


CREATION DU PARC INFORMATIQUE (AD)

PARCOURS	SISR <input checked="" type="checkbox"/>	SLAM <input type="checkbox"/>
-----------------	---	--------------------------------------

Lieu de réalisation	Sikiwis UERP	 ERP By SIKIWIS
Période de réalisation	Du : 01.10.2023	Au : 01.02.2024
Modalité de réalisation	SEUL <input type="checkbox"/>	EN EQUIPE <input checked="" type="checkbox"/>

Intitulé de la mission	Création du parc informatique (AD)
Description du contexte de la mission	Création du parc informatique (AD) afin de centraliser les ressources informatiques et humaines

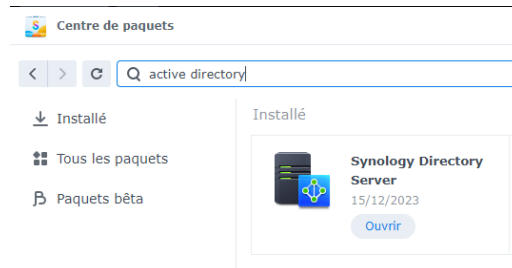
Contraintes & Résultat	Ressources fournies / contraintes techniques / Résultats attendu
	Serveur Synology, PC, Windows 10/11 Pro
Productions associées	Liste des documents produits et description

Modalités d'accès aux productions	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage

Création d'un parc informatique (AD)

Mise en place

La mise en place de l'Active Directory débute en installant le paquet adéquat dans le gestionnaire des paquets du serveur Synology.



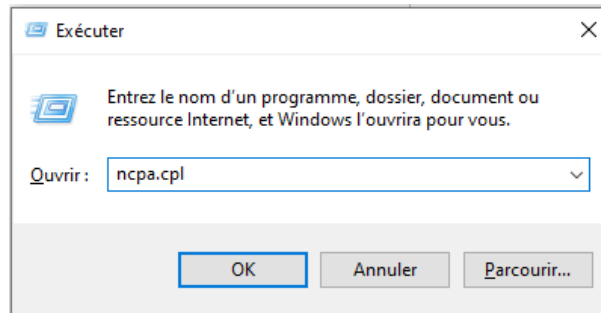
Paquet Active Directory à télécharger

Mise en place du serveur Synology

- Connexion du serveur au routeur (box).
- Configuration en se connectant à l'aide du navigateur.

Constitution du domaine

- Ncpa.cpl => désactiver IPv6 => aller dans l'IP v4 => mettre l'IP du serveur et de la box en DNS



Création d'un parc informatique (AD)

1) Mise en place

1.1) Matériel utilisé

L'active directory a été mis en place sur un NAS de la marque synology, RS1221+

Processeur	Modèle CPU	AMD Ryzen V1500B
	Quantité de CPU	1
	L'architecture de l'unité centrale	64-bit
	Fréquence du processeur	4-core 2.2 GHz
	Moteur de cryptage matériel (AES-NI)	✓
Mémoire	Mémoire système	4 GB DDR4 ECC SODIMM
	Module de mémoire pré-installé	4 GB (4 GB x 1)
	Total des emplacements mémoire	2
Capacité de mémoire maximale		32 GB (16 GB x 2)
Remarques		<ul style="list-style-type: none">• Synology se réserve le droit de remplacer les modules de mémoire par des modules d'une fréquence identique ou supérieure en fonction de l'état du cycle de vie du produit du fournisseur. Soyez assuré que la compatibilité et la stabilité ont été rigoureusement vérifiées selon les mêmes critères pour garantir des performances identiques.• Sélectionnez les modules de mémoire Synology pour une compatibilité et une fiabilité optimales. Synology n'offre pas une garantie complète du produit ni d'assistance technique si des modules mémoires autres que ceux de Synology sont utilisés pour l'extension de la mémoire.• Pour plus d'informations sur les configurations de mémoire recommandées, consultez le Guide d'installation matérielle de votre produit Synology.
Stockage	Baie(s) de disque dur	8
	Max. baies de disque dur avec l'unité d'expansion	12 (RX418 x 1)
	Type de lecteur compatible* (Voir tous les disques durs pris en charge)	<ul style="list-style-type: none">• 3.5" SATA HDD• 2.5" SATA HDD• 2.5" SATA SSD
	Disque remplaçable à chaud*	✓
	Remarques	* « Type de disque compatible » indique les disques qui ont été testés comme étant compatibles avec les produits Synology. Ce terme n'indique pas la vitesse maximale de connexion de chaque baie de disque.

