

Caron Cyprien

BTS SIO 2

Document de validation de compétences

AP-2 SAVEOL

16/09-30/09/2025

Groupe 1

Présentation du contexte d'entreprise

En 2001, deux coopératives agricoles de la région brestoise ont fusionné et donné naissance à la société coopérative agricole Savéol (qui signifie « lever de Soleil » en breton).

Savéol a été rejointe en 2012 par la coopérative du "Val Nantais" spécialisée notamment dans la Culture de mâche ainsi que par la société d'intérêt collectif agricole "Les primeurs du mistral" produisant également des tomates à Lançon de Provence près de Marseille. En deux décennies, Savéol est devenue le leader de la production de tomates en France (plus de 70 000 tonnes par an).

La société Savéol propose des prestations pour environ une centaine de maraichers adhérents, principalement situés dans le département du Finistère. Ces prestations sont les suivantes : gestion la chaîne commerciale (marketing, conditionnement, commercialisation et livraison) ; conseil technique en agronomie ; recherche et développement de nouvelles espèces et de modes de production innovants plus respectueux de l'environnement.

A l'heure actuelle, 80% de la production est commercialisée sur le territoire métropolitain et 20% part à l'export vers les pays limitrophes de la France. La valorisation et la commercialisation des produits frais fragiles que sont les tomates et les fraises nécessitent une organisation et une logistique particulièrement rodées et efficaces. En effet, la récolte quotidienne, qui peut dépasser les 800 tonnes, sera déposée par les producteurs serristes dans l'une des deux stations de conditionnement afin d'être emballée dans un packaging adapté au mode de vente et de transport. Les clients de Savéol (des enseignes de grande et moyenne surface ou des grossistes) sont assurés que leur commande sera livrée le lendemain au plus tard.

L'esprit d'innovation qui anime les administrateurs de la coopérative Savéol dans ses choix d'évolution se ressent aussi au niveau du pilotage et de la gestion de son système d'information. Le périmètre d'action de l'équipe du service informatique est diversifié et concerne la gestion de projet, le développement d'applications, l'assistance fonctionnelle utilisateur, la supervision et l'administration ainsi que la maintenance système et réseau.

Le service informatique, sous la direction de M. Netralli, compte une nouvelle chef de projet, Mme Farez, trois techniciens réseau et système, ainsi que deux personnes en charge des solutions logicielles.

Vous êtes accueillis au sein de cette équipe. Il vous est précisé que votre domaine d'intervention concernera les fonctions liées à la gestion et à l'évolution de l'infrastructure système et réseau du siège de SAVEOL.

Objectifs attendus

L'entreprise Savéol vise à sécuriser ses services grâce au cloisonnement via des VLANs. Un projet est en cours pour mettre en production un serveur web sécurisé dans une zone DMZ. Le DSI souhaite également étendre l'infrastructure réseau en ajoutant une DMZ et une zone Internet, répondant ainsi aux besoins des employés tout en maximisant la sécurité.

Conditions de Réalisation

Environnement

- Savéol dispose de 6 switchs Cisco dont un de niveau 3.
- Un routeur Zyxel pour le pare-feu et un routeur Cisco 2911 pour la connexion Internet.
- 2 serveurs physiques : un pour la DMZ et un pour le LAN, équipés d'Hyper-V.

Contraintes de Mise en Production

- Utiliser le protocole de routage RIP V2.
- Accès Internet pour services et serveurs du LAN et DMZ sans modifier la configuration du routeur principal (192.168.4.254).
- Le serveur web dans la DMZ doit être accessible depuis le LAN et l'extérieur.
- Respecter le plan d'adressage et de nommage de l'entreprise.
- Sauvegardes automatiques des configurations du lundi au vendredi.
- Chaque membre devra avoir ses propres serveurs virtualisés.
- Accès aux services AD pour tous les services.
- Impossible pour les services de communiquer entre eux.
- Le pare-feu doit permettre les connexions vers le serveur web depuis le LAN et Internet.
- Accès sécurisé à Internet pour la zone LAN.
- Limiter l'accès aux éléments de la DMZ.
- Seule l'équipe IT doit administrer les interconnexions avec un contrôle d'accès.

- Accès au TFTP réservé au service IT.
- D'éventuelles règles supplémentaires peuvent être ajoutées avec accord.

Validation des Documents

- Compiler l'ensemble des configurations et maintenir à jour les documents tels que schémas réseau, adresses IP, et mots de passe.
- Rédiger un rapport de tests pour valider la solution.

Responsabilités

- Le commanditaire fournira les informations nécessaires à l'infrastructure.
- Le prestataire mettra en place un système opérationnel et une documentation technique pour le transfert de compétences, ainsi qu'une présentation technique.

Missions à Réaliser

Planification du Projet

- Élaborer un planning GANTT avec Trello, en définissant des tâches précises par personne.

Réalisation du Schéma Réseau

- Modifier le schéma pour inclure tous les éléments physiques et logiques. Imprimer et conserver ce document.

Paramétrage du Pare-feu et du Switch

- Recenser les permissions et interdictions d'accès, ainsi que les rôles des serveurs et ports associés. Configurer le routeur pare-feu.

Routage et Liaison Internet

- Etablir la communication avec Internet en respectant les contraintes techniques.

Administration Distante

- Permettre à l'équipe IT d'accéder à distance aux nouveaux équipements.

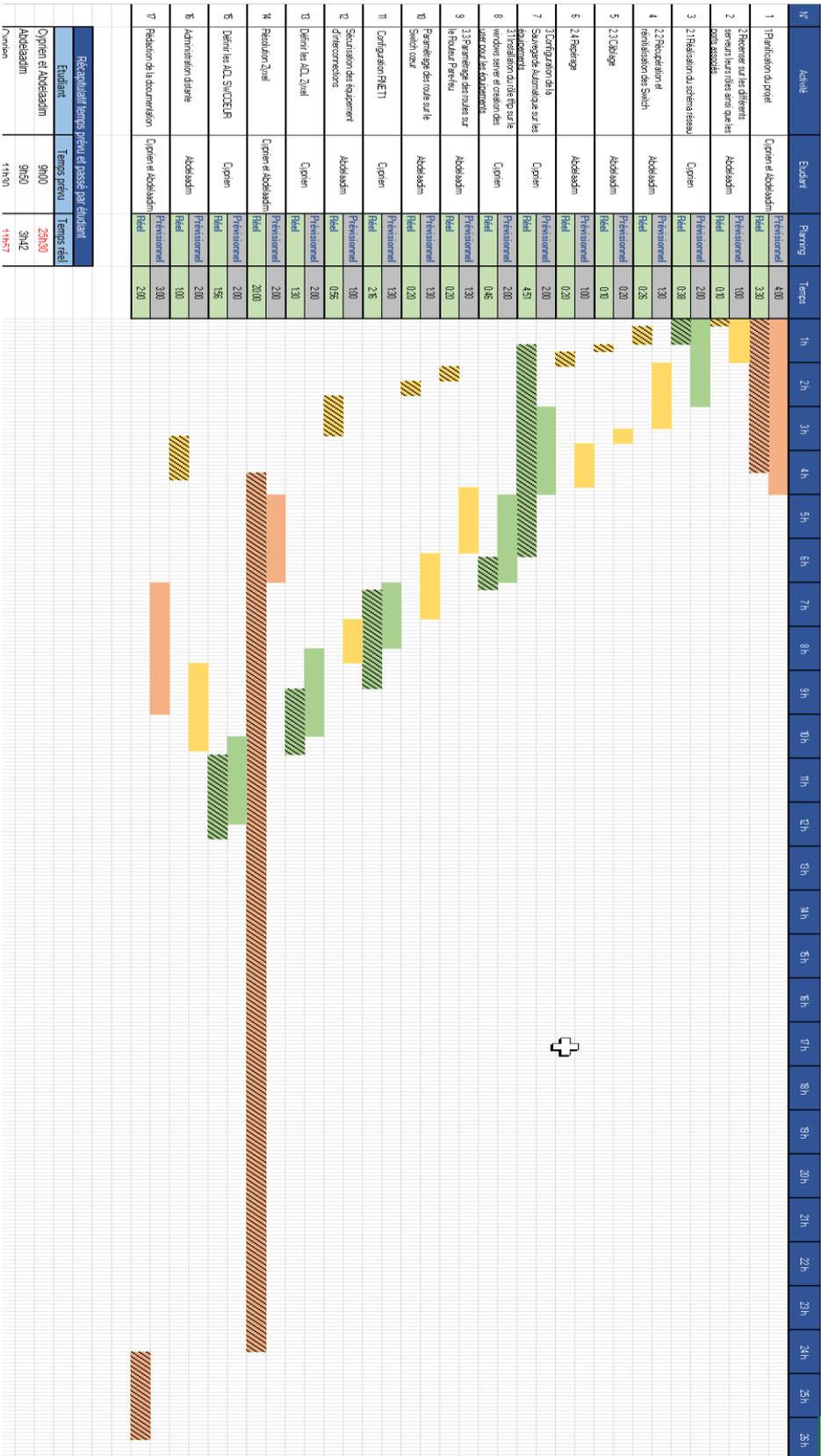
Sauvegarde

- Automatiser les sauvegardes nécessaires dans un espace dédié, les mardis, jeudis à 17h30, et vendredis à 12h30.

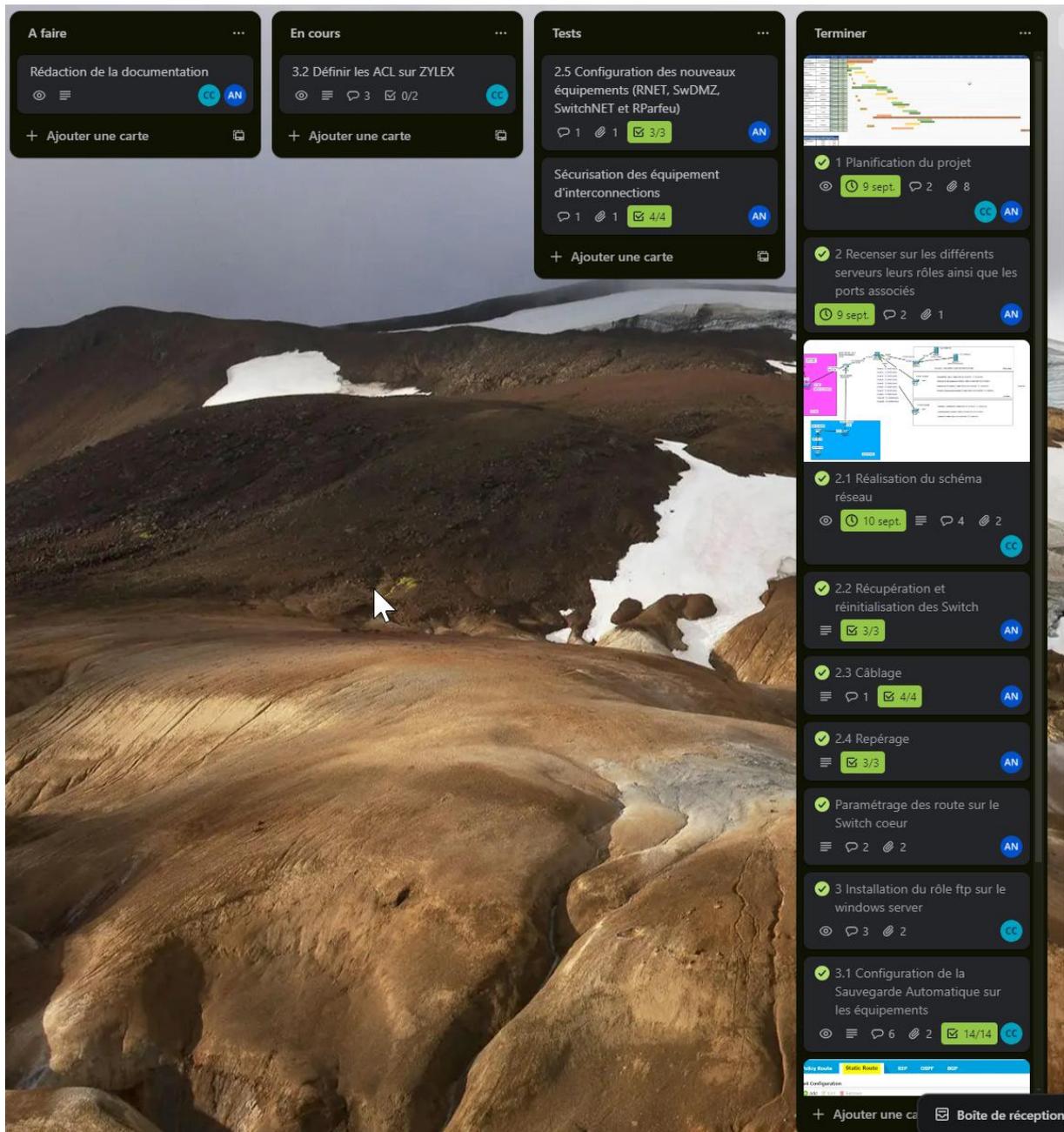
Plan de travail

1 Planification du projet

Création d'un tableau Trello et d'un diagramme de Gantt pour organiser le projet.



Création d'un Trello pour le suivi des activités.

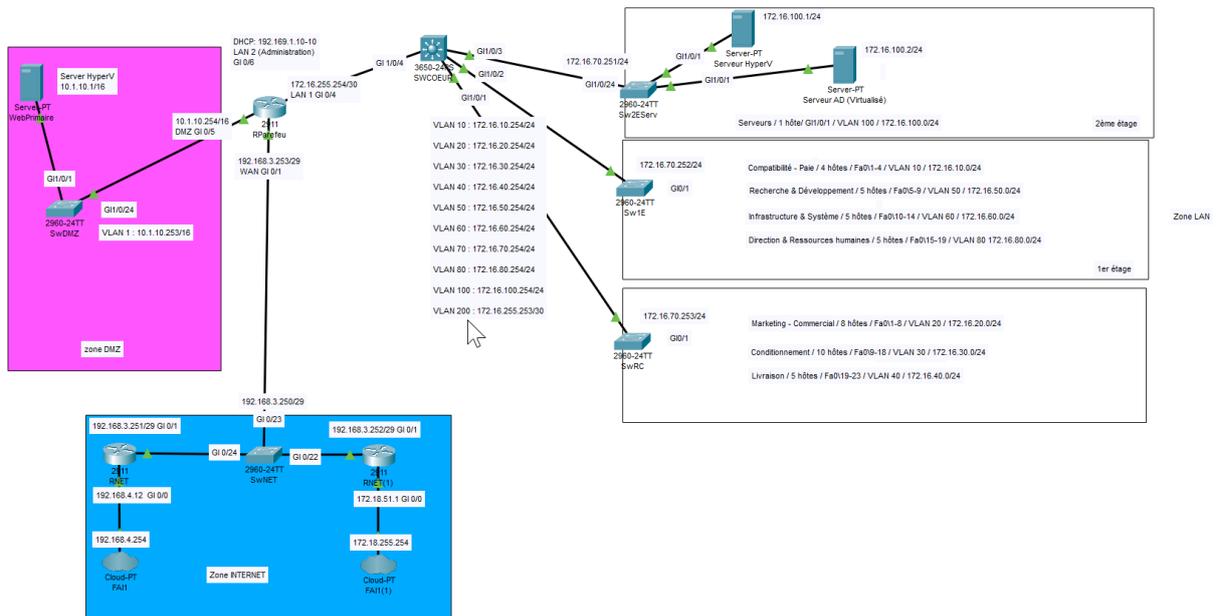


2 Recenser sur les différents serveurs leurs rôles ainsi que les ports associés
Élaboration d'un tableau Excel répertoriant les serveurs et leurs fonctions, qui sera utile pour les ACL à venir.

Serveur :	Ports :	Rôle:
NTP		123 Synchronisation du temps
WEB	80/443	Accéder à une page web
AD		389 Permettre l'accès à l'annuaire AD
FTP	20/21	Sauvegarde des équipements

2.1 Réalisation du schéma réseau

Actualisation du schéma réseau existant.

