

---

# SAE.4.Cyber 01

-

## Compte rendu

Date	30/04/2025
Membre	LEBON Johan MONTEGU Jeremie LEPERLIER Aymeric

---

## **Table des matières**

<b>Introduction.....</b>	<b>3</b>
<b>Présentation de la situation.....</b>	<b>4</b>
<b>Topologie du LAB.....</b>	<b>4</b>
<b>Découpage en tâches.....</b>	<b>5</b>
- Tâche 1 – Pare-feu et DMZ.....	6
- Tâche 2 – Service web sécurisé.....	14
- Tâche 3 – Serveur de noms (DNS) primaire pour rt-bank.re.....	34
- Tâche 3 (suite) – Mise en place du DNS secondaire.....	37
- Tâche 4 – Mise en place et sécurisation de l'infrastructure Active Directory.....	39
<b>Conclusion.....</b>	<b>69</b>
<b>Tableau des acronymes.....</b>	<b>70</b>
<b>Annexe :.....</b>	<b>71</b>

---

## **Introduction**

Dans le cadre de la SAÉ 4.CYBER 0, notre équipe a été chargée de mettre en œuvre une infrastructure sécurisée pour RT Bank, une institution bancaire avec un site central à Saint-Denis et une succursale à Saint-Pierre. Ce projet vise à déployer et sécuriser un système d'information complet comprenant un pare-feu, des serveurs web en cluster dans une DMZ, un service DNS redondant, ainsi qu'une infrastructure Active Directory.

Les objectifs principaux de ce projet sont de :

- Mettre en place une architecture réseau sécurisée multi-sites
- Assurer la disponibilité et la sécurité des services critiques
- Implémenter les bonnes pratiques de cybersécurité selon les recommandations de l'ANSSI
- Garantir une gestion efficace et sécurisée des identités via Active Directory

Ce compte-rendu présente notre démarche, les solutions techniques mises en œuvre, ainsi que les résultats obtenus pour répondre aux exigences du cahier des charges.

## Présentation de la situation

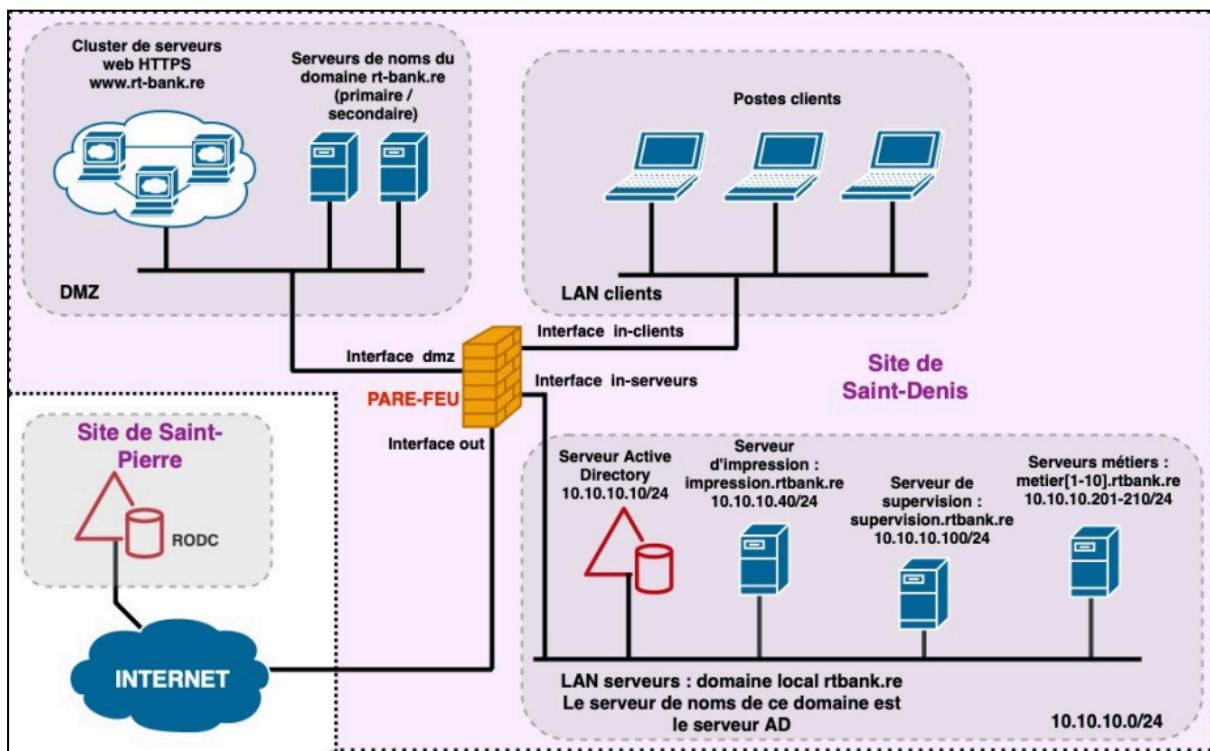
Vous êtes administrateur réseau et sécurité d'une institution bancaire nommée RT Bank.

Vous êtes chargé de mettre en place l'architecture présentée sur la diapositive suivante.

- Quelques informations complémentaires :

- o Le site central est situé à Saint-Denis, et une succursale est présente à Saint-Pierre.
- o Deux noms de domaines sont utilisés :
  - rt-bank.re : usage externe, pour identifier le serveur web public, pour définir les adresses mail, etc. Le serveur de noms associé est dans la DMZ.
  - rtkbank.re : usage interne, pour identifier les serveurs internes (impression, serveurs métiers) : le serveur de noms est réalisé par le serveur Active Directory. Ce domaine est strictement interne et ne doit être accessible que depuis le LAN des clients.

## Topologie du LAB



---

## **Découpage en tâches**

**Tâche 1** : installer un pare-feu avec quatre interfaces.

**Tâche 2** : mettre en place un cluster de serveurs web dans la DMZ.

Le service HTTP doit être sécurisé en :

- Disponibilité : redondance et équilibrage de charge
- Intégrité - Confidentialité - Authenticité (Preuve) : utilisation d'un certificat et configuration de TLS

**Tâche 3** : installer un serveur de noms pour le domaine **rt-bank.re** dans la DMZ et le sécuriser en disponibilité avec un serveur de noms secondaire

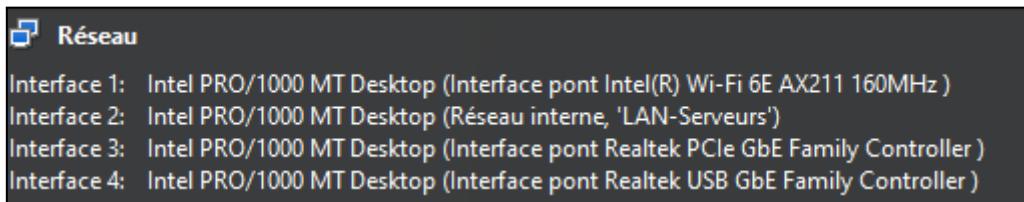
**Tâche 4** : installer et sécuriser un serveur Active Directory

---

## - Tâche 1 – Pare-feu et DMZ

Configuration du pare-feu PFSENSE et mise en place de la DMZ :

Configuration de quatre interfaces réseau sur VirtualBox :



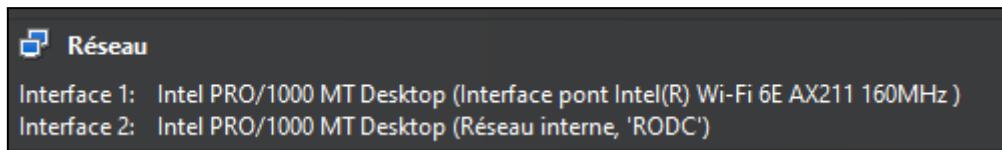
La première interface est configurée en mode pont pour la connexion WiFi, permettant l'accès Internet au pare-feu.

La deuxième interface est dédiée au LAN-Serveurs en réseau interne, configurée sur la même machine que PFSense.

La troisième interface est configurée en mode pont vers un premier PC via câble RJ45, permettant la connexion des machines de la DMZ.

La quatrième interface est également configurée en mode pont, utilisant un adaptateur USB-RJ45 sur le PC principal pour connecter un second PC. Cette interface est dédiée au LAN-Clients.

Configuration du second pare-feu avec deux interfaces :



La première interface est configurée en mode pont pour la connexion WiFi, assurant l'accès Internet.

La deuxième interface est dédiée au réseau interne du RODC.

## - Plan d'adressage

Configuration réseau détaillée pour chaque interface et machine sur le pare-feu principal :

Interface	Adresse	Masque	Gateway
WAN (em0)	192.168.51.75	255.255.254.0	192.168.50.1
LAN-Serveurs (em1)	10.10.10.1	255.255.255.0	
Serveur AD	10.10.10.10	255.255.255.0	10.10.10.1
Serveur d'impression	10.10.10.40	255.255.255.0	10.10.10.1
Serveur de Supervision	10.10.10.100	255.255.255.0	10.10.10.1
Serveur métier 1	10.10.10.201	255.255.255.0	10.10.10.1
Serveur métier 2	10.10.10.202	255.255.255.0	10.10.10.1
DMZ (em2)	172.16.10.1	255.255.255.0	
Serveur Apache 1	172.16.10.10	255.255.255.0	172.16.10.1
Serveur Apache 2	172.16.10.11	255.255.255.0	172.16.10.1
Serveur HAProxy 1	172.16.10.15	255.255.255.0	172.16.10.1
Serveur HAProxy 2	172.16.10.16	255.255.255.0	172.16.10.1
Serveur DNS 1	172.16.10.20	255.255.255.0	172.16.10.1
Serveur DNS 2	172.16.10.21	255.255.255.0	172.16.10.1
LAN-Clients (em3)	192.168.100.1	255.255.255.0	
Client 1	DHCP via AD	255.255.255.0	192.168.100.1
Client 2	DHCP via AD	255.255.255.0	192.168.100.1
Client 3	DHCP via AD	255.255.255.0	192.168.100.1

Configuration réseau détaillée pour chaque interface et machine sur le pare-feu secondaire :

Interface	Adresse	Masque	Gateway
WAN (em0)	192.168.51.76	255.255.254.0	192.168.50.1
LAN-Serveurs (em1)	10.10.20.1	255.255.255.0	
Serveur AD RODC	10.10.20.10	255.255.255.0	10.10.20.1

### - Configuration du NAT statique

Une règle de NAT statique a été configurée pour rediriger le trafic vers notre serveur web sur le port 8080. Cette configuration permet d'assurer l'accessibilité du service web depuis l'extérieur tout en maintenant la sécurité de notre infrastructure.

Transfert de port										
Règles										
	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	8080	172.16.10.100	443 (HTTPS)		  

### - Configuration des règles de pare feu

#### WAN

Flottant(e) WAN LAN OPT1 OPT2 IPsec											
Règles (Faire glisser pour changer l'ordre)											
	États	Protocole	Source	Port	Destination	Port	Passerelle	d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/>	0/197 KiB	IPv4 TCP/ UDP	WAN subnets	*	WAN address	53 (DNS)	*			aucun	  
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	172.16.10.100	443 (HTTPS)	*			aucun	NAT   

Pour commencer notre première règle concerne la gestion du service DNS, où nous autorisons le trafic sur le port 53 pour permettre la résolution des noms de domaine depuis l'extérieur vers nos serveurs DNS internes.

## LAN-SERVEURS

Règles (Faire glisser pour changer l'ordre)											
	Etats	Protocole	Source	Port	Destination	Port	Passerelle	d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/>	0/1,87 MiB	*	*	*	LAN Address	443 80	*	*		Règle anti-bloque	
<input type="checkbox"/>	109/36,17 MiB	IPv4	*	LAN subnets	*	*	*	*	aucun	Default allow LAN to any rule	  

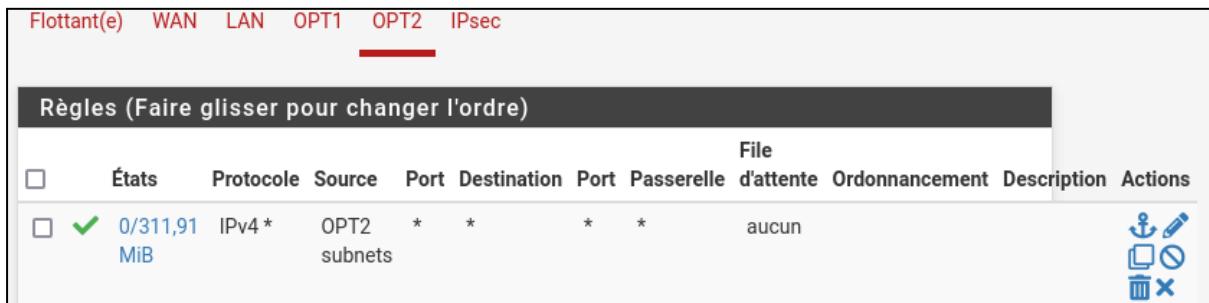
En ce qui concerne le réseau LAN-SERVEURS, nous avons initialement configuré une politique d'accès permissive pour faciliter la phase de déploiement. Cette configuration temporaire autorise tous les accès sortants depuis le LAN-SERVEURS. Une fois l'infrastructure stabilisée, nous affinerons ces règles de filtrage pour appliquer une politique de sécurité plus restrictive, suivant le principe du moindre privilège.

## DMZ

Règles (Faire glisser pour changer l'ordre)											
	Etats	Protocole	Source	Port	Destination	Port	Passerelle	d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP/ UDP	*	*	*	53 (DNS)	*				  

Pour la DMZ, nous avons implémenté une règle de filtrage spécifique pour le service DNS. Cette configuration autorise le trafic UDP/TCP sur le port 53, permettant ainsi aux serveurs DNS de notre DMZ de répondre aux requêtes de résolution de noms. Cette règle constitue une première étape dans la sécurisation de notre DMZ, et nous ajusterons les paramètres de sécurité au fur et à mesure du déploiement des autres services.

## LAN-CLIENTS



The screenshot shows a network configuration interface with a header bar containing "Flottant(e)", "WAN", "LAN", "OPT1", "OPT2", and "IPsec". Below this is a section titled "Règles (Faire glisser pour changer l'ordre)". A table lists a single rule:

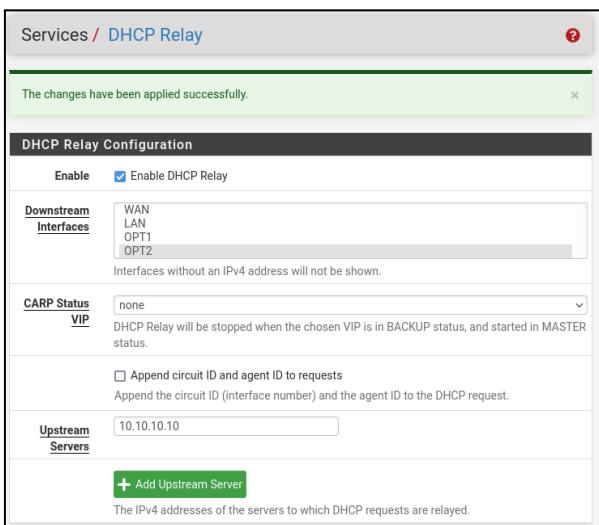
	Etats	Protocole	Source	Port	Destination	Port	Passerelle d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/311,91 MiB	IPv4 *	OPT2 subnets	*	*	*	*	aucun		 

Pour le réseau LAN-CLIENTS, nous avons établi une règle de filtrage permettant la communication entre les sous-réseaux. Cette configuration initiale assure la connectivité de base pour les postes clients. Comme pour les autres segments du réseau, nous affinerons progressivement ces règles pour optimiser la sécurité tout en maintenant les fonctionnalités nécessaires aux utilisateurs.

### - Configuration du relai DHCP pour l'AD

Un serveur DHCP a été implémenté dans l'Active Directory pour gérer la distribution automatique des adresses IP dans le réseau LAN-Clients. La configuration comprend :

- Activation de l'option DHCP Relay sur PFsense
- Définition des interfaces de distribution
- Configuration de l'adresse IP du serveur DHCP
- Paramétrage des plages d'adresses à distribuer



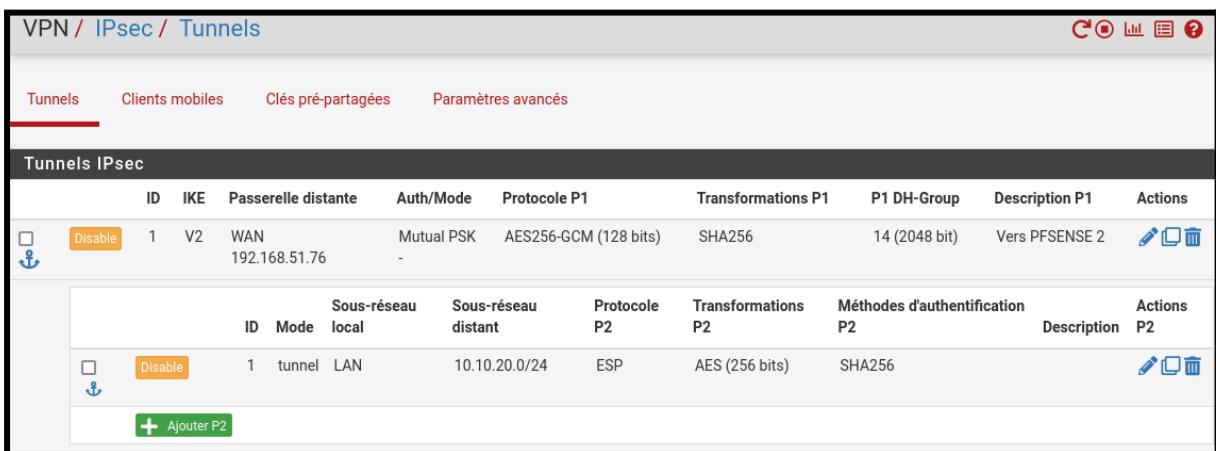
The screenshot shows the "DHCP Relay Configuration" screen. It includes fields for "Enable" (checked), "Downstream Interfaces" (set to OPT2), "CARP Status" (set to "none"), and "Upstream Servers" (set to 10.10.10.10). A message at the top indicates "The changes have been applied successfully."

### - Configuration du VPN IPsec sur les deux pare-feu

Pour établir une connexion sécurisée entre les deux sites de RT Bank, nous avons mis en place un tunnel VPN IPsec. Sur le premier pare-feu, nous avons utilisé l'adresse IP 192.168.51.75 comme point de terminaison. Le tunnel a été configuré avec des paramètres de sécurité robustes, notamment le protocole de chiffrement AES256-GCM avec une clé de 128 bits, garantissant ainsi la confidentialité des données transmises.

La configuration de la Phase 2 du tunnel IPsec a été effectuée en spécifiant le réseau LAN comme sous-réseau local. Pour renforcer la sécurité, nous avons implémenté le protocole d'authentification SHA256, assurant l'intégrité des données échangées entre les sites.

Des règles de filtrage spécifiques ont été mises en place pour gérer le trafic VPN. Ces règles, configurées en IPv4, permettent la communication avec les sous-réseaux LAN et assurent un fonctionnement bidirectionnel du tunnel. Cette configuration permet aux utilisateurs des deux sites de communiquer de manière sécurisée, tout en maintenant une séparation claire entre les différents réseaux.