Le niveau fonctionnel du domaine est égal à windows Server 2008 R2

Version de Samba: 4.10

Possibilité d'ajouter des ordinateurs >windows 7 et macOS et Linux

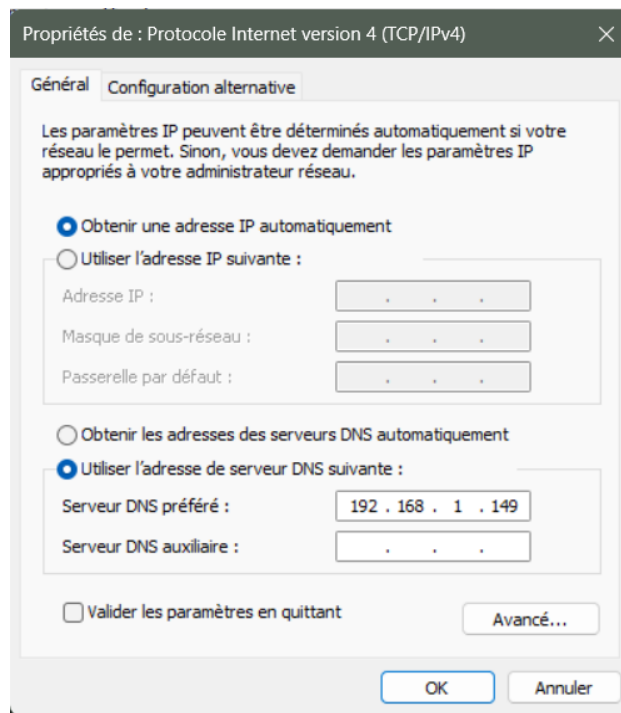
Authentification basée sur Kerberos

Le NAS s'allumera automatiquement lundi à 8h30, puis s'éteindra automatiquement vendredi à 20h30

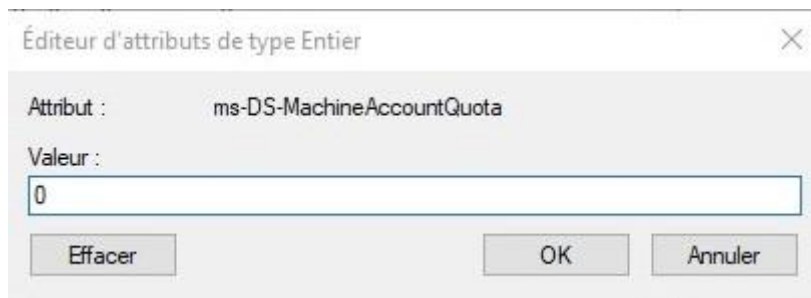
Les lan 1, 2, 3 sont en ip statique, la lan 4 est en dhcp(pour les bugs)

Création d'un parc informatique (AD)

1.2) Ajout d'ordinateurs au domaine



Avant d'ajouter un ordinateur au domaine, l'adresse du serveur DNS du pc doit être l'ip du NAS.

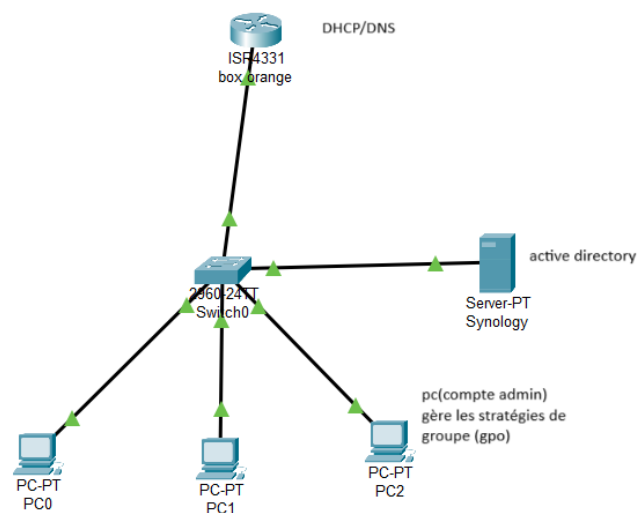


L'ajout d'ordinateurs au domaine peut être uniquement fait par un utilisateur du groupe administrateur.

Création d'un parc informatique (AD)

1.3) Topologie de l'Active Directory

L'Active Directory est installé sur le NAS ; le DHCP et le DNS sont gérés par le routeur.



A) Fonctionnalités et rôles




Contrôleur de domaine : sikiwis.local
gpo group owner: securite
admin: compte 500

B) Disque RAID

Un Raid 5 sera mis en place.

Création d'un parc informatique (AD)

1.7. Stratégie de groupes

	RSAT : gestionnaire de serveur	59,3 Mo 11/12/2023
	RSAT : outils Active Directory Domain Services Directory et services LDS (Lightweight Directory Services)	33,0 Mo 11/12/2023
	RSAT : outils de gestion de stratégie de groupe	36,0 Mo 11/12/2023

Les GPO sont mises en place avec RSAT, sur une machine Windows intégrée au domaine, dans la rubrique outil, “gestion et stratégies de groupe”. Le compte doit avoir les privilèges administrateur.

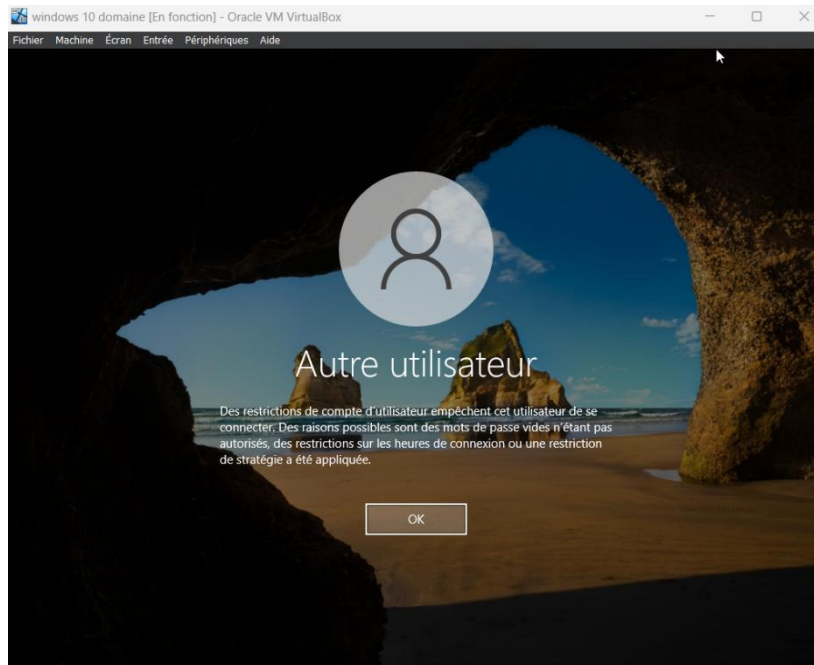
Règles mise en place :

