

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Matys CHAGOT / Nathan MICHEL / Melvin PATEL / Milan LELIEVRE - 2025/2026

FICHE RÉSEAU ET SERVEURS



CONTEXTE ET OBJECTIF :

TechUniverse, entreprise spécialisée dans la vente de produits technologiques, connaît une forte hausse de fréquentation sur son site web. L'infrastructure actuelle n'étant pas dimensionnée pour supporter ce trafic, le site subit ralentissements, erreurs et indisponibilités. Ces problèmes dégradent l'expérience client et entraînent des pertes commerciales. Pour remédier à cette situation, la direction lance un projet visant à améliorer la **haute disponibilité de la DMZ**, en tenant compte de la surcharge des serveurs et du manque d'hôtes. Parallèlement, l'entreprise souhaite déployer une **solution d'accès distant** pour ses télétravailleurs. Votre rôle consiste à préparer cette nouvelle architecture en réalisant une **maquette de test** à l'aide de machines virtuelles, afin de valider l'intégration de la future solution.



STORMSHIELD

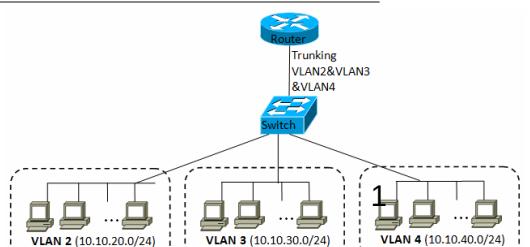


Figure 12.5. 802.1Q trunk between the router and the switch

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

SOMMAIRE :

I. MATÉRIEL ET RESSOURCES

II. SCHÉMA DU RÉSEAU

III. RÉALISATION DE L'INFRASTRUCTURE

1. Mise en place des serveurs HAProxy.....(P6-7)
2. Mise en place de la haute disponibilité pour les HAProxy.....(P7-11)
3. Mise en place des serveurs Apache2.....(P11)
4. Configuration du routeur Stormshield.....(P12-13)
5. Importation de l'annuaire.....(P14-16)
6. Création du VPN Client.....(P16-21)
7. Installation du serveur AD.....(P22-29)
8. Déploiement d'un partage de fichiers.....(P22-29)

IV. RÉCAP DE L'INFRASTRUCTURE

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

MATÉRIEL ET RESSOURCES :

- Switch [Cisco 2960-X Series](#)



- Serveurs [Dell PowerEdge T340 Tower Server](#)



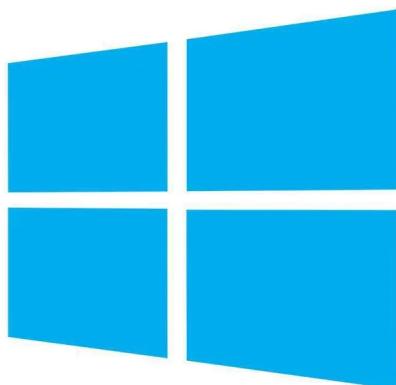
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

- L'OS Debian 12 pour les serveurs



debian

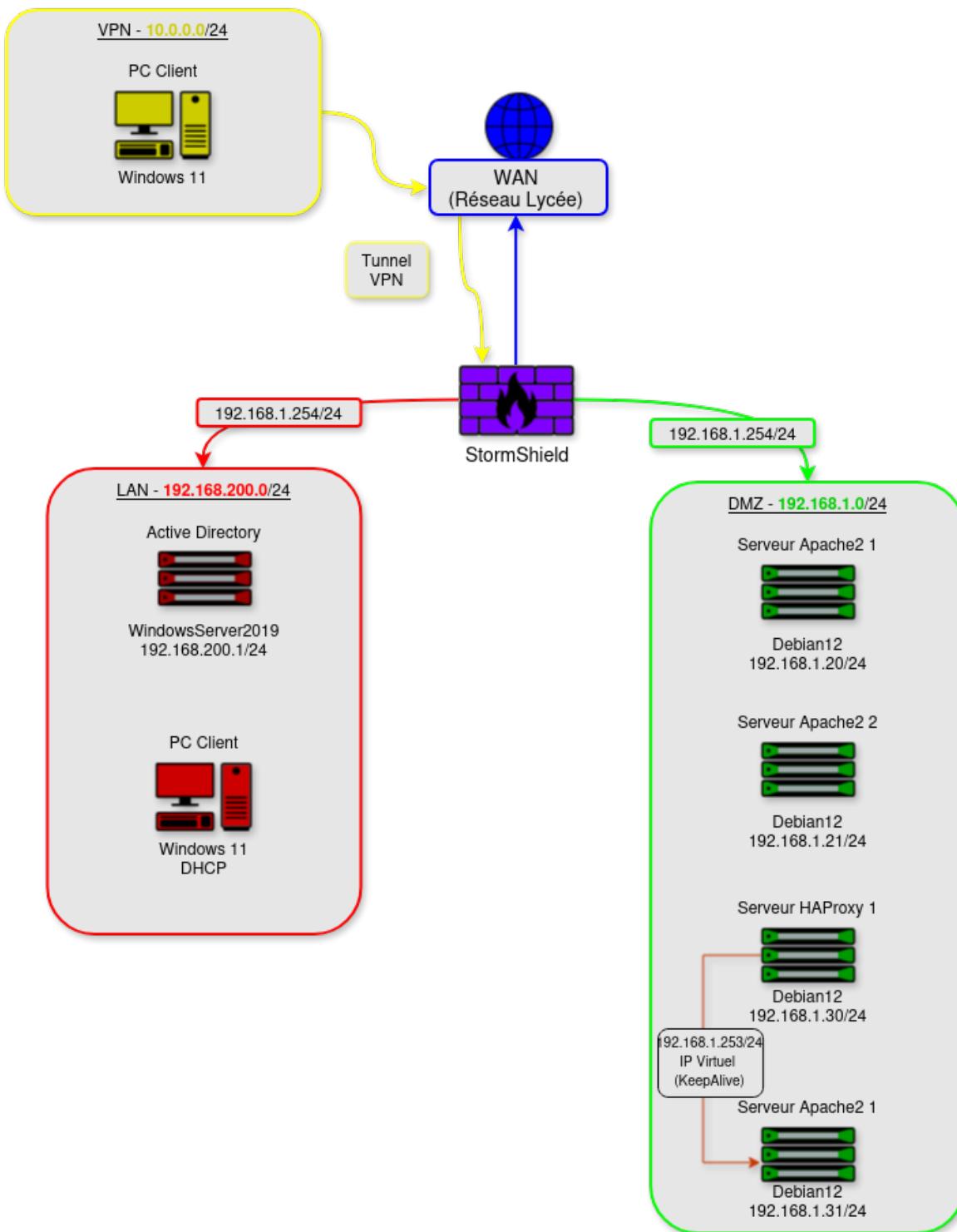
- L'AD sera en windows serveur 2019



Server 2019 Standard

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

SCHÉMA DU RÉSEAU :



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Liens de notre Trello

1. Mise en place des serveurs HAProxy

- Installation haproxy : apt install haproxy

Pour configurer le service et mettre en place la haute disponibilité de notre site web HAProxy, il suffit de rentrer cette configuration dans /etc/haproxy/haproxy.cfg :

```
global
    log /dev/log local0

defaults
    mode http
    timeout connect 5000ms
    timeout client 50000ms
    timeout server 50000ms

frontend http_front      # interface entre les clients et HAProxy (reçois les requêtes)
    bind *:80           #ports
    default_backend http_back

backend http_back         #interface entre HAProxy et les serveurs web réels (envoie les
requêtes vers les serveurs)
    balance roundrobin   # Distribution séquentielle du trafic à chaque serveur à tour de
rôle.
    server server1 192.168.1.20:80 check    # "check" Permet la vérification du serveur web et le
    server server2 192.168.1.21:80 check      # Désactive si celui ci est non-fonctionnelle
```

La configuration pour les deux serveurs doit être la même. Il est également possible d'ajouter une page de stats sur le HAProxy pour voir tout le trafic entrant sur les pages web publiées par ce dernier. Pour ce faire, il suffit d'ajouter quelques paramètres :

```
acl is_stats path_beg /stats
use_backend stats_backend if is_stats
```

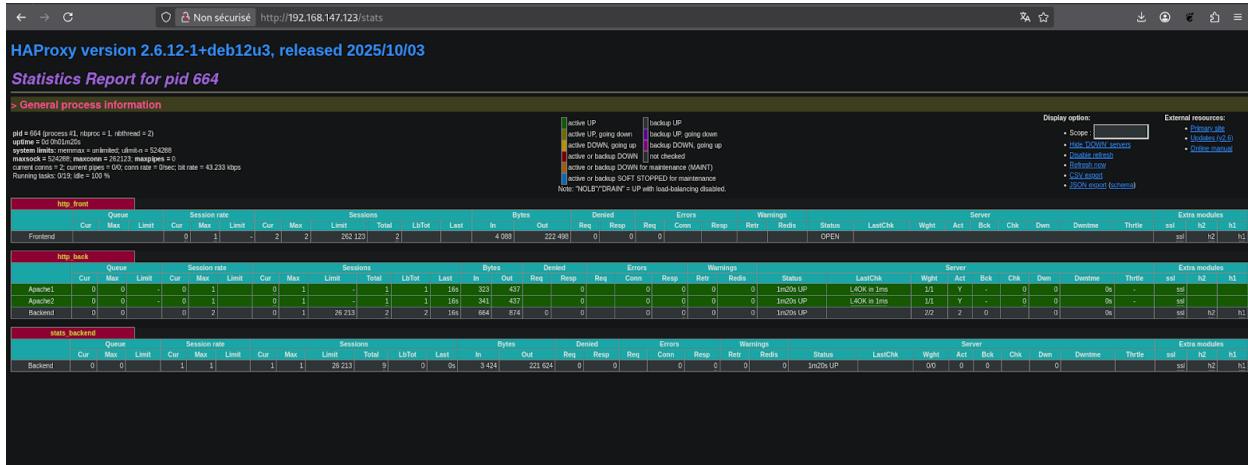
à ajouter dans le “**frontend http_front**”.

Il est également nécessaire de créer le backend correspondant à la page de stats

```
backend stats_backend
    stats enable
    stats uri /stats  stats refresh 10s
    stats show-modules
```

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Une fois les modifications faites, une nouvelle page est disponible sur l'adresse suivante : <http://<ip-du-stormshield>/stats>



The screenshot shows the HAProxy statistics page at <http://192.168.147.123/stats>. The top header indicates "HAProxy version 2.6.12-1+deb12u3, released 2025/10/03". Below it, a "Statistics Report for pid 664" is displayed. The page includes a legend for status colors (green for active UP, purple for backup UP, etc.) and a "Display option" section with checkboxes for "Ssl offload", "HTTP/2 support", "Update now", "Check interval", and "Check manual". The main content is divided into sections: "General process information", "http frontend", "http backend", and "stats backend". Each section contains tables for "Session rate" and "Sessions" with columns for Cur, Max, Limit, Bytes, Denied, Errors, Warnings, and Server statistics like LastChk, Wght, Act, Bck, Chk, Dwn, and Throttle. The "Extra modules" column shows values for ssl, h2, and h3.

2. Mise en place de la haute disponibilité pour les HAProxy

Ensuite, nous avons installé le service KeepAlive qui sert à **gérer une IP virtuelle partagée** entre plusieurs serveurs afin **d'éviter les interruptions de service**, ce qui **améliore la robustesse d'une DMZ** en assurant un basculement automatique et en **priorisant les serveurs** selon leur niveau d'importance.

La première chose à faire était donc d'installer KeepAlive sur les VMs via la commande : apt install keepalived.

Puis, cd /etc/keepalived afin de changer le nom du fichier.

```
root@TemplateDebian12:/etc/keepalived# mv keepalived.conf.sample keepalived.conf
```

Suite à cela, nous accédons à "nano /etc/keepalived/keepalived.conf" et nous copions le message dans la doc du cluster.

DOCUMENTATION CONFIGURER

UN RÉSEAU D'ENTREPRISE

La configuration du fichier devrait ressembler à ceci :

```
vrrp_script reload_haproxy {
    script "killall -0 haproxy"
    interval 1
}

vrrp_instance VI_1 {
    virtual_router_id 80
    state MASTER ou SLAVE
    priority 100 / 90 pour le Slave
    # Check inter-load balancer toutes les 1 secondes
    advert_int 1
    # Synchro de l'état des connexions entre les LB sur l'interface
    enp0s3
    lvs_sync_daemon_interface enp0s3
    interface enp0s3
    # Authentification mutuelle entre les LB, identique sur les deux
    membres
    authentication {
        auth_type PASS
        auth_pass secret
    }
    # Interface réseau commune aux deux LB
    virtual_ipaddress {
        192.168.1.253/32 brd 192.168.1.255 scope global
    }

    track_script {
        reload_haproxy
    }
}
```

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Les éléments surlignés sont à changer impérativement afin de se connecter entre HAProxy et de permettre le Loadbalancing (qui permet de passer d'un serveur à l'autre).

```
GNU nano 7.2                                     /etc/keepalived/keepalived.conf

vrrp_script reload_haproxy {
    script "killall -0 haproxy"
    interval 1
}

vrrp_instance VI_1 {
    virtual_router_id 80
    state SLAVE
    priority 90
    # Check inter-load balancer toutes les 1 secondes
    advert_int 1
    # Synchro de l'état des connexions entre les LB sur l'interface enp0s3
    lvs_sync_daemon_interface enp0s3
    interface enp0s3
    # Authentification mutuelle entre les LB, identique sur les deux membres
    authentication {
        auth_type PASS
        auth_pass secret
    }
    # Interface réseau commune aux deux LB
    virtual_ipaddress {
        192.168.1.253/32 brd 192.168.1.255 scope global
    }
    track_script {
        reload_haproxy
    }
}
```

Vérifier que l'ip soit bien la bonne en faisant un ip a :

```
root@HAProxy1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8b:9b:b9 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.31/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe8b:9bb9/64 scope link
            valid_lft forever preferred_lft forever
root@HAProxy1:~#
```

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Nous voyons que quand le master est éteint, le slave récupère l'adresse ip du master.