The screenshot shows two main sections of a network configuration interface:

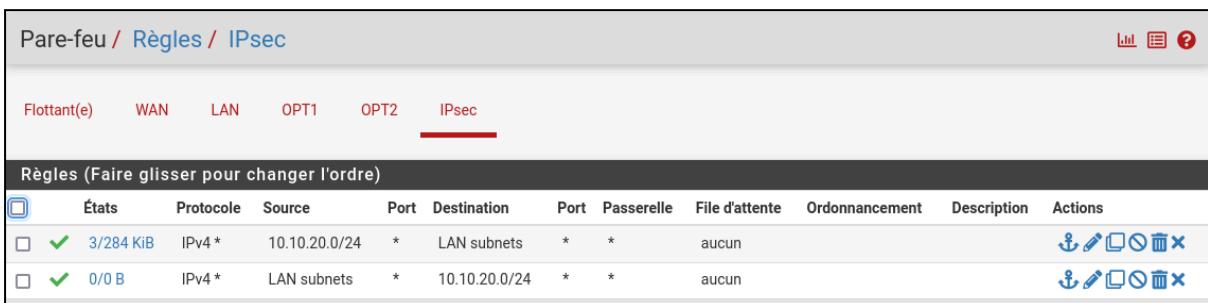
- Tunnels / IPsec / Tunnels:** This section displays an IPsec tunnel configuration. The table has columns for ID, IKE, Passerelle distante, Auth/Mode, Protocole P1, Transformations P1, P1 DH-Group, Description P1, and Actions. One entry is shown:
 

<input type="checkbox"/>	Disable	1	V2	WAN 192.168.51.76	Mutual PSK	AES256-GCM (128 bits)	SHA256	14 (2048 bit)	Vers PFSENSE 2	
--------------------------	---------	---	----	----------------------	------------	-----------------------	--------	---------------	----------------	--

 A detailed view of the tunnel parameters is also shown:
 

ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description P2	Actions
1	tunnel	LAN	10.10.20.0/24	ESP	AES (256 bits)	SHA256		
- Pare-feu / Règles / IPsec:** This section displays IPsec rule configurations. The table has columns for Flottant(e), WAN, LAN, OPT1, OPT2, and IPsec. Two rules are listed:
 

Flottant(e)	WAN	LAN	OPT1	OPT2	IPsec				
<input type="checkbox"/>	✓ 3/284 KIB	IPv4 *	10.10.20.0/24	*	LAN subnets	*	*	aucun	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN subnets	*	10.10.20.0/24	*	*	aucun	



This screenshot shows the IPsec rule configuration section from the previous interface. It lists two rules:

États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓ 3/284 KIB	IPv4 *	10.10.20.0/24	*	LAN subnets	*	*	aucun		
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	LAN subnets	*	10.10.20.0/24	*	*	aucun		

Utilisation de l'adresse 192.168.51.76 pour le deuxième pfSense

VPN / IPsec / Tunnels

IPsec Tunnels																															
ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description Actions																								
<input type="checkbox"/>	1	V2 WAN 192.168.51.75	Mutual PSK -	AES256-GCM (128 bits)	SHA256	14 (2048 bit)	Vers PFSENSE 1																								
<table border="1"> <thead> <tr> <th>ID</th> <th>Local Mode Subnet</th> <th>Remote Subnet</th> <th>P2 Protocol</th> <th>P2 Transforms</th> <th>P2 Auth Methods</th> <th>P2 Description</th> <th>P2 actions</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> </td> <td>1 tunnel LAN</td> <td>10.10.10.0/24</td> <td>ESP</td> <td>AES (256 bits)</td> <td>SHA256</td> <td></td> <td> </td> </tr> <tr> <td colspan="8"><a href="#">+ Add P2</a></td> </tr> </tbody> </table>								ID	Local Mode Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 Description	P2 actions	<input type="checkbox"/>	1 tunnel LAN	10.10.10.0/24	ESP	AES (256 bits)	SHA256			<a href="#">+ Add P2</a>							
ID	Local Mode Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 Description	P2 actions																								
<input type="checkbox"/>	1 tunnel LAN	10.10.10.0/24	ESP	AES (256 bits)	SHA256																										
<a href="#">+ Add P2</a>																															

Firewall / Rules / IPsec

Rules (Drag to Change Order)										
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description Actions
<input type="checkbox"/>	3/13 KIB	IPv4 *	10.10.10.0/24	*	LAN subnets	*	*	none		
<input type="checkbox"/>	0/0 B	IPv4 *	LAN subnets	*	10.10.10.0/24	*	*	none		

## - Configuration du Résolveur DNS

**Options générales du DNS Resolver**

<b>Activer</b>	<input checked="" type="checkbox"/> Activer les résolutions DNS
<b>Port d'écoute</b>	53
Le port utilisé pour répondre aux requêtes DNS. Il devrait normalement être laissé vide, à moins qu'un autre service n'ait besoin d'utiliser le port TCP/UDP numéro 53.	
<b>Activer le service SSL/TLS</b>	<input type="checkbox"/> Répondre aux requêtes SSL/TLS entrantes des clients locaux. Configure le DNS Resolver pour agir comme un serveur DNS sur SSL/TLS qui peut répondre aux requêtes des clients qui supportent également le DNS sur TLS. L'activation de cette option désactive le comportement de routage automatique de la réponse de l'interface, donc elle fonctionne mieux avec des liaisons d'interface spécifiques.
<b>Certificat SSL/TLS</b>	GUI default (67e63fae82ede)
Le certificat de serveur à utiliser pour le service SSL/TLS, la chaîne CA sera déterminée automatiquement.	
<b>Port d'écoute SSL/TLS</b>	853
Le port utilisé pour répondre aux requêtes DNS SSL/TLS ; il devrait normalement être laissé vide, à moins qu'un autre service n'ait besoin de se lier au port TCP/UDP 853.	
<b>Interfaces réseau</b>	Tout WAN LAN OPT1 OPT2
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.	
<b>Interfaces réseau sortantes</b>	Tout WAN LAN OPT1 OPT2
Interfaces réseau utilisées par le DNS Resolver pour envoyer des requêtes aux serveurs faisant autorité et pour recevoir leurs réponses. Par défaut, toutes les interfaces sont utilisées.	

**Surcharges d'hôtes**

Hôte	Domaine parent de l'hôte	IP à renvoyer pour l'hôte	Description	Actions
www	rt-bank.re	192.168.51.75		 

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and

Paramètres généraux   Paramètres avancés   Listes d'accès

Listes d'accès pour contrôler l'accès au serveur de résolution DNS

Nom de liste d'accès	Action	Description	Actions
DNS PUBLIC	allow		 

Nouvelle liste d'accès

**Nom de la liste d'accès**

DNS PUBLIC

Donner un nom de liste d'accès.

**Action**

Autoriser

**Interdire:** Arrête les requêtes des hôtes dans le netblock défini ci-dessous.

**Refuser:** Arrête les requêtes des hôtes dans le netblock défini ci-dessous, mais envoie un message d'erreur DNS rcode REFUSED au client.

**Autoriser:** Autoriser les requêtes des hôtes dans le netblock défini ci-dessous.

**Autoriser Snoop:** Autoriser l'accès récursif et non récurrent des hôtes dans le netblock défini ci-dessous. Utilisé pour le snooping du cache et idéalement, ne doit être configuré que pour l'hôte administratif.

**Interdire Non-local:** Permet uniquement les requêtes autorisées de données locales à partir d'hôtes dans le netblock défini ci-dessous. Les messages refusés sont abandonnés.

**Refuser Non-local:** Permet uniquement les requêtes autorisées de données locales des hôtes dans le netblock défini ci-dessous. Envoie un message d'erreur DNS rcode REFUSED au client pour les messages qui ne sont pas autorisés.

**Description**

Une description doit être renseignée ici pour référence administrative.

**Réseaux**

192.168.51.75

/ 23

Réseau/masque

Description

---

- **Tâche 2 – Service web sécurisé**

### **Installation du premier serveur web Apache**

Pour assurer un service web sécurisé et performant, nous avons procédé à l'installation du serveur Apache en plusieurs étapes structurées :

- **Installation des packages**

Nous avons d'abord effectué une mise à jour complète du système en exécutant la commande 'sudo apt update' pour actualiser la liste des paquets disponibles, suivie de 'sudo apt upgrade' pour mettre à jour l'ensemble des packages installés. Ensuite, nous avons procédé à l'installation du serveur Apache2 via la commande dédiée.

```
# Mettre à jour la liste des paquets disponibles  
sudo apt update
```

```
# Mettre à jour tous les paquets installés  
sudo apt upgrade
```

```
# Installer le serveur web Apache  
sudo apt install apache2
```

- **Vérification du service :**

Après l'installation, nous avons vérifié la disponibilité du service web en deux temps :

J'ai tout d'abord installé netstat avec la commande :

```
apt-get install net-tools
```

Puis j'ai vérifié que le port 80 était bien en écoute avec la commande suivante:

```
netstat -ntl
```

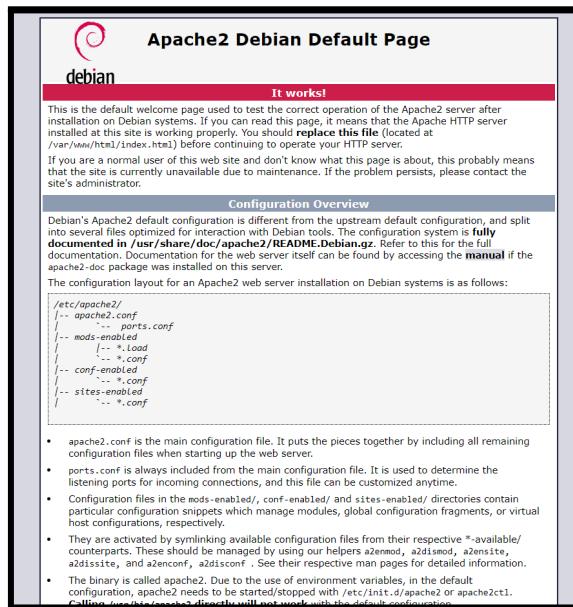
```
root@debian:~# netstat -ntl
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale           Adresse distante       Etat
tcp      0      0 127.0.0.1:631              0.0.0.0:*
                                         ::::*
tcp6     0      0 :::80                      ::::*
                                         ::::*
tcp6     0      0 :::1:631                  ::::*
                                         ::::* LISTEN
                                         ::::* LISTEN
                                         ::::* LISTEN
```

L'analyse des résultats confirme que le serveur Apache est correctement installé et opérationnel, avec le port 80 en état d'écoute (LISTEN) sur toutes les interfaces réseau (0.0.0.0). Cette configuration permet d'accepter les connexions entrantes sur l'ensemble des interfaces disponibles.

#### - Test de validation du serveur web

Après l'installation, nous avons procédé à la vérification de l'accessibilité du serveur Apache. En utilisant l'adresse IP du serveur dans un navigateur web, nous avons pu accéder à la page d'accueil par défaut d'Apache2 sur Debian. L'affichage correct de cette page de test confirme plusieurs points essentiels :

- Le serveur web Apache est correctement installé et en cours d'exécution
- Le service est accessible via le réseau
- La configuration de base est fonctionnelle



---

## **Modification de la page d'accueil**

### **- Localisation et analyse des fichiers de configuration**

Pour personnaliser la page d'accueil du serveur web, nous avons d'abord procédé à l'identification des fichiers de configuration essentiels. En examinant le répertoire '/etc/apache2/sites-available', nous avons pu localiser les fichiers de configuration par défaut du serveur Apache2.

```
cd /etc/apache2/sites-available
```

```
<VirtualHost *:80>
    # The ServerName directive sets the request so
    # the server uses to identify itself. This is
    # redirection URLs. In the context of virtual
    # specifies what hostname must appear in the r
    # match this virtual host. For the default vi
    # value is not decisive as it is used as a las
    # However, you must set it for any further vi
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
```

La capture d'écran montre le contenu du répertoire sites-available avec les fichiers de configuration par défaut.

Le fichier 000-default.conf contient la configuration du site par défaut, dont la directive DocumentRoot qui pointe vers le dossier /var/www/html.

---

- **Analyse du contenu web par défaut**

Une inspection du répertoire '/var/www/html' a révélé la présence du fichier index.html, qui constitue la page d'accueil par défaut d'Apache.

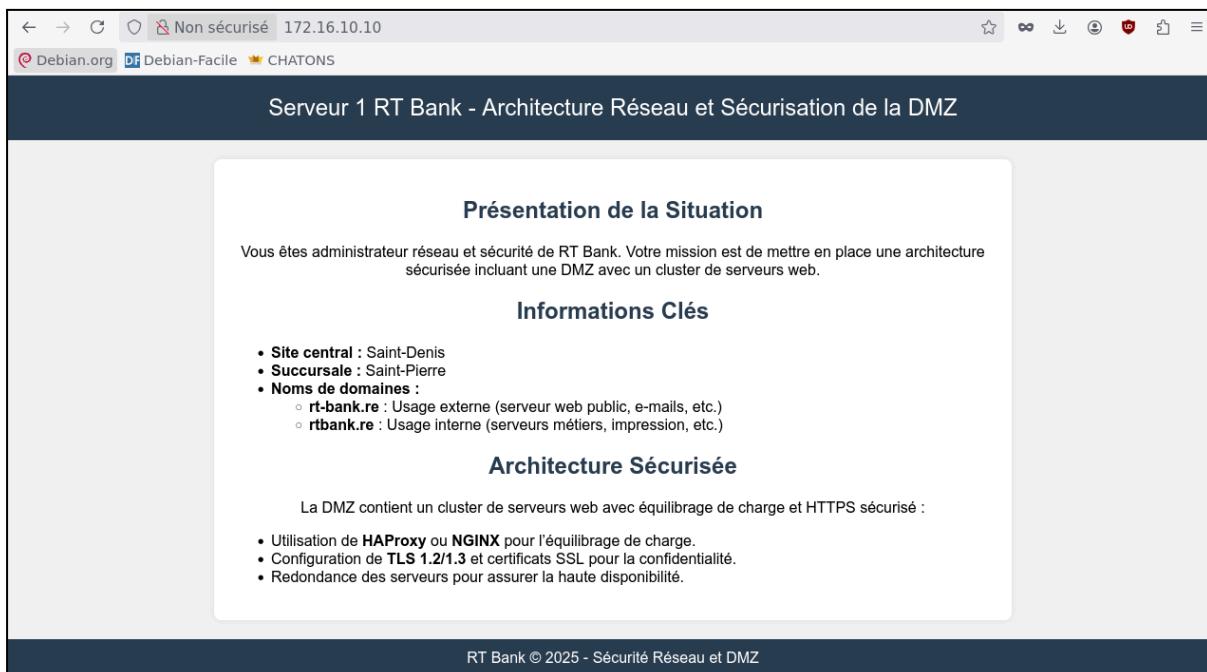
```
ls /var/www/html
```

```
root@debian:/etc/apache2/sites-available# ls /var/www/html/
index.html
```

- **Personnalisation de la page d'accueil**

Nous avons ensuite procédé à la personnalisation de la page d'accueil pour refléter l'identité de RT Bank. La nouvelle interface comprend :

- Une présentation claire de la situation et du contexte
- Les informations clés sur l'infrastructure
- Une description détaillée de l'architecture sécurisée
- L'identification spécifique "Serveur 1"



---

## **Sécurisation HTTPS**

### **- Génération du certificat auto-signé**

Pour sécuriser notre serveur web, nous avons d'abord installé OpenSSL. Nous avons ensuite généré un certificat auto-signé avec une validité de 365 jours et une clé RSA de 2048 bits. Lors de la configuration, nous avons spécifié le nom de domaine complet (FQDN) comme [www.rt-bank.re](http://www.rt-bank.re).

```
apt-get install openssl
cd /etc/apache2
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -out /etc/apache2/server.pem -keyout
/etc/apache2/server.key
```

### **- Création du site sécurisé**

Nous avons créé une architecture dédiée pour le site HTTPS, comprenant : un dossier distinct pour le contenu HTTPS, une page d'accueil spécifique pour la version sécurisée.

```
cd /var/www
mkdir html_ssl
nano index.html
```

### **- Configuration HTTPS**

La sécurisation a été effectuée en deux étapes : Activation du module SSL d'Apache, Configuration du site sécurisé par défaut via a2ensite

```
#Activer le module ssl :
sudo a2enmod ssl
#puis le site sécurisé :
sudo a2ensite default-ssl
```

- **Configuration du site sécurisé**

Le fichier default-ssl.conf a été modifié pour établir la configuration du VirtualHost HTTPS, permettant ainsi une connexion sécurisée au serveur web.

```
cd /etc/apache2/sites-available
nano default-ssl.conf

<VirtualHost *:443>
    DocumentRoot /var/www/html_ssl
    ServerName www.rt-bank.re
    SSLEngine on
    SSLCertificateFile /etc/apache2/server.pem
    SSLCertificateKeyFile /etc/apache2/server.key
</VirtualHost>
```

- **Validation de la configuration HTTPS**

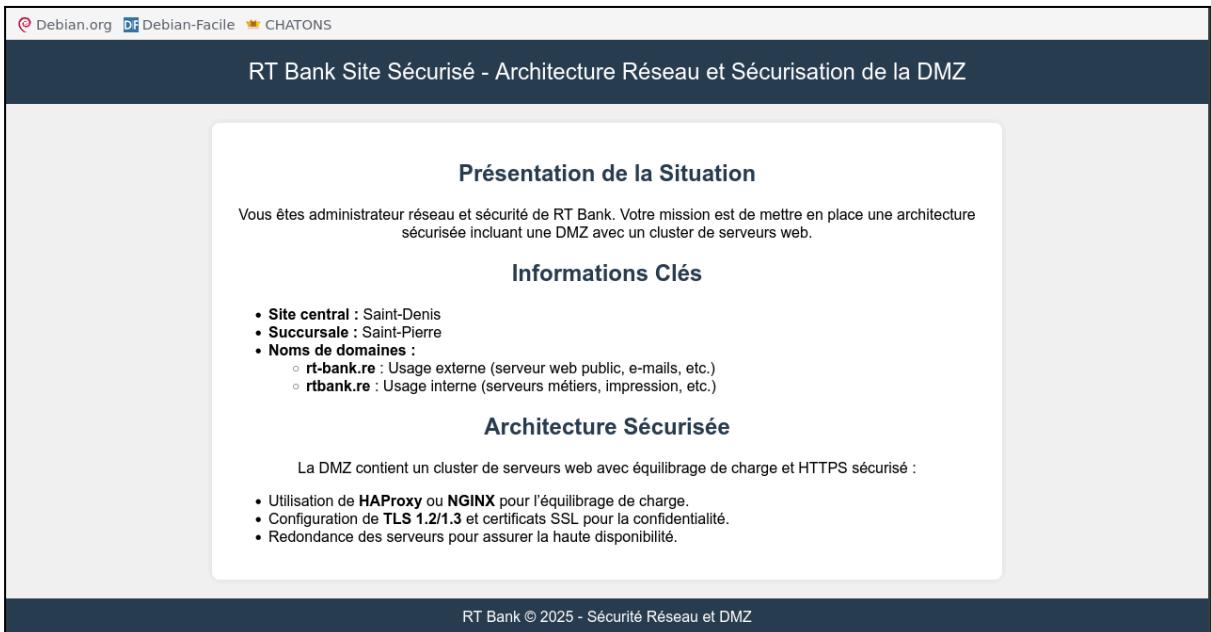
Une analyse des ports actifs via la commande netstat a confirmé la configuration correcte du serveur Apache : Port 443 (HTTPS) opérationnel et en état d'écoute, Port 80 (HTTP) maintenu pour la compatibilité, Les deux services sont correctement configurés sur toutes les interfaces (0.0.0.0)

```
netstat -ntl
```

```
root@debian:/etc/apache2/sites-available# netstat -ntl
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Adresse locale                Adresse distante      Etat
tcp      0      0 127.0.0.1:631                  0.0.0.0:*
                                         ::::*
                                         ::::*
                                         ::::*
                                         ::::*
                                         ::::*
                                         ::::*
```

---

J'ai ensuite accédé au site sécurisé en HTTPS :



The screenshot shows a web browser window with the following details:

- Top bar: Debian.org, Debian-Facile, CHATONS
- Title bar: RT Bank Site Sécurisé - Architecture Réseau et Sécurisation de la DMZ
- Main content area:
  - Présentation de la Situation**: You are a network and security administrator for RT Bank. Your mission is to implement a security architecture including a DMZ with a web server cluster.
  - Informations Clés**:
    - Site central : Saint-Denis
    - Succursale : Saint-Pierre
    - Noms de domaines :
      - rt-bank.re : External usage (public web server, emails, etc.)
      - rtbank.re : Internal usage (business servers, printing, etc.)
  - Architecture Sécurisée**: The DMZ contains a load-balanced web server cluster with HTTPS security.
    - Use of HAProxy or NGINX for load balancing.
    - TLS 1.2/1.3 configuration and SSL certificates for confidentiality.
    - Redundant servers for high availability.
- Bottom bar: RT Bank © 2025 - Sécurité Réseau et DMZ

Comme attendu, le navigateur affiche un avertissement de sécurité en raison de l'utilisation d'un certificat auto-signé. Après acceptation de l'exception de sécurité, l'accès au site HTTPS est pleinement fonctionnel, confirmant ainsi la bonne configuration du protocole de sécurité.

