

---

## Création d'une infrastructure supervisée avec intégration Linux

---



## 1) MISE EN ŒUVRE DU PROJET

- 1.1) Schéma d'architecture réseau
- 1.2) Plan d'adressage

## 2) DOCUMENTATION TECHNIQUE

- 2.1) Configuration pare-feu avec pfSense ( primaire et secondaire)
- 2.2) Configuration d'un CARP

Active Directory – Service d'annuaire

- 2.3) Déploiement de l'Active Directory sur deux contrôleurs de domaine (SRV-AD-01 & SRV-AD-02)

DHCP – Dynamic Host Configuration Protocol

- 2.4) Installation et configuration du service DHCP avec basculement sur les serveurs SRV-AD-01 et SRV-AD-02

- 2.5) Test du fonctionnement DHCP sur un poste client
- 2.6) Ajout des clients Windows au domaine supformation.lan

Serveur WSUS

- 2.7) Installation et configuration du service WSUS

GPO – Gestion des stratégies de groupe

- 2.8) Mise en place de GPO de sécurité et de gestion des utilisateurs
- 2.9) Déploiement de GPO pour l'environnement de travail

Configuration des serveurs Linux

Samba (serveur de fichiers)

- 3.0) Intégration d'un serveur Samba au domaine et mise en place de partages réseau accessibles depuis Windows