- politique mot de passe
- déploiement installation de logiciel
- autoriser les utilisateurs à installer des logiciels
- firewall du domaine
- désactivation du compte invité
- interdiction de l'identification NTLMV1 et LM au server
- spouleur d'impression

Lorsqu'un compte sans délégation, sans contrainte est configuré et que le service spouleur d'impression est utilisé, des informations d'identification peuvent être envoyées comme les hache des utilisateurs.

Création d'un parc informatique (AD)

- stratégie d'audit
audit de la gestion des groupes de sécurité,
(Les audit de sécurité sont fait avec pingcastle et specops)
- restreindre l'accès à certains comptes uniquement aux pc autorisés
- Veille de l'écran après 15 minutes d'inactivité
- le navigateur par défaut est chrome (erreur de règle)



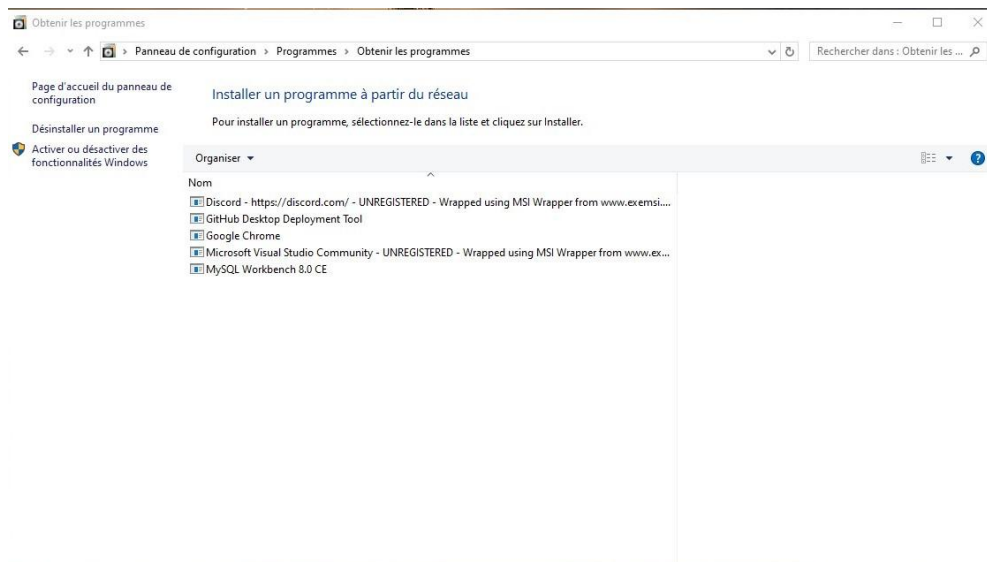
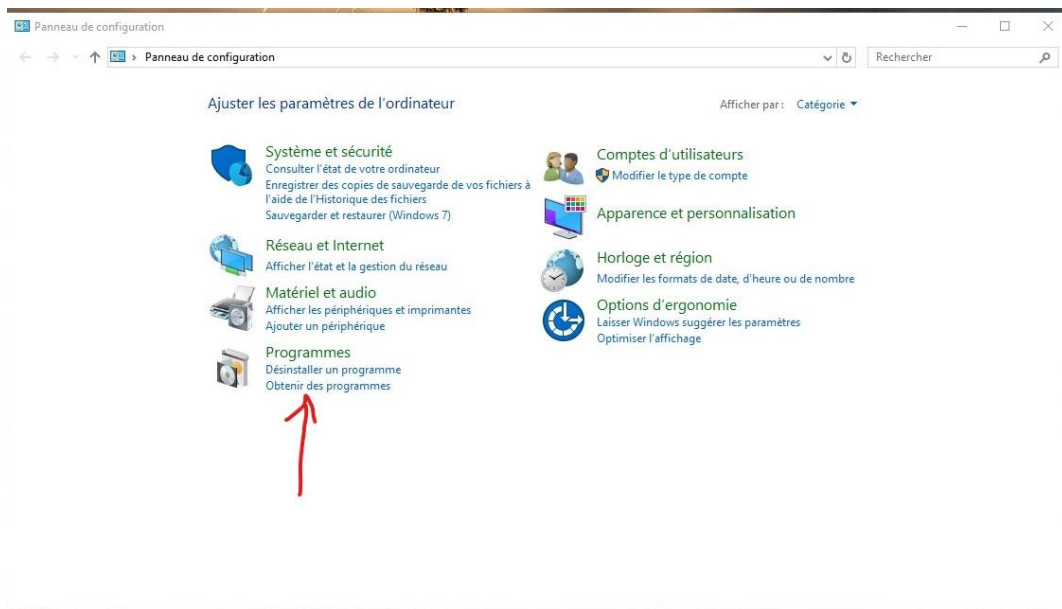
Les comptes avec des privilèges pourront uniquement être utilisés sur certains ordinateurs.

