

Au cours de la SAÉ 2.04, nous avons assumé le rôle d'agents d'une société locale de services du numérique, sollicités par une entreprise qui souhaitait refaire une partie de son système et de son réseau. Notre mission était structurée en plusieurs étapes importantes, que nous avons abordées

Plan d'adressage et Vlans.....	8
Configuration des commutateurs:.....	8
Mise en place des trunk :.....	9
Configuration du DHCP sous pfSense.....	10
la plage d'adresse ip :.....	10
Attribution des adresses aux sous-interfaces.....	10
Activations du service DHCP :.....	11
Configuration vpn IPsec.....	12
Mise en place de IPsec:.....	12
Les règles de pare feux IPsec:.....	14
Configuration de Windows Server.....	16
Créer les utilisateurs et les groupes.....	25
Préparer les dossiers de partage.....	26
Configuration du partage dans smb.conf.....	27

[PARTIE HARDWARE]

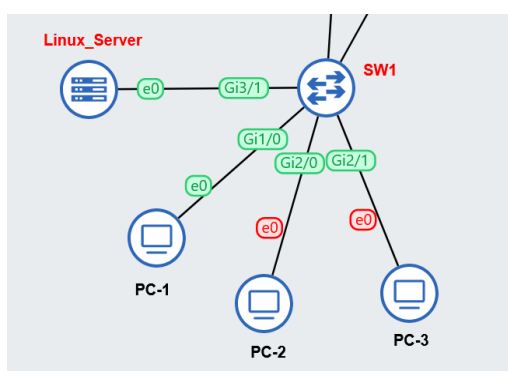
Dans le cadre du projet, nous avons travaillé sur la mise en place d'un réseau comprenant une maison mère située à Saint Pierre et une succursale basée à Saint Denis. Notre objectif était de créer une infrastructure robuste et fonctionnelle, en utilisant différents composants tels qu'un serveur Windows, un serveur UNIX, des postes clients Windows, ainsi que la suite de collaboration Zimbra. Tout au long du projet, nous avons adopté une approche progressive, nous permettant de réaliser des avancées incrémentales et d'interagir régulièrement avec les parties prenantes pour garantir leur satisfaction.

Tout d'abord, pour assurer une gestion efficace de notre mission, nous avons utilisé l'outil ProjectLibre pour créer un planning détaillé. Grâce à cette plateforme de gestion de projet, nous avons pu organiser et structurer les différentes étapes de notre mission, attribuer des ressources, définir des délais et suivre l'avancement de chaque tâche. Cela nous a permis

de travailler de manière méthodique et de respecter les échéances fixées, tout en garantissant la qualité des livrables.

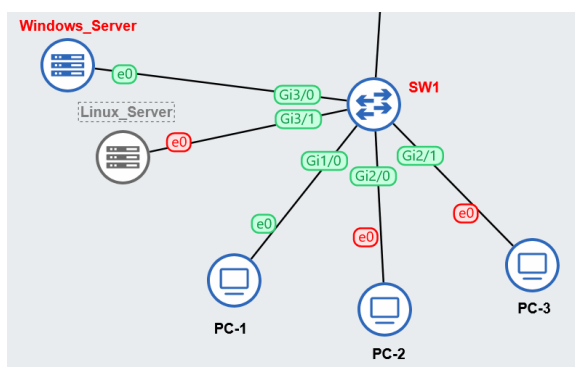
[ProjectLibre screen]

Pour la deuxième étape de notre projet, nous avons installé une machine Linux Server à la maison mère de Saint Pierre. Ensuite, nous avons configuré 3 machines Windows pour servir de postes clients. Tous les équipements ont été connectés à un switch de niveau 3, permettant une communication fluide entre eux. Nous avons également établi la liaison au niveau IP en effectuant des pings pour tester la connectivité.



Installation du Linux serveur et des 3 machines windows le tout connecté a un switch de niveau 3.

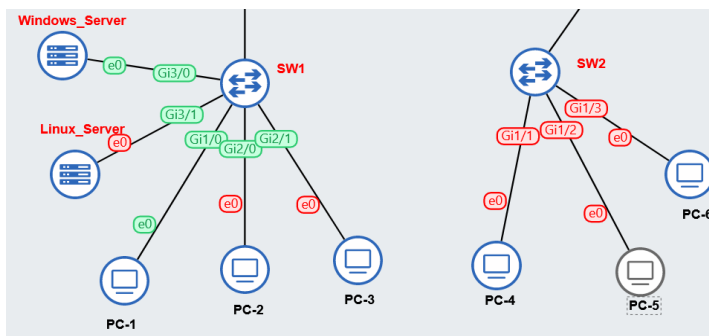
Ensuite nous avons fait migrer le système de gestion des comptes utilisateurs et leur espace privatif sur le serveur Windows. Ce changement a été effectué en installant un serveur Windows et en configurant les comptes utilisateurs en tant qu'utilisateurs itinérants. Le fonctionnement du système a été testé avec succès.



Installation du Windows serveur et configuration des comptes et des espaces privatif sur le serveur windows.

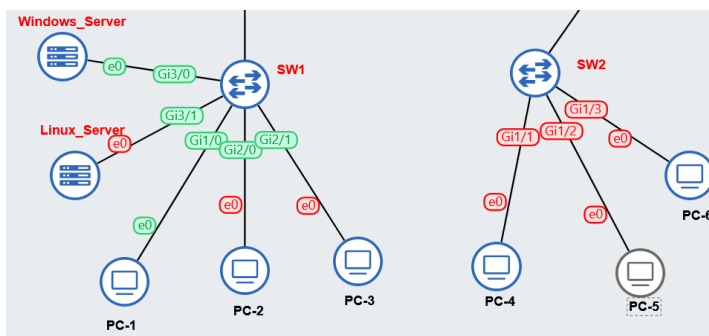
Par la suite nous avons mis en place le réseau à la succursale de Saint Denis. Cela a été réalisé en installant trois machines Windows supplémentaires et en les connectant à un

switch de niveau 3. L'adressage IP a été configuré pour permettre la communication entre les différents équipements du réseau.



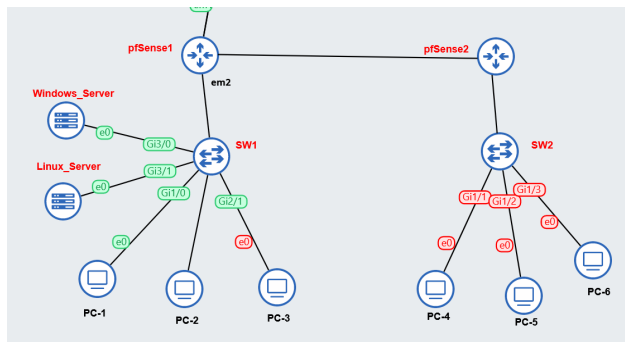
Mise en place de la deuxième succursale à St-Denis avec l'installation de 3 machines windows le tout connecté à un switch de niveau 3.

Ensuite, nous avons mis en place une configuration VLAN entre la maison mère de Saint Pierre et la succursale de Saint Denis. Cette configuration a été réalisée en définissant les VLAN 10,20,30 sur les switches de niveau 3.



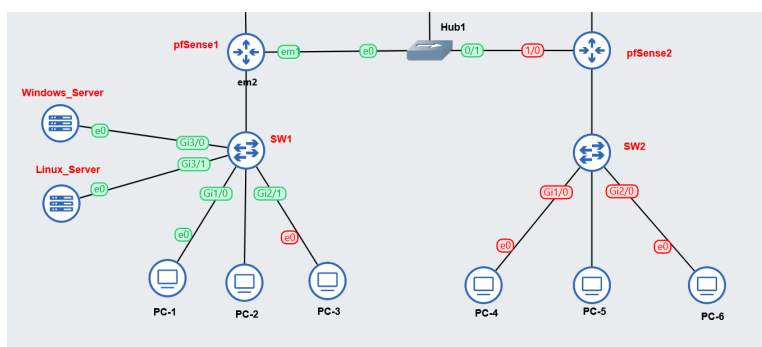
Configuration des VLAN 10,20,30 dans les deux succursales grâce au switches de niveaux 3

De plus, il nous a fallu installer des routeurs pour faciliter la communication entre la maison mère de Saint Pierre et la succursale de Saint Denis. L'objectif étant d'assurer la redondance et la haute disponibilité du réseau. Le fonctionnement du réseau avec les deux routeurs a été testé avec succès.



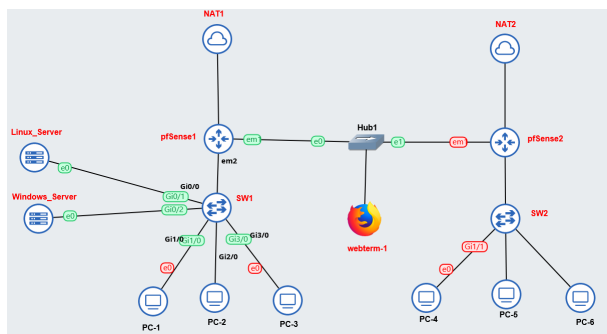
Un routeur a été installé et configuré pour permettre le routage des paquets entre les deux sites. Le fonctionnement du routeur a été testé avec succès.

Installation des serveurs DHCP sur les routeurs (Pfsense) pour faciliter l'attribution automatique des adresses IP aux équipements du réseau. Un serveur DHCP a été installé dans chaque succursale et configuré pour distribuer les adresses IP aux postes clients Windows. Le fonctionnement du serveur DHCP a été testé avec succès.



Installation d'un serveur DHCP sur le Pfsense pour l'attribution des adresses IP des postes clients.

