SERVEUR DE LOG
KIWI SYSLOG
SERVEUR

SYSLOG SERVEUR

INSTALLATION ROUTEUR CISCO 2600

On se connecte au routeur avec notre serveur en câble console, on utilise le logiciel Putty qui est un émulateur de terminal. En effet, on se connecte via le port COM. Mise en service d'un lien SSH par la suite.

INSTALLATION ROUTEUR CISCO 3B1

On se connecte au routeur via un navigateur internet en saisissant son IP dans l'URL : 10.10.1.254 car c'est un routeur qui ne s'utilise pas en CLI.

Pour se connecter on utilise l'identifiant : cisco et le password : Ensitech2022

LE WAN

Le port WAN du routeur est configuré en G0/0 en DHCP.

LE LAN

Le LAN est configuré en G0/1 en 10.0.0.1 255.255.254.0 (/23)

Configuration du routeur

Enable

Conf t

Int g0/0 / interface WAN

Ip address dhcp

/*Ip address 172.22.101.199 255.255.0.0*/ —> en IP statique.

Ip route 0.0.0.0 0.0.0.0 172.22.100.1

No shutdown

Exit

Int g0/1 / interface LAN

Ip address 10.0.0.1 255.255.254.0

Ip dhcp pool lan

Network 10.0.0.0 255.255.254.0

Default-router 10.0.0.1

Dns-server 8.8.8.8 8.8.4.4

Ip dhcp excluded 10.10.1.1 10.10.1.100

access-list 1 permit 10.10.0.0 0.0.1.255

ip nat inside source list 1 interface **g0/0 (je sors sur l'interface 0/0 inside : lan vers → Wan)**

int g0/0

ip nat outside

int g0/1

ip nat inside

ip route 0.0.0.0 0.0.0.0 192.168.50.1

ip route 10.10.0.0 255.255.254.0 10.0.0.2

Configuration du routeur pour les messages Syslog :

Clock set 14 :23 :00 february 01 2023

Services timestamps

Logging trap 7

Logging facility local7

Logging 10.10.1.100

Ip nat log translations syslog

No ip nat log translations syslog

Show logging

No logging console informational (stop log routeur)

Sauvegarde

Copy running-config startup-config

Ou

Write memory

Voir la configuration

Show run (voir la conf)

INSTALLATION WINDOWS 10 SUR NOTRE SERVEUR

Téléchargement de l'image en .iso de Windows 10. On effectue une clef bootable avec Rufus et on boot sur la clef.

Installation du système d'exploitation.

Configuration d'une adresse IP fixe en 10.10.1.100 255.255.254.0

INSTALLATION KIWI SYSLOG SERVEUR

Téléchargement sur https://www.solarwinds.com/fr/kiwi-syslog-server.

Installation du logiciel KiwiSyslog version 9.8.

