DOCUMENTATION TECHNIQUE

Contexte rest0.fr

Projet	: Contexte rest0.fr
Document	: Documentation technique
Version	: 1.0
Date	: 11 mai 2025
Rédacteur	: TENEUR Mathéo
Organisation	: rest0.fr

Table des matières

Présentation du contexte rest0.fr 3
1 – Stormshield et segmentation du réseau par VLAN 7
1.1 – Segmentation VLAN et configuration du switch Cisco 7
1.1.1 – Segmentation VLAN 7
1.1.2 – Configuration de l'accès en SSH au Switch 8
1.2 - Stormshield 10
2 – installation et configuration de l'Active Directory 12
3 – DHCP 13
3.1 – Configuration du serveur DHCP 13
3.2 – Mise en place DHCP Relay 14
4 – TFTP 15
4.1 – Sécurisation du SSH avec connexion par clé 15
4.2 – Serveur TFTP 15
5 - GLPI 17
5.1 - Installation 17
5.2 - Gestion des habilitations 20
5.3 - Inventaire 22
5.3.1 – Clients Windows 22
5.3.2 – Clients Linux 24
5.3.3 – Clients SNMP 25
5.4 - Modèle ticket 27
6 - Partage de Fichier Windows 30
7 - Nextcloud 34
7.1 – Installation de Nextcloud 34
7.2 – Comptes & Privilèges (pour la connexion à Nextcloud) 39
7.3 – Liaison Nextcloud avec le partage de fichier Windows 41
7.4 – Accès à Nextcloud depuis Internet 43

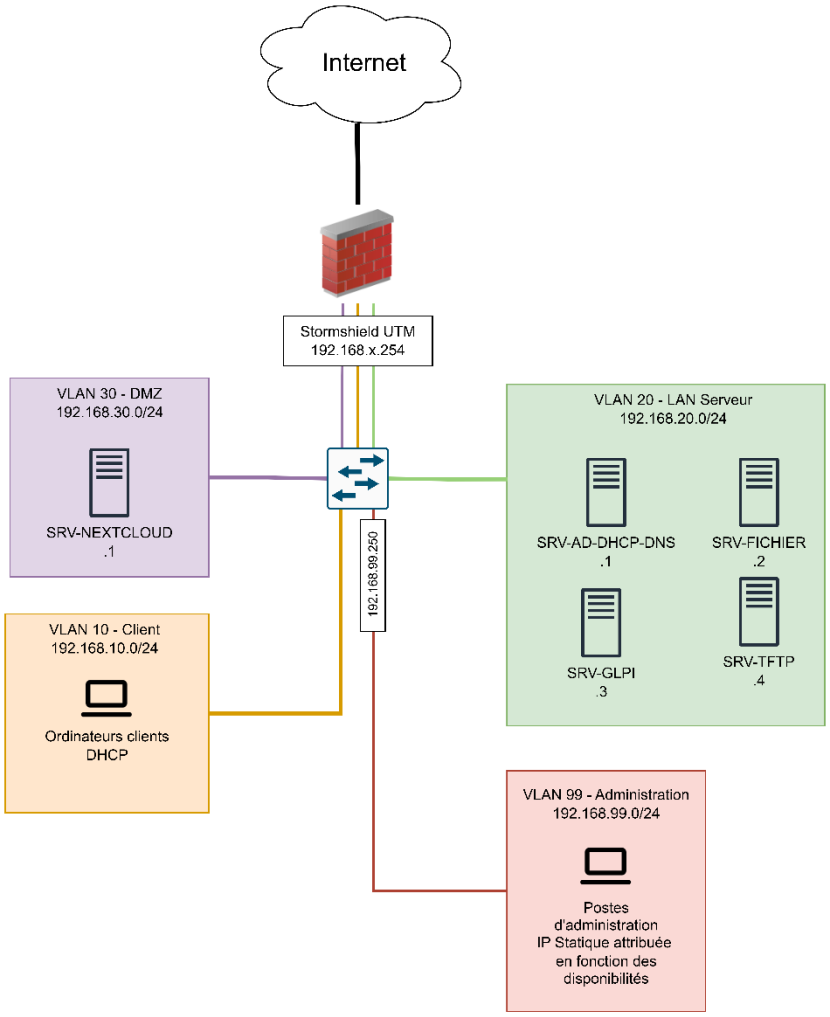
Présentation du contexte rest0.fr

La société rest0.fr a développé une application web permettant de mettre en ligne les avis des clients à propos des restaurants où ils ont mangé. Rest0.fr connait depuis ces derniers mois un succès grandissant.

Le parc de postes de travail et d'équipements actifs a donc grandement augmenté et le DSI aimerait mettre en place des solutions d'infrastructure qui permettent d'améliorer la sécurité et l'exploitation de son parc.

Actuellement, le réseau de l'entreprise n'est pas segmenté : les postes utilisateurs se trouvent sur le même réseau que le datacenter hébergeant les serveurs. Afin de renforcer la sécurité et de pouvoir appliquer une politique « Zero Trust », une segmentation du réseau sera mise en place.

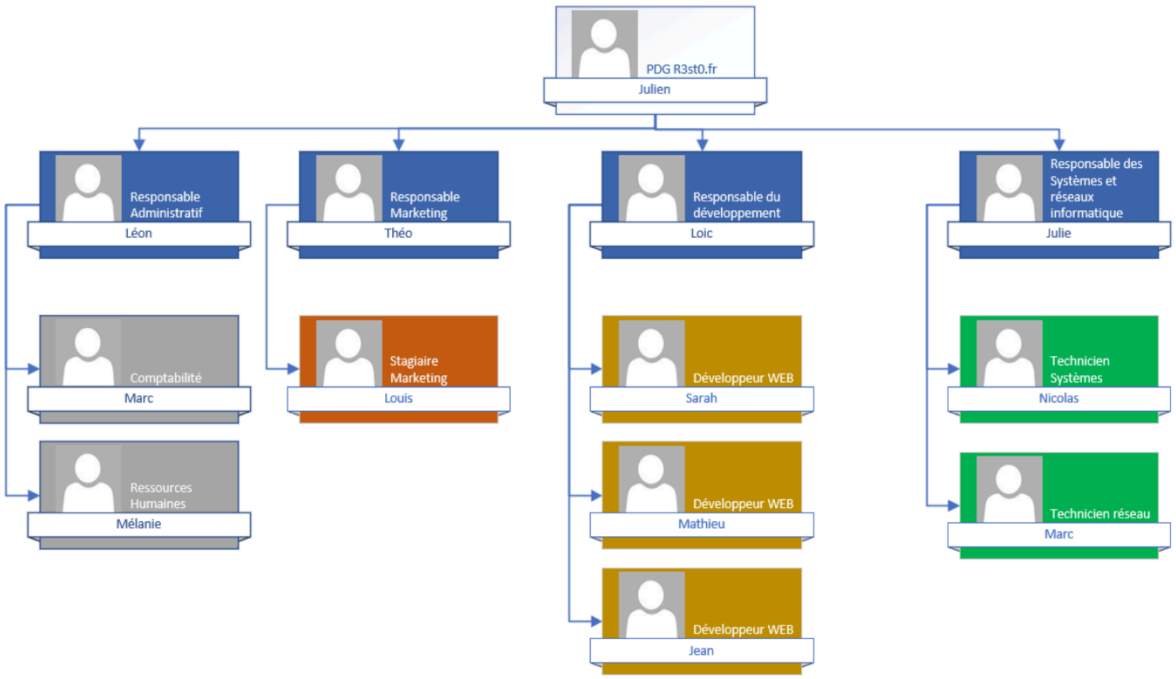
Voici comment le réseau de la société sera structuré :



Actuellement, l'ensemble des salariés d'un même service utilise un compte local partagé. Cette organisation nuit à la traçabilité des actions, rendant l'imputabilité difficile. De plus, la création et la gestion manuelle de ces comptes représentent une perte de temps pour les équipes informatiques.

Afin d'améliorer la gestion des identités et de renforcer la sécurité, un domaine Active Directory sera mis en place sur un serveur Windows Server 2019.

Des comptes nominatifs seront créés à partir de l'organigramme de l'entreprise pour garantir l'imputabilité des utilisateurs. Par ailleurs, des comptes administrateurs nominatifs dédiés seront créés conformément aux recommandations de l'ANSSI.



L'ensemble des postes de travail de l'entreprise utilisait jusqu'à présent un adressage IP statique. Afin d'automatiser l'attribution des adresses, un serveur DHCP sera déployé sur Windows Server 2019, avec la mise en place d'un relais DHCP entre les VLANs Client et Serveur.

Par ailleurs, la configuration actuelle des équipements réseau n'est pas sauvegardée. Pour y remédier, un serveur TFTP sera installé afin de centraliser et sécuriser les sauvegardes de configurations des équipements.

La gestion du parc informatique est actuellement réalisée manuellement à l'aide d'un tableur Excel. Cette méthode, sujette à des oublis de saisie de la part des techniciens, engendre un inventaire incomplet et peu fiable.

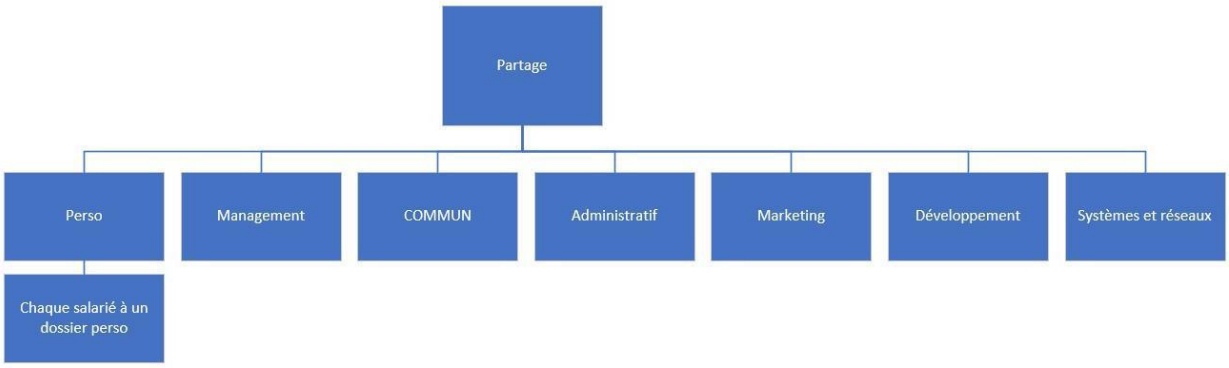
De plus, aucun guichet unique n'existe pour centraliser les demandes ou les signalements d'incidents. Les utilisateurs contactent l'équipe informatique par e-mail ou par téléphone, sans possibilité de suivi structuré.

Pour améliorer la gestion des demandes et automatiser l'inventaire du parc, un serveur GLPI sera mis en place. Il permettra de centraliser les tickets et de maintenir un inventaire à jour grâce à l'agent GLPI. Un serveur GLPI vas être mit en place afin de centraliser les demandes et les incidents et de pouvoir tenir un inventaire des équipements à jour automatiquement.

Actuellement, les collaborateurs de l'entreprise conservent l'intégralité de leurs fichiers localement sur leur poste de travail.

Il n'y a pas d'outil simple qui permet de faire de la collaboration entre des collègues. Le partage interne de documents s'effectue principalement par e-mail ou via des services en ligne tels que WeTransfer, ce qui pose des problèmes de sécurité et de performance.

Afin d'y remédier, un serveur de fichiers sous Windows Server 2019 sera mis en place pour centraliser les données et proposer un accès sécurisé via des répertoires partagés en SMB. Ces répertoires seront automatiquement mappés en lecteurs réseau à l'aide de stratégies de groupe (GPO).

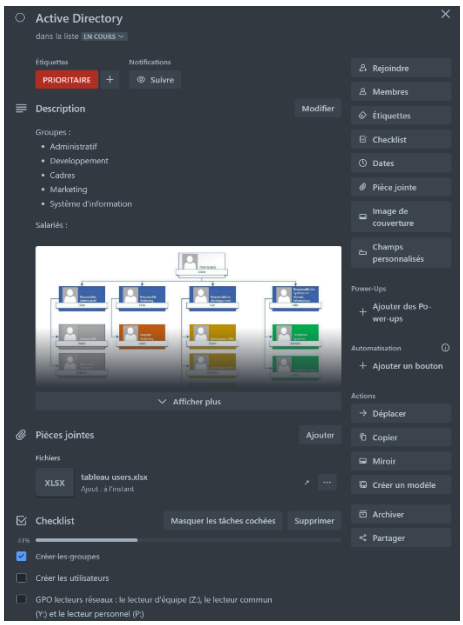


Afin de faciliter le travail à distance, le Directeur des Systèmes d'Information (DSI) souhaite mettre en place une solution sécurisée de partage et de synchronisation de fichiers pour les salariés en télétravail.

Pour cela, un serveur Nextcloud sera déployé et rendu accessible via Internet. Cette solution open source permettra aux utilisateurs d'accéder à leurs documents professionnels depuis n'importe où, tout en garantissant le contrôle des données et la confidentialité des échanges.

Afin de structurer efficacement mon travail et de suivre l'avancement des différentes étapes, j'ai choisi de gérer ce projet à l'aide de Trello

J'ai pu créer plusieurs listes représentant les grandes phases du projet (à faire, en cours, terminé), y ajouter des cartes pour chaque tâche, et y associer des commentaires et des pièces jointes. Cet outil m'a permis de mieux visualiser la progression du projet et de prioriser les actions à mener.



Toujours dans un souci d'organisation, un cahier de tests sera réalisé en fin de projet afin de valider le bon fonctionnement de la solution et de repérer d'éventuels dysfonctionnements à corriger.

1 – Stormshield et segmentation du réseau par VLAN

1.1 – Segmentation VLAN et configuration du switch Cisco

1.1.1 – Segmentation VLAN

Dans un premier temps, je configure le switch. Cela permettra d'attribuer les VLAN. Il ne restera plus qu'à configurer le routeur pour que le réseau soit opérationnel.

Afin de préparer la configuration du switch, GNS3 a été utilisé. Les noms des interfaces seront donc différents de ceux du switch utilisé en production, mais la configuration reste identique. Il suffira d'adapter les interfaces.