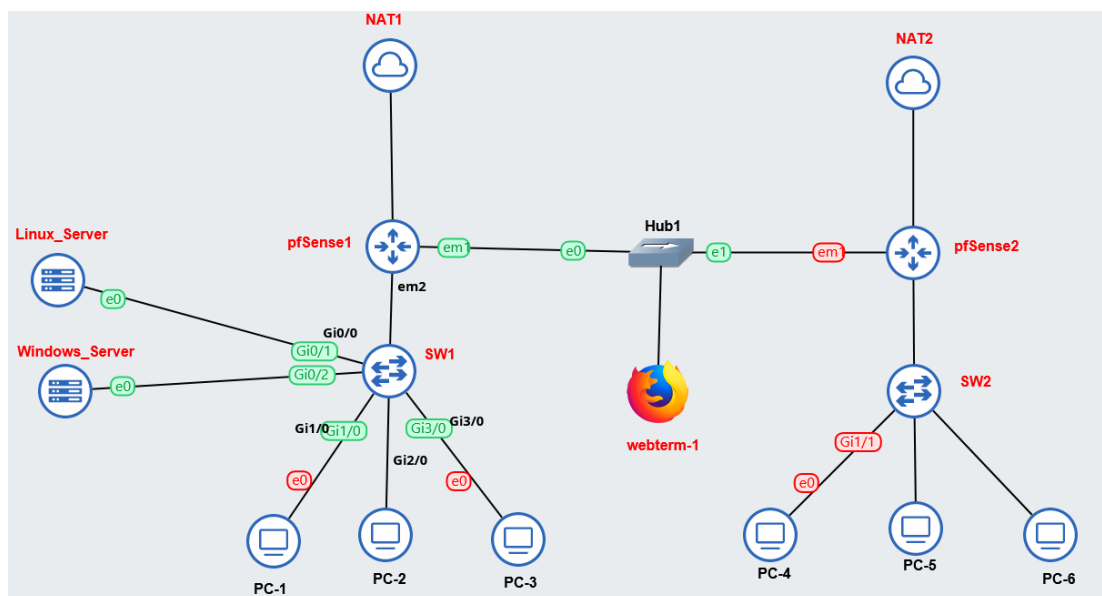
Enfin il restait à configurer les utilisateurs dans Zimbra pour mettre en place une solution de messagerie professionnelle et collaborative qui permet d'avoir des boîtes aux lettres électroniques dédiées aux employés de l'entreprise ainsi que Samba pour faciliter le partage de fichiers et d'imprimantes entre les ordinateurs du réseau ce qui permet aux ordinateurs Windows et non-Windows de se comprendre et de partager des ressources.



Ajout du service de messagerie en ligne Zimbra pour tous ceux qui veulent accéder à leur boîte mails et ajout du service de partage de fichiers Samba sur le serveur Linux.

[PARTIE SOFTWARE]

Dans cette partie de votre projet, nous nous sommes concentrés sur le déploiement du réseau d'une petite entreprise. Cette étape était primordiale pour assurer la connectivité et le bon fonctionnement des systèmes informatiques. Pour atteindre cet objectif, nous avons configuré les routeurs (Pfsense), les commutateurs (switch) et les pare-feu (firewall) de manière à répondre aux besoins spécifiques de l'entreprise. Pour avoir une idée et une meilleure compréhension visuelle de la structure du réseau et des relations entre les différents éléments voici la représentation de la topologie réseau comme nous pouvons le voir ci-dessous.



Après avoir vu la représentation globale de la topologie nous allons ensuite aborder la mise en place des VLANs d'adressage et des VLANs. Cette étape nous a permis d'améliorer la gestion et la segmentation du réseau, en attribuant des adresses IP spécifiques à chaque VLAN et en regroupant les appareils en fonction de leurs besoins et de leurs autorisations d'accès. Cette approche nous a permis de garantir une meilleure sécurité, une optimisation du trafic réseau et une plus grande flexibilité dans la gestion des ressources.

Problèmes rencontrés lors de la SAE

Un bug lors de la réalisation de la SAE était les pings entre les PC. Les pings ne passaient pas par moment alors que tout était bien configuré comme le montre la capture d'écran ci-dessous

```
C:\Users\Windows>ping 192.168.2.3

Envoi d'une requête 'Ping' 192.168.2.3 avec 32 octets de données :
Réponse de 192.168.2.3 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.2.3 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.2.3 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.2.3 : octets=32 temps=3 ms TTL=127

Statistiques Ping pour 192.168.2.3:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\Windows>ping 192.168.2.3

Envoi d'une requête 'Ping' 192.168.2.3 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.2.3:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

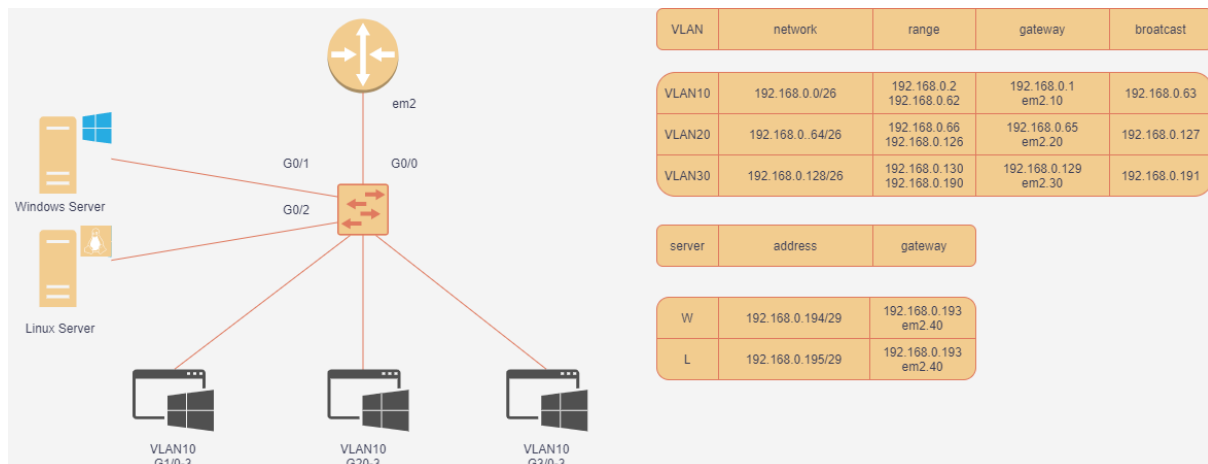
On a constaté aussi une augmentation du ping

Les pings de la partie "Test" ont été obtenus après plusieurs tentatives

Certains pings de cette section ont été considérés comme validés avec avoir reçu au moins 1 ping même si ce ping a une latence très élevée

Certains PC ont été remplacés par des VPCs pour pouvoir tester la connectivité entre les PC et les succursales

Plan d'adressage et Vlan



Vlan 10, réservé à la Direction, **Vlan 20**, réservé aux utilisateurs et le **Vlan 30** réservés aux Serveurs

Configuration des commutateurs:

mise en place des vlans :

On peut commencer la configuration des Vlans et ça commence par leur donner un nom.

Vlan 10	Gi1/0-3
Vlan 20	Gi2/0-3
Vlan 30	Gi3/0-3

exemple de configuration:

```
switch(config)#vlan 10
switch(config-vlan)#name direction
```


Par la suite, nous avons attribué des interfaces aux Vlan.

Vlan 10	Direction
Vlan 20	Utilisateurs
Vlan 30	Serveurs

exemple de configuration:

```
switch#config terminal
switch(config)#interface range gi1-3/0
switch(config-if-range)#switchport mode access vlan 30
switch(config-if-range)#no shutdown
```



la procédure est à réaliser sur les deux commutateurs.

Mise en place des trunk :

Pour les commutateurs :

Comme nous pouvons le voir les interfaces gi0/0 sur commutateur 1 et l'interface gi0/0 du commutateur 2 seront en mode trunk a leur routeur respectifs. On procède de la manière suivante.

```
switch(config)#interface <num interface>
switch(config-if)#switchport trunk encapsulation dot1q
switch(config-if)#switchport mode trunk
switch(config-if)#switchport trunk allowed vlan 10,20,30
switch(config-if-range)#no shutdown
```

Configuration du DHCP sous pfSense

la plage d'adresse ip :

Pour cette étape, nous allons utiliser la méthode VLSM "Variable Length Subnet Mask".

Adresse réseau selon les vlan :

Vlan 10	192.168.0.0/26
Vlan 20	192.168.0.64/26
Vlan 30	192.168.0.126/26

Plage d'adresse valide par sous-réseaux :

adresse de réseau	plage valide	broadcast
192.168.0.0/26	192.168.0.2 / 192.168.0.62	192.168.0.63
192.168.0.64/26	192.168.0.66 / 192.168.0.126	192.168.0.127
192.168.0.126/26	192.168.0.130 / 192.168.0.190	192.168.0.191

Attribution des adresses aux sous-interfaces

Avec le terminal de pfSense :

Pour commencer la configuration, choisit l'option 2 (set interfaces IP address)

```

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

```

On choisit le numéro de l'une des sous interface

