

SERVEUR DE LOG KIWI SYSLOG SERVEUR

SYSLOG SERVEUR

INSTALLATION ROUTEUR CISCO 2900

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.

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)

INSTALLATION ROUTEUR CISCO 2900

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 KIWISYSLOG SERVEUR

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

Installation du logiciel KiwiSyslog version 9.8.

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

Le port TCP:1468

Le port SNMP:162

CONFIGURATION DES SOURCES D'ECOUTES

File —> setup —> input

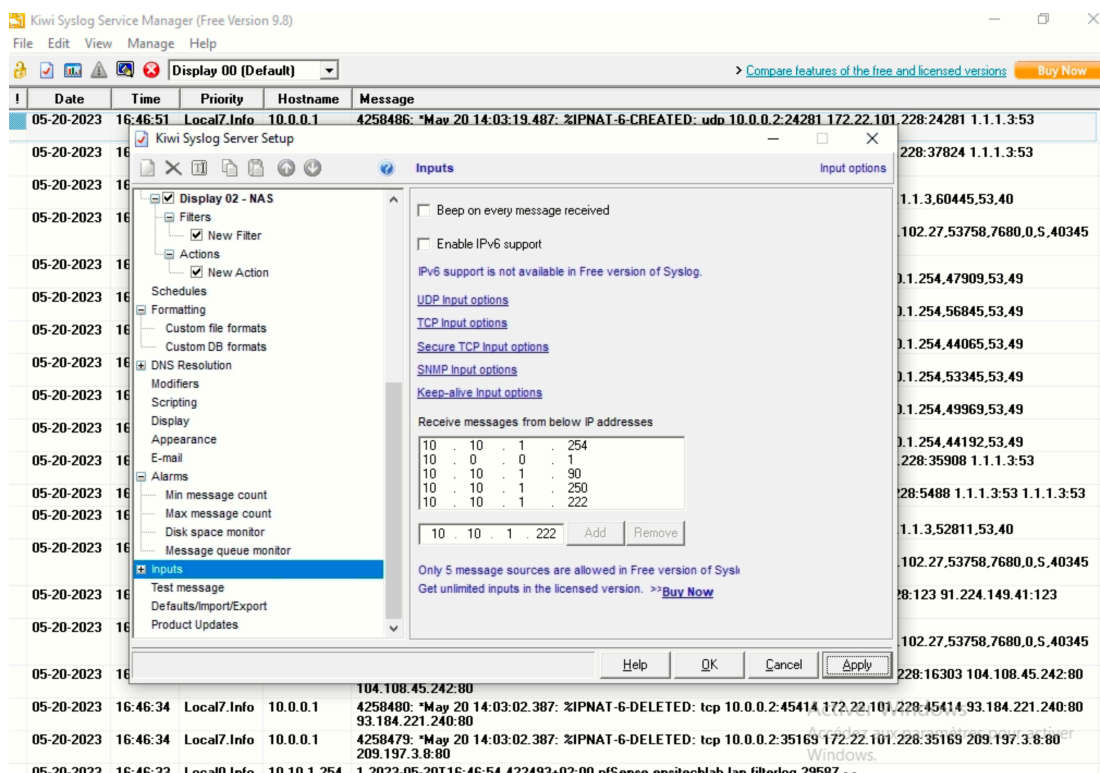
On saisit les adresses IP des machines dont on souhaite récupérer les messages systèmes.

10.0.0.1 : le routeur Cisco 2900

10.10.1.254: le Pfense

10.10.1.90: Le NAS: Network Attached Storage

10.10.1.22: Cisco 3b1 accès Wifi



CONFIGURATION DU PFSense POUR LES MESSAGES SYSLOGS

The screenshot shows the 'Remote log servers' configuration page in pfSense. At the top, there are three input fields: the first contains '10.10.1.100', and the other two contain 'IP[:port]'. Below these is a section titled 'Remote Syslog Contents' with a list of event categories, each with a checkbox. The checked categories are: System Events, Firewall Events, DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client), Captive Portal Events, and Wireless Events (hostapd). Other categories like DNS Events, PPP Events, General Authentication Events, VPN Events, Gateway Monitor Events, Routing Daemon Events, Network Time Protocol Events, and Wireless Events (hostapd) are unchecked. At the bottom of the list, there is a note: 'Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.' A blue 'Save' button is located at the bottom left of the configuration area.