---

- **Configuration TLS**

```
#activer le module headers
sudo a2enmod headers

#Modifiez le fichier de configuration TLS :
sudo nano /etc/apache2/mods-available/ssl.conf

#Ajoutez ou modifiez les paramètres suivants :
SSLPotocol all -SSLv3 -TLSv1 -TLSv1.1 # Désactive SSLv3, TLS 1.0 et
1.1
SSLCipherSuite HIGH:!aNULL:!MD5          # Utilise des suites
cryptographiques sécurisées
SSLHonorCipherOrder on                   # Priorise les choix du serveur
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains" # Active HSTS

#Verification configuration TLS
openssl s_client -connect 192.168.50.68:443
```

```

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 18 (self-signed certificate)
---

Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol : TLSv1.3
    Cipher   : TLS_AES_256_GCM_SHA384
    Session-ID: 5C5030816B36648AE6497C98DADAAFFCC1EB5A70DFB8A4A3F7FD2F3C11F27F77D
    Session-ID-ctx:
        Resumption PSK: 74F167891244BEBBCA2389D3041206DE02617AD2723D20417E3BCEF8CF18
04F6D0A91ECC9341ACF9FCD3FB10B95840D5
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - f2 bf eb 73 b7 aa 34 24-57 75 6b 2d c2 1c 67 d3  ...s..4$Wuk-..g.
    0010 - 01 d7 b3 2b 73 b0 f0 05-93 b3 f3 8f a4 5e af c1  ...+s.....^..

    Start Time: 1743140553
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0

---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol : TLSv1.3
    Cipher   : TLS_AES_256_GCM_SHA384
    Session-ID: 5287E0D8F303FD6DDDA9D14F01C7A28541C03887333E7BDA7FC856D36934165F
    Session-ID-ctx:
        Resumption PSK: 73054DA707FA3C16D2C876747CC2E0B4F36B08D52FE479A2AFB556704C0D
35B3194CB65ED306E63BFA6A745B3E7E2592
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - 8e 01 c0 f3 ec ea e9 17-b9 3a 7d 15 d2 49 79 7a  ....:}..Iyz
    0010 - 73 0d 67 18 4d 99 6e e3-a0 5f 92 e3 98 42 0e 4c  s.g.M.n._...B.L

    Start Time: 1743140553
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: no
    Max Early Data: 0

---
read R BLOCK
closed

```

---

## **Mise en place de la haute disponibilité**

### **- Installation du second serveur Apache**

Pour assurer la redondance du service web, nous avons déployé un second serveur Apache sur une nouvelle machine virtuelle. Cette installation reprend la configuration du premier serveur, avec une modification de la page d'accueil pour l'identifier comme "Serveur 2".

### **- Installation et configuration de HAProxy**

HAProxy (High Availability Proxy) est un logiciel libre de répartition de charge et de mise en miroir de serveurs au sein d'un cluster. Il peut être utilisé pour équilibrer la charge entre plusieurs serveurs, pour rediriger les requêtes vers des serveurs en cas de panne d'un élément du cluster, et pour protéger les serveurs contre les attaques de déni de service (DoS).

HAProxy a été installé sur une troisième machine virtuelle pour assurer : La répartition de charge entre les serveurs web, La redirection des requêtes en cas de panne, La protection contre les attaques par déni de service (DDoS)

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install haproxy
```

### **- Configuration de HAProxy**

Le fichier de configuration /etc/haproxy/haproxy.cfg a été paramétré avec : Un frontend écoutant sur les ports 80 (HTTP) et 443 (HTTPS), Un backend configuré en mode HTTP avec équilibrage de charge roundrobin, Des vérifications de santé (health checks) sur les deux serveurs web, La gestion des cookies pour assurer la persistance des sessions

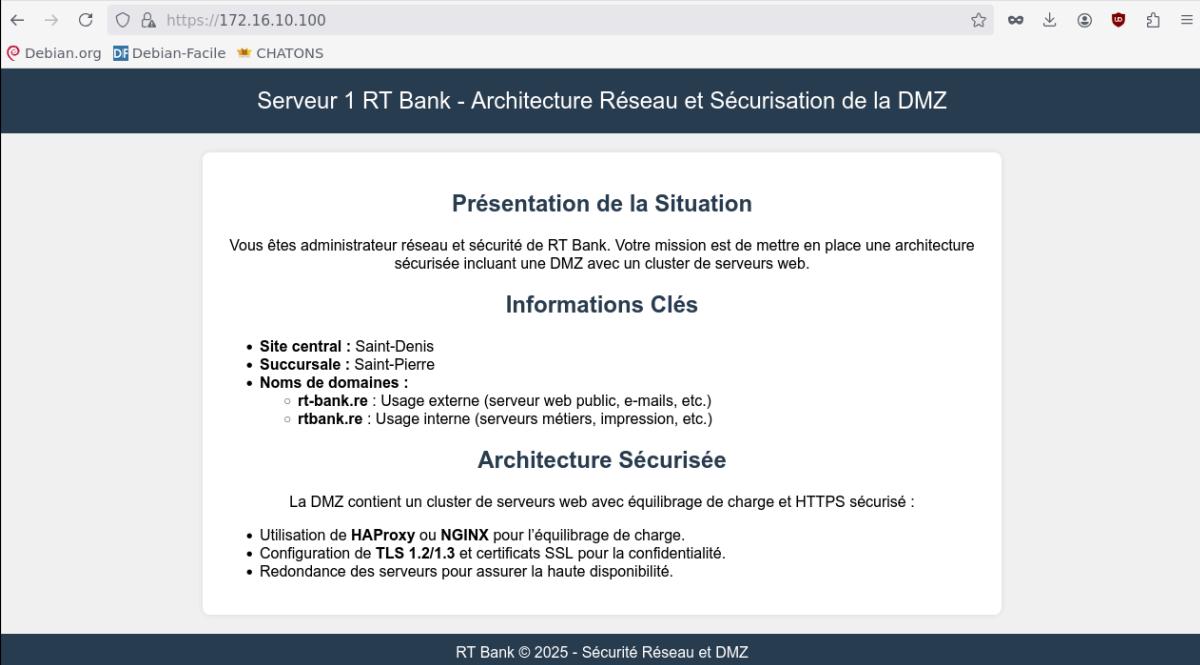
```
frontend front
    bind 172.16.10.100:80
    default_backend serveurs_web
    bind 172.16.10.100:443 ssl crt /etc/ssl/certs/haproxy.pem

backend serveurs_web
    mode http
    cookie SERVEURUSED insert indirect nocache
    balance roundrobin
    server serveur1 172.16.10.10:80 cookie serveur1 check
    server serveur2 172.16.10.11:80 cookie serveur2 check
```

---

- **Tests de validation de la haute disponibilité**

**Test 1: Vérification de l'accès via HAProxy**



← → C ⌂ ⓘ https://172.16.10.100

Debian.org Debian-Facile CHATONS

Serveur 1 RT Bank - Architecture Réseau et Sécurisation de la DMZ

Présentation de la Situation

Vous êtes administrateur réseau et sécurité de RT Bank. Votre mission est de mettre en place une architecture sécurisée incluant une DMZ avec un cluster de serveurs web.

Informations Clés

- Site central : Saint-Denis
- Succursale : Saint-Pierre
- Noms de domaines :
  - rt-bank.re : Usage externe (serveur web public, e-mails, etc.)
  - rtbody.re : Usage interne (serveurs métiers, impression, etc.)

Architecture Sécurisée

La DMZ contient un cluster de serveurs web avec équilibrage de charge et HTTPS sécurisé :

- Utilisation de **HAProxy** ou **NGINX** pour l'équilibrage de charge.
- Configuration de **TLS 1.2/1.3** et certificats SSL pour la confidentialité.
- Redondance des serveurs pour assurer la haute disponibilité.

RT Bank © 2025 - Sécurité Réseau et DMZ

Les tests ont confirmé l'accès réussi aux serveurs web via l'adresse IP du répartiteur de charge HAProxy (172.16.10.100). La page web s'affiche correctement avec tous ses éléments, démontrant le bon fonctionnement de la configuration de base.

**Test 2: Vérification de l'alternance entre serveurs**

L'alternance entre les serveurs a été vérifiée en effectuant des rafraîchissements successifs de la page. Le comportement observé confirme que : La méthode “roundrobin” fonctionne comme prévu, les requêtes sont distribuées de manière séquentielle entre les serveurs, à chaque nouvelle connexion, HAProxy bascule automatiquement vers le serveur suivant

Cette configuration assure une répartition équitable de la charge et garantit la continuité du service en cas de défaillance d'un des serveurs.

### - Persistante basée sur des cookies

Le paramètre cookie déclenche la persistante basée sur les cookies. Il demande à HAProxy d'envoyer un cookie au client et de l'associer avec le nom du serveur qui a fourni la réponse initiale. Cela permet au client de continuer à communiquer avec ce même serveur pendant toute la durée de sa session.

### - Configuration de la persistante des sessions

La persistante des sessions a été configurée dans le backend de HAProxy avec les paramètres suivants : Utilisation de cookies pour le suivi des sessions, Configuration spécifique pour chaque serveur avec des identifiants uniques, Serveur 1 : 172.16.10.10:80 avec cookie serveur1, Serveur 2 : 172.16.10.11:80 avec cookie serveur2.

```
cookie SERVERUSED insert indirect nocache
server apache1 172.16.10.10:80 cookie serveur1
server apache2 172.16.10.11:80 cookie serveur2
```

Serveur 1 RT Bank - Architecture Réseau et Sécurisation de la DMZ

**Présentation de la Situation**

Vous êtes administrateur réseau et sécurité de RT Bank. Votre mission est de mettre en place une architecture sécurisée incluant une DMZ avec un cluster de serveurs web.

**Informations Clés**

- Site central : Saint-Denis
- Succursale : Saint-Pierre
- Noms de domaines :
  - rt-bank.re : Usage externe (serveur web public, e-mails, etc.)
  - rtbank.re : Usage interne (serveurs métiers, impression, etc.)

**Architecture Sécurisée**

La DMZ contient un cluster de serveurs web avec équilibrage de charge et HTTPS sécurisé :

- Utilisation de **HAProxy** ou **NGINX** pour l'équilibrage de charge.
- Configuration de **TLS 1.2/1.3** et certificat SSL pour la confidentialité.
- Redondance des serveurs pour assurer la haute disponibilité.

RT Bank © 2025 - Sécurité Réseau et DMZ

Cookies											Filtrer les éléments	
	Nom	Valeur	Domain	Path	Expiration / Durée maximum	Taille	HttpOnly	Secure	SameSite	Dernier accès	G	
https://172.16.10.100	SERVEURUSED	serveur1	172.16.10.100	/	Session	19	false	false	None	Wed, 09 Apr 2025 04:24:33 GMT	+ G	
Stockage de session												
Stockage cache												
Indexed DB												
Stockage local												

Les tests de validation ont confirmé l'efficacité de cette configuration : lors d'accès répétés, le navigateur est systématiquement dirigé vers le même serveur (serveur 1), démontrant que la persistante des sessions basée sur les cookies fonctionne correctement. Cette configuration garantit une expérience utilisateur cohérente tout en maintenant l'équilibrage de charge.

---

- **Visualisation des statistiques**

Avec HAProxy Stats, il est possible de visualiser des informations sur le nombre de connexions, le transfert de données, l'état du serveur, et plus encore. Comme il est basé sur un navigateur, il suffit d'utiliser un navigateur web pour obtenir des informations en temps réel sur l'implémentation HAProxy.

- **Configuration des statistiques HAProxy**

Nous avons ajouté une section frontend dédiée aux statistiques dans le fichier haproxy.cfg avec les paramètres suivants : Activation des statistiques via 'stats enable', Écoute sur le port 9000 (bind 172.16.10.100:9000), Activation des logs globaux, Configuration de l'authentification avec identifiants admin:admin, Définition de l'URL d'accès aux statistiques (/stats)

```
frontend stats
    stats enable
    bind 172.16.10.100:9000
    log global

    stats auth admin:admin
    stats uri /stats
```

La vérification a confirmé l'accès à l'interface de statistiques via l'URL <http://172.16.10.100:9000/stats>, nécessitant une authentification pour garantir la sécurité des données de monitoring.



⊕ 172.16.10.100:9000

This site is asking you to sign in.

Nom d'utilisateur

Mot de passe

Annuler Sign in

Non sécurisé 172.16.10.100:9000/stats

Debian.org DF Debian-Facile ★ CHATONS

**HAProxy version 2.6.12-1+deb12u1, released 2023/12/16**

**Statistics Report for pid 657**

> General process information

front																			External resources:										
Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server									
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Downtm	Thritle
Frontend	0	1	-	0	1	282	123	1	864	1800	0	0	0	0	0	0	0	0	0	OPEN									

serveurs_web																			External resources:												
Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server											
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Downtm	Thritle		
serveur1	0	0	-	0	2	0	1	-	2	1	7m24s	864	1800	0	0	0	0	0	0	0	0	7m27s UP	L4OK in 0ms	1/1	Y	-	0	0	0s	-	
serveur2	0	0	-	0	0	0	0	-	0	0	?	0	0	0	0	0	0	0	0	0	0	7m27s UP	L4OK in 0ms	1/1	Y	-	0	0	0s	-	
Backend	0	0	-	0	2	0	1	262	123	2	1	7m24s	864	1800	0	0	0	0	0	0	0	0	7m27s UP		2/2	2	0	0	0	0s	-

stats																			External resources:										
Queue			Session rate			Sessions						Bytes		Denied		Errors		Warnings		Server									
Cur	Max	Limit	Cur	Max	Limit	Cur	Max	Limit	Total	LbTot	Last	In	Out	Req	Resp	Req	Conn	Resp	Retr	Redis	Status	LastChk	Wght	Act	Bck	Chk	Dwn	Downtm	Thritle
Frontend	1	2	-	1	1	262	123	6				1114	886	0	0	2					OPEN								

## **Mise en place de la haute disponibilité de HTTPS**

### **- Création du certificat**

Un certificat et une clé privée ont été créés sur le serveur HAProxy avec une validité de 365 jours et une clé RSA 2048 bits.

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/server.key -out /etc/ssl/certs/server.pem
```

### **- Configuration des certificats HAProxy**

La mise en place a nécessité plusieurs étapes : Fusion du certificat et de la clé privée dans un fichier unique, Attribution des permissions appropriées (chmod 600), Modification des droits de propriété (chown root:root).

```
cat /etc/ssl/certs/server.pem /etc/ssl/private/server.key > /etc/ssl/certs/haproxy.pem
chmod 600 /etc/ssl/certs/haproxy.pem
chown root:root /etc/ssl/certs/haproxy.pem
```

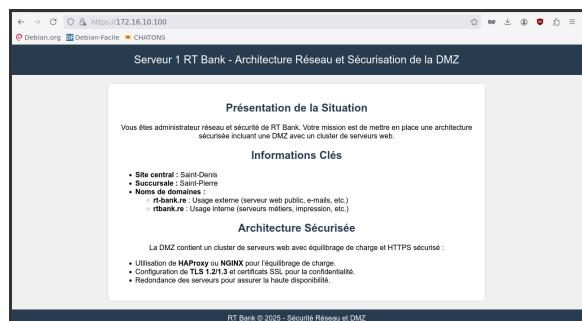
### **- Configuration HAProxy pour HTTPS**

La configuration frontend a été mise à jour pour inclure le support HTTPS sur le port 443, en spécifiant le chemin vers le certificat fusionné.

```
bind 192.168.1.56:443 ssl cert /etc/ssl/certs/haproxy.pem
```

### **- Vérifier que vous pouvez vous connecter sur les serveurs en HTTPS :**

Sur le serveur 1 :



**AFFICHER LE CERTIFICAT : WWW.RT-BANK.RE** X

<b>Généralités</b>	<b>Détails</b>
<b>Émis pour</b>	
Nom commun (CN)	www.rt-bank.re
Organisation (O)	Internet Widgits Pty Ltd
Unité d'organisation (OU)	<Ne fait pas partie du certificat>
<b>Émis par</b>	
Nom commun (CN)	www.rt-bank.re
Organisation (O)	Internet Widgits Pty Ltd
Unité d'organisation (OU)	<Ne fait pas partie du certificat>
<b>Durée de validité</b>	
Émis le	vendredi 28 mars 2025 à 09:06:29
Expire le	samedi 28 mars 2026 à 09:06:29
<b>Empreintes SHA-256</b>	
Certificat	823090fcde4107f50d154017b86e3969c06ea296fb1a0306558b951b0390b8ef
Clé publique	ce4440cc8ca88a043e105fc1ddab3629c18ae6ef97b5119c267addf971952f11

Des tests d'accès ont confirmé le bon fonctionnement du protocole HTTPS sur le serveur 1, démontrant la réussite de l'implémentation de la connexion sécurisée à travers HAProxy.

---

## **Mise en place de la haute disponibilité HAProxy**

Pour assurer une disponibilité optimale de notre infrastructure, nous avons mis en place un système de redondance HAProxy. Dans un premier temps, nous avons dupliqué notre serveur HAProxy existant sur une nouvelle machine virtuelle. L'installation du service keepalived a été effectuée via la commande 'sudo apt install keepalived'.

```
sudo apt install keepalived
```

La configuration du premier HAProxy en tant que maître a été réalisée avec les paramètres suivants :

- Nous avons défini son état comme MASTER pour établir sa priorité
- L'interface réseau eth0 a été configurée comme interface principale
- Une priorité de 101 lui a été attribuée pour garantir sa position dominante
- Un système d'authentification sécurisé a été mis en place
- L'adresse IP virtuelle 172.16.10.100/24 a été configurée
- Des scripts de notification ont été implémentés pour gérer les transitions d'état

```
vrrp_instance VI_1 {  
    state MASTER  
    interface eth0  
    virtual_router_id 51  
    priority 101  
    advert_int 1  
    authentication {  
        auth_type PASS  
        auth_pass MonSuperMotDePasseSecret  
    }  
    virtual_ipaddress {  
        172.16.10.100/24  
    }  
    notify_master "/etc/keepalived/haproxy_start.sh"  
    notify_stop "/etc/keepalived/haproxy_stop.sh"  
    notify_backup "/etc/keepalived/haproxy_start.sh"  
}
```

Pour le second HAProxy, configuré en mode esclave, nous avons établi :

- Un état BACKUP pour son rôle secondaire
- La même configuration d'interface et d'authentification que le maître
- Une priorité de 100, intentionnellement inférieure au maître
- La même adresse IP virtuelle pour assurer la continuité du service
- Des scripts de notification identiques pour maintenir la cohérence du système

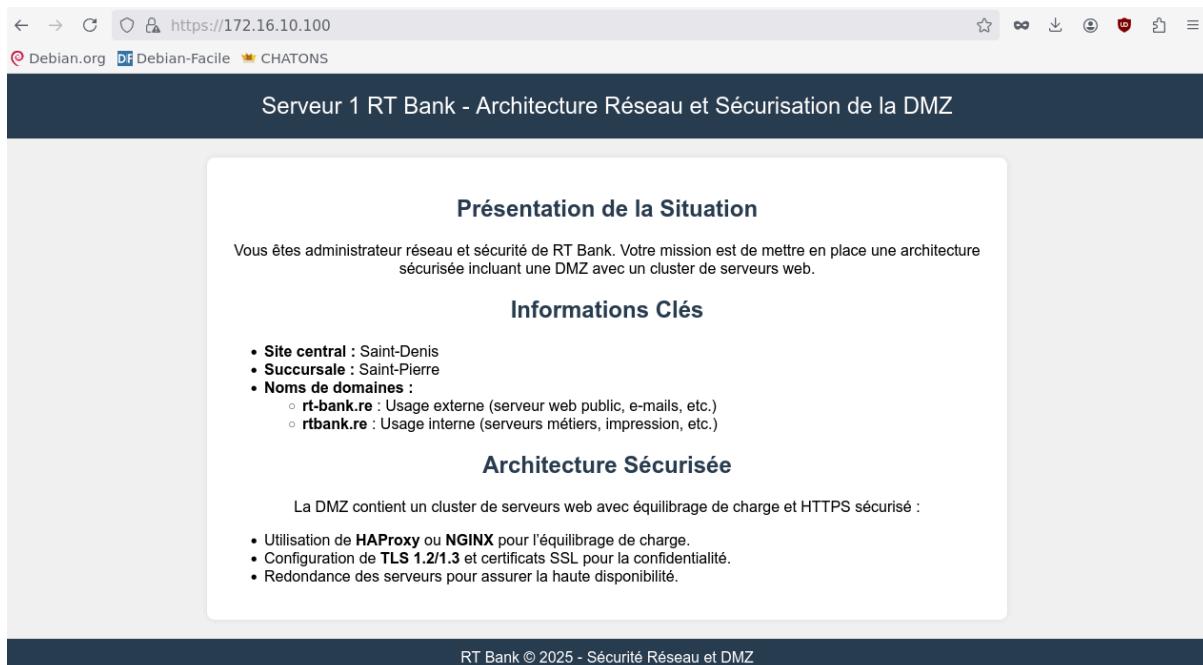
```
vrrp_instance VI_1 {  
    state BACKUP  
    interface eth0  
    virtual_router_id 51  
    priority 100  
    advert_int 1  
    authentication {  
        auth_type PASS  
        auth_pass MonSuperMotDePasseSecret  
    }  
    virtual_ipaddress {  
        172.16.10.100/24  
    }  
    notify_master "/etc/keepalived/haproxy_start.sh"  
    notify_stop "/etc/keepalived/haproxy_stop.sh"  
    notify_backup "/etc/keepalived/haproxy_start.sh"  
}
```

---

- **Vérification**

Pour valider le bon fonctionnement de notre configuration de haute disponibilité, nous avons effectué une série de tests :

Nous avons d'abord vérifié l'accès au service via l'adresse IP virtuelle (172.16.10.100). Le site web s'est affiché correctement, confirmant le fonctionnement normal du HAProxy principal.