```

7 - VLAN10 (em2.10
8 - VLAN20 (em2.20
9 - VLAN30 (em2.30

```

Par la suite on peut suivre les étapes suivantes:

- attribution de l'adresse
- choix du masque
- le reste ne nous intéresse. On passe à l'action suivante ou on choisit **no** si on a la possibilité.

Avec l'interface web de pfsense :

Il nous suffit d'aller sur l'interface web de pfsense, de sélectionner l'interface qui nous intéresse et de lui attribuer une ip.

The screenshot shows the 'General Configuration' tab for a network interface in pfSense. The 'Enable' section has the 'Enable interface' checkbox checked. The 'Description' field contains 'vlan10'. The 'IPv4 Configuration Type' is set to 'Static IPv4'. Below this, the 'IPv4 Address' field is set to '192.168.2.1' with a subnet mask of '26'. The 'IPv4 Upstream gateway' is set to 'None', with a green button labeled '+ Add a new gateway' next to it. A note at the bottom states: 'If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.'

Activations du service DHCP :

Maintenant que nous avons attribué nos adresses aux sous interfaces, on va pouvoir activer le service dhcp.

Pour ce faire nous allons sur l'interface web de pfsense. Puis dans le menu nous allons sélectionner **Service > DHCP server**.

On peut désormais activer le DHCP server sur les interfaces de nos VLAN en cochant la case **Enable DHCP server on VLAN"num vlan" interface**.

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on VLAN10 interface

Et enfin on définit le pool d'adresse.

Subnet	192.168.2.0	
Subnet mask	255.255.255.192	
Available range	192.168.2.1 - 192.168.2.62	
Range	<input type="text" value="192.168.2.2"/> <input type="text" value="192.168.2.62"/>	<div>From</div> <div>To</div>



Il faut faire attention à ne pas mettre l'adresse de l'interface dans le pool.

Il est important de souligner que nous avons choisi d'utiliser cette méthode pour la SAE 204 afin d'éviter toute coupure de service en cas de problème lié au serveur DHCP. Pour la deuxième succursale, cette méthode rend également les tests plus faciles. Cependant, il est également possible de configurer un serveur DHCP séparé et d'utiliser le pfSense comme relais DHCP.

Configuration vpn IPsec

Le vpn nous permet d'établir une connexion site à site entre les deux succursales.

Mise en place de IPsec:

La configuration de l'IPsec est composée de 2 phases.


La phase 1 de IPsec est utilisée pour établir une connexion sécurisée entre les deux extrémités, en négociant les paramètres de sécurité pour la session. Cela inclut l'authentification, la méthode de chiffrement, la clé de chiffrement et la durée de vie de la session.

La phase 2 de IPsec est utilisée pour établir une connexion sécurisée pour le trafic réel, en utilisant les paramètres de sécurité négociés lors de la phase 1. Cette phase est également

appelée la "session de données" et permet la transmission de données de manière sécurisée entre les deux extrémités.

configuration de la phase 1:


Pour commencer nous devons aller dans l'onglet **VPN>IPsec** et on clique sur **add P1**.

General Information	
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
Key Exchange version	IKEv2 <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	IPv4 <small>Select the Internet Protocol family.</small>
Interface	WAN <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	192.168.122.178 <small>Enter the public IP address or host name of the remote gateway. </small>
Description	pfsense1 to pfsense2 <small>A description may be entered here for administrative reference (not parsed).</small>

On définit l'interface et l'adresse ip qui nous servira de gateway.



Il faut bien faire attention de bien spécifier l'adresse WAN de Pfsense cible.

Phase 1 Proposal (Authentication)	
Authentication Method	Mutual PSK <small>Must match the setting chosen on the remote side.</small>
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	sae21 <small>Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.</small> 

On doit aussi configurer les authentifications et on doit faire attention que ce champ soit le même sur l'autre routeur pfsense. Et on peut laisser le reste par défaut.

configuration de la phase 2:

Nous devons aller dans l'onglet **VPN>IPsec** et on clique sur **Show phase 2 Entries** puis on clique sur **add**.

General Information			
Disabled <input type="checkbox"/> Disable this phase 2 entry without removing it from the list.			
Mode	Tunnel IPv4		
Local Network	Network	172.22.0.0	/ 24