Voici la segmentation par port qui sera mise en place :

- Les ports 1 à 6 (Ethernet 0/0 à 1/1 sur GNS3) sont affectés au VLAN 10.
- Les ports 7 à 12 (Ethernet 1/2 à 2/3 sur GNS3) sont affectés au VLAN 20.
- Les ports 13 à 18 (Ethernet 3/0 à 4/1 sur GNS3) sont affectés au VLAN 30.
- Les ports 19 à 23 (Ethernet 4/2 à 5/2 sur GNS3) sont affectés au VLAN 99.
- Le port 24 (Ethernet 5/3 sur GNS3) est configuré en trunk pour permettre la transmission des VLANs 10, 20, 30 et 99 vers le routeur.

Dans un premier temps, je crée tous mes VLANs en leur attribuant un nom afin qu'ils soient facilement reconnaissables.

```
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN_CLIENT
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN_SERVEUR
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name DMZ
Switch(config-vlan)#exit
Switch(config)#vlan 99
Switch(config-vlan)#name VLAN_ADMIN
Switch(config-vlan)#exit
```

Je sélectionne les interfaces appartenant au VLAN 10, je les configure en mode « access » et j'indique qu'elles doivent associer les trames au VLAN 10. J'effectue un « no shutdown » afin d'activer les interfaces si elles sont désactivées.

```
Switch(config)#int range Eth 0/0 - 3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#no shut
Switch(config-if-range)#exit
Switch(config)#int range Eth 1/0 - 1
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#no shut
Switch(config-if-range)#exit
```

Je répète l'opération pour les ports de tous les VLANs.

Je vais à présent configurer le port 24 (Ethernet 5/3 sur GNS3) en mode trunk.

La différence entre un port en mode trunk et un port en mode access réside dans la gestion des VLANs. Un port en mode access est associé à un seul VLAN. Lorsqu'un appareil est connecté à ce port et envoie une trame, celle-ci est automatiquement taggué à ce VLAN. Un port en mode trunk peut transporter plusieurs VLANs simultanément en utilisant le VLAN ID (VID) pour identifier chaque trame et déterminer à quel VLAN elle appartient.

Comme il s'agit de la première configuration en mode trunk sur cette interface, le switch a besoin qu'on lui précise le protocole d'encapsulation à utiliser pour les trames VLAN.

```
Switch(config)#int Eth 5/3
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,20,30,99
Switch(config-if)#no shut
Switch(config-if)#exit
```

1.1.2 – Configuration de l'accès en SSH au Switch

Pour l'instant, l'accès au switch se fait en série. Je vais maintenant mettre en place le SSH afin de pouvoir administrer le switch à distance.

Pour avoir accès au switch à distance une IP est nécessaire. Etant donné que le réseau d'administration est le 192.168.99.0/24 et conformément au schéma réseau se seras l'IP 192.168.99.250 qui lui seras attribuée.

```
Switch(config)#int vlan 99
Switch(config-if)#ip address 192.168.99.250 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
```

Ensuite, je vais générer une paire de clés RSA, mais je dois d'abord configurer le nom de domaine du switch. Celui-ci est nécessaire pour former le FQDN (Fully Qualified Domain Name), c'est-à-dire le nom complet du switch sur le réseau (par exemple Switch.rest0.fr).

```
Switch(config)#ip domain-name rest0.fr
Switch(config)#crypto key generate rsa
The name for the keys will be: Switch.rest0.fr
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

Switch(config)#
*May  8 17:14:19.026: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Je vais ensuite configurer la version SSH et assigner ce protocole à une ligne VTY (qui correspond aux accès à distance via les protocoles Telnet ou SSH). Enfin, je viens spécifier la méthode d'authentification.

```
Switch(config)#ip ssh version 2
Switch(config)#line vty 0 4
Switch(config-line)#transport input ssh
Switch(config-line)#login local
Switch(config-line)#username matheo.teneur.admin password Btssio64
```

Je défini un mot de passe pour le mode enable afin de pouvoir avoir accès à ce mode en SSH et je configure l'authentification par clé sur le switch.

```
Switch(config)#enable password Btssio64
```

```
Switch(config)#ip ssh pubkey-chain
Switch(conf-ssh-pubkey)#username matheo.teneur.admin
Switch(conf-ssh-pubkey-user)#key-string
Switch(conf-ssh-pubkey-data)#$TaYBGdhE/nNhn7BWhhHBV16fsxnh1usCNtJnU33m+d
Switch(conf-ssh-pubkey-data)#$-key-20250508 matheo.teneur.admin@0.0.0.0
Switch(conf-ssh-pubkey-data)#exit
Switch(conf-ssh-pubkey-user)#exit
Switch(conf-ssh-pubkey)#exit
```

Cela revient à mettre une clé publique associé à un utilisateur dans authorized_keys sur Debian.

Je peux donc désormais accéder à mon switch par clé

```
Using username "matheo.teneur.admin".
Authenticating with public key "rsa-key-20250508"

Switch>
```

Je sauvegarde la configuration

```
Switch#copy run start
Destination filename [startup-config]?
Building configuration...
Compressed configuration from 3519 bytes to 1651 bytes[OK]
Switch#copy run tftp://192.168.20.4/switch-config
Address or name of remote host [192.168.20.4]?
Destination filename [switch-config]?
!!
3519 bytes copied in 0.280 secs (12568 bytes/sec)
```

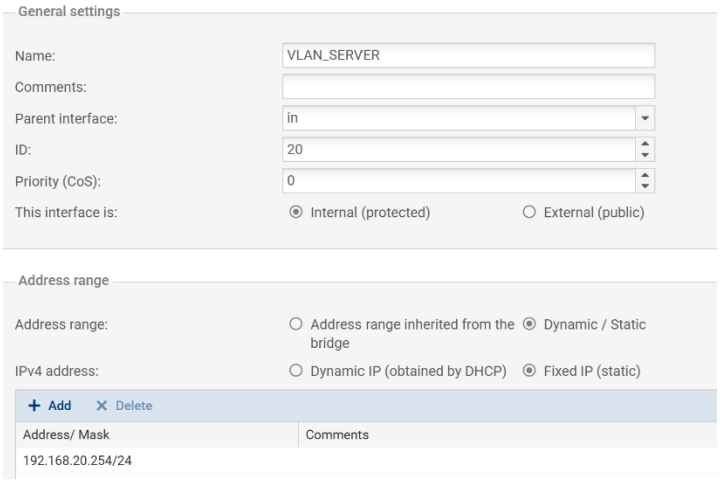
(La dernière capture d'écran à été réalisée après avoir configurer le serveur TFTP)

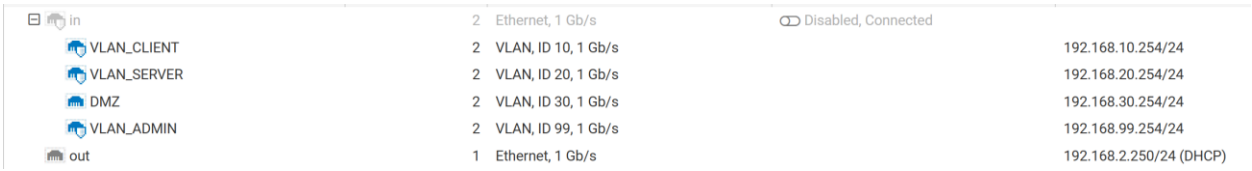
1.2 - Stormshield

J'utilise un Stormshield car étant un UTM il permet de de centraliser à la fois le routage et la sécurité réseau dans un seul équipement. Il embarque un IDS/IPS qui permet d'analyser en direct le traffic et de prévenir les menaces potentielles.

La gestion par objets proposée par Stormshield est également très intéressante. Elle permet d'attribuer des noms clairs aux machines, réseaux ou services, ce qui rend la configuration plus lisible. En cas de modification de l'infrastructure, il suffit de mettre à jour l'objet concerné pour que le changement soit automatiquement pris en compte dans toutes les règles qui l'utilisent.

Stormshield dispose actuellement de deux interfaces : l'interface "in" et l'interface "out" (WAN). Dans Configuration > Network > Interfaces, j'ai désactivé l'interface "in" et créé mes VLANs en les associant à cette interface.

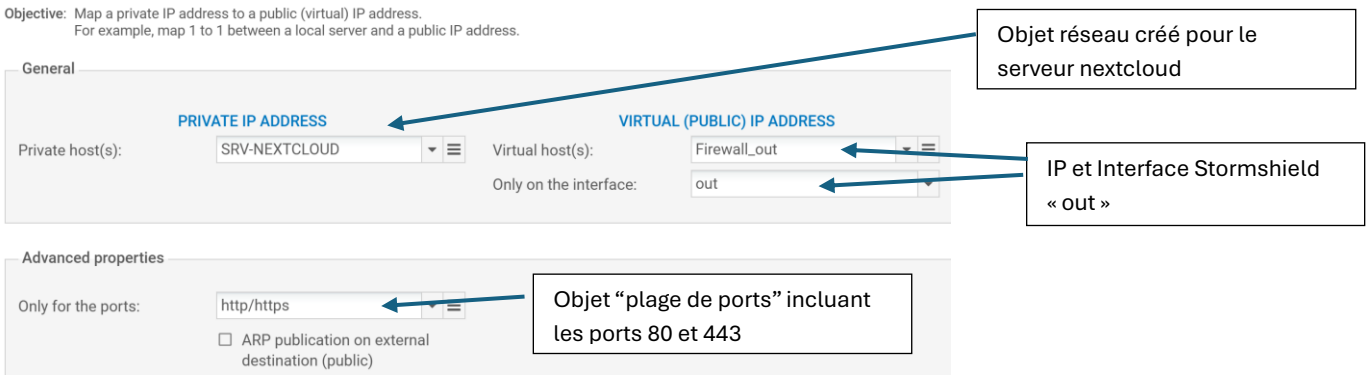




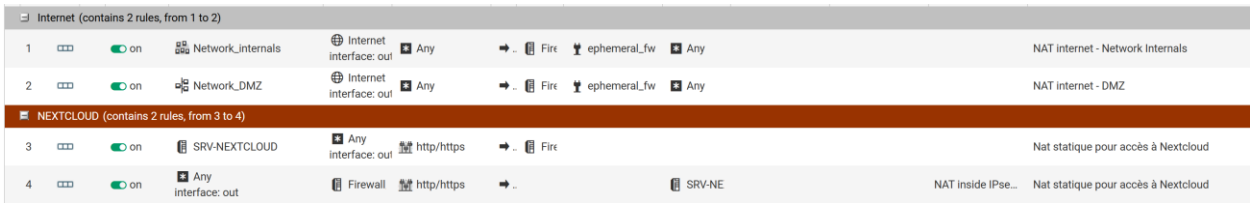
J'ajoute une règle de filtrage autorisant tout le trafic dans Configuration > Security Policy > Filter - NAT. Les règles de filtrage seront ajoutées une fois l'architecture déployée. Cela permet de minimiser les problèmes lors du déploiement. Une fois l'architecture fonctionnelle, les règles de filtrage seront mises en place.

Une fois les VLAN configurés, je mets en place le NAT. Quatre règles sont nécessaires : une règle de NAT dynamique pour l'accès à Internet depuis le LAN, une pour l'accès à internet depuis la DMZ, une règle pour rediriger le trafic provenant d'Internet sur les ports 80 et 443 vers les ports 80 et 443 (HTTP/HTTPS) du serveur Nextcloud et une quatrièeme pour permettre au serveur Nextcloud de leur répondre.

Pour l'accès aux serveurs internes depuis le WAN Stormshield embarque un utilitaire qui vas nous simplifier la rédaction de la règle :



Voici la configuratin des règles de NAT :



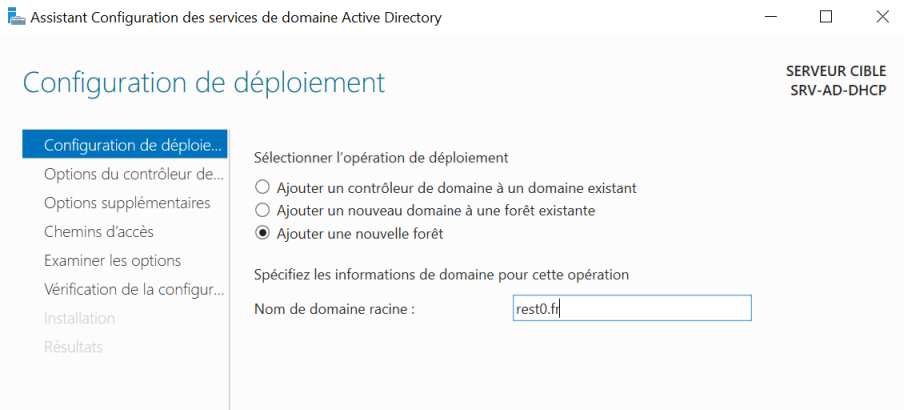
2 – installation et configuration de l'Active Directory

Installation du rôle AD DS.

Le rôle DNS est installé automatiquement avec le rôle AD DS.

Une fois installé, je renomme le serveur en « SRV-AD-DHCP » via les paramètres système avancés puis je redémarre

Ensuite, il faut promouvoir le serveur en contrôleur de domaine. Etant donné que la forêt rest0.fr n'existe pas il faut ajouter une nouvelle forêt.



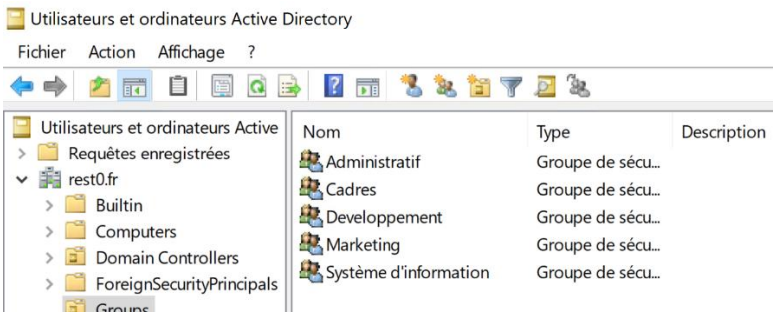
Il est nécessaire de définir un mot de passe pour le compte « Administrateur » du domaine et le mot de passe DSRM qui est un mot de passe unique utilisé pour accéder au mode de restauration des services d'annuaire.

Concernant les chemins d'accès et options je laisse les valeurs par défaut.

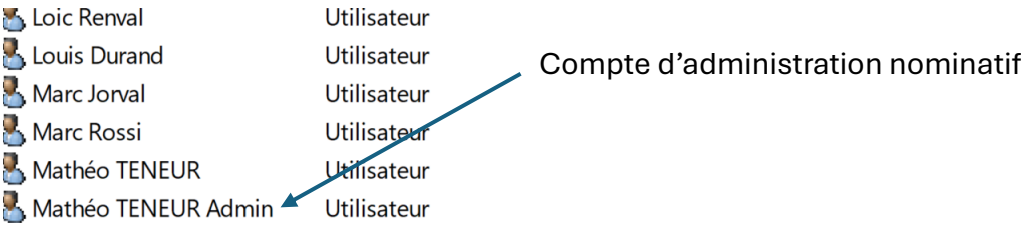
Une fois l'Active Directory configurer le serveur vas redémarrer.

Je me connecte au système et crée un compte personnel ainsi qu'un compte d'administration nominatif. Afin de disposer des mêmes privilèges que le compte Administrateur, j'ajoute mon compte aux mêmes groupes auxquels appartient ce dernier.

Dans l'utilitaire « Utilisateurs et ordinateurs Active Directory », je crée une Unité d'Organisation (OU) nommée « groups », dans laquelle je vais organiser tous les groupes.

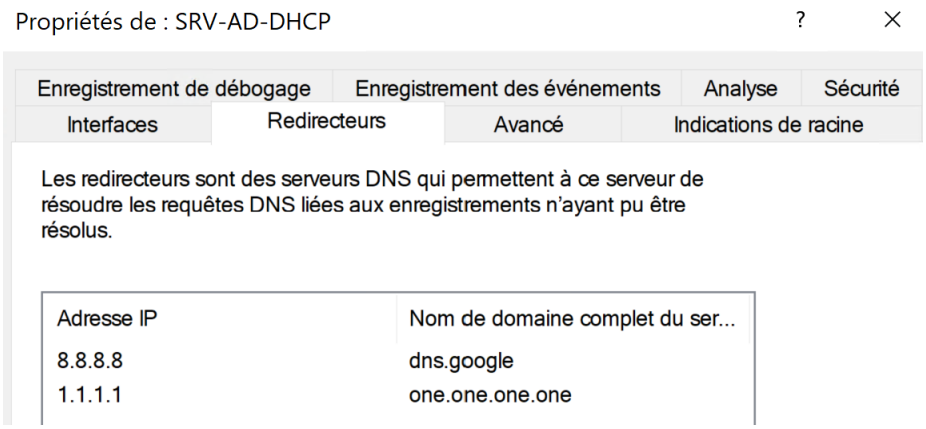


Une fois tous les groupes créés, je crée les utilisateurs en suivant la nomenclature « prenom.nom » et je les affecte à leurs groupes respectifs.



Dans la console DNS, j'ai ajouté les adresses 8.8.8.8 (Google DNS) et 1.1.1.1 (Cloudflare DNS) comme redirigeant DNS.

Cela permet au serveur DNS local de résoudre les requêtes qui ne peuvent pas être traitées par le serveur DNS interne, en redirigeant les demandes vers des serveurs DNS publics.



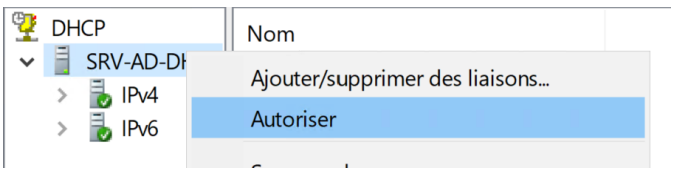
3 – DHCP

3.1 – Configuration du serveur DHCP

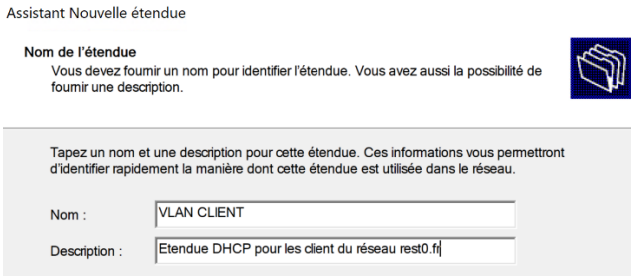
J'ouvre le Gestionnaire de serveur. Dans le menu Gérer, je sélectionne « Ajouter des rôles et fonctionnalités ».

Je sélectionne Rôle > Serveur DHCP et clique sur Suivant. Je confirme l'installation et clique sur Installer.

Après l'installation, j'ouvre la console DHCP. En cliquant sur le serveur je sélectionne « Autoriser »



Enfin, je lie mon serveur au compte Administrateur de l'Active Directory afin de lui donner les autorisations nécessaires à son fonctionnement puis je créé une nouvelle étendue que je nomme « VLAN CLIENT »

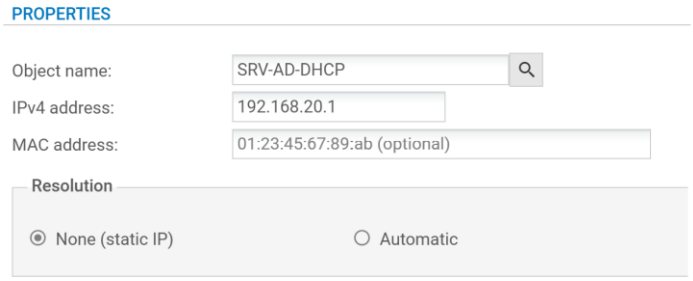


Lors de la création de l'étendue, je configure la durée du bail (par défaut fixée à 8 jours) et je laisse les autres paramètres de délai inchangés. Lorsqu'on me demande si je souhaite configurer les options du serveur maintenant ou plus tard, je sélectionne « Configurer les options DHCP maintenant ». Je définis l'adresse IP de mon Stormshield comme passerelle et je configure mon serveur AD et 8.8.8.8 comme serveurs DNS.

3.2 – Mise en place DHCP Relay

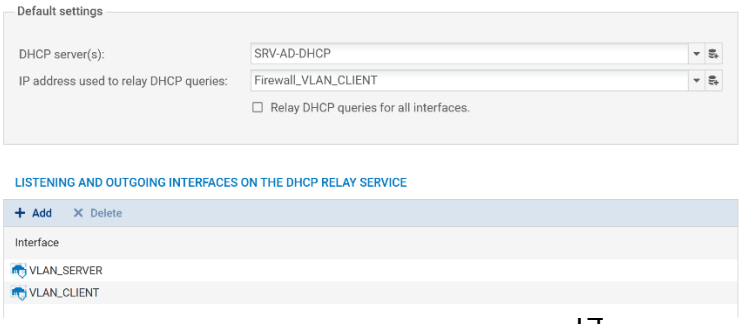
Dans l'onglet Configuration > Network > DHCP, j'active le DHCP Relay sur Stormshield.

Je crée un objet réseau de type hôte pour mon serveur AD/DHCP :



Je le configure en tant que serveur DHCP. Étant donné que je souhaite transmettre les demandes du VLAN CLIENT, je le définis comme IP source pour relayer les requêtes DHCP.

Je spécifie les réseaux VLAN SERVER et VLAN CLIENT comme réseaux d'entrée et de sortie pour le service DHCP Relay.



4 – TFTP

4.1 – Sécurisation du SSH avec connexion par clé

Tout d'abord je vais sécuriser la connexion au serveur TFTP. Je vais donc désactiver l'authentification SSH par mot de passe et mettre place la connexion par clé.

On génère une paire de clé (sur Windows j'utilise PuttyGen et sur Linux OpenSSL) en ED25519 (recommandation de l'ANSSI)

Étant donné que le système du client SSH est sous Windows, je sauvegarde la clé privée dans le répertoire « .ssh » de l'utilisateur. Ensuite, je la déplace dans le répertoire rest0.fr (un répertoire que j'ai créé pour stocker les différentes clés utilisées pour me connecter aux serveurs de rest0.fr). Enfin, chaque clé est placée dans un sous-dossier correspondant au nom du serveur (par exemple, .ssh/rest0.fr/srv-tftp), afin d'avoir un jeu de clés distinct par serveur. Cela permet de garantir que dans le cas où une paire de clés serait compromise, les autres clés restent sécurisées.

Connexion en ssh classique (login+mdp) au serveur TFTP puis j'ouvre /userAvecLequelJeVeuxMeConnecterAvecMaClé/.ssh/authorized_keys

Je place la clé publique associée à la clé privée, en indiquant à la fin le login autorisé avec cette clé et l'adresse IP depuis laquelle la connexion est permise.