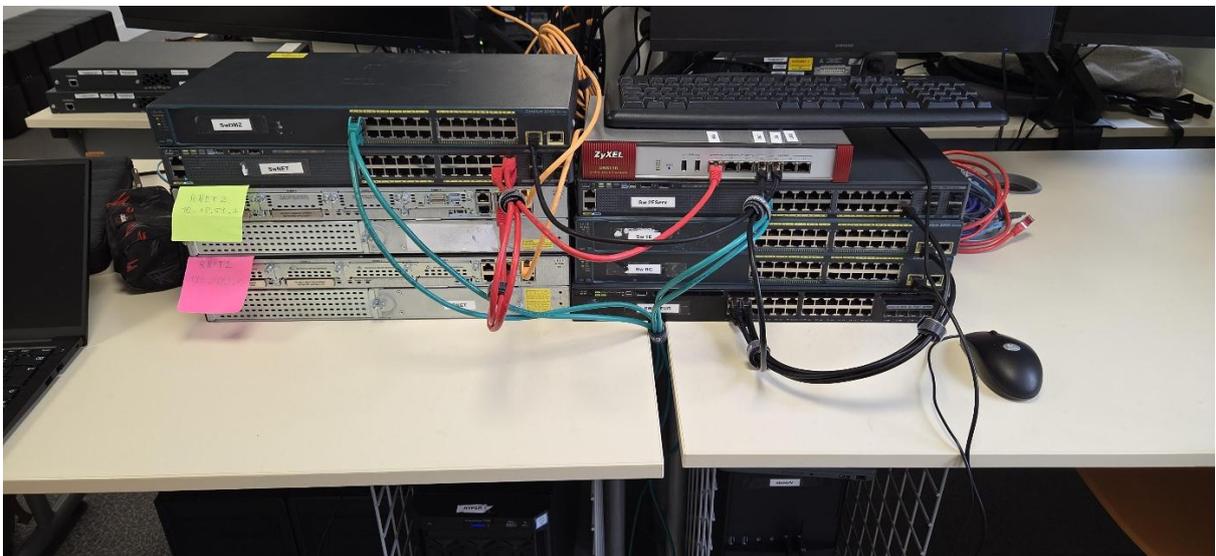


2.2 Récupération et réinitialisation des Switch

Rétablissement et réinitialisation des commutateurs.

2.3 Câblage

Interconnexion des nouveaux équipements en les câblant ensemble.



2.4 Repérage

Impression de petites étiquettes à coller sur les équipements pour les identifier et les distinguer.

3 Configuration de la Sauvegarde Automatique sur les équipements

Implémentation d'une sauvegarde automatique à l'aide de scripts sur les équipements d'interconnexion.

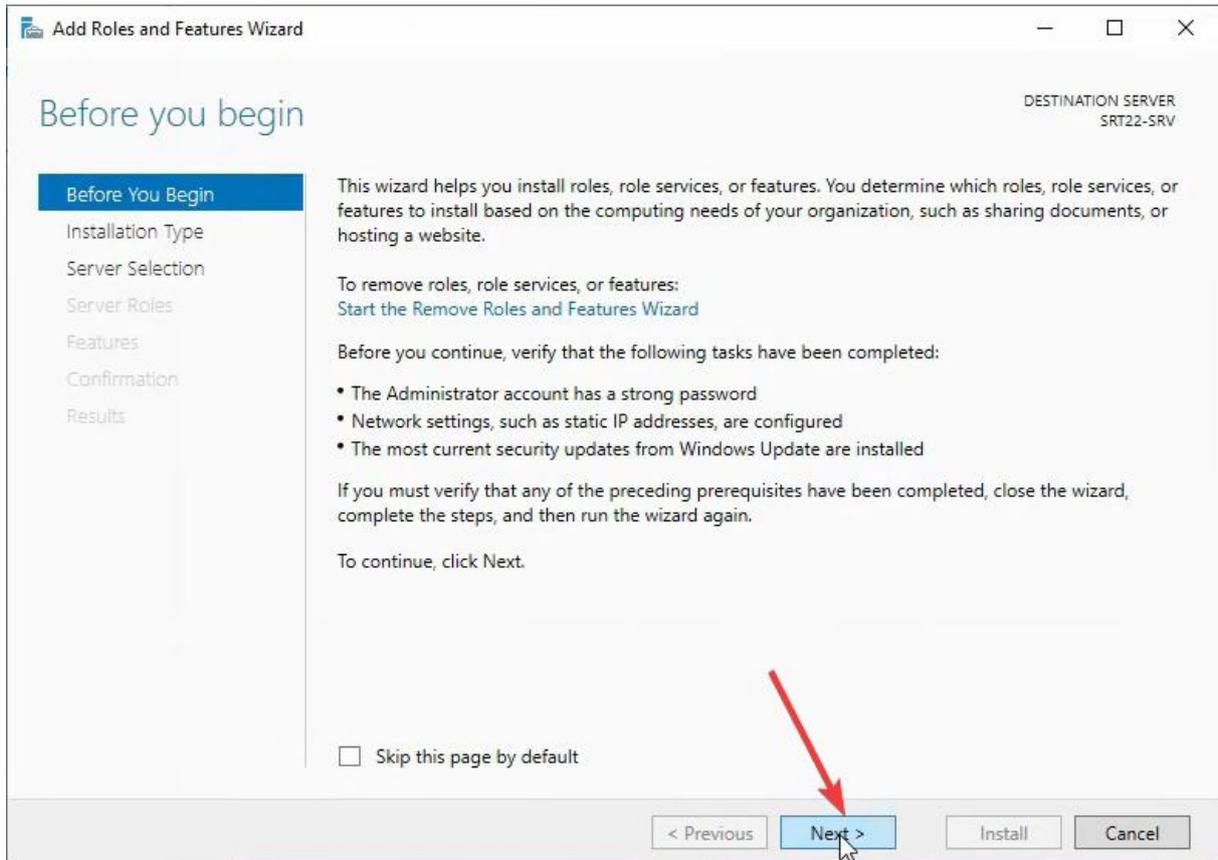
Automatiser toutes les sauvegardes nécessaires sur un espace dédié TFTP ou autre, les mardis, jeudis et vendredis à 17h30.

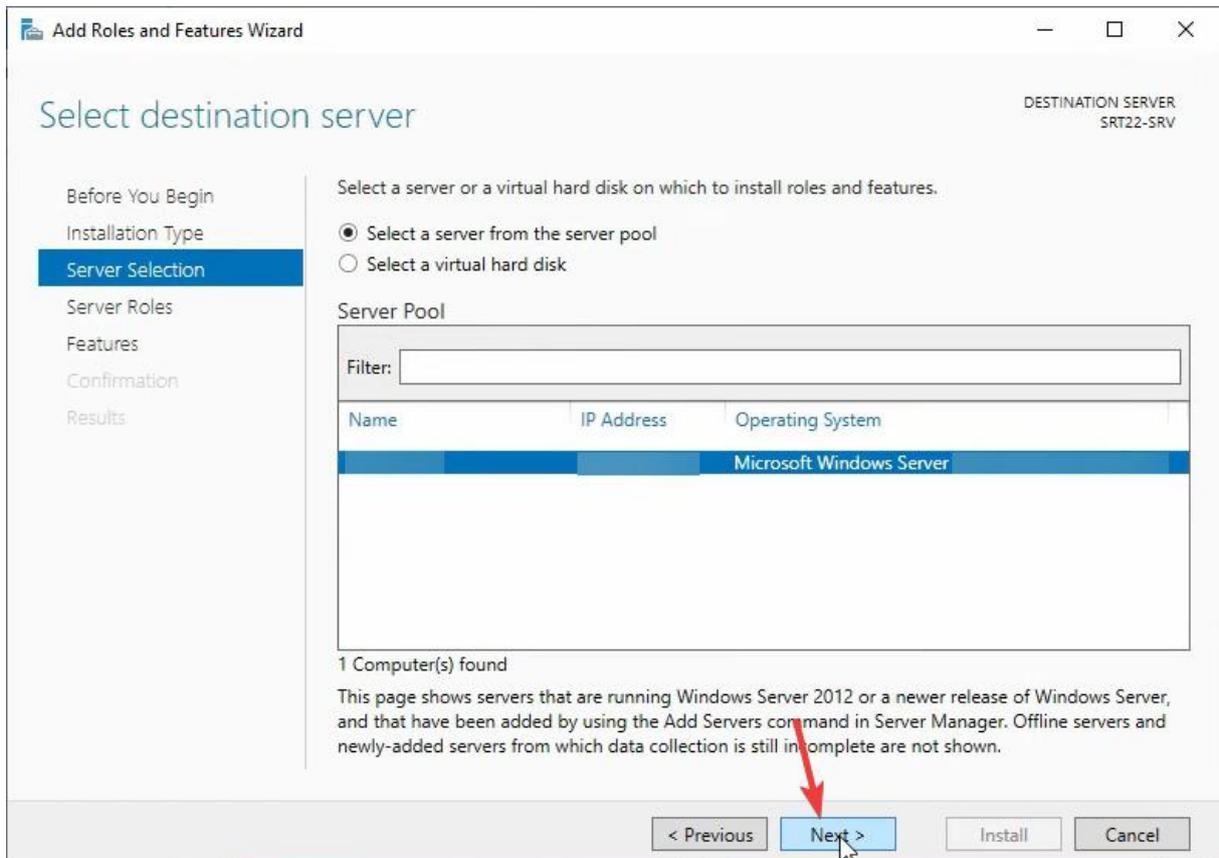
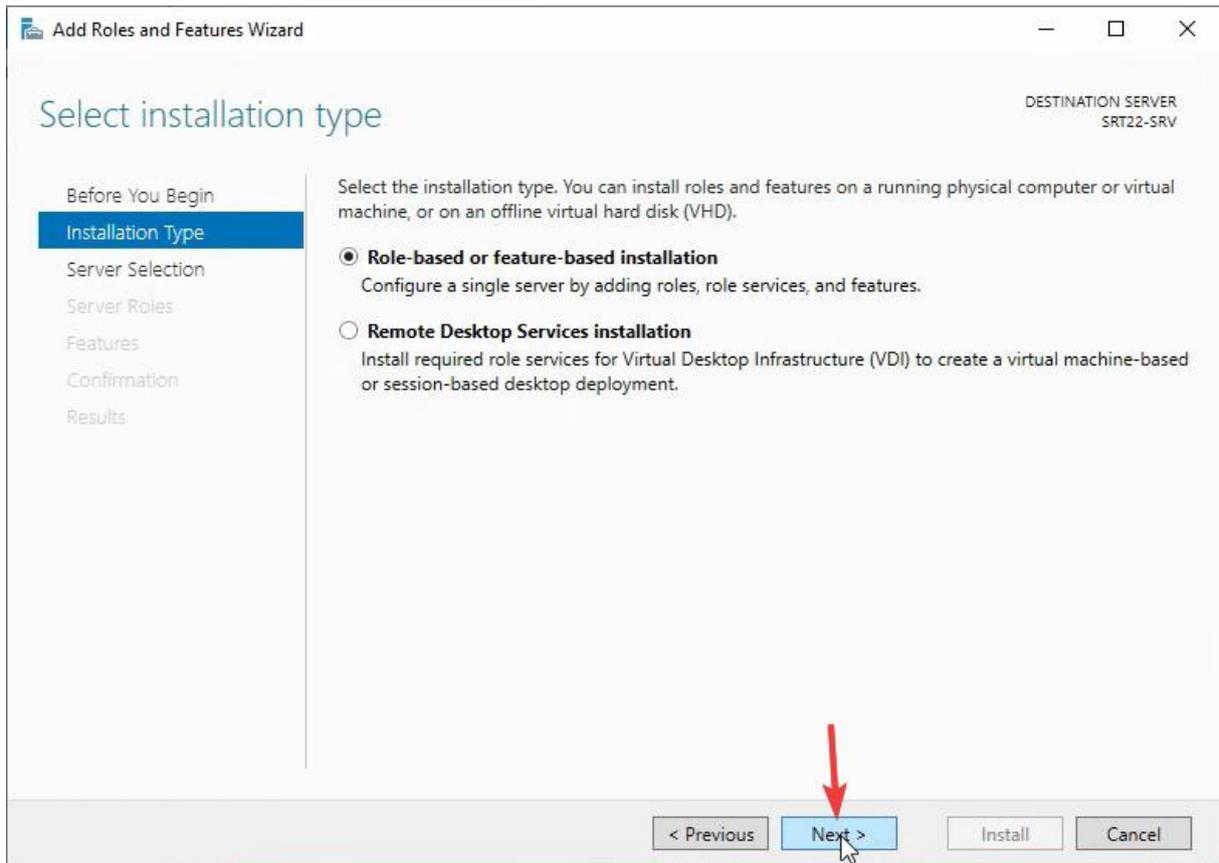
Un serveur FTP est requis, car le NAS n'est pas encore mis en place dans notre maquette.

J'ai donc installé le rôle IIS sur le serveur Windows pour qu'il serve de serveur FTP.

J'ai réalisé une procédure d'installation et de configuration du serveur FTP et testé son bon fonctionnement.

Installation rôle WinSrv FTP





Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Web Server Role (IIS)

Role Services

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Device Health Attestation
- DHCP Server
- DNS Server
- Fax Server
- File and Storage Services (1 of 12 installed)
- Host Guardian Service
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services
- Volume Activation Services
- Web Server (IIS)**
- Windows Deployment Services
- Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

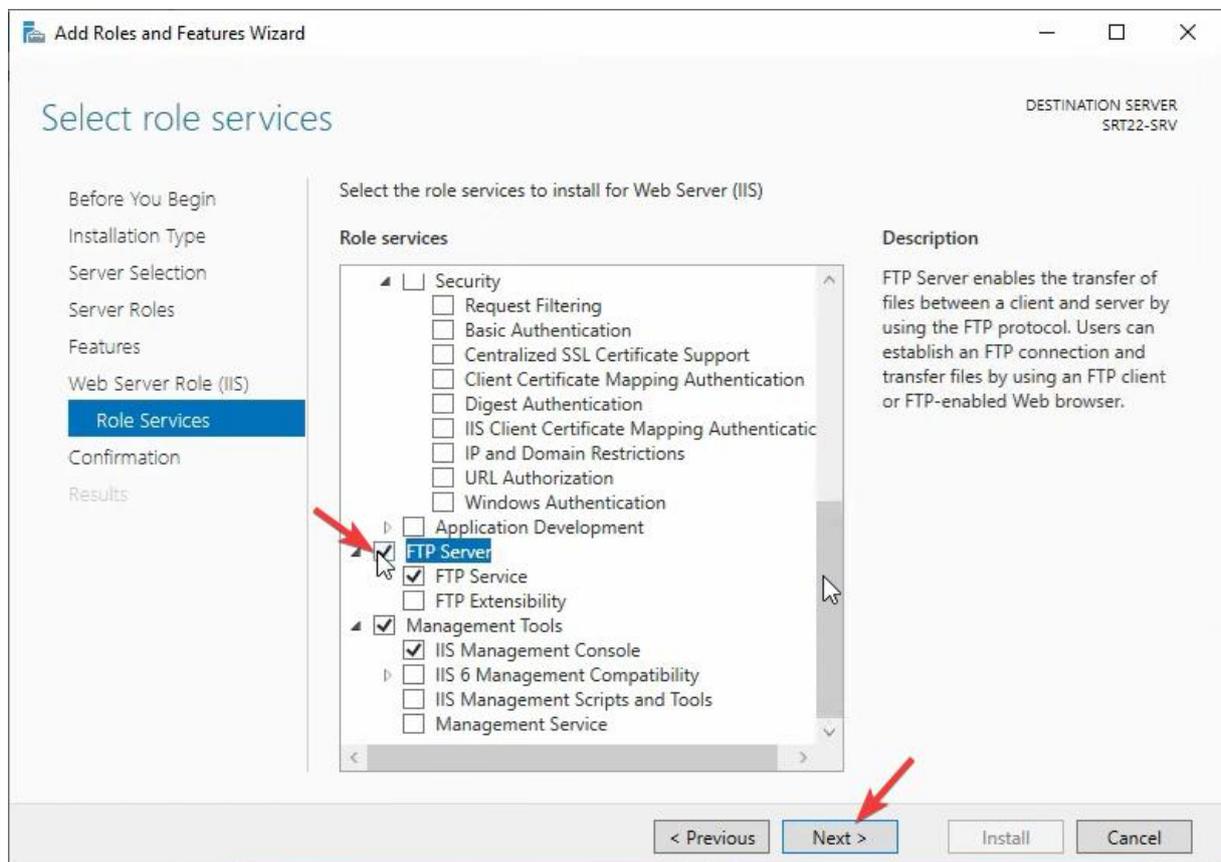
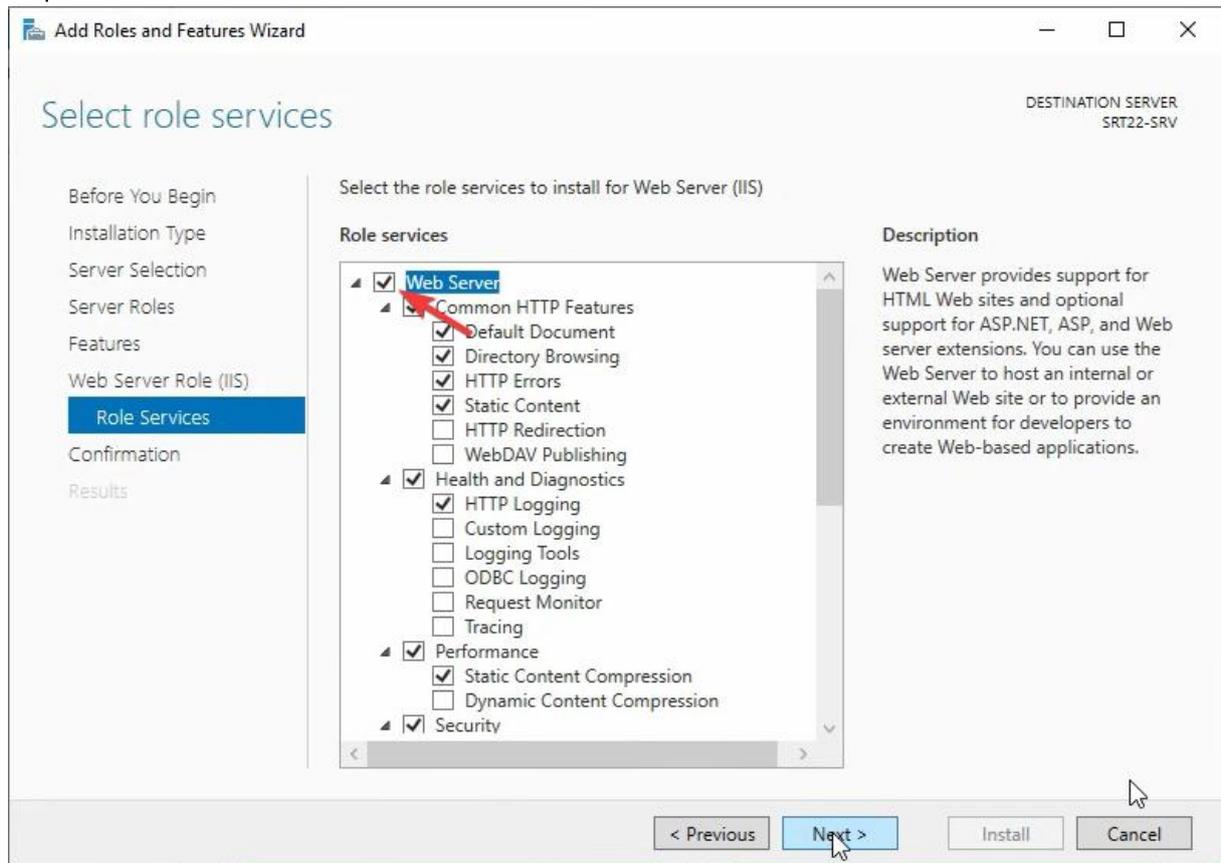
< Previous