CONFIGURATION DU NAS POUR LES MESSAGES SYSLOGS

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

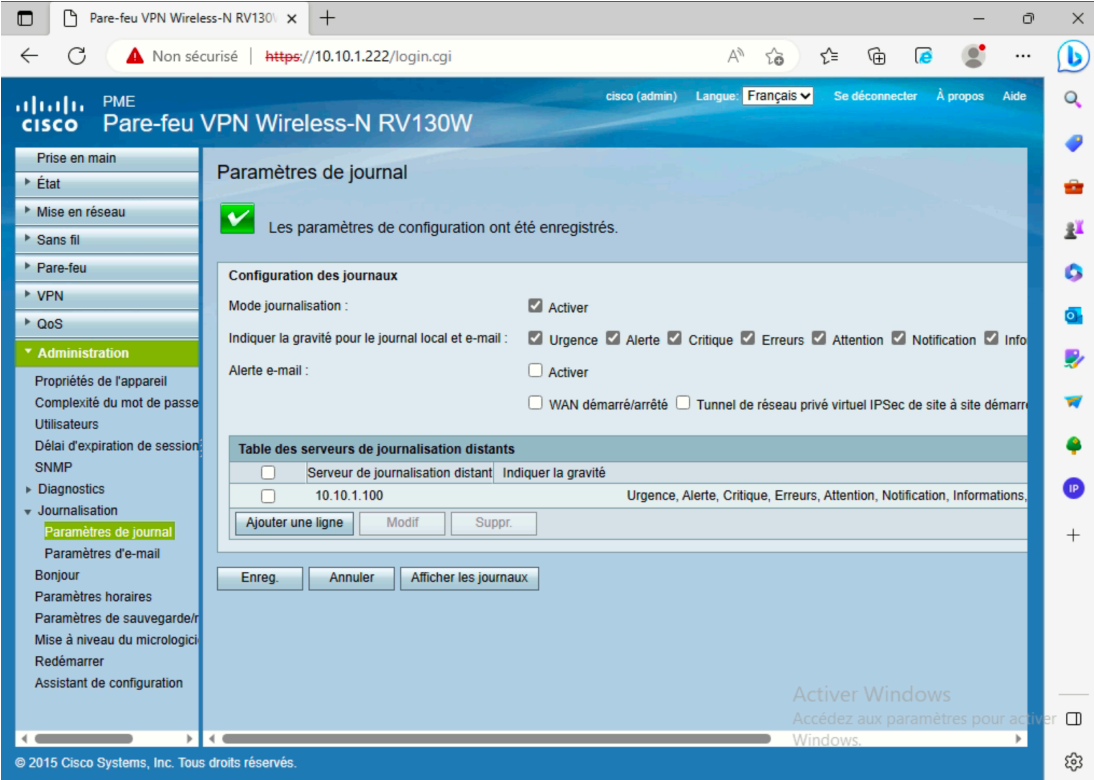
The screenshot shows the 'Centre des journaux' (Log Center) configuration page in pfSense. The page is titled 'Emplacement' and 'Filtres de journal'. A checkbox 'Envoyer des journaux à un serveur syslog' is checked. Below this, there are four input fields: 'Serveur' (10.10.1.100), 'Port' (514), 'Protocole de transfert' (UDP), and 'Format du journal' (BSD (RFC 3164)). There is also an unchecked checkbox for 'Activer la connexion sécurisée (SSL)' and a button 'Importer le certificat'. At the bottom of the configuration area, there is a button 'Envoyer un journal de test'. A 'Réinitialiser' button is on the left and an 'Appliquer' button is on the right. The page number '5 éléments' is visible at the bottom right.

IP LAN NAS : 10.10.1.90

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

CONFIGURATION DU ROUTEUR CISCO3B1 POUR LES MESSAGES SYSLOGS

On se connecte au routeur via l'URL puisqu'il ne s'utilise pas en CLI avec son adresse 10.10.1.222. On entre dans sa configuration en tant qu'administrateur et on ajoute un paramètre de journalisation.