```
 GNU nano 7.2                                                    /home/loic/.ssh/authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIe+wW6c/FjXmvQ9aZyUUcJY5miyP4c8Jha6Z4Gpav2h eddsa-key-20250422 loic@0.0.0.0
```

Pour me connecter avec loic depuis toutes les IPs.

Je me connecte avec la clé via PuTTY et je désactive l'authentification par mot de passe dans le fichier /etc/ssh/sshd_config en définissant « PasswordAuthentication no »

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
```

4.2 – Serveur TFTP

Pour installer le serveur je mets à jour la liste des paquets avec la commande « apt update » et j'installe le paquet tftp-hpa avec la commande « apt install tftpd-hpa »

Il faut ensuite configurer les options du serveur via son fichier de configuration dans « /etc/default/tftpd-hpa »

```
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS=":69"
TFTP_OPTIONS="--secure --create"
```

- **TFTP_USERNAME :** Cette ligne spécifie le nom d'utilisateur sous lequel le serveur TFTP s'exécute.
- **TFTP_DIRECTORY :** Cette ligne définit le répertoire racine du serveur TFTP où les fichiers seront stockés
- **TFTP_ADDRESS :** Définit l'adresse IP et le port sur lesquels le serveur TFTP écoute. Ici, le serveur accepte des connexions sur toutes les interfaces réseau disponibles sur le port par défaut (69).
- **TFTP_OPTIONS :**
    - **–secure :** Cette option assure que le serveur TFTP fonctionne dans un mode sécurisé, en limitant les actions possibles aux répertoires autorisés
    - **--create** : Cette option permet au serveur de créer de nouveaux fichiers s'ils n'existent pas déjà lorsque le client tente de les transférer

Je donne les permissions à l'utilisateur « tftp » sur le répertoire « /srv/tftp » afin qu'il puisse y modifier son contenu.

```
root@srv-tftp:~# chown tftp:tftp /srv/tftp
```

Je sauvegarde la configuration du switch sur le serveur TFTP et je vérifie qu'elle a bien été enregistrée dans le répertoire sous le nom « switch-config ».

```
root@srv-tftp:~# ls /srv/tftp/
switch-config
root@srv-tftp:~# cat /srv/tftp/switch-config

!
! Last configuration change at 18:08:40 UTC Thu May 8 2025 by matheo.teneur.admin
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable password Btssio64
!
username matheo.teneur.admin privilege 15 password 0 Btssio64
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip cef
!
!
no ip domain-lookup
ip domain-name rest0.fr
no ipv6 cef
ipv6 multicast rpf use-bgp
!
```

5 - GLPI

5.1 - Installation

Je vais installer le serveur GLPI sur un Debian 12. Je configure l'accès par clé comme pour le serveur TFTP.

J'ai me suis aider de ce tutoriel e de la documentation officielle de GLPI pour installer le serveur : https://www.it-connect.fr/installation-pas-a-pas-de-glpi-10-sur-debian-12/

Je mets à jour la liste des paquets et les paquets. Je viens installer un serveur LAMP (Linux Apache MariaDB PHP)

Puis j'installe toutes extensions PHP requises pour le bon fonctionnement de GLPI :

apt-get install php-xml php-common php-json php-mysql php-mbstring php-curl php-gd php-intl php-zip php-bz2 php-imap php-apcu

J'installe également l'extension php-ldap car je vais synchroniser l'annuaire de GLPI à l'annuaire du domaine rest0.fr

Je me connecte à MySQL pour créer une base de données GLPI et créer un utilisateur pour administrer cette base de données.

```
MariaDB [(none)]> CREATE DATABASE db_glpi;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON db_glpi.* TO glpi_adm@localhost IDENTIFIED BY "Btssio64";
Query OK, 0 rows affected (0,000 sec)

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

(Tous les mots de passe du projet son Btssio64 ou Btssio64* car c'est une maquette. Dans un environnement de production j'aurais mis des mots de passes robustes.)

Je crée le répertoire /var/www/glpi, puis Je télécharge ensuite la dernière version de l'archive de GLPI dans /tmp à l'aide de la commande wget. J'extrais le contenu de l'archive dans /var/www/glpi.

J'attribue la propriété à l'utilisateur et au groupe www-data (utilisés par Apache2), en appliquant ces droits récursivement à tout le contenu du répertoire.

A présent je vais déplacer les répertoires config et files de GLPI dans /etc/glpi/config et /var/lib/glpi/files et créer le répertoire /var/log/glpi pour les journaux afin de suivre les recommandations de l'éditeur.

Une fois ceci effectué j'attribue l'utilisateur et le groupe www-data propriétaire des répertoires /etc/glpi, /var/lib/glpi et /var/log/glpi.

Je viens indiquer à GLPI où aller chercher les données via le fichier /var/www/glpi/inc/downstream.php :

```
 GNU nano 7.2              /var/www/glpi/inc/downstream.php
<?php
define('GLPI_CONFIG_DIR', '/etc/glpi/');
if (file_exists(GLPI_CONFIG_DIR . '/local_define.php')) {
    require_once GLPI_CONFIG_DIR . '/local_define.php';
}
```

Je créer le fichier /etc/glpi/local_define.php destiné à préciser les chemins vers les répertoires "files" et "log" :

```
 GNU nano 7.2                 /etc/glpi/local_define.php
<?php
define('GLPI_VAR_DIR', '/var/lib/glpi/files');
define('GLPI_LOG_DIR', '/var/log/glpi');
```

Je viens configurer le VirtualHost de GLPI via le fichier /etc/apache2/sites-available/glpi.rest0.fr

```
 GNU nano 7.2                                  /etc/apache2/sites-available/glpi.rest0.fr.conf *
<VirtualHost *:80>
    ServerName glpi.rest0.fr

    DocumentRoot /var/www/glpi/public

    # If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving multiple applications),
    # you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the GLPI directory itself.
    # Alias "/glpi" "/var/www/glpi/public"

