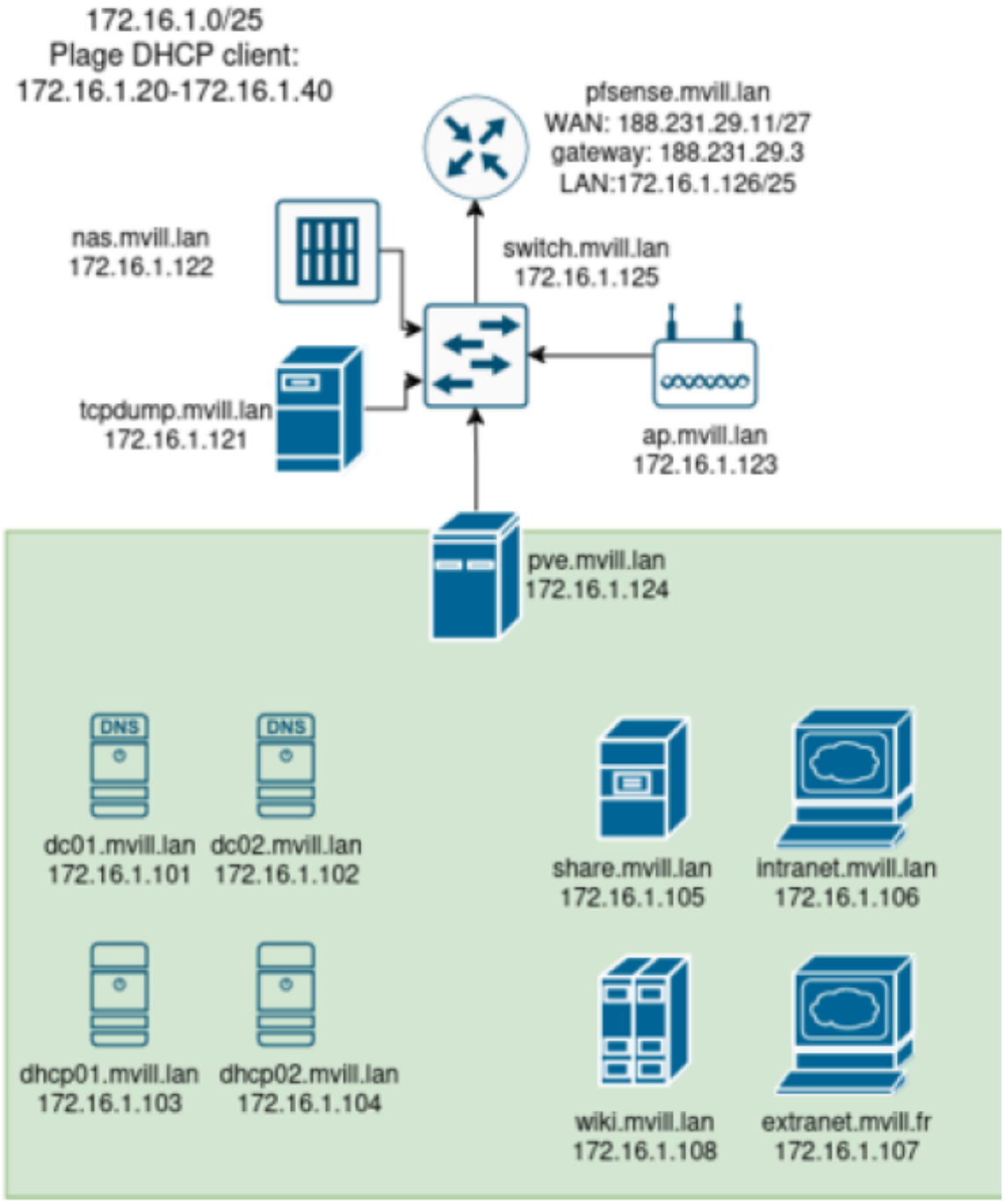
MVILL CORP

MVILL CORP

Présentation
Bienvenue chez La MillCorp, une entreprise innovante à la pointe de l'intelligence artificielle.
Fondée en 2022, notre mission est de transformer les idées audacieuses en solutions
intelligentes pour un avenir durable et connecté.
Notre vision :
Chez MillCorp, nous croyons que l'intelligence artificielle peut être un catalyseur de
changement positif. Nous aspirons à rendre la technologie accessible à tous, en facilitant la
prise de décisions éclairées et en optimisant les processus pour les entreprises de toutes
tailles.
Nos réalisations :
Nous avons déjà collaboré avec des entreprises leaders dans divers secteurs, notamment la
santé, la finance et le retail, en leur fournissant des solutions qui ont transformé leur manière
de travailler.

Infrastructure :



TO DO LIST

- Pas de segmentation de réseau : réseau à plat,;ou bien segmentation simple (c'est du SysAdmin pas du NetAdmin)
- 1 PFSense
- 1 Switch SOHO manageable avec possibilité de port mirroring
- Un réseau Classe B/25
- Un "gros" serveur pour faire de l'ESX ou du Proxmox

● Des Tours physiques si besoin
● 1 NAS
● Des VM locales sur vos machines avec VMWare Workstation ou VirtualBox
● Une AP

Rôles systèmes à installer
● DC1+DNS sous winserver
● DC2+DNS sous winserver
● Serveur DHCP sous Winserver
● Serveur DHCP de basculement sous Winserver
● File Serveur sous Win server
● Backup sur NAS
● 1 serveur LAMPS site frontal en mode nat avec redirection
● 1 serveur IIS en intranet/"sharepoint" light seulement pour les users du domaine
● 1 Wiki d'entreprise locale pour la doc
● 1 Machine qui va recueillir les données http passées en formulaire clair (type dcpdump avec filtre >>rapport.txt ou mieux) en port mirroring avec analyse à posteriori
et des clients VMs WIn 10/11
Formalisme
● 1000 users importés en powershell
● 5 gpo utiles
● Une continuité de nommage nbt, dns
● toutes les ressources sont assignables en FQDN
● intégrer les serveurs linux dans le domaine
● tous les accès sont sécurisés HTTPS et/ou SSH...
● vous devez tendre à un centralisme avec une CA Interne sous Windows Server /
PFsense
● vous devez instaurer au maximum une stratégie de mot de passe forte et centralisée
● Une sécurité renforcée de manière transversale

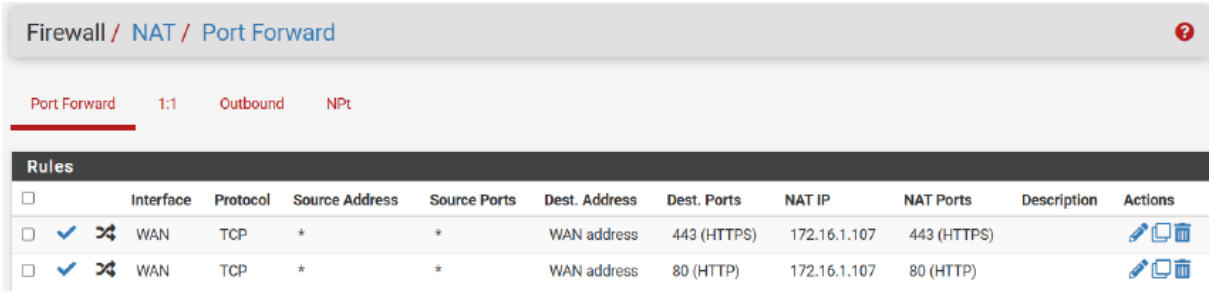
1. Installer Apache
sudo apt install apache2 -y
systemctl enable apache2

```
root@SRV-LAMP:/home/ais# systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enab
     Active: active (running) since Fri 2024-10-25 14:18:01 CEST; 2h 41min ago
       Docs: https://httpd.apache.org/docs/2.4/
```