Next >

Install

Cancel

Décocher le rôle serveur Web, nous n'en aurons pas besoin, puis descendre jusqu'au serveur FTP et cliquer dessus



Add Roles and Features Wizard

DESTINATION SERVER: SRT22-SRV

Confirm installation selections

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Web Server (IIS)

- FTP Server
- FTP Service
- Management Tools
- IIS Management Console

Export configuration settings
Specify an alternate source path

< Previous Next > **Install** Cancel

- Accueil
- Galerie
- Bureau
- Téléchargement
- Documents
- Images
- Musique
- Vidéos
- System32
- FTPData
- Bat
- Python
- Ce PC**
- Disque local (F:)
- Réseau

Nom	Modifié le	Type	Taille
FTPData	16/09/2025 13:54	Dossier de fichiers	
inetpub	10/09/2025 14:21	Dossier de fichiers	
PerfLogs	01/04/2024 09:02	Dossier de fichiers	
Programmes	10/09/2025 14:16	Dossier de fichiers	
Programmes (x86)	10/09/2025 14:16	Dossier de fichiers	
Scripts	16/09/2025 11:02	Dossier de fichiers	
Utilisateurs	04/09/2025 08:57	Dossier de fichiers	
Windows	16/09/2025 10:33	Dossier de fichiers	

Gestionnaire des services Internet (IIS)

SRV-HYPER-V-GRP > Sites

Fichier Affichage Aide

Connexions

Pages de démarrage
SRV-HYPER-V-GRP (SRV-HYP)
Pools d'applications

Ajouter un site Web...
Actualiser
Ajouter un site FTP...
Basculer vers l'affichage du contenu

Sites

Filtrer: Atteindre Afficher tout Regrouper par: Aucun regroupement

Nom	Identificateur...	État	Liaison	Chemin d'accès
1		Arrêté (Au...		%SystemDrive%\inetpub\wwwroot
2		Démarré (f...	*21: (ftp)	C:\FTPData

Actions

- Ajouter un site Web...
Définir les valeurs par défaut des sites Web...
- Ajouter un site FTP...
Définir les valeurs par défaut des sites FTP...
- Aide

Affichage des fonctionnalités Affichage du contenu

Prêt

Ajouter un site FTP

Informations sur le site

Nom du site FTP :
SAVE_FTP

Répertoire de contenu

Chemin d'accès physique :
C:\FTPData

Précédent Suivant Terminer Annuler



Liaison et paramètres SSL

Liaison

Adresse IP :

172.16.100.1

Port :

21

Activer les noms des hôtes virtuels :

Hôte virtuel (exemple : ftp.contoso.com) :

Démarrer automatiquement le site FTP

SSL

Pas de SSL

Autoriser SSL

Exiger SSL

Certificat SSL :

Non sélectionné

Sélectionner...

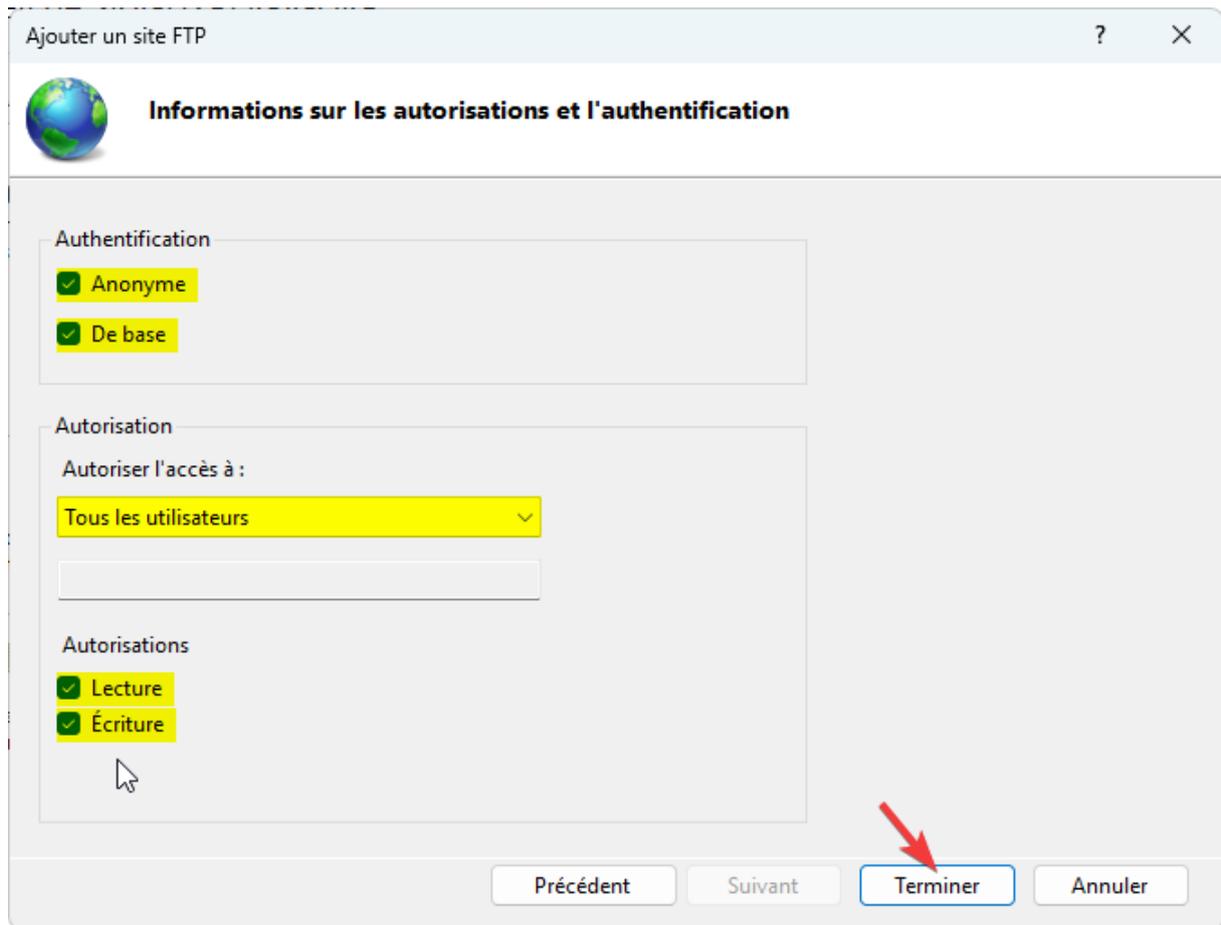
Afficher...

Précédent

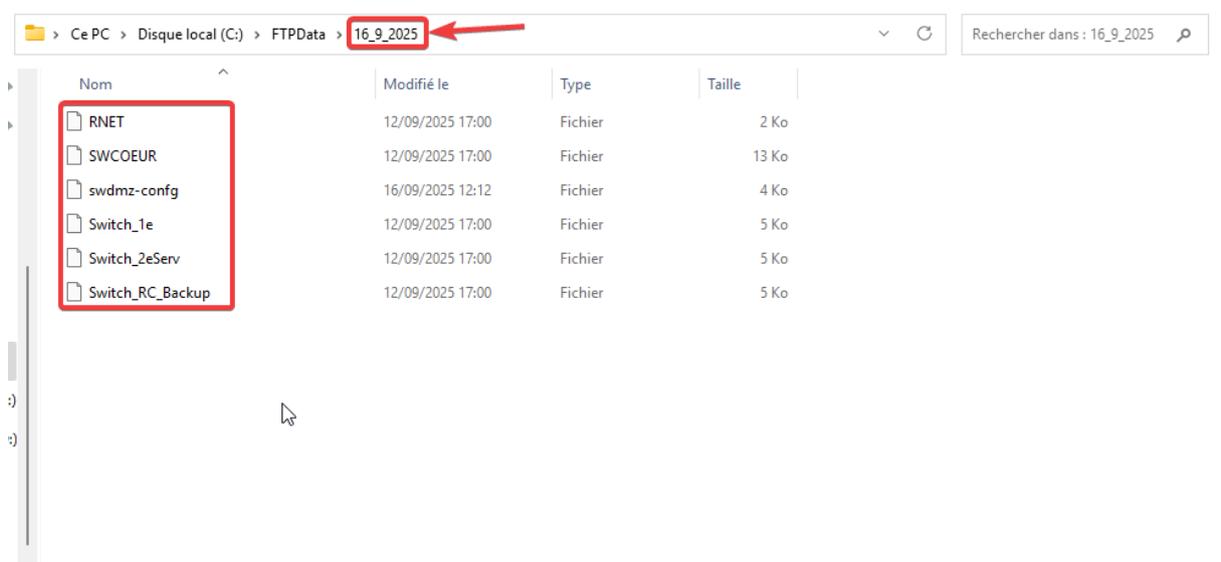
Suivant

Terminer

Annuler



Puis j'ai testé un « Copy running config ftp : 172.16.100.1 » sur le Switch SW2EServ



Donc le serveur FTP fonctionne bien

Sauvegarde automatique des équipements et création du script

Voici la procédure que nous avons établie pour assurer la sauvegarde de chaque équipement :

```
Switch_RC#conf t
Switch_RC(config)#file prompt quiet
Switch_RC(config)# kron policy-list BackupAuto
Switch_RC(config-kron-policy)#cli wr
Switch_RC(config-kron-policy)#cli copy running-config ftp://172.16.100.1/nom-switch
Switch_RC (config-kron-policy)#exit
```

Effectue la politique automatiquement le mardi, mercredi, jeudi, vendredi

```
kron occurrence BackupAutoMardi at 17:00 Tue recurring
policy-list BackupAuto
Exit
kron occurrence BackupAutoMercredi at 17:00 Wed recurring
policy-list BackupAuto
Exit
kron occurrence BackupAutoJeudi at 17:00 Thu recurring
policy-list BackupAuto
Exit
kron occurrence BackupAutoVendredi at 17:00 Fri recurring
policy-list BackupAuto
Exit
```

Le résultat attendu est que chaque switch configuré enregistre sa configuration sur le serveur FTP.

RNET	16/09/2025 17:00	Fichier	3 Ko
startup-config.conf	16/09/2025 17:14	Fichier CONF	37 Ko
SWCOEUR	16/09/2025 17:00	Fichier	13 Ko
SWDMZ	16/09/2025 16:59	Fichier	4 Ko
Switch_1e	16/09/2025 17:00	Fichier	5 Ko
Switch_2eServ	16/09/2025 17:00	Fichier	5 Ko
SwichNET	23/09/2025 11:20	Fichier	4 Ko

Nous pouvons clairement constater que chaque switch ainsi que le routeur ont enregistré leur fichier de configuration. Seul le ZYXEL n'a pas suivi cette méthode, car elle ne fonctionne pas sur cet équipement.

J'ai donc dû créer un script .bat permettant de se connecter en FTP au ZYXEL et d'enregistrer automatiquement le fichier de configuration.

Script :

```
@echo off
echo Connexion au serveur FTP...

set FTP_SERVER=172.16.255.254
set FTP_USER=admin
set FTP_PASS=admin
set REMOTE_PATH=conf
set FILE_NAME=startup-config.conf
set LOCAL_PATH=C:\FTPData

echo open %FTP_SERVER% > ftpcmd.txt
echo user %FTP_USER% %FTP_PASS% >> ftpcmd.txt
echo binary >> ftpcmd.txt
echo cd %REMOTE_PATH% >> ftpcmd.txt
echo get %FILE_NAME% %LOCAL_PATH%\%FILE_NAME% >> ftpcmd.txt
echo bye >> ftpcmd.txt

ftp -n -s:ftpcmd.txt

del ftpcmd.txt

timeout /t 5 /nobreak >nul
exit
```

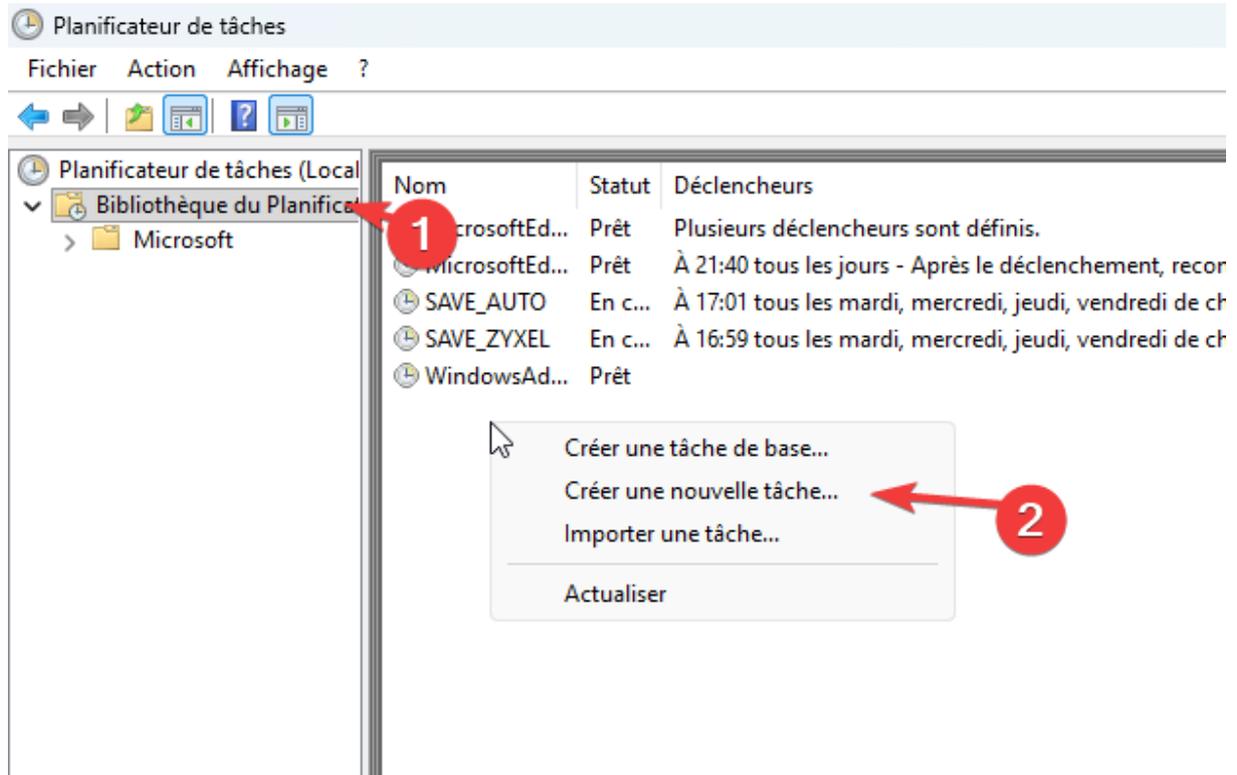
Le résultat attendu lors de l'exécution du script est d'obtenir le fichier de configuration du ZYXEL dans le dossier *FTPData*