Le port UDP configurer est en écoute sur le port : 514

Le port TCP:1468

Le port SNMP:162

CONFIGURATION DES SOURCES D'ECOUTES

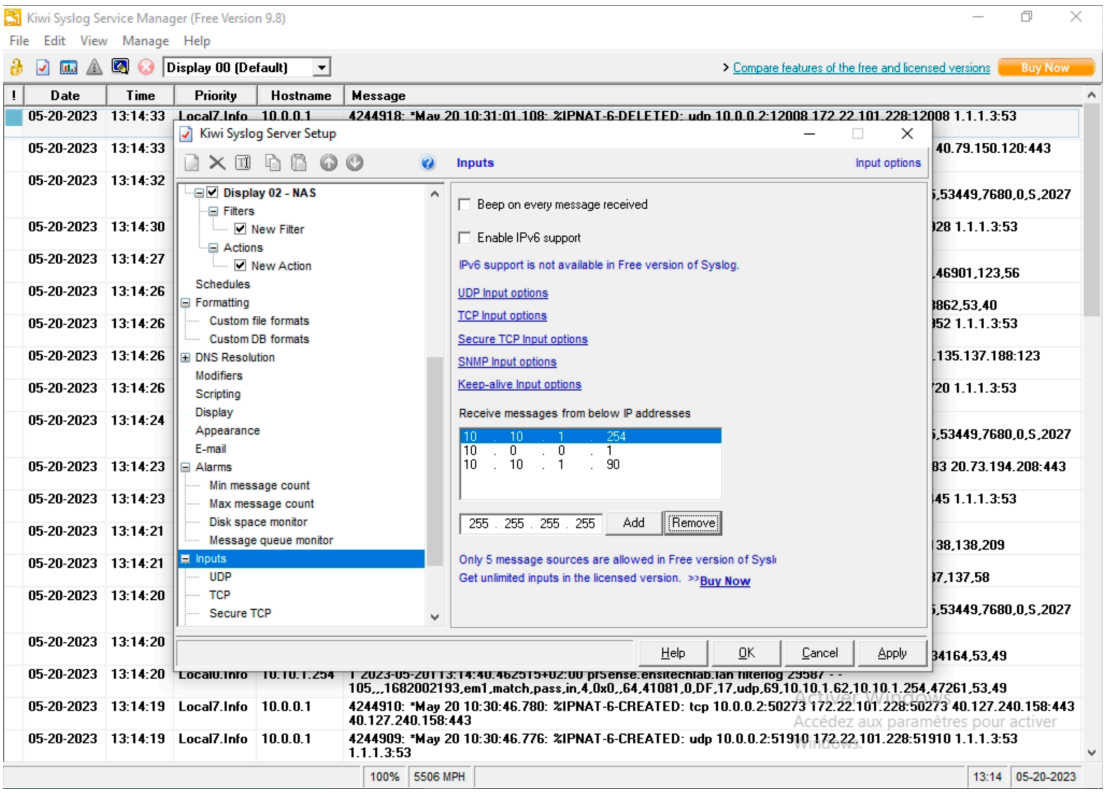
File —> setup —> input

On saisit les adresses IP des machines dont on souhaite récupérer les messages systèmes.