2. Fichier Configuration

```
 GNU nano 7.2     /etc/apache2/sites-available/doc.mvill.lan.conf
<VirtualHost *:80>

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

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

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

</VirtualHost>
```

3.NAT



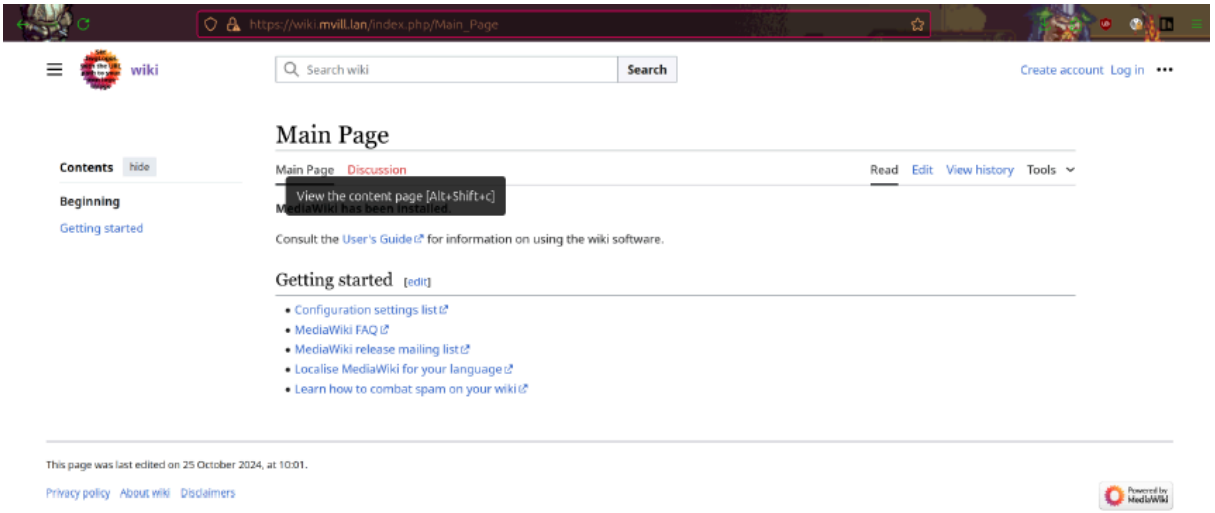
4. Redirection HTTPS

```
<VirtualHost *:80>
        RedirectPermanent / https://doc.mvill.fr/
</VirtualHost>
<IfModule mod_ssl.c>
SSLStaplingCache shmcb:/var/run/apache2/stapling_cache(128000)
<VirtualHost *:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

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

        ServerName doc.mvill.fr
        SSLCertificateFile /etc/letsencrypt/live/doc.mvill.fr/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/doc.mvill.fr/privkey.pem
        Include /etc/letsencrypt/options-ssl-apache.conf
        Header always set Strict-Transport-Security "max-age=31536000"
        SSLUseStapling on
        Header always set Content-Security-Policy upgrade-insecure-requests
</VirtualHost>
</IfModule>
```

Configuration Vhost pour le wiki

```
tech@wiki:~$ cat /etc/apache2/sites-available/wiki.mvill.lan.conf
<VirtualHost *:80>
        Redirect Permanent / https://wiki.mvill.lan
</VirtualHost>

<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerName wiki.mvill.lan
                DocumentRoot /var/www/html/wiki

                <Directory /var/www/html/wiki/>
                        Options Indexes FollowSymLinks
                        AllowOverride None
                        Require all granted
                </Directory>

                        ErrorLog ${APACHE_LOG_DIR}/wiki.mvill.lan-error.log
                        CustomLog ${APACHE_LOG_DIR}/wiki.mvill.lan-access.log combined
                SSLEngine on
                SSLCertificateFile      /etc/apache2/apache.pem
        </VirtualHost>
</IfModule>
```

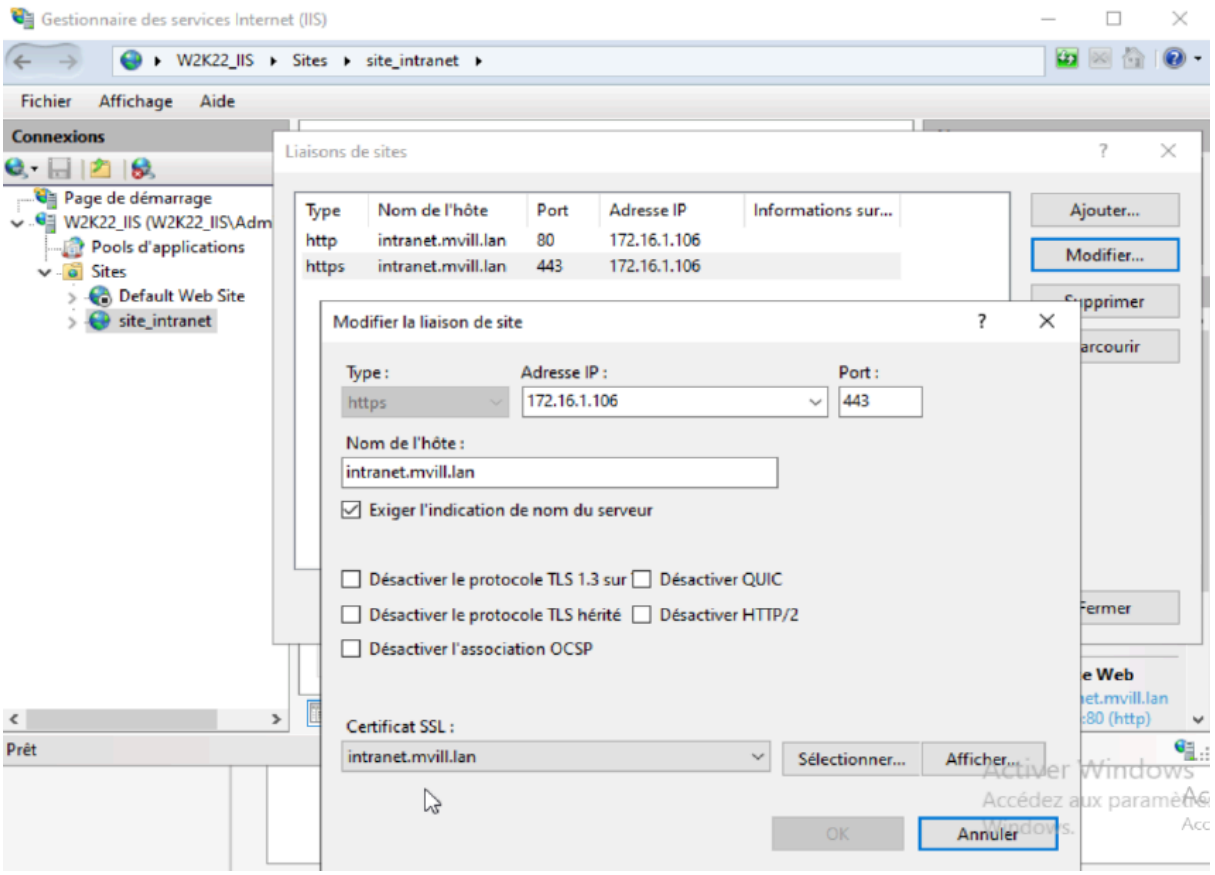
Page d'accueil du wiki:



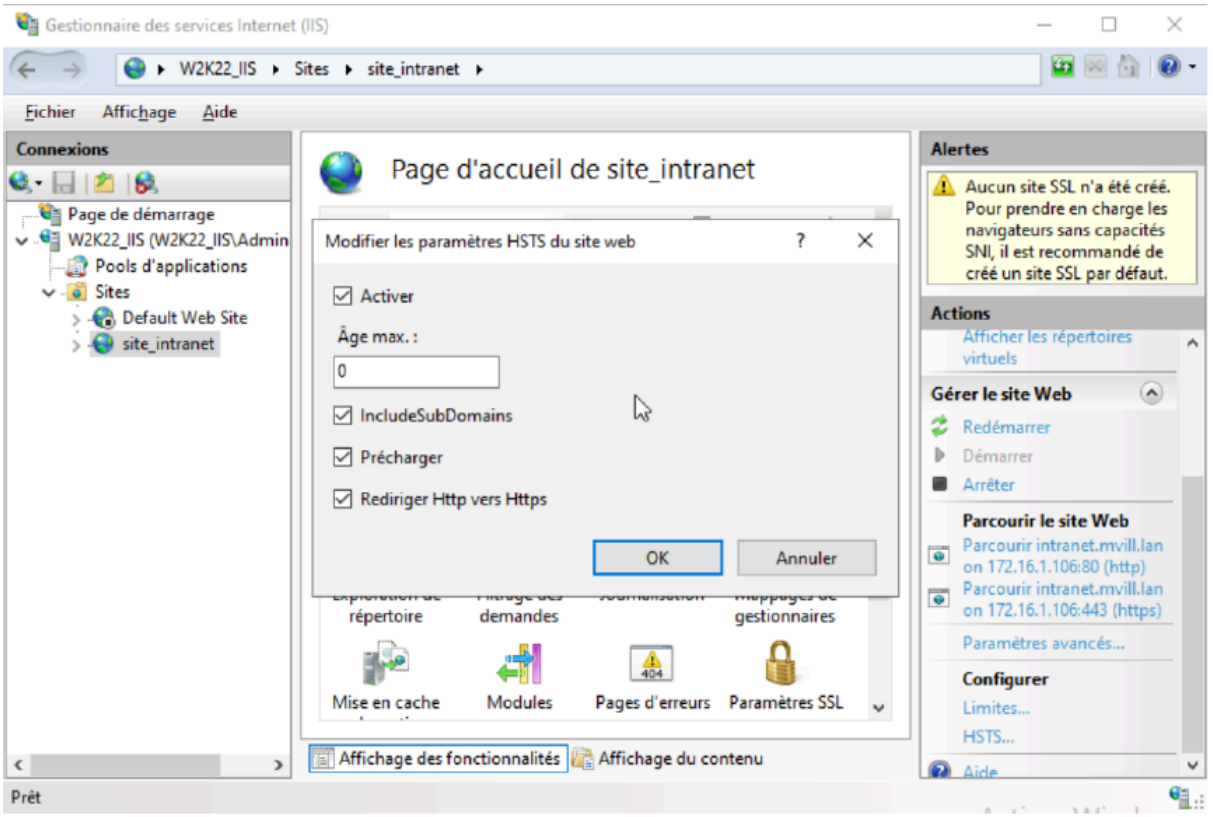
IIS

Page intranet de l'entreprise :

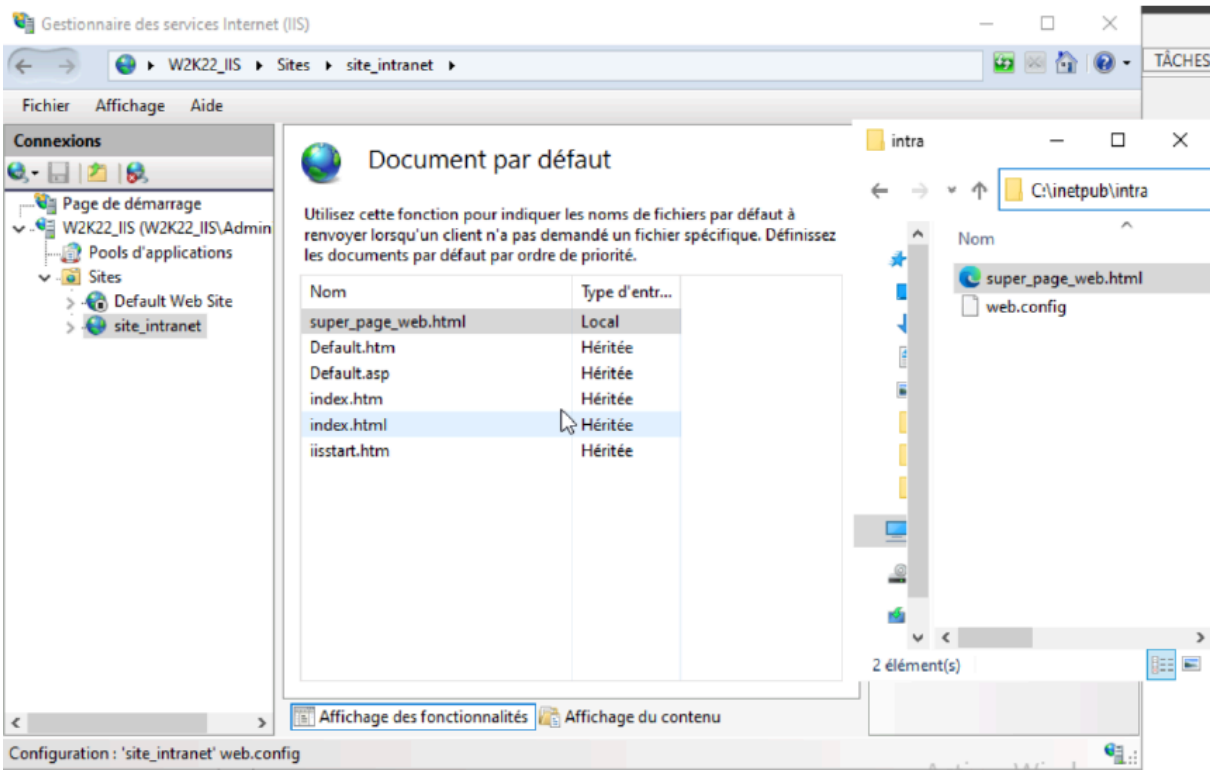
Configuration de la liaison sur IIS :


Gestionnaire des services Internet (IIS)
W2K22_IIS ▸ Sites ▸ site_intranet ▸
Fichier Affichage Aide
Connexions
Page de démarrage
W2K22_IIS (W2K22_IIS\Adm
Pools d'applications
Sites
Default Web Site
site_intranet
Liaisons de sites
Type Nom de l'hôte Port Adresse IP Informations sur...
http intranet.mvill.lan 80 172.16.1.106
https intranet.mvill.lan 443 172.16.1.106
Ajouter...
Modifier...
Supprimer
Parcourir
Fermer
Modifier la liaison de site
Type :
https
Adresse IP :
172.16.1.106
Port :
443
Nom de l'hôte :
intranet.mvill.lan
Exiger l'indication de nom du serveur
Désactiver le protocole TLS 1.3 sur
Désactiver QUIC
Désactiver le protocole TLS hérité
Désactiver HTTP/2
Désactiver l'association OCSP
Certificat SSL :
intranet.mvill.lan
Sélectionner...
Afficher...
OK
Annuler
Prêt