Enfin, une fois le master rallumé, pour repasser en master il faut changer le paramètre "priority" et mettre un plus petit nombre sur le slave.

```
root@HAProxy1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8b:9b:b9 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.31/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet 192.168.1.253/32 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe8b:9bb9/64 scope link
            valid_lft forever preferred_lft forever
root@HAProxy1:~#
```

Le Master a bien l'adresse ip virtuel :

```
root@HAProxy2:/etc/keepalived# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:08:23:b7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.32/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet 192.168.1.253/32 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe08:23b7/64 scope link
            valid_lft forever preferred_lft forever
root@HAProxy2:/etc/keepalived#
```

Quand le Master fonctionne bien, l'IP est :

```
root@HAProxy1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8b:9b:b9 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.31/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe8b:9bb9/64 scope link
            valid_lft forever preferred_lft forever
root@HAProxy1:~#
```

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Quand le Master est down, le Slave récupère bien l'adresse ip virtuel :

```
root@HAProxy1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8b:9b:b9 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.31/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet 192.168.1.253/32 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe8b:9bb9/64 scope link
            valid_lft forever preferred_lft forever
root@HAProxy1:~#
```

Dès que le Master est up il récupère directement l'adresse ip virtuel :

```
root@HAProxy2:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:08:23:b7 brd ff:ff:ff:ff:ff:ff
        inet 192.168.1.32/24 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet 192.168.1.253/32 brd 192.168.1.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe08:23b7/64 scope link
            valid_lft forever preferred_lft forever
root@HAProxy2:~# _
```

3. Mise en place des serveurs Apache2

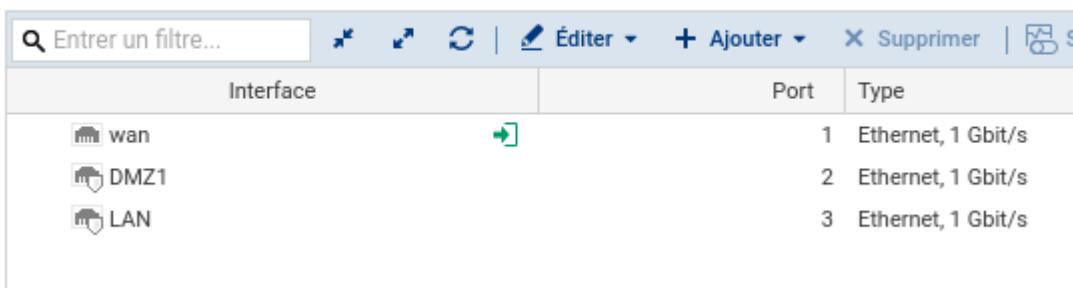
La première étape pour héberger le site web est tout d'abord de l'importer sur le serveur Apache via SSH, SFTP, ou encore SCP. Nous l'avons stocké dans le répertoire suivant : "[/var/www/TechUnivers](#)". Il ne reste plus qu'à faire le virtual host dans Apache en créant le fichier [**001-default.conf**](#) dans le répertoire de configuration d'apache "[/etc/apache2/site-available](#)". Vous pouvez l'activer ensuite avec la commande `a2ensite`.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

4. Configuration du routeur stormshield

Tout d'abord, configurer les interfaces du routeur, il comporte deux réseaux internes ainsi que son réseau **WAN**.

RÉSEAU / INTERFACES



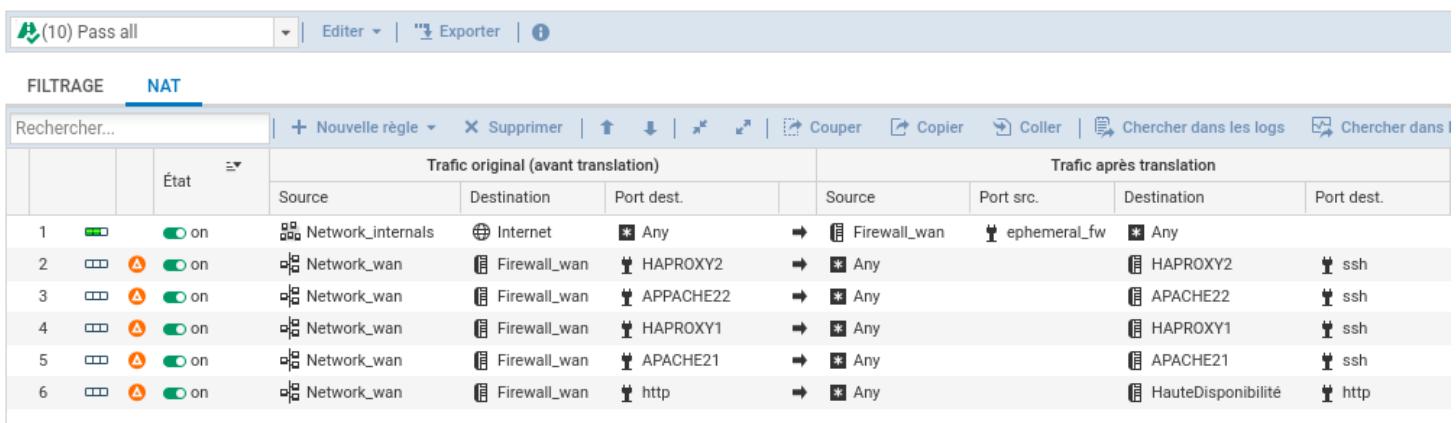
Interface	Port	Type
wan	1	Ethernet, 1 Gbit/s
DMZ1	2	Ethernet, 1 Gbit/s
LAN	3	Ethernet, 1 Gbit/s

Les différentes plages d'adresse sont donc les suivantes :

- **WAN** : **192.168.147.0/24** (Réseau du lycée)
- **DMZ1** : **192.168.1.0/24**
- **LAN** : **192.168.200.0/24**

Ensuite, afin d'obtenir une meilleure productivité, nous allons mettre en place des règles de **NAT** pour pouvoir exposer notre site web sur internet, mais également quelques services en plus comme le **SSH** pour accéder à chaque machine respective en dehors de notre réseau et autres.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT



Filtrage		NAT							
Rechercher...		+ Nouvelle règle	X Supprimer	↑ ↓ ↻ ↺ ↻ ↺	Couper	Copier	Coller	Chercher dans les logs	Chercher dans l
Trafic original (avant translation)		Trafic après translation							
		Source	Destination	Port dest.		Source	Port src.	Destination	Port dest.
1	on	Network_internals	Internet	* Any	→	Firewall_wan	ephemeral_fw	* Any	
2	on	Network_wan	Firewall_wan	Haproxy2	→	* Any		Haproxy2	ssh
3	on	Network_wan	Firewall_wan	Apache22	→	* Any		Apache22	ssh
4	on	Network_wan	Firewall_wan	Haproxy1	→	* Any		Haproxy1	ssh
5	on	Network_wan	Firewall_wan	Apache21	→	* Any		Apache21	ssh
6	on	Network_wan	Firewall_wan	http	→	* Any		HauteDisponibilité	http

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Ces règles de NAT permettront donc de :

- Donnez internet au réseau interne du routeur
- Se connecter en **SSH** en dehors du **LAN**
- Publier le site web

Pour ce qui des règles de filtrages, dans ce projet, il ne suffit que d'autoriser les clients du VPN à accéder au partage de fichiers Windows.

<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> passer	* Any	<input checked="" type="checkbox"/> Firewall_wan	<input checked="" type="checkbox"/> http <input checked="" type="checkbox"/> https <input checked="" type="checkbox"/> ldap
<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> passer	<input checked="" type="checkbox"/> VPN_UDP <input checked="" type="checkbox"/> VPN_TCP	<input checked="" type="checkbox"/> Network_LAN	<input checked="" type="checkbox"/> microsoft-ds <input checked="" type="checkbox"/> ldap <input checked="" type="checkbox"/> dns
<input checked="" type="checkbox"/> on	<input checked="" type="checkbox"/> passer	* Any	<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> Any

Ces trois règles sont donc les seules règles de filtrages mis en place (la troisième est même optionnelle). Il ne manquera plus qu'un block all en dernière règle.

Ces règles de filtrages permettront donc de :

1. Permettre l'accès aux **services** souhaité de l'**extérieur** (publier le site, le panel admin et l'annuaire Active Directory pour les clients VPN)
2. Permettre l'accès aux partages de fichiers et au serveurs DNS pour les **clients VPN**
3. Permettre le **ping** sur toutes les interfaces pour de meilleurs diagnostics et ainsi améliorer les maintenances liées à divers problèmes réseaux.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

5. Importation de l'annuaire

Ensuite, pour que les utilisateurs de l'Active Directory puisse se connecter au **VPN**, il faut configurer un annuaire comme celui ci-dessous :

CONFIGURATION

+ Ajouter un annuaire

Domain name: techunivers.local

CONFIGURATION STRUCTURE

Activer l'utilisation de l'annuaire utilisateur

Serveur: AD

Port: ldap

Domaine racine (Base Dn): DC=techunivers,DC=local

Identifiant: CN=Administrateur,CN=Users

Mot de passe:

Connexion sécurisée (SSL)

Configuration avancée

Dans cette annuaire, le serveur correspond à l'adresse IP de l'active Directory (transformé en objet), le port par défaut de **LDAP** est **389**, le domaine racine et l'identifiant sont disponible eux sur l'Active Directory dans “[Utilisateurs et Ordinateurs de l'active directory](#)” avec “[fonctionnalité avancée](#)” de cochée.

Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Ajouter/supprimer des colonnes...

Grandes icônes

Petites icônes

Liste

Détails

Utilisateurs, contacts, groupes et ordinateurs en tant que conteneurs

Fonctionnalités avancées

Options de filtre...

Personnaliser...

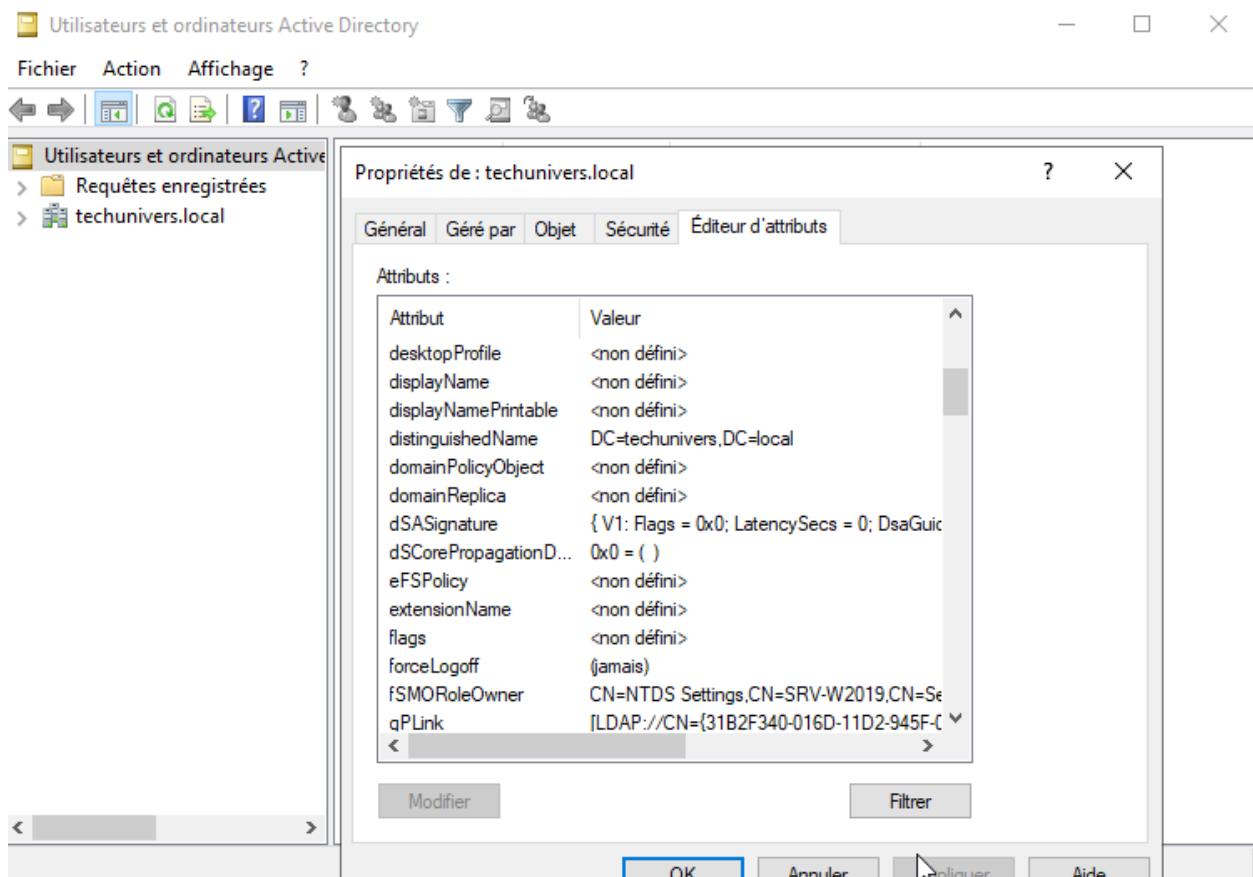
Program Data Conteneur Default location for stor...