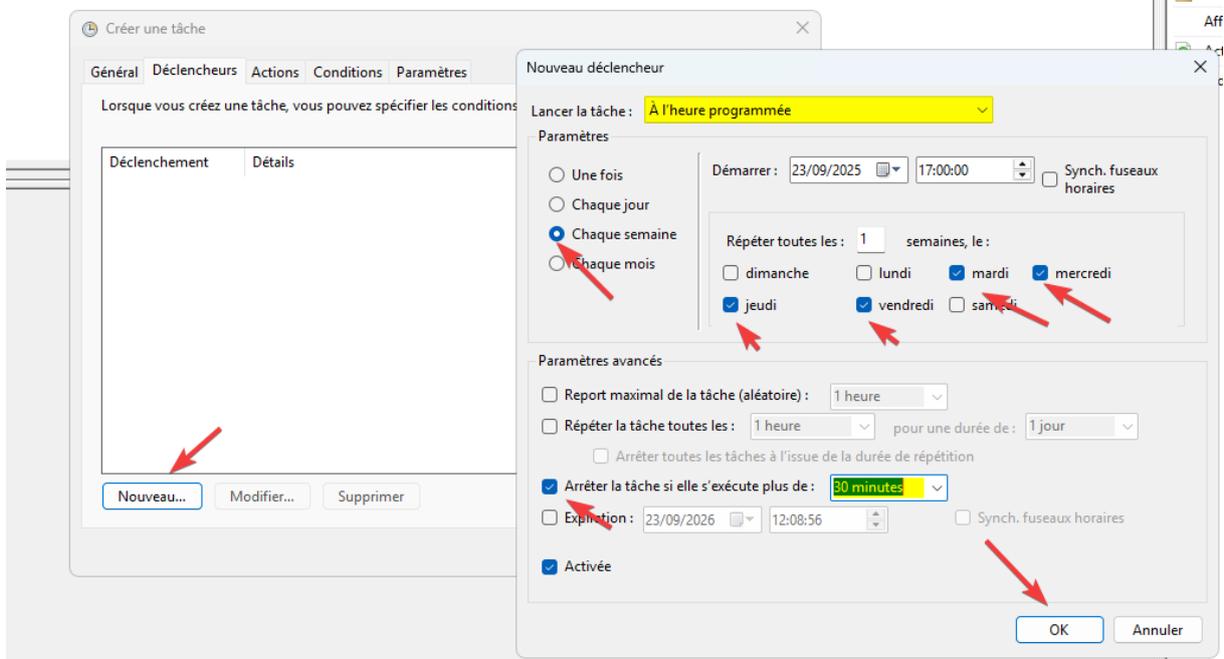
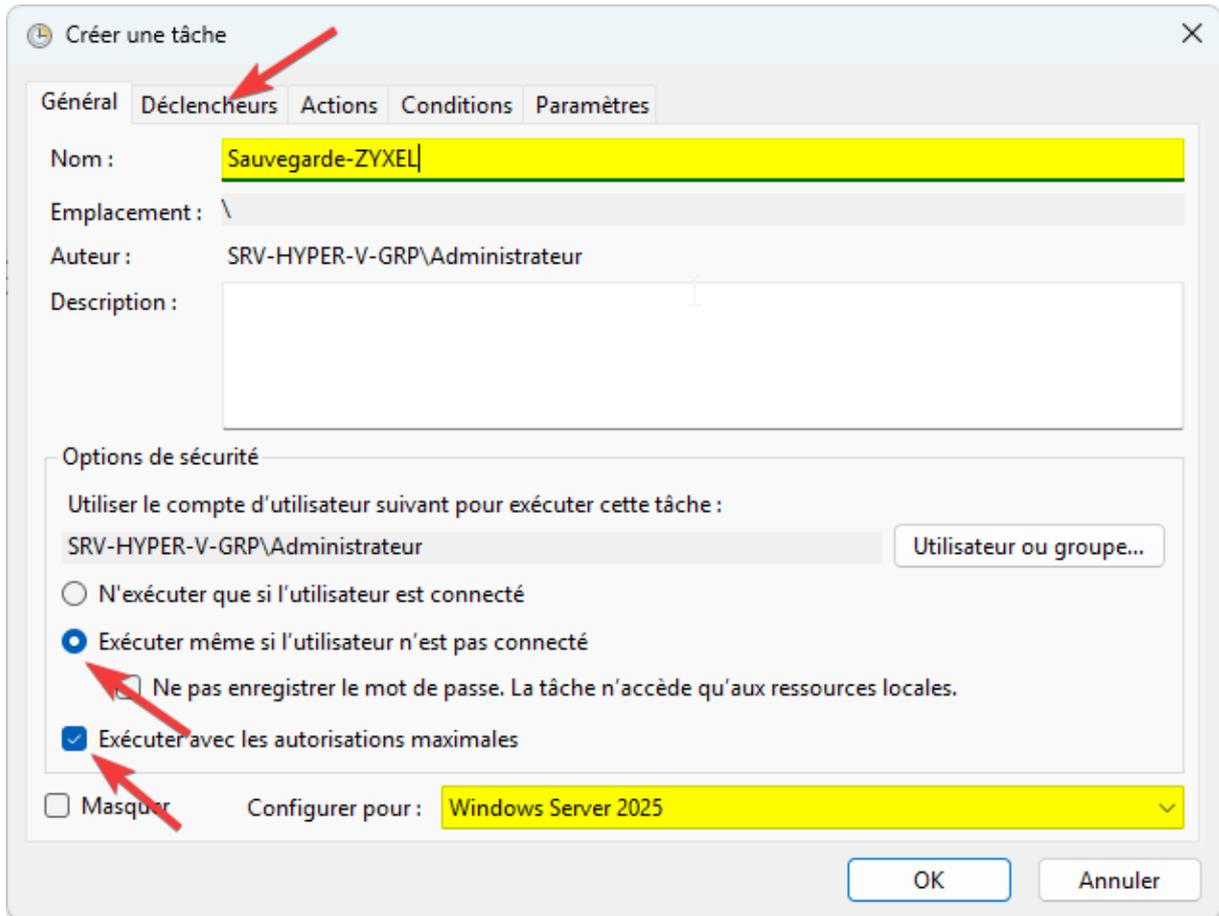
 RNET	18/09/2025 17:00	Fichier	3 Ko
 startup-config.conf	23/09/2025 09:38	Fichier CONF	37 Ko
 SWCOEUR	18/09/2025 17:00	Fichier	13 Ko
 SWDMZ	18/09/2025 16:59	Fichier	4 Ko
 SwichNET	23/09/2025 11:20	Fichier	4 Ko
 Switch_1e	18/09/2025 17:00	Fichier	5 Ko
 Switch_2eServ	18/09/2025 17:00	Fichier	5 Ko
 Switch_RC_Backup	18/09/2025 17:00	Fichier	5 Ko

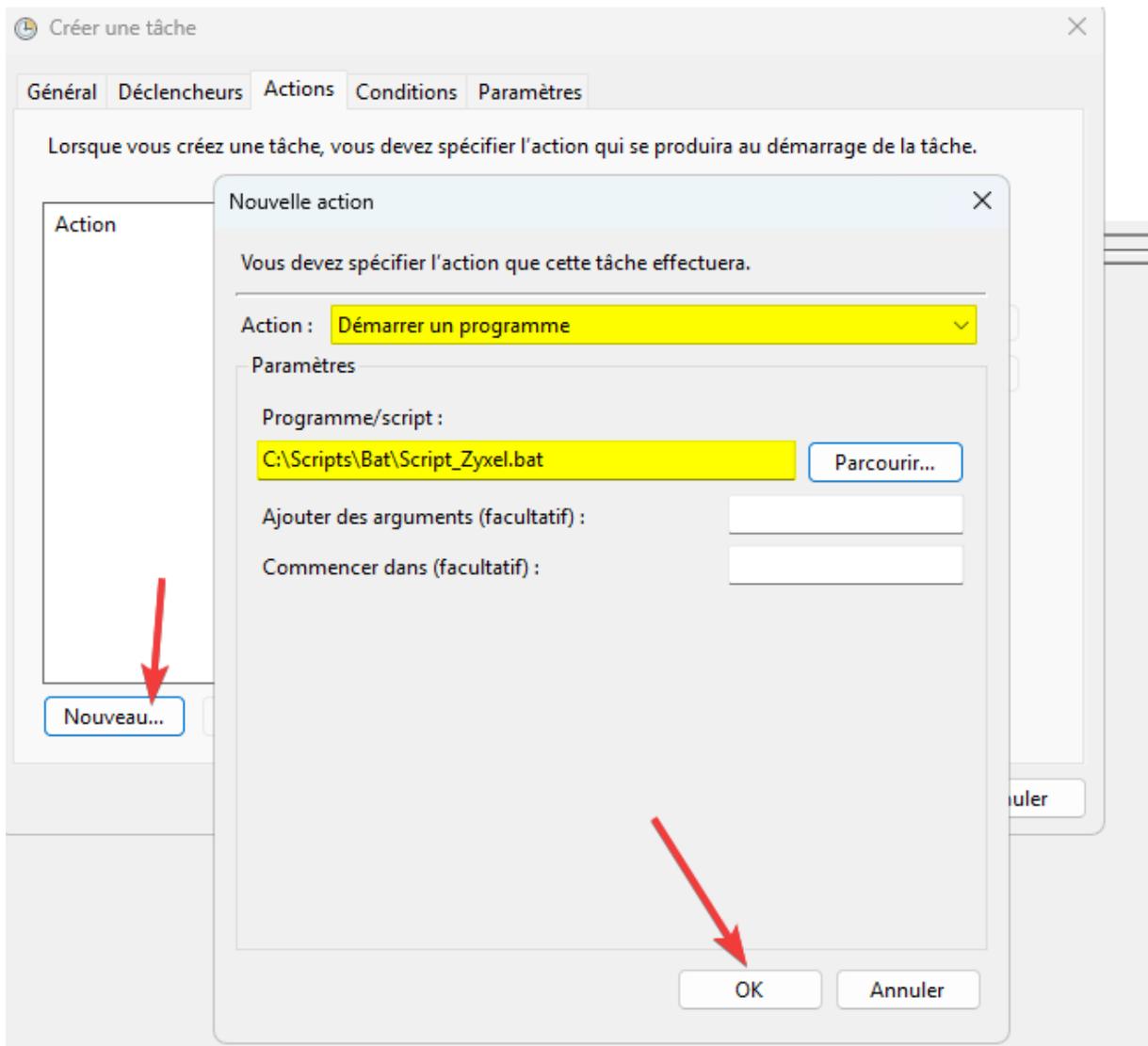
Nous pouvons constater que la sauvegarde a bien été transférée dans le dossier *FTPData*.

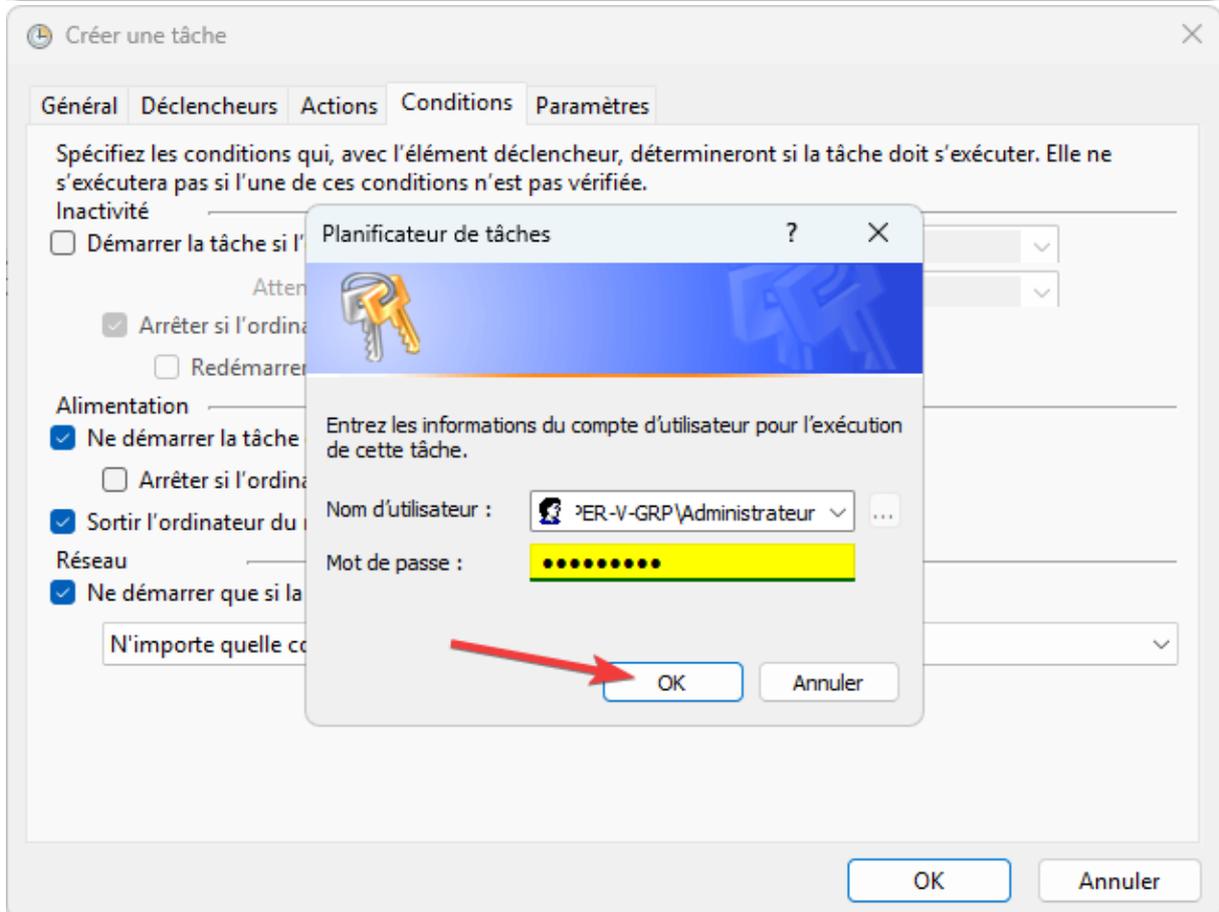
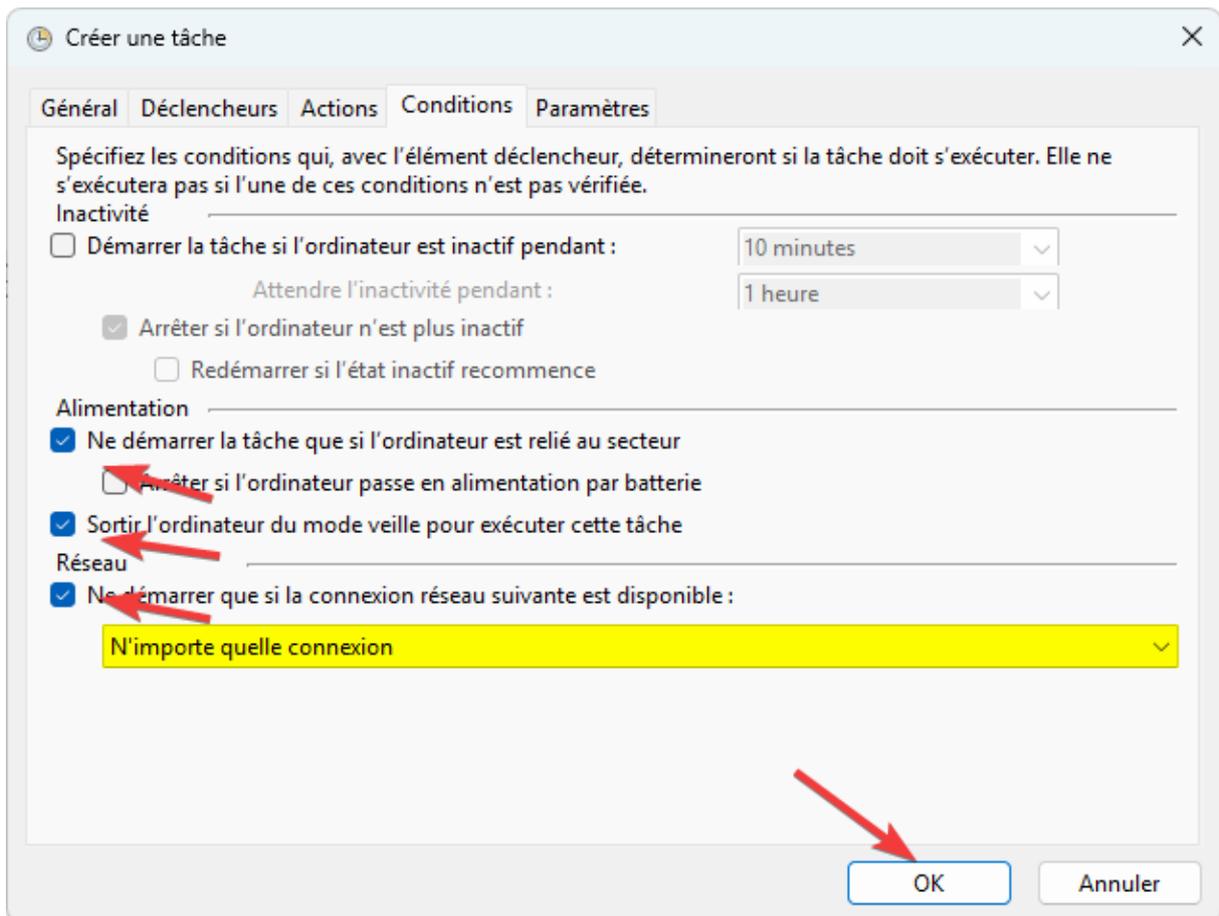
Automatisation du script