    <Directory /var/www/glpi/public>
        Require all granted

        RewriteEngine On

        # Redirect all requests to GLPI router, unless file exists.
        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>
</VirtualHost>
```

Les lignes « RewriteCond %{REQUEST_FILENAME} !-f » et « RewriteRule ^(.*)$ index.php [QSA,L] » font partie de la configuration de réécriture d'URL d'Apache. Elles servent à rediriger les requêtes vers le fichier index.php si la ressource demandée n'existe pas en tant que fichier.

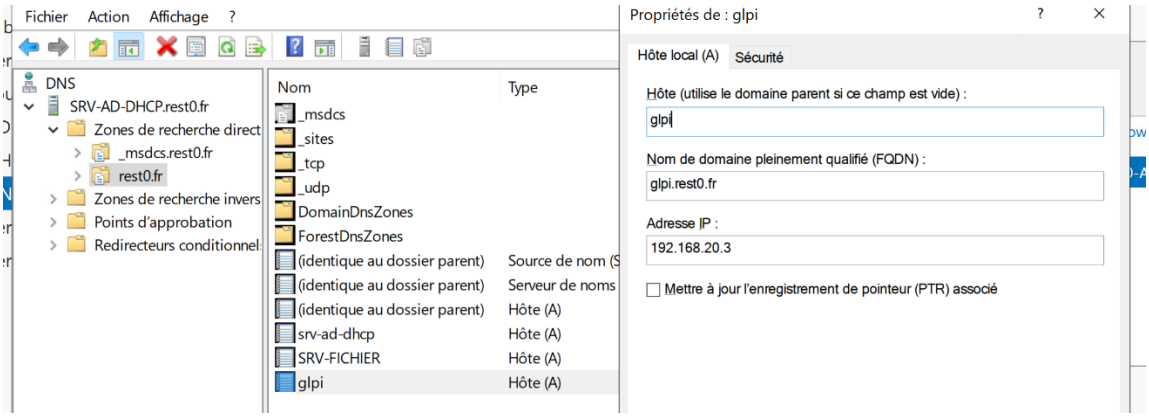
Cela permet de centraliser la gestion des routes dans un seul fichier, ce qui est le cas de GLPI.

Je désactive le VirtualHost par défaut avec la commande « a2dissite 000-default.conf », je peux également supprimer le répertoire /var/www/html qui devient inutile puis j'active le VirtualHost de GLPI avec la commande « a2ensite glpi.rest0.fr.conf ».

Je dois activer le module Apache « rewrite » indispensable pour la réécriture d'URL. J'entre donc la commande « a2enmod rewrite ».

J'active l'option session.cookie_httponly dans le fichier php.ini, qui configure les paramètres de fonctionnement de PHP. Cette directive renforce la sécurité en empêchant l'accès au cookie de session PHP via JavaScript côté client.

J'ai créé un enregistrement DNS de type A dans le DNS du domaine, pointant vers l'adresse IP de GLPI (192.168.20.3), afin que les utilisateurs puissent y accéder via son URL. Cela permet également d'effectuer toutes les configurations en utilisant son nom de domaine. Ainsi, si l'adresse IP venait à changer, il suffirait de modifier l'enregistrement DNS.



Je peux dorénavant redémarrer Apache avec la commande « systemctl restart apache2 ». GLPI est accessible à l'adresse glpi.rest0.fr

Je dois configurer les options relatives au « backend » de GLPI.

Je renseigne les informations concernant la base de données que j'ai créé pour GLPI.

5.2 - Gestion des habilitations

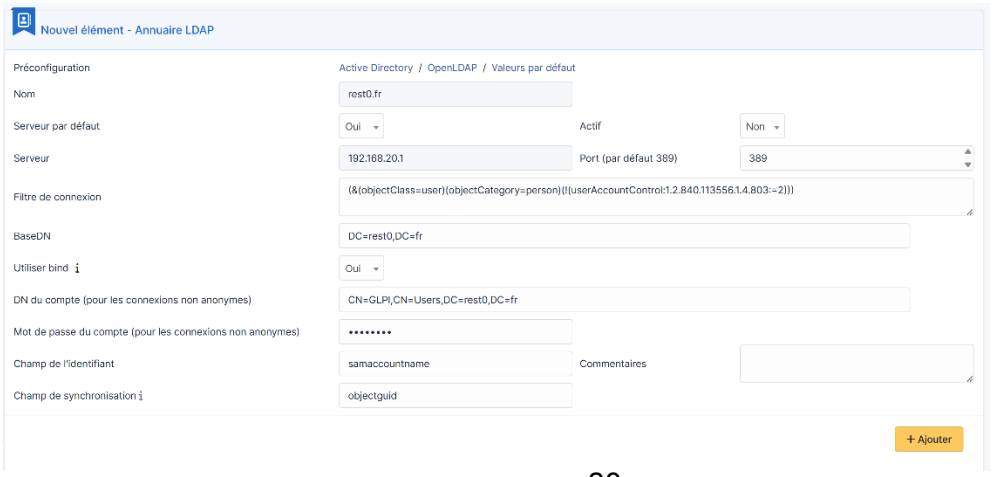
La gestion des habilitations sur GLPI est gérée comme suit :

- Les membres du groupe « Admins du domaine » sont attribué au profil super-admin.
- Les membres du groupes « Système d'information » sont attribué au profil technicien.
- Les membres du groupes « Cadres » sont attribué au profil Self-Service.
- Les membres du groupes « Administratif / Marketing / Développement » sont attribué au profil Observer

Pour gérer le plus simplement et efficacement les habilitations j'ai synchronisé l'annuaire GLPI avec l'annuaire du domaine Active Directory.

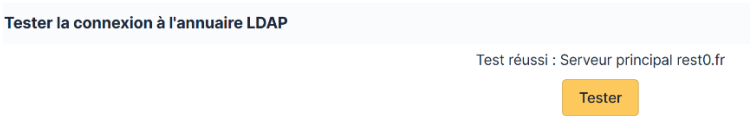
Pour faire cela j'ai commencé par créer un compte de service pour GLPI puis dans l'interface Web du serveur je me suis rendu dans Configuration > Authentification > Annuaire LDAP > Ajouter

Et j'ai configurer toutes les options nécessaires. Concernant le filtre de connexion c'est le filtre par défaut pour un domaine Active Directory.

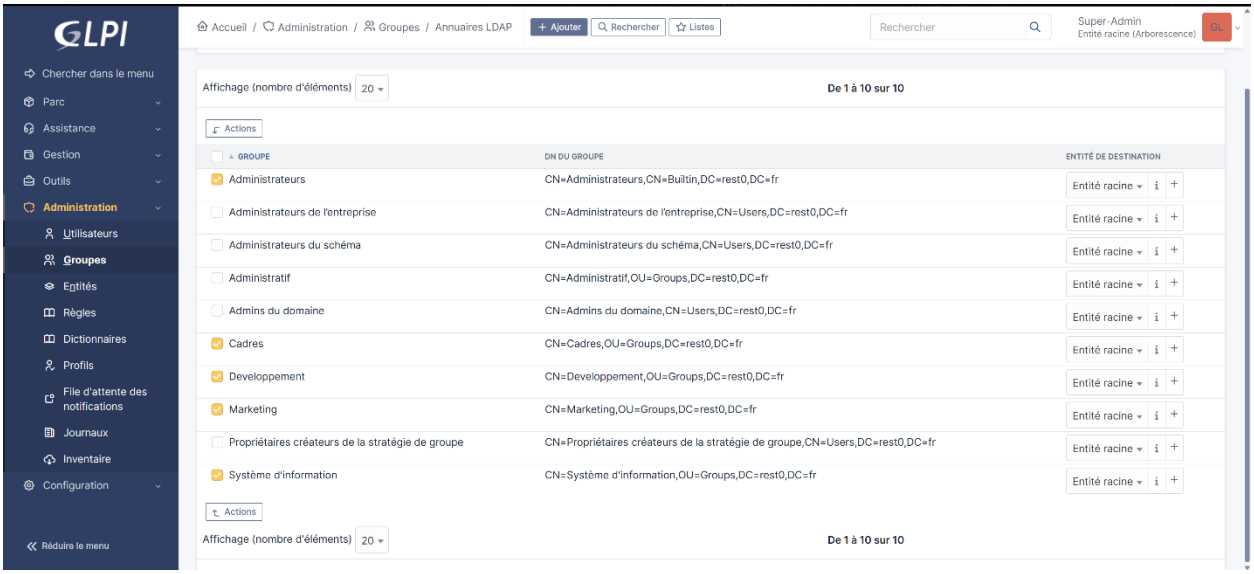


Contexte rest0.fr

Je teste la connexion au domaine avec le compte GLPI :

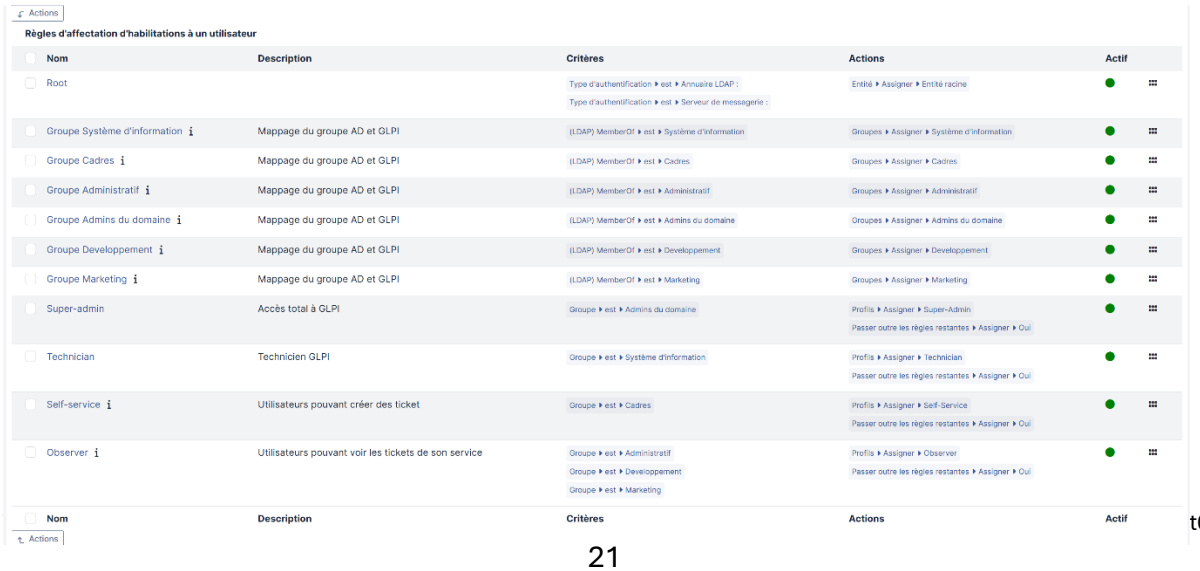


Une fois connecté au domaine je vais importer les groupes Active Directory nécessaires à la gestion des utilisateurs. Pour ce faire je me rends dans Administration > Groupes > Liaison annuaires LDAP > Importation de nouveaux groupes puis je sélectionne les groupes dont j'ai besoins



Je les importe. Ils apparaissent dorénavant dans Administration > Groupes et peuvent être attribués à des utilisateurs ou dans des règles.

Je viens donc faire mes règles pour mapper les utilisateurs dans les bons groupes et leur assigner le bon profil en fonction de leur(s) groupe(s) Active Directory



t0.fr

5.3 - Inventaire

Je vais utiliser glpi-agent, un outil basé sur un fork de FusionInventory (une copie du code source du projet, modifiable indépendamment de l'auteur d'origine). En effet, FusionInventory, qui était jusqu'alors la référence pour l'inventaire des équipements dans GLPI via un agent, a été abandonné.

C'est désormais glpi-agent qui a repris le développement du projet.

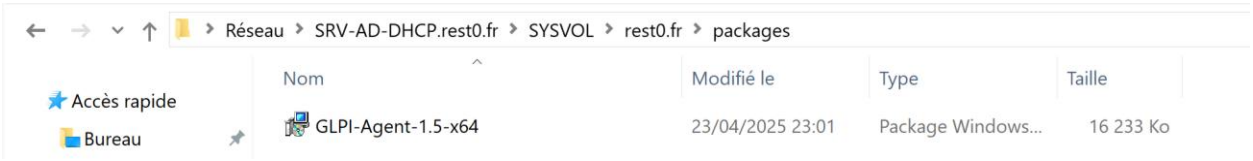
Pour les équipements ne fonctionnant pas sous Windows ou Linux (Cisco IOS et Stormshield), j'utiliserai le protocole SNMP afin de réaliser leur inventaire.

J'aurais besoin d'installer le plugin GLPI Inventory afin de réaliser des injections de fichier d'inventaire XML générer à partir des inventaires en SNMP.

5.3.1 – Clients Windows

Je vais récupérer le dernier package d'installation de glpi-agent sur la page github du projet : https://github.com/glpi-project/glpi-agent/releases/

Je créé un répertoire « packages » dans le SYSVOL de mon domaine et j'y dépose le .msi pour installer glpi-agent sur Windows.



Je créer une GPO avec pour installer le .msi de glpi-agent.

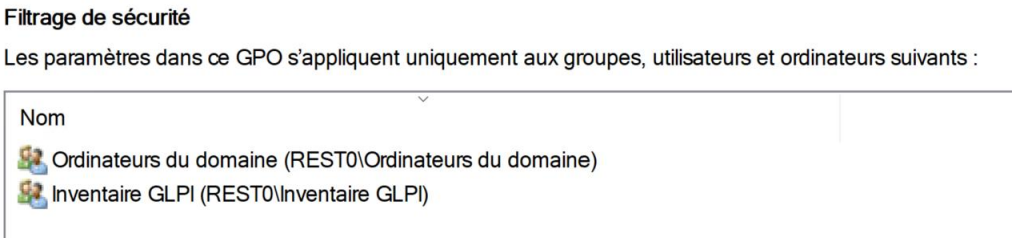
L'agent GLPI stocke ses paramètres sous formes de clés de registre. Pour le configurer on vas donc venir modifier les clés de registre nécessaires.

Contexte rest0.fr

Ces clés permettent de définir le serveur GLPI auquel envoyer les inventaires, ainsi que les réseaux autorisés à effectuer une demande d'inventaire.

Je crée un groupe Active Directory nommé « Inventaire GLPI » afin d'installer l'agent GLPI sur les ordinateurs qui ne sont pas membres du groupe « Ordinateurs du domaine » tel que les contrôleurs de domaine.

Dans les paramètres de filtrage de sécurité de la GPO, je retire « Utilisateurs authentifiés » et le remplace par « Ordinateurs du domaine » et « Inventaire GLPI ».



Cependant, cette modification supprime « Utilisateurs authentifiés » de la délégation, ce qui rend la GPO illisible. Pour y remédier, j'ajoute manuellement « Utilisateurs authentifiés » avec des droits en lecture dans la délégation.

J'ajoute le serveur Active Directory à « inventaire GLPI »

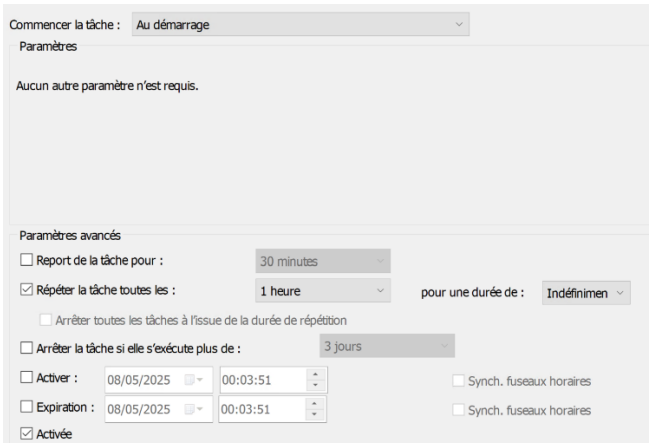
Je redémarre un ordinateur du domaine pour voir si cela fonctionne. Ce n'est pas possible de faire un gpupdate car c'est une stratégie ordinatrice qui installe le msi.

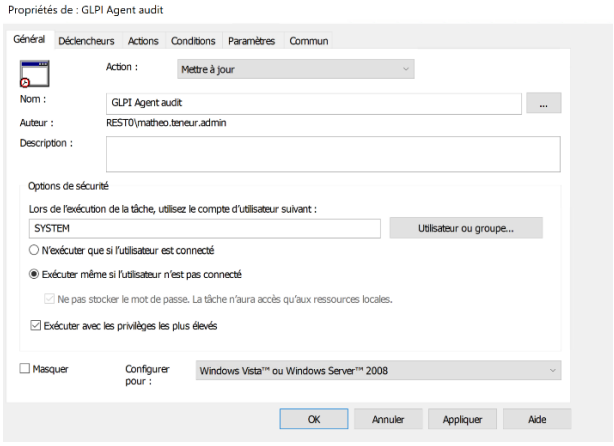
Le client GLPI s'installe correctement et les clés de registre sont bien configurées.

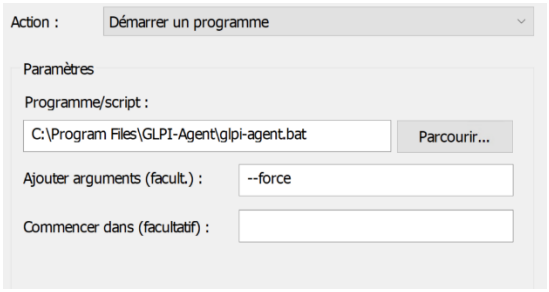
Je force un inventaire à l'aide du script C:\Program Files\GLPI-Agent\glpi-agent.bat avec l'option --force.

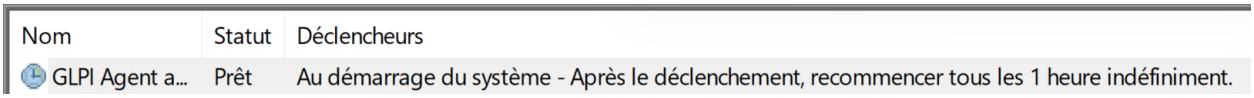
L'ordinateur remonte correctement dans le tableau de bord de GLPI, ce qui confirme que la GPO fonctionne et configure correctement glpi-agent.

Pour programmer un inventaire chaque heure dès le démarrage des machines Windows, je déploie une tâche planifiée via la GPO GLPI Agent.









Cette tâche planifiée exécute le script C:\Program Files\GLPI-Agent\glpi-agent.bat avec l'option --force, en utilisant le compte SYSTEM, même si aucun utilisateur n'est connecté.

Cela permet de garantir que les inventaires sont réalisés automatiquement et régulièrement, sans dépendre de l'ouverture de session d'un utilisateur.

5.3.2 – Clients Linux

Pour installer la dernière version de l'agent GLPI, je me rends sur le GitHub du projet et je copie le lien de la dernière version du « Linux Installer », au format .pl.

Sur la machine à inventorier, je télécharge le fichier dans /tmp avec wget, puis je l'exécute avec perl (l'équivalent de bash script.sh, mais pour les scripts Perl).

Lors de l'installation, je renseigne les informations du serveur GLPI de destination.