System Conteneur Builtin system settings

TPM Devices msTPM-Infor... msTPM-Infor...

Users Conteneur Default container for up...

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE



Il suffira seulement d'effectuer un clique droit sur le groupe / dossier à importer pour avoir le fameux Domaine Racine. Pour l'identifiant il est visible dans la même option mais sélectionné sur un utilisateur plutôt qu'un groupe.

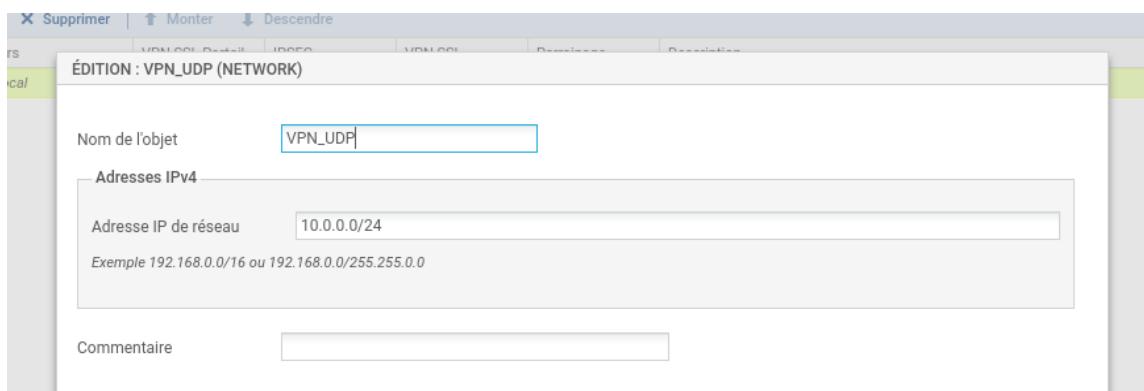
Le mot de passe correspond à celui de l'utilisateur qui se connecte à l'**AD** avec le stormshield.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

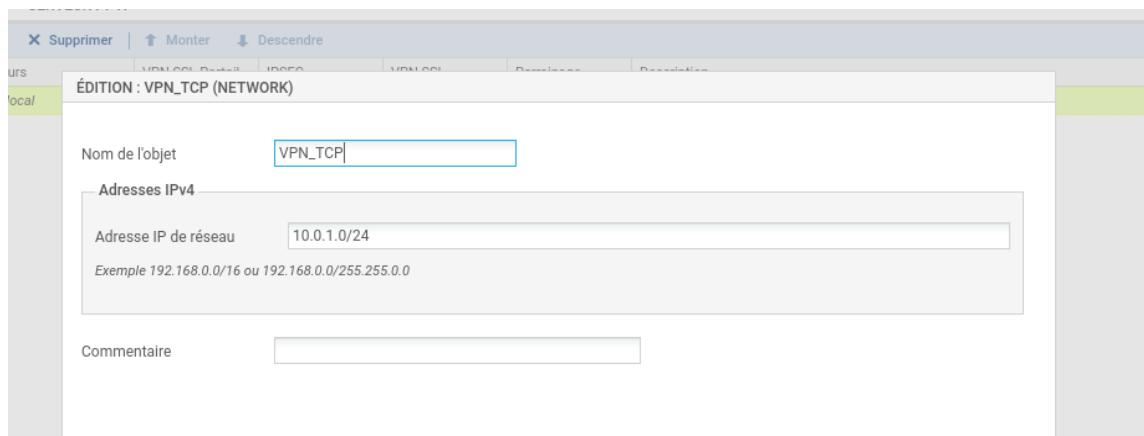
6. Création du **VPN Client**

Tout d'abord, deux objets sont nécessaires à la configuration du **VPN**

- **VPN UDP** : sert donc à la circulation des paquets client en **UDP**



- **VPN TCP** : sert donc à la circulation des paquets client en **TCP**



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Nous pouvons ensuite activer le **VPN SSL** et le configurer tel que montré ci-dessous.

The screenshot shows the configuration interface for a device named EVA1. The main menu on the left includes sections like Configuration, Système, Réseau, Objets, Utilisateurs, Politique de Sécurité, Protection applicative, and VPN. The current section is 'VPN / VPN SSL'. A sub-section titled 'PARAMÈTRES GÉNÉRAUX' is selected. It shows the following configuration:

- Adresse IP publique (ou FQDN) de l'UTM utilisée: 192.168.147.188
- Réseaux ou machines accessibles: Network_Internal
- Réseau assigné aux clients (UDP): VPN_UDP
- Réseau assigné aux clients (TCP): VPN_TCP
- Maximum de tunnels simultanés autorisés: 124

Below this, there is a section for 'Paramètres DNS envoyés au client' with fields for Nom de domaine, Serveur DNS primaire, and Serveur DNS secondaire, all set to 'Configuré pour le firewall'.

Descendre tout en bas dans “**VPN SSL**” et paramètre général puis exporter le fichier de conf.

The screenshot shows the configuration interface for a device named EVA1. The left sidebar has sections like Authentification, Enrôlement, Configuration des annuaires, Politique de Sécurité, Protection applicative, VPN, VPN IPsec, VPN SSL (which is selected), and Notifications. The main panel shows the 'VPN SSL' configuration with the following sections:

- Scripts à exécuter sur le client**: Fields for 'Script à exécuter lors de la connexion' and 'Script à exécuter lors de la déconnexion', both with browse and delete buttons. A 'Réinitialiser' button is also present.
- Certificats**: Fields for 'Certificat serveur' (openvpnserver) and 'Certificat client' (openvpnclient).
- Configuration**: A button labeled 'Exporter le fichier de configuration'.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Aller dans “Utilisateurs” et ajouter le groupe **AD** pour les utilisateurs de **VPN** créer dans le serveur **AD**.

The screenshot shows the Stormshield Network Security interface version 4.8.11. The main menu on the left includes sections for MONITORING, CONFIGURATION, and UTILISATEURS. Under UTILISATEURS, 'Utilisateurs' is selected. The central panel displays a list of users and groups from Active Directory, including 'Lecteurs des journaux d'événements@techuniver...', 'Opérateurs d'assistance de contrôle d'accès@tech...', and 'Utilisateurs@techunivers.local'. A new group 'VPN_users' is being added, with its name and description fields filled. The 'Droits d'accès' tab is visible on the right side of the screen.

Aller dans Droits d'accès pour autoriser le groupe que nous avons ajouté précédemment .

The screenshot shows the 'Utilisateurs / Droits d'accès' configuration page. The 'Droits d'accès' tab is selected in the sidebar. The main panel shows a table for defining access rules. A new rule is being added for the 'VPN_users' group, which is listed in the 'Utilisateur - groupe d'utilisateurs' column. The 'Etat' column shows 'Activé'. The 'VPN SSL Portail' and 'IPSEC' columns have their status set to 'Autoriser' (Allow). Other columns like 'VPN SSL', 'Parrainage', and 'Description' are also present.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Si jamais il faut autoriser tous les utilisateurs, aller dans accès par défaut.

The screenshot shows the 'CONFIGURATION' tab selected in the top navigation bar. Under 'UTILISATEURS / DROITS D'ACCÈS', the 'ACCÈS PAR DÉFAUT' tab is active. It displays settings for 'Accès VPN' and 'Parrainage'. In the 'Accès VPN' section, 'Profil VPN SSL Portail' is set to 'Interdire', 'Politique IPsec' is set to 'Interdire', and 'Politique VPN SSL' is set to 'Autoriser'. In the 'Parrainage' section, 'Politique de parrainage' is set to 'Autoriser'. The left sidebar shows other configuration sections like 'Utilisateurs', 'Droits d'accès' (which is currently selected), 'Authentification', 'Enrôlement', and 'Configuration des annuaires'.

Maintenant pour tester :

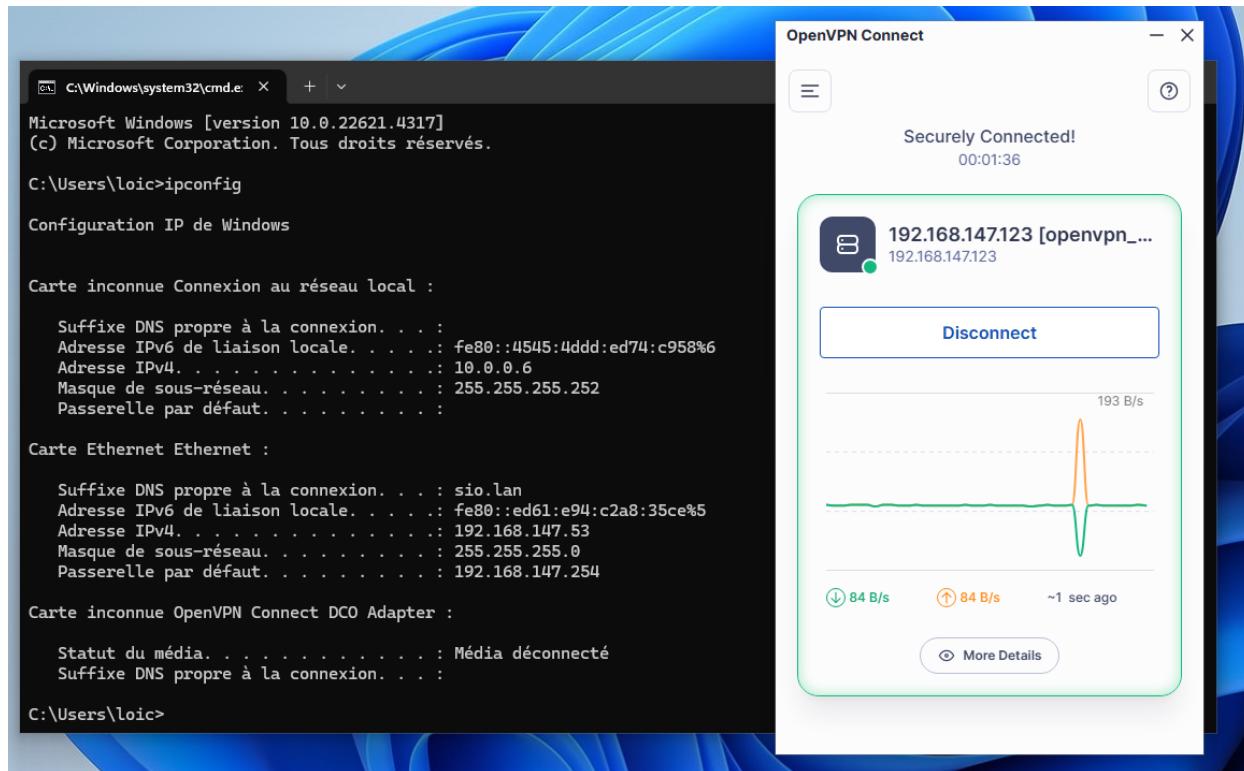
- Ouvrir un Windows client pour se connecter en **VPN**.
- Utiliser un compte présent dans le groupe autorisé au **VPN**.
- Installer le fichier de configuration précédemment téléchargé tel que celui-ci :

▼ Aujourd'hui

	openvpn-connect-3.8.0.4528_signed	14/11/2025 08:48	Package Windows...	113 228 Ko
	openvpn_mobile_client	14/11/2025 08:46	OVPN Profile	6 Ko

- Ouvrir un logiciel de connexion **VPN**, ici [OpenVPN](#) et y importer le fichier de configuration téléchargé précédemment.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE



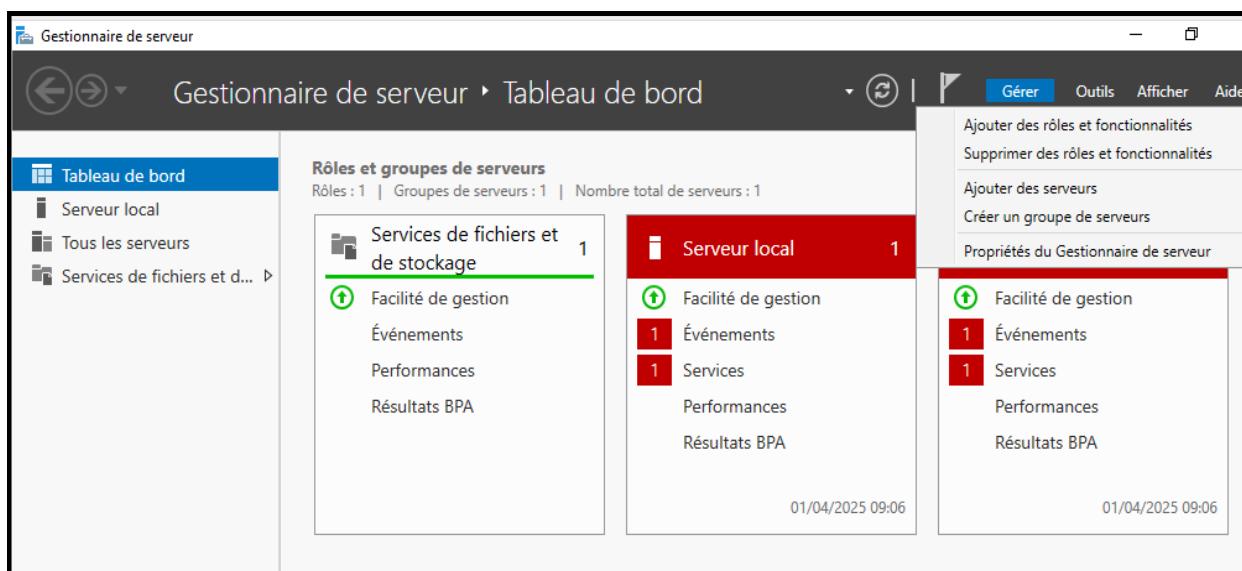
On voit donc ici que le tunnel **VPN** marche, la carte réseau “virtuelle” dans le PC est bien dans la plage — [10.0.0.0/24](#) — et les paquets ont bien l’air de passer à travers le **VPN**.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

7. Installation du serveur AD

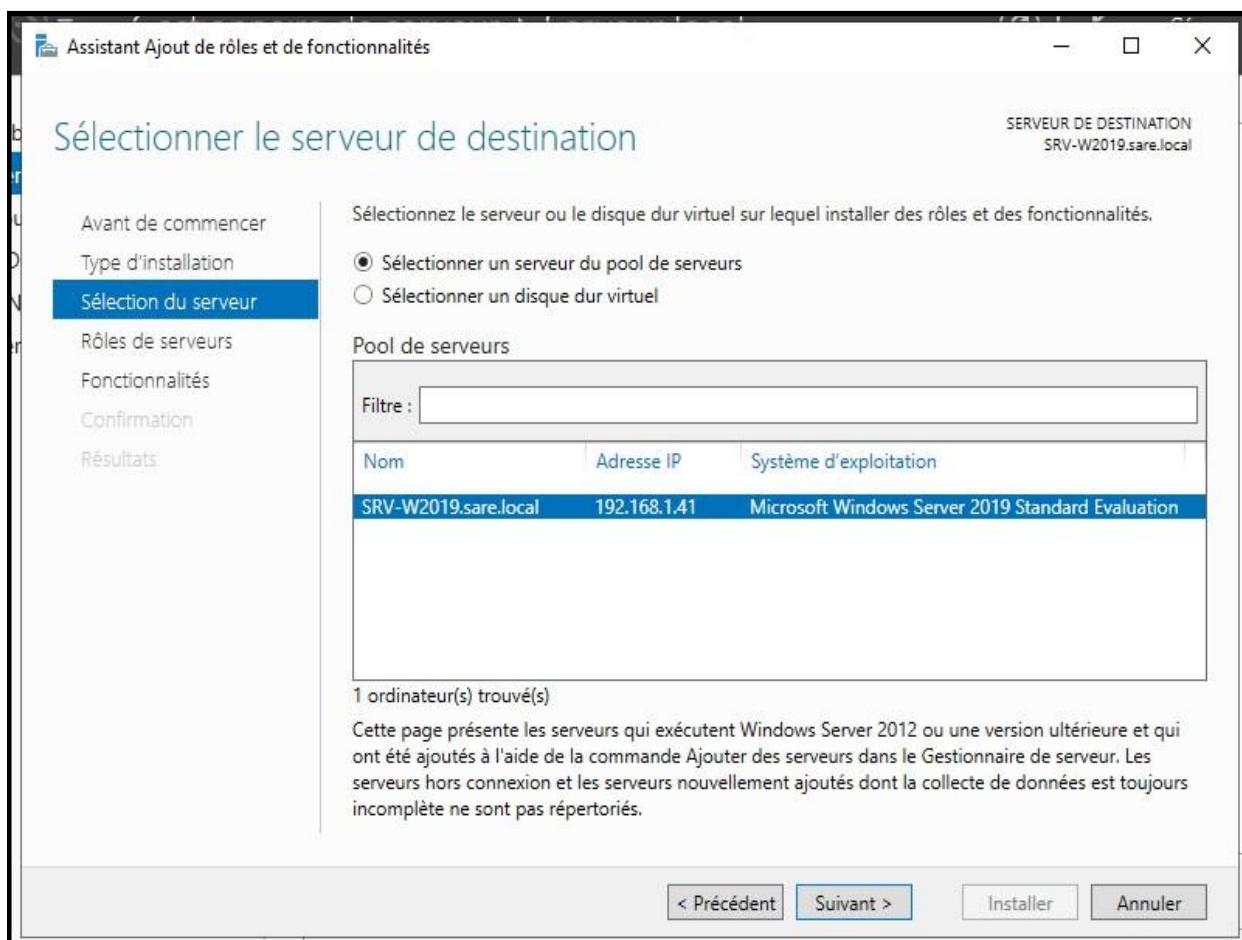
Ouvrez le gestionnaire de serveur puis cliquez “**Gérer**” puis sur « **Ajouter des rôles et des fonctionnalités** »

Suivre les instructions de l’assistant.



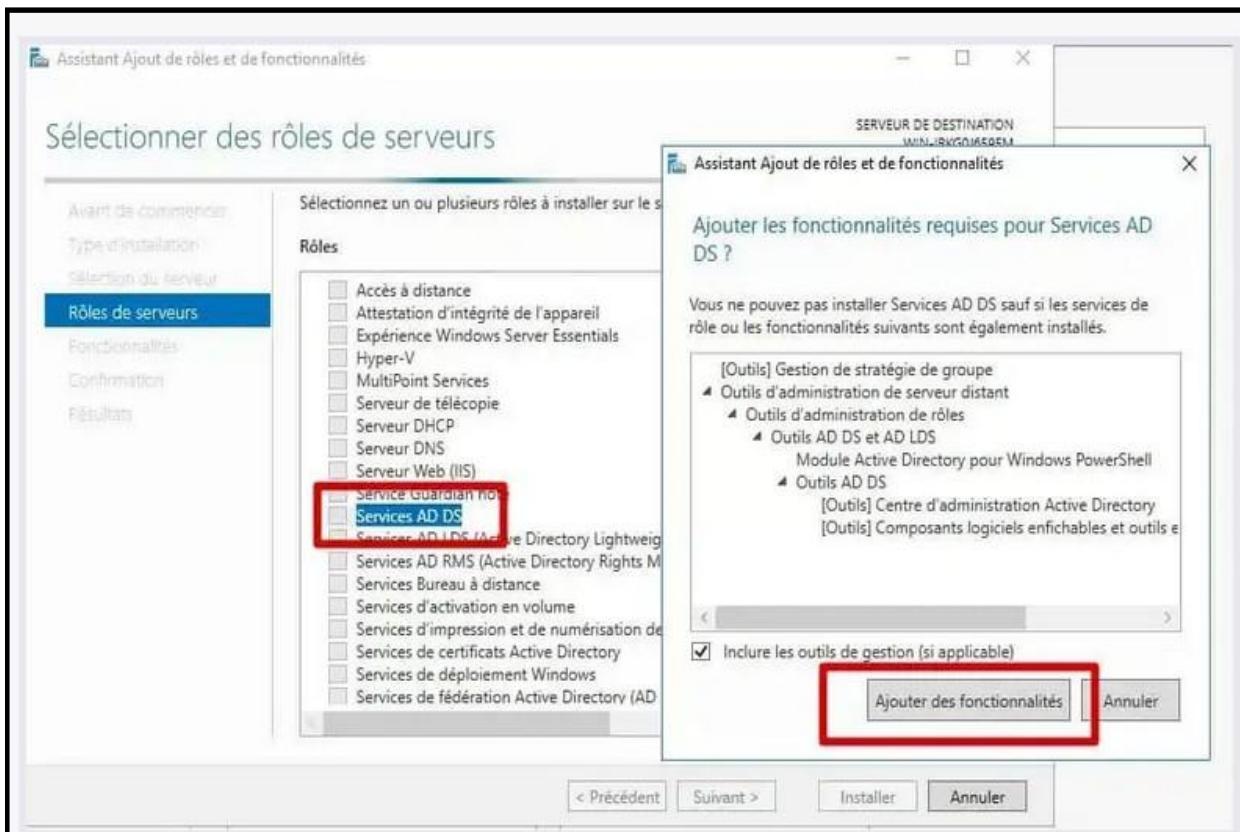
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Sélectionner votre serveur.



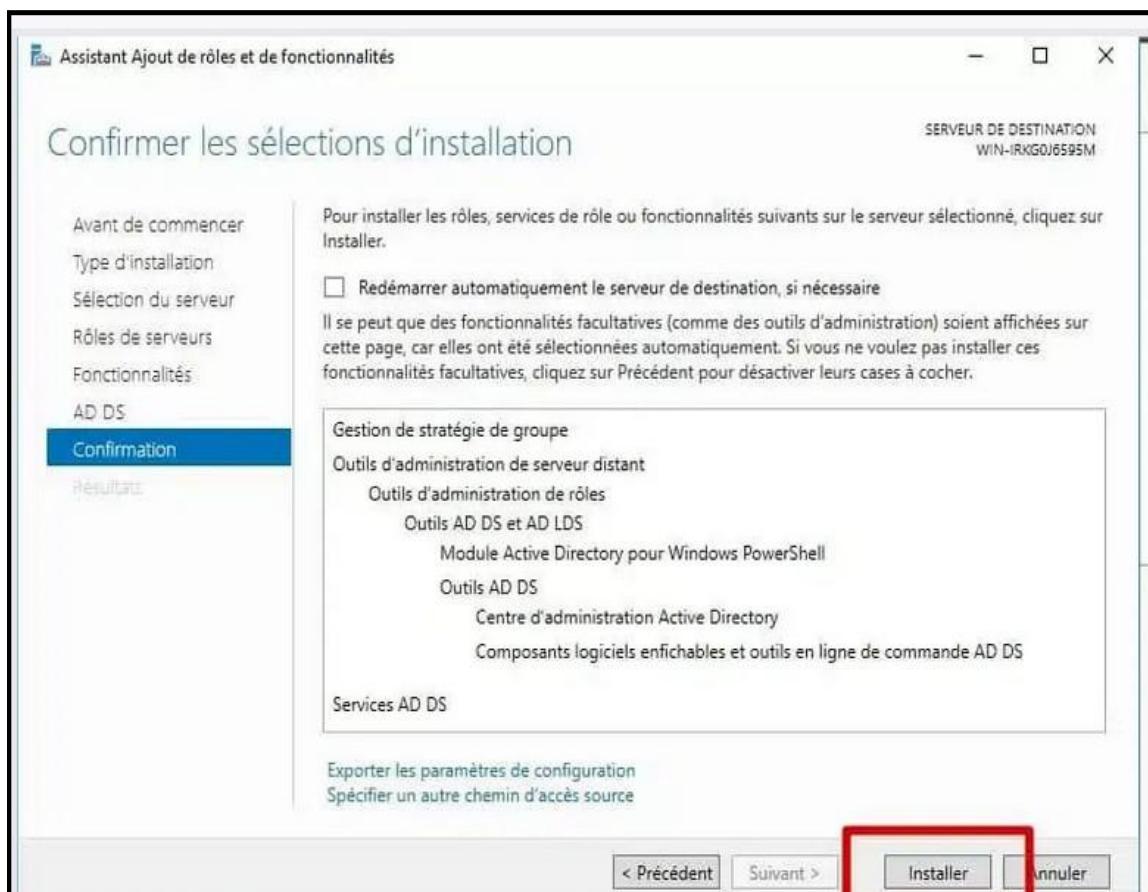
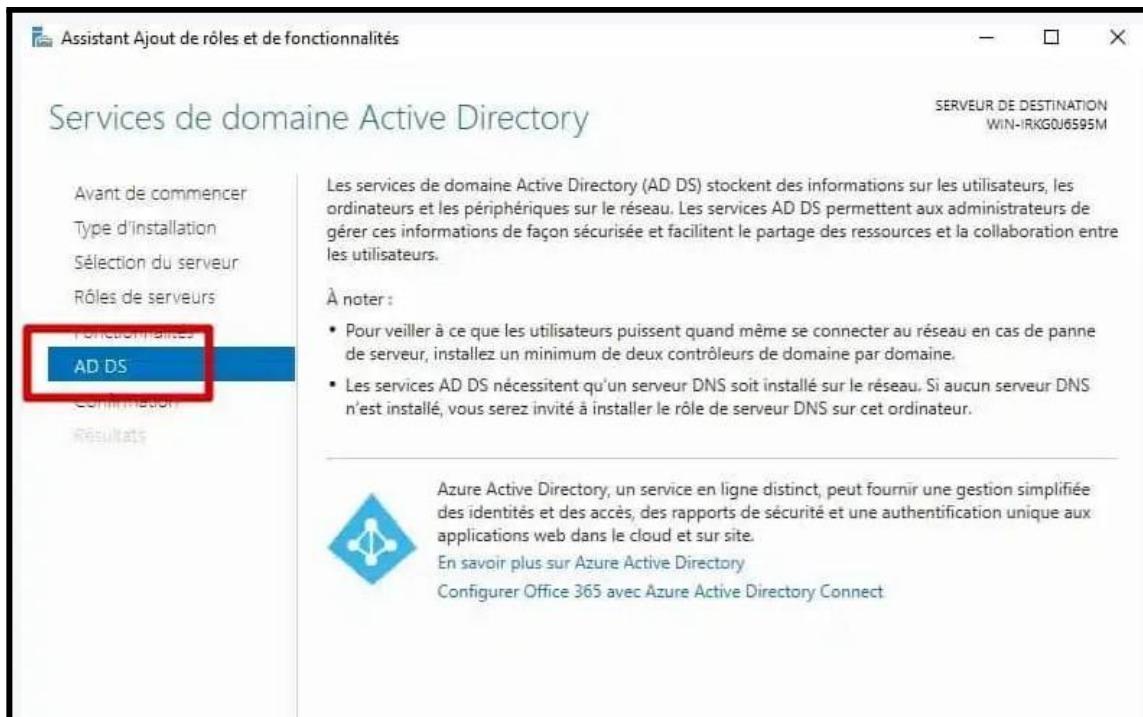
DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Cocher la case **Service AD DS** et faire “Ajouter des fonctionnalités”.