Maintenant que le code en .bat fonctionne correctement il faut automatiser l'exécution on se retrouve donc sur le server ftp dans le planificateur de tache



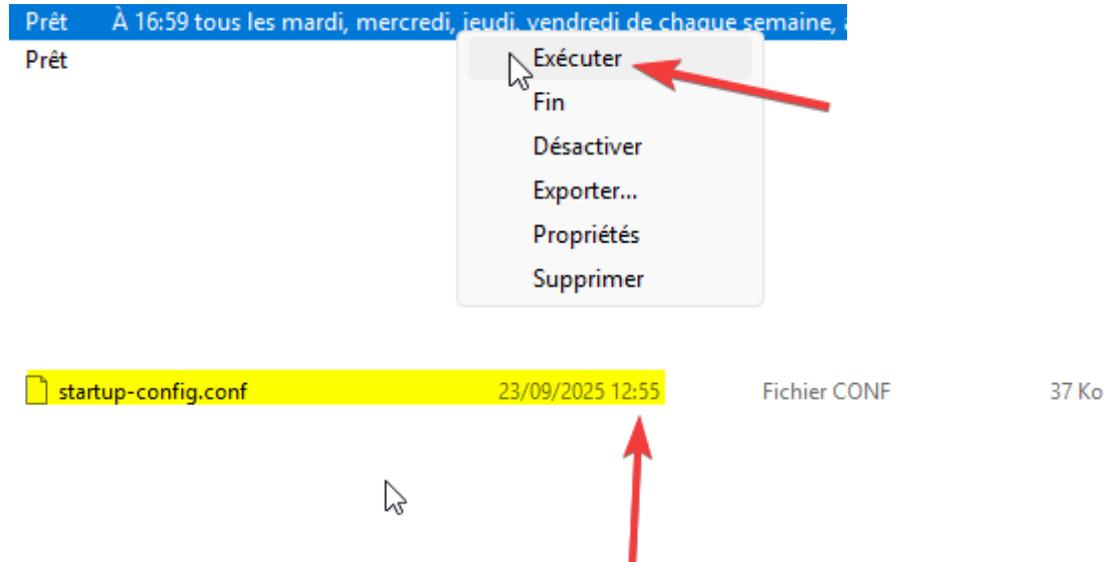






Le résultat attendu, après la configuration, est que les soirs où la sauvegarde est automatisée, le fichier de configuration soit enregistré automatiquement.

Si on clique sur la tâche et que l'on exécute il devrait faire la sauvegarde



L'automatisation de l'exécution de la tâche fonctionne correctement.

Bien que l'automatisation des sauvegardes soit désormais opérationnelle, un problème subsiste : chaque nouvelle sauvegarde écrase la précédente.

J'ai donc écrit un script en Python qui récupère les sauvegardes du jour et les déplace dans un nouveau dossier, situé dans *FTPData* et nommé selon la date du jour au format «jour_mois_année »

Le résultat attendu est que les sauvegardes du jour soient automatiquement déplacées dans un dossier dont le nom suit un format particulier, basé sur la date du jour

Script :

```
#Pour le cree le dossier
import os
#Pour le copier coller
import shutil
#Pour le nom du dossier
from datetime import datetime

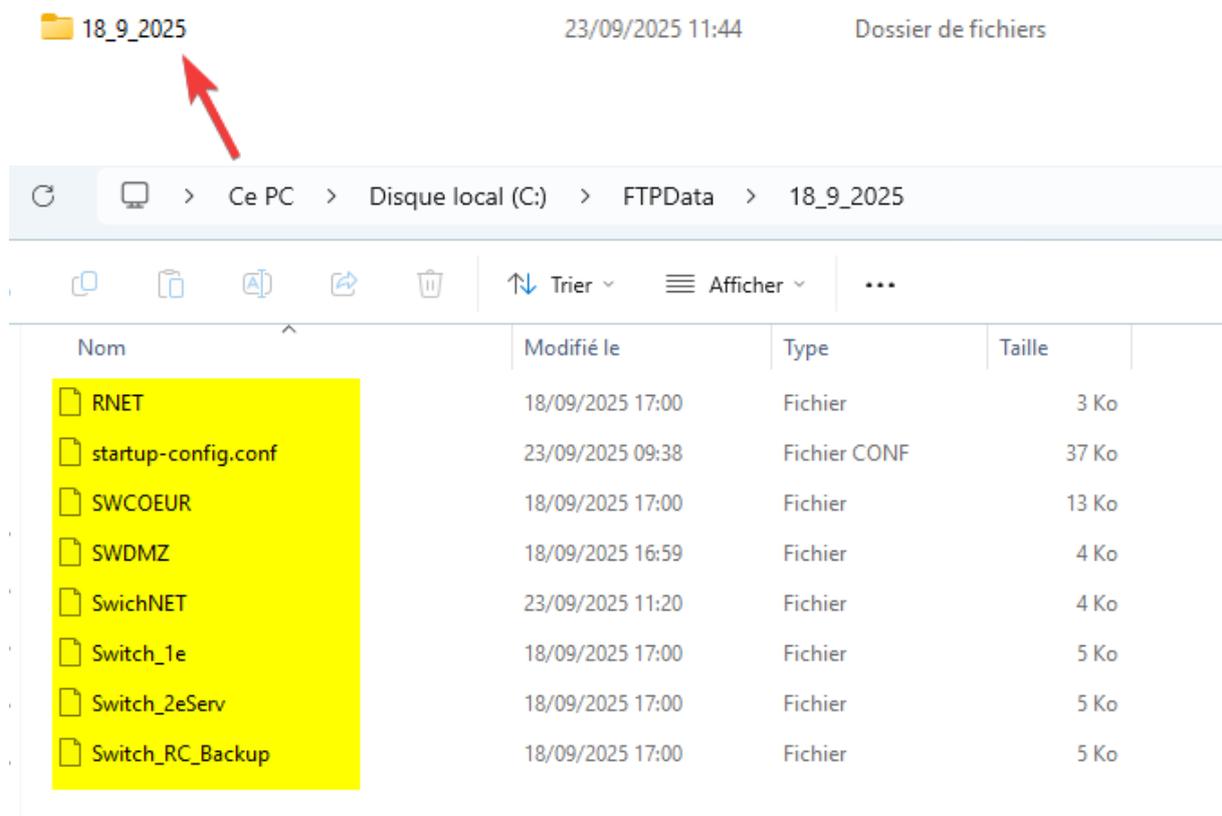
Date = datetime.now()
#Ceation des variable de chemin
FilePathSrc = "C:/FTPData/"
FilePathDst = "C:/FTPData/"+str(Date.day)+'_'+str(Date.month)+'_'+str(Date.year)
#Liste des fichier a copier dans un dossier
Files = ["startup-
config.conf","RNET","SWCOEUR","SWDMZ","Switch_1e","Switch_2eServ","Switch_RC_Backup","S
WDMZ"]

#verification dossier (s'il n'est pas crée il le crée)
```

```
if not os.path.exists(FilePathDst):
    os.mkdir(FilePathDst)

for file in Files:
    try:
        shutil.move(f"{FilePathSrc}{file}", FilePathDst)
    except:
        print("fichier introuvable")
```

Une fois cela fait, il a fallu exécuter le script. Pour cela, j'ai installé la dernière version de Python sur le serveur FTP, puis j'ai lancé le script. Celui-ci a correctement créé un dossier nommé selon la date du jour et y a transféré tous les fichiers de configuration. Le script a donc fonctionné comme prévu.



23/09/2025 11:44 Dossier de fichiers

Ce PC > Disque local (C:) > FTPData > 18_9_2025

Nom	Modifié le	Type	Taille
RNET	18/09/2025 17:00	Fichier	3 Ko
startup-config.conf	23/09/2025 09:38	Fichier CONF	37 Ko
SWCOEUR	18/09/2025 17:00	Fichier	13 Ko
SWDMZ	18/09/2025 16:59	Fichier	4 Ko
SwichNET	23/09/2025 11:20	Fichier	4 Ko
Switch_1e	18/09/2025 17:00	Fichier	5 Ko
Switch_2eServ	18/09/2025 17:00	Fichier	5 Ko
Switch_RC_Backup	18/09/2025 17:00	Fichier	5 Ko

Il faut maintenant automatiser le déplacement des fichiers. Pour cela, nous retournons dans le Planificateur de tâches.

Planificateur de tâches

Fichier Action Affichage ?

Planificateur de tâches (Local)

Bibliothèque du Planificateur de tâches

Microsoft

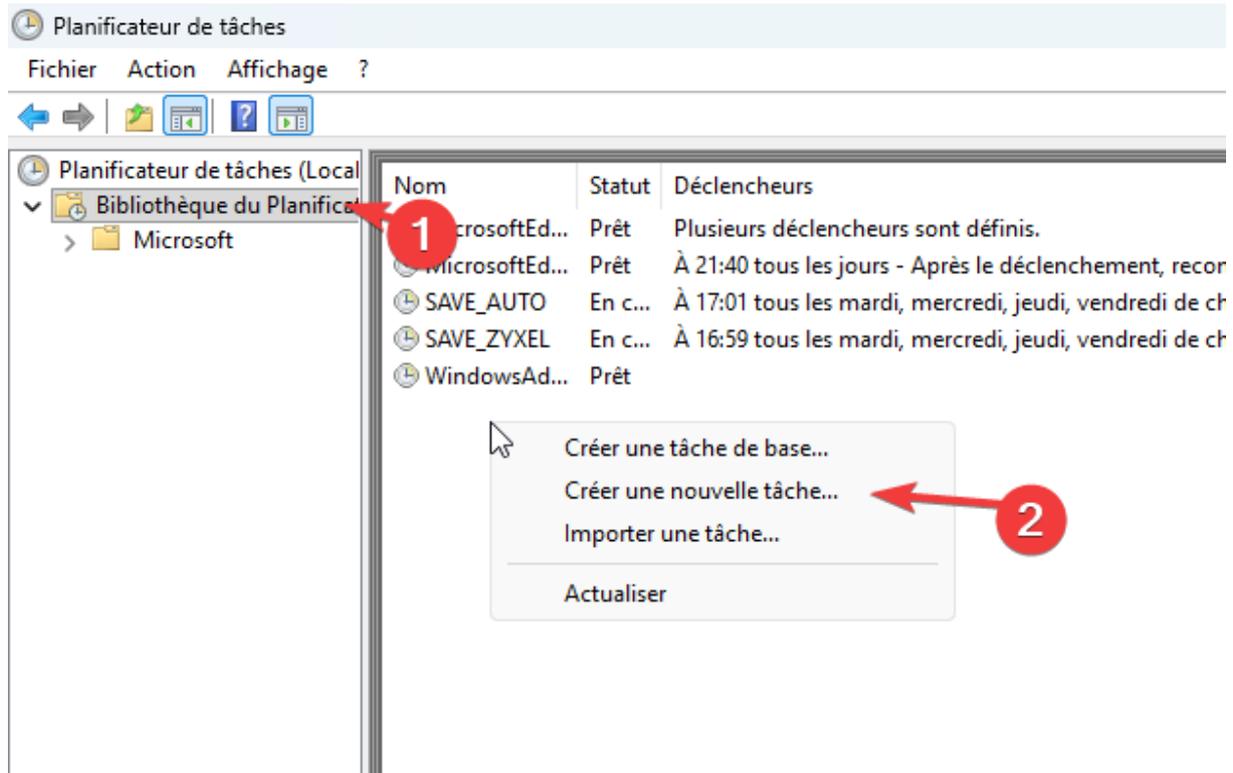
Nom	Statut	Déclencheurs
MicrosoftEd...	Prêt	Plusieurs déclencheurs sont définis.
MicrosoftEd...	Prêt	À 21:40 tous les jours - Après le déclenchement, recor
SAVE_AUTO	En c...	À 17:01 tous les mardi, mercredi, jeudi, vendredi de ch
SAVE_ZYXEL	En c...	À 16:59 tous les mardi, mercredi, jeudi, vendredi de ch
WindowsAd...	Prêt	

Créer une tâche de base...

Créer une nouvelle tâche...

Importer une tâche...

Actualiser



Changer le nom de la tâche par Save_Auto

Créer une tâche

Général Déclencheurs Actions Conditions Paramètres

Nom : Sauvegarde-ZYXEL

Emplacement : \

Auteur : SRV-HYPER-V-GRP\Administrateur

Description :

Options de sécurité

Utiliser le compte d'utilisateur suivant pour exécuter cette tâche :
SRV-HYPER-V-GRP\Administrateur

N'exécuter que si l'utilisateur est connecté

Exécuter même si l'utilisateur n'est pas connecté

Ne pas enregistrer le mot de passe. La tâche n'accède qu'aux ressources locales.