```
root@srv-tftp:/tmp# perl glpi-agent-1.14-linux-installer.pl
Installing glpi-agent v1.14...
glpi-agent is about to be installed as service

Provide an url to configure GLPI server:
> http://glpi.rest0.fr/front/inventory.php

Provide a path to configure local inventory run or leave it empty:
>

Provide a tag to configure or leave it empty:
>
Applying configuration...
Enabling glpi-agent service...
```

Je lance un inventaire avec la commande « glpi-agent », puis j'active le service au démarrage avec « systemctl enable glpi-agent »

```
root@srv-tftp:/tmp# glpi-agent
[info] target server0: server http://glpi.rest0.fr/front/inventory.php
[info] sending prolog request to server0
[info] server0 answer shows it supports GLPI Agent protocol
[info] sending contact request to server0
[info] running task Inventory
[info] New inventory from srv-tftp-2025-04-24-02-34-43 for server0
```

Pour lancer un inventaire toutes les heures sur les machines Linux, j'utilise cron pour exécuter la commande « glpi-agent » chaque heure.

5.3.3 – Clients SNMP

Pour inventorier mes équipements en SNMP, j'utilise le programme glpi-netinventory (en complément de glpi-agent) ainsi que le plugin GLPI Inventory.

J'installe le paquet .deb de NetInventory depuis le GitHub du projet. Ce programme permet d'interpréter les résultats de snmpwalk et de générer des fichiers XML à injecter dans GLPI Inventory.

J'installe le plugin GLPI Inventory depuis la boutique des plugins de GLPI.

Je crée un répertoire snmp.d dans le dossier de configuration de glpi-agent. Tous les scripts qu'il contient sont exécutés une fois par heure par /usr/local/bin/run-snmp-scripts.sh (le répertoire /usr/local/bin/ étant utilisé par défaut pour les scripts personnalisés), lui-même lancé par une tâche cron.

Cette configuration me permet de simplement copier, configurer et placer les scripts de supervision dans le répertoire snmp.d pour qu'ils soient automatiquement exécutés une fois par heure.

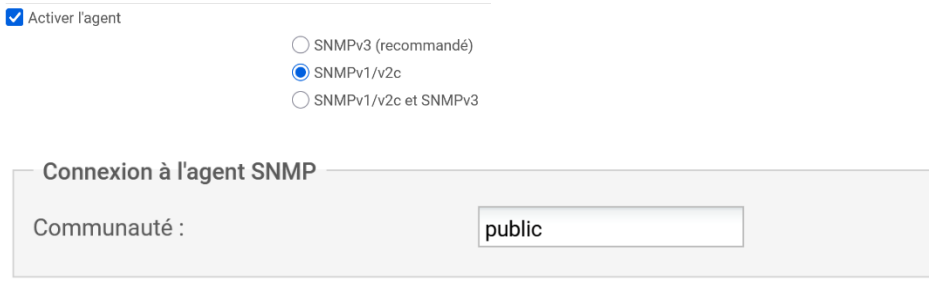
Je décide d'indiquer manuellement dans le script le nom des équipements afin de mieux les repérer dans GLPI.

J’indique également manuellement le numéro de série. En effet, j’ai rencontré des problèmes de doublons, car le numéro de série ne remonte pas correctement : mauvaise interprétation des données fournies par la MIB pour les équipements Stormshield, et absence de numéro de série pour le switch, car il s’agit d’un IOU GNS3.

Exemple du script d’inventorisation du routeur Stormshield :

```
  GNU nano 7.2                                                    /etc/glpi-agent/snmp.d/FW-SIEGE.sh
#!/bin/bash

# --- Configuration de l'inventaire ---
TS=$(date +%s)                              # Timestamp pour nommer les fichiers temporairement
IP="192.168.20.254"                         # Adresse IP de l'équipement à inventorier
SNMP_COMMUNITY="public"                     # Communauté SNMP
SN="VMSNSX09K0639A9"                        # Numéro de série ou identifiant unique
NAME="FW-SIEGE"                             # Nom convivial de l’équipement
GLPI_URL="http://glpi.rest0.fr/marketplace/glpiinventory/"  # URL du plugin d’inventaire GLPI

# --- Fichiers temporaires ---
SNMP_FILE="/tmp/glpi-inventory-snmp.tmp.${SN}.${TS}.snmp"
XML_FILE="/tmp/glpi-inventory-snmp.tmp.${SN}.${TS}.xml"

# --- Étape 1 : Récupération SNMP ---
# Exécution d’un snmpwalk pour récupérer les informations de l’équipement
snmpwalk -v2c -c "$SNMP_COMMUNITY" "$IP" > "$SNMP_FILE"

# --- Étape 2 : Génération du fichier XML d’inventaire ---
# Conversion du fichier SNMP en XML utilisable par GLPI
glpi-netinventory --file "$SNMP_FILE" > "$XML_FILE"

# --- Étape 3 : Nettoyage du XML et injection de NAME/SERIAL ---
# Suppression des balises NAME et SERIAL existantes (si présentes)
sed -i '/<NAME>.*<\/NAME>/d' "$XML_FILE"
sed -i '/<SERIAL>.*<\/SERIAL>/d' "$XML_FILE"

# Insertion des nouvelles balises NAME et SERIAL juste avant </INFO>
sed -i "/<\/INFO>/i \ \ \ \ <SERIAL>$SN</SERIAL>" "$XML_FILE"
sed -i "/<\/INFO>/i \ \ \ \ <NAME>$NAME</NAME>" "$XML_FILE"

# --- Étape 4 : Envoi du fichier XML à GLPI ---
# Lancement de l’injection vers GLPI, en capturant la sortie et le code retour
INJECT_OUTPUT=$(glpi-injector -f "$XML_FILE" --no-ssl-check --no-compression -u "$GLPI_URL" 2>&1)
INJECT_EXIT_CODE=$?

# --- Étape 5 : Logging en fonction du résultat ---
if [ $INJECT_EXIT_CODE -eq 0 ]; then
    logger -t GLPI-INVENTORY-SNMP "Inventaire réussi pour $NAME (S/N : $SN)"
else
    logger -t GLPI-INVENTORY-SNMP "ÉCHEC de l'inventaire pour $NAME (S/N : $SN). Erreur : $INJECT_OUTPUT"
fi

# --- Nettoyage des fichiers temporaires ---
rm -f "$SNMP_FILE" "$XML_FILE"

# --- Fin du script ---
```

J’active l'agent SNMP sur Stormshield avec la version v2c, en configurant la communauté à « public ».

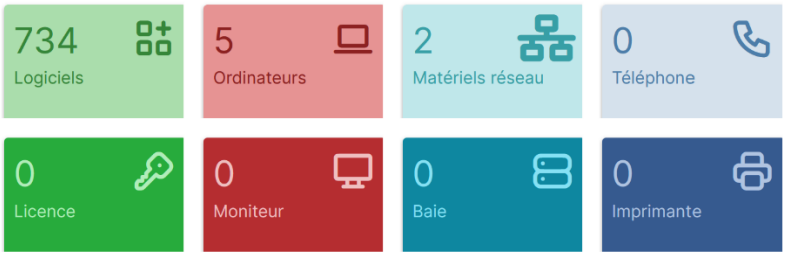


Sur le switch, je crée une access-list qui permet uniquement à l'IP 192.168.20.3 (le serveur GLPI) d'accéder au switch.

Ensuite, j'entre la commande « snmp-server community public RO 10 » pour activer SNMP avec la communauté publique et appliquer l'ACL qui restreint l'accès.