Faites à nouveau suivant , puis suivant pour démarrer l'installation des rôles puis installer.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

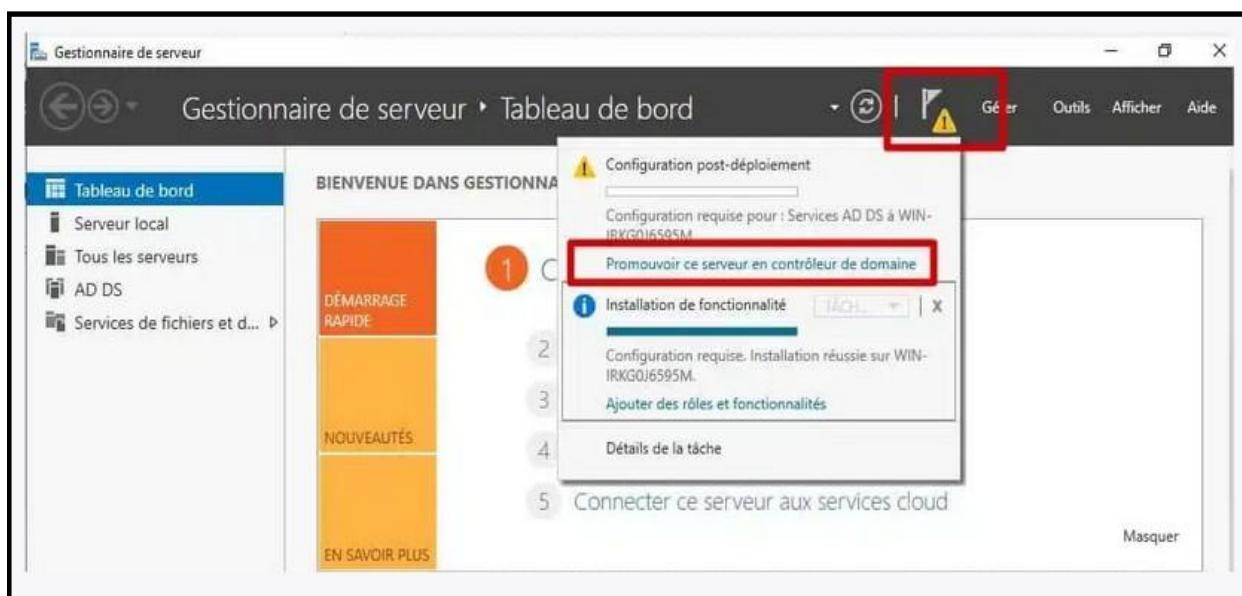


DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Le système installe les binaires, les fichiers de configuration et les outils. Ensuite nous allons exécuter l'assistant pour créer le domaine.

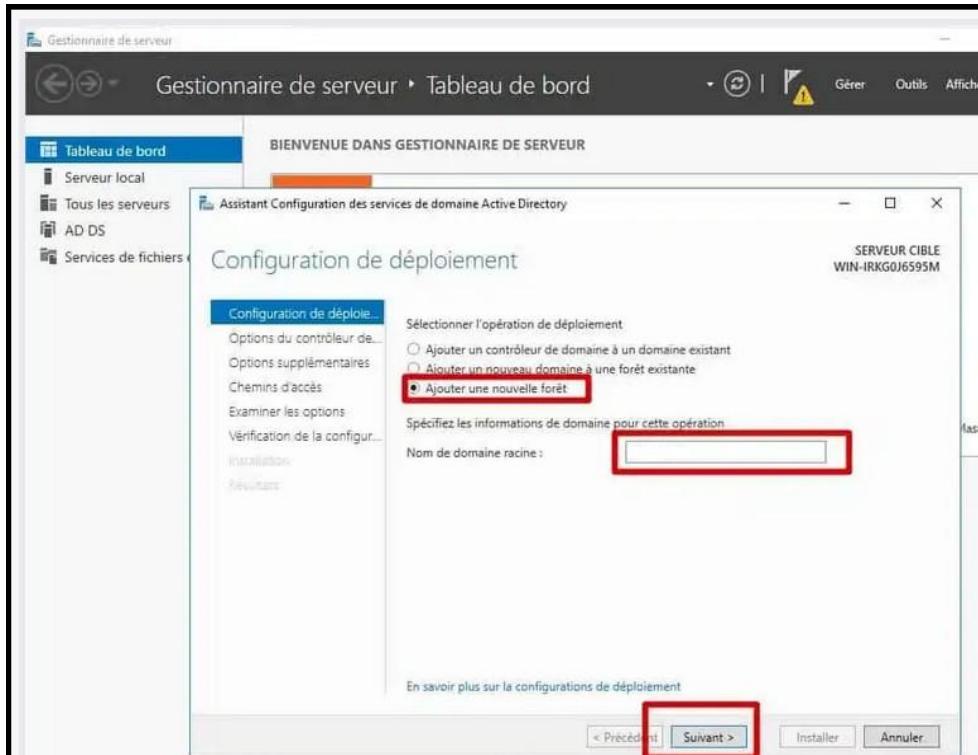
Une fois terminé, vous devriez voir un triangle jaune en haut du gestionnaire de serveur. C'est la méthode choisie par **Microsoft**, mais on aurait pu tout aussi bien passer par l'assistant.

Cliquez dessus pour finaliser la configuration, nous allons le promouvoir **contrôleur de domaine**.

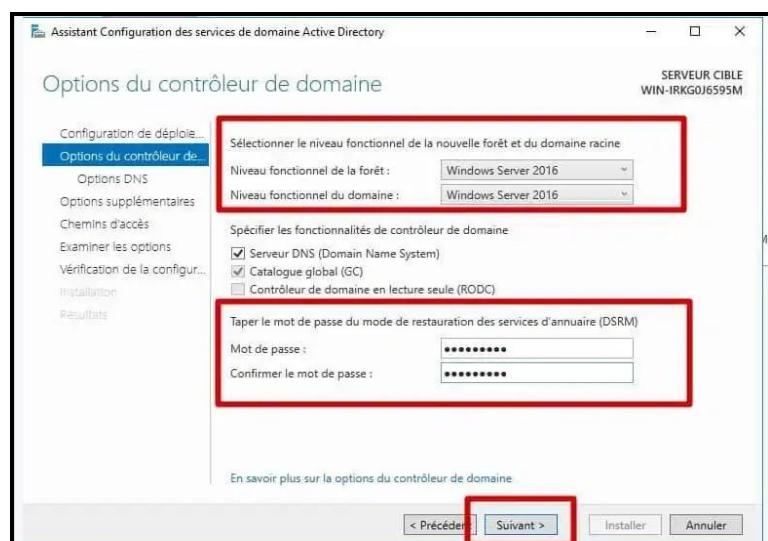


DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Saisir un nom pour votre domaine local. Dans notre exemple, il s'agit de [techunivers.local](#)

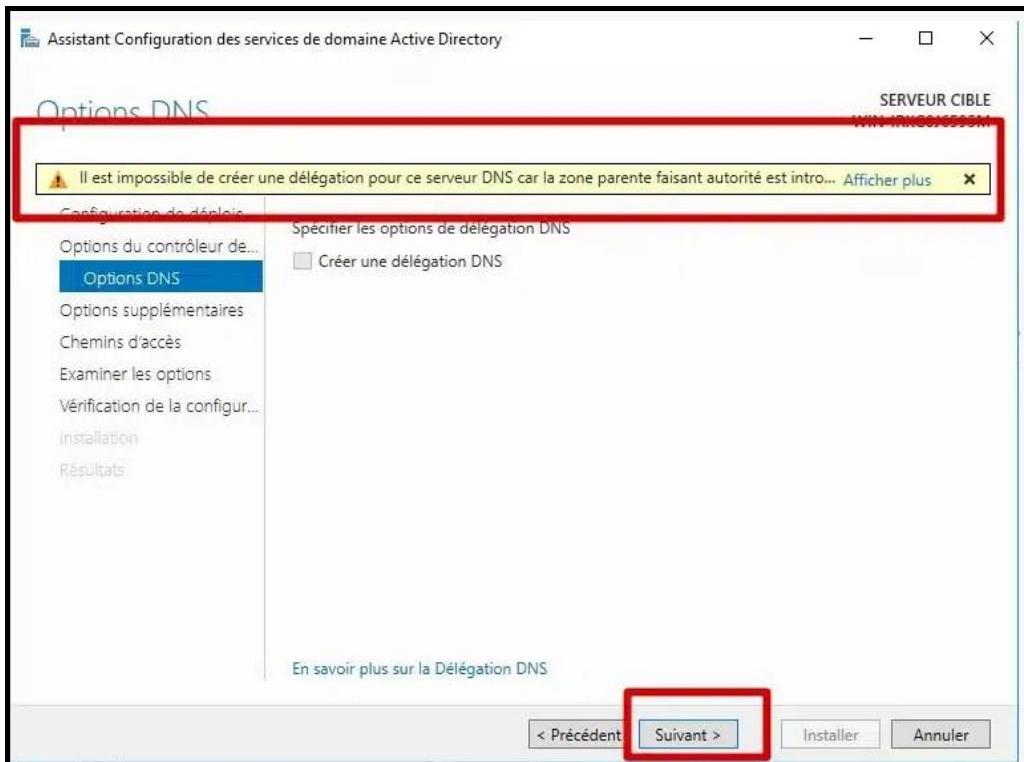


On choisit quelle version de **Windows Server** on autorise pour gérer le domaine au niveau de la forêt. Définir ensuite un mot de passe de restauration : il doit contenir des **chiffres**, des **lettres** et être de **plus de 8 caractères**.



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

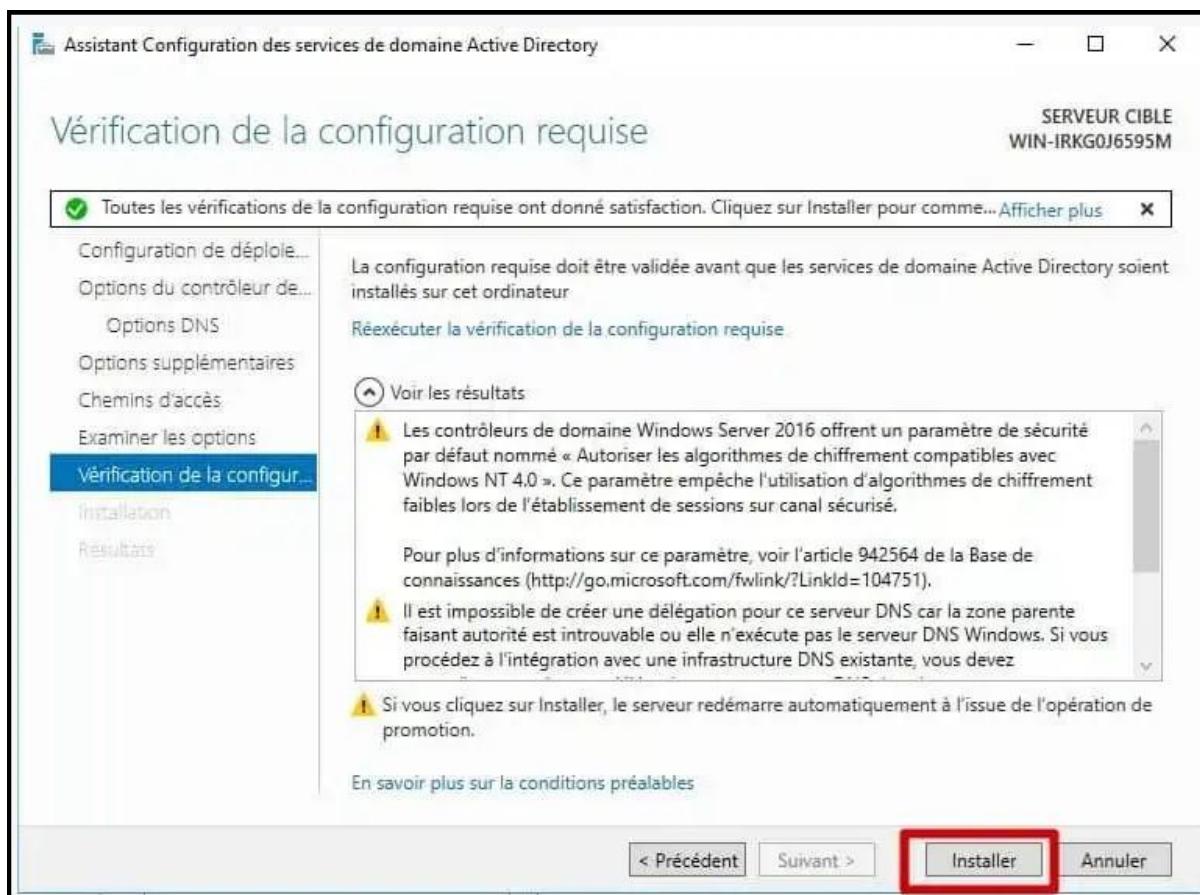
Laissez ensuite les options par défaut et ne tenez pas compte de l'avertissement sur la délégation **DNS**. Ce message est normal car l'assistant détecte que le nom de domaine choisi n'a aucun lien avec internet (**techuniverse.local**). Ce n'est pas un .com ou autre.