The screenshot shows the Cisco VPN Firewall configuration interface in a web browser. The browser address bar shows the URL <https://10.10.1.222/login.cgi>. The page title is "PME Pare-feu VPN Wireless-N RV130W". The left sidebar shows the navigation menu with "Administration" expanded and "Journalisation" selected. The main content area is titled "Paramètres de journal" and displays a success message: "Les paramètres de configuration ont été enregistrés." Below this, the "Configuration des journaux" section shows the following settings:

- Mode journalisation : Activer
- Indiquer la gravité pour le journal local et e-mail : Urgence Alerte Critique Erreurs Attention Notification Info
- Alerte e-mail : Activer
- WAN démarré/arrêté Tunnel de réseau privé virtuel IPsec de site à site démarré/arrêté

The "Table des serveurs de journalisation distants" section contains the following table:

Severeur de journalisation distant	Indiquer la gravité
<input type="checkbox"/> 10.10.1.100	Urgence, Alerte, Critique, Erreurs, Attention, Notification, Informations.

Buttons for "Ajouter une ligne", "Modif", and "Suppr." are visible below the table. At the bottom of the configuration area, there are buttons for "Enreg.", "Annuler", and "Afficher les journaux". The footer of the page reads "© 2015 Cisco Systems, Inc. Tous droits réservés." and "Activer Windows" is visible in the bottom right corner.

MISE EN PLACE D'UNE AUTOMATISATION DE SAUVEGARDE DU FICHER 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.

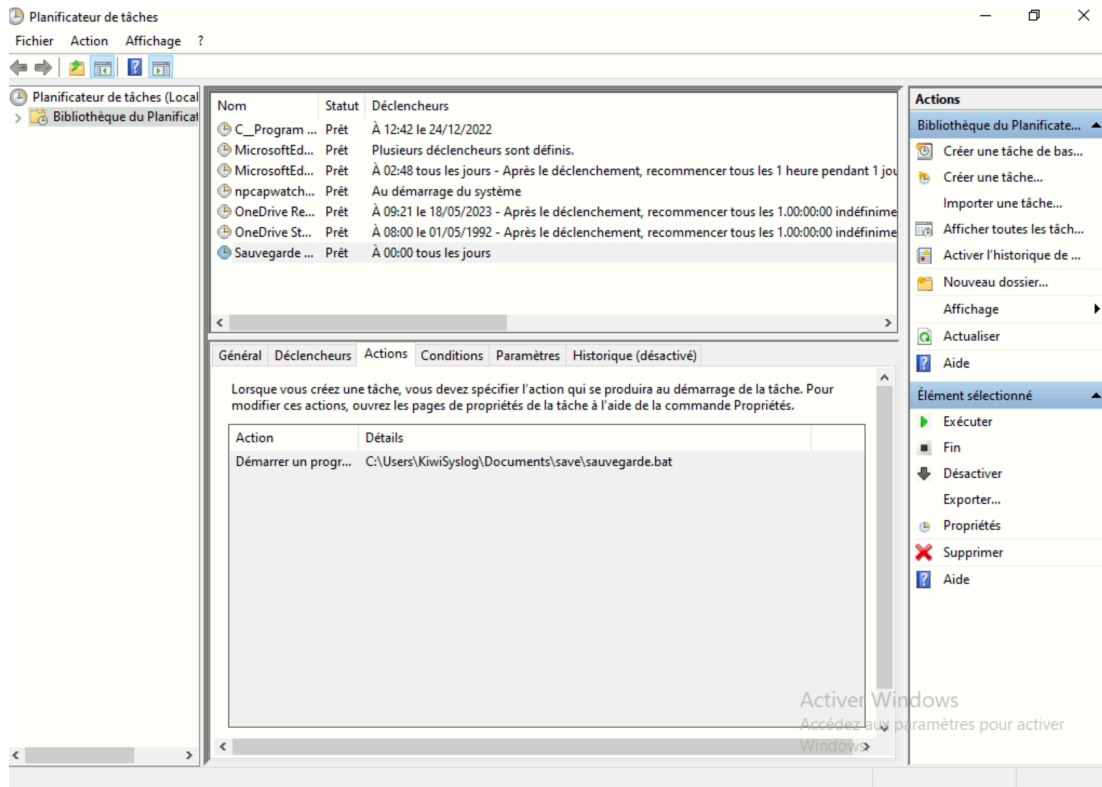
/R: Remplace les fichiers en lecture seule.