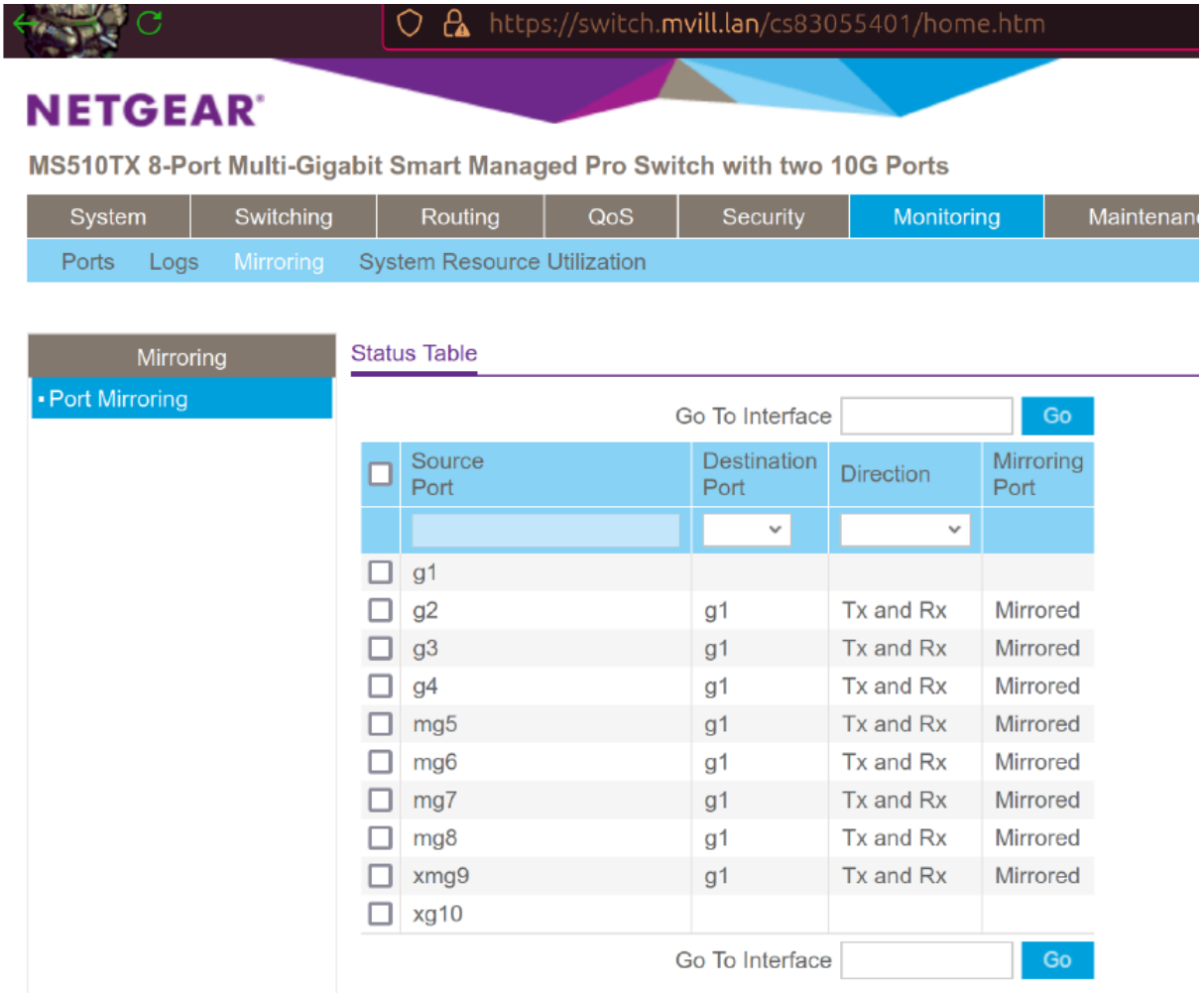
HSTS activé :


Gestionnaire des services Internet (IIS)
W2K22_IIS ▸ Sites ▸ site_intranet ▸
Fichier Affichage Aide
Connexions
Page de démarrage
W2K22_IIS (W2K22_IIS\Admin
Pools d'applications
Sites
Default Web Site
site_intranet
Page d'accueil de site_intranet
Modifier les paramètres HSTS du site web
Activer
Âge max. :
0
IncludeSubDomains
Précharger
Rediriger Http vers Https
OK
Annuler
Mise en cache
Modules
Pages d'erreurs
Paramètres SSL
Affichage des fonctionnalités
Affichage du contenu
Alertes
Aucun site SSL n'a été créé. Pour prendre en charge les navigateurs sans capacités SNI, il est recommandé de créé un site SSL par défaut.
Actions
Afficher les répertoires virtuels
Gérer le site Web
Redémarrer
Démarrer
Arrêter
Parcourir le site Web
Parcourir intranet.mvill.lan on 172.16.1.106:80 (http)
Parcourir intranet.mvill.lan on 172.16.1.106:443 (https)
Paramètres avancés...
Configurer
Limites...
HSTS...
Aide
Prêt

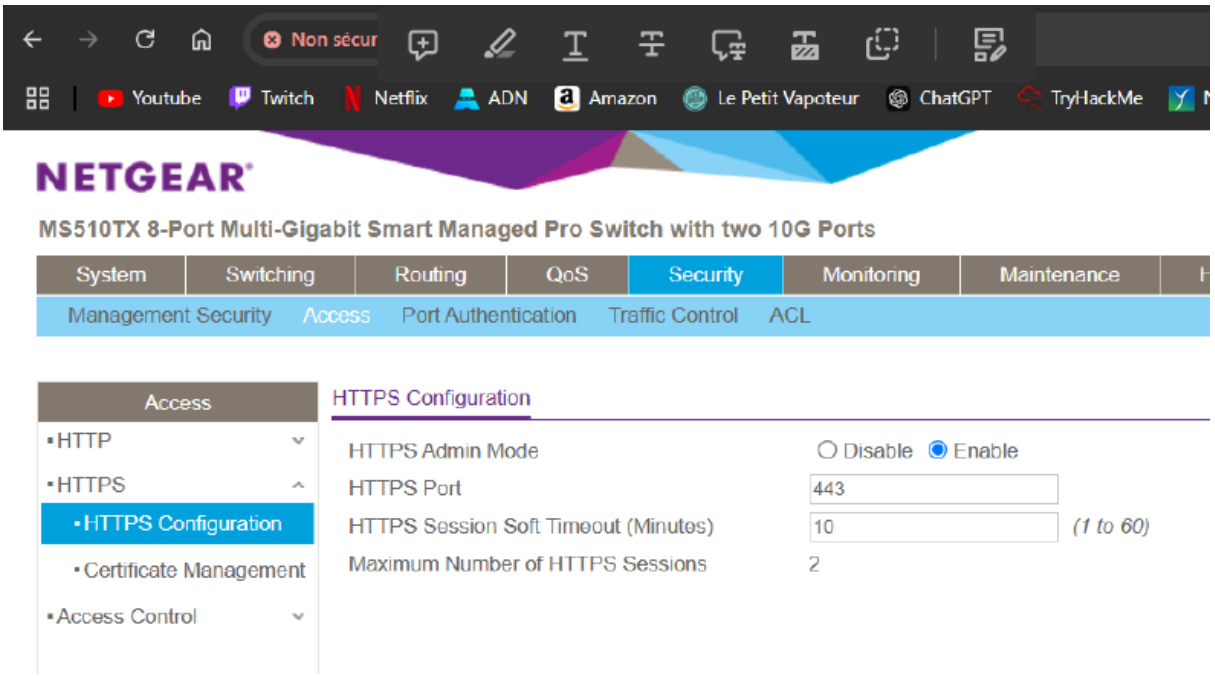
Dossier et fichier html changés :