Serveur 1 RT Bank - Architecture Réseau et Sécurisation de la DMZ

**Présentation de la Situation**

Vous êtes administrateur réseau et sécurité de RT Bank. Votre mission est de mettre en place une architecture sécurisée incluant une DMZ avec un cluster de serveurs web.

**Informations Clés**

- Site central : Saint-Denis
- Succursale : Saint-Pierre
- Noms de domaines :
  - rt-bank.re : Usage externe (serveur web public, e-mails, etc.)
  - rbtbank.re : Usage interne (serveurs métiers, impression, etc.)

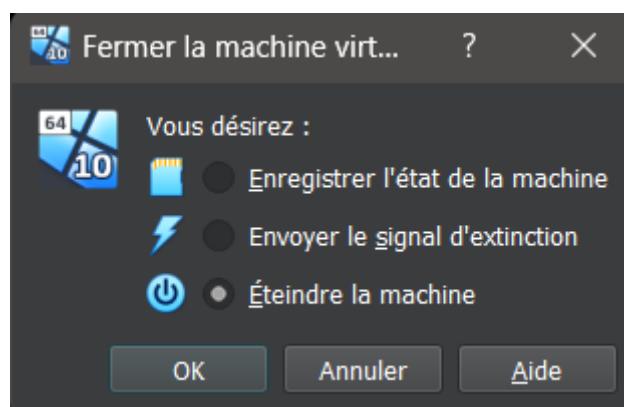
**Architecture Sécurisée**

La DMZ contient un cluster de serveurs web avec équilibrage de charge et HTTPS sécurisé :

- Utilisation de **HAProxy** ou **NGINX** pour l'équilibrage de charge.
- Configuration de TLS 1.2/1.3 et certificats SSL pour la confidentialité.
- Redondance des serveurs pour assurer la haute disponibilité.

RT Bank © 2025 - Sécurité Réseau et DMZ

Pour tester le mécanisme de basculement, nous avons procédé à l'arrêt du premier HAProxy. Cette opération simule une panne du serveur principal.

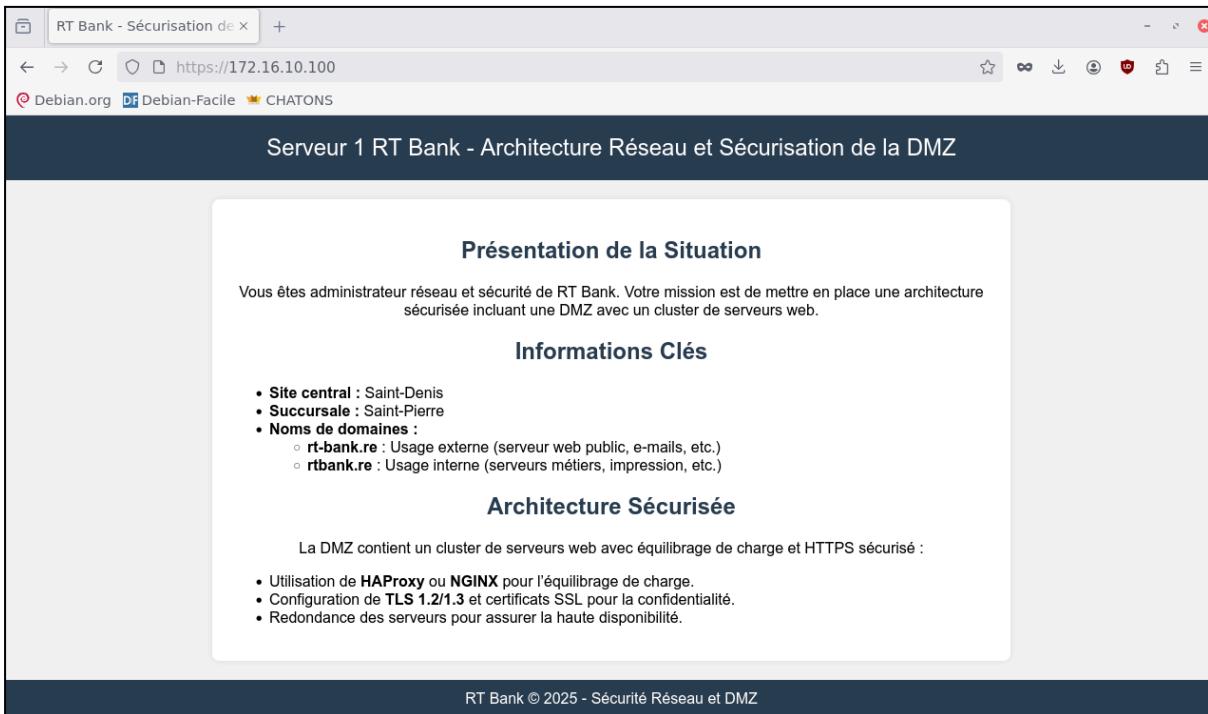


---

Une nouvelle vérification de l'accès au service a confirmé que le second HAProxy a bien repris l'adresse IP virtuelle (172.16.10.100), assurant ainsi la continuité du service sans interruption pour les utilisateurs.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel stat
    link/ether 08:00:27:ad:94:c0 brd ff:ff:ff:ff:ff:ff
      inet 172.16.10.16/24 brd 172.16.10.255 scope global eth0
        valid_lft forever preferred_lft forever
      inet 172.16.10.100/24 scope global secondary eth0
        valid_lft forever preferred_lft forever
      inet6 fe80::a00:27ff:fead:94c0/64 scope link
        valid_lft forever preferred_lft forever
```

Pour la validation finale de la haute disponibilité HAProxy, nous avons procédé à un test de connexion via l'adresse IP virtuelle. L'accès au site a été immédiatement rétabli.



Cette dernière vérification confirme le fonctionnement optimal de la redondance entre les serveurs HAProxy. La bascule s'est effectuée de manière transparente, sans impact perceptible pour les utilisateurs finaux, démontrant ainsi l'efficacité de notre configuration de haute disponibilité.

---

- **Tâche 3 – Serveur de noms (DNS) primaire pour rt-bank.re**

**a. Objectif**

Dans cette étape, nous avons mis en place un serveur DNS principal pour le domaine **rt-bank.re**, hébergé dans la **DMZ**, conformément au cahier des charges. Ce serveur devait permettre la résolution des noms de domaine internes de la RT Bank, tout en étant sécurisé, notamment en autorisant les transferts de zone uniquement vers un DNS secondaire.

---

**b. Mise en place du serveur DNS principal**

**1. Déclaration de la zone**

Nous avons commencé par déclarer la zone **rt-bank.re** dans le fichier **/etc/bind/named.conf.local** :

```
zone "rt-bank.re" {
    type master;
    file "/etc/bind/zones/db.rt-bank.re";
    allow-transfer { 172.16.10.21; }; // autorise le DNS secondaire
};
```

Cette configuration indique que le serveur est maître de la zone, et autorise les transferts de zone uniquement vers l'adresse IP du DNS secondaire.

---

## 2. Fichier de zone : db.rt-bank.re

Dans le fichier **/etc/bind/zones/db.rt-bank.re**, nous avons défini les enregistrements nécessaires :

```
@      IN  SOA ns.rt-bank.re. admin.rt-bank.re. (
          2025040101 ; Serial
          3600        ; Refresh
          1800        ; Retry
          604800      ; Expire
          86400       ; Minimum TTL

          IN  NS      ns.rt-bank.re.
          IN  NS      ns2.rt-bank.re.

ns     IN  A      172.16.10.20
ns2    IN  A      172.16.10.21
www   IN  A      172.16.10.100
```

Nous avons défini un enregistrement SOA, deux serveurs de noms (primaire et secondaire), et un enregistrement A pour **www.rt-bank.re**.

## 3. Configuration des options globales

Dans le fichier **/etc/bind/named.conf.options**, nous avons laissé la configuration par défaut, avec les lignes importantes suivantes :

```
dnssec-validation auto;
listen-on-v6 { any; };
```

Cela permet de répondre aux requêtes IPv6, et d'utiliser DNSSEC si activé.

### c. Vérification du bon fonctionnement

Nous avons effectué une requête de test en local pour vérifier que le nom **www.rt-bank.re** est bien résolu :

```
dig @localhost www.rt-bank.re
```

```
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 1232  
; COOKIE: db6ce71f3a8ebef80100000067fcae9789a5b5376cd4a990 (good)  
;; QUESTION SECTION:  
.www.rt-bank.re. IN A  
  
;; ANSWER SECTION:  
www.rt-bank.re. 86400 IN A 172.16.10.100  
  
;; Query time: 0 msec  
;; SERVER: ::1#53(localhost) (UDP)  
;; WHEN: Mon Apr 14 10:43:35 +04 2025  
;; MSG SIZE rcvd: 87  
  
root@debianVM:~#
```

La réponse indique que la configuration du serveur DNS principal est opérationnelle.

---

## - Tâche 3 (suite) – Mise en place du DNS secondaire

### a. Objectif

Pour assurer une **haute disponibilité** du service DNS et éviter tout point de défaillance, nous avons mis en place un **serveur DNS secondaire** pour le domaine **rt-bank.re**. Ce serveur se synchronise automatiquement avec le serveur maître situé également dans la DMZ, et permet de prendre le relais en cas d'indisponibilité du maître.

### b. Configuration du serveur secondaire

Nous avons configuré le serveur comme **esclave** dans le fichier **/etc/bind/named.conf.local** :

```
zone "rt-bank.re" {
    type slave;
    masters { 172.16.10.20; }; // IP du DNS primaire
    file "/var/cache/bind/db.rt-bank.re";
};
```

Cette configuration permet au DNS secondaire de récupérer automatiquement le fichier de zone auprès du maître.

### c. Vérification du transfert de zone

Nous avons testé le **transfert de zone** à l'aide de la commande suivante, exécutée depuis le serveur secondaire :

```
dig AXFR rt-bank.re @172.16.10.20
```

Le résultat montre que tous les enregistrements ont bien été récupérés :

```
root@debianVM:~# dig AXFR rt-bank.re @172.16.10.20
;
; <>> DiG 9.18.33-1~deb12u2-Debian <>> AXFR rt-bank.re @172.16.10.20
;; global options: +cmd
rt-bank.re.          86400   IN      SOA    ns.rt-bank.re. admin.rt-bank.re.
2025040101 3600 1800 604800 86400
rt-bank.re.          86400   IN      NS     ns.rt-bank.re.
rt-bank.re.          86400   IN      NS     ns2.rt-bank.re.
ns.rt-bank.re.       86400   IN      A      172.16.10.20
ns2.rt-bank.re.      86400   IN      A      172.16.10.21
www.rt-bank.re.      86400   IN      A      172.16.10.100
rt-bank.re.          86400   IN      SOA    ns.rt-bank.re. admin.rt-bank.re.
2025040101 3600 1800 604800 86400
;
```

#### d. Fichier de zone téléchargé

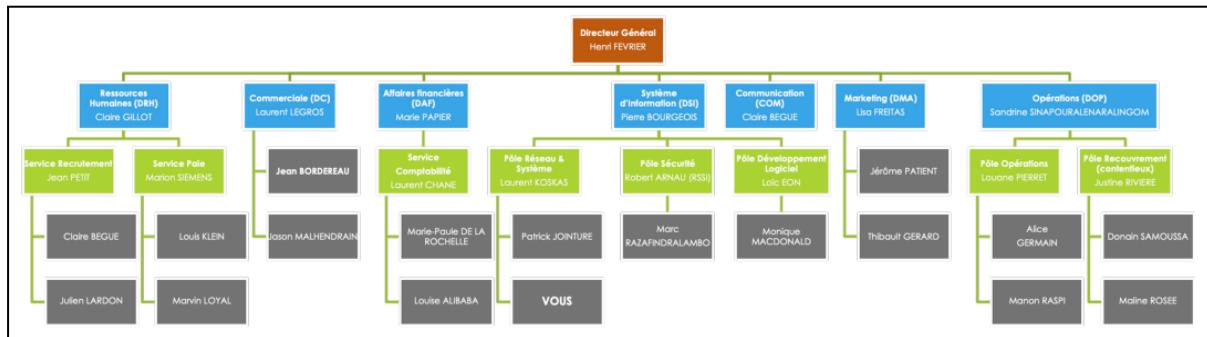
Le transfert de zone a généré un fichier local automatiquement dans le répertoire **/var/cache/bind/** :