	Type	Address	
Local network component of this IPsec security association.			
NAT/BINAT translation	None		/ 0
	Type	Address	
If NAT/BINAT is required on this network specify the address to be translated			
Remote Network	Network	172.22.2.0	/ 24
	Type	Address	
Remote network component of this IPsec security association.			
Description	dmz to pfsense2		
A description may be entered here for administrative reference (not parsed).			

Comme vous pouvez le voir le local network correspond à notre DMZ et le Remote network correspond au réseau distant ici celui de la deuxième succursale.

On peut faire la même configuration pour le pfsense 2 mais il faut juste changer le **remote gateways** dans la **phase 1** et le **local network**, le **remote network** dans la **phase 2**

Les règles de pare feu IPsec:

Pour que la connexion IPsec fonctionne correctement, on doit ajouter à minima des règles de pare-feu.

Il y a au moins deux règles de filtrage à implémenter : celles autorisant le trafic depuis la DMZ vers les réseaux du site distant ; et celles autorisant le trafic depuis le réseau du site distant vers la DMZ.

Pour Pfsense 1: :

Floating WAN LAN LOCAL SERIAL DMZ VLAN10 VLAN20 VLAN30 **IPsec**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/672 B	IPv4 *	*	*	*	*	none			

Add Add Delete Save Separator

Floating WAN LAN LOCAL SERIAL **DMZ** VLAN10 VLAN20 VLAN30 IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	DMZ net	*	172.22.2.0/24	*	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.22.2.0/24	*	DMZ net	*	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 *	172.22.0.0/23	*	DMZ net	*	*	none		
<input type="checkbox"/>	✗	0/16 KiB	IPv4 *	*	*	*	*	none			

Add Add Delete Save Separator

Pour Pfsense 2 :

Floating WAN LAN LOCAL SERIAL DMZ VLAN10 VLAN20 VLAN30 **IPsec**

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/672 B	IPv4 *	*	*	*	*	none			

Add Add Delete Save Separator

Floating WAN LAN **OPT1** VLAN10 VLAN20 VLAN30 OPT5 IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/2 KiB	IPv4 *	*	*	*	*	none			

Add Add Delete Save Separator

Pour le moment les règles sont très permissives et c'est volontaire. Cela nous permet dans un premier temps de vérifier le fonctionnement.

Par la suite nous devons nous rendre dans **Status>Ipsec** et démarrer la connexion sur les deux routeurs.

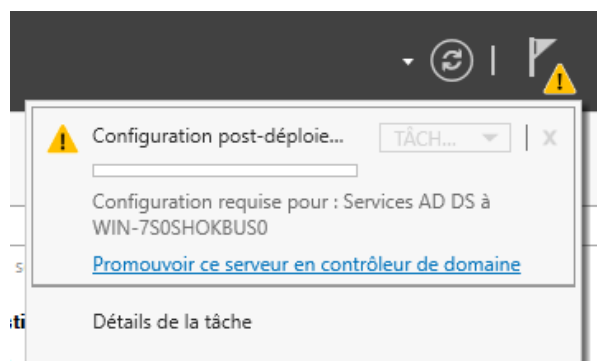
Configuration de Windows Server

1-1 Installation et configuration d'Active Directory

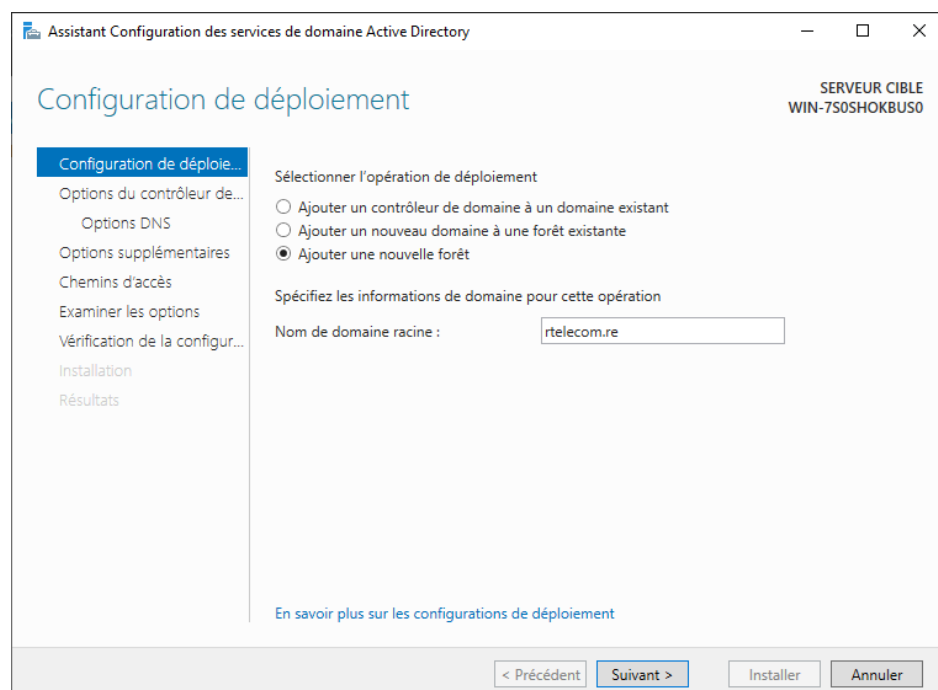
Après avoir installé les services AD DS, DNS depuis le panneau de rôle et de fonctionnalité

Nous avons choisi comme nom de domaine pour le domaine Active Directory : rtelecom.re

Pour commencer, on définit le serveur comme contrôleur de domaine



Pour commencer, nous créons une nouvelle forêt avec le nom de domaine ci-dessus



Définition du mot de passe de restauration

Ici le mot de passe choisi est **Windows123@**

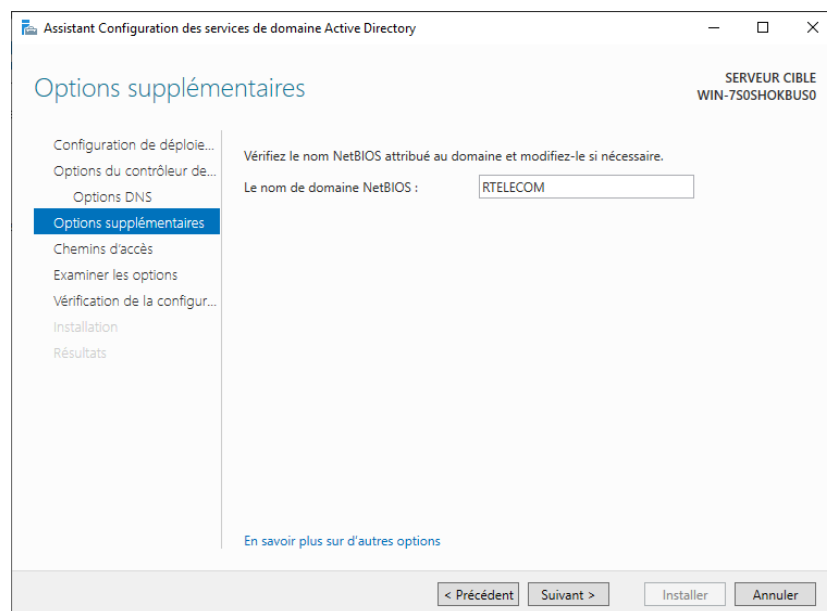
⚠ Ce mot de passe est peu complexe et est utilisé seulement dans le cadre de la SAE et non en production

The screenshot shows the 'Options du contrôleur de domaine' (Domain Controller Options) window in the 'Assistant Configuration des services de domaine Active Directory'. The window title is 'Assistant Configuration des services de domaine Active Directory'. The target server is 'SERVEUR CIBLE WIN-7S0SHOKBUS0'. The left sidebar contains a list of options: 'Configuration de déploiement...', 'Options du contrôleur de domaine...' (selected), 'Options DNS', 'Options supplémentaires', 'Chemins d'accès', 'Examiner les options', 'Vérification de la configuration...', 'Installation', and 'Résultats'. The main area is titled 'Options du contrôleur de domaine' and contains the following settings:

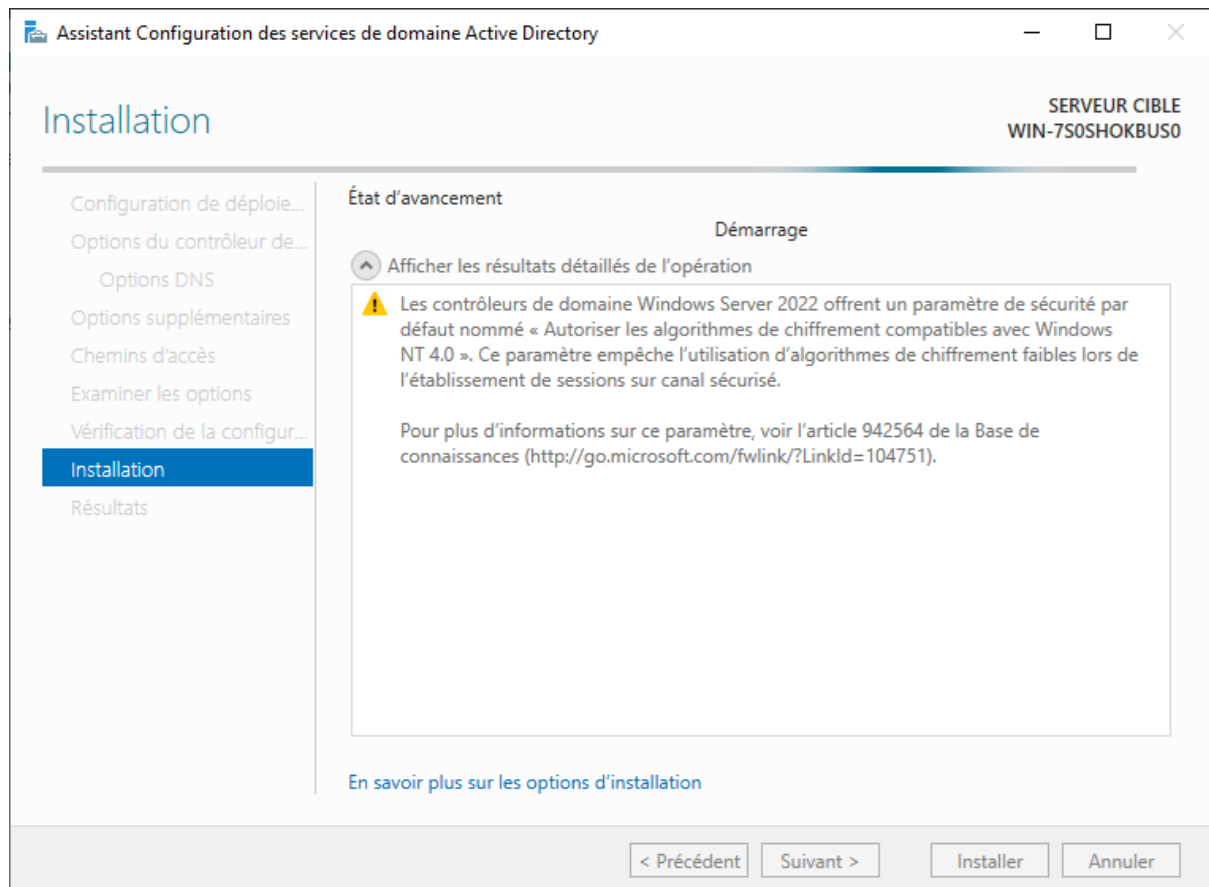
- Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine:
 - Niveau fonctionnel de la forêt : Windows Server 2016
 - Niveau fonctionnel du domaine : Windows Server 2016
- Spécifier les fonctionnalités de contrôleur de domaine:
 - ☒ Serveur DNS (Domain Name System)
 - ☒ Catalogue global (GC)
 - ☐ Contrôleur de domaine en lecture seule (RODC)
- Taper le mot de passe du mode de restauration des services d'annuaire (DSRM):
 - Mot de passe : [masked]
 - Confirmer le mot de passe : [masked]

At the bottom, there is a link 'En savoir plus sur les options pour le contrôleur de domaine' and navigation buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