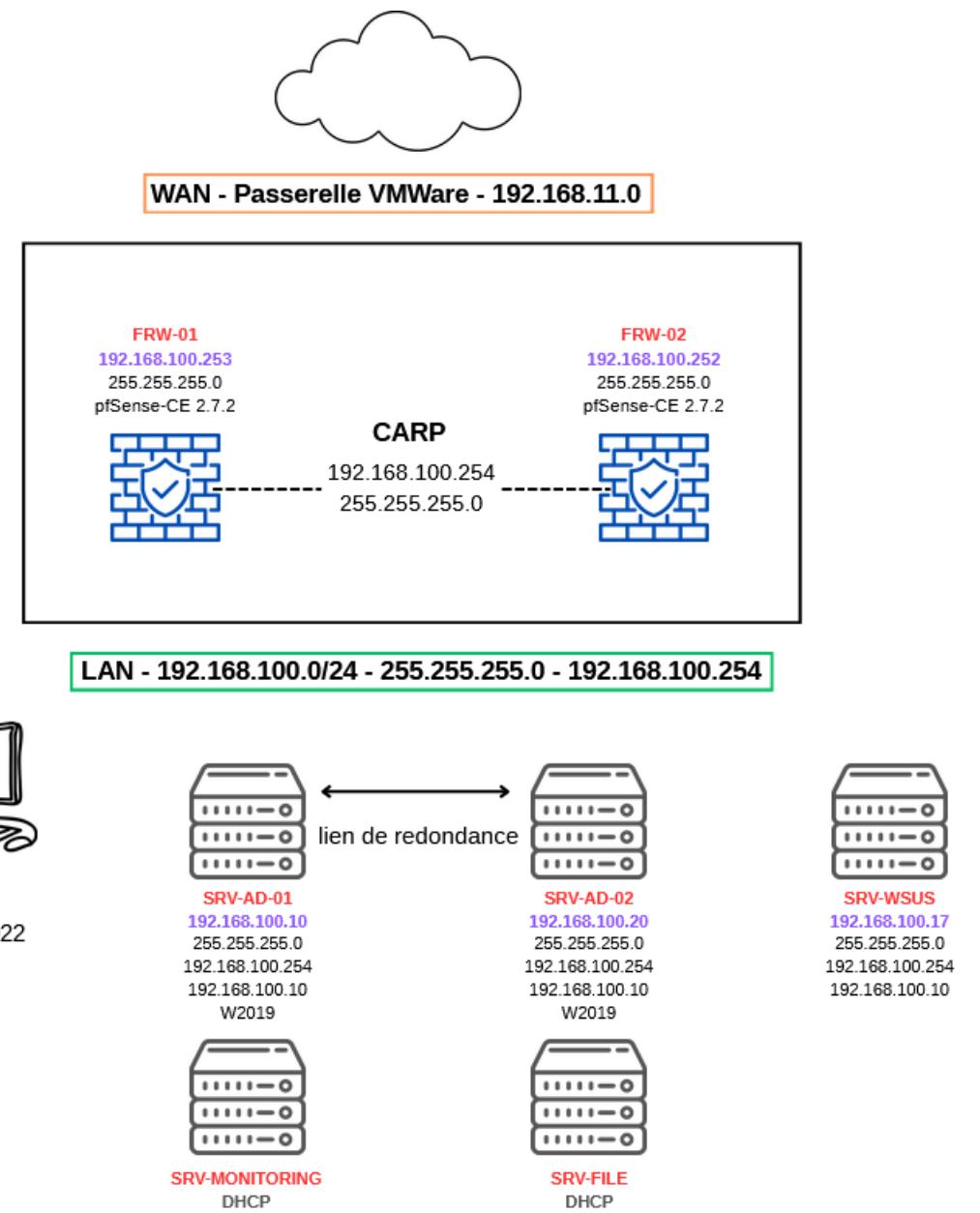
Serveur de monitoring

Zabbix – Solution de supervision et de monitoring

- 3.1) Installation de Zabbix et déploiement des agents sur les machines Windows et Ubuntu
- 3.2) Configuration des agents dans la console d'administration Zabbix

## 1) MISE EN ŒUVRE DU PROJET

### 1.1) Schéma d'architecture réseau



## 1.2) Plan d'adressage

NAME	ADRESSE IP	MASK	PASSERELLE	OS	ROLES	APPS/SOFTS
SRV-AD-01	192.168.100.10	255.255.255.0	192.168.100.254	WS2019	AD DS/DNS/DHCP	Zabbix Agents
SRV-AD-02	192.168.100.20	255.255.255.0	192.168.100.254	WS2019	AD DS/DNS/DHCP	Zabbix Agents
SRV-WSUS	192.168.100.17	255.255.255.0	192.168.100.254	WS2019	WSUS	Zabbix Agents
FRW-01	192.168.100.253	255.255.255.0		pfSense-CE-2.7.2	PARE-FEU	Zabbix Agents
FRW-02	192.168.100.252	255.255.255.0		pfSense-CE-2.7.2	PARE-FEU	Zabbix Agents
SRV-MONITORING	DHCP	DHCP	DHCP	Ubuntu 22.04	MONITORING	Zabbix
SRV-FILE	DHCP	DHCP	DHCP	Ubuntu 22.04	SRV FICHIERS	Zabbix Agents
PC01	DHCP	DHCP	DHCP	Ubuntu 22.04	CLIENT	GPO

## 2) DOCUMENTATION TECHNIQUE

### 2.1) Configuration pare-feu avec pfSense ( primaire et secondaire)

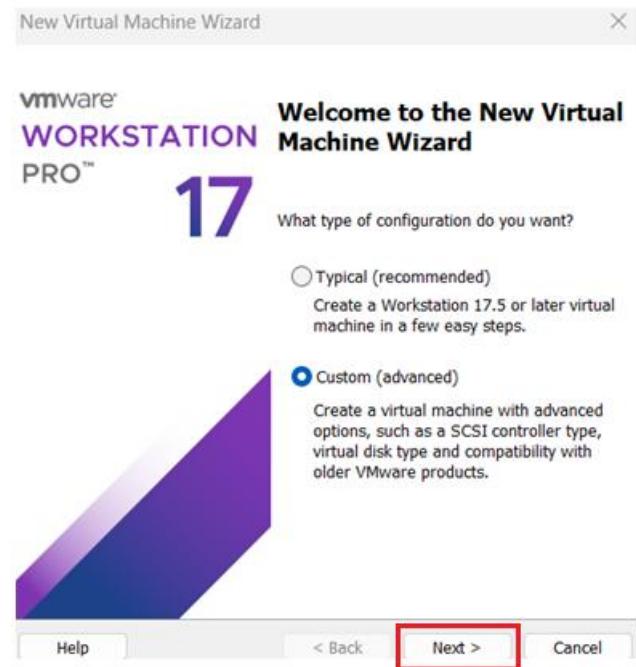
Prérequis de création des machines virtuelles :

2 machines virtuelles (VM)

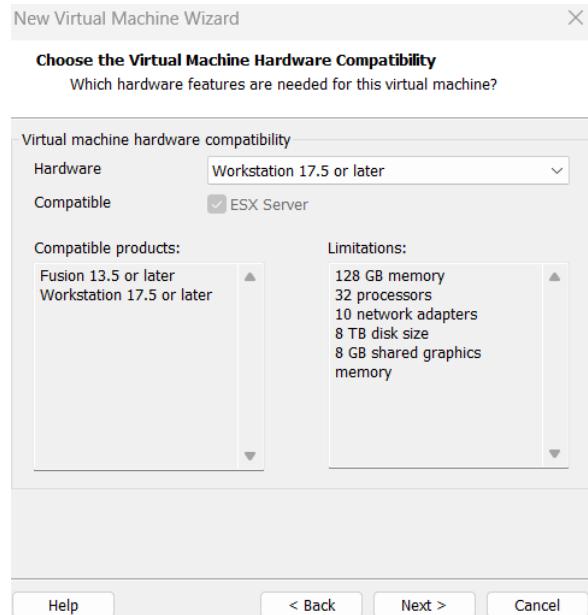
- Configuration :
  - 256 Mo de RAM
  - 1 processeur
  - 1 disque dur de 20 Go
  - 2 cartes réseau (1 en NAT, 1 en réseau interne (LAN))