Ensuite laissez les options par défaut pour le **NetBIOS** (options supplémentaires) et les chemins d'accès.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

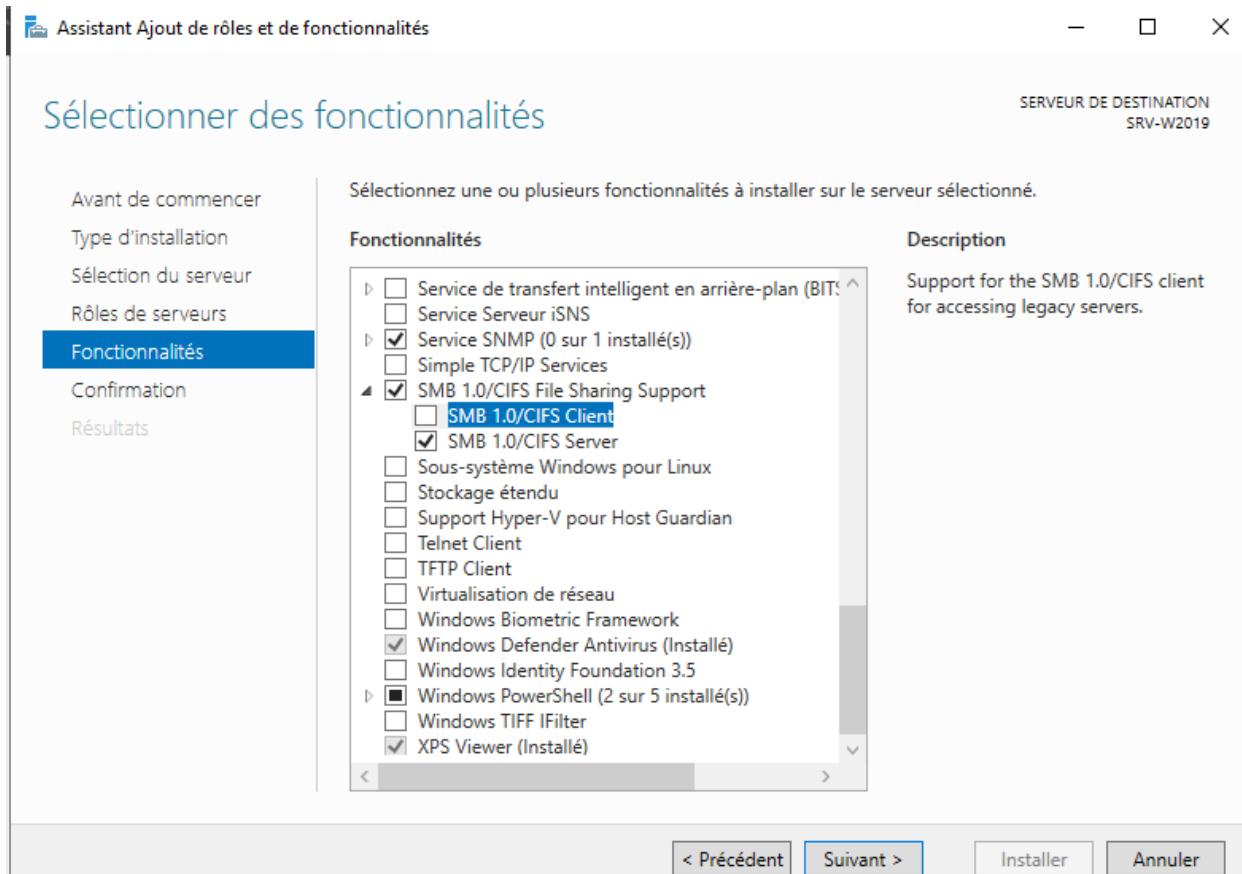
Enfin, une vérification de la configuration sera effectuée. Ignorer les différents avertissements.



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

8. Déploiement d'un partage de fichiers

Tout d'abord, Samba doit être installé sur le Windows Server. Dans notre cas, il faut **Samba Serveur** et non **Samba Client**.

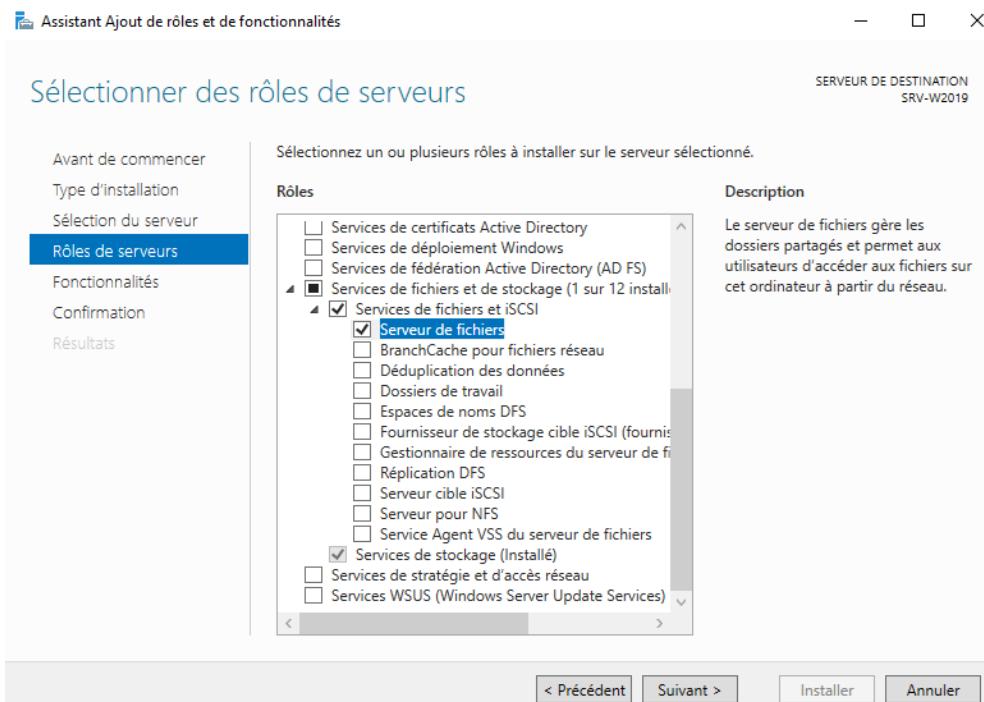


Le service samba sert à créer plusieurs partages de fichiers accessibles via le réseau, il est très flexible et fonctionne tout aussi bien sur Linux que sur Windows.

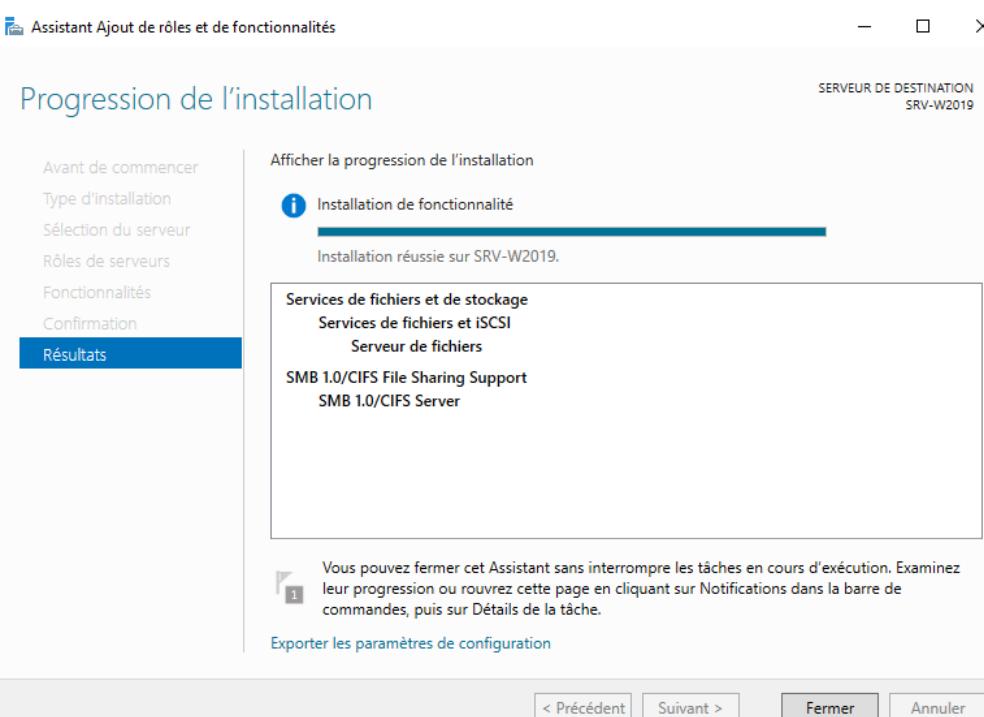
Ce service est normalement installé automatiquement sur Windows Serveur si le service Active Directory à été installé.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Il faut également installer le gestionnaire de partage de fichiers.

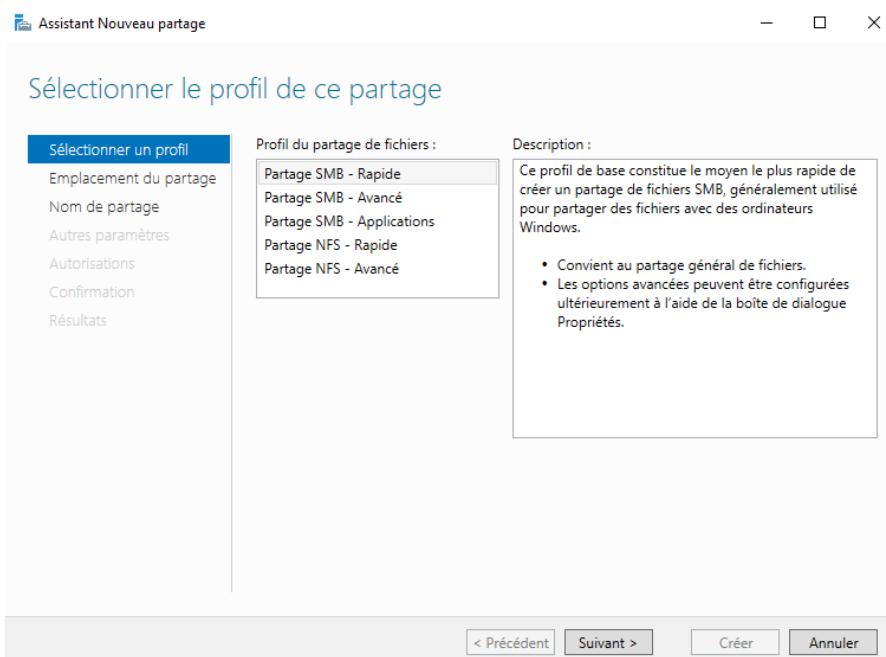


Puis il faut lancer l'installation.



DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Ensuite, vous pouvez lancer l'assistant de nouveau partage dans l'onglet partage dans l'assistant serveur.