Puis, on valide le nom NetBIOS



Pour terminer, on installe les services Active Directory



Puis une fois les services installés le serveur redémarre. Une fois que le serveur a redémarré, on peut voir que l'on est membre du domaine

Nom de l'ordinateur	WIN-7S0SHOKBUS0
Domaine	rtelecom.re
Pare-feu Microsoft Defender	Domaine : Actif
Gestion à distance	Activé
Bureau à distance	Désactivé
Association de cartes réseau	Désactivé
Ethernet0 2	Adresse IPv4 attribuée par DHCP, Compatible IPv6
Version du système d'exploitation	Microsoft Windows Server 2022 Standard Evaluation
Informations sur le matériel	VMware, Inc. VMware20,1

Utilisateurs Active Directory

Une fois active directory installé, nous le configurons en ajoutant des utilisateurs, une unité d'organisation.

Étant limité par la vitesse des switch de notre topologie, nous ne pouvons pas créer de profil itinérant, car les temps de transfert des données des utilisateurs serait beaucoup trop important.

Nous utiliserons les utilisateurs suivants :

Nom	Prénom	Nom d'ouverture de session	Mot de passe	Groupes	Unité d'organisation
HUET	Charles	c.huet	1234Util1	utilisateur	utilisateur
ANTIN	Romuald	r.antin	1234Util2	utilisateur	utilisateur
PETIT	Arnaud	a.petit	1234Util3	utilisateur	utilisateur
ARHIMAN	Ludovic	l.arhiman	1234Admin1	administration	administration
CAYAMBO	Pierre	p.cayambo	1234Admin2	administration	administration
GRONDIN	Dany	d.grondin	1234Admin3	administration	administration

Configuration d'Active Directory

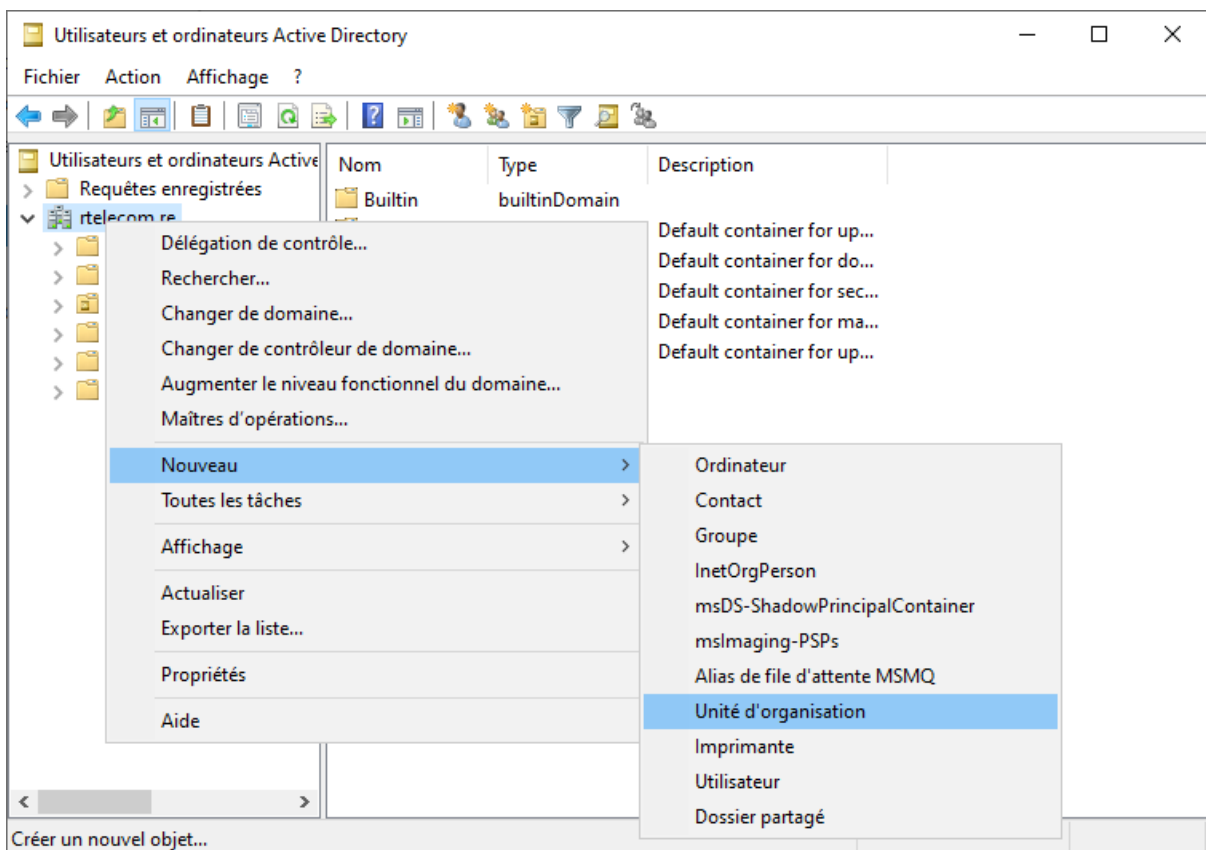
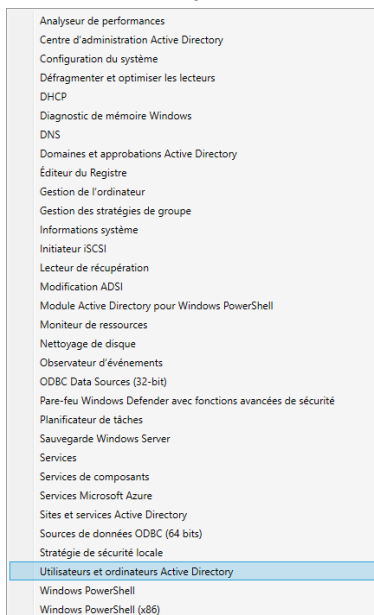
Création et configuration d'une unité d'organisation

Qu'est-ce qu'une unité d'organisation ?

“ Une unité organisationnelle (OU) ou unité d'organisation est un conteneur dans un domaine Microsoft Active Directory qui peut contenir des utilisateurs, des groupes et des ordinateurs. Il est la plus petite unité par laquelle un administrateur peut affecter des paramètres de stratégie ”

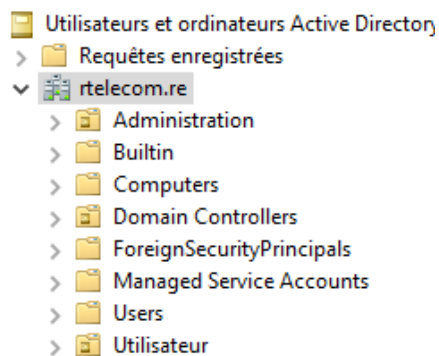
Dans Active Directory, une unité d'organisation est une sorte de dossier virtuel qui nous permet de regrouper des objets similaires, tels que des utilisateurs, des ordinateurs ou d'autres ressources, en fonction de nos besoins organisationnels. Cela nous aide à mieux gérer et sécuriser notre réseau informatique.

Premièrement, nous créons l'unité d'organisation dans le panneau "Utilisateur et ordinateur Active Directory"

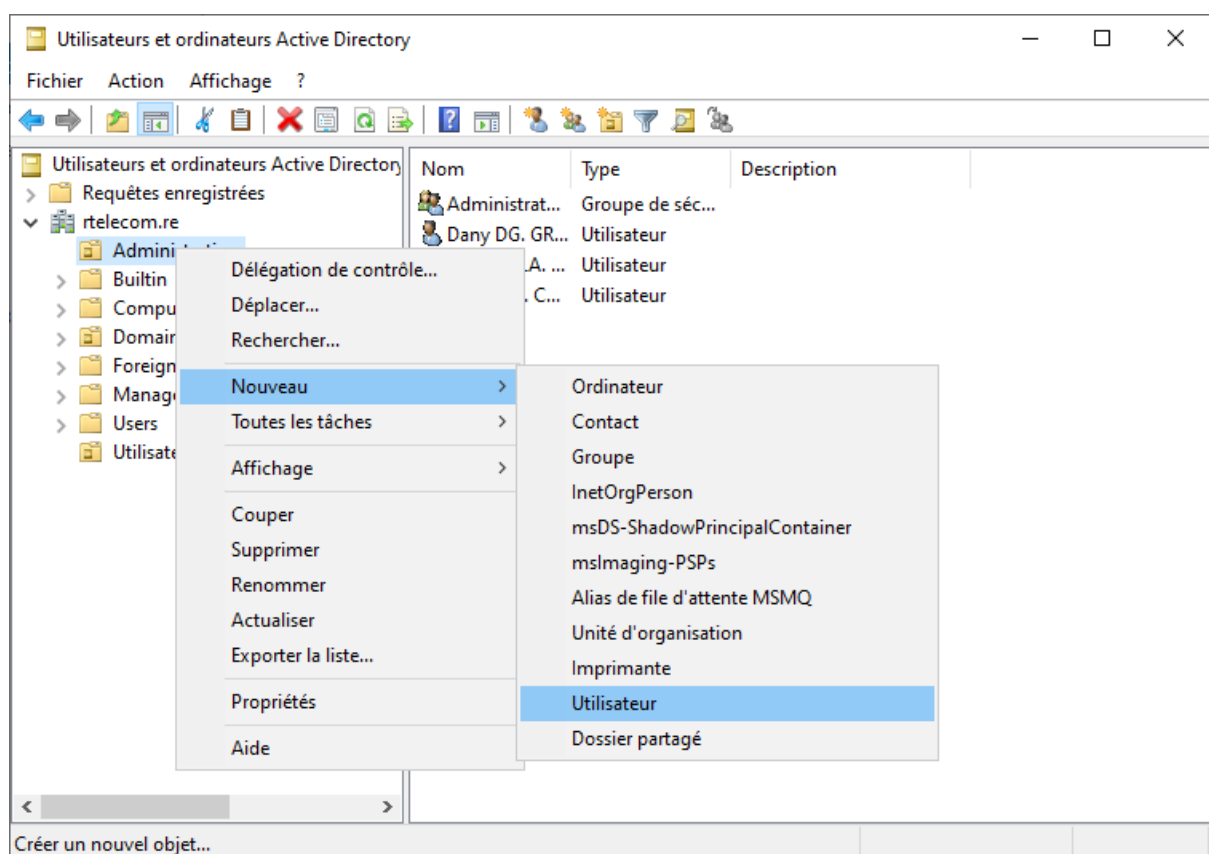


Nous allons créer deux Unités d'organisation

- Administration ⇒ pour le groupe administration
- Utilisateur ⇒ pour les employés



Puis, on ajoute les utilisateurs du tableau ci-dessus



Ajout des utilisateurs

Puis, il nous suffit d'entrer les informations du tableau pour chaque utilisateur

Nouvel objet - Utilisateur

Créer dans : rtelecom.re/Administration

Prénom : Initiales :

Nom :

Nom complet :

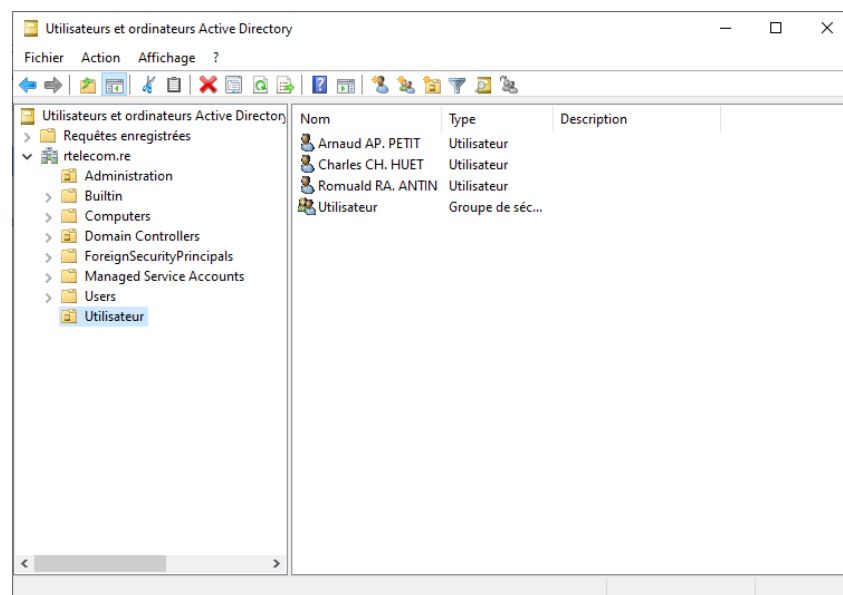
Nom d'ouverture de session de l'utilisateur : @rtelecom.re

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) : RTELECOM\

< Précédent Suivant > Annuler

Cela nous donne le résultat suivant

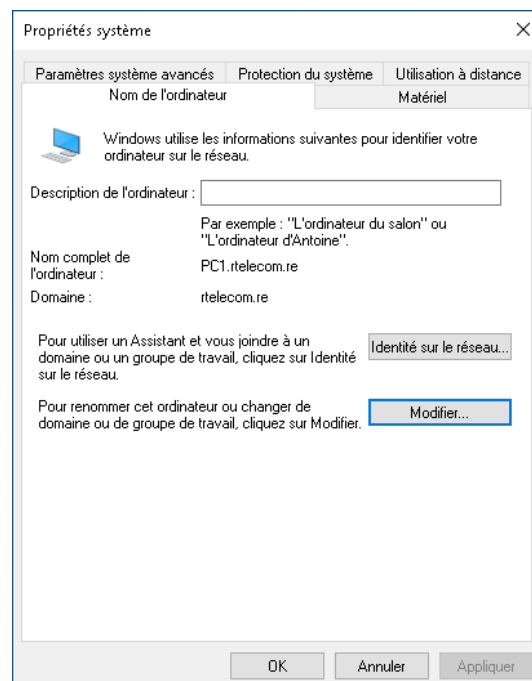
Nom	Type	Description
Administration	Groupe de séc...	
Dany DG. GRONDIN	Utilisateur	
Ludovic LA. ARHI...	Utilisateur	
Pierre PC. CAYAM...	Utilisateur	



Jonctions de domaine Active Directory avec les clients

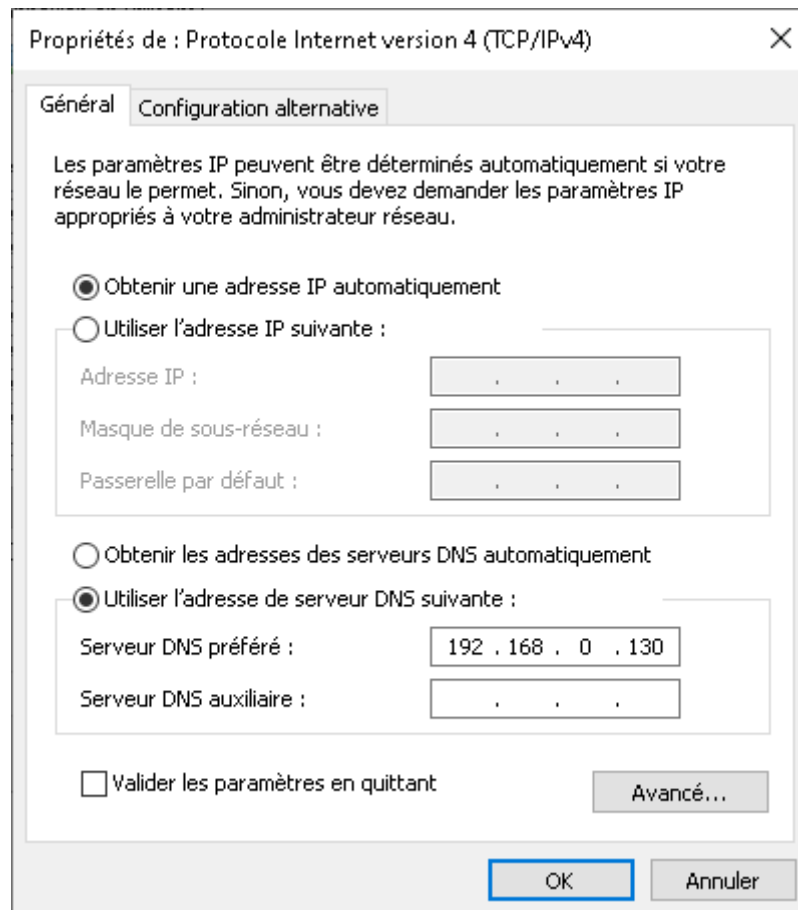
Sur les postes clients, pour pouvoir rejoindre le domaine Active Directory et pouvoir se connecter avec les utilisateurs déclarer précédemment, il faut rejoindre le domaine Active Directory

Pour rejoindre un domaine il faut se rendre dans **Propriété du système > Nom de l'ordinateur**

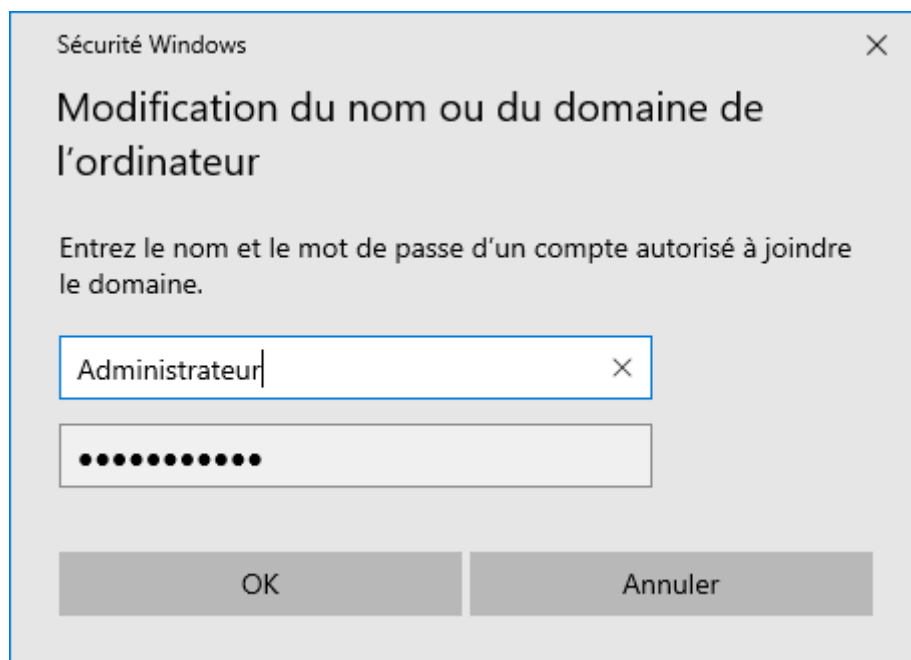


Puis cliquer sur modifier et entrer le nom de domaine que l'on souhaite rejoindre. Le nom de domaine à entrer est celui que nous avons créé dans Windows Server plus tôt ici le nom de domaine est **rtelecom.re**

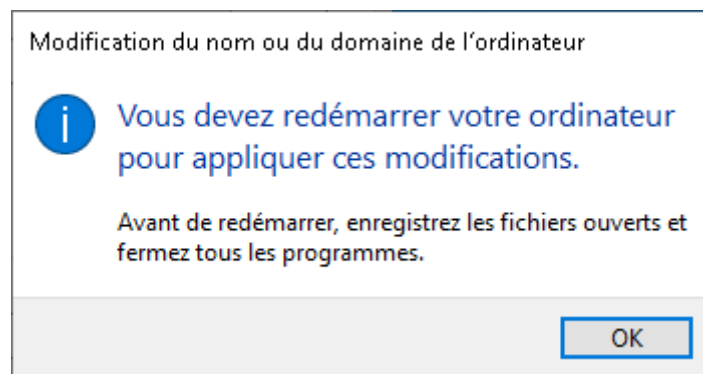
Pour pouvoir joindre le domaine il faut définir le serveur en tant que serveur DNS primaire



Une fois le domaine rejoint il nous faut entrer le mot de passe du compte administrateur que nous avons défini sur Windows Server.



Un message de bienvenue apparaît puis on nous demande de redémarrer la machine pour appliquer les changements



Configuration de Samba

[installation de samba]

Créer les utilisateurs et les groupes

Chaque utilisateur correspond à un département : Direction et utilisateur