Système d'exploitation : *pfSense Community Edition 2.7.2*

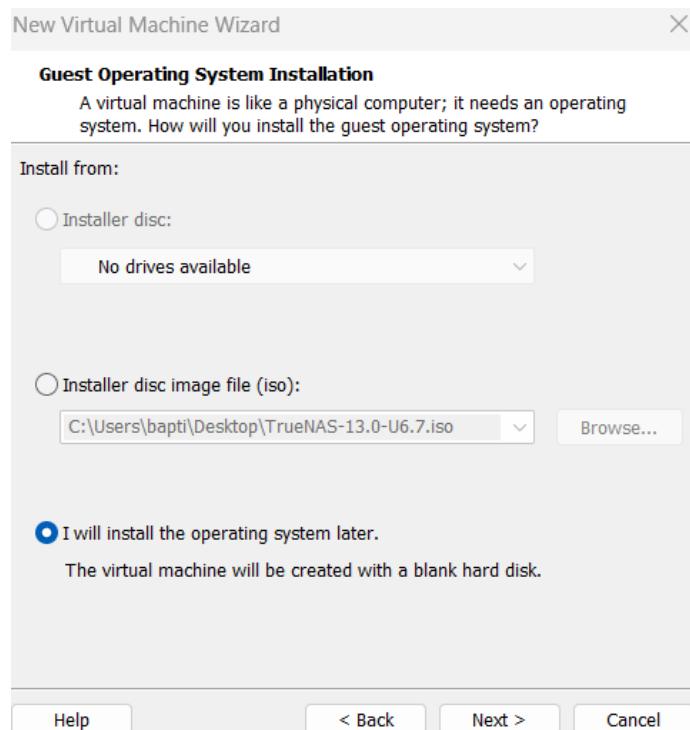
Sélection du mode de configuration avancé pour créer une machine virtuelle personnalisée.



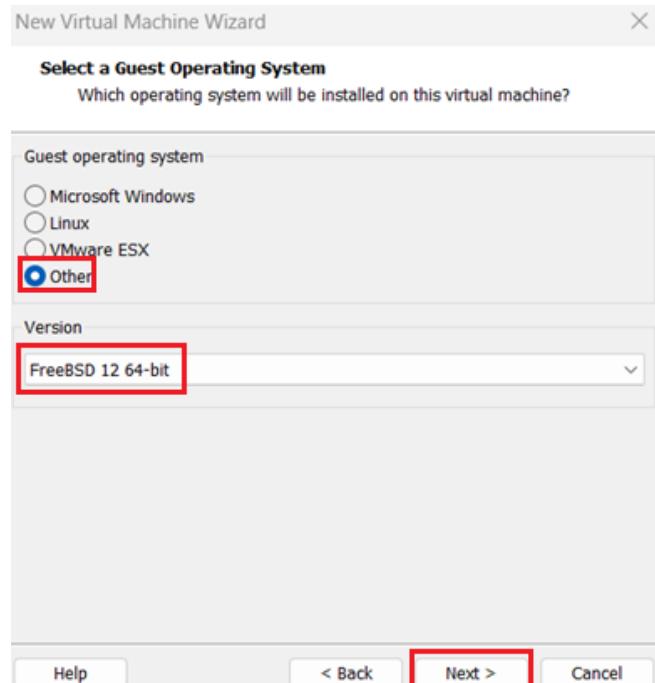
Choix de la compatibilité matérielle avec Workstation 17.5 ou version ultérieure.