Création d'un parc informatique (AD)

1.8) Déploiement des applications

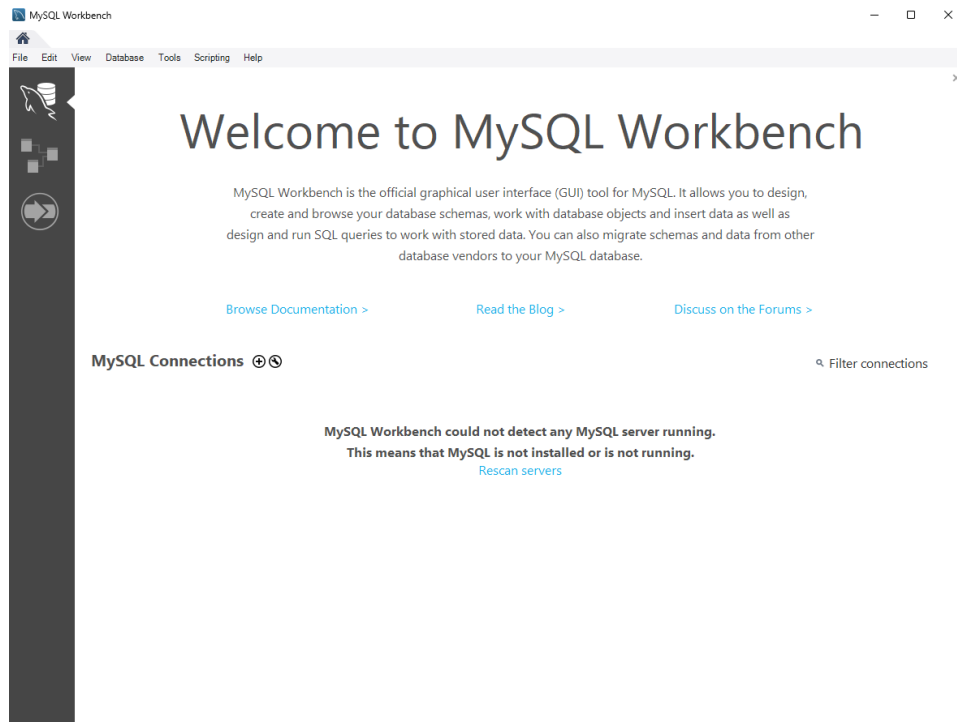
Lors de l'installation de nouveaux ordinateurs, les logiciels pourront être installés en fonction des groupes auxquels l'utilisateur fait partie.

L'installation peut se faire de manière automatique, à l'aide d'un script PowerShell, ou manuellement de la manière suivante :

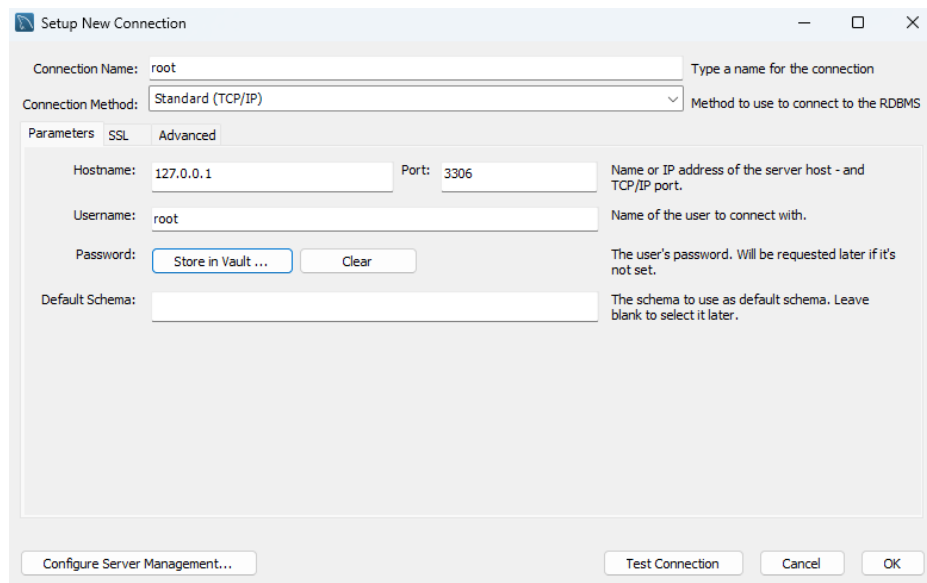


Création d'un parc informatique (AD)