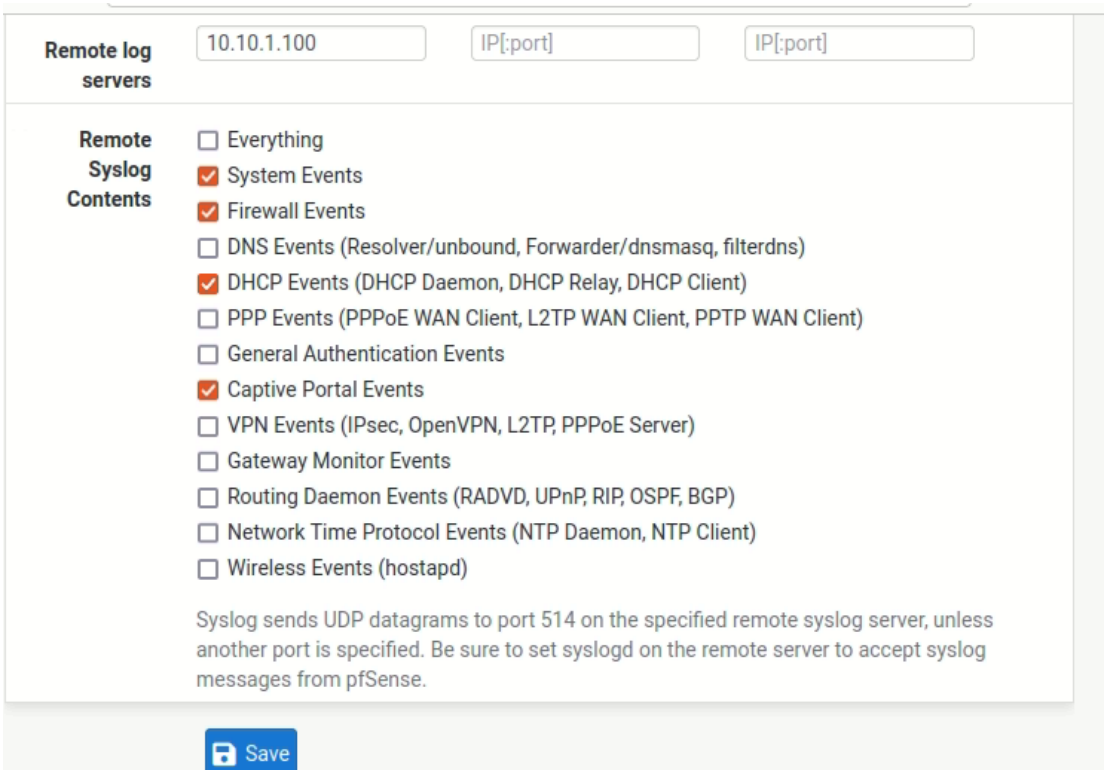
10.0.0.1 : le routeur Cisco 2600

10.10.1.254: le Pfsense

10.10.1.90: Le NAS: Network Attached Storage

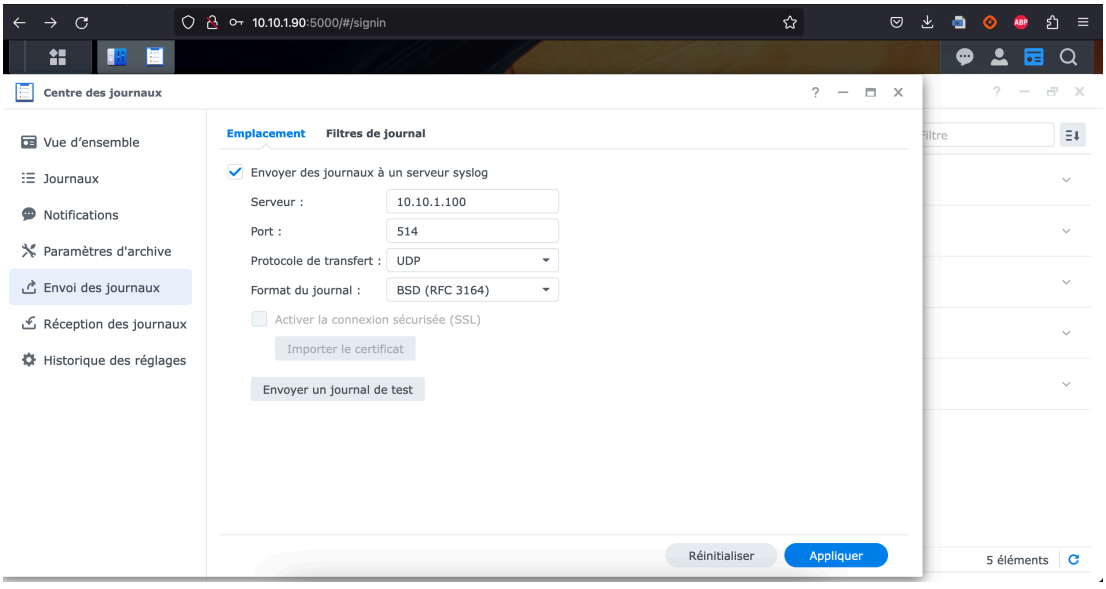


CONFIGURATION DU PFSENSE POUR LES MESSAGES SYSLOGS



CONFIGURATION DU NAS POUR LES MESSAGES SYSLOGS

Panneau de configuration, centre des journaux, envois des journaux.



IP LAN NAS : 10.10.1.90

Accès à distance : http://QuickConnect.to/Ensitech

MISE EN PLACE D'UNE AUTOMATISATION DE SAUVEGARDE DU FICHIER LOG

J'ai utiliser un script bash :

«xcopy C:\"Program Files (x86)"\Syslogd\Logs\ \\NAS-BACKUP\KiwiSyslog /D /E /C /R /H /K /Y»

Il copie le fichier source : C:\"Program Files (x86) »\Syslogd\Logs vers NAS-BACKUP\KiwiSyslog avec des paramètres.

Les paramètres concernés:

/D : Copie tous les fichiers sources qui sont plus récents que les fichiers de destination existants.

/E: Copie les répertoires et sous-répertoires, y compris les vides.

/C: Continue la copie même si des erreurs se produisent.