```
Switch(config)#access-list 10 permit 192.168.20.3
Switch(config)#snmp-server community public RO 10
```

On voit à présent les équipements dans GLPI avec toutes leurs informations (IP, MAC ect..)



5.4 - Modèle ticket

Les modèles de tickets peuvent faire gagner un temps précieux aux administrateurs et techniciens du système d'information. En effet, ils standardisent les processus de gestion des incidents, ce qui permet de réduire les erreurs humaines et d'assurer une cohérence dans les réponses.

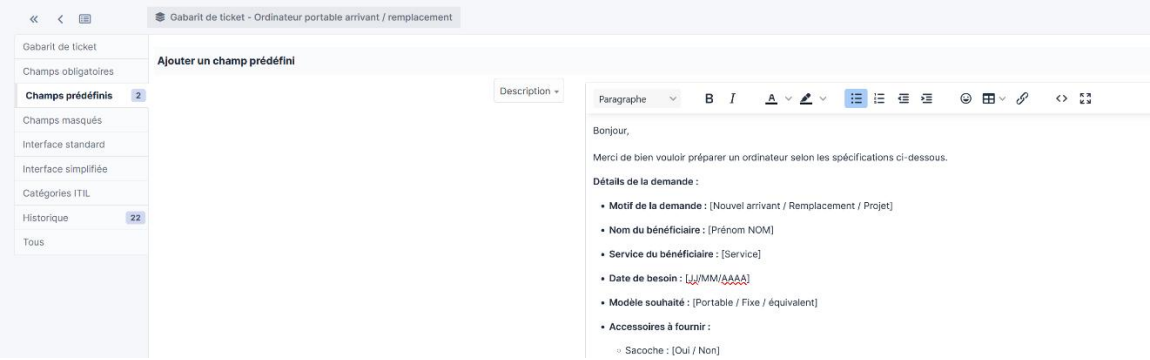
De plus, en pré-remplissant les tickets récurrents, tels que la demande d'un poste informatique, les techniciens peuvent se concentrer davantage sur la résolution des demandes et des incidents, plutôt que sur la collecte des données.

Pour créer des modèles de tickets, je vais dans Assistance > Tickets > Gabarit de tickets.

D'abord, je modifie le modèle « default », qui correspond à ce que l'utilisateur voit de base lorsqu'il crée un nouveau ticket.

Il n'y a que la description qui est obligatoire par défaut, je rajoute donc le titre et la catégorie.

Je fais un gabarit « Demande ordinateur [arrivant / remplacement] et « Demande de déverrouillage de session AD »). Un gabarit est un modèle prédéfini qui sert de base pour compléter un ticket.



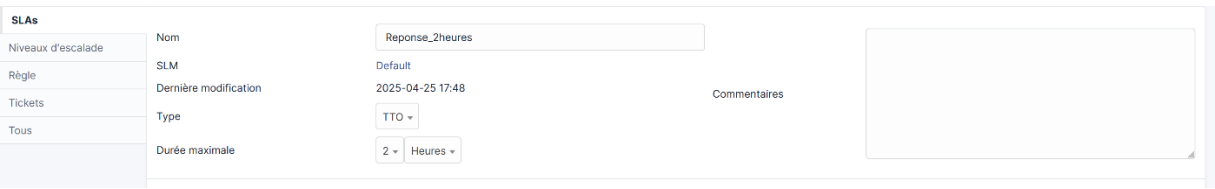
Ensuite, je crée les catégories ITIL dans Configuration > Intitulés > Assistance > Catégorie ITIL. Cela me permet d'attribuer un gabarit de ticket à un utilisateur en fonction de son problème, facilitant ainsi la gestion des incidents et des demandes en fonction de la nature de l'assistance requise.

Je fais les catégories suivantes :

Après configurer les catégorie ITIL je vais créer des SLA (Service-Level Agreement). Un SLA est un accord entre le Système d'information (ou un prestataire de services) et un client (qu'il s'agisse d'un utilisateur interne ou d'un client externe), qui définit les niveaux de service attendus, tels que les délais de réponse, la disponibilité et la qualité du service.

Je vais dans Configuration > Niveaux de services et je créer « Default »

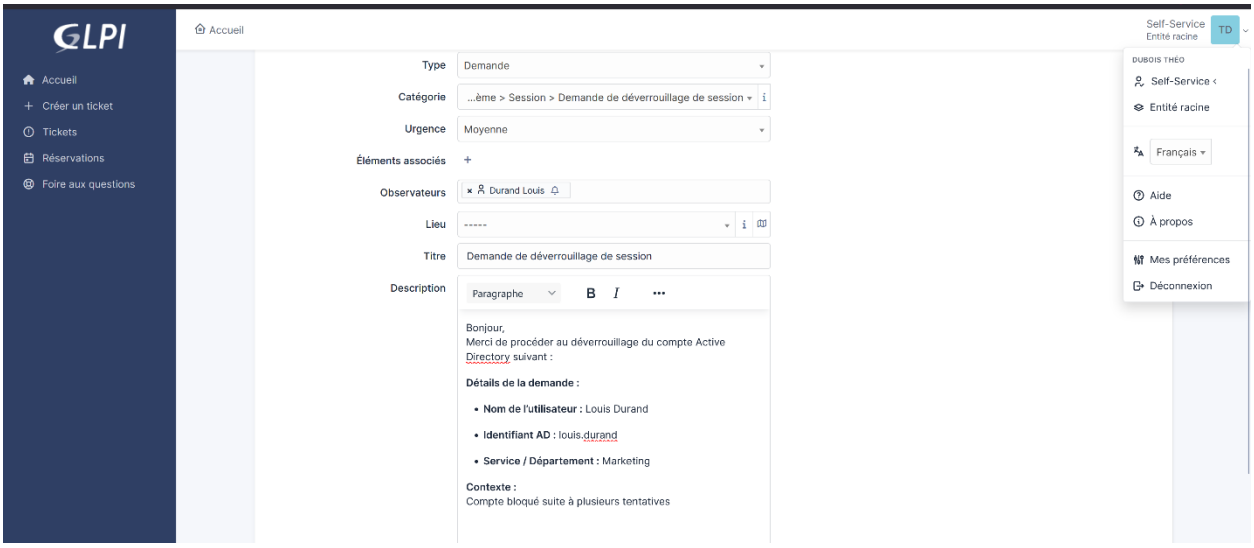
Dans default j'ajoute le SLA « Reponse_2h » en TTO (Time To Own) et je configure la durée maximale à 2h



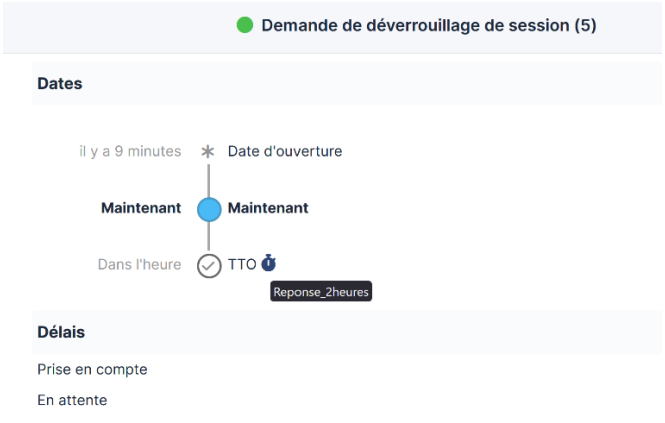
Je configure un deuxième SLA que j'appelle « Reponse_1jour », toujours en TTO. Je définis l'option « Fin d'un jour ouvré » sur « non » afin que la durée soit de 24 heures réelles et non 24 heures ouvrées. Je configure ensuite la durée maximale à 1 jour.

Je définir la SLA TTO du gabarit du ticket « Mise à disposition d'un ordinateur » à « Reponse_1jour » et du gabarit du ticket « Demande de déverrouillage de session » à « Reponse_2heures »

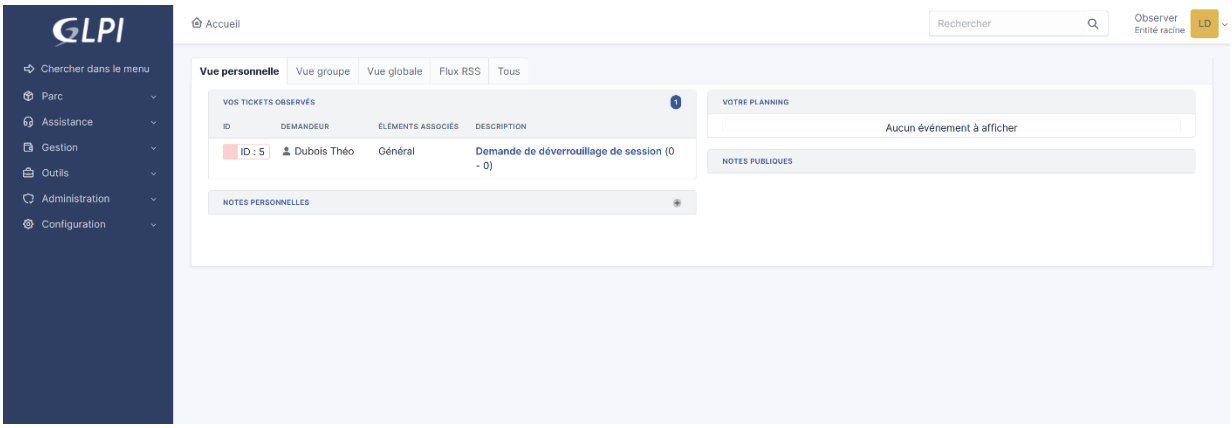
Afin de tester la configuration de GLPI, je me connecte avec un utilisateur du groupe « Cadre » pour créer un ticket destiné à un utilisateur qui n'est pas membre du groupe « Cadre ». Je crée un ticket de demande de déverrouillage de session AD. Le gabarit est correctement appliqué. Je complète et soumets le ticket.



Je me connecte avec un utilisateur travaillant au système d'information. Il a bien accès aux tickets, peut répondre, les modifier, créer et clôturer. Le SLA est visible lorsqu'un utilisateur soumet un ticket avec un SLA, et on voit également lorsqu'un ticket est en retard.



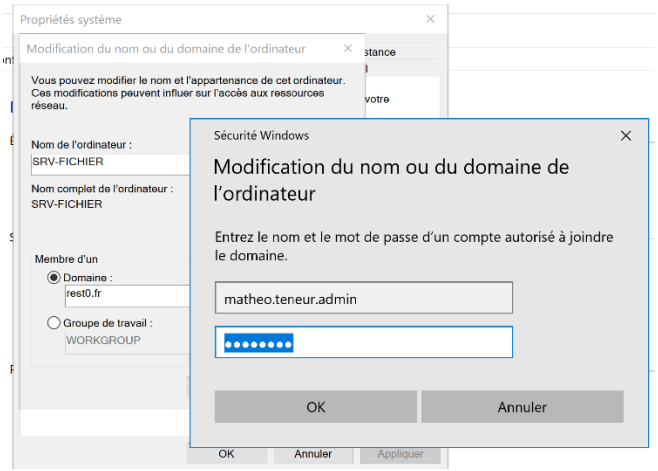
Je me connecte avec l'utilisateur pour lequel le ticket a été créé, ce qui me permet de tester si les utilisateurs « pas cadres » peuvent voir les tickets auxquels ils sont attribués, sans pouvoir créer de ticket.



L'utilisateur peut vsoir les tickets créés pour lui, sans avoir la possibilité de créer de tickets.

6 - Partage de Fichier Windows

Afin de gérer les habilitations des répertoires SMB, je joins le serveur au domaine Active Directory de rest0.fr. En premier lieu, je renomme le serveur Windows en « SRV-FICHIER » afin de mieux l'identifier dans l'Active Directory, puis je l'intègre au domaine sans le promouvoir en contrôleur de domaine, via Paramètres système avancés > Domaine.



Je crée un répertoire nommé « Partage » à la racine du serveur de fichiers, qui accueille tous les répertoires partagés selon l'arborescence définie dans le sujet.

Autorisations appliquées :

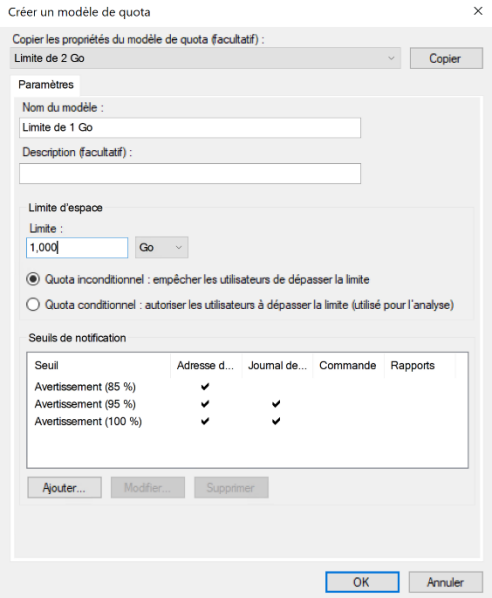
- COMMUN : Les administrateurs ont un contrôle total, les utilisateurs ont un accès en lecture/écriture.

- Répertoires de service : Les administrateurs ont un contrôle total et les groupes correspondant à chaque service disposent d'un accès en lecture/écriture.
- Répertoires personnels : Les administrateurs ont un contrôle total et chaque utilisateur est propriétaire de son répertoire avec un accès en lecture/écriture.
- L'héritage des autorisations est désactivé sur tous les répertoires partagés pour des raisons de sécurité. Cela évite qu'un dossier parent, avec des droits permissifs, transmette ces droits à un sous-dossier sensible.
- Je supprime les autorisations du groupe « CRÉATEUR PROPRIÉTAIRE » sur tous les répertoires partagés. En effet, un utilisateur pourrait autrement modifier les permissions de ses fichiers/dossiers, bloquant l'accès à des personnes légitimes ou le donnant à d'autres indésirables.
- Le compte système (« SYSTEM ») conserve un accès en contrôle total à tous les répertoires, ce qui est nécessaire pour le bon fonctionnement de Windows.
- Le propriétaire des partages est remplacé par le groupe « Admins du domaine », sauf pour les répertoires personnels où chaque utilisateur reste propriétaire de son propre dossier.
- Le répertoire « perso$ » est masqué grâce au symbole « $ », afin qu'il ne soit pas visible par les autres utilisateurs. Chaque utilisateur ne voit que son propre dossier nominatif.
- Seuls les administrateurs du domaine et le système ont accès à perso$, en contrôle total.

Pour définir des quotas, j'installe le rôle Gestionnaire de ressources du serveur de fichiers.

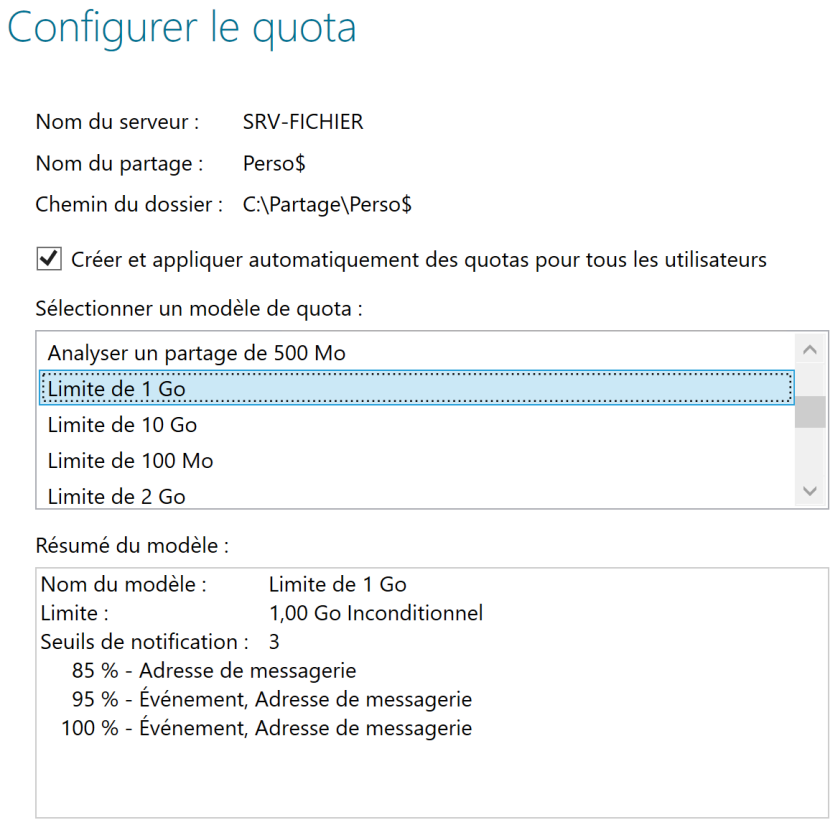
Comme il n'existe pas de modèles de quota de 1 Go ou 500 Mo par défaut, je vais dans Gestionnaire de ressources du serveur de fichiers > Gestion des quotas > Modèles de quotas, puis je crée un nouveau modèle.

Je copie les propriétés du modèle de quota de 10 Go afin de réutiliser la configuration des alertes, puis je modifie le nom du modèle ainsi que la limite de quota selon les besoins.



Les quotas définis dans le sujet sont configurés dans le gestionnaire de serveur dans « Partages » puis clic droit « configurer un quota » ou via « Gestionnaire de ressources du serveur de fichiers » et en définissant des quota manuellement en indiquant le réperoire.

Pour les dossiers perso il est mieux de faire un quota de perso$ et de répliquer aux sous-dossiers pour que tout se fasse automatiquement.



Je mappe les lecteur avec une GPO qui j'appelle « Mappage des lecteurs réseaux »

Dans Configuration utilisateur -> Préférences -> Paramètres Windows -> Mappage de lecteurs

Je mappe pour tous les utilisateurs :

\\SRV-FICHIER\Perso$\%username% -> Personnel (P:) -> Par défaut (utilisateurs du domaine)

\\SRV-FICHIER\Commun -> Commun (Y:) -> Par défaut (utilisateurs du domaine)

Pour les utilisateurs membres du groupe cadres :

\\SRV-FICHIER\Management -> Management (X:) -> Ciblage au niveau de l'élément : Groupe -> Cadres

Pour chaque « équipe » :

\\SRV-FICHIER\[EQUIPE] -> [EQUIPE] (Z:) -> Ciblage au niveau de l'élément : Groupe -> [EQUIPE]

Exemple :

\\SRV-FICHIER\Marketing -> Marketing (Z:) -> Ciblage par groupe : Marketing

Nom	Ordre	Action	Chemin d'accès	Reconnecter
P:	1	Mettre ...	\\SRV-FICHIER\Perso$\%US...	Oui
X:	3	Mettre ...	\\SRV-FICHIER\Management	Oui
Y:	2	Mettre ...	\\SRV-FICHIER\Commun	Oui
Z:	4	Mettre ...	\\SRV-FICHIER\Administratif	Oui
Z:	5	Mettre ...	\\SRV-FICHIER\Marketing	Oui
Z:	6	Mettre ...	\\SRV-FICHIER\Developpe...	Oui
Z:	7	Mettre ...	\\SRV-FICHIER\Systèmes et ...	Oui

Les utilisateurs ont désormais accès aux partages SMB Commun, Perso ainsi que celui de leur(s) service(s) respectif(s).

7 - Nextcloud

7.1 – Installation de Nextcloud

Le serveur Nextcloud est installé sur une machine Debian 12. Étant exposé à Internet, il est placé dans la DMZ.

Je crée un enregistrement DNS de type A pour le nom nextcloud.rest0.fr pointant vers l'adresse IP 192.168.30.1 sur le serveur SRV-AD-DHCP car cela permet aux utilisateurs de se connecter plus facilement au serveur Nextcloud en utilisant un simple.

Je mets à jour les dépôts et les paquets du système à l'aide des commandes *apt update* et *apt upgrade*, puis j'installe les paquets nécessaires au fonctionnement de Nextcloud :

apt install wget unzip apache2 mariadb-server php8.2 php8.2-common php8.2-curl php8.2-gd php8.2-intl php8.2-mbstring php8.2-xmlrpc php8.2-mysql php8.2-xml php8.2-cli php8.2-zip -y

Je lance a2enmod php8.2 pour m'assurer que l'extension PHP 8.2 est bien active dans Apache2.

Je désactive le VirtualHost par défaut avec la commande suivante : a2dissite 000-default.conf

Je génère une paire de clé auto-signé avec OpenSSL

Ensuite, je crée un VirtualHost pour Nextcloud en copiant la configuration fournie dans la documentation officielle, que je place dans le répertoire /etc/apache2/sites-available/.
Le nom de domaine configuré comme alias est nextcloud.rest0.fr.

Attention : il est impératif de nommer le fichier avec l'extension .conf (par exemple nextcloud.rest0.fr.conf), sans quoi Apache ne pourra pas activer le site et générera une erreur (vérifié lors de mes tests).

J'active le VirtualHost avec la commande suivante : *a2ensite nextcloud.rest0.fr.conf*

J'active également tous les modules Apache2 requis et recommandés par la documentation de Nextcloud : *a2enmod rewrite headers env dir mime*

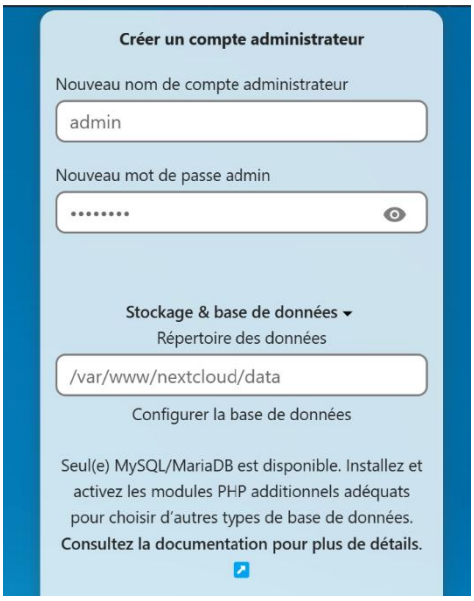
Je redémarre le service apache2, puis je télécharge l'archive contenant les fichiers Nextcloud dans le répertoire /tmp. Ensuite, je décompresse l'archive dans /tmp/nextcloud, et je déplace son contenu dans /var/www/nextcloud avec la commande mv nextcloud/* /var/www/nextcloud/

Je m'assure que le service apache2 ait un accès complet aux fichiers de Nextcloud en exécutant *chown -R www-data:www-data /var/www/nextcloud/*.

Je crée la base de données nextcloud et j'accorde tous les privilèges à l'utilisateur nextcloud_adm sur cette base.

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud_adm'@'localhost' IDENTIFIED BY 'Btssio64';
```