1.9) Installation des dumps



appuyer sur +



Création d'un parc informatique (AD)

appuyer sur store in vault, définir un mdp puis ok

```
Command Prompt (MariaDB 1  X + v)

Setting environment for MariaDB 11.3 (x64)

C:\Windows\System32>mysql -u root -p
Enter password: ****
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 8
Server version: 11.3.2-MariaDB mariadb.org binary distribution

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 entreprise;
Query OK, 1 row affected (0.001 sec)

MariaDB [(none)]> |
```

```
MariaDB [(none)]> use entreprise;
Database changed
MariaDB [entreprise]> CREATE USER 'user'@'localhost' IDENTIFIED BY '';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> CREATE USER 'user'@'127.0.0.1' IDENTIFIED BY '';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> CREATE USER 'user'@'%' IDENTIFIED BY '';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> GRANT ALL PRIVILEGES ON *.* TO 'user'@'localhost';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> GRANT ALL PRIVILEGES ON *.* TO 'user'@'127.0.0.1';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> GRANT ALL PRIVILEGES ON *.* TO 'user'@'%';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]>
MariaDB [entreprise]> CREATE USER 'crm_user'@'localhost' IDENTIFIED BY 'crm_user';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> CREATE USER 'crm_user'@'127.0.0.1' IDENTIFIED BY 'crm_user';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> CREATE USER 'crm_user'@'%' IDENTIFIED BY 'crm_user';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> GRANT ALL PRIVILEGES ON *.* TO 'crm_user'@'localhost';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]> GRANT ALL PRIVILEGES ON *.* TO 'crm_user'@'127.0.0.1';
Query OK, 0 rows affected (0.001 sec)

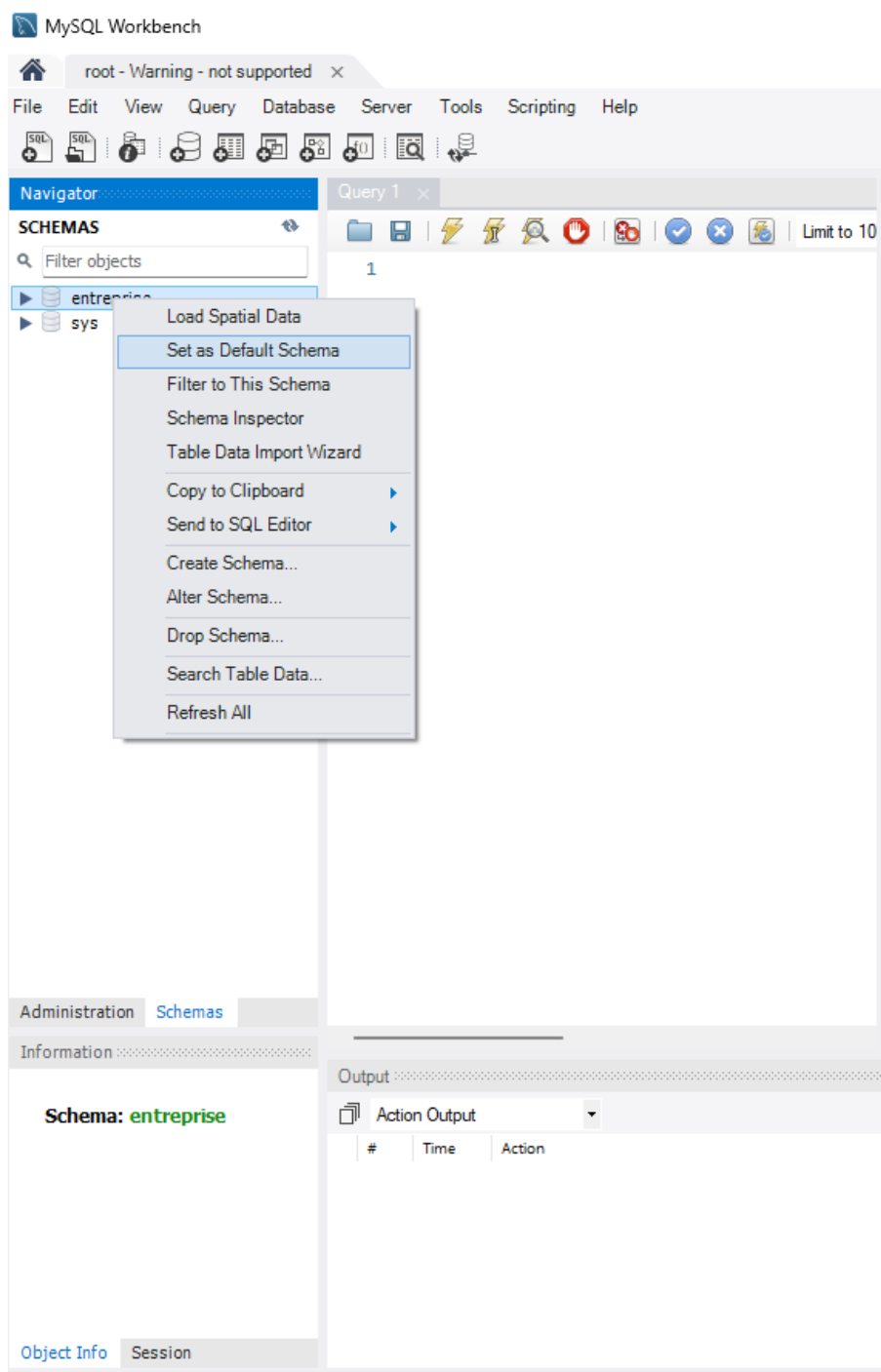
MariaDB [entreprise]> GRANT ALL PRIVILEGES ON *.* TO 'crm_user'@'%';
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]>
MariaDB [entreprise]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [entreprise]>
MariaDB [entreprise]> exit;
```

Création d'un parc informatique (AD)

```
C:\Windows\System32>mysql -u root -p entreprise <F:\dump06032024.sql  
Enter password: ****
```



Création d'un parc informatique (AD)

Seconde méthode :

- Ouvrir le fichier dump avec bloc note
- Copier le contenu
- Coller le contenu directement dans la base de données "entreprise" dans MySQL
- Exécuter le code

Création d'un parc informatique (AD)

1.4- Applications installées par groupes.....