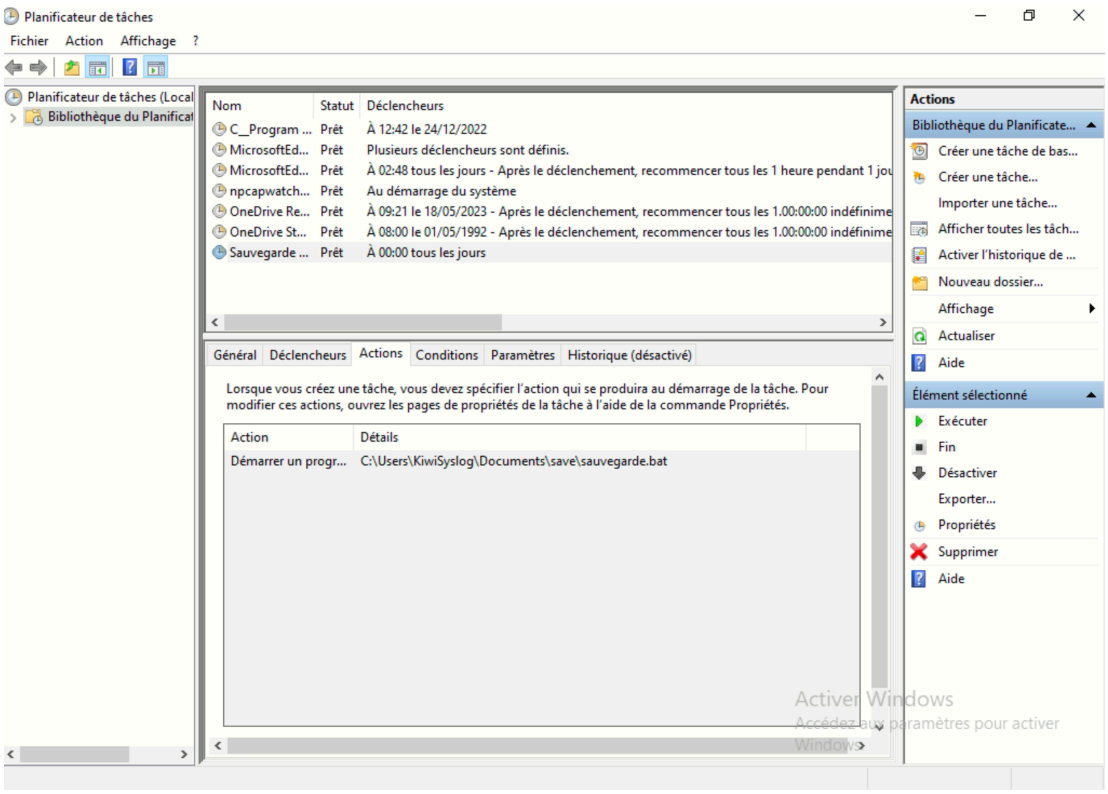
/R: Remplace les fichiers en lecture seule.

/H: Copie les fichiers avec des attributs de fichier système et masqués.

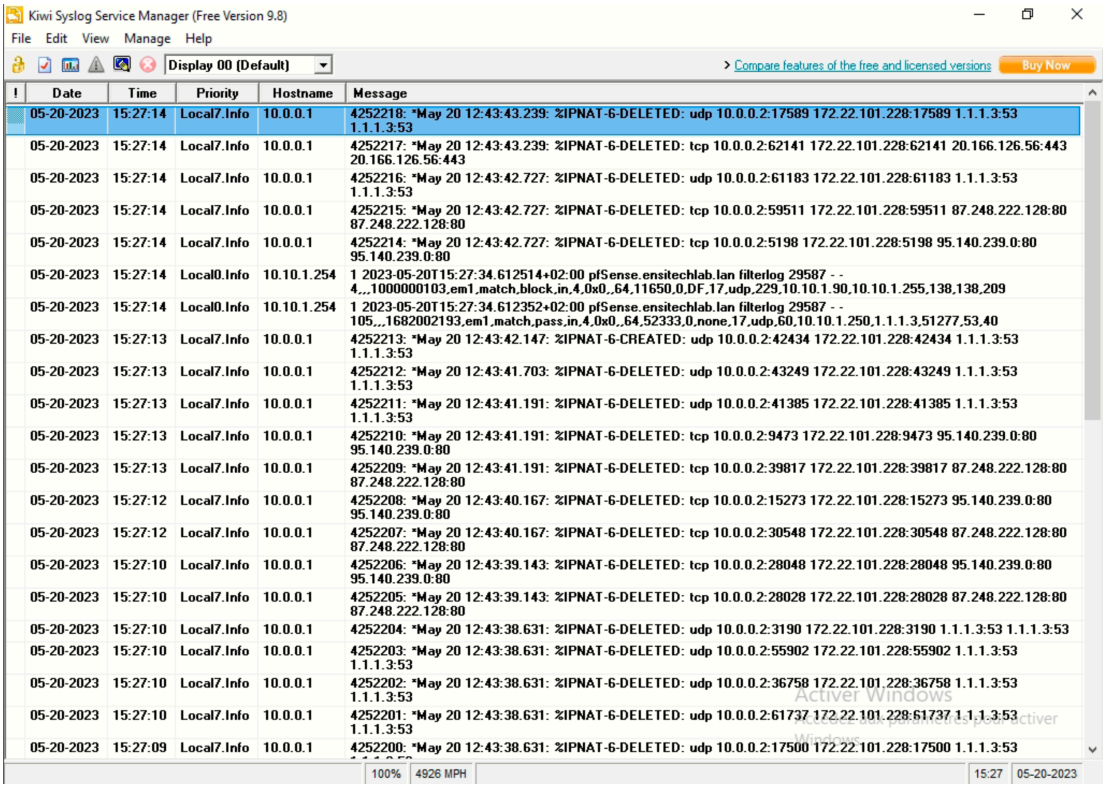
/K: Copie les attributs de fichiers.