Exécuter avec les autorisations maximales

Masquer

Configurer pour : Windows Server 2025

OK Annuler

Créer une tâche

Général Déclencheurs Actions Conditions Paramètres

Lorsque vous créez une tâche, vous pouvez spécifier les conditions

Déclenchement Détails

Nouveau... Modifier... Supprimer

Nouveau déclencheur

Lancer la tâche : À l'heure programmée

Paramètres

Une fois

Chaque jour

Chaque semaine

Chaque mois

Démarrer : 23/09/2025 17:00:00

Synch. fuseaux horaires

Répéter toutes les : 1 semaines, le :

dimanche lundi mardi mercredi

jeudi vendredi samedi

Paramètres avancés

Report maximal de la tâche (aléatoire) : 1 heure

Répéter la tâche toutes les : 1 heure pour une durée de : 1 jour

Arrêter toutes les tâches à l'issue de la durée de répétition

Arrêter la tâche si elle s'exécute plus de : 30 minutes

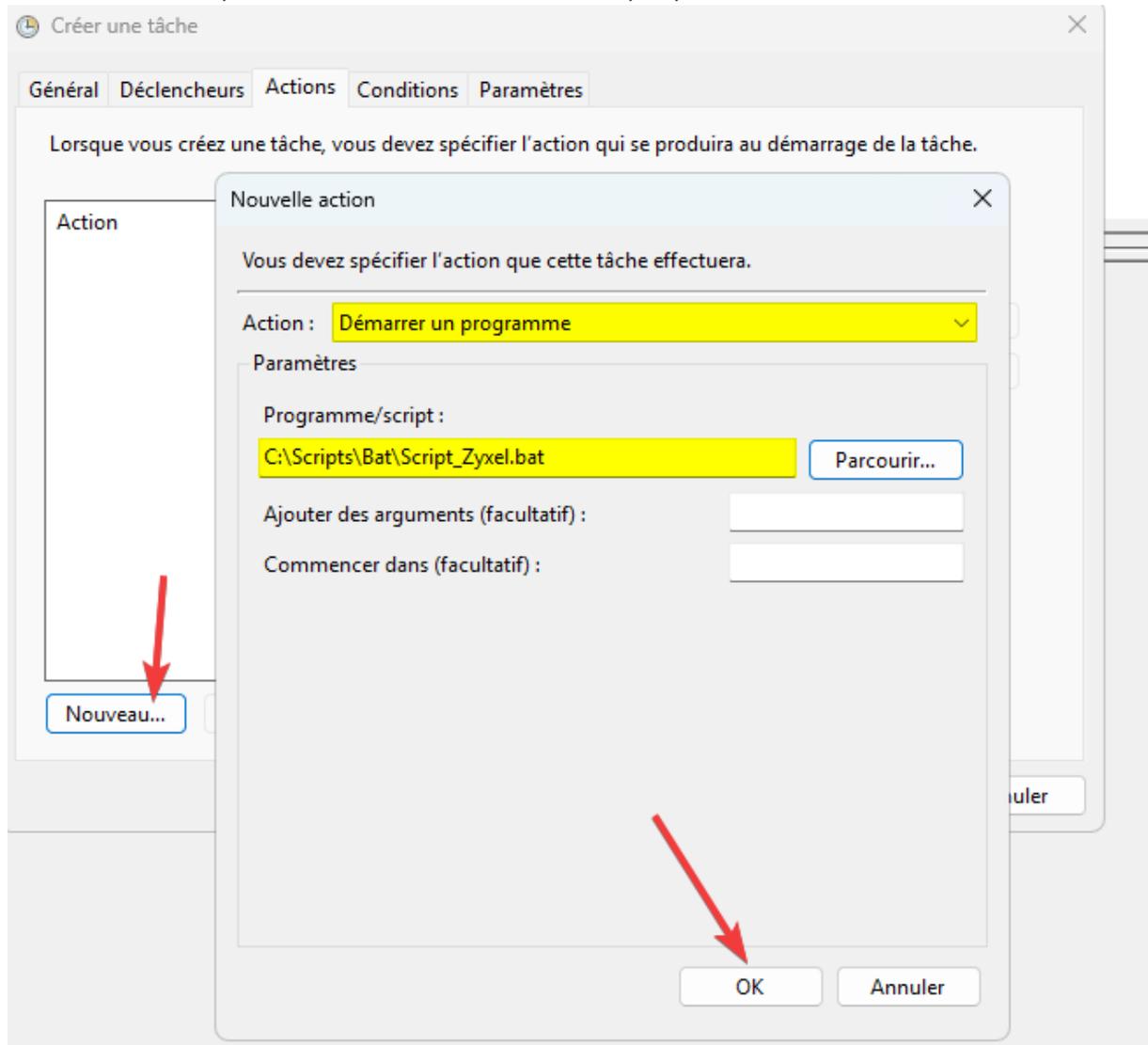
Expiration : 23/09/2026 12:08:56

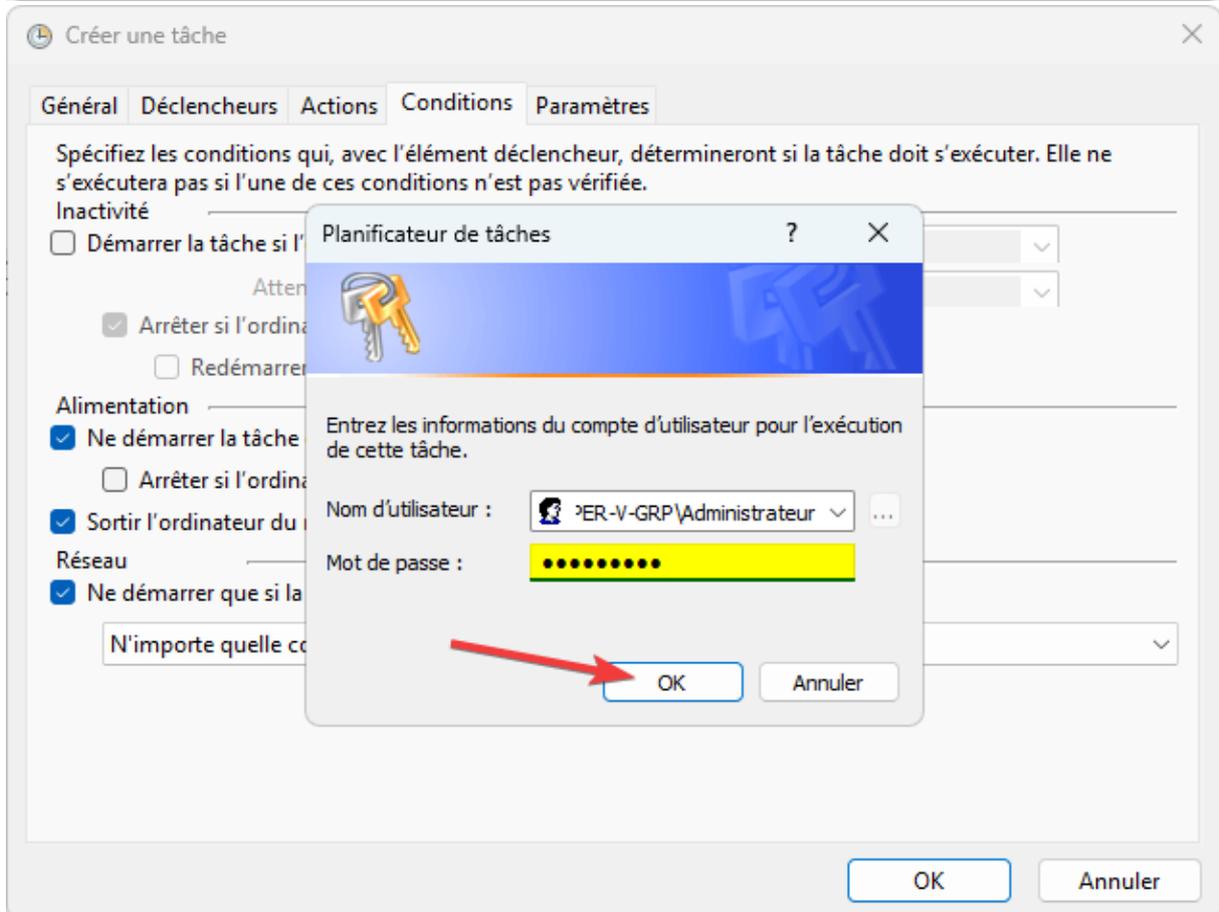
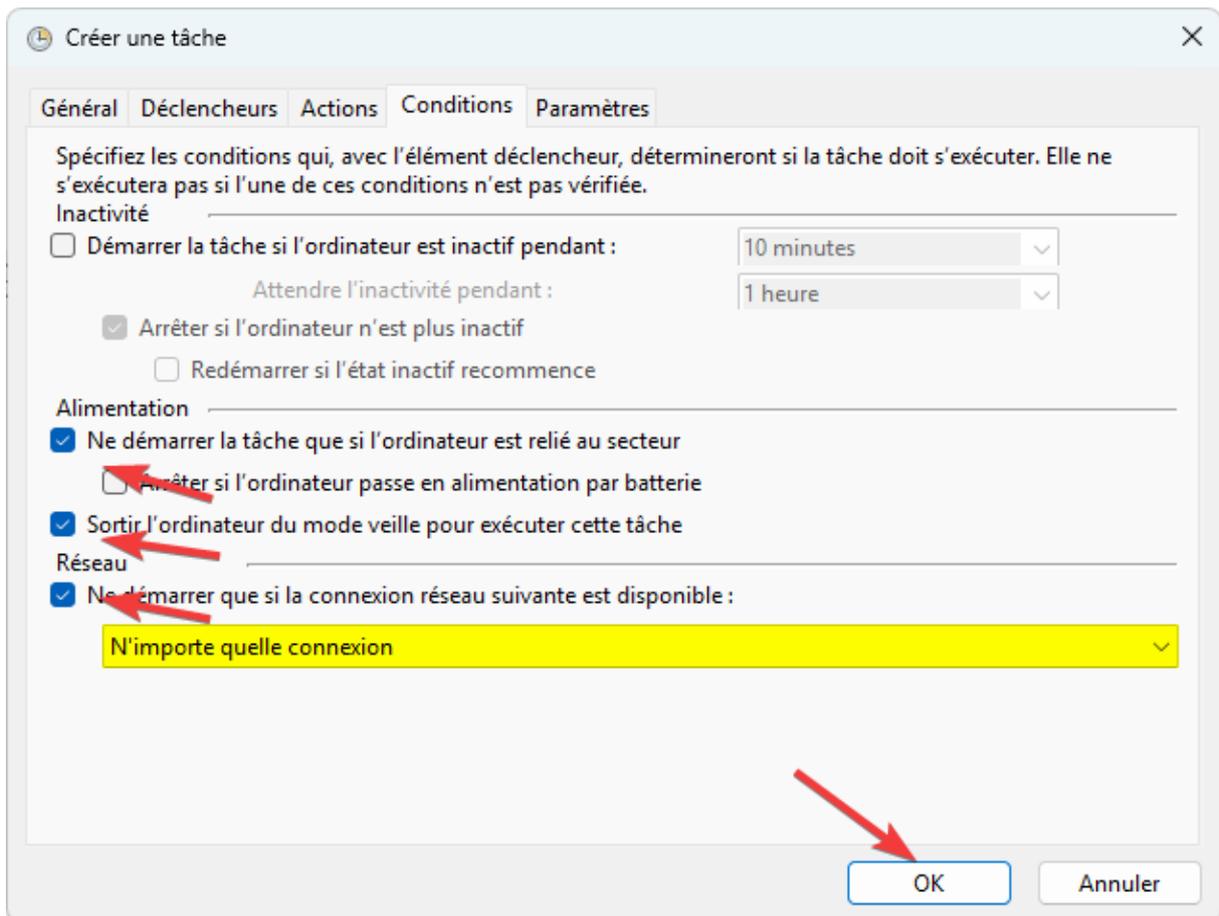
Synch. fuseaux horaires

Activée

OK Annuler

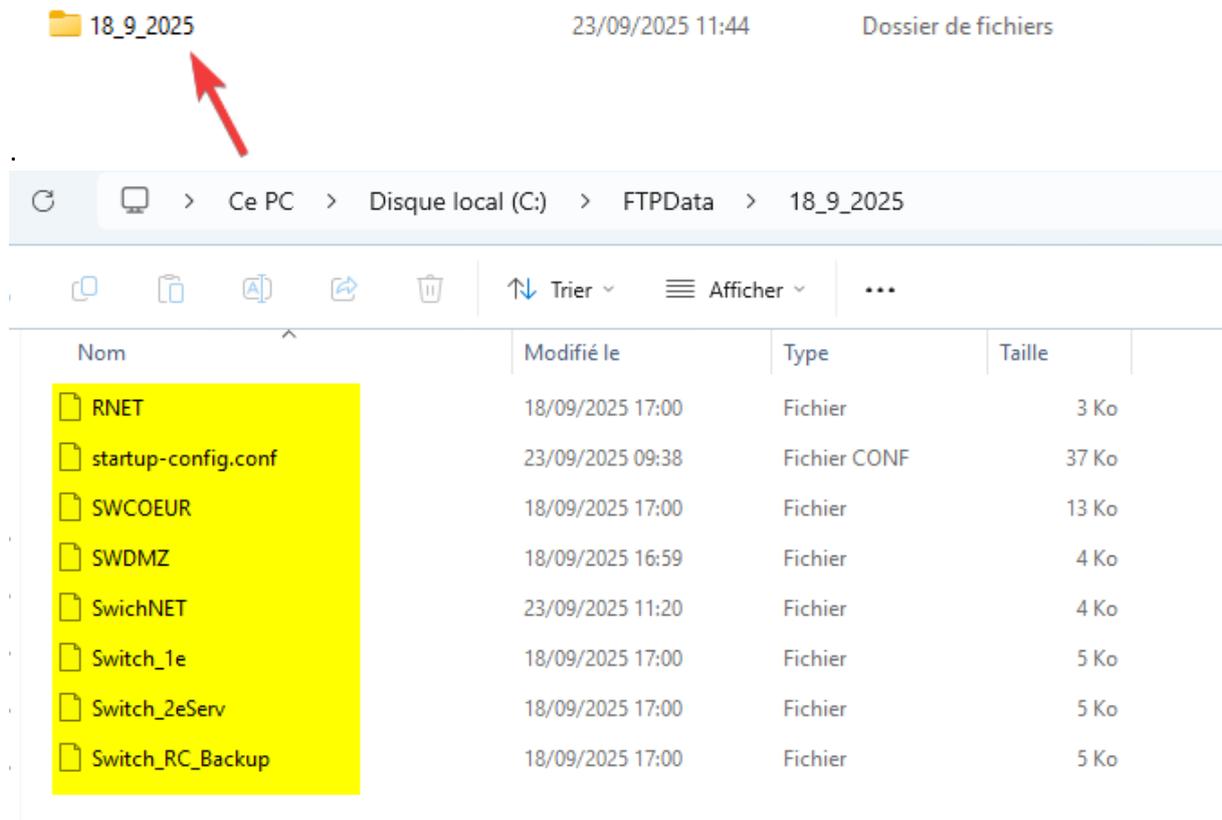
Sélectionner le script à exécuter, en l'occurrence le script Python





Il suffit ensuite de cliquer sur 'OK' pour valider la tâche.

Le résultat attendu, après la configuration, est que les soirs où la sauvegarde est automatisée, la sauvegarde soit transférée dans un dossier nommé selon la date du jour.



Le script a été automatisé avec succès.

3.3 Paramétrage des routes sur le Routeur Pare-feu

Configuration du routeur ZYXEL (protocoles RIP et route par défaut).

Paramétrage des routes sur le Routeur Pare-feu

Avec le protocole RIP, nous devons disposer de toutes les routes accessibles, ainsi que d'une Route par défaut pour pouvoir accéder à Internet

```
router rip
version 2
network wan1
network lan1
network dmz
```

```
Router# ping 172.16.255.253
PING 172.16.255.253 (172.16.255.253) 56(84) bytes of data.
64 bytes from 172.16.255.253: icmp_seq=1 ttl=254 time=1.59 ms
64 bytes from 172.16.255.253: icmp_seq=2 ttl=254 time=1.53 ms
64 bytes from 172.16.255.253: icmp_seq=3 ttl=254 time=1.57 ms

--- 172.16.255.253 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.539/1.568/1.595/0.039 ms
Router# ping 172.16.70.254
PING 172.16.70.254 (172.16.70.254) 56(84) bytes of data.
64 bytes from 172.16.70.254: icmp_seq=1 ttl=254 time=1.56 ms
64 bytes from 172.16.70.254: icmp_seq=2 ttl=254 time=1.85 ms
64 bytes from 172.16.70.254: icmp_seq=3 ttl=254 time=1.60 ms

--- 172.16.70.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.567/1.674/1.851/0.126 ms
Router# ping 172.16.100.1
PING 172.16.100.1 (172.16.100.1) 56(84) bytes of data.
64 bytes from 172.16.100.1: icmp_seq=1 ttl=127 time=0.322 ms
64 bytes from 172.16.100.1: icmp_seq=2 ttl=127 time=0.299 ms
64 bytes from 172.16.100.1: icmp_seq=3 ttl=127 time=0.297 ms

--- 172.16.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.297/0.306/0.322/0.011 ms
```

```
ip route 0.0.0.0 0.0.0.0 192.168.3.254
```

Toutes les routes sont correctement paramétrées sur le ZYXEL, ce qui nous permet d'accéder à l'ensemble de notre réseau local ainsi qu'à Internet, comme le confirme la réussite des tests de ping

3.4 Paramétrage des routes sur le Switch cœur

Configuration du Switch cœur (protocoles RIP et route par défaut).

