
- 5 - Mise en production et suivi régulier.

Etude de sauvegarde des données en externe

1) Objectifs :

L'objectif est d'identifier la meilleure stratégie de sauvegarde externe pour l'entreprise.

2) Analyse des besoins :

Type de données à sauvegarder, volume des données, sécurité, fréquence de sauvegarde et budget alloué au sauvegarde.

3) Options de stockage externe :

Type de sauvegarde	Cloud Privé	Cloud Public	Cloud Hybride
Avantages	Contrôle des données Personnalisation Haute sécurité	Evolutivité Réduction des coûts Paiement à l'usage Redondance géographique	Meilleure flexibilité Contrôle et souplesse
Inconvénients	Coût élevé Complexité de gestion	Sécurité partagée Dépendance à l'opérateur Cloud Risque de coûts cachés	Gestion complexe Coûts potentiellement plus élevés

4) Comparaison et critères de choix :

Sécurité et conformité	Coût	Evolutivité	Performance et latence
Garantir que la solution choisie respecte la sécurité (chiffrement, localisation des données).	Analyser les coûts de lancement, récurrents, et les économies réalisables.	Le fait que la solution croît avec les besoins de l'entreprise	Pour les données importantes, la latence doit être minimale.

5) Plan de mise en œuvre :

- 1 - Identifier les données à sauvegarder
- 2 - Sélection du modèle cloud (privé, public, hybride)
- 3 - Mise en place de la solution choisie
- 4 - Formation des équipes et documentation

Conclusion :

Les solutions de sauvegarde des VM's et des données en externe doit être cohérent avec les besoins de sécurité, de performance et le budget de l'entreprise.

11) CONCLUSION

Que vous a apporté, personnellement et techniquement, votre période en entreprise ?

La réalisation de ce TP m'a vraiment aider à confirmer encore plus ce que j'ai appris tout au long de ma formation, cela m'a également permis de trouver une certaine confiance en moi par rapport à l'informatique et aux problèmes qui me sont donner, et que maintenant avec de la recherche et de la détermination j'arrive à résoudre les problèmes qui me sont proposé. Techniquement j'ai pu bien appréhender le mécanisme de base de données, son utilisation ainsi qu'à un niveau débutant le langage SQL. Egalement la mise en place d'un serveur LAMP avec un site wordpress. J'ai beaucoup aimé relever les différents défi tout au long de TP.

Le scripting également, le fait de faire des scripts de sauvegarde m'a aider à comprendre encore mieux la réalisation de script et les éventuels erreurs et optimisation que je peut rencontrer ou mettre en place.

Avez-vous rencontré des difficultés et comment les avez-vous surmontées ?

Ma première vraie difficulté était par rapport au certificat, cela faisait assez longtemps que nous l'avions vu en cours, j'ai donc repris les cours et mes notes en plus de recherche sur des sites comme it-connect ou autres, pour bien appréhender le mécanisme de la certification.

Ma deuxième difficulté était au niveau de la base données mariadb pour bien comprendre comment , et ou, tout se relie (ex : relier la base de données wordpress au serveur web). Après avoir suivi plusieurs tutoriel, recommencer l'installation d'une base données et d'un serveur web plusieurs fois que j'ai bien compris.

Dernière grosse difficulté la mise en place du service de supervision Nagios, mais en cherchant j'ai pu réussir à bien organiser mes fichiers avec différents OS (*linuxhosts.cfg* et *windowshosts.cfg*), pour ainsi gagner en lisibilité et donc permettre de mieux comprendre le fonctionnement de Nagios

Pour surmonter toutes ces difficultés je me suis aider de l'intelligence artificiel (ChatGPT, Gemini entre autres) mais aussi de recherches internet et de sites comme par exemple IT-Connect ou des youtubeurs comme benlinux par exemple, ainsi que des forums et des blogs. Et aussi bien sur des cours vidéo de l'ENI, des TP ainsi que de mes notes.

Confirme-t-il votre choix de parcours professionnel ?

Oui, j'aimerais vraiment être technicien informatique, mon goût pour la technologie, ma curiosité, le fait d'être minutieux, fera de moi, j'en suis sûr, un bon technicien informatique.

Les perspectives d'évolution ainsi que le nombre d'offre ainsi que la diversité des offres sur le marché de l'emploi de l'informatique ne font que confirmer le bon choix d'avoir fait cette formation.