```
root@debianVM:~# ls -l /var/cache/bind/
total 12
-rw-r--r-- 1 bind bind 303 14 avril 10:38 db.rt-bank.re
-rw-r--r-- 1 bind bind 1421 14 avril 10:08 managed-keys.bind
-rw-r--r-- 1 bind bind 3020 14 avril 10:08 managed-keys.bind.jnl
root@debianVM:~#
```

Cela confirme que la synchronisation est fonctionnelle et que le serveur secondaire peut répondre aux requêtes même si le primaire est indisponible.

## - Tâche 4 – Mise en place et sécurisation de l'infrastructure Active Directory

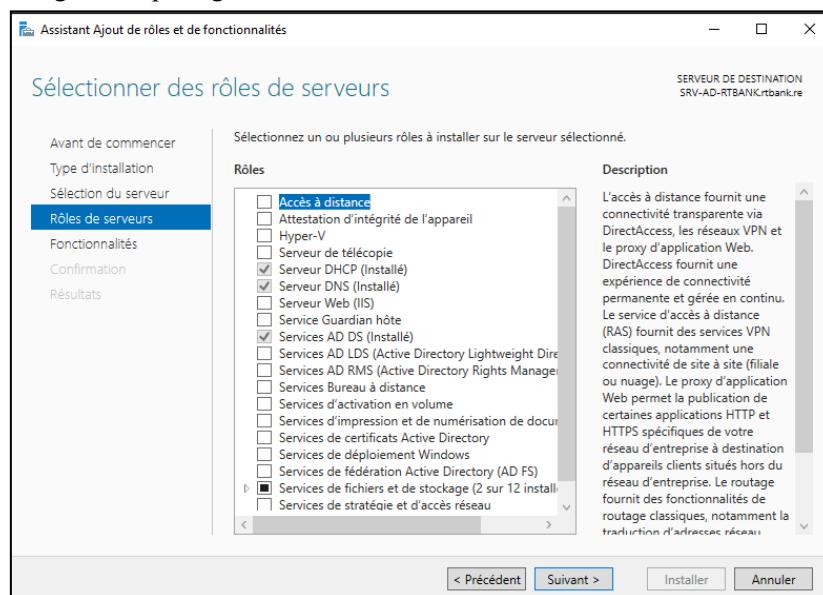
Dans le cadre de la sécurisation de l'infrastructure RT Bank, nous avons procédé à l'implémentation d'un Active Directory selon un organigramme hiérarchique détaillé. Cette structure organisationnelle reflète la complexité et les besoins spécifiques de l'entreprise, avec une répartition claire des différents services et départements.



## - Installation et configuration de l'AD

Nous avons déployé l'Active Directory principal avec les fonctionnalités essentielles suivantes :

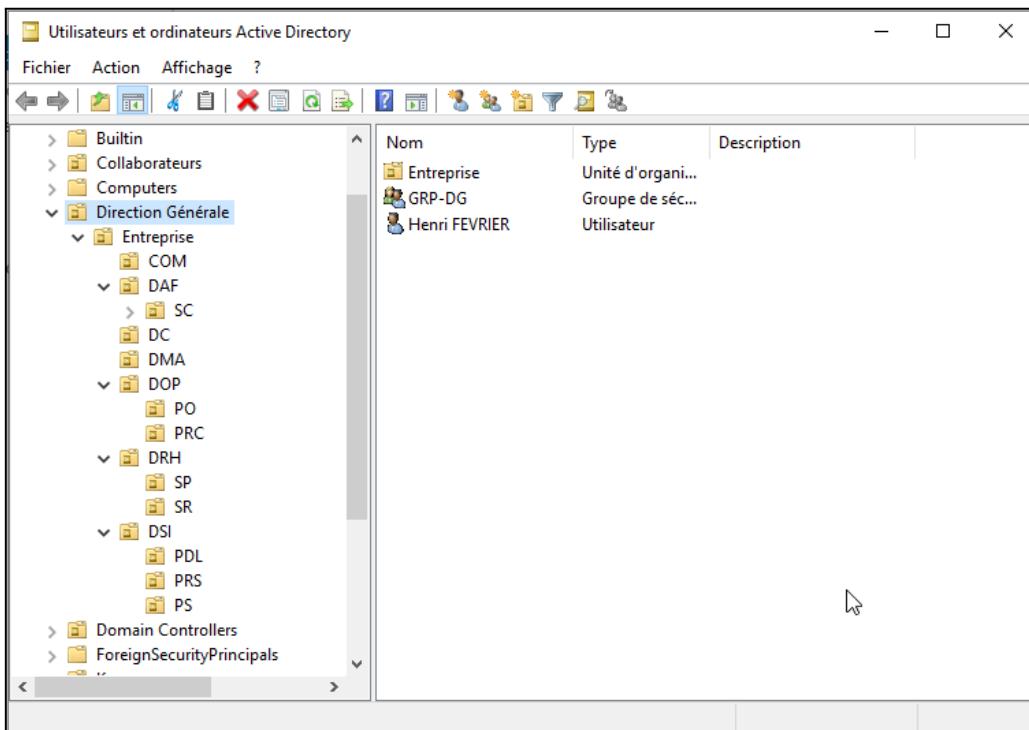
- Services DNS intégrés pour la résolution de noms
- Service DHCP pour la gestion dynamique des adresses IP
- Services de certificats pour sécuriser les communications
- Services de gestion des stratégies de groupe
- Services de stockage et de partage de fichiers



### - Créations des OU et des utilisateurs de l'organigramme

Suivant la structure détaillée de l'organigramme de RT Bank, nous avons mis en place une arborescence complète dans l'Active Directory. La création des différentes Unités d'Organisation reflète fidèlement la hiérarchie de l'entreprise, en commençant par la Direction Générale et ses subdivisions, puis en descendant vers les départements spécifiques comme la DSI, la DRH et leurs services associés.

Chaque utilisateur a ensuite été intégré dans son unité d'organisation respective, avec une attention particulière portée à l'attribution des droits d'accès. Les groupes de sécurité ont été configurés en fonction des responsabilités et des besoins spécifiques de chaque service, assurant ainsi une gestion cohérente des permissions dans l'ensemble de l'infrastructure.



The screenshot shows the Windows Active Directory Users and Computers management console. The left pane displays a tree view of the organizational units (OU) structure:

- Builtin
- Collaborateurs
- Computers
- Direction Générale
  - Entreprise
  - DAF
    - SC
    - DC
    - DMA
  - DOP
    - PO
    - PRC
  - DRH
    - SP
    - SR
  - DSI
    - PDL
    - PRS
    - PS
- Domain Controllers
- ForeignSecurityPrincipals

The right pane lists three objects under the "Entreprise" OU:

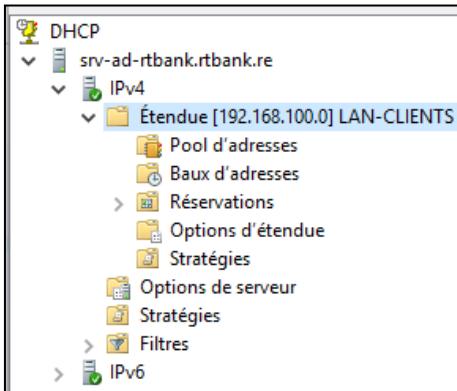
Nom	Type	Description
Entreprise	Unité d'organis...	
GRP-DG	Groupe de séc...	
Henri FEVRIER	Utilisateur	

## - Configuration du DHCP

La configuration du service DHCP a été réalisée avec précision pour gérer efficacement la distribution des adresses IP au sein du réseau LAN-Clients. Nous avons défini une plage d'adresses IP allant de 192.168.100.150 à 192.168.100.200, avec une configuration de la passerelle du LAN-Clients sur 192.168.100.1.

Pour garantir un fonctionnement optimal du réseau, nous avons également configuré les paramètres DNS de l'Active Directory. Cette configuration permet aux clients d'accéder non seulement au domaine interne, mais aussi à la DMZ pour consulter la page web via [www.rt-bank.re](https://www.rt-bank.re) ou via l'adresse HTTPS 192.168.51.75.

Le service DHCP a été configuré pour distribuer automatiquement les paramètres réseau nécessaires, incluant les serveurs DNS et la passerelle par défaut, facilitant ainsi l'intégration transparente des nouveaux clients dans l'infrastructure et dans le domaine rtbank.re en interne



DHCP	srv-ad-rtbank.rtbank.re	Adresse IP de début	Adresse IP de fin	Description
	IPv4	192.168.100.150	192.168.100.200	Plage d'adresses pour la distribution
	Étendue [192.168.100.0] LAN-CLIENTS			
	Pool d'adresses			

DHCP	srv-ad-rtbank.rtbank.re	Adresse IP du client	Nom	Expiration du bail	Type
	IPv4	192.168.100.150	Client2.rtbank.re	22/04/2025 13:54:30	DHCP
	Étendue [192.168.100.0] LAN-CLIENTS	192.168.100.151	Client1.rtbank.re	23/04/2025 09:29:11	DHCP
	Pool d'adresses	192.168.100.154	Client3.rtbank.re	16/04/2025 09:04:14	DHCP

DHCP	srv-ad-rtbank.rtbank.re	Nom d'option	Fournisseur	Valeur	Nom de
	IPv4	003 Routeur	Standard	192.168.100.1	Aucun
	Étendue [192.168.100.0] LAN-CLIENTS	006 Serveurs DNS	Standard	10.10.10.10, 172.16.10.20, 172.16.10.21	Aucun
	Pool d'adresses	015 Nom de domaine DNS	Standard	rtbank.re	Aucun
	Baux d'adresses				
	Réservations				
	Options d'étendue				

	Adresse MAC	Description
✓ D8-BB-C1-B5-08...	D8-BB-C1-B5-08...	PC-AYMERIC-UNIV.rbank.re
✓ 00-E0-4C-68-03-9A	00-E0-4C-68-03-9A	DESKTOP-LI98837.rbank.re

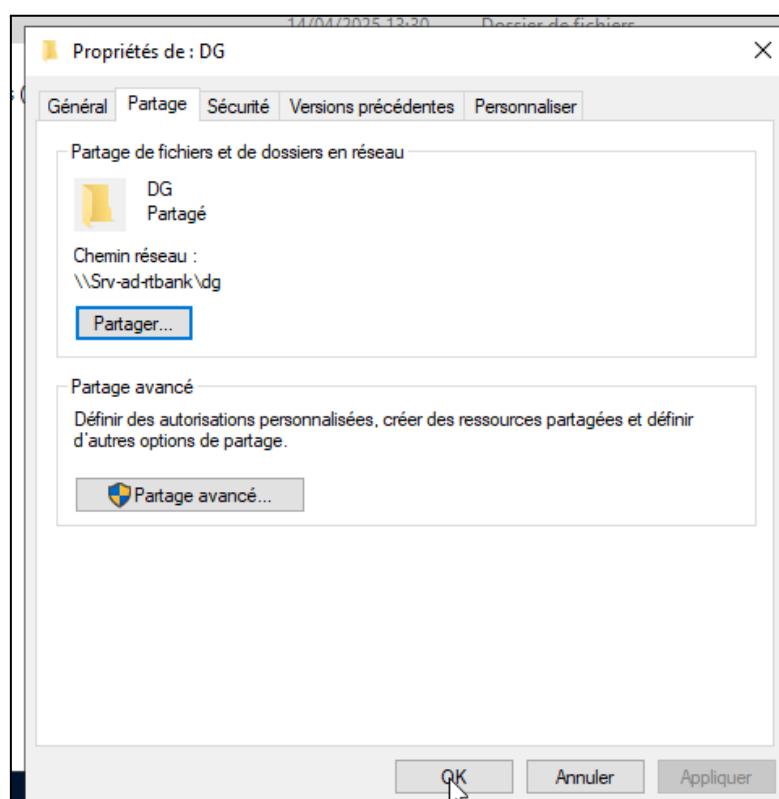
## - Configuration de la GPO lecteur réseau

La mise en place d'une stratégie de groupe (GPO) pour le lecteur réseau a débuté avec la création d'un dossier spécifique pour la Direction générale. Cette GPO servira de modèle pour les autres groupes de l'organisation.

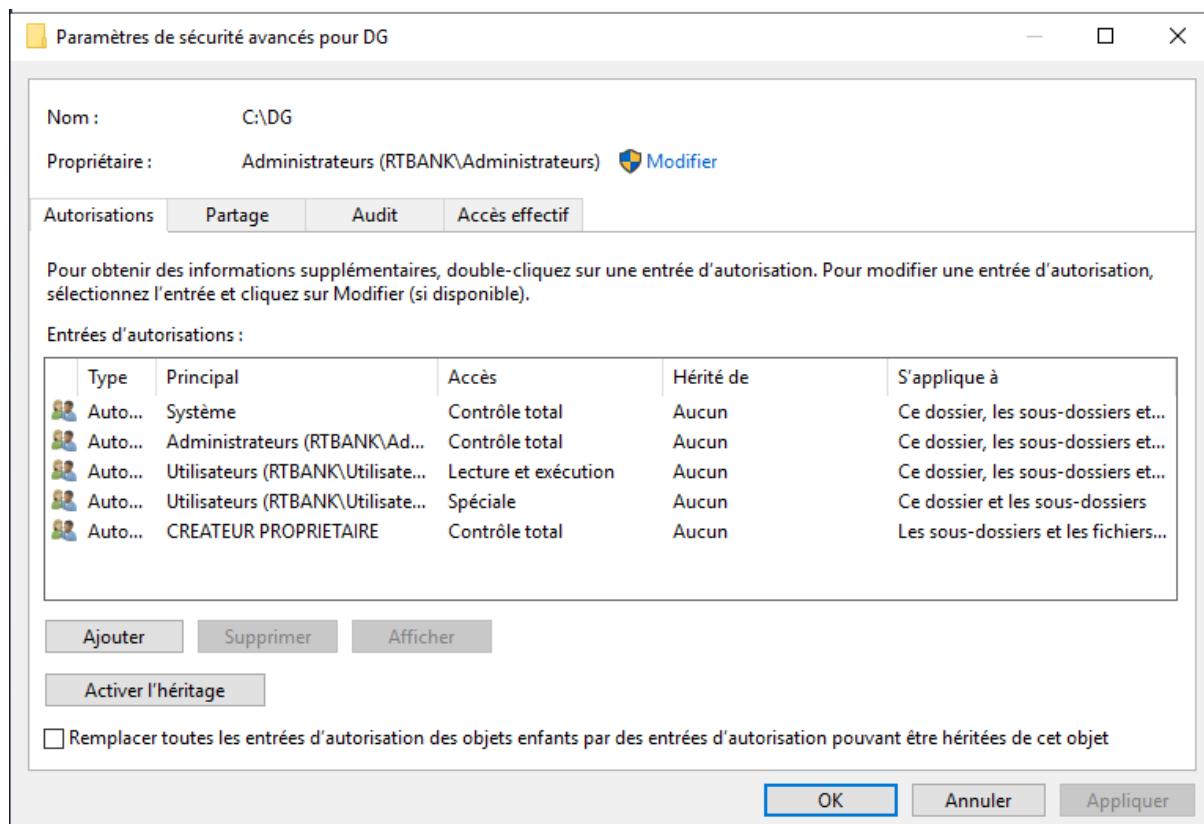
Dans un premier temps, nous avons créé un dossier nommé "DG" dans l'arborescence du système :

	Nom	Modifié le	Type	Taille
Accès rapide				
Bureau	DG	14/04/2025 13:30	Dossier de fichiers	

Une fois le dossier créé, nous avons accédé aux propriétés de partage en effectuant un clic droit sur le dossier. Dans l'onglet "Partage", nous avons configuré les paramètres de partage réseau, permettant ainsi d'établir les bases de notre stratégie de groupe pour la gestion des accès aux ressources partagées.

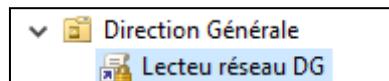


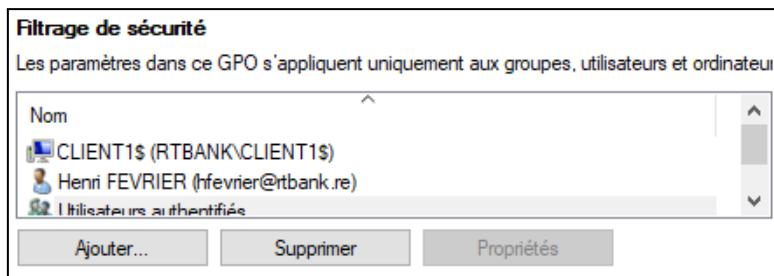
Dans les paramètres de sécurité avancés du dossier DG, nous avons désactiver l'héritage pour personnaliser les permissions



Ensuite, nous avons créé une GPO spécifique "Lecteur réseau DG" dans la section Direction Générale des stratégies de groupe. Pour renforcer la sécurité, nous avons mis en place un filtrage précis qui inclut :

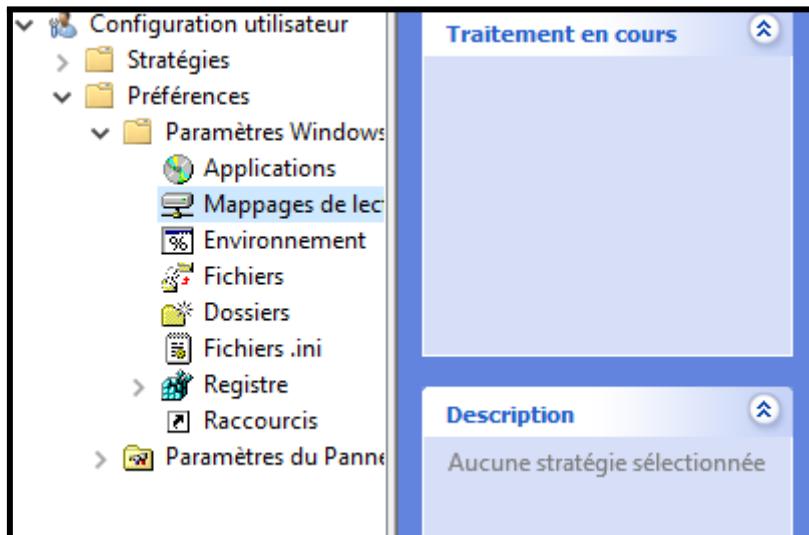
- Le PC client spécifique de connexion
- L'utilisateur "hfevrier"
- Les paramètres d'authentification nécessaires



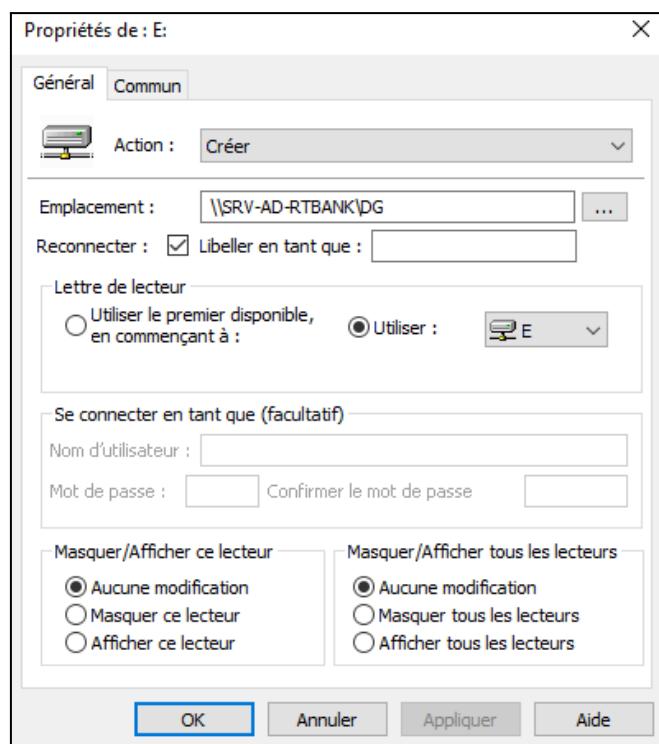


Nous aurions pu spécifier le groupe mais vu qu'il n'y a qu'un seul utilisateur je précise directement l'utilisateur.

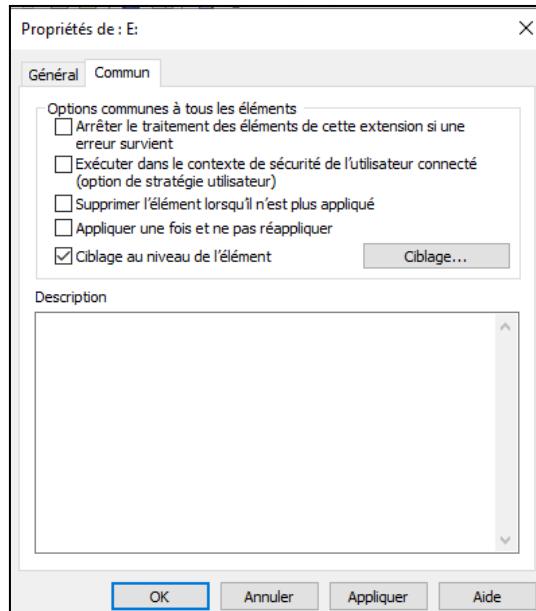
Nous avons accédé aux paramètres avancés en suivant le chemin : Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs.



nous avons ajouté un nouvel élément avec les paramètres suivants :

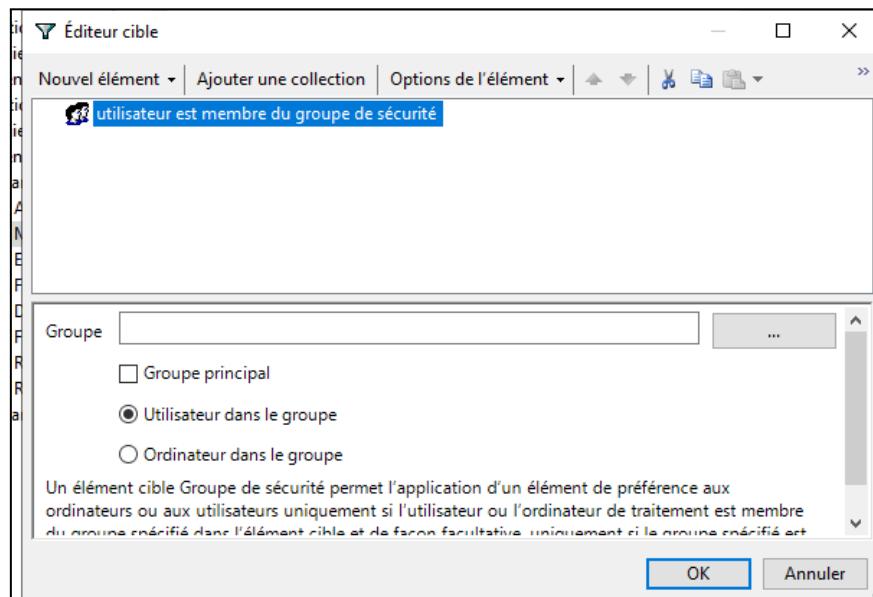


Ensuite dans l'onglet commun :

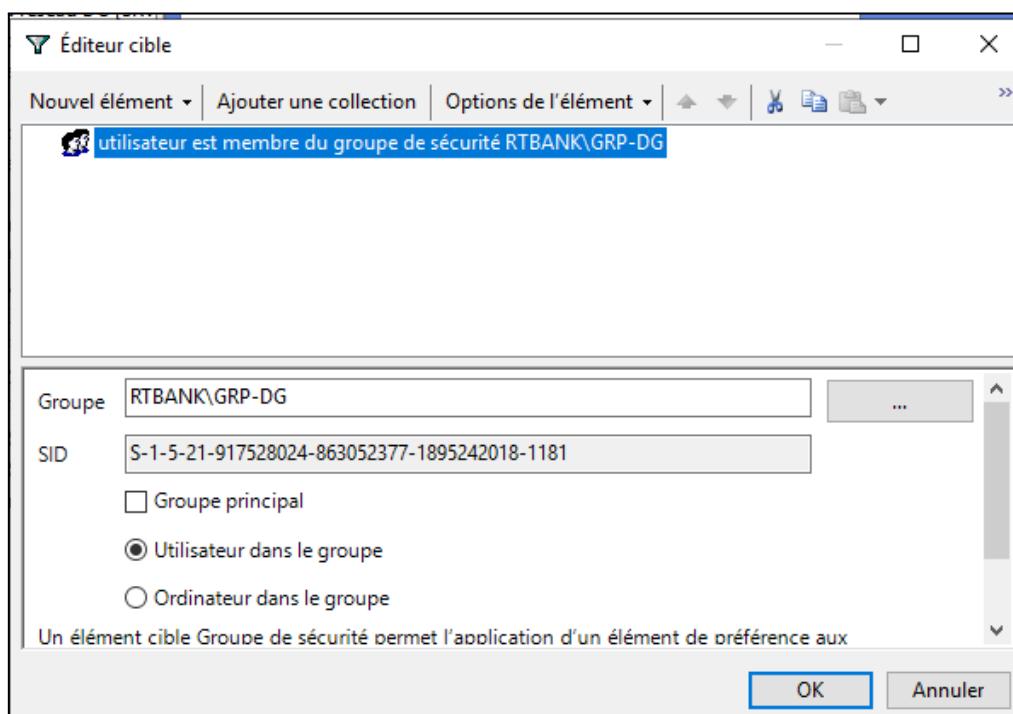


---

Nous avons cliqué sur l'option "ciblage" puis "nouvel élément" pour accéder aux groupes de sécurité. Ensuite, nous avons précisé le nom du groupe pour lequel nous souhaitons configurer le lecteur réseau DG, en l'occurrence RTBANK\GRP-DG.



Sur les trois petits points on précise le nom du groupe pour lequel on cible le lecteur réseau le DG :

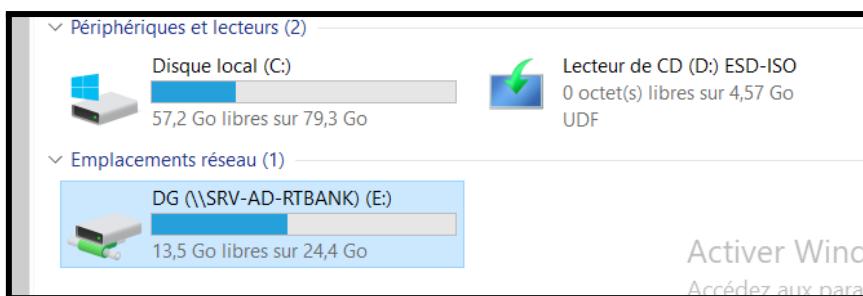


---

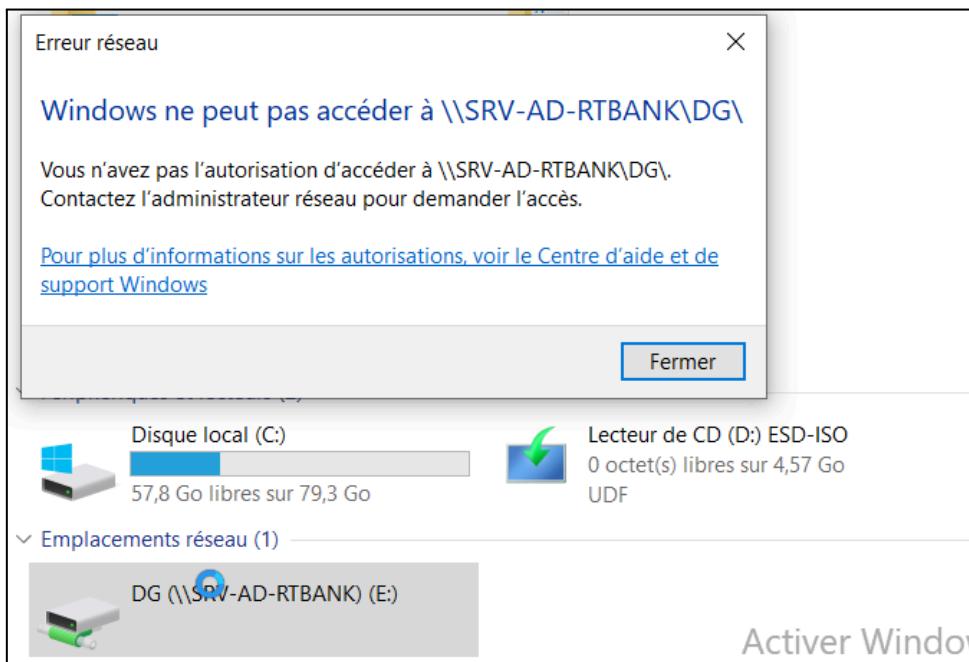
Dans la fenêtre de l'éditeur cible, nous avons spécifié que l'utilisateur doit être membre du groupe de sécurité RTBANK\GRP-DG.

Nous avons vérifié le bon fonctionnement du mappage en nous connectant avec l'utilisateur "hfevrier". Pour actualiser la GPO, nous avons exécuté la commande 'gpupdate /force'. Le résultat confirme que notre lecteur réseau est bien visible et accessible pour l'utilisateur "hfevrier".