```
adduser administration  
adduser utilisateur
```

Une fois les utilisateurs créés, on assigne des mots de passes à chaque utilisateur avec samba

```
smbpasswd -a administration
```

Le nouveau mot de passe sera demandé.

```
New SMB password:  
Retype new SMB password:
```

Ici les mots de passes sont admin et user pour les utilisateurs respectifs administration et utilisateur

Puis on ajoute deux groupes administration et utilisateur pour samba
Ici le but est de faire en sorte que chaque département ait un samba séparé

```
addgroup administration
```

```
addgroup utilisateur
```

Puis on ajoute l'utilisateur administration au groupe du même nom

```
gpasswd -a administration administration
```

```
gpasswd -a utilisateur utilisateur
```

Préparer les dossiers de partage

On crée deux dossier pour le partage pour nos deux utilisateur

```
mkdir /srv/admin-share  
mkdir /srv/user-share
```

Ensuite, on va attribuer le groupe "*administration*" comme groupe propriétaire du dossier /srv/admin-share

```
chgrp -R administration /srv/admin-share
```

Puis on fait la même chose pour le groupe "utilisateur" pour le dossier /srv/user-share

```
chgrp -R utilisateur /srv/user-share
```

On termine par ajouter les droits en lecture et en écriture sur les deux dossier

```
chmod -R g+rw /srv/user-share  
chmod -R g+rw /srv/admin-share
```

Configuration du partage dans smb.conf

On ajoute les blocs suivant dans le fichier smb.conf

On configure le partage pour l'utilisateur "administrateur"

```
[administrateur]
  comment = Partage de données
  path = /srv/admin-share
  guest ok = no
  read only = no
  browseable = yes
  valid users = @administrateur
```

Puis, pour l'utilisateur "utilisateur"

```
[utilisateur]
  comment = Partage de données
  path = /srv/user-share
  guest ok = no
  read only = no
  browseable = yes
  valid users = @utilisateur
```

Puis on redémarre Samba

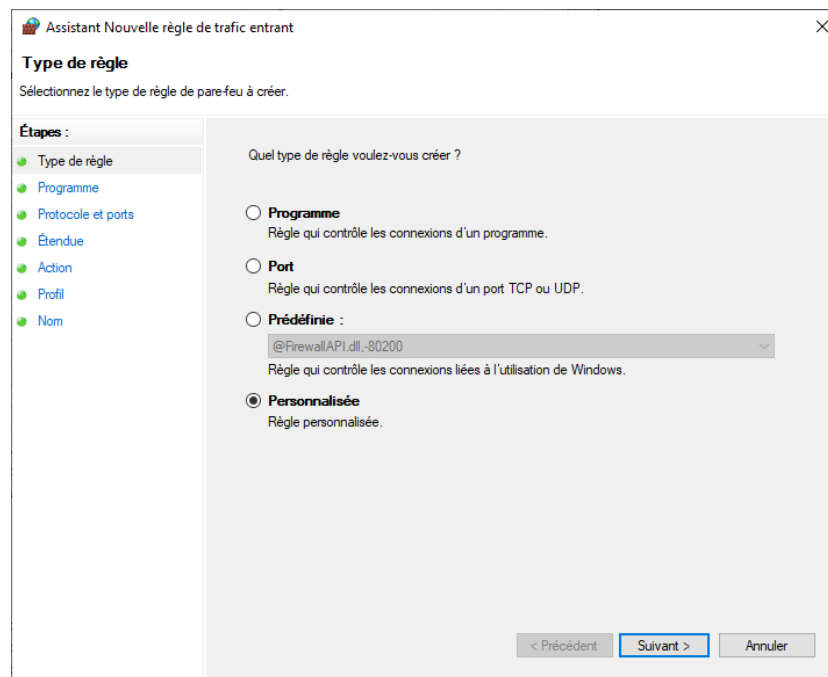
```
systemctl restart smbd
```

Tests de la topologie

Tests de connectivité et DHCP

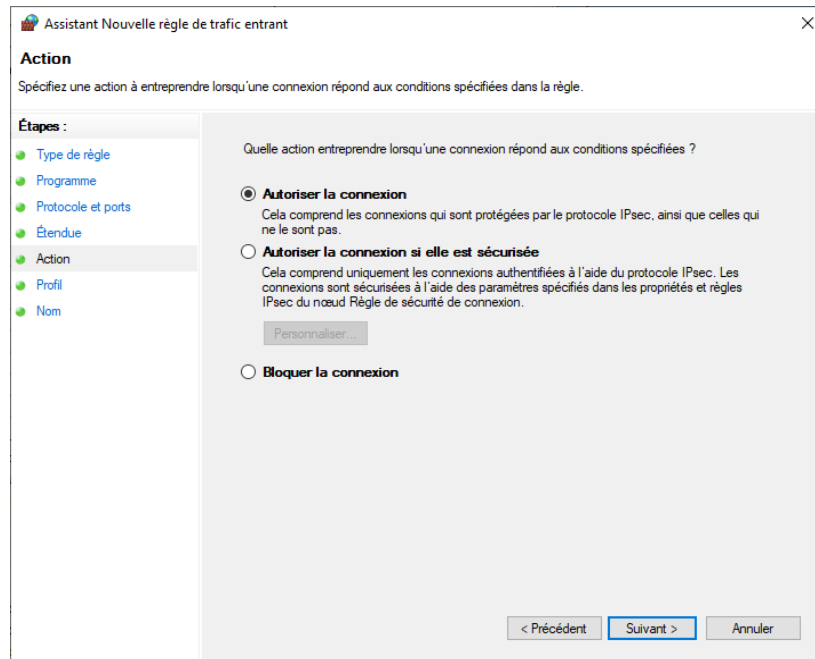
Par défaut les ping sont bloqués par le pare-feu de windows nous allons donc créer des règles ICMP en entrée et sortie sur le pare-feu

Dans le pare feu windows on ajoute un nouvelle règle personnaliser

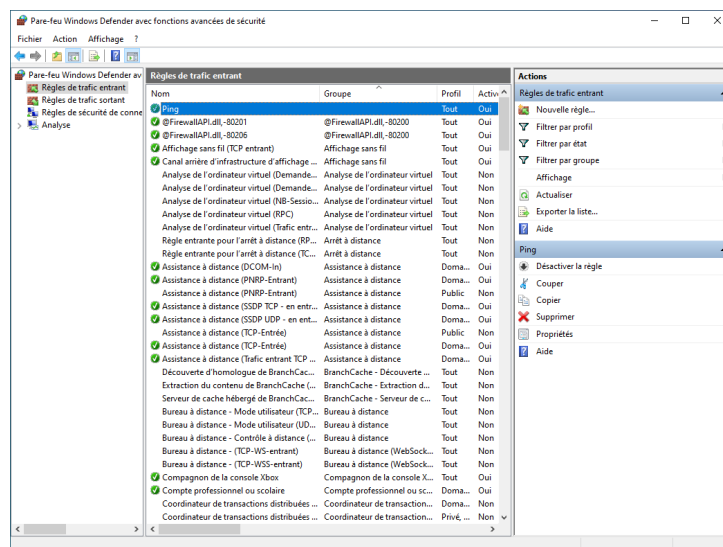


on autorise cette règle pour tous les programmes puis on sélectionne dans les protocoles le protocole ICMPv4 qui est le protocole utilisé pour les ping en IPV4

on autorise toutes les adresse ip puis on autorise la connexion



La règle a été créer en entrée il faut aussi la créer en sortie



La topologie intégrant un routage inter-vlan, ces tests de connectivités testeront aussi le ping d'un vlan à l'autre. Les IP sont ici toutes obtenues par DHCP

Ping entre les pc de la première succursale

PC1 [VLAN10] ⇒ PC2 [VLAN20]

Adresse IP PC1

Carte Ethernet Ethernet0 2 :