/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 :

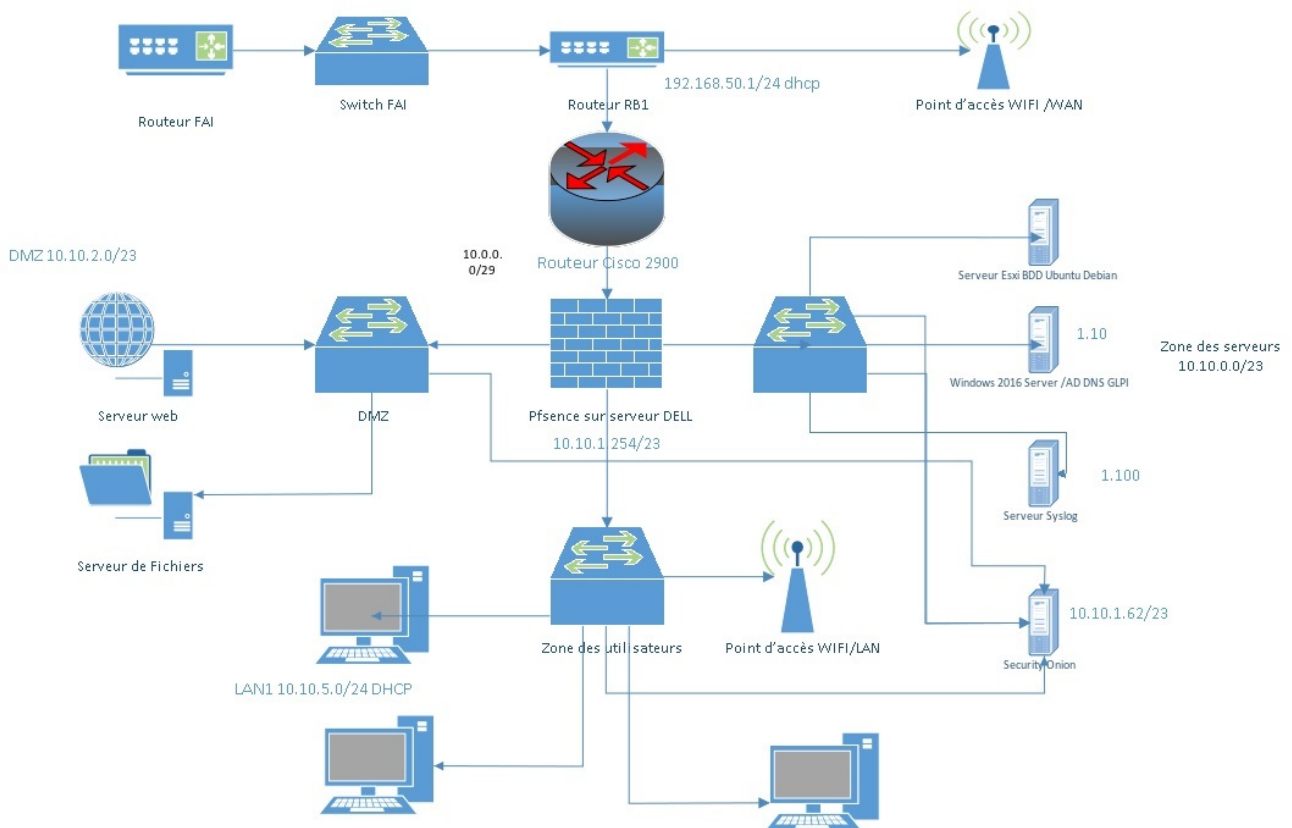
Kiwi Syslog Service Manager (Free Version 9.8)

File Edit View Manage Help

Display 00 (Default) [Compare features of the free and licensed versions](#) [Buy Now](#)