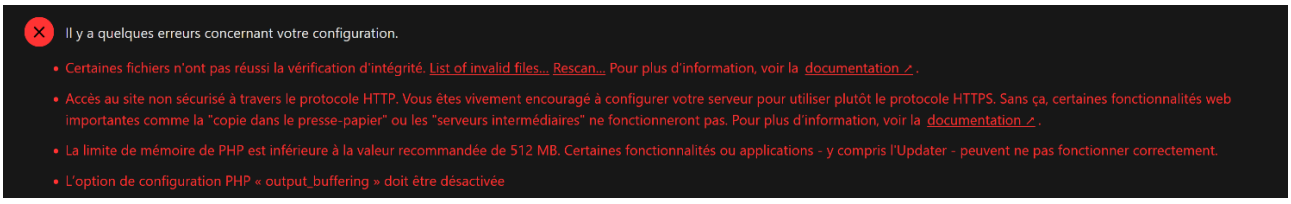
Je me connecte à l'interface d'administration web de Nextcloud via http://nextcloud.rest0.fr, puis je renseigne les informations de connexion à la base de données ainsi que les identifiants pour l'administrateur de base de Nextcloud.

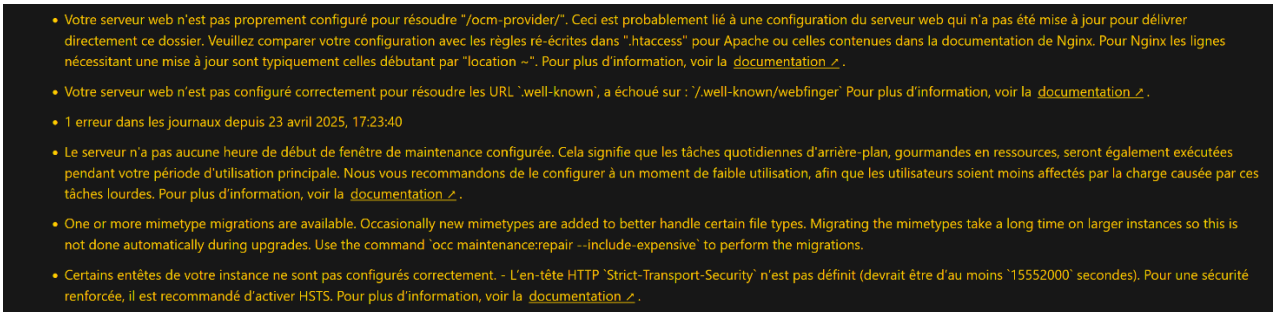


Je crée un nouveau compte d'administration pour Nextcloud, nommé admin, avec le mot de passe Btssio64, le temps de synchroniser Nextcloud à l'Active Directory.

Une fois l'installation terminée, j'ignore les applications recommandées.

Lorsque je vais dans les paramètres de Nextcloud, le serveur signale des problèmes de configuration.





Je modifie les paramètres PHP dans le fichier /etc/php/8.2/apache2/php.ini en suivant les documentations officielles de Nextcloud disponibles aux l'adresse suivante :

https://docs.nextcloud.com/server/latest/admin_manual/installation/php_configuration.html

https://docs.nextcloud.com/server/latest/admin_manual/configuration_files/big_file_upload_configuration.html

Je désactive l'option output_buffering en ajoutant un ; devant output_buffering = 4096 car cette option peut entraîner des erreurs ou des comportements inattendus dans Nextcloud.

Ensuite, je modifie les paramètres suivants :

- upload_max_filesize = 16G
- post_max_size = 16G
- max_input_time = 3600
- max_execution_time = 3600
- memory_limit = 512M

Pour passer le site en https :

Je génère une clé privé RSA avec 4096 bits avec openssl :

openssl genpkey -algorithm RSA -out nextcloud.rest0.fr.key -pkeyopt rsa_keygen_bits:4096

Ensuite, je crée un certificat auto-signé à partir de cette clé privée :

openssl req -new -x509 -key nextcloud.rest0.fr.key -out nextcloud.rest0.fr.cert -days 365 -subj "/CN=nextcloud.rest0.fr"

expliquation de la commande :

- **openssl** : Lance l'outil OpenSSL qui permet de générer des clés, certificats, et gérer des connexions sécurisées.

- **req** : Utilise le module req pour générer une requête de certificat ou un certificat X.509 (ici, un certificat auto-signé).
- **-new** : Crée une nouvelle requête ou un nouveau certificat (dans ce cas, un certificat auto-signé).
- **-x509** : Génère directement un certificat X.509 auto-signé au lieu d'un fichier CSR (Certificate Signing Request).
- **-key nextcloud.rest0.fr.key** : Indique la clé privée à utiliser pour signer le certificat. La clé privée correspond à la clé publique qui sera incluse dans le certificat.
- **-out nextcloud.rest0.fr.cert** : Spécifie le fichier de sortie du certificat généré, ici nommé nextcloud.rest0.fr.cert.
- **-days 365** : Définit la durée de validité du certificat. Ici, le certificat sera valide pendant 365 jours (1 an).
- **-subj "/CN=nextcloud.rest0.fr"** : Définit le sujet du certificat, ici spécifiant que le Common Name (CN) du certificat est nextcloud.rest0.fr (ton domaine ou nom de serveur).

Je déplace la clé privée dans le répertoire /etc/ssl/private/ et le certificat dans /etc/ssl/certs

Ensuite, j'active le module ssl d'Apache2 en utilisant la commande a2enmod ssl

Enfin, je décommente la ligne opcache.interned_strings_buffer=8 et je la définit à 16 dans le fichier php.ini pour améliorer les performances du serveur Nextcloud.

Après avoir résolu les erreurs liées à l'intégrité des fichiers, j'ai identifié que celles-ci étaient causées par trois fichiers manquants : .htaccess, .user.ini, et dep5. Pour résoudre ce problème, j'ai re-téléchargé l'archive de Nextcloud et, cette fois, je l'ai copiée dans le répertoire web en utilisant l'option -f pour m'assurer que tous les fichiers nécessaires étaient correctement transférés. Cela a permis de corriger l'intégrité des fichiers, et le système fonctionne désormais correctement.

Je modifie le VirtualHost pour activer le HTTPS puis j'ajoute la configuration suivante dans le virtualhost de Nextcloud pour activer le HSTS, ce qui oblige les navigateurs à utiliser uniquement HTTPS pour se connecter au serveur :

```
<IfModule mod_headers.c>
  Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
</IfModule>
```

J'ajoute également la configuration suivante au début du virtualhost pour rediriger toutes les URLs HTTP vers HTTPS. Cela permet non seulement de sécuriser l'accès, mais aussi d'éviter les erreurs 404 Not Found si un utilisateur saisit une URL avec http au lieu de https :

```
<VirtualHost *:80>
    ServerName nextcloud.rest0.fr
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
</VirtualHost>
```

J'obtiens donc ce VirtualHost :

```
<VirtualHost *:80>
    ServerName nextcloud.rest0.fr
    RewriteEngine On
    RewriteCond %{HTTPS} off
    RewriteRule ^ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
</VirtualHost>

<VirtualHost *:443>
    DocumentRoot /var/www/nextcloud/
    ServerName  nextcloud.rest0.fr

    SSLEngine on
    SSLCertificateFile      /etc/ssl/certs/nextcloud.rest0.fr.cert
    SSLCertificateKeyFile   /etc/ssl/private/nextcloud.rest0.fr.key

    <Directory /var/www/nextcloud/>
      Require all granted
      AllowOverride All
      Options FollowSymLinks MultiViews

      <IfModule mod_dav.c>
        Dav off
      </IfModule>

      <IfModule mod_headers.c>
        Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"
      </IfModule>
    </Directory>
</VirtualHost>
```

Dans le répertoire Nextcloud, je rends le fichier occ exécutable avec la commande suivante :

chmod +x occ

Ensuite, je lance la commande *occ maintenance:repair --include-expensive* pour réparer le système, comme demandé dans le message d'erreur. Cette commande exécute une série de vérifications et de réparations sur l'installation de Nextcloud.

```
One or more mimetype migrations are available. Occasionally new mimetypes are added to better handle certain file types. Migrating the mimetypes take a long time on larger instances so this is not done automatically during upgrades. Use the command `occ maintenance:repair --include-expensive` to perform the migrations.
```

J’ajoute la ligne suivante dans le fichier nextcloud/config/config.php :
'maintenance_window_start' => 1

Cette ligne configure l'heure de début de maintenance pour Nextcloud.

Je modifie la crontab de l'utilisateur www-data (l'utilisateur sous lequel Apache2 fonctionne) en exécutant la commande *crontab -u www-data -e*.

Puis j’ajoute la ligne */5 * * * * php -f /var/www/nextcloud/cron.php.

Cela permet de planifier l'exécution du script cron.php de Nextcloud toutes les 5 minutes, comme indiqué dans la documentation de Nextcloud, pour que les tâches planifiées, comme les notifications ou la synchronisation des fichiers, soient correctement exécutées à intervalle régulier.