Avec le protocole RIP, nous devons disposer de toutes les routes accessibles, ainsi que d'une route par défaut pour pouvoir accéder à Internet.

```

SWCOEUR#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 172.16.255.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.16.255.254
      10.0.0.0/16 is subnetted, 1 subnets
R     10.1.0.0 [120/1] via 172.16.255.254, 00:00:11, Vlan200
      172.16.0.0/16 is variably subnetted, 20 subnets, 3 masks
C     172.16.10.0/24 is directly connected, Vlan10
L     172.16.10.254/32 is directly connected, Vlan10
C     172.16.20.0/24 is directly connected, Vlan20
L     172.16.20.254/32 is directly connected, Vlan20
C     172.16.30.0/24 is directly connected, Vlan30
L     172.16.30.254/32 is directly connected, Vlan30
C     172.16.40.0/24 is directly connected, Vlan40
L     172.16.40.254/32 is directly connected, Vlan40
C     172.16.50.0/24 is directly connected, Vlan50
L     172.16.50.254/32 is directly connected, Vlan50
C     172.16.60.0/24 is directly connected, Vlan60
L     172.16.60.254/32 is directly connected, Vlan60
C     172.16.70.0/24 is directly connected, Vlan70
L     172.16.70.254/32 is directly connected, Vlan70
C     172.16.80.0/24 is directly connected, Vlan80
L     172.16.80.254/32 is directly connected, Vlan80
C     172.16.100.0/24 is directly connected, Vlan100
L     172.16.100.254/32 is directly connected, Vlan100
C     172.16.255.252/30 is directly connected, Vlan200
L     172.16.255.253/32 is directly connected, Vlan200
      192.168.3.0/29 is subnetted, 1 subnets
R     192.168.3.248 [120/1] via 172.16.255.254, 00:00:11, Vlan200
SWCOEUR#

```

```

SWCOEUR#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/13/24 ms
SWCOEUR#

```

Toutes les routes sont correctement paramétrées sur le switch cœur, ce qui nous permet d'accéder à l'ensemble de notre réseau local ainsi qu'à Internet, comme le confirme la réussite des tests de ping.

3.5 Configuration RNET1

Paramétrage du routeur RNET1 (RIP, route par défaut, NAT statique, et PAT).

Configuration_RNET1

Paramétrage des interfaces du routeur (@IP)

```

interface GigabitEthernet0/0
 ip address 192.168.4.12 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.3.251 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!

```

Pour la configuration automatique du routage nous avons dû mettre en place le RIP V2 sur le routeur. J'ai déclaré que la gi 0/0 devait être une passive interface car elle est reliée à notre FAI et il ne doit pas recevoir les routes de mon LAN.

```

router rip
 version 2
 passive-interface GigabitEthernet0/0
 network 192.168.3.0
 no auto-summary

```

Ajout d'une route par défaut pour pouvoir accéder à internet

```

S* 0.0.0.0/0 [1/0] via 192.168.4.254
    10.0.0.0/16 is subnetted, 1 subnets

```

Mise en place du NAT et du PAT sur le routeur : deux NAT statique ont été configuré pour permettre l'accès à un serveur situé dans la DMZ et pour accéder au server AD pour SSH les équipements, tandis qu'un PAT a été mis en œuvre afin de permettre à l'ensemble du réseau local (LAN) d'accéder à Internet.

```
ip nat inside source list NET_LAN interface GigabitEthernet0/0 overload
ip nat inside source static 10.1.10.1 192.168.4.13
ip nat inside source static 172.16.100.2 192.168.4.14
ip route 0.0.0.0 0.0.0.0 192.168.4.254
```

Paramétrage du NAT Intérieur et Extérieur sur les interfaces

```
interface GigabitEthernet0/0
 ip address 192.168.4.12 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.3.251 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
```

Ajout d'un server NTP pour la synchronisation du temps pour résoudre un problème rencontré dans la mise en place de la sauvegarde automatique

```
!
scheduler allocate 20000 1000
ntp server 0.fr.pool.ntp.org prefer
!
```

Paramétrage d'un script pour la sauvegarde automatique sur les équipements

```
kron occurrence BackupAutoVendredi at 17:00 Fri recurring
policy-list BackupAuto
!
kron occurrence BackupAutoMardi at 17:00 Tue recurring
policy-list BackupAuto
!
kron occurrence BackupAutoMercredi at 17:00 Wed recurring
policy-list BackupAuto
!
kron occurrence BackupAutoJeudi at 17:00 Thu recurring
policy-list BackupAuto
!
kron policy-list BackupAuto
cli wr
cli copy running-config ftp://172.16.100.1/RNET
```

4 Sécurisation des équipements d'interconnexion

Permettre à l'équipe IT d'accéder à distance à tous les nouveaux équipements depuis le LAN et Internet, tout en respectant le cahier des charges. Nous avons suivi cette procédure pour la configuration des équipements :

Procédure de sécurisation des équipements cisco

Mise en place du ssh :

```
Ip domain-name saveol.local
username admin secret admin
crypto key generate rsa modulus 2048
line vty 0 4
transport input ssh
login local
exit
```

Mise en place du mot de passe pour l'accès par câble console :

```
line console 0
password admin
login local
```

Désactivation des ports non utilisés :

```
Interface fa0/X
Shutdown
```

4.1 Définir les ACL Zyxel

Implémentation des ACL sur le ZYXEL.

Zyxel

Permit https , dns , ftp (dev) Lan->DMZ

Permit https , dns , ftp WAN->DMZ

Permit HTTPS LAN->WAN

Prior...	Status	Name	From	To	IPv4 Source	IPv4 Destinati...	Service	Device	User	Schedule	Acti...	Log	Profile
1		WAN_SRV_LAN	WAN	LAN1	any	SRV_AD	RDP	any	any	none	allow	no	
2		SRV_LAN_WAN_SSH	LAN1	WAN	SRV_AD	EQUIPEMEN...	SSH	any	any	none	allow	no	
3		SRV_LAN_DMZ_SSH	LAN1	DMZ	SRV_AD	SWDMZ	SSH	any	any	none	allow	no	
4		IT_LAN_PING	LAN1	any [Excludi...	IT_LAN	any	PING	any	any	none	allow	no	
5		IT_LAN_WAN_SSH	LAN1	WAN	IT_LAN	EQUIPEMEN...	SSH	any	any	none	allow	no	
6		IT_LAN_DMZ_SSH	LAN1	DMZ	IT_LAN	SWDMZ	SSH	any	any	none	allow	no	
7		WAN_DMZ_FTP	WAN	DMZ	any	SRV_DMZ	FTP	any	any	none	allow	no	
8		LAN_DMZ_HTTPS	LAN1	DMZ	any	SRV_DMZ	HTTPS	any	any	none	allow	no	
9		LAN_DMZ_DNS	LAN1	DMZ	any	any	DNS	any	any	none	allow	no	
10		NIP_DMZ	DMZ	ZyWALL	SWDMZ	any	NIP	any	any	none	allow	no	
11		NIP_LAN	LAN1	ZyWALL	SWCOEUR	any	NIP	any	any	none	allow	no	
12		SAVE_WAN	WAN	LAN1	EQUIPEMEN...	SRV_HYPERV	FTP	any	any	none	allow	no	
13		SAVE_DMZ	DMZ	LAN1	SWDMZ	SRV_HYPERV	FTP	any	any	none	allow	no	
14		LAN1_DNS	LAN1	WAN	SRV_AD	any	DNS	any	any	none	allow	no	
15		LAN1_HTTPS	LAN1	WAN	any	any	HTTPS	any	any	none	allow	no	
16		DMZ_to_WAN	DMZ	WAN	SRV_DMZ	any	any	any	any	none	allow	no	
17		IPSec_VPN_Outgoing	IPSec_VPN	any [Excludi...	any	any	any	any	any	none	allow	no	
18		SSL_VPN_Outgoing	SSL_VPN	any [Excludi...	any	any	any	any	any	none	allow	no	
19		TUNNEL_Outgoing	TUNNEL	any [Excludi...	any	any	any	any	any	none	allow	no	
20		LAN1_to_Device	LAN1	ZyWALL	IT_LAN	any	any	any	any	none	allow	no	
21		LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	any	none	allow	no	
22		DMZ_to_Device	DMZ	ZyWALL	any	any	Default_All...	any	any	none	allow	no	
23		WAN_to_Device	WAN	ZyWALL	any	any	Default_All...	any	any	none	allow	no	
24		IPSec_VPN_to_Device	IPSec_VPN	ZyWALL	any	any	any	any	any	none	allow	no	
25		SSL_VPN_to_Device	SSL_VPN	ZyWALL	any	any	any	any	any	none	allow	no	
26		TUNNEL_to_Device	TUNNEL	ZyWALL	any	any	any	any	any	none	allow	no	
		Def...	any	any	any	any	any	any	any	none	deny	log	

4.2 Résolution Zyxel

Gestion des divers problèmes rencontrés avec le ZyXEL.

Nous avons rencontré plusieurs soucis avec le ZyXEL, notamment le fait que les ACL ne s'appliquaient qu'après un redémarrage.

Après une réinitialisation pour tenter de résoudre le problème, le ZyXEL a activé le NAT par défaut, ce qui nous a coûté 20 heures de recherche pour identifier la panne, alors que la cause était que l'interface WAN était en mode externe. Actuellement, nous rencontrons encore un problème : lorsque nous appliquons les ACL, le protocole RIP ne fonctionne plus.

4.3 Définir les ACL SWCOEUR

Mise en œuvre des ACL sur le Switch Cœur.

Seul les VLANs **100,80,70,60** ne sont pas concernée par les access list du switch cœur ils ont le droit a tout.

ACL VLAN]100,80,70,60[

```
deny tcp any 172.16.100.0 0.0.0.255 eq 22 ssh
```

```
deny tcp any 172.16.100.0 0.0.0.255 eq 69 ftp
```

```
deny icmp any 172.16.100.0 0.0.0.255 ping
```

```
permit ip any 172.16.100.0 0.0.0.255
```

```
deny ip any 172.16.0.0 0.0.255.255
```

```
permit ip any any
```

```
interface Vlan10
 ip address 172.16.10.254 255.255.255.0
 ip access-group LAN in
!
interface Vlan20
 ip address 172.16.20.254 255.255.255.0
 ip access-group LAN in
!
interface Vlan30
 ip address 172.16.30.254 255.255.255.0
 ip access-group LAN in
!
interface Vlan40
 ip address 172.16.40.254 255.255.255.0
 ip access-group LAN in
!
interface Vlan50
 ip address 172.16.50.254 255.255.255.0
 ip access-group LAN in
!
interface Vlan60
 ip address 172.16.60.254 255.255.255.0
!
interface Vlan70
 ip address 172.16.70.254 255.255.255.0
!
interface Vlan80
 ip address 172.16.80.254 255.255.255.0
!
interface Vlan100
 ip address 172.16.100.254 255.255.255.0
!
interface Vlan200
 ip address 172.16.255.253 255.255.255.252
```

```
Extended IP access list LAN
 10 deny tcp any 172.16.100.0 0.0.0.255 eq 22
 20 deny tcp any 172.16.100.0 0.0.0.255 eq 69
 30 deny icmp any 172.16.100.0 0.0.0.255 (11 matches)
 40 permit ip any 172.16.100.0 0.0.0.255
 50 deny ip any 172.16.0.0 0.0.255.255
 60 permit ip any any (1 match)
```

Configuration IP du pc de test dans le VLAN 20

```

Carte Ethernet Ethernet :
    Suffixe DNS propre à la connexion. . . . :
    Description. . . . . : Realtek PCIe GbE Family Controller
    Adresse physique . . . . . : FC-34-97-80-5D-A2
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . . : Oui
    Adresse IPv6 de liaison locale. . . . . : fe80::51d0:3070:7506:3a%2(préféré)
    Adresse IPv4. . . . . : 172.16.20.1(préféré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : mardi 23 septembre 2025 15:25:47
    Bail expirant. . . . . : mercredi 24 septembre 2025 15:34:06
    Passerelle par défaut. . . . . : 172.16.20.254
    Serveur DHCP . . . . . : 172.16.20.254
    IAID DHCPv6 . . . . . : 217855127
    DUID de client DHCPv6. . . . . : 00-01-00-01-30-49-A5-50-FC-34-97-80-5D-A2
    Serveurs DNS. . . . . : 172.16.100.2
    NetBIOS sur Tcpi. . . . . : Activé

```

Test ping entre 2 hôtes dans un même VLAN (réussi)

La connexion doit réussir car nous autorisons les pings entre deux hôtes

```

Statistiques Ping pour 172.16.20.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

C:\Users\Cyprien>ping 172.16.20.2

Envoi d'une requête 'Ping' 172.16.20.2 avec 32 octets de données :
Réponse de 172.16.20.2 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.20.2 : octets=32 temps=1 ms TTL=128
Réponse de 172.16.20.2 : octets=32 temps<1ms TTL=128
Réponse de 172.16.20.2 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 172.16.20.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

```

Test ping entre un hôte et la Gateway (échec)

La connexion doit échouer car nous n'autorisons pas les pings vers la gateway

```
C:\Users\Cyprien>ping 172.16.20.254

Envoi d'une requête 'Ping' 172.16.20.254 avec 32 octets de données :
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 172.16.20.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

C:\Users\Cyprien>ping 172.16.30.254

Envoi d'une requête 'Ping' 172.16.30.254 avec 32 octets de données :
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 172.16.30.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

C:\Users\Cyprien>ping 172.16.40.254

Envoi d'une requête 'Ping' 172.16.40.254 avec 32 octets de données :
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 172.16.40.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

C:\Users\Cyprien>
```

Test de connexion LDAP depuis un pc hôte (réussi)