I	Date	Time	Priority	Hostname	Message
	05-20-2023	15:27:14	Local7.Info	10.0.0.1	4252218: *May 20 12:43:43.239: %IPNAT-6-DELETED: udp 10.0.0.2:17589 172.22.101.228:17589 1.1.1.3:53
	05-20-2023	15:27:14	Local7.Info	10.0.0.1	4252217: *May 20 12:43:43.239: %IPNAT-6-DELETED: tcp 10.0.0.2:62141 172.22.101.228:62141 20.166.126.56:443
	05-20-2023	15:27:14	Local7.Info	10.0.0.1	4252216: *May 20 12:43:42.727: %IPNAT-6-DELETED: udp 10.0.0.2:61183 172.22.101.228:61183 1.1.1.3:53
	05-20-2023	15:27:14	Local7.Info	10.0.0.1	4252215: *May 20 12:43:42.727: %IPNAT-6-DELETED: tcp 10.0.0.2:59511 172.22.101.228:59511 87.248.222.128:80
	05-20-2023	15:27:14	Local7.Info	10.0.0.1	4252214: *May 20 12:43:42.727: %IPNAT-6-DELETED: tcp 10.0.0.2:5198 172.22.101.228:5198 95.140.239.0:80
	05-20-2023	15:27:14	Local0.Info	10.10.1.254	1 2023-05-20T15:27:34.612514+02:00 pfSense.ensitechlab.lan filterlog 29587 -- 4...1000000103.em1.match.block.in.4.0x0..64.11650.0.DF.17.udp.229.10.10.1.90.10.10.1.255.138.138.209
	05-20-2023	15:27:14	Local0.Info	10.10.1.254	1 2023-05-20T15:27:34.612352+02:00 pfSense.ensitechlab.lan filterlog 29587 -- 105...1682002193.em1.match.pass.in.4.0x0..64.52333.0.none.17.udp.60.10.10.1.250.1.1.1.3.51277.53.40
	05-20-2023	15:27:13	Local7.Info	10.0.0.1	4252213: *May 20 12:43:42.147: %IPNAT-6-CREATED: udp 10.0.0.2:42434 172.22.101.228:42434 1.1.1.3:53
	05-20-2023	15:27:13	Local7.Info	10.0.0.1	4252212: *May 20 12:43:41.703: %IPNAT-6-DELETED: udp 10.0.0.2:43249 172.22.101.228:43249 1.1.1.3:53
	05-20-2023	15:27:13	Local7.Info	10.0.0.1	4252211: *May 20 12:43:41.191: %IPNAT-6-DELETED: udp 10.0.0.2:41385 172.22.101.228:41385 1.1.1.3:53
	05-20-2023	15:27:13	Local7.Info	10.0.0.1	4252210: *May 20 12:43:41.191: %IPNAT-6-DELETED: tcp 10.0.0.2:9473 172.22.101.228:9473 95.140.239.0:80
	05-20-2023	15:27:13	Local7.Info	10.0.0.1	4252209: *May 20 12:43:41.191: %IPNAT-6-DELETED: tcp 10.0.0.2:39817 172.22.101.228:39817 87.248.222.128:80
	05-20-2023	15:27:12	Local7.Info	10.0.0.1	4252208: *May 20 12:43:40.167: %IPNAT-6-DELETED: tcp 10.0.0.2:15273 172.22.101.228:15273 95.140.239.0:80
	05-20-2023	15:27:12	Local7.Info	10.0.0.1	4252207: *May 20 12:43:40.167: %IPNAT-6-DELETED: tcp 10.0.0.2:30548 172.22.101.228:30548 87.248.222.128:80
	05-20-2023	15:27:10	Local7.Info	10.0.0.1	4252206: *May 20 12:43:39.143: %IPNAT-6-DELETED: tcp 10.0.0.2:28048 172.22.101.228:28048 95.140.239.0:80
	05-20-2023	15:27:10	Local7.Info	10.0.0.1	4252205: *May 20 12:43:39.143: %IPNAT-6-DELETED: tcp 10.0.0.2:28028 172.22.101.228:28028 87.248.222.128:80
	05-20-2023	15:27:10	Local7.Info	10.0.0.1	4252204: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:3190 172.22.101.228:3190 1.1.1.3:53 1.1.1.3:53
	05-20-2023	15:27:10	Local7.Info	10.0.0.1	4252203: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:55902 172.22.101.228:55902 1.1.1.3:53
	05-20-2023	15:27:10	Local7.Info	10.0.0.1	4252202: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:36758 172.22.101.228:36758 1.1.1.3:53
	05-20-2023	15:27:10	Local7.Info	10.0.0.1	4252201: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:61737 172.22.101.228:61737 1.1.1.3:53
	05-20-2023	15:27:09	Local7.Info	10.0.0.1	4252200: *May 20 12:43:38.631: %IPNAT-6-DELETED: udp 10.0.0.2:17500 172.22.101.228:17500 1.1.1.3:53