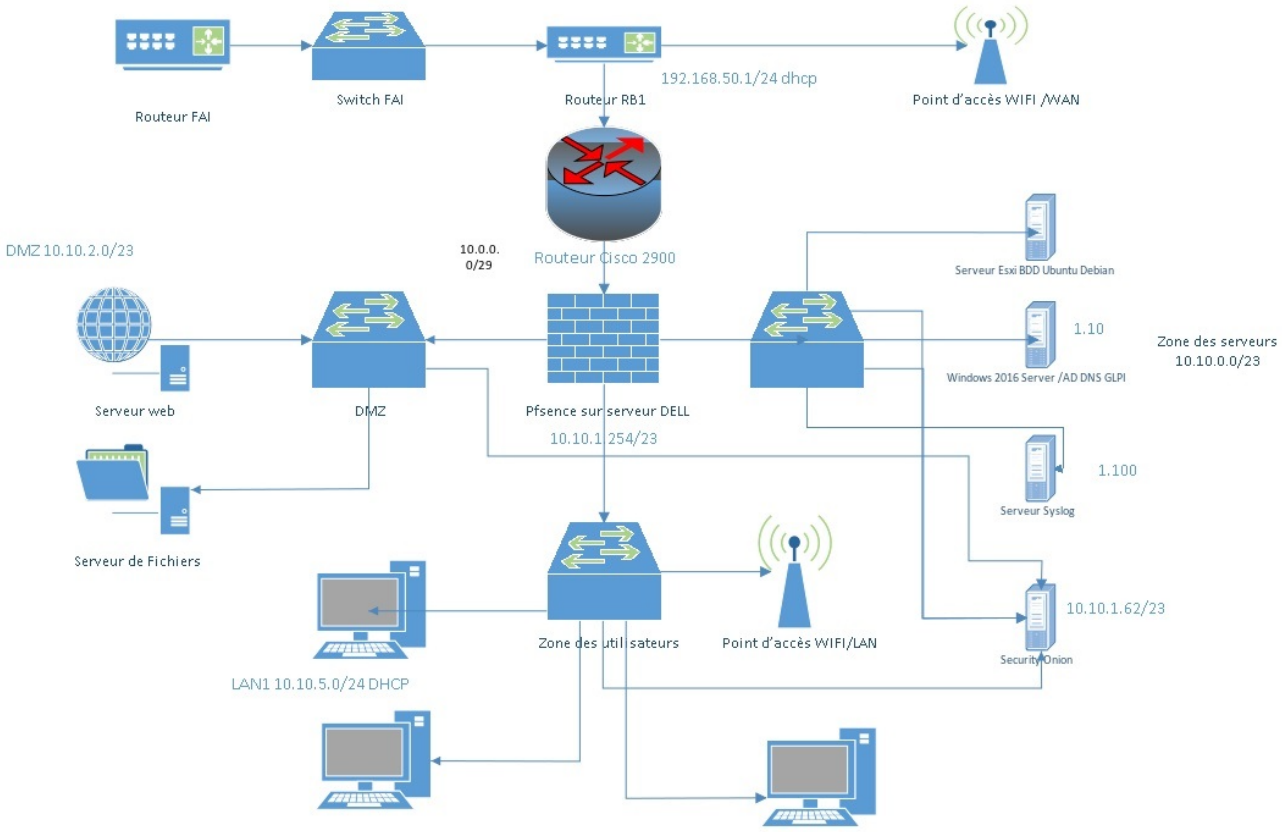
/Y: Supprime l'invite à confirmer que vous souhaitez remplacer un fichier de destination existant.

Dans le planificateur de tâche Windows, on crée une tâche que l'on nomme sauvegardes des journaux. On y ajoute un déclencheur, ici tous les jours à minuit. Puis une action, le fichier script.



Le serveur Kiwi en service :





Vous retrouverez ce projets menée en autonomie ci-dessous :

https://astro-portfolio-serres-nicolas.vercel.app/projet