```
gpupdate /force
```



Pour garantir la sécurité du système, nous avons également effectué un test de contrôle en nous connectant avec l'utilisateur "jlebon" afin de vérifier que l'accès au lecteur mappé est bien restreint aux seuls utilisateurs autorisés.



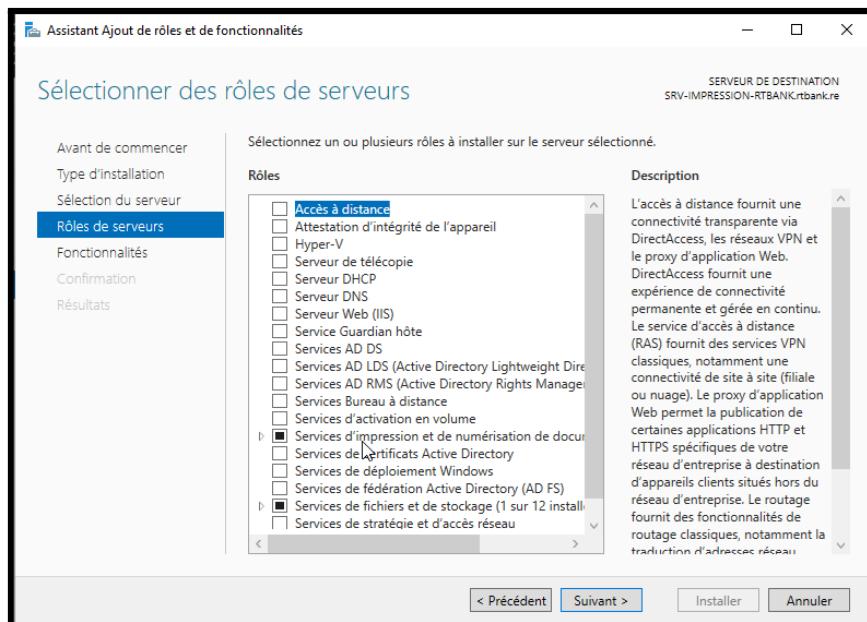
---

Comme nous pouvons le voir, l'utilisateur "jlebon" n'a pas accès au dossier DG, donc la GPO est bien appliquée et les autorisations sont bien configurées, nous avons donc répété la même chose pour chaque organisation de l'entreprise.

## - Installation et configuration du “serveur d'impression” dans l'AD

L'installation et la configuration du serveur d'impression dans l'Active Directory ont été réalisées méthodiquement. Un second serveur Windows a d'abord été déployé et intégré au domaine [rtbank.re](http://rtbank.re). Sur ce serveur, nous avons installé le rôle de serveur d'impression et de numérisation de documents pour centraliser la gestion des ressources d'impression.

Pour faciliter l'accès des utilisateurs à ces ressources, nous avons prévu la création d'une stratégie de groupe (GPO). Cette GPO permettra de déployer automatiquement les imprimantes aux utilisateurs du domaine, simplifiant ainsi la gestion des accès aux périphériques d'impression et garantissant une distribution cohérente des ressources d'impression à travers l'organisation.



## - Configuration du “serveur de supervision cacti”

La mise en place du serveur de supervision Cacti a été effectuée avec une configuration précise pour assurer un monitoring efficace de notre infrastructure. Nous avons commencé par créer deux sites distincts dans Cacti :

- - Un site pour RTBANK-SP (Saint-Pierre)
- - Un site pour RTBANK-SD (Saint-Denis)

Tous les 4 Sites							
Nom du site	ID	Équipements	Ville	État	Pays		
Core	2	0					
Edge	1	0					
RTBANK-SD	3	12					
RTBANK-SP	4	1					

Après la configuration initiale des sites, nous avons procédé à l'ajout des équipements à superviser dans notre infrastructure.

Tous les 14 Équipements							
Description de l'équipement	Nom d'hôte	ID	Graphiques	Sources de données	État	Actif depuis	
Client 1	192.169.100.150	13	4	4	Down	15h:21m	
Local Linux Machine	localhost	1	4	5	Up	N/A	
SERVEUR APACHE 1	172.16.10.10	7	7	8	Up	N/A	
SERVEUR APACHE 2	172.16.10.11	8	7	8	Up	N/A	
Serveur de supervision cacti	10.10.10.100	3	4	5	Up	N/A	
SERVEUR DNS 1	172.16.10.20	11	4	5	Up	N/A	
SERVEUR DNS 2	172.16.10.21	12	4	5	Up	N/A	
SERVEUR HAProxy 1	172.16.10.15	9	4	5	Up	N/A	
SERVEUR HAProxy 2	172.16.10.16	10	4	5	Up	N/A	
SRV-AD-METIER1	10.10.10.201	5	4	4	Down	4m	
SRV-AD-METIER2	10.10.10.202	6	0	0	Down	4m	
SRV-AD-RTBANK	10.10.10.10	2	4	4	Up	N/A	
SRV-IMPRESSION-RTBANK	10.10.10.40	4	4	4	Down	4m	
SRV-RODC-RTBANK	10.10.20.10	14	4	4	Down	13h:25m	

Pour compléter la configuration de la supervision, nous avons défini des paramètres spécifiques pour chaque équipement supervisé. Par exemple, pour le serveur Apache, nous avons configuré :

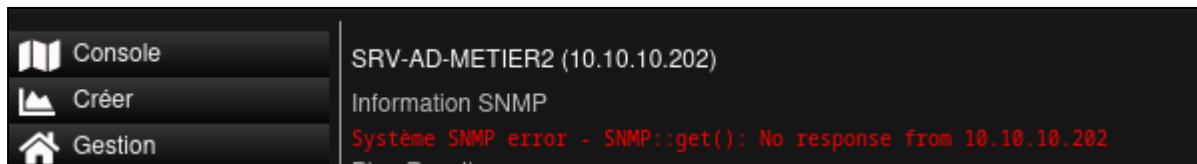
- La description et le nom d'hôte avec son adresse IP (172.16.10.10)
- Le protocole SNMP avec ses paramètres de communauté
- Les intervalles de vérification et les seuils d'alerte
- Le nombre de tentatives de ping et les délais d'attente

Equipement [éditer : SERVEUR APACHE 1]

Options générales de l'équipement

Description ?	SERVEUR APACHE 1
Nom d'hôte ?	172.16.10.10
Emplacement ?	Aucun
Association du collecteur ?	Main Poller
Site de l'équipement ?	RTBANK-SD
Modèle d'équipement ?	Apache Webserver
Nombre de Threads pour la collecte ?	1 Thread
Désactiver l'équipement ?	
Options SNMP	
Version de SNMP ?	Version 2
Communauté SNMP ?	public
Port SNMP ?	161
Délai maximum pour le SNMP ?	500
Nombre maximum d'OID par requête GET ?	10 OID's
Bulk Walk Maximum Répétitions ?	Auto Detect/Set on first Re-Index
Options de disponibilité/d'accès	
Détection des équipements tombés en panne ?	Ping et SNMP Uptime
Méthode de Ping ?	Ping ICMP
Délai maxi ?	400
Nombre de tentatives de Ping ?	1

Nous avons également dû configurer le service SNMP sur les réseaux LAN-Serveurs et DMZ pour permettre la supervision de tous les équipements. Cette étape était cruciale car sans elle, nous obtenions des erreurs de connexion SNMP, empêchant la collecte des données de supervision.



Pour assurer une supervision efficace sur les serveurs Linux, nous avons configuré le service SNMP en modifiant le fichier /etc/snmp/snmpd.conf. La configuration a nécessité plusieurs étapes :

La modification du fichier a été réalisée avec l'éditeur nano, où nous avons ajouté les paramètres nécessaires pour permettre l'accès aux données de supervision. Une attention particulière a été portée à la configuration des agentAddress pour garantir une collecte appropriée des données.

Après la modification du fichier de configuration, nous avons redémarré le service SNMP via la commande 'systemctl restart snmp'. Cette action a été suivie d'une vérification dans Cacti pour confirmer le bon fonctionnement de la supervision. Les modifications apportées permettent désormais une collecte fiable des données de supervision sur l'ensemble de nos serveurs Linux.

Pour régler le problème modifier les fichiers suivants :

**nano /etc/snmp/snmpd.conf**

chercher agentaddress dans la barre de recherche de nano avec ctrl + w

Il faut mettre un hashtag devant le **agentaddress 127.0.0.1[:1]** et rajoutez en dessous **agentaddress udp:161,udp6[:1]:161** comme ceci :

```
GNU nano 7.2                               /etc/snmp/snmpd.conf *

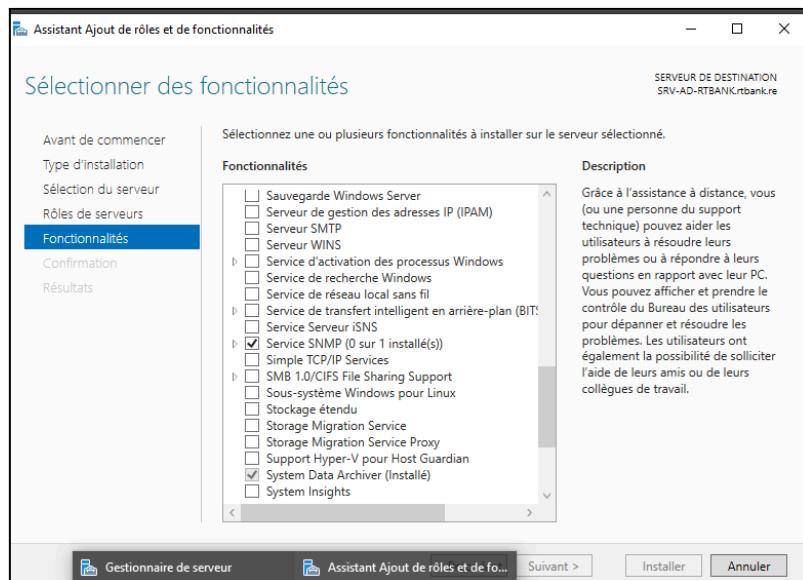
# agentaddress: The IP address and port number that the agent
# By default the agent listens to any and all traffic from
# interface on the default SNMP port (161). This allows
# specify which address, interface, transport type and port
# want the agent to listen on. Multiple definitions of
# are concatenated together (using ':').
# arguments: [transport:]port[@interface/addrress]...,