Développeurs :

- Github desktop(automatique)
- GitLab(manuel)
- Discord(automatique)
- visual Studio (automatique)
- Google Chrome (automatique)
- firefox (manuel)
- mysqlWorbench (automatique)
- chat synology server(automatique)
- mariaDB (manuel)
- skype (manuel)

Chef de projet :

- ganttproject
- discord
- OVH
- Google Chrome
- skype

1.4- Commandes utiles.....

“exécuter” :

- cmd
- rsop.msc (savoir les gpo appliqués)

cmd :

- gpupdate (actualiser les gpo modifiés)
- gpupdate /force (actualiser toutes les gpo)
- gpresults (savoir le groupe, les gpo)

1.10 - Surveillance du réseau.....

Utilisation du logiciel Livebox Monitor v1.3

Création d'un parc informatique (AD)

2) Normes de sécurité

2.1) Règles serveur

☐ Activer l'en-tête « Server » dans les réponses HTTP

En tête « Server » personnalisé :

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.19045.3693]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Dev06>curl -I http://192.168.1.27
HTTP/1.1 200 OK
Date: Fri, 08 Dec 2023 09:08:40 GMT
Content-Type: text/html
Content-Length: 497
Last-Modified: Fri, 08 Dec 2023 09:07:27 GMT
Connection: keep-alive
Keep-Alive: timeout=20
ETag: "6572dccb-1f1"
Cache-Control: no-cache
Accept-Ranges: bytes
```

L'en-tête serveur a été enlevé, cela permet de masquer le type de l'instance lors de scan réseau.

Port DSM (HTTP) :

Port DSM (HTTPS) :

☒ Rediriger automatiquement les connexions HTTP vers HTTPS pour le bureau DSM

Les connexions sont automatiquement redirigées vers le protocole https, les ports de connexions par défaut ont été modifiés.

Création d'un parc informatique (AD)

2.2) Sauvegardes automatiques

Une sauvegarde automatique de l'active directory a lieu tous les jours, les 3 dernières sauvegardes sont préservées. Les sauvegardes automatiques se font dans plusieurs emplacements externes. (Pas encore configuré)

2.3) Gestion des Clés dossiers partagés

La gestion des clés des différents fichiers partagés se fait sur le Synology et sur un périphérique externe.

Gestionnaire de clés

Ajouter

Exporter la clé

Chiffrement

Supprimer

Configurer

Dossier partagé	État	Description	Chiffre	Montage ...	
sécurité	Déconnecter		Clé machine	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Annuler