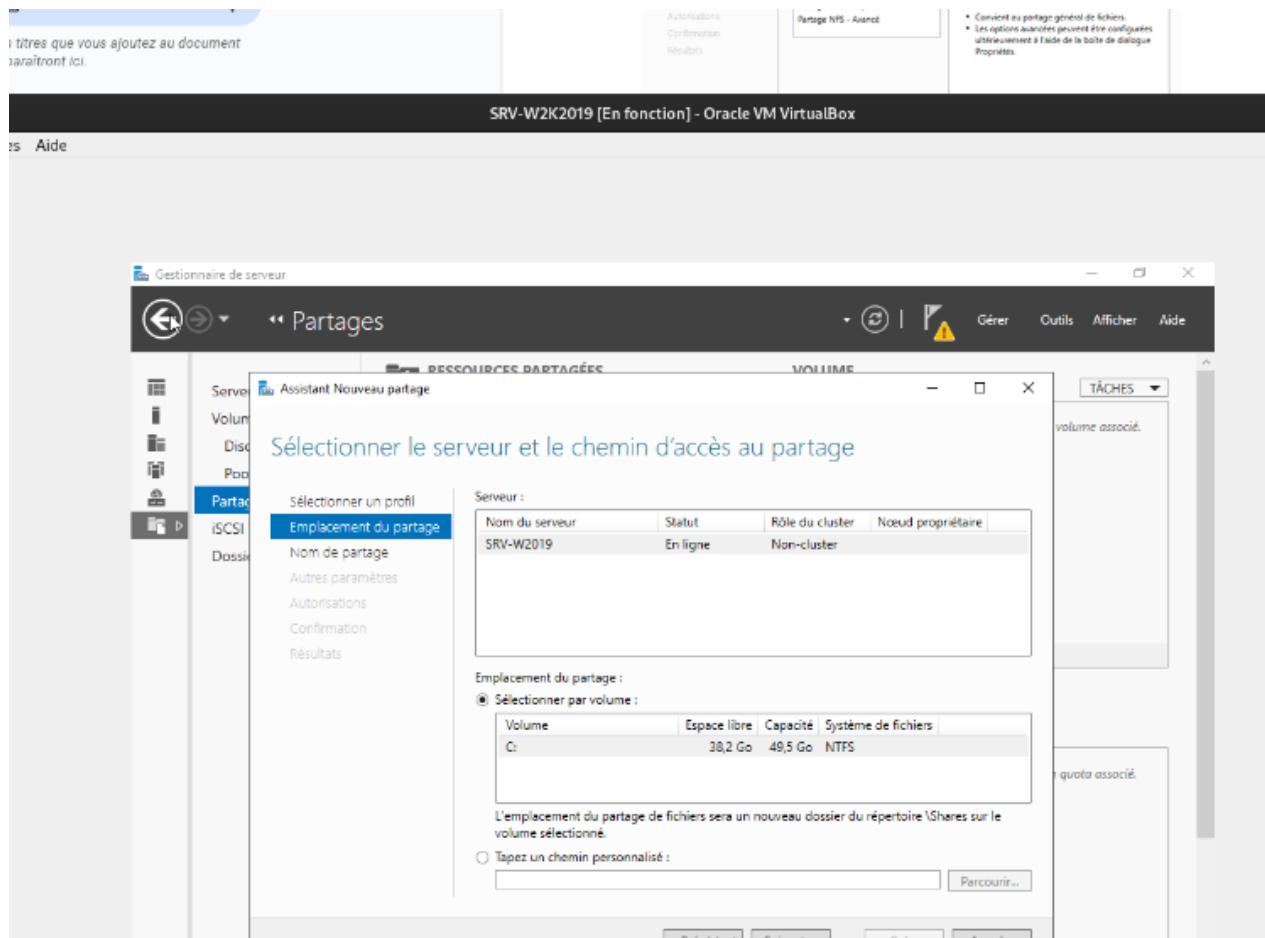


Vous pouvez sélectionner le partage rapide.

La prochaine étape sera d'entrer l'**emplacement du partage**, cela correspond au disque dur auquel vous voulez mettre votre partage.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

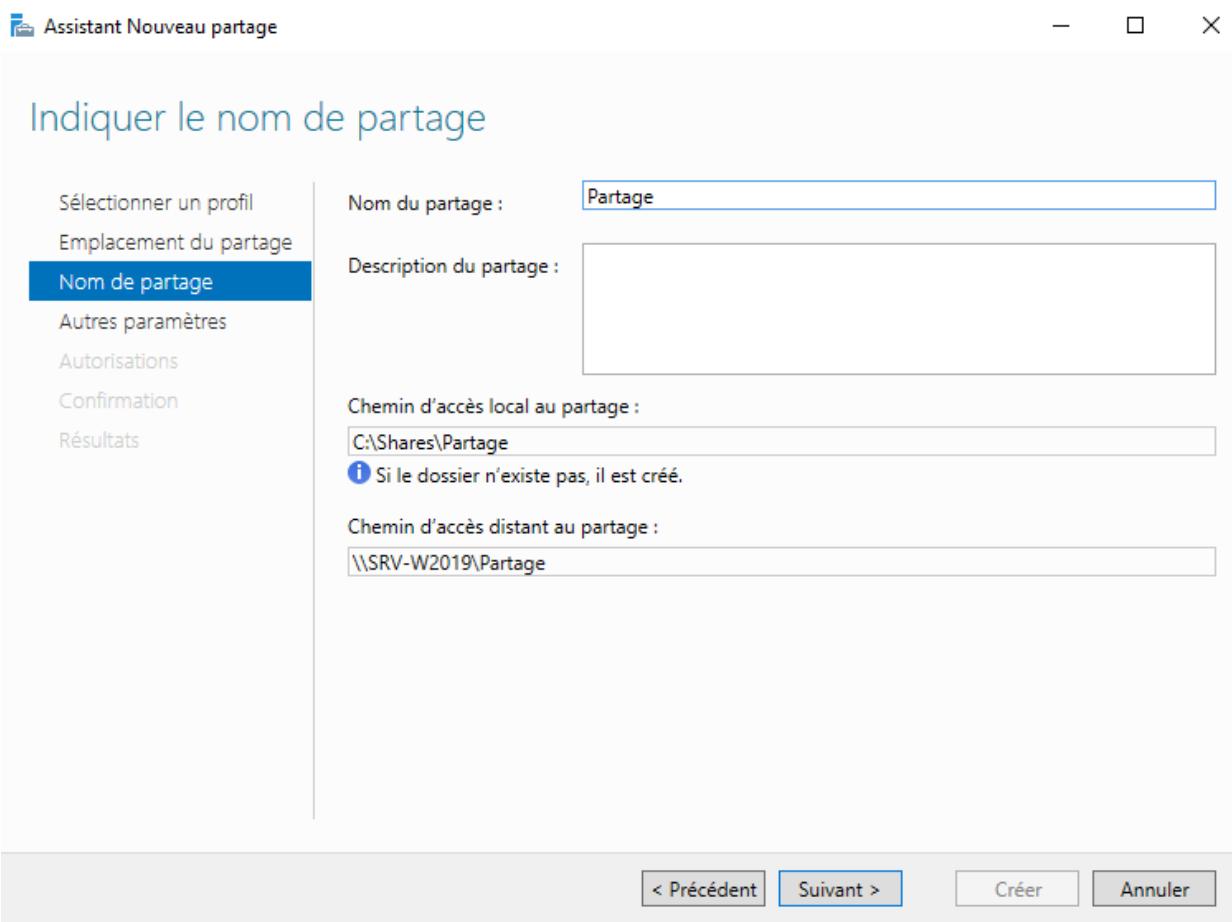
C'est donc ici que se déroule le **partage de fichier**.



Le partage de fichiers consiste à rendre un dossier accessible à plusieurs utilisateurs sur un réseau. Un ordinateur ou un serveur héberge les données et les met à disposition via un protocole comme **SMB** ou **NFS**. Nous pouvons définir les droits pour contrôler qui peut lire, modifier ou supprimer les fichiers. Les utilisateurs accèdent ensuite au dossier partagé comme s'il était local.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

La page suivante est donc destinée au nom du partage et aux dossiers de partage. Il est également possible d'utiliser un disque entier pour le partage, le chemin d'accès serait donc : "[<Lettre du disque>:\](#)"



Vous pouvez passer la page suivante, elle n'est pas nécessaire dans notre cas.

Maintenant, il ne manque plus que des autorisations à faire pour les accès au partage. Par défaut, tout le monde a accès au partage. Pour notre projet, nous avons limité l'accès à ce partage uniquement aux utilisateurs étant dans le groupe **VPN**.

Pour ce faire, il faut modifier les permissions du partage dans l'onglet "**Autorisations**".

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Spécifier les autorisations pour contrôler l'accès

Sélectionner un profil
Emplacement du partage
Nom de partage
Autres paramètres

Autorisations

Confirmation
Résultats

Les autorisations d'accès aux fichiers sur un partage sont définies par le biais d'une combinaison d'autorisations sur des dossiers, des partages et éventuellement une stratégie d'accès centrale.

Autorisations du partage : Contrôle total pour Tout le monde

Autorisations sur le dossier :

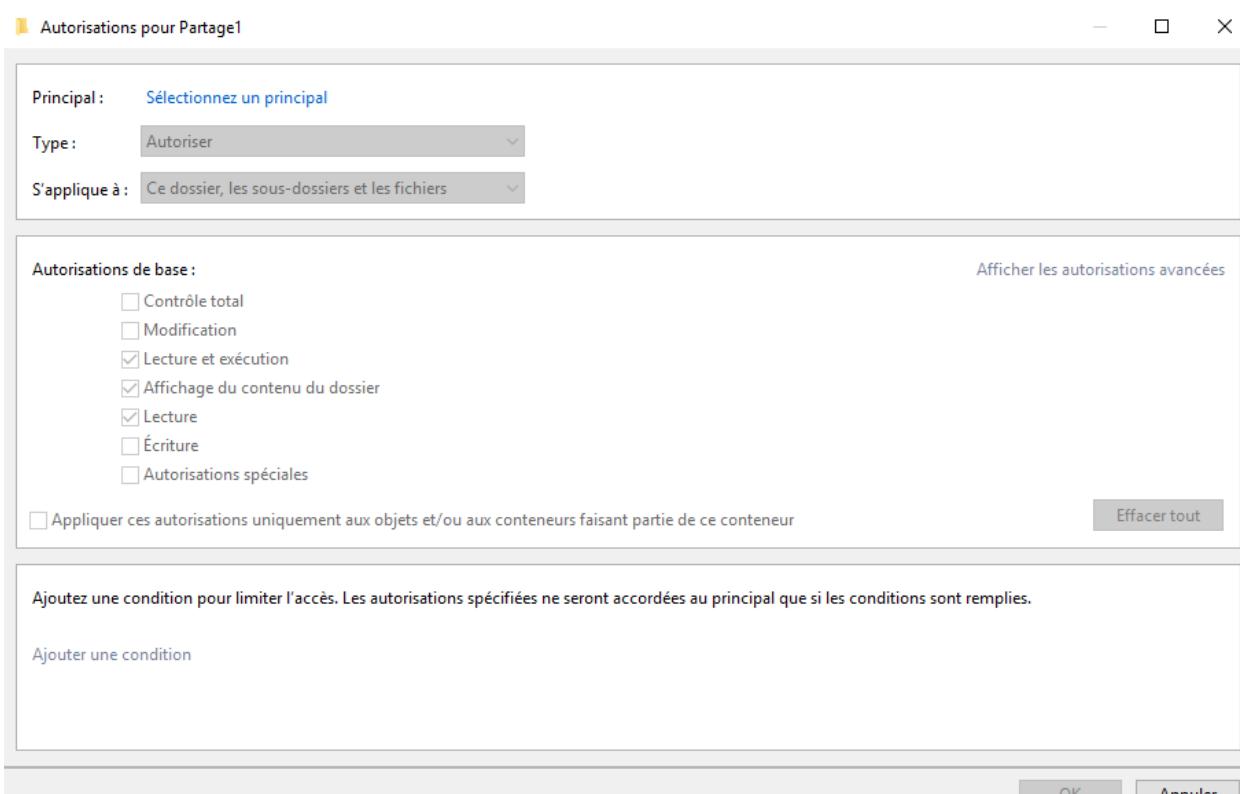
Type	Principal	Accès	S'applique à
Autoris...	CREATEUR PROPRIETAIR...	Contrôle total	Les sous-dossiers et les fichiers seul
Autoris...	BUILTIN\Utilisateurs	Spécial	Ce dossier et les sous-dossiers
Autoris...	BUILTIN\Utilisateurs	Lecture et exécution	Ce dossier, les sous-dossiers et les f
Autoris...	BUILTIN\Administrateurs	Contrôle total	Ce dossier, les sous-dossiers et les f
Autoris...	AUTORITE NT\Système	Contrôle total	Ce dossier, les sous-dossiers et les f

< >

[Personnaliser les autorisations...](#)

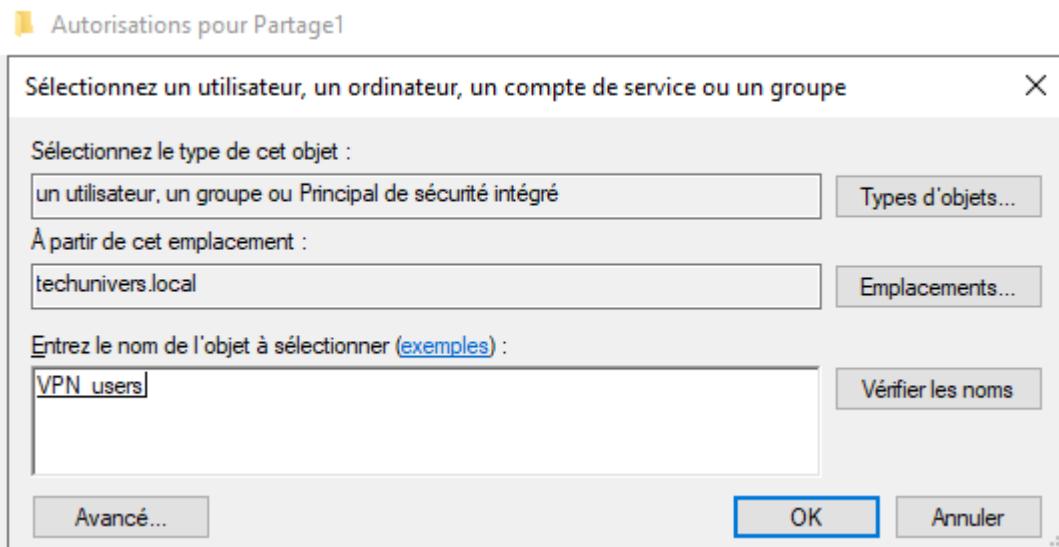
Sur l'image au-dessus, ce sont les permissions configurées par défaut.
Pour limiter l'accès au partage, il est nécessaire de supprimer les autorisations en lien avec les utilisateurs simples.