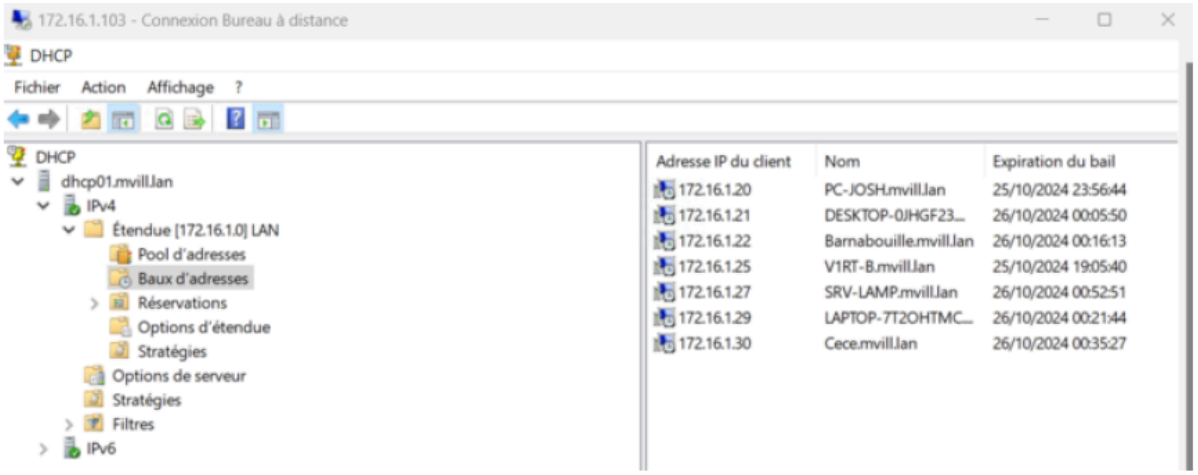
Configuration du port mirroring pour le box de capture:



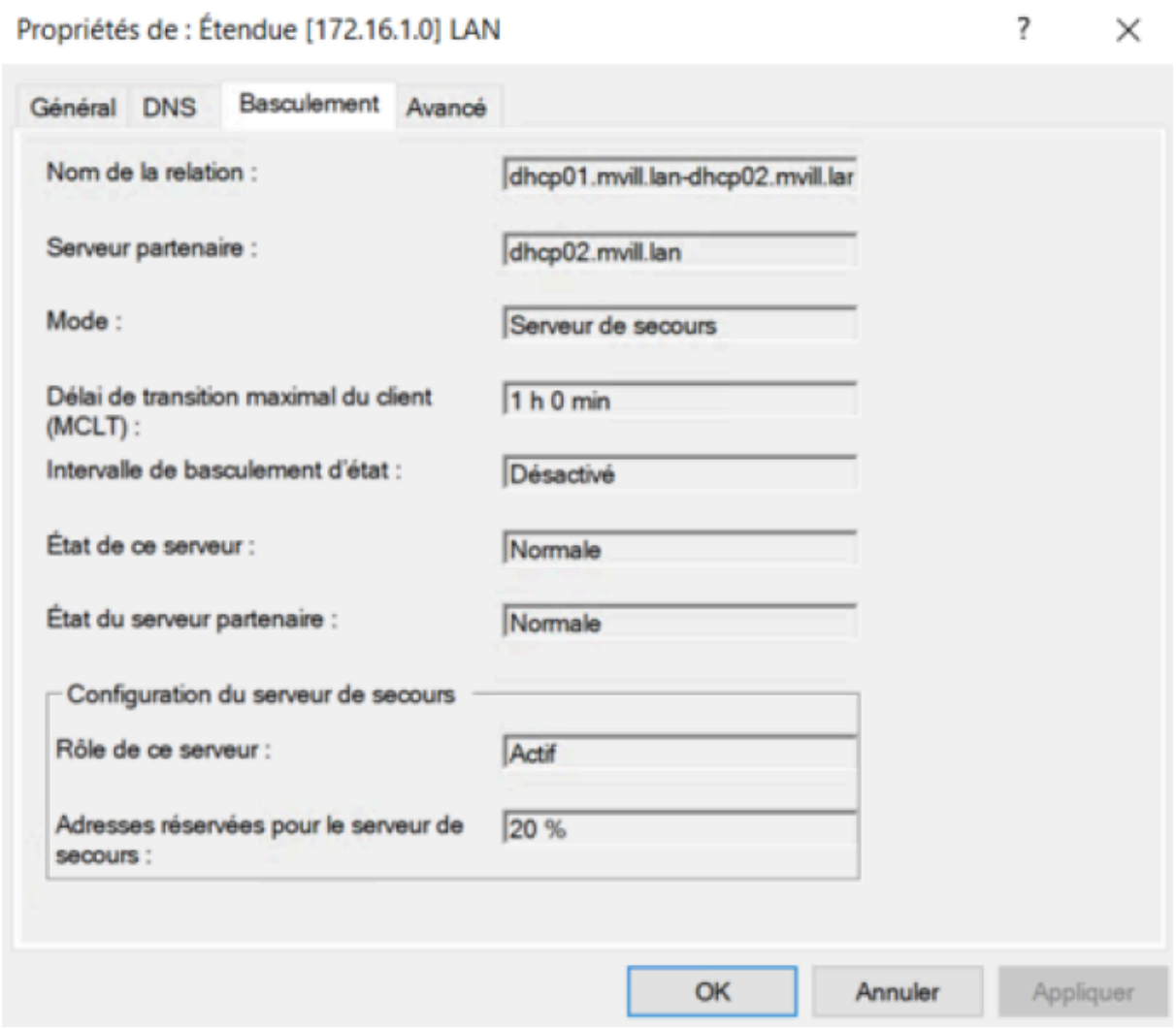
Config du switch en https:



Configuration des étendus DHCP:



Configuration du fail-over DHCP:



Formalisme

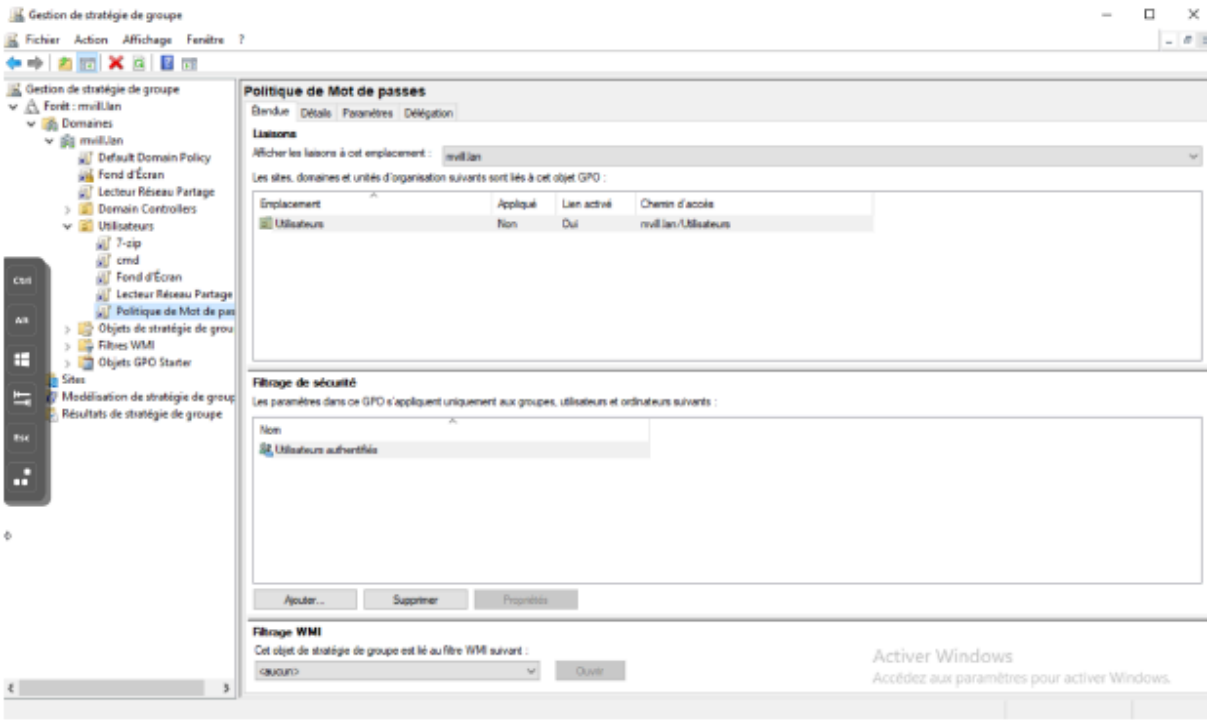
● 1000 users importés en powershell

Voici notre script PowerShell :