```
Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . : Intel(R) PRO/1000 MT Network Connection
Adresse physique . . . . . : 00-0C-29-F0-85-95
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::b935:46b3:e36e:f384%11(préfééré)
Adresse IPv4. . . . . : 192.168.0.2(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.192
Bail obtenu. . . . . : jeudi 15 juin 2023 12:23:29
Bail expirant. . . . . : jeudi 15 juin 2023 15:14:06
Passerelle par défaut. . . . . : 192.168.0.1
Serveur DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 117443625
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-07-F3-4A-00-0C-29-F0-85-95
Serveurs DNS. . . . . : 192.168.0.130
NetBIOS sur Tcpip. . . . . : Activé
```

Adresse IP PC2

Carte Ethernet Ethernet0 2 :

```
Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . : Intel(R) PRO/1000 MT Network Connection
Adresse physique . . . . . : 00-0C-29-5D-D7-81
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::a045:5e10:4f77:6bfd%6(préfééré)
Adresse IPv4. . . . . : 192.168.0.66(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.192
Bail obtenu. . . . . : jeudi 15 juin 2023 13:14:43
Bail expirant. . . . . : jeudi 15 juin 2023 15:14:43
Passerelle par défaut. . . . . : 192.168.0.65
Serveur DHCP . . . . . : 192.168.0.65
IAID DHCPv6 . . . . . : 117443625
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-07-F3-4A-00-0C-29-F0-85-95
Serveurs DNS. . . . . : 192.168.0.65
NetBIOS sur Tcpip. . . . . : Activé
```



```
C:\Users\Windows>ping 192.168.0.66

Envoi d'une requête 'Ping' 192.168.0.66 avec 32 octets de données :
Réponse de 192.168.0.66 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.0.66 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.0.66 : octets=32 temps=10 ms TTL=127
Réponse de 192.168.0.66 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 192.168.0.66:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 10ms, Moyenne = 4ms
```

Test de connectivité validé, le PC1 et 2 communiquent

PC1 [VLAN10] ⇒ PC3 [VLAN20]

Adresse IP PC3

```
Carte Ethernet Ethernet0 2 :

Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . : Intel(R) PRO/1000 MT Network Connection
Adresse physique . . . . . : 00-0C-29-72-25-A2
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::6daf:1f6d:e520:5f80%6(préfééré)
Adresse IPv4. . . . . : 192.168.0.67(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.192
Bail obtenu. . . . . : jeudi 15 juin 2023 13:28:07
Bail expirant. . . . . : jeudi 15 juin 2023 15:28:05
Passerelle par défaut. . . . . : 192.168.0.65
Serveur DHCP . . . . . : 192.168.0.65
IAID DHCPv6 . . . . . : 117443625
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-07-F3-4A-00-0C-29-F0-85-95
Serveurs DNS. . . . . : 192.168.0.65
NetBIOS sur Tcpip. . . . . : Activé
```

```
C:\Users\Windows>ping 192.168.0.2

Envoi d'une requête 'Ping' 192.168.0.2 avec 32 octets de données :
Réponse de 192.168.0.2 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.0.2 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.0.2 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.0.2 : octets=32 temps=2 ms TTL=127

Statistiques Ping pour 192.168.0.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 2ms, Moyenne = 2ms
```

Test de connectivité validé, le PC1 et 3 communiquent

PC2 [VLAN20] ⇒ PC3 [VLAN20]

```
C:\Users\Windows>ping 192.168.0.67

Envoi d'une requête 'Ping' 192.168.0.67 avec 32 octets de données :
Réponse de 192.168.0.67 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.67 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.67 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.67 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.0.67:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Test de connectivité validé, le PC2 et 3 communiquent

Tous les PC de la première succursale communiquent

Ping entre les pc de la deuxième succursale

PC4 [VLAN10] ⇒ PC5 [VLAN20]

Adresse IP PC4

```
Carte Ethernet Ethernet0 2 :

  Suffixe DNS propre à la connexion. . . : home.arpa
  Description. . . . . : Intel(R) PRO/1000 MT Network Connection
  Adresse physique . . . . . : 00-0C-29-DD-FD-3E
  DHCP activé. . . . . : Oui
  Configuration automatique activée. . . : Oui
  Adresse IPv6 de liaison locale. . . . : fe80::957c:4d21:7dbb:86bf%6(préfééré)
  Adresse IPv4. . . . . : 192.168.2.3(préfééré)
  Masque de sous-réseau. . . . . : 255.255.255.192
  Bail obtenu. . . . . : jeudi 15 juin 2023 16:07:11
  Bail expirant. . . . . : jeudi 15 juin 2023 18:07:10
  Passerelle par défaut. . . . . : 192.168.2.1
  Serveur DHCP . . . . . : 192.168.2.1
  IAID DHCPv6 . . . . . : 117443625
  DUID de client DHCPv6. . . . . : 00-01-00-01-2C-07-F3-4A-00-0C-29-F0-85-95
  Serveurs DNS. . . . . : 192.168.2.1
  NetBIOS sur Tcpip. . . . . : Activé
```

Adresse IP PC5

Carte Ethernet Ethernet0 2 :

```
Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . : Intel(R) PRO/1000 MT Network Connection
Adresse physique . . . . . : 00-0C-29-82-2E-54
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::6d0f:a589:a69:5702%4(préféré)
Adresse IPv4. . . . . : 192.168.2.2(préféré)
Masque de sous-réseau. . . . . : 255.255.255.192
Bail obtenu. . . . . : jeudi 15 juin 2023 16:08:31
Bail expirant. . . . . : jeudi 15 juin 2023 18:08:33
Passerelle par défaut. . . . . : 192.168.2.1
Serveur DHCP . . . . . : 192.168.2.1
IAID DHCPv6 . . . . . : 117443625
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-07-F3-4A-00-0C-29-F0-85-95
Serveurs DNS. . . . . : 192.168.2.1
NetBIOS sur Tcpip. . . . . : Activé
```

C:\Users\Windows>ping 192.168.2.3

```
Envoi d'une requête 'Ping' 192.168.2.3 avec 32 octets de données :
Réponse de 192.168.2.3 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.2.3 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.2.3 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.2.3 : octets=32 temps=3 ms TTL=127
```

Statistiques Ping pour 192.168.2.3:

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms
```

Test de connectivité validé, le PC 4 et 5 communiquent

PC4 [VLAN10] ⇒ PC6 [VLAN20]

Carte Ethernet Ethernet0 2 :

```
Suffixe DNS propre à la connexion. . . : home.arpa
Description. . . . . : Intel(R) PRO/1000 MT Network Connection
Adresse physique . . . . . : 00-0C-29-CC-BC-85
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::93e:68b8:c9b5:6cb2%5(préféré)
Adresse IPv4. . . . . : 192.168.2.66(préféré)
Masque de sous-réseau. . . . . : 255.255.255.192
Bail obtenu. . . . . : jeudi 15 juin 2023 19:05:21
Bail expirant. . . . . : jeudi 15 juin 2023 21:05:19
Passerelle par défaut. . . . . : 192.168.2.65
Serveur DHCP . . . . . : 192.168.2.65
IAID DHCPv6 . . . . . : 117443625
DUID de client DHCPv6. . . . . : 00-01-00-01-2C-07-F3-4A-00-0C-29-F0-85-95
Serveurs DNS. . . . . : 192.168.2.65
NetBIOS sur Tcpip. . . . . : Activé
```

PC5 [VLAN20] ⇒ PC6 [VLAN20]

Les PC 5 et 6 ont été remplacés par des VPC

Adresse IP PC 5

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC5	192.168.2.5/26 fe80::250:79ff:fe66:6801/64	192.168.2.1	00:50:79:66:68:01	20114	127.0.0.1:20115

Adresse IP PC 6

NAME	IP/MASK	GATEWAY	MAC	LPORT	RHOST:PORT
PC6	192.168.2.68/26 fe80::250:79ff:fe66:6800/64	192.168.2.65	00:50:79:66:68:00	20116	127.0.0.1:20117

PC5> ping 192.168.2.68