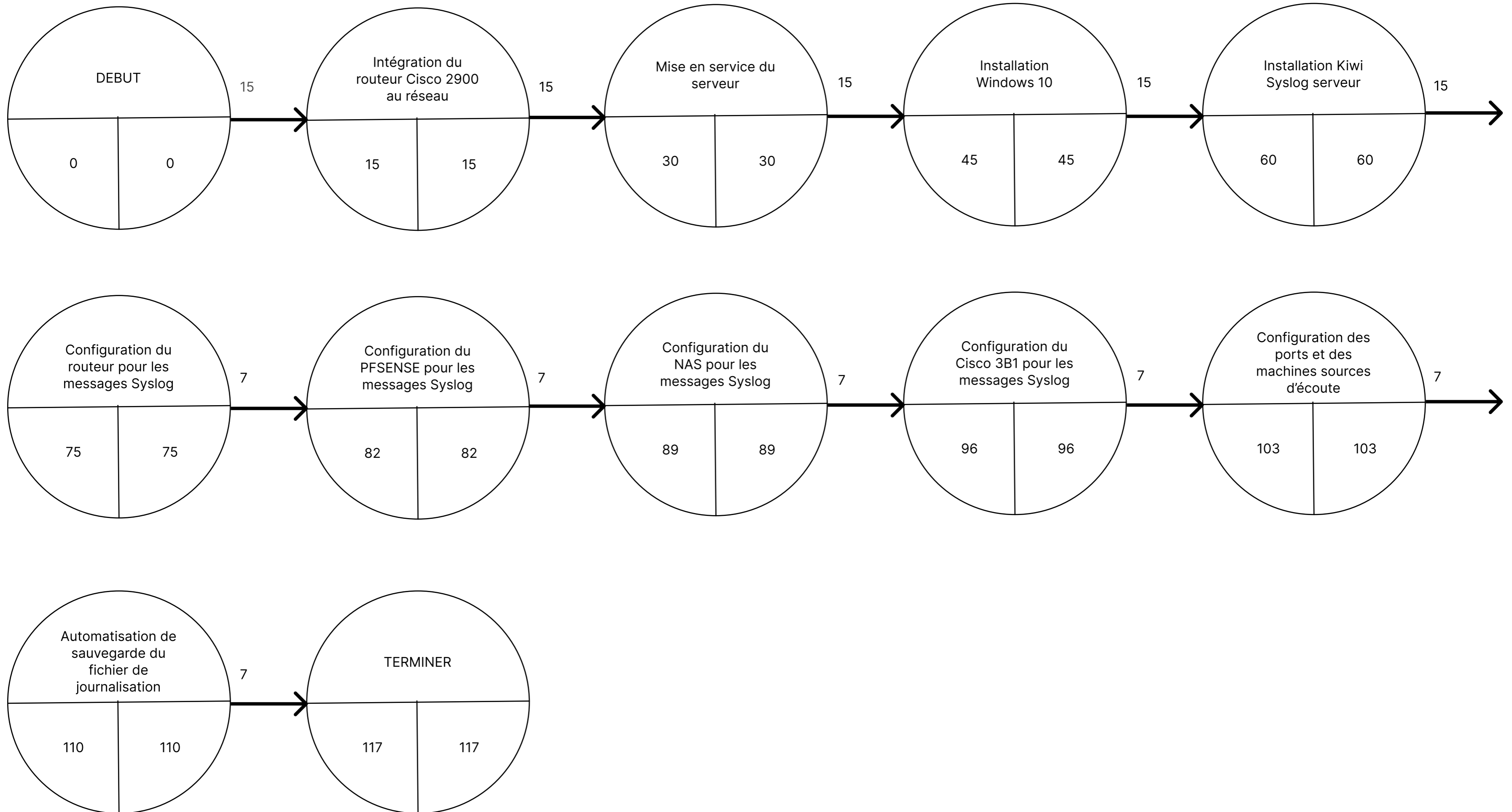
100% | 4926 MPH | 15:27 | 05-20-2023



Vous retrouverez ce projets menée en autonomie ci-dessous :

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

Serveur Kiwi Syslog - Diagrammes **théoriques**



Serveur Kiwi Syslog - Diagrammes effectifs