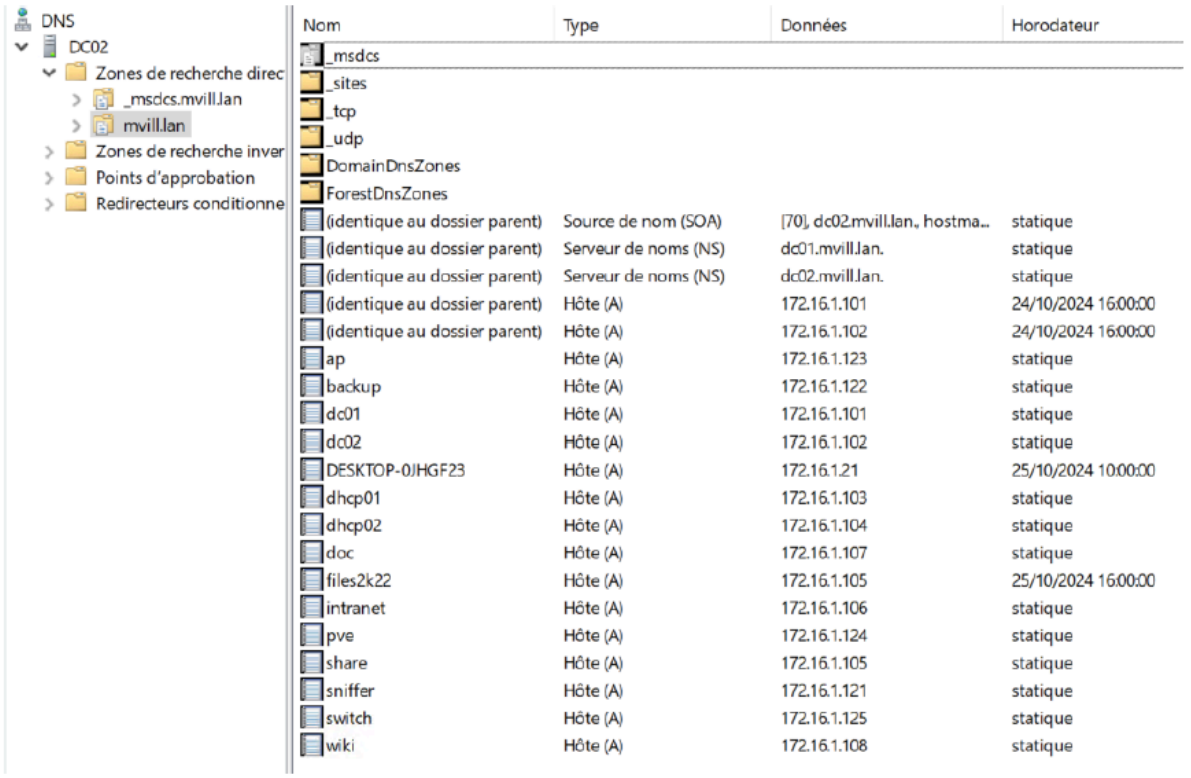
```
$CSVFile = "C:\Scripts\users.csv"
$CSVData = Import-CSV -Path $CSVFile -Delimiter ";" -Encoding UTF8
Foreach($Utilisateur in $CSVData){
$UtilisateurPrenom = $Utilisateur.Prenom
$UtilisateurNom = $Utilisateur.Nom
$UtilisateurLogin = ($UtilisateurPrenom).Substring(0,1) + "." + $UtilisateurNom
$UtilisateurEmail = "$UtilisateurLogin@mvill.lan"
# Vérifier la présence de l'utilisateur dans l'AD
if (Get-ADUser -Filter {SamAccountName -eq $UtilisateurLogin})
{
Write-Warning "L'identifiant $UtilisateurLogin existe déjà dans l'AD"
}
else
{
New-ADUser -Name "$UtilisateurNom $UtilisateurPrenom" `
-DisplayName "$UtilisateurNom $UtilisateurPrenom" `
-GivenName $UtilisateurPrenom `
-Surname $UtilisateurNom `
-SamAccountName $UtilisateurLogin `
-EmailAddress $UtilisateurEmail `
-UserPrincipalName "$UtilisateurLogin@mvill.lan" `
-Path "OU=Utilisateurs,DC=mvill,DC=lan" `
-AccountPassword(ConvertTo-SecureString "a32K@4uasE@*6P" -AsPlainText
-Force) -passThru `
-Enabled $true `
Write-Output "Création de l'utilisateur : $UtilisateurLogin ($UtilisateurNom
$UtilisateurPrenom)"
```

Nous avons utilisé notamment le fichier user.csv qui regroupe les 1000 utilisateurs.

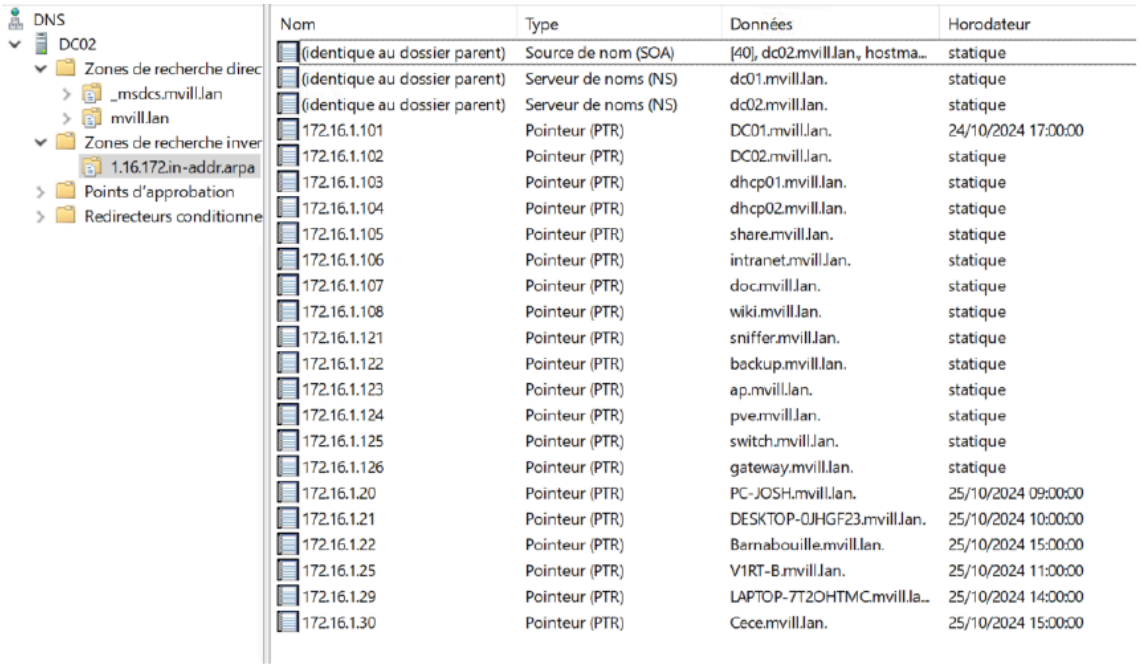
● 5 GPO utiles



Partie DNS :