#agentaddress 127.0.0.1[:1]
agentaddress udp:161,udp6[:1]:161
```

Enregistrez les modifications faites sur ce fichier. Dans le terminal tapez **systemctl restart snmp**. Puis repartez sur votre serveur cacti et actualisez votre page, repartez dans Gestion > Équipements puis allez dans "Supervision du serveur cacti" et normalement ça vous affichera cela :

Pour configurer le service SNMP sur les serveurs Windows, nous avons suivi une procédure spécifique en deux étapes principales.

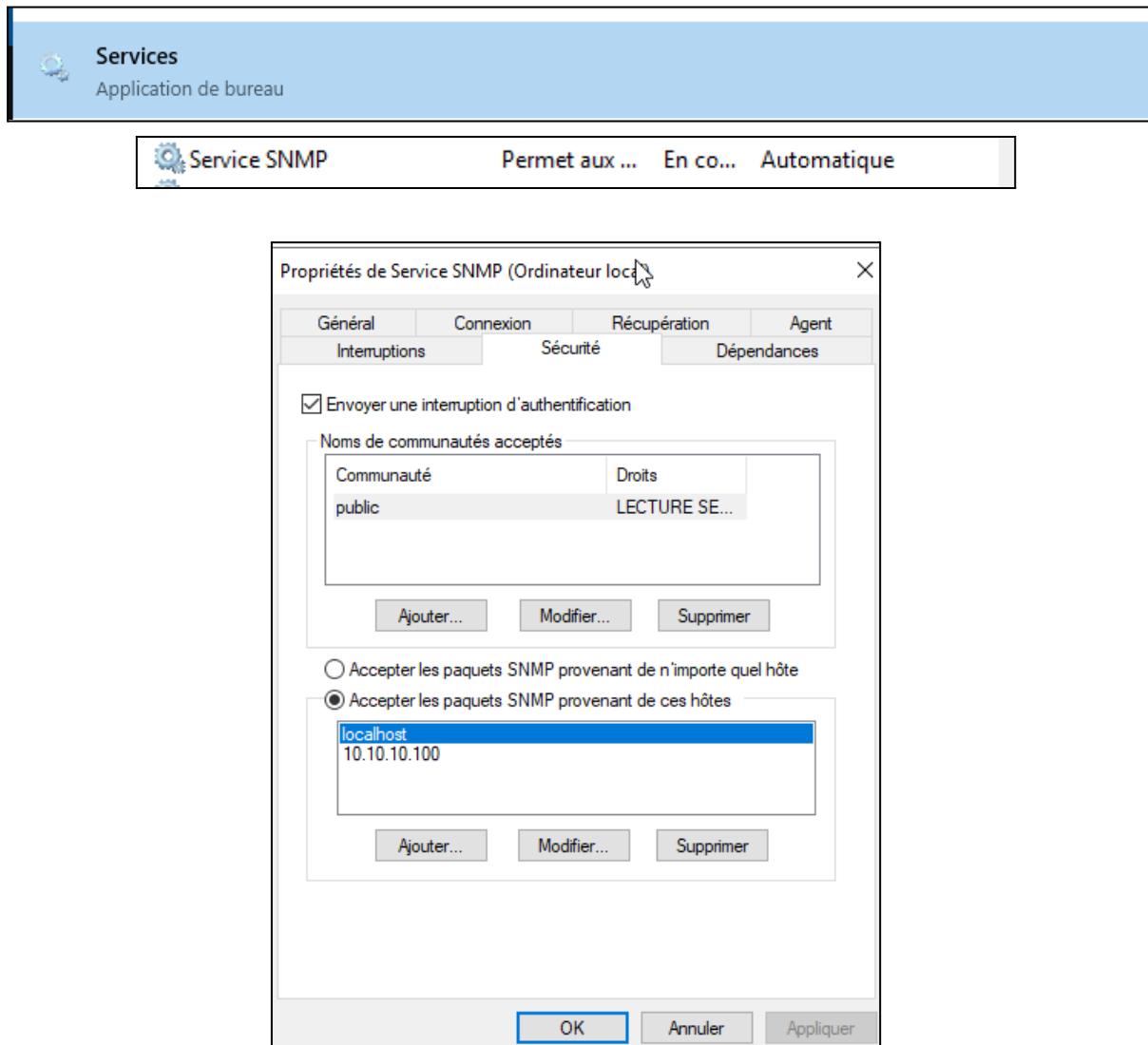
Dans un premier temps, nous avons ajouté les fonctionnalités SNMP via le gestionnaire de serveur Windows. Cette installation permet d'activer les services nécessaires à la supervision de l'environnement Windows.



---

Ensuite, nous avons accédé aux Services pour configurer le service SNMP. Dans l'onglet sécurité, nous avons paramétré :

- Le nom de communauté "public"
- L'autorisation des paquets SNMP provenant des hôtes spécifiques
- L'adresse IP de notre serveur de supervision (10.10.10.100)

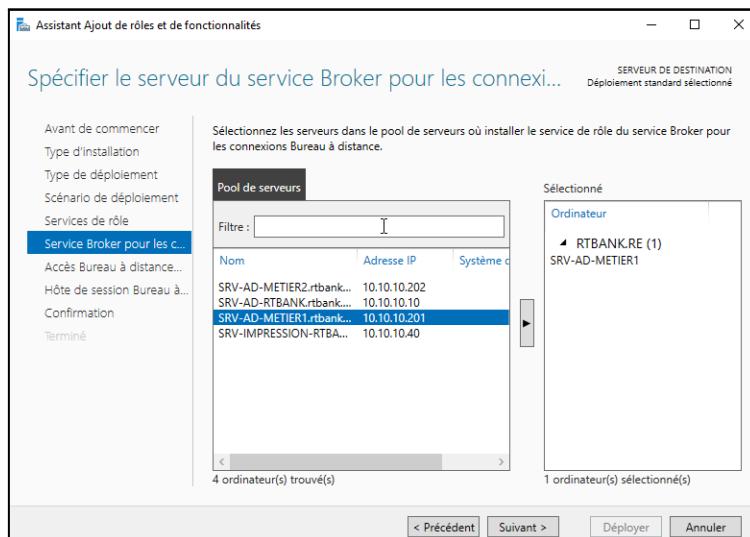


Ces configurations permettent désormais une communication sécurisée entre nos serveurs Windows et notre système de supervision Cacti.

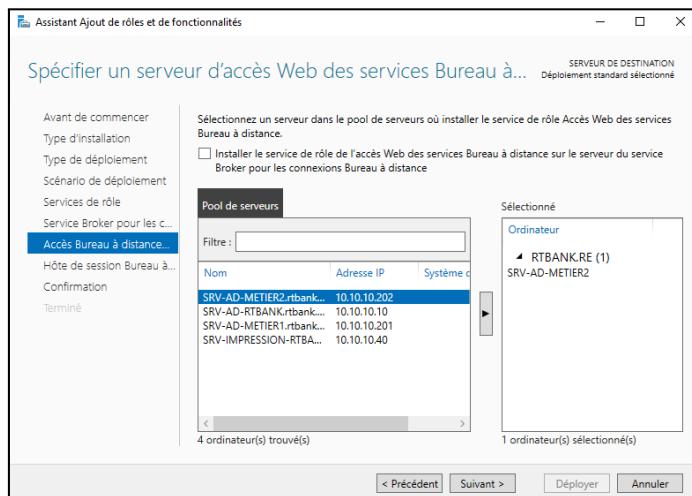
## - Installation et configuration des “serveur métiers” dans l’AD

Pour enrichir notre infrastructure, nous avons ajouté deux serveurs métiers supplémentaires avec une configuration RDS (Remote Desktop Services). Cette mise en place permet aux utilisateurs d'accéder à leur bureau à distance de manière sécurisée.

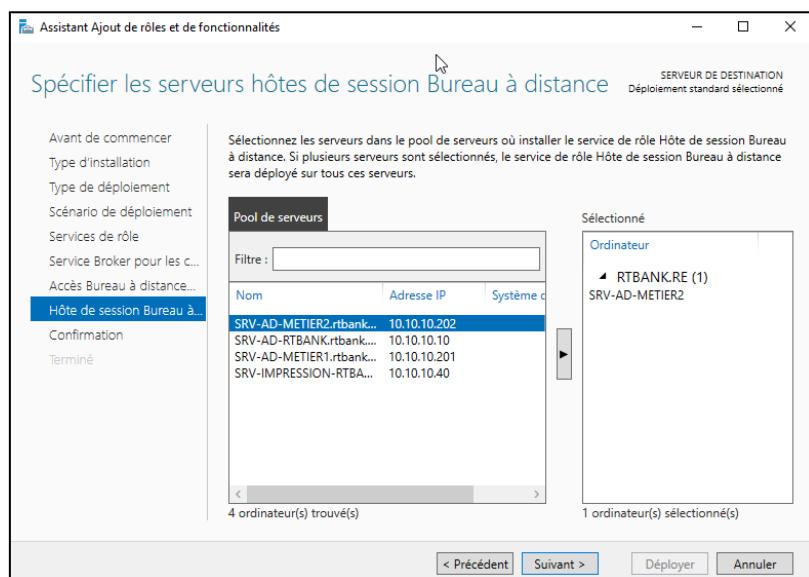
Sur le premier serveur métier, nous avons configuré le rôle de broker RDS. Ce serveur agit comme point central de gestion des connexions à distance, assurant une distribution efficace des sessions utilisateurs.



Pour le second serveur métier, nous avons mis en place le service Bureau à distance Web. Cette configuration permet aux utilisateurs d'accéder à leurs applications et bureaux via une interface web sécurisée, offrant ainsi une solution flexible pour le travail à distance.

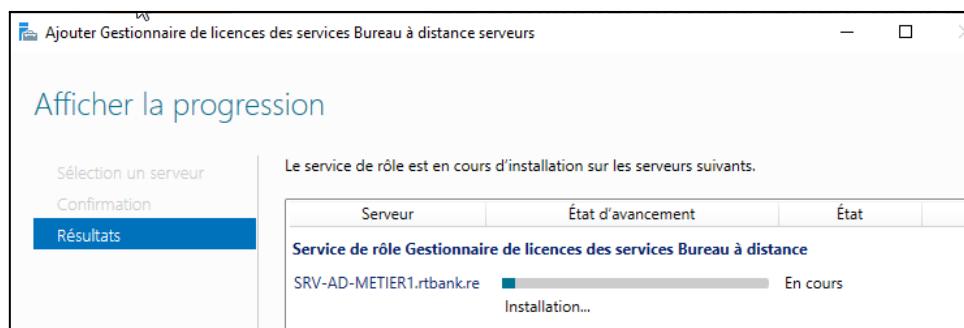
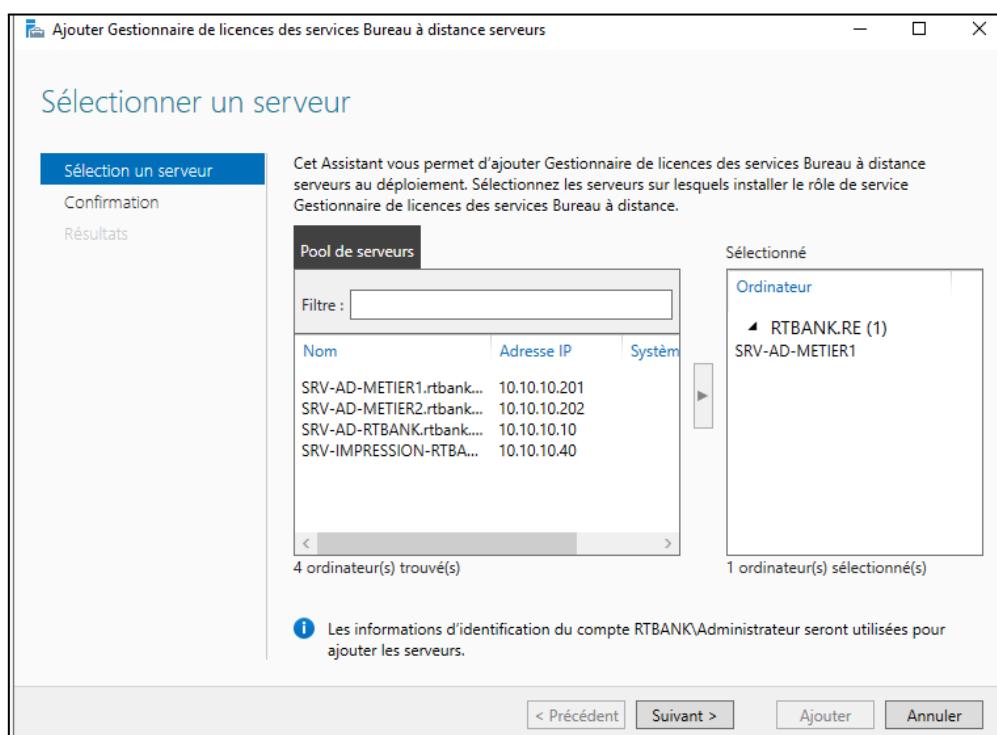


Et je spécifie comme serveur hôte de session le serveur métier 2 :



Une fois l'infrastructure RDS déployée, nous avons configuré le gestionnaire de licences sur le serveur métier 1. Cette étape est cruciale pour la gestion centralisée des licences des services Bureau à distance. Le gestionnaire de licences permet de :

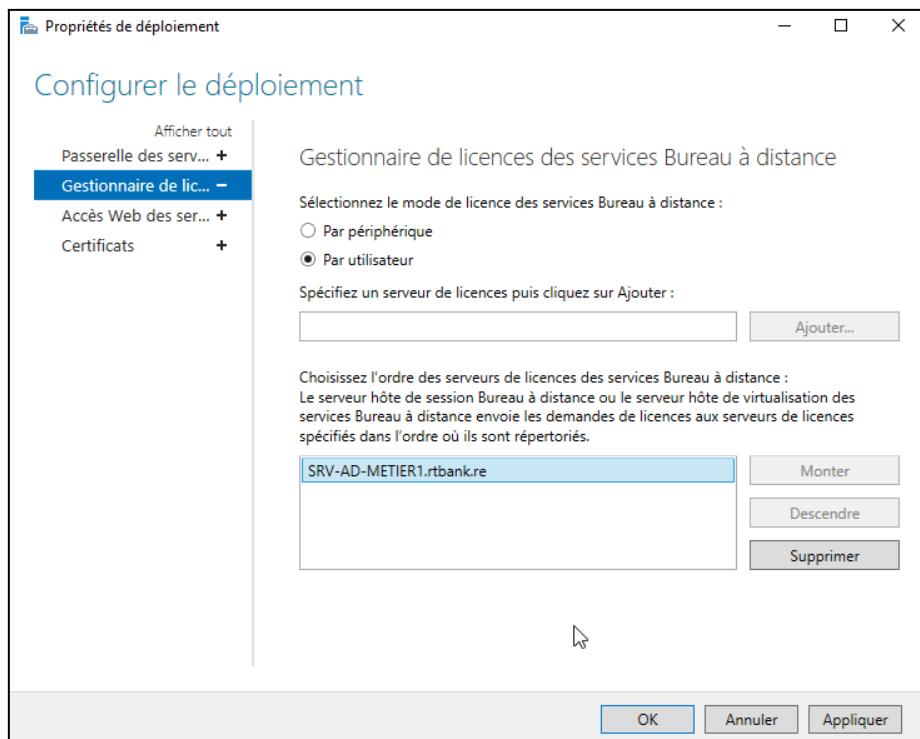
- Contrôler et suivre l'utilisation des licences RDS
- Assurer la conformité des accès utilisateurs
- Gérer efficacement les droits d'utilisation des services Bureau à distance



La configuration de notre ferme RDS présente une architecture complète et fonctionnelle avec les rôles suivants distribués sur nos différents serveurs :

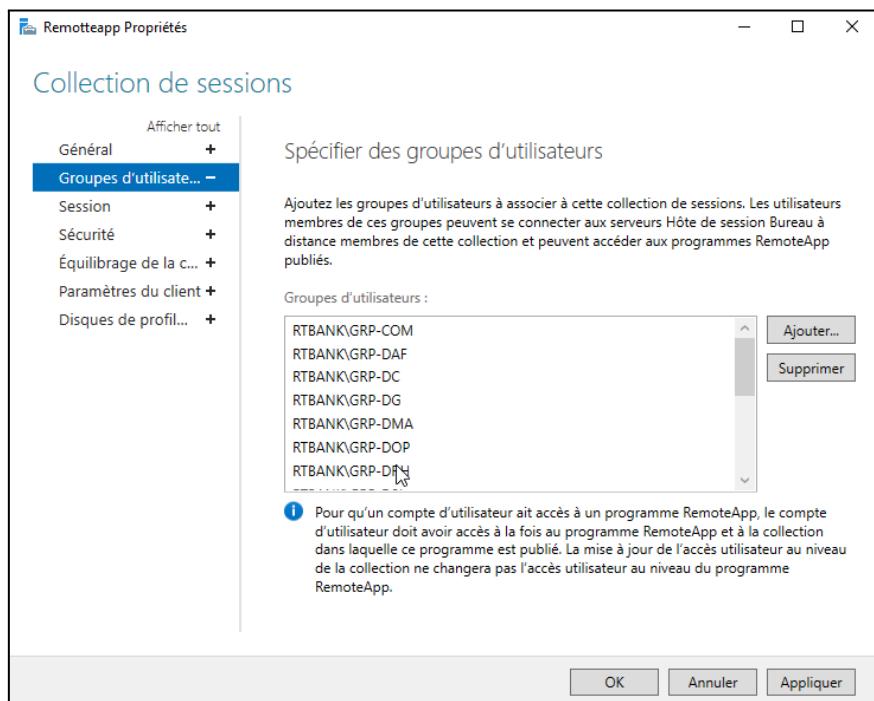
- [SRV-AD-METIER1.RTBANK.RE](http://SRV-AD-METIER1.RTBANK.RE) assure le rôle de Service Broker pour les connexions Bureau à distance et la gestion des licences
- [SRV-AD-METIER2.rtbank.re](http://SRV-AD-METIER2.rtbank.re) héberge l'hôte de session Bureau à distance et l'accès Web aux services

SERVEURS DE DÉPLOIEMENT	
Dernière actualisation le 15/04/2025 10:45:59   Tous les s... <span>TÂCHES ▾</span>	
Nom de domaine complet d...	Service de rôle installé
SRV-AD-METIER1.RTBANK.RE	Service Broker pour les connexions Bureau à distance
SRV-AD-METIER1.RTBANK.RE	Gestionnaire de licences des services Bureau à distance
SRV-AD-METIER2.rtbank.re	Hôte de session Bureau à distance
SRV-AD-METIER2.rtbank.re	Accès Web des services Bureau à distance



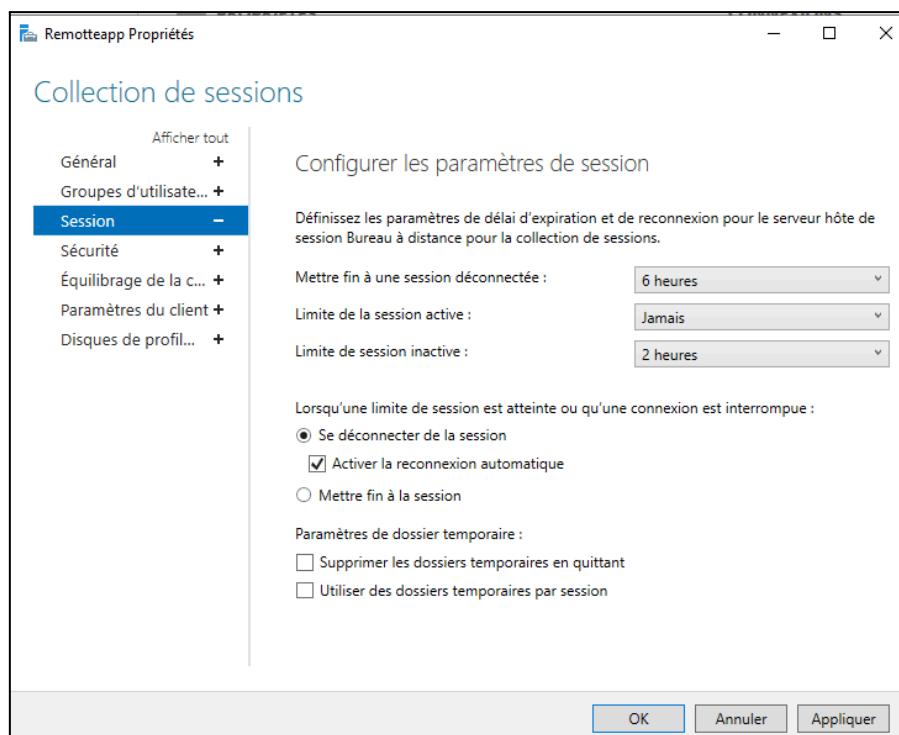
---

Nous avons spécifié tous les groupes d'utilisateurs de l'arborescence de notre domaine [rtbank.re](http://rtbank.re). Cette configuration permet de définir précisément quels groupes auront accès aux services Bureau à distance.

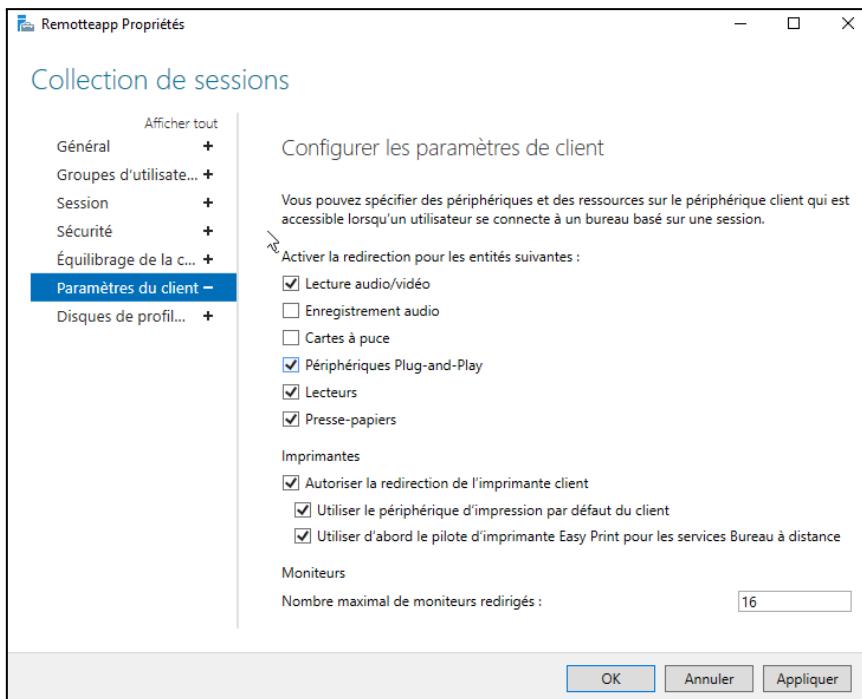


Puis nous avons défini les paramètres de session pour chaque utilisateur, notamment :

- Les limites de durée des sessions actives et inactives
- Les options de déconnexion automatique
- La gestion des sessions temporaires
- Les paramètres de reconnexion

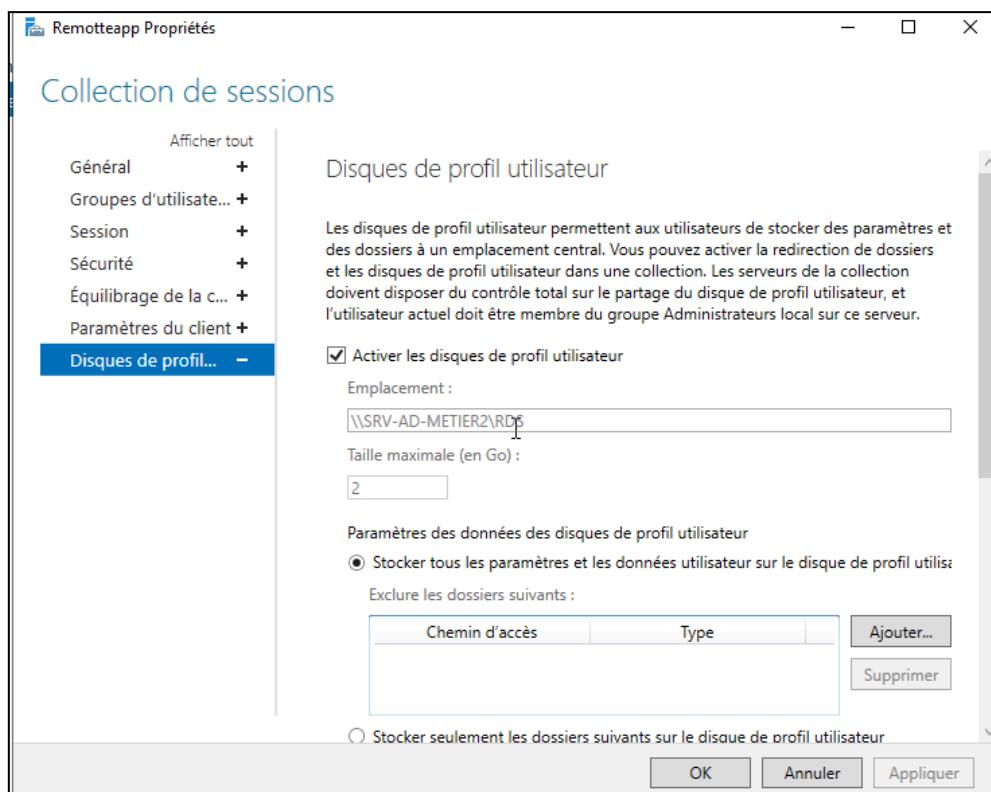


Ainsi que les paramètres du client :



---

Sur le Serveur métier 2, nous avons configuré un dossier de disques de profil utilisateur spécifique. Cette configuration permet de stocker de manière centralisée les paramètres personnalisés pour chaque session utilisateur. Les profils itinérants ainsi créés assurent que les utilisateurs retrouvent leur environnement personnalisé quelle que soit la machine utilisée pour se connecter.



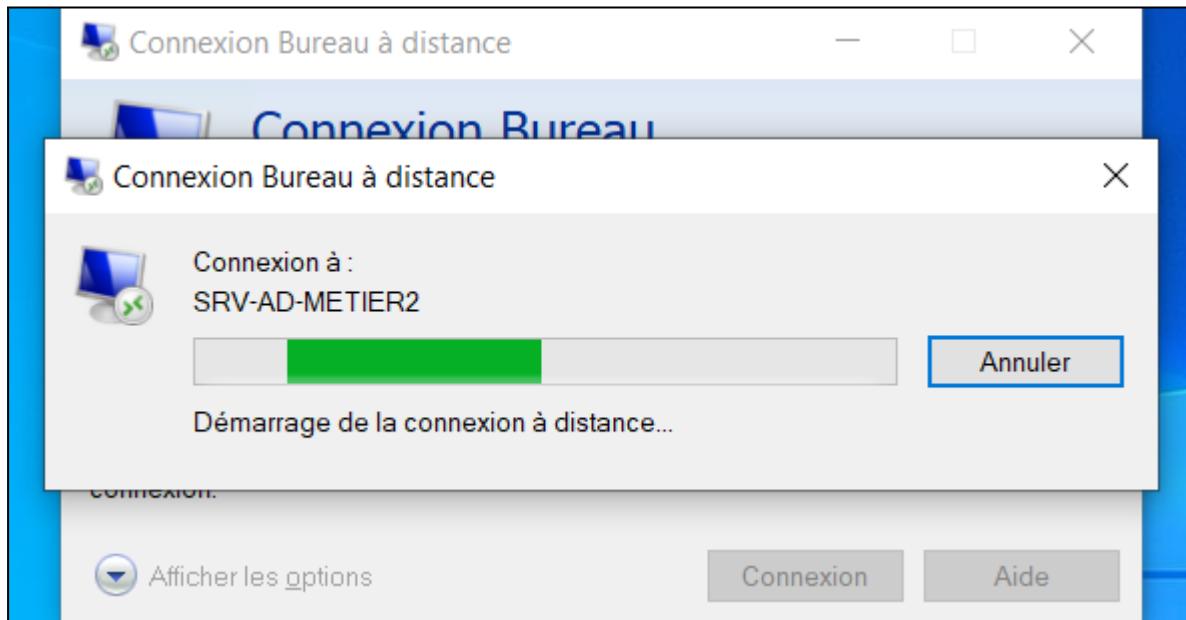
De plus, nous avons déployé plusieurs programmes RemoteApp pour faciliter l'accès aux applications :

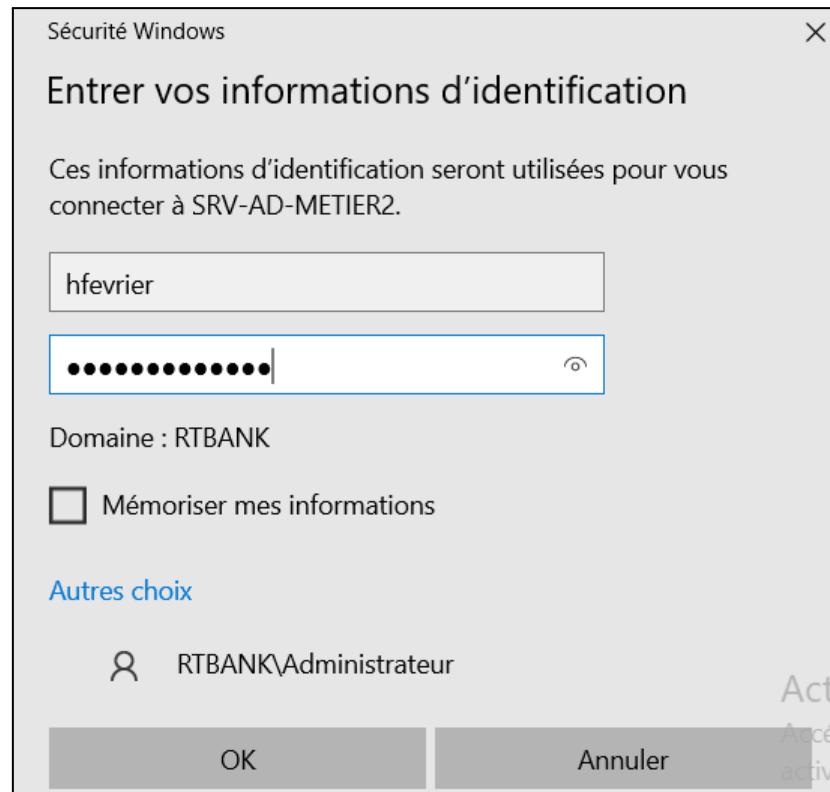
- La Calculatrice (win32calc)
- L'outil de capture d'écran (SnippingTool)
- Le logiciel Paint (mspaint)

Ces applications sont maintenant accessibles via l'interface Web RDS, offrant aux utilisateurs un accès simplifié aux outils essentiels depuis n'importe quel poste de travail.

PROGRAMMES REMOTEAPP		
Dernière actualisation le 15/04/2025 11:08:14   Programmes R... TÂCHES		
Nom du programme RemoteApp	Alias	Visible dans l'Accès Web de
Calculatrice	win32calc	Oui
Outil Capture d'écran	SnippingTool	Oui
Paint	mspaint	Oui

Après avoir finalisé l'ensemble de la configuration de notre ferme RDS, nous avons procédé à une phase de tests approfondis. Pour valider le bon fonctionnement du système, nous avons utilisé le compte de l'utilisateur "hfevrier" comme profil de test. La connexion depuis le client 1 s'est établie sans difficulté, démontrant la stabilité de notre configuration.