```
84 bytes from 192.168.2.68 icmp_seq=1 ttl=63 time=7.984 ms
84 bytes from 192.168.2.68 icmp_seq=2 ttl=63 time=2.983 ms
84 bytes from 192.168.2.68 icmp_seq=3 ttl=63 time=3.253 ms
84 bytes from 192.168.2.68 icmp_seq=4 ttl=63 time=3.614 ms
84 bytes from 192.168.2.68 icmp_seq=5 ttl=63 time=3.179 ms
```

Test de connectivité validé, le PC 5 et 6 communiquent

Ping entre les PC des deux Succursales

PC1 [VLAN10] ⇒ PC4 [VLAN10]

PC1 [VLAN10] ⇒ PC5 [VLAN20]

PC1 [VLAN10] ⇒ PC6 [VLAN20]

PC2 [VLAN20] ⇒ PC4 [VLAN10]

PC2 [VLAN20] ⇒ PC5 [VLAN20]

PC2 [VLAN20] ⇒ PC5 [VLAN20]

PC3 [VLAN20] ⇒ PC4 [VLAN10]

PC3 [VLAN20] ⇒ PC5 [VLAN20]

PC3 [VLAN20] ⇒ PC6 [VLAN20]

Ping entre les PC des deux succursales et les serveurs Windows et Linux

Succursale 1

PC1 [VLAN10] ⇒ Windows Server [VLAN30]

```
C:\Users\Windows>ping 192.168.0.130

Envoi d'une requête 'Ping' 192.168.0.130 avec 32 octets de données :
Réponse de 192.168.0.130 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.0.130 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.0.130 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.0.130 : octets=32 temps=3 ms TTL=127

Statistiques Ping pour 192.168.0.130:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 3ms, Moyenne = 3ms
```

PC1 [VLAN10] ⇒ Linux Server [VLAN30]

PC2 [VLAN20] ⇒ Windows Server [VLAN30]

PC2 [VLAN20] ⇒ Linux Server [VLAN30]

PC3 [VLAN20] ⇒ Windows Server [VLAN30]

PC3 [VLAN20] ⇒ Linux Server [VLAN30]

Succursale 2

PC4 [VLAN10] ⇒ Windows Server [VLAN30]

PC4 [VLAN10] ⇒ Linux Server [VLAN30]

PC5 [VLAN20] ⇒ Windows Server [VLAN30]

PC5 [VLAN20] ⇒ Linux Server [VLAN30]

PC6 [VLAN20] ⇒ Windows Server [VLAN30]

PC6 [VLAN20] ⇒ Linux Server [VLAN30]

Test de résolutions des noms de domaines pour l'ensemble des machines vers un nom de domaine sur internet

Ce test permettra de tester la connectivité internet des machines

Succursale 1

PC1 [VLAN10] ⇒ google.com

Test de connectivité internet réussi, le PC1 arrive à communiquer avec internet

```
C:\Users\Windows>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.170.46] avec 32 octets de données :
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=46 ms TTL=126

Statistiques Ping pour 172.217.170.46:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 45ms, Maximum = 46ms, Moyenne = 45ms
```

PC2 [VLAN20] ⇒ google.com

```
C:\Users\Windows>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.170.46] avec 32 octets de données :
Réponse de 172.217.170.46 : octets=32 temps=46 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=46 ms TTL=126

Statistiques Ping pour 172.217.170.46:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 45ms, Maximum = 46ms, Moyenne = 45ms
```

Test de connectivité internet réussi, le PC2 arrive à communiquer avec internet

PC3 [VLAN20] ⇒ google.com

```
C:\Users\Windows>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.170.46] avec 32 octets de données :
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=46 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=45 ms TTL=126

Statistiques Ping pour 172.217.170.46:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 45ms, Maximum = 46ms, Moyenne = 45ms
```

Test de connectivité internet réussi, le PC3 arrive à communiquer avec internet

Succursale 2

PC4 [VLAN10] ⇒ google.com

```
C:\Users\Windows>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.170.46] avec 32 octets de données :
Réponse de 172.217.170.46 : octets=32 temps=2003 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=2163 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=2125 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=1512 ms TTL=126

Statistiques Ping pour 172.217.170.46:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1512ms, Maximum = 2163ms, Moyenne = 1950ms
```

Test de connectivité internet réussi, le PC4 arrive à communiquer avec internet

PC5 [VLAN20] ⇒ google.com

```
C:\Users\Windows>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.170.46] avec 32 octets de données :
Réponse de 172.217.170.46 : octets=32 temps=1824 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=1739 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=2008 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=1463 ms TTL=126

Statistiques Ping pour 172.217.170.46:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1463ms, Maximum = 2008ms, Moyenne = 1758ms
```


PC6 [VLAN20] ⇒ google.com

```
C:\Users\Windows>ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.170.46] avec 32 octets de données :
Réponse de 172.217.170.46 : octets=32 temps=2686 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=2540 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=2206 ms TTL=126
Réponse de 172.217.170.46 : octets=32 temps=1827 ms TTL=126

Statistiques Ping pour 172.217.170.46:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1827ms, Maximum = 2686ms, Moyenne = 2314ms
```

Test de connectivité internet réussi, le PC6 arrive à communiquer avec internet

Les PC des deux succursales peuvent communiquer avec internet

Test de l'Active Directory

Les bugs de ping énoncés plus haut nous empêchent de faire de l'Active Directory sur 6 pc répartie en 2 succursales nous avons donc choisi de ne mettre que 2 pc dans la topologie sous Windows 10 et 4 VPCs (1 PC Windows + 2 VPCs par succursale)

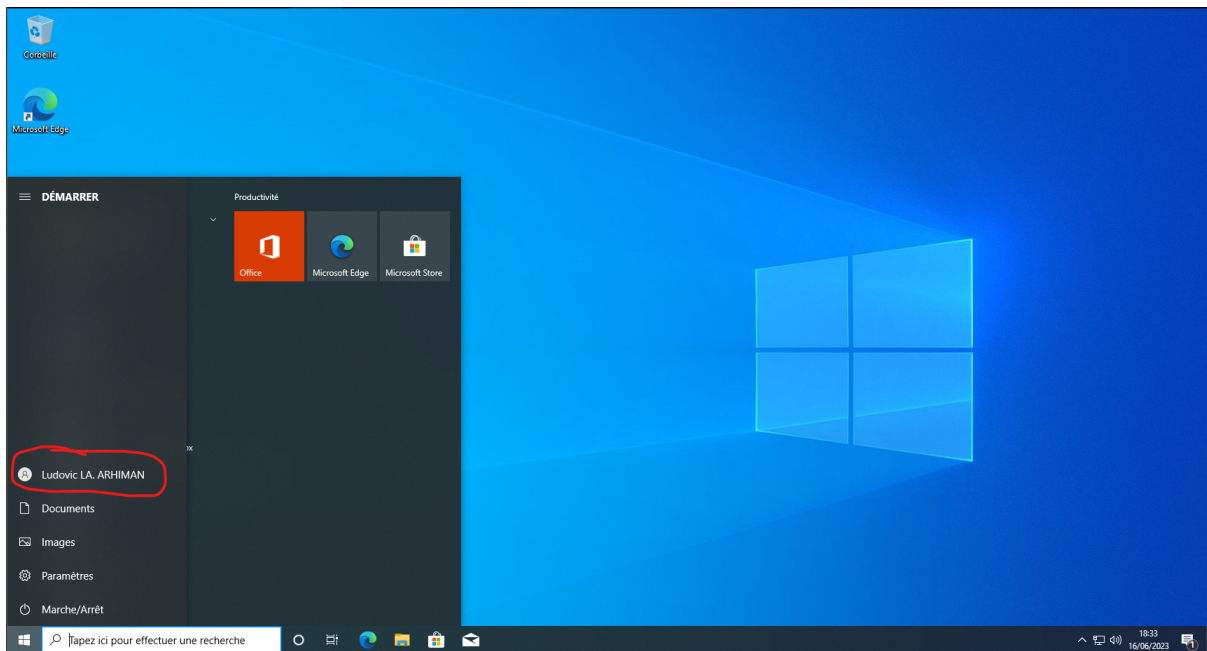
Test d'adhésion au domaine Active directory

PC1[VLAN 10] : SALLE 1

On se connecte avec l'utilisateur

l.arhiman avec le mot de passe 1234Admin1

sur le PC1. Ici on peut voir que l'on arrive à bien se connecter avec l'utilisateur



Test du serveur Linux

Test du serveur de partage de fichier Samba

Au cours de cette SAÉ 2.04, nous avons été confrontés à une configuration particulière. L'entreprise cliente dispose de deux succursales, pour lesquelles nous avons mis en place un serveur Windows, hébergeant les clients requis, ainsi qu'un serveur UNIX. Les postes clients fonctionnaient sous Windows, conformément aux exigences spécifiques de l'entreprise. De plus, nous avons intégré Zimbra Collaboration Suite, une suite logicielle de collaboration, pour faciliter la communication interne et la gestion des emails au sein de l'entreprise.

En tant que professionnels des réseaux et des télécommunications, cette mission nous a permis d'explorer des architectures variées, allant d'un simple réseau domestique à un réseau local d'entreprise. Notre rôle était de comprendre l'agencement des équipements de télécommunication, des équipements réseau, des terminaux et des protocoles indispensables au bon fonctionnement du réseau. Grâce à notre expertise et à notre engagement, nous avons réussi à mener à bien les différentes missions qui nous étaient confiées par nos clients, en veillant à leur entière satisfaction.