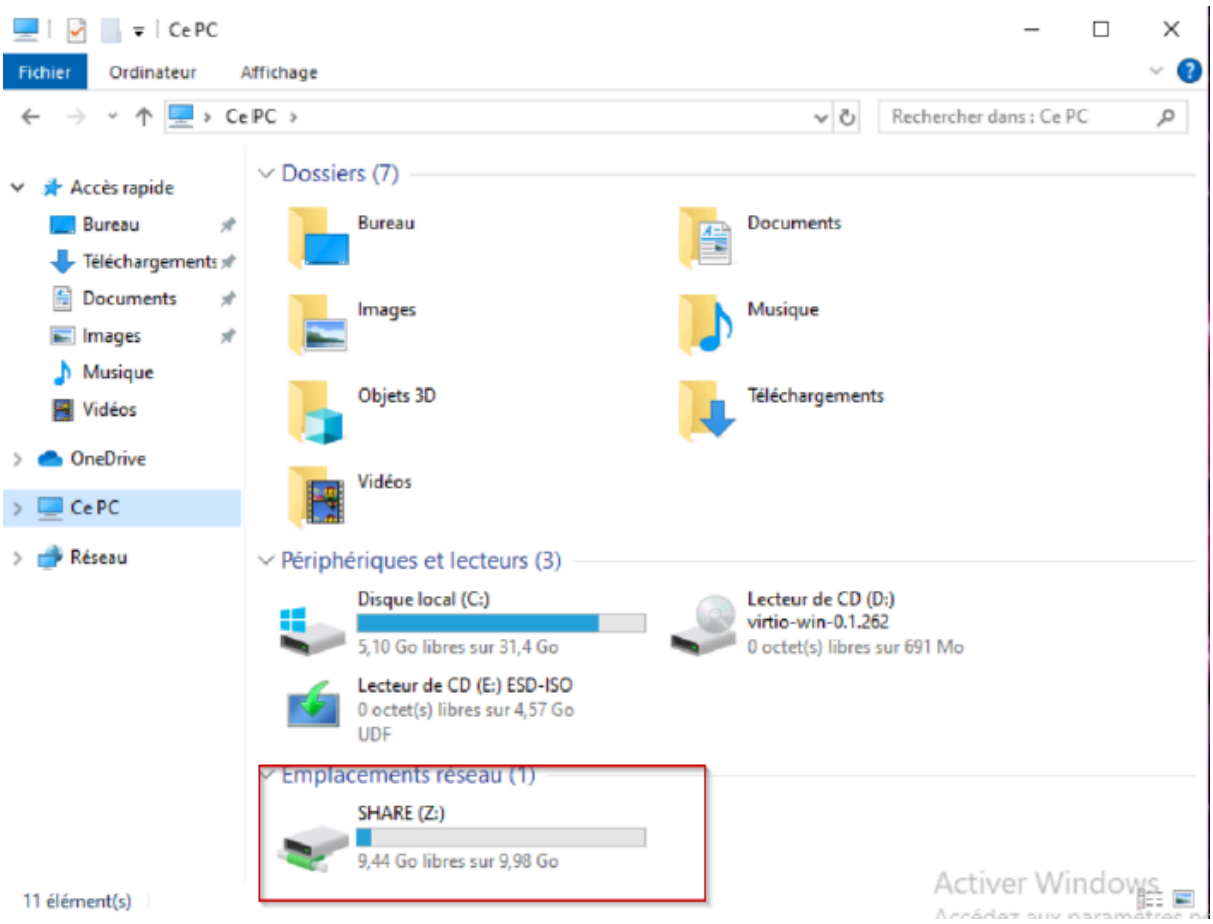


Nom	Type	Données	Horodateur
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(identique au dossier parent)	Source de nom (SOA)	[70], dc02.mvill.lan., hostma...	statique
(identique au dossier parent)	Serveur de noms (NS)	dc01.mvill.lan.	statique
(identique au dossier parent)	Serveur de noms (NS)	dc02.mvill.lan.	statique
(identique au dossier parent)	Hôte (A)	172.16.1.101	24/10/2024 16:00:00
(identique au dossier parent)	Hôte (A)	172.16.1.102	24/10/2024 16:00:00
ap	Hôte (A)	172.16.1.123	statique
backup	Hôte (A)	172.16.1.122	statique
dc01	Hôte (A)	172.16.1.101	statique
dc02	Hôte (A)	172.16.1.102	statique
DESKTOP-0JHGF23	Hôte (A)	172.16.1.21	25/10/2024 10:00:00
dhcp01	Hôte (A)	172.16.1.103	statique
dhcp02	Hôte (A)	172.16.1.104	statique
doc	Hôte (A)	172.16.1.107	statique
files2k22	Hôte (A)	172.16.1.105	25/10/2024 16:00:00
intranet	Hôte (A)	172.16.1.106	statique
pve	Hôte (A)	172.16.1.124	statique
share	Hôte (A)	172.16.1.105	statique
sniffer	Hôte (A)	172.16.1.121	statique
switch	Hôte (A)	172.16.1.125	statique
wiki	Hôte (A)	172.16.1.108	statique