UVHD-S-1-5-21-917528024-863052377-18...	15/04/2025 11:06	Fichier image de d...	167 936 Ko
UVHD-template	15/04/2025 11:02	Fichier image de d...	102 400 Ko

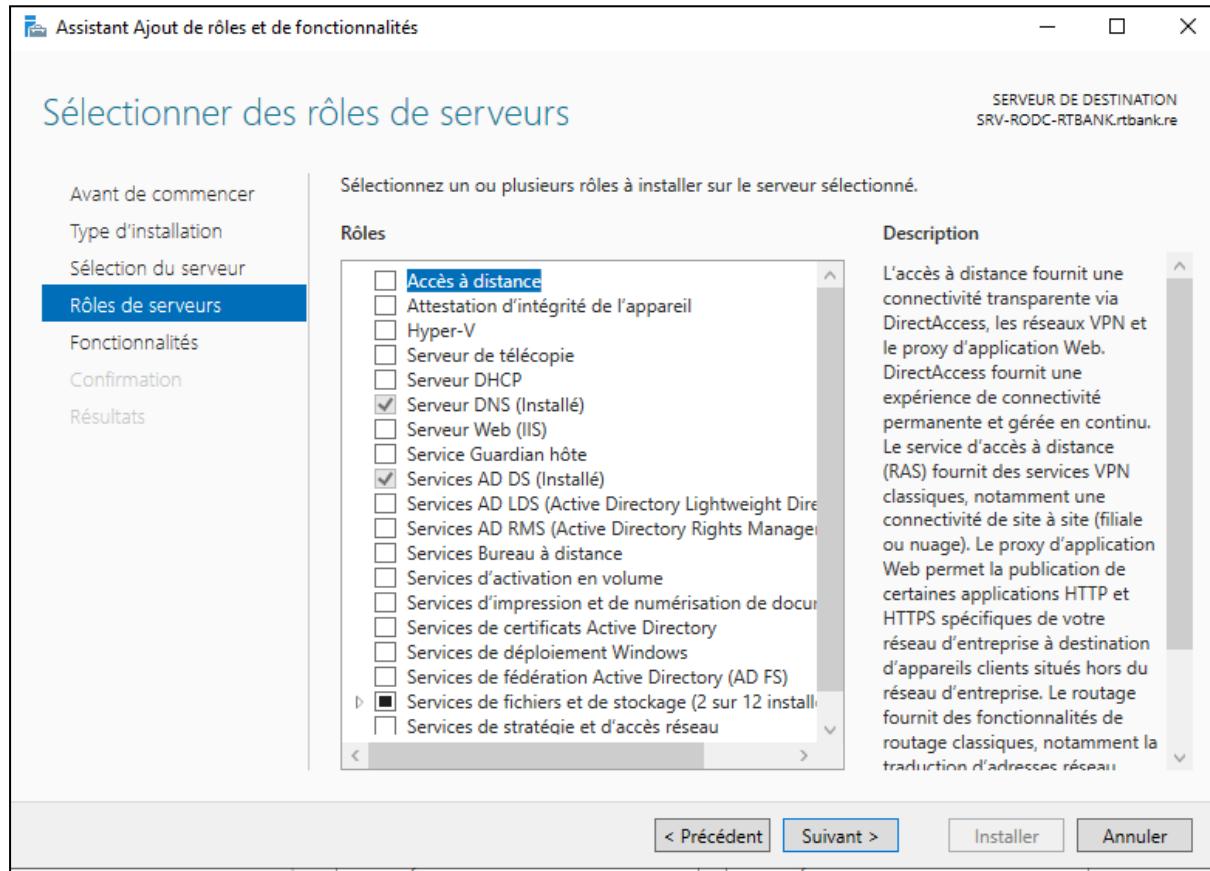
Le système a automatiquement généré un disque de profil personnalisé pour l'utilisateur "hfevrier", confirmant le bon fonctionnement de la gestion des profils utilisateurs. Cette création de profil garantit que les paramètres et préférences de l'utilisateur seront conservés entre les sessions.

Ces résultats positifs démontrent que notre ferme RDS est désormais pleinement opérationnelle, offrant une solution robuste et fiable pour l'accès à distance aux ressources de l'entreprise.

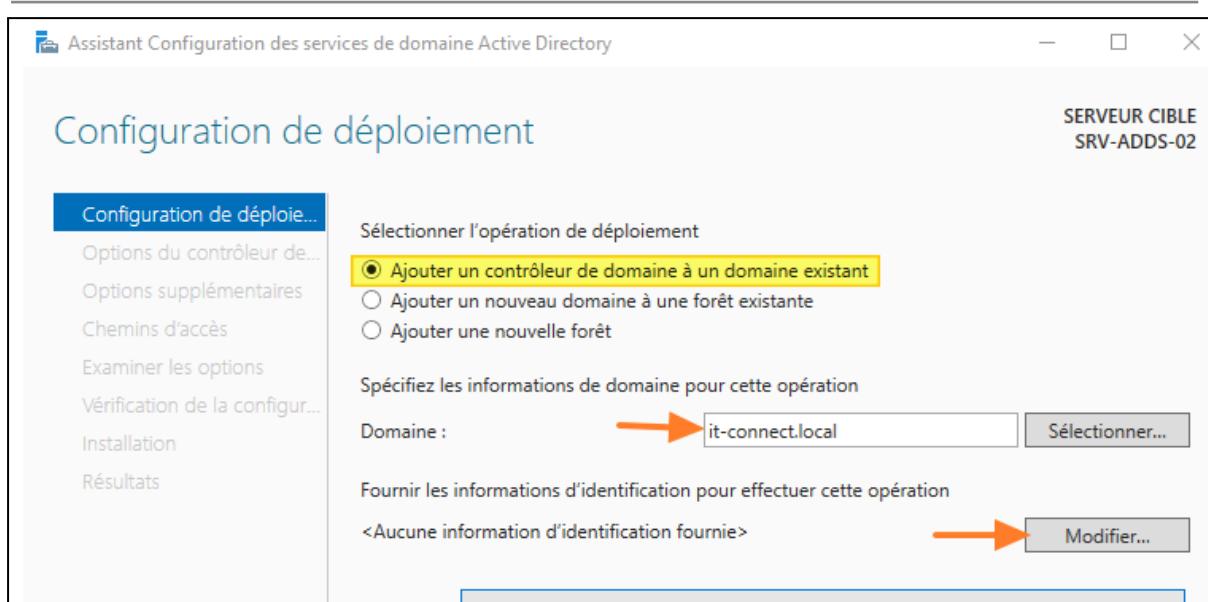
## - Configuration de l'AD RODC

Nous allons ajouter la machine distante du site de st pierre sur le domaine rtbank.re en RODC.

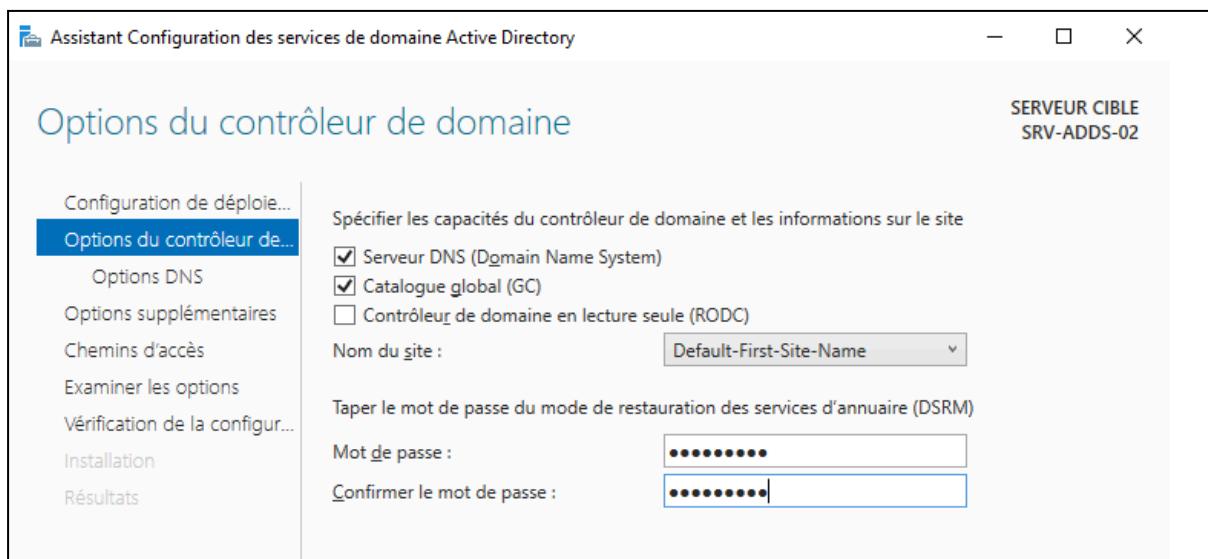
On installe les fonctionnalités AD DS et DNS sur l'AD RODC :



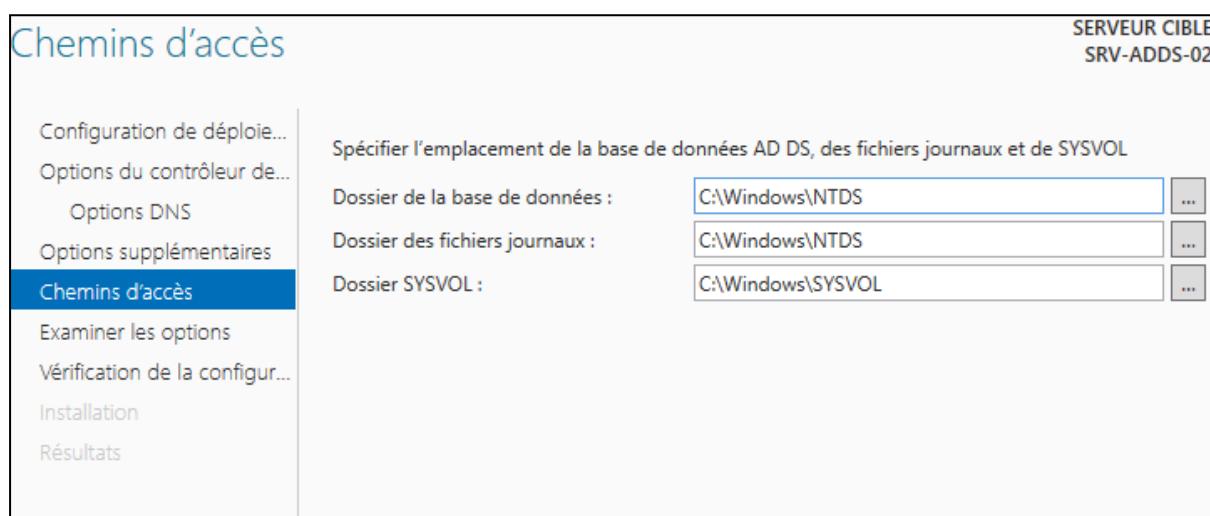
une fois installé nous avons promu cette machine en contrôleur de domaine et nous l'avons ajouté à un domaine comme dans l'exemple ci dessous mais en tapant le nom de domaine rtbank.re :

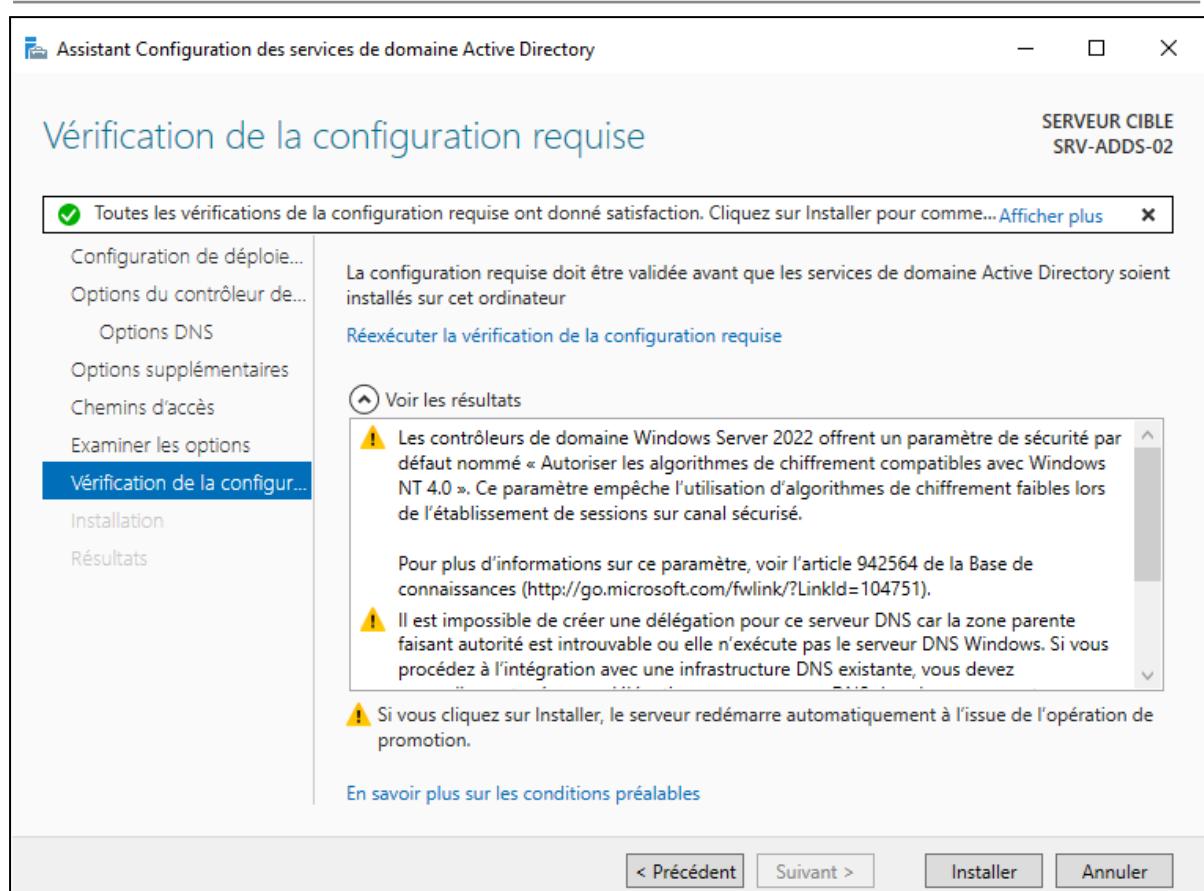


Nous avons coché l'option du contrôleur de domaine en lecture seule (RODC) et taper le mot de passe du mode de restauration comme dans l'exemple ci dessous :



Nous avons choisi de répliquer depuis le serveur principal 10.10.10.10





L'installation du contrôleur de domaine en lecture seule (RODC) est désormais terminée, renforçant ainsi la sécurité et l'efficacité de notre infrastructure Active Directory sur le site de Saint-Pierre.

---

## Conclusion

En conclusion de ce projet SAÉ 4.CYBER 01, nous avons réussi à mettre en place une infrastructure réseau sécurisée complète pour RT Bank, répondant aux exigences spécifiées dans le cahier des charges.

Nos principales réalisations comprennent :

- L'implémentation d'un pare-feu avec une DMZ sécurisée
- La mise en place d'un cluster de serveurs web hautement disponible
- Le déploiement d'un service DNS redondant
- La configuration d'une infrastructure Active Directory robuste
- L'installation d'un système de supervision centralisé
- La mise en place d'un accès distant sécurisé via RDS

La redondance des services critiques assure une haute disponibilité de l'infrastructure, tandis que les mécanismes de sécurité mis en place (certificats SSL, GPO, filtrage réseau) garantissent la confidentialité et l'intégrité des données.

Les tests effectués confirment le bon fonctionnement de l'ensemble des services et leur conformité aux exigences de sécurité. Cette infrastructure offre désormais à RT Bank une base solide et sécurisée pour ses opérations, avec la possibilité d'évoluer selon les besoins futurs de l'entreprise.

---

## Perspectives futures

Dans le cadre des améliorations futures de la sécurité, nous prévoyons d'effectuer un audit approfondi de notre domaine à l'aide de l'outil Ping Castle. Cet outil permettra d'identifier d'éventuelles vulnérabilités et de renforcer davantage la sécurité de notre infrastructure Active Directory en interne.

Nous avons également initié la mise en place d'une stratégie de groupe (GPO) pour la gestion centralisée des impressions. Cette configuration permettra de déployer automatiquement les imprimantes aux utilisateurs selon leurs besoins et leurs droits d'accès, simplifiant ainsi la gestion des ressources d'impression dans l'entreprise. Cette GPO nécessitera des ajustements et des tests supplémentaires pour garantir son fonctionnement optimal.

Il est prévu d'affiner les règles de filtrage sur l'ensemble des interfaces du pare-feu. Par exemple, pour optimiser la supervision via Cacti, nous devrons autoriser spécifiquement les protocoles ICMP et SNMP entre le LAN-Clients et le LAN-Serveurs.

---

De même, une révision complète des règles de filtrage sera nécessaire pour chaque interface (DMZ, WAN, OPT1, OPT2) afin d'appliquer le principe de moindre privilège tout en garantissant le bon fonctionnement des services essentiels.

### **Tableau des acronymes**

<b>Acronyme</b>	<b>Signification</b>	<b>Description</b>
DMZ	DeMilitarized Zone	Zone démilitarisée, segment isolé du réseau
DNS	Domain Name System	Système de noms de domaine
AD	Active Directory	Service d'annuaire de Microsoft
GPO	Group Policy Object	Stratégie de groupe
HTTPS	HyperText Transfer Protocol Secure	Protocole de transfert hypertexte sécurisé
SSL	Secure Sockets Layer	Protocole de sécurisation des échanges
RDS	Remote Desktop Services	Services Bureau à distance
SNMP	Simple Network Management Protocol	Protocole de gestion de réseau
DHCP	Dynamic Host Configuration Protocol	Protocole de configuration dynamique des hôtes
NAT	Network Address Translation	Translation d'adresses réseau
RODC	Read-Only Domain Controller	Contrôleur de domaine en lecture seule
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	Autorité nationale en matière de sécurité informatique
FQDN	Fully Qualified Domain Name	Nom de domaine complet
OU	Organizational Unit	Unité d'organisation dans l'Active Directory

---

**Annexe :**

Installation du serveur d'impression et configuration des GPO du serveur d'impression

[https://www.youtube.com/watch?v=l4yX5O\\_-nRk](https://www.youtube.com/watch?v=l4yX5O_-nRk)

<https://www.youtube.com/watch?v=xy5GYdvcrD0>

Promouvoir un contrôleur de domaine en RODC :

<https://www.it-connect.fr/active-directory-adds-ajouter-un-controleur-de-domaine-a-un-domaine-existant>

GPO lecteur réseau :

<https://www.it-connect.fr/comment-monter-un-lecteur-reseau-par-gpo>