7.2 – Comptes & Privilèges (pour la connexion à Nextcloud)

J’installe le module php-ldap pour permettre l'intégration avec LDAP via la commande *apt install php-ldap*

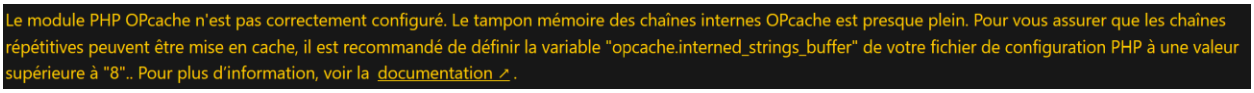
Ensuite, j’active le module ldap d'Apache avec la commande suivante *a2enmod ldap*

Efin, je redémarre Apache2 pour appliquer les modifications *systemctl restart apache2*

Pour synchroniser Nextcloud avec l'Active Directory (AD), je me réfère à cette documentation : https://rdr-it.com/nextcloud-configurer-la-liaison-ldap-active-directory/

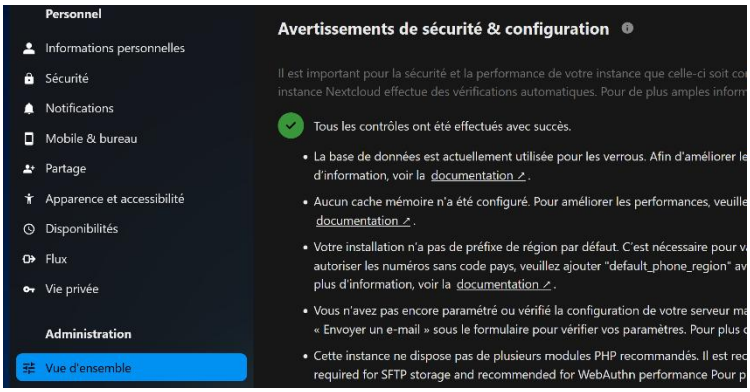
Dans l'interface de Nextcloud, je vais dans Applications -> Packs d’applications, puis je télécharge et active le pack "LDAP user and group backend".

Ensuite, je modifie la configuration de PHP en ajustant la directive opcache.interned_strings_buffer à 64 (64Mo de cache) dans le fichier php.ini car j’ai ce message d’erreur. Etan

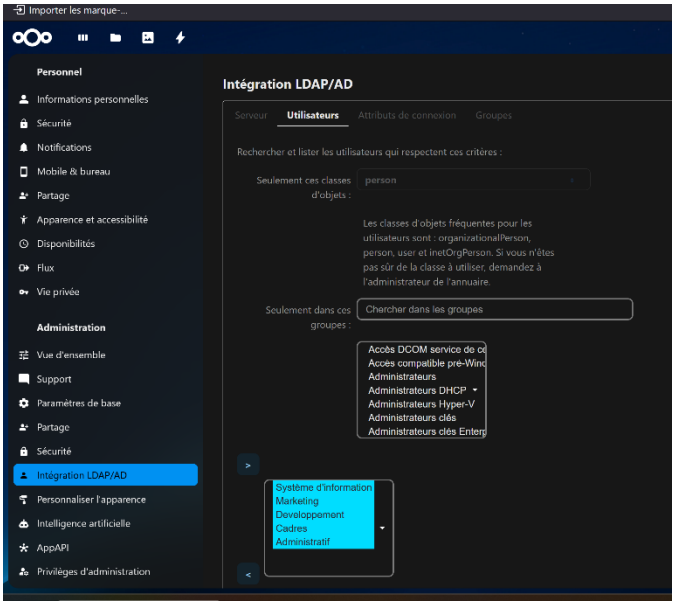


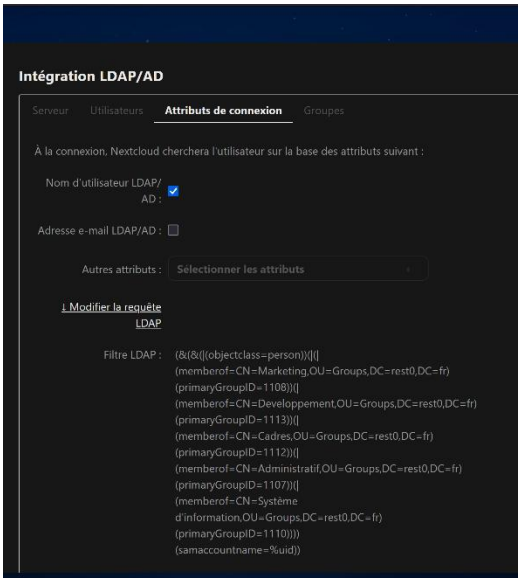
Je crée un compte de service Nextcloud dans l'Active Directory (AD) pour permettre à Nextcloud d'interagir avec l'AD, notamment pour l'authentification et la gestion des utilisateurs.

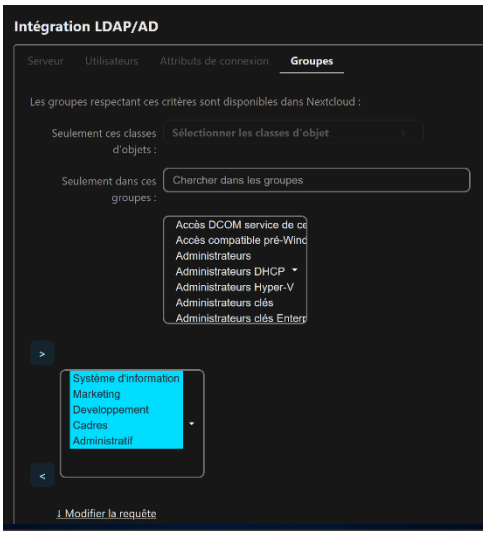
Je vérifie la configuration et constate que tout est bon.



Je renseigne toutes les informations nécessaires dans la section "Intégration LDAP/AD" des paramètres d'administration de Nextcloud. Cela inclut les éléments suivants :







Le groupe permettant d'administrer Nextcloud s'appelle "admin". Il est créé par défaut lors de l'installation de Nextcloud. Cependant, il n'est pas possible d'automatiser l'ajout des membres d'un groupe Active Directory directement au groupe "admin" de Nextcloud via l'intégration LDAP/AD.

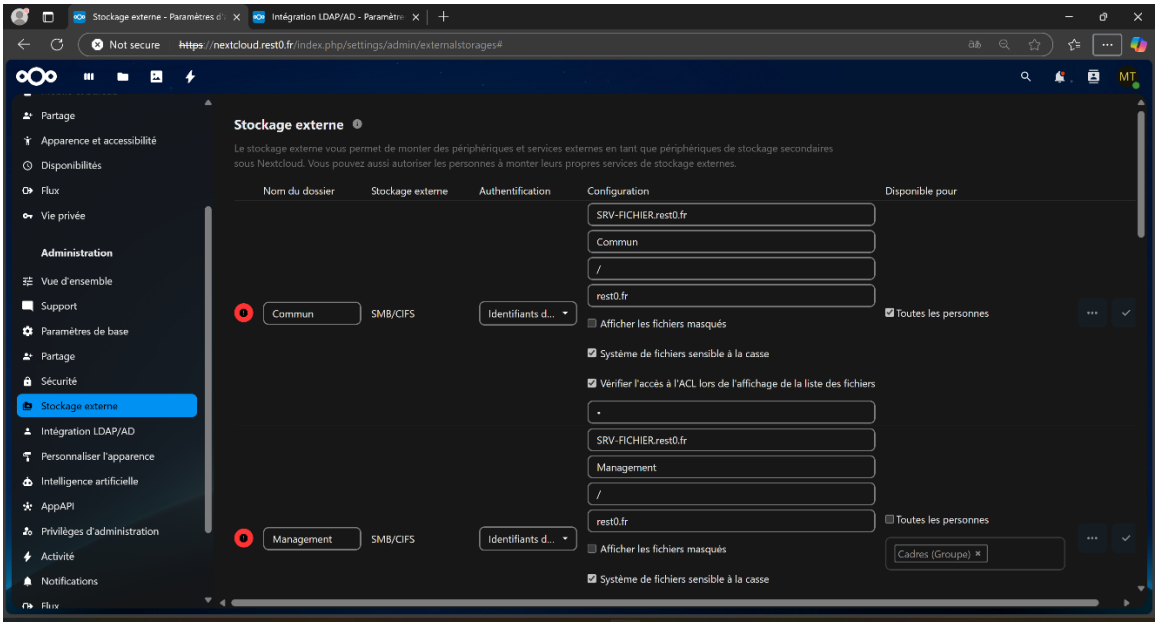
Il est donc nécessaire d'ajouter manuellement les utilisateurs du groupe AD admin ou d'autres groupes AD qui doivent avoir des privilèges d'administration sur Nextcloud, en les inscrivant directement dans le groupe "admin" de Nextcloud après la synchronisation des utilisateurs.

7.3 – Liaison Nextcloud avec le partage de fichier Windows

J'installe le paquet smbclient sur le serveur Debian (et non sur Nextcloud) pour permettre l'accès aux partages SMB/CIFS. Je fais cela avec la commande *apt install smbclient*

Ensuite, je me rends dans Applications, puis je télécharge et active le pack "External storage support" dans Nextcloud. Ce pack permet d'ajouter la prise en charge de différents systèmes de stockage externe, y compris les partages SMB/CIFS, et d'intégrer ces partages dans l'interface Nextcloud.

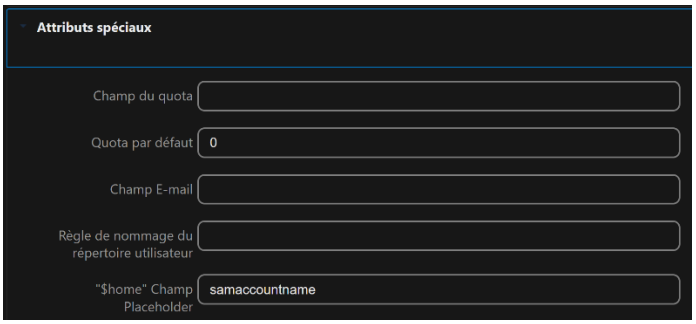
Dans Paramètres d'administration -> Stockage externe, j'ajoute les dossiers Management, Commun, Administratif, Marketing, Développement et Systèmes et Réseaux en configurant chacun d'eux pour qu'il pointe vers le partage SMB/CIFS approprié.

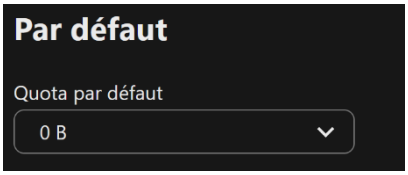


Pour les dossiers personnels des utilisateurs, je me rends dans Paramètres d'administration -> Intégration LDAP/AD -> Serveur : 192.68.20.1 -> Avancé -> Attributs spéciaux et je définis "$home" Champ Placeholder à "samaccountname".

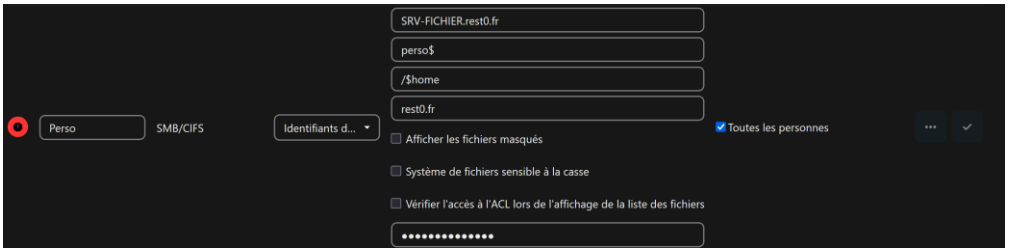
Ainsi, la variable $home des utilisateurs est égale à leur samaccountname, qui correspond également aux noms de leurs répertoires personnels dans Nextcloud. Cela permet d'associer chaque utilisateur à son répertoire personnel de manière dynamique.

J'en profite pour mettre le quota par défaut à 0 B (ainsi que dans Comptes -> Paramètres gestion des comptes -> Quotas par défaut : 0 B) afin que les utilisateurs ne puisse pas mettre de donnée sur le serveur nextcloud mais uniquement sur les partages SMB.





Ensuite, j'ajoute le partage des répertoires personnels à Nextcloud en utilisant la variable $home comme sous-dossier. Cette variable correspond au samaccountname des utilisateurs, ce qui fait que chaque utilisateur accède à son répertoire personnel nommé en fonction de son samaccountname.



J'ai utilisé « Identifiants de connexion, sauvegardés pour la session » comme méthode d'authentification pour les partages SMB. Cela permet d'utiliser les mêmes identifiants de connexion que ceux de Nextcloud pour accéder aux partages SMB. Ainsi, les utilisateurs se connectent automatiquement aux partages SMB en utilisant leurs identifiants Nextcloud (qui sont ceux d'Active Directory et donc également pour les partages SMB).

Cependant, en raison d'un bug connu de Nextcloud, un mot de passe est demandé lors de la configuration des partages SMB.

Voir : https://github.com/nextcloud/server/issues/52227

J'indique un mot de passe qui est sans importance pour contourner cette demande, même cela entraîne un échec de la connexion cela n'affecte toutefois en rien le bon fonctionnement du partage SMB.

En effet, malgré le message d'échec dans la configuration, le partage fonctionne correctement et les utilisateurs peuvent y accéder sans problème.

J'ai supprimé les fichiers et dossiers du répertoire nextcloud/core/skeleton/, car le contenu de ce dossier se clone automatiquement dans le répertoire des nouveaux utilisateurs (comme Photos, Documents, etc.).

Étant donné que Nextcloud est uniquement destiné à faire un lien vers les partages SMB, je ne souhaite aucune donnée locale dans Nextcloud.

7.4 – Accès à Nextcloud depuis Internet

Étant donné que la règle de NAT permettant l'accès au serveur Nextcloud a été configurée en amont lors de la configuration du routeur Stormshield

Il ne reste plus qu'à modifier le fichier nextcloud/config/config.php, et plus particulièrement la section trusted_domains, qui définit les adresses autorisées pour accéder à Nextcloud.

```
'trusted_domains' =>
array (
  0 => "nextcloud.rest0.fr",
),
```

Je redémarre le service Apache avec *systemctl restart apache2*.Je peux accéder à l'interface Web de Nextcloud dorénavant. les utilisateurs peuvent visualiser, télécharger et modifier les documents de leurs partages SMB directement depuis un poste distant.

Après installation de l'application Nextcloud sur iOS et Windows, la configuration s'effectue de la même manière : l'application demande l'authentification, elle ouvre la page Web de Nextcloud pour la connexion, puis revient automatiquement à l'application une fois la connexion validée. Les clients mobile et desktop proposent les mêmes fonctionnalités que l'interface Web bien que plus optimisés pour chaque plateforme.

Tous les clients se synchronisent avec le partage SMB du répertoire personnel de l'utilisateur.