OK

Déchiffrement des dossiers partagés avec le gestionnaire de clé interne.

Montage

☒ Saisissez la clé de chiffrement :

☐ Importer la clé de chiffrement :

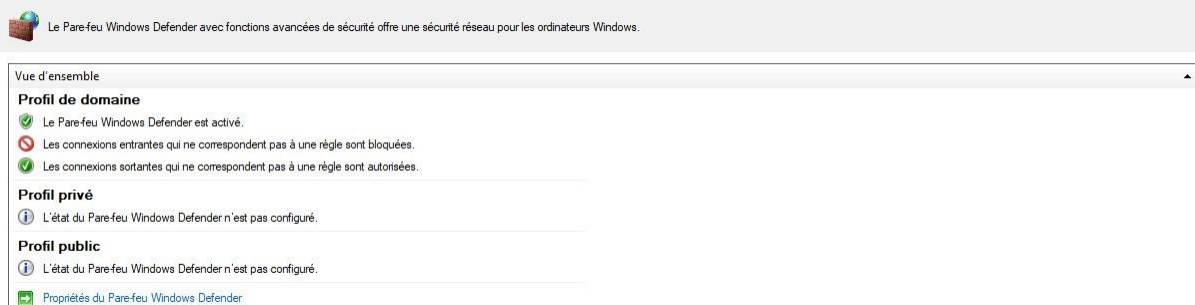
Parcourir

Annuler

OK

Création d'un parc informatique (AD)

2.4) Firewalls



Un pare-feu est mis en place sur le domaine, il filtre les connexions entrantes, mais pas celles sortantes.

2.5- VPN (pas encore configuré)

Un VPN est mis en place avec OpenVpn Connector. Le VPN est configuré en mode full tunneling. Toutes les connexions passeront directement par le vpn, toutes les connexions seront filtrées.

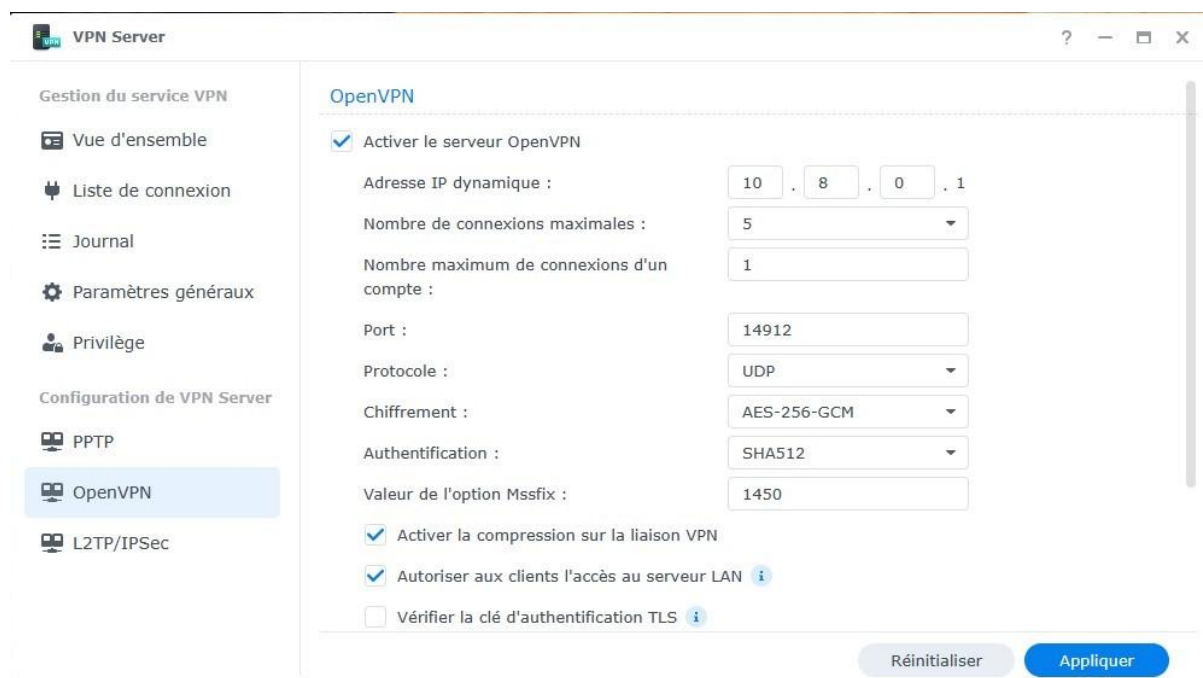


Création d'un parc informatique (AD)

Il est utilisé pour l'accès distant. Il est installé sur le port 14912

Activer	Application/Service	Port interne	Port externe	Protocole	Équipement	IP externe	
<input checked="" type="checkbox"/>	Synologyvpn	14912	14912	UDP	192.168.1.27	Toutes	

Une règle spéciale a été créer sur le routeur.



The screenshot shows the 'VPN Server' configuration window for 'OpenVPN'. The left sidebar contains a menu with 'Gestion du service VPN' (Overview, List of connections, Journal, General parameters, Privilege) and 'Configuration de VPN Server' (PPTP, OpenVPN, L2TP/IPSec). The 'OpenVPN' section is selected. The main area shows the 'OpenVPN' configuration with the following settings:

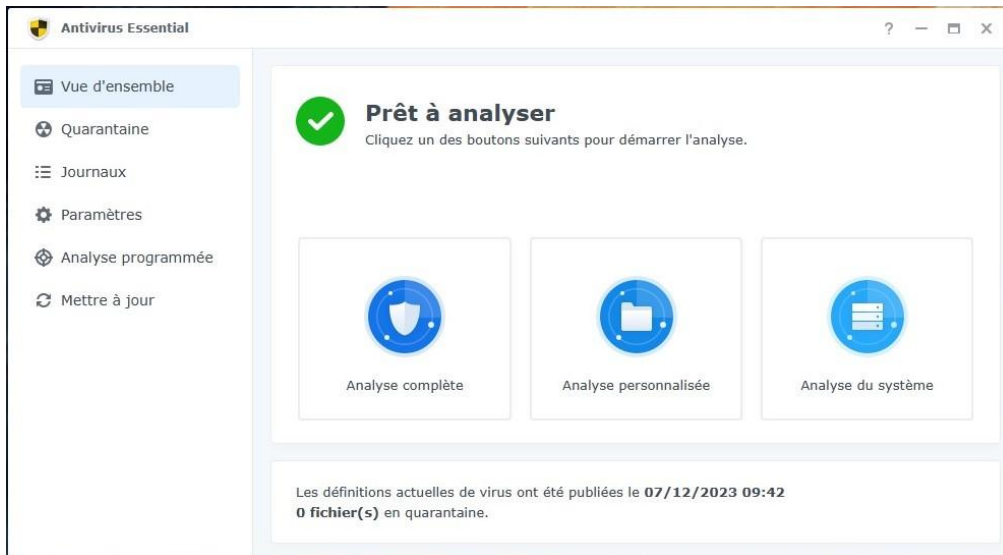
- ☒ Activer le serveur OpenVPN
- Adresse IP dynamique : 10 . 8 . 0 . 1
- Nombre de connexions maximales : 5
- Nombre maximum de connexions d'un compte : 1
- Port : 14912
- Protocole : UDP
- Chiffrement : AES-256-GCM
- Authentification : SHA512
- Valeur de l'option Mssfix : 1450
- ☒ Activer la compression sur la liaison VPN
- ☒ Autoriser aux clients l'accès au serveur LAN [i](#)
- ☐ Vérifier la clé d'authentification TLS [i](#)

At the bottom right, there are buttons for 'Réinitialiser' (Reset) and 'Appliquer' (Apply).

Les transmissions passant par le VPN sont chiffrées pour des raisons de sécurité.

Création d'un parc informatique (AD)

2.6) Antivirus



L'antivirus utilisé sur le serveur est un antivirus essentiel, les machines clients utilisent l'antivirus intégré à Windows. Les fichiers partagés sont analysés lundi, mercredi et vendredi, il y a une analyse complète du système le jeudi.