La connexion doit réussir car nous autorisons les connexions LDAP dans les ACL

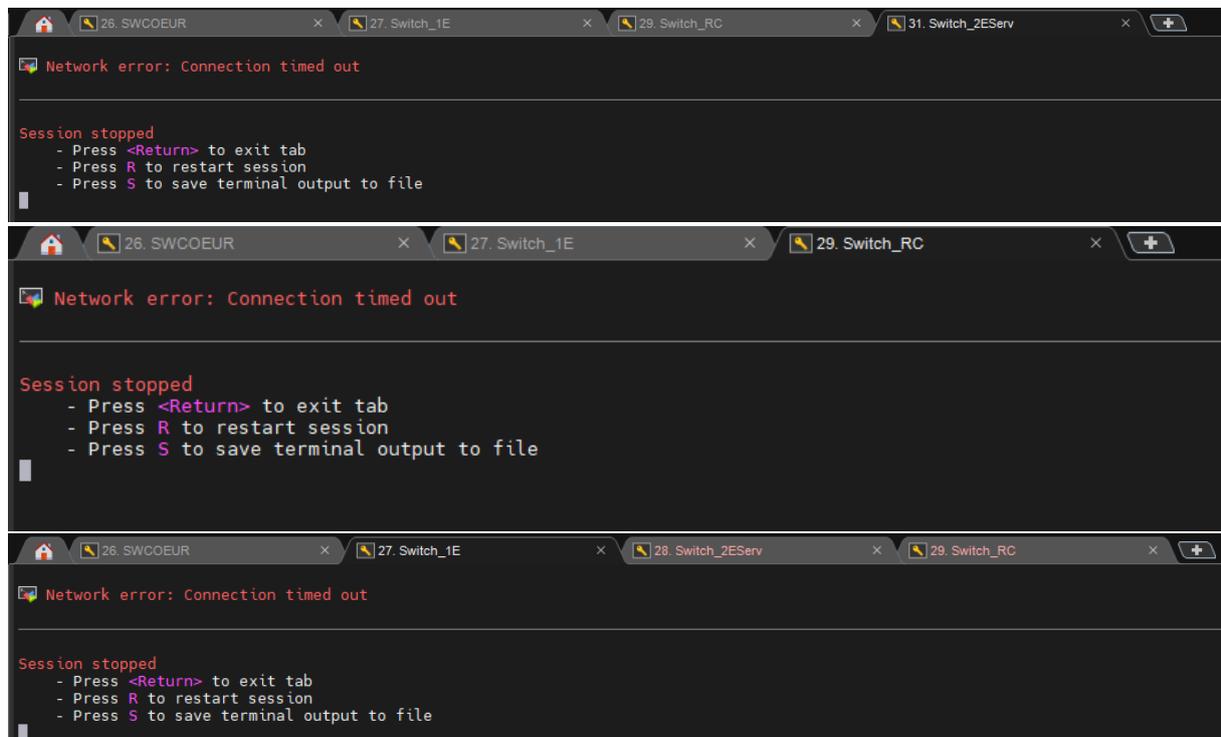


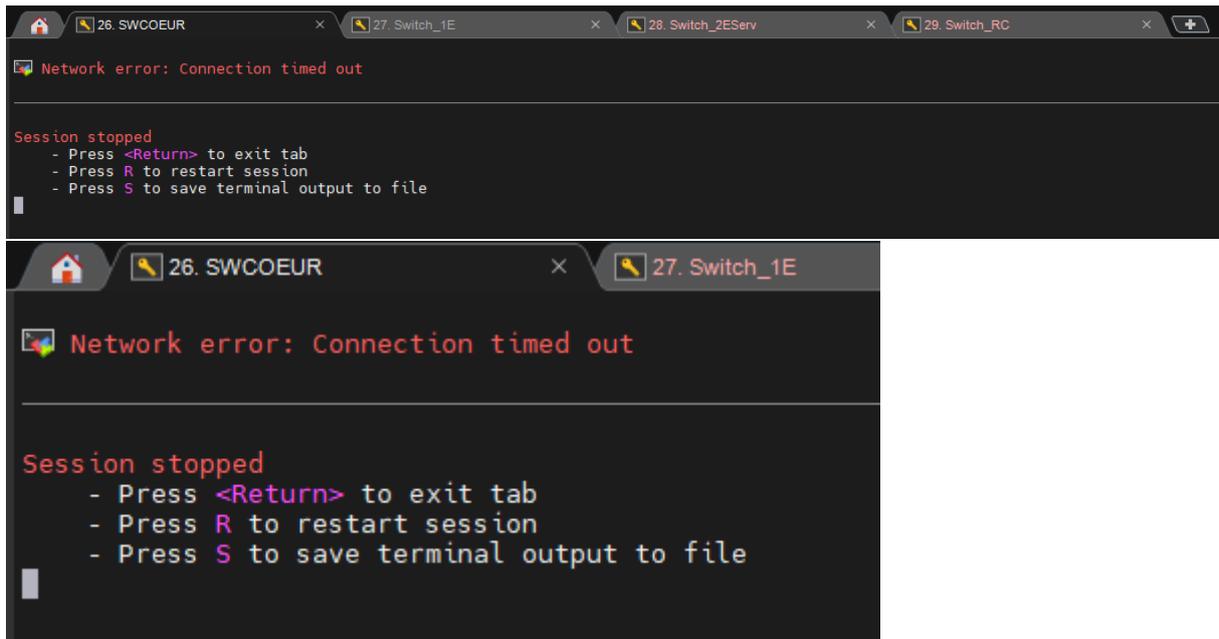
Configuration IP du deuxième poste

```
Suffixe DNS propre à la connexion. . . . :  
Description. . . . . : ASIX USB to Gigabit Ethernet Family Adapter  
Adresse physique . . . . . : 08-26-AE-33-74-7F  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . . : Oui  
Adresse IPv6 de liaison locale. . . . . : fe80::4329:27cb:c7db:106e%52(préfééré)  
Adresse IPv4. . . . . : 172.16.20.2(préfééré)  
Masque de sous-réseau. . . . . : 255.255.255.0  
Bail obtenu. . . . . : mardi 23 septembre 2025 15:54:28  
Bail expirant. . . . . : mercredi 24 septembre 2025 15:54:28  
Passerelle par défaut. . . . . : 172.16.20.254  
Serveur DHCP . . . . . : 172.16.20.254  
IAID DHCPv6 . . . . . : 872949422  
DUID de client DHCPv6. . . . . : 00-01-00-01-30-32-26-24-C8-5E-A9-3B-90-B1  
Serveurs DNS. . . . . : 172.16.100.2  
NetBIOS sur Tcip. . . . . : Activé
```

Test de connexion au switch et routeur depuis le réseau en .20 (échec)

La connexion doit échouer car les ACL n'autorisent aucune connexion de ce réseau vers le réseau 172.16.70.0





Test ping entre un utilisateur en .20 vers le VLAN serveur (échec)

La connexion doit échouer car nous n'autorisons pas les pings vers les serveurs depuis ce VLAN

```

Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::4329:27cb:c7db:106e%17
    Adresse IPv4. . . . . : 172.16.20.1
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 172.16.20.254

Carte réseau sans fil Wi-Fi :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . :

Carte Ethernet Connexion réseau Bluetooth :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . :

C:\Users\abdel>ping 172.16.100.1

Envoi d'une requête 'Ping' 172.16.100.1 avec 32 octets de données :
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.
Réponse de 172.16.20.254 : Impossible de joindre le réseau de destination.

Statistiques Ping pour 172.16.100.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),

C:\Users\abdel>

```

Test de connexion ftp entre un utilisateur en .20 vers ZYXEL (échec)

La connexion doit échouer car nous n'autorisons pas le FTP vers les serveurs depuis ce VLAN

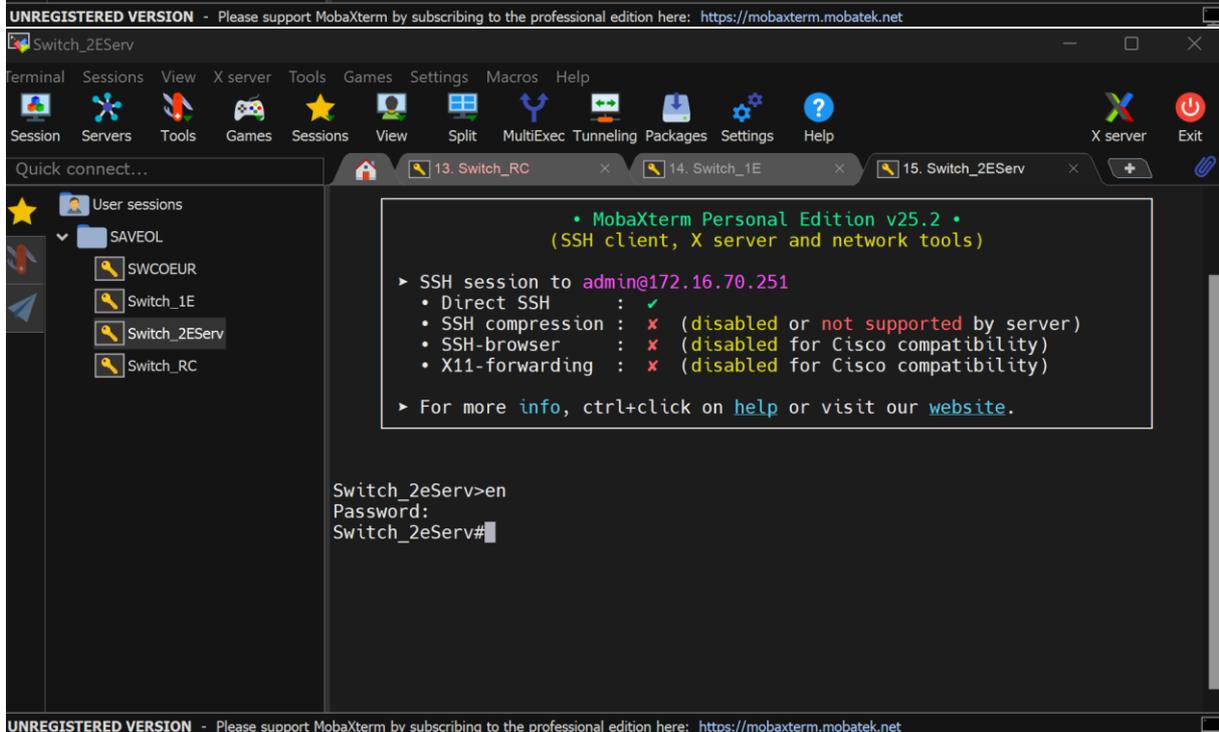
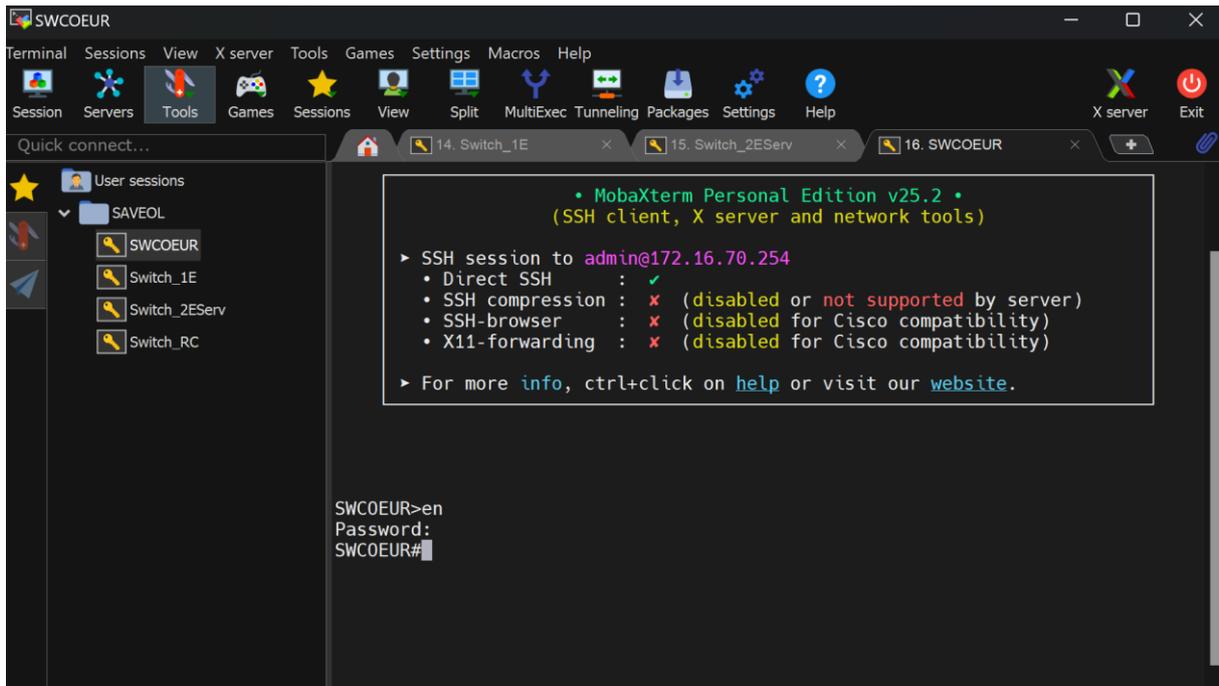
```
C:\Users\abdel>ftp 172.16.255.254
> ftp: connect :Délai de connexion dépassé
```

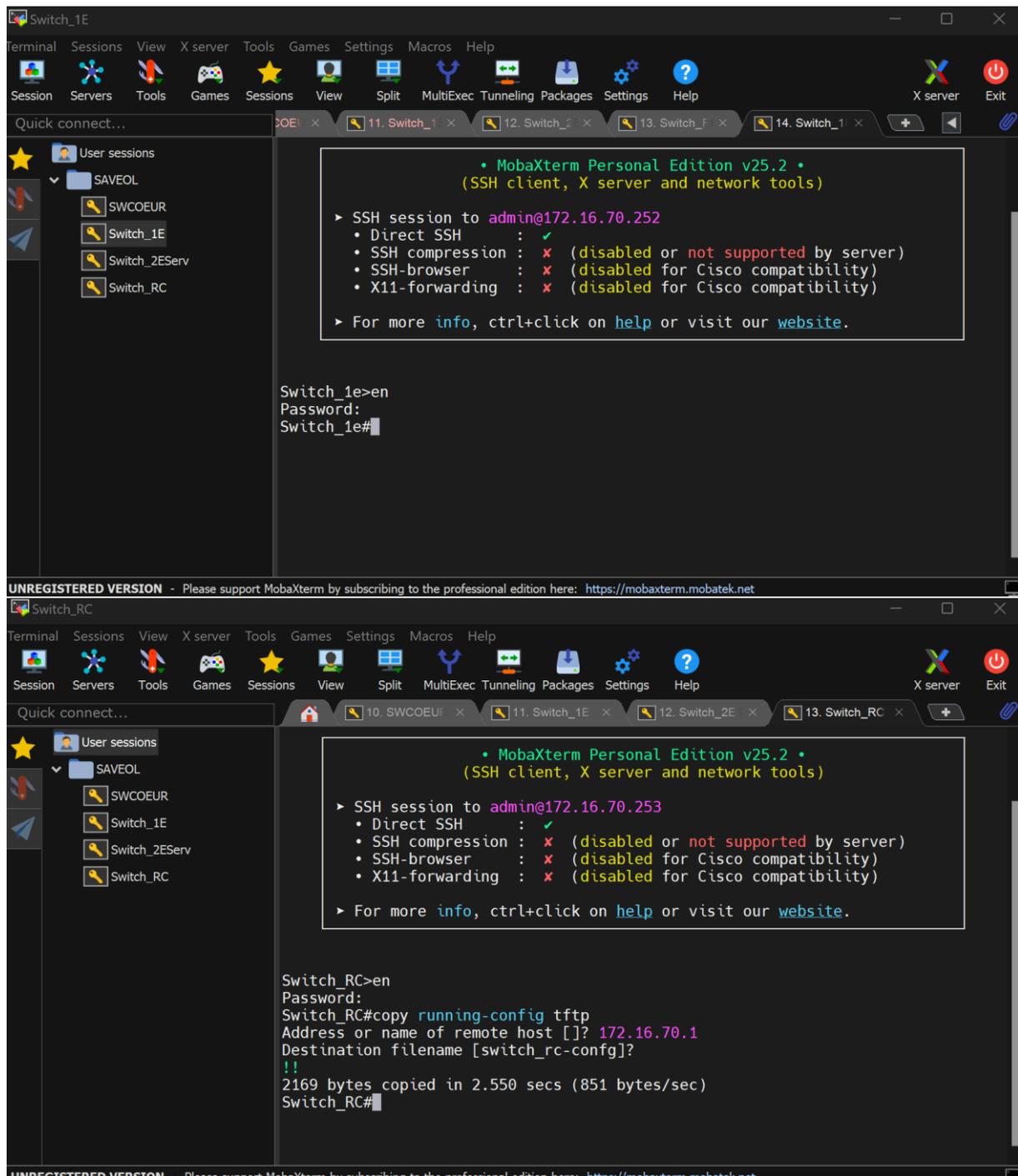
Configuration IP du pc dans le VLAN 60 IT

```
Carte Ethernet Ethernet 2 :
  Suffixe DNS propre à la connexion. . . :
  Description. . . . . : ASIX USB to Gigabit Ethernet Family Adapter
  Adresse physique . . . . . : 08-26-AE-33-74-7F
  DHCP activé. . . . . : Oui
  Configuration automatique activée. . . : Oui
  Adresse IPv6 de liaison locale. . . . : fe80::4329:27cb:c7db:106e%17(préfééré)
  Adresse IPv4. . . . . : 172.16.60.1(préfééré)
  Masque de sous-réseau. . . . . : 255.255.255.0
  Bail obtenu. . . . . : mardi 30 septembre 2025 14:35:14
  Bail expirant. . . . . : mercredi 1 octobre 2025 14:35:15
  Passerelle par défaut. . . . . : 172.16.60.254
  Serveur DHCP . . . . . : 172.16.60.254
  IAID DHCPv6 . . . . . : 872949422
  DUID de client DHCPv6. . . . . : 00-01-00-01-30-32-26-24-C8-5E-A9-3B-90-B1
  Serveurs DNS. . . . . : 172.16.100.2
  NetBIOS sur Tcpi. . . . . : Activé
```

Test de connexion au switch et routeur depuis le réseau en .60 (réussite)

La connexion doit réussir car l'IT a tous les droits





Test de connexion FTP depuis le pc en .60 vers ZyXEL (reussite)

Test de ping depuis le pc en .60 vers les serveurs réseau (réussite)

La connexion doit réussir car l'IT a tous les droits

```
Statistiques Ping pour 172.16.255.254:
```

```
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

```
Durée approximative des boucles en millisecondes :
```

```
  Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

```
Ctrl+C
```

```
^C
```

```
C:\Users\abdel>ftp 172.16.255.254
```

```
Connecté à 172.16.255.254.
```

```
220 FTP Server (USG FLEX 500) [::ffff:172.16.255.254]
```

```
500 OPTS UTF8 not understood
```

```
Utilisateur (172.16.255.254:(none)) :
```

```
500 USER: command requires a parameter
```

```
Échec de l'identification.
```

```
ftp> bye
```

```
221 Goodbye.
```

```
C:\Users\abdel>ping 172.16.100.1
```

```
Envoi d'une requête 'Ping' 172.16.100.1 avec 32 octets de données :
```

```
Réponse de 172.16.100.1 : octets=32 temps<1ms TTL=127
```

```
Réponse de 172.16.100.1 : octets=32 temps<1ms TTL=127
```

```
Réponse de 172.16.100.1 : octets=32 temps=1 ms TTL=127
```

```
Réponse de 172.16.100.1 : octets=32 temps<1ms TTL=127
```

```
Statistiques Ping pour 172.16.100.1:
```

```
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
```

```
Durée approximative des boucles en millisecondes :
```

```
  Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```