Ensuite, il est possible de mettre le groupe **VPN** en propriétaire du dossier de partage.
Dans la fenêtre ci-dessous.

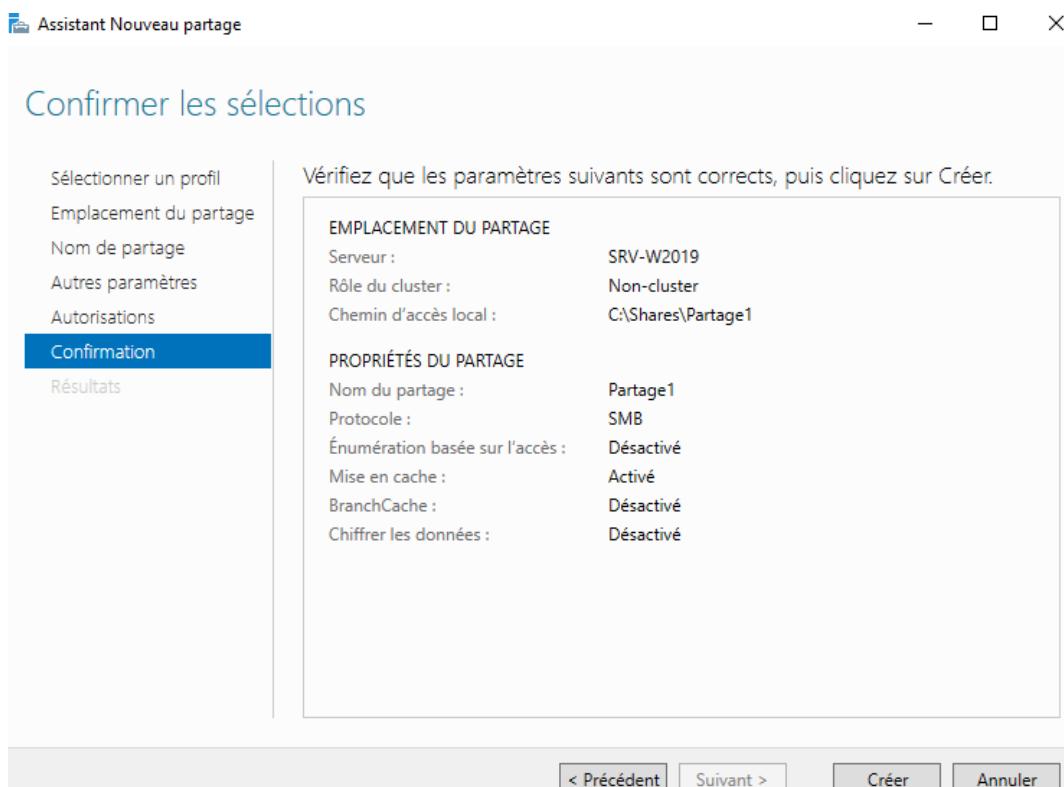


DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Pour rechercher le groupe est le définir, il faut cliquer sur “**Sélectionnez un principal**”, puis rechercher le groupe souhaité.



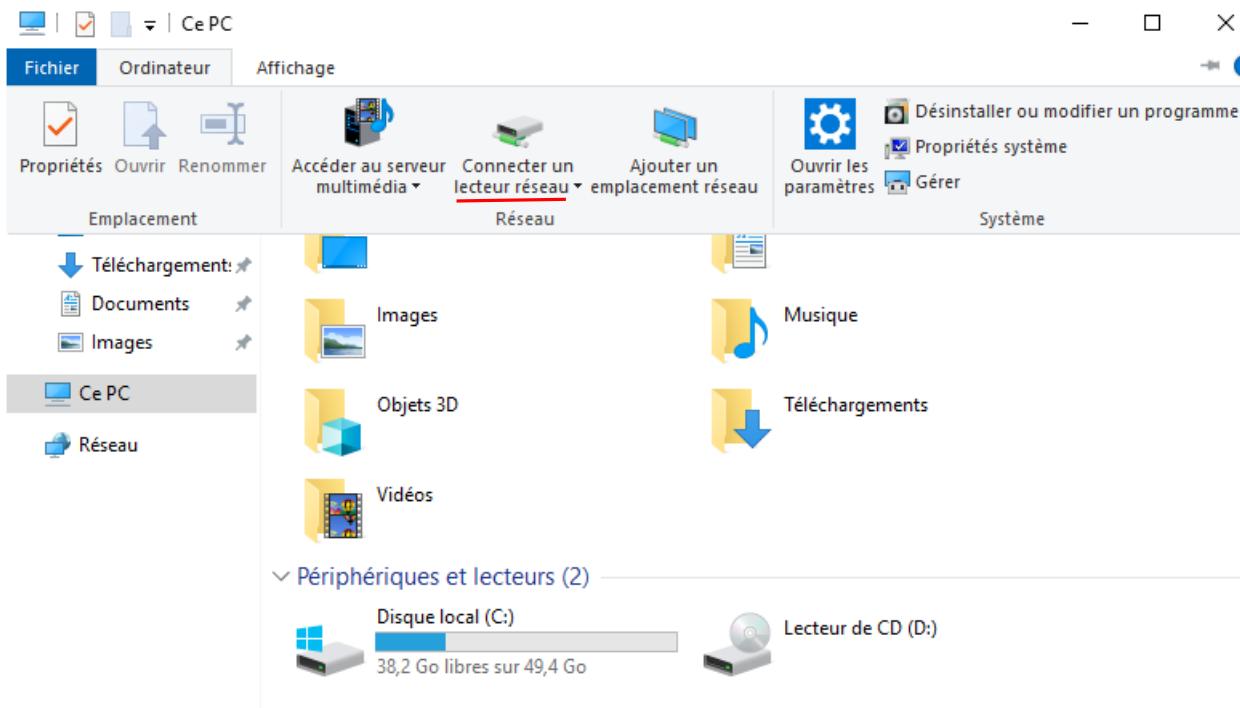
Une fois que c'est fait, il est possible de valider et le groupe sera propriétaire.



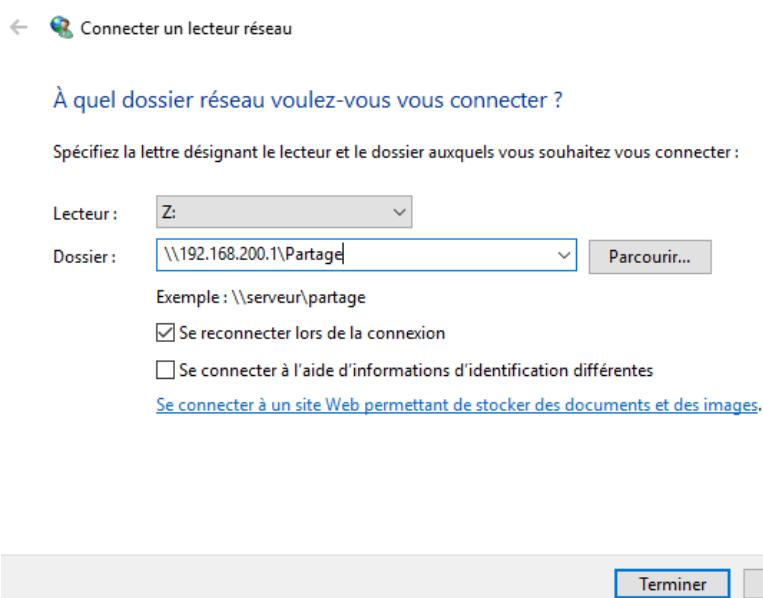
Voilà à quoi devrait ressembler le partage de fichiers.

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Pour ce connecter au partage, sur le client, une option “**Connecter un lecteur réseau**” est disponible et sert à connecter des partages de fichiers sur le PC.



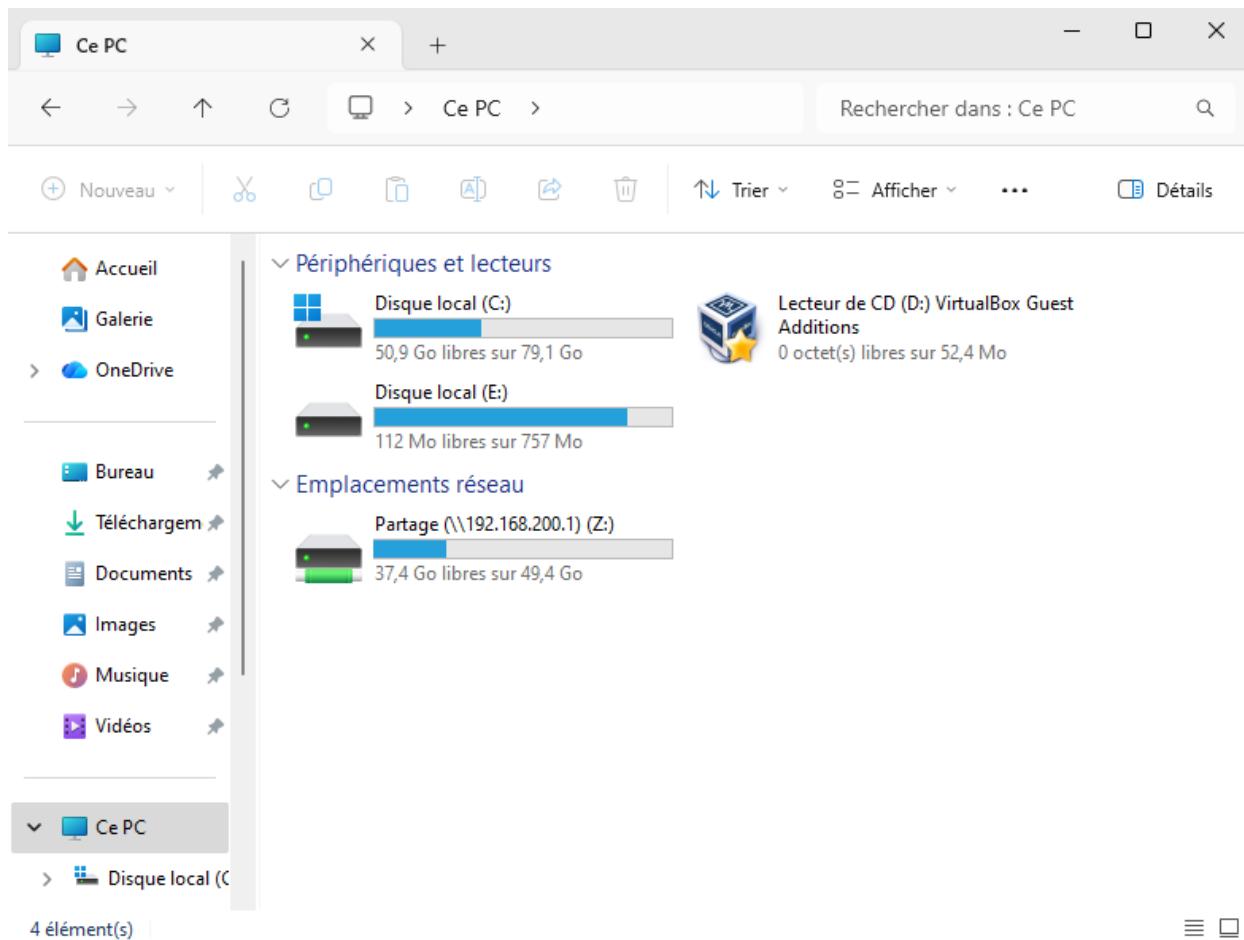
Une fois dans “**Connecter un lecteur réseau**”, le dossier correspond au chemin configuré dans le partage, en adaptant l’adresse IP contre le disque de partage du serveur.



Le dossier correspond donc à “\\<IP/Nom de votre serveur>\<Nom du partage>”

DOCUMENTATION CONFIGURER UN RÉSEAU D'ENTREPRISE

Une autre page va s'afficher pour demander les identifiants, il ne faut plus qu'à rentrer un identifiant étant dans le groupe VPN et le partage devrait s'afficher et fonctionner.



Le partage de fichiers devrait s'afficher dans la rubrique "[Ce PC](#)", dans "[Emplacement réseau](#)".