2.7 Politique de mot de passe

Les mots de passes doivent au minimum avoir :

- ≥ 8 caractères
- ≥ 1 majuscule
- ≥ 1 caractères spéciaux
- Doivent être changer 1/an
- Doivent être changer lors de la première connexion
- Se verrouille après 7 erreurs pendant 15 minutes

<input checked="" type="checkbox"/> Seuil de verrouillage	<input type="text" value="7"/>	fois
Réinitialiser le compteur de verrouillage après	<input type="text" value="15"/>	<input type="text" value="minutes"/>
<input type="checkbox"/> Durée du verrouillage	<input type="text" value="30"/>	<input type="text" value="minutes"/>

Création d'un parc informatique (AD)

2.8) Protection DDoS

^ Protection DoS (Denial-of-Service)

Interface réseau :

LAN 1

La protection DoS (dénier de service) aide à éviter les attaques malveillantes sur Internet.

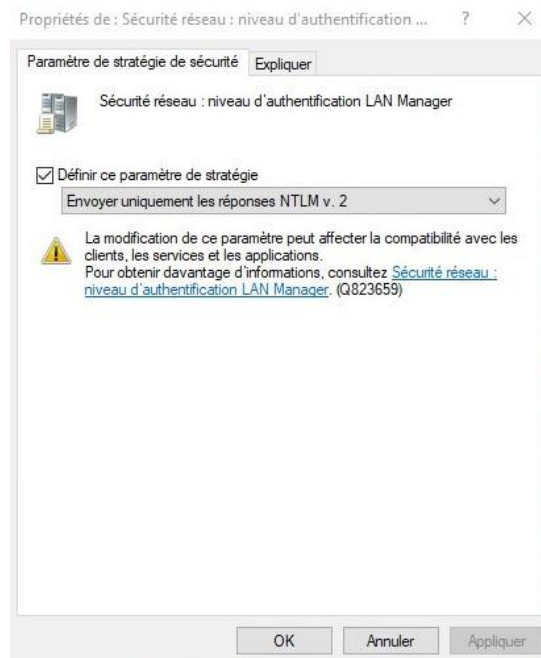
☒ Activer la protection DoS

Le NAS ne traitera pas toutes les requêtes, pour éviter d'être surchargé par des pings en masse.

2.9) NTLMv1

Le protocole d'identification aux serveurs sont maintenant kerberos, NTLMv1 et LM sont obsolètes et sont souvent trouvant par des attaques brute force. Pour des raisons de sécurité l'identification est uniquement autorisée avec NTLM v2

(Si problème d'identification ajouter des autorisations)

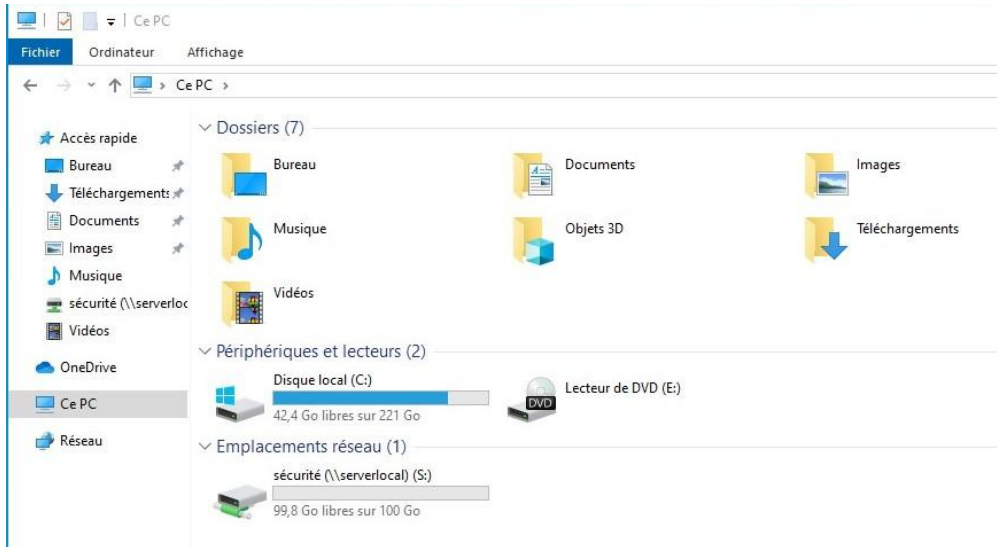


2.10) Tier Model

Création d'un parc informatique (AD)

3) Serveurs de fichiers partagés

3.1) Fichiers partagés



Les fichiers sont accessibles de cette manière ou en écrivant le chemin réseau, pour cet exemple “\\serverlocal\sécurité”

Chaque groupe a un fichier partager chiffré, les quotas(extensible) sont les suivants

-dev 500 go

-sécurité 100go

Les fichiers partagés disposent d'une corbeille. La corbeille ne peut être vidée uniquement par l'administrateur.

Création d'un parc informatique (AD)

3.3) Synology chat service

Un service de messagerie privée est accessible avec les identifiants de l'active directory.
Si les conversations doivent être chiffrées, les utilisateurs devront indiquer les clés. Pour y accéder il faut aller à l'adresse suivante :

<http://192.168.1.149/sikiwischat>