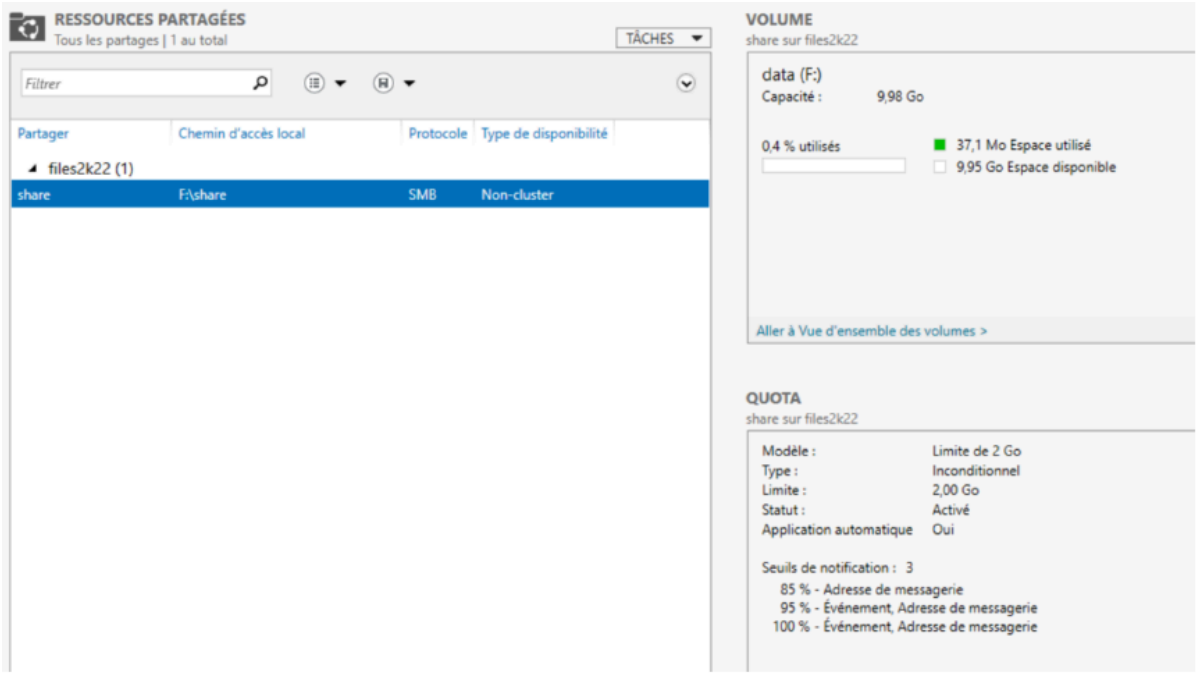


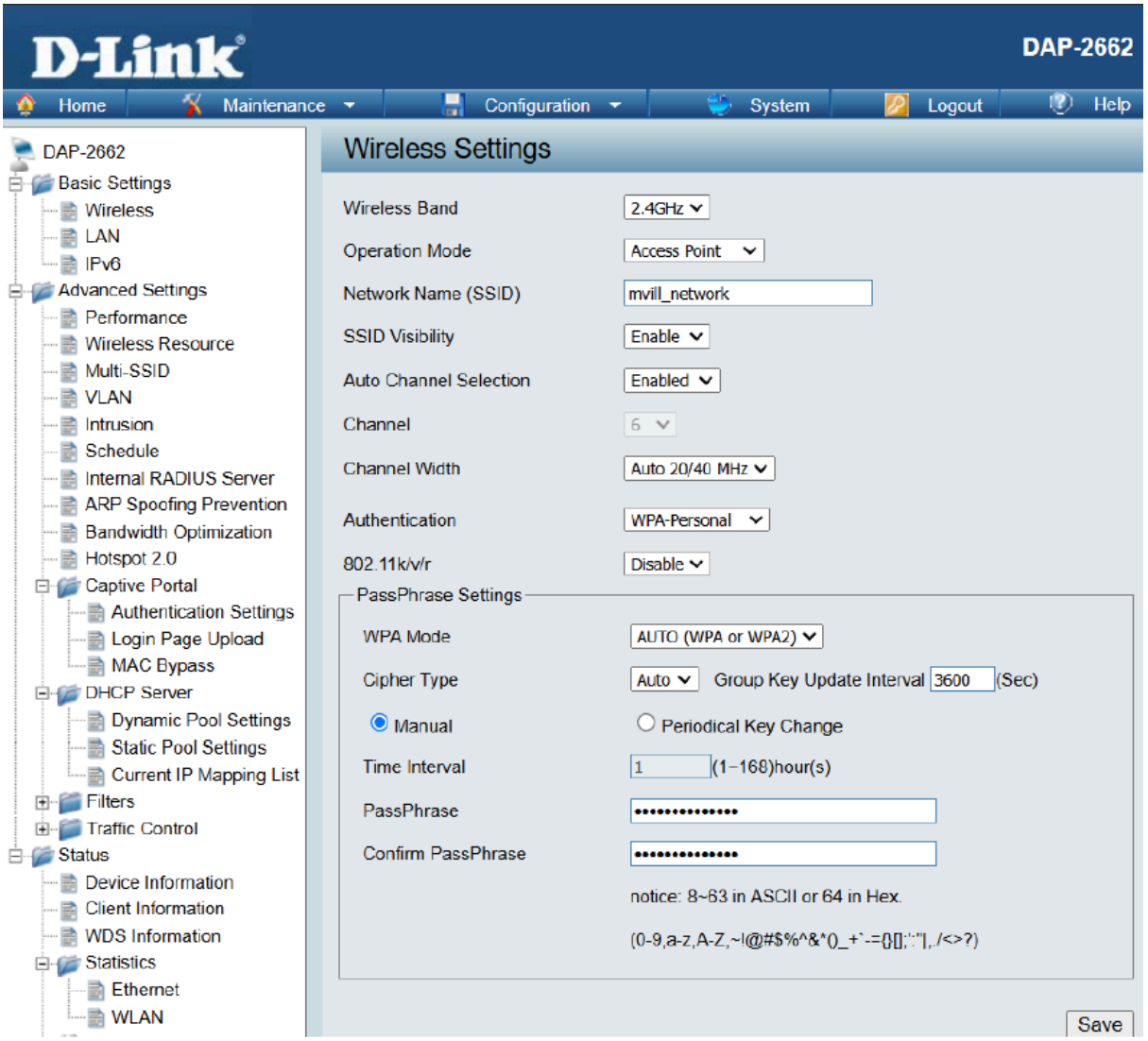
Mise en place d'un fond d'écran avec une installation d'un logiciel automatique 7-Zip
présent sur le bureau :

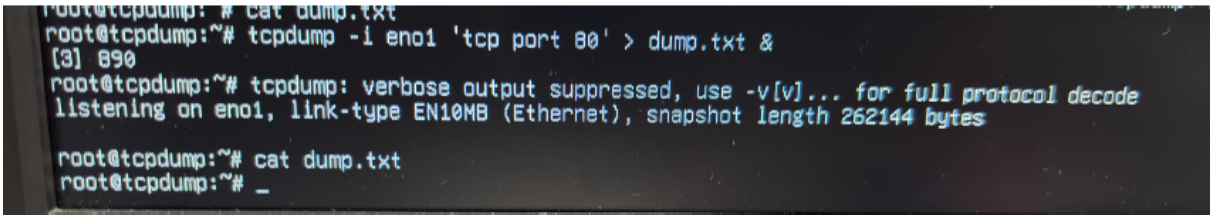
Le lecteur réseau :



Exemple de partage sur windows server avec quotas:


RESSOURCES PARTAGÉES
Tous les partages | 1 au total
TÂCHES
Filtrer
Partager
Chemin d'accès local
Protocole
Type de disponibilité
files2k22 (1)
share
F:\share
SMB
Non-cluster
VOLUME
share sur files2k22
data (F:)
Capacité : 9,98 Go
0,4 % utilisés
37,1 Mo Espace utilisé
9,95 Go Espace disponible
Aller à Vue d'ensemble des volumes >
QUOTA
share sur files2k22
Modèle : Limite de 2 Go
Type : Inconditionnel
Limite : 2,00 Go
Statut : Activé
Application automatique Oui
Seuils de notification : 3
85 % - Adresse de messagerie
95 % - Événement, Adresse de messagerie
100 % - Événement, Adresse de messagerie


D-Link
DAP-2662
Home
Maintenance
Configuration
System
Logout
Help
DAP-2662
Basic Settings
Wireless
LAN
IPv6
Advanced Settings
Performance
Wireless Resource
Multi-SSID
VLAN
Intrusion
Schedule
Internal RADIUS Server
ARP Spoofing Prevention
Bandwidth Optimization
Hotspot 2.0
Captive Portal
Authentication Settings
Login Page Upload
MAC Bypass
DHCP Server
Dynamic Pool Settings
Static Pool Settings
Current IP Mapping List
Filters
Traffic Control
Status
Device Information
Client Information
WDS Information
Statistics
Ethernet
WLAN
Wireless Settings
Wireless Band
2.4GHz
Operation Mode
Access Point
Network Name (SSID)
mvill_network
SSID Visibility
Enable
Auto Channel Selection
Enabled
Channel
6
Channel Width
Auto 20/40 MHz
Authentication
WPA-Personal
802.11k/v/r
Disable
PassPhrase Settings
WPA Mode
AUTO (WPA or WPA2)
Cipher Type
Auto
Group Key Update Interval
3600
(Sec)
Manual
Periodical Key Change
Time Interval
1
(1~168)hour(s)
PassPhrase
Confirm PassPhrase
notice: 8~63 in ASCII or 64 in Hex.
(0-9,a-z,A-Z,~!@#$%^&*()_+`-={}[];:"|,./<>?)
Save


root@tcpdump:~# tcpdump -i eno1 'tcp port 80' > dump.txt &
[3] 890
root@tcpdump:~# tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eno1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
root@tcpdump:~# cat dump.txt
root@tcpdump:~# _