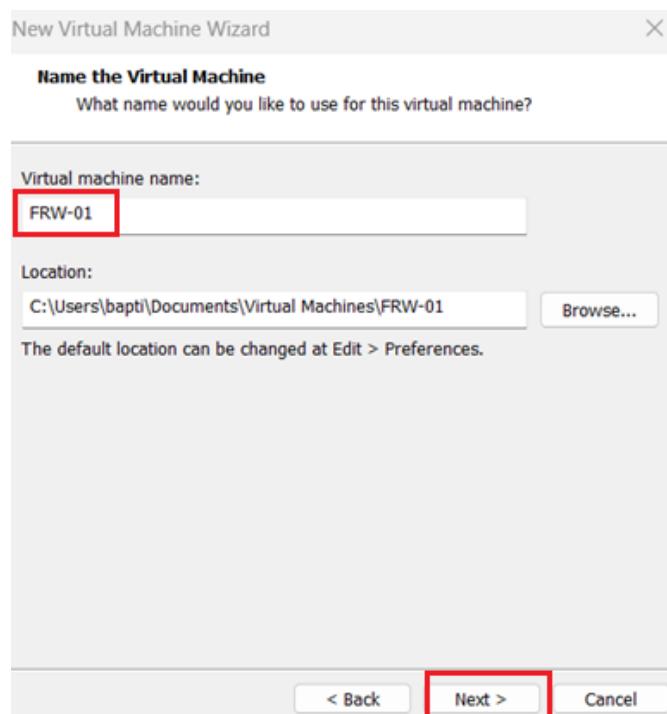
Sélection de l'option pour installer le système d'exploitation ultérieurement.



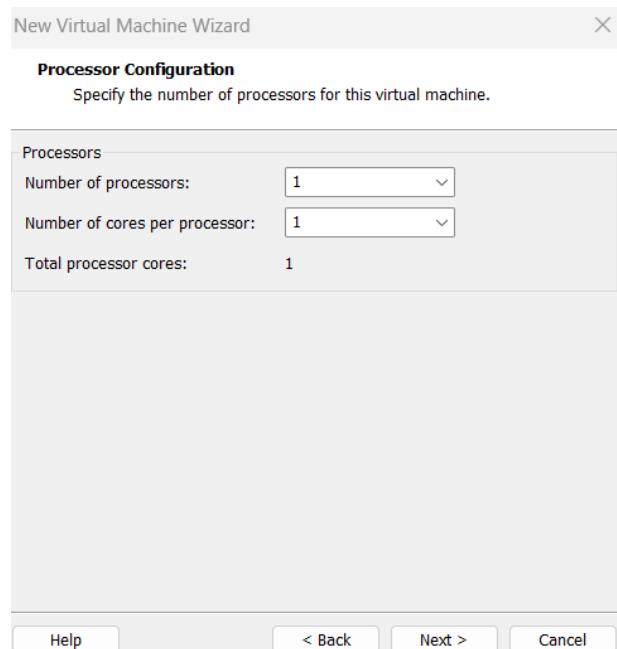
Choix du système invité en tant que FreeBSD 12 64-bit, adapté à pfSense.



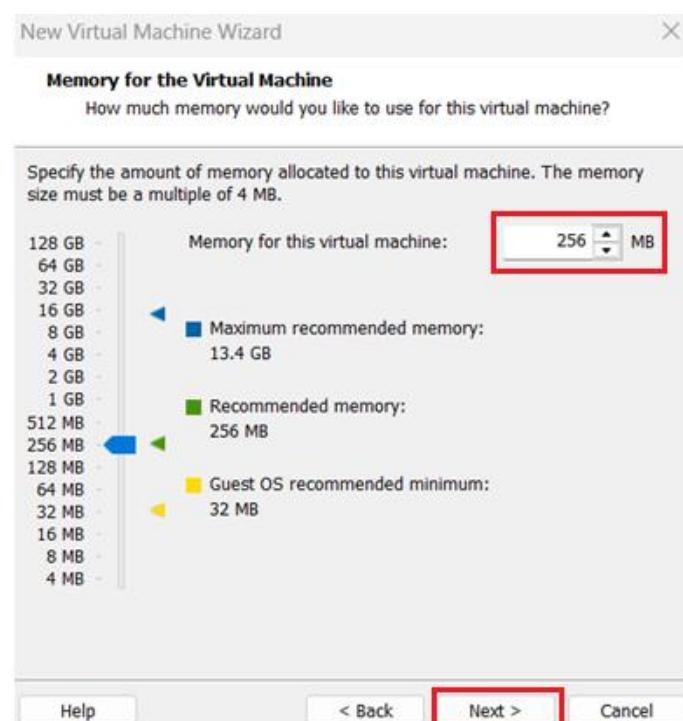
Nom de la machine virtuelle défini sur FRW-01, correspondant au premier pare-feu pfSense.



Configuration du processeur : 1 processeur avec 1 cœur alloué à la machine virtuelle.



Attribution de 256 Mo de RAM à la machine virtuelle, conforme à la recommandation minimale du système invité.



Choix du type de connexion réseau, à adapter selon l'architecture prévue.

New Virtual Machine Wizard X

**Network Type**  
What type of network do you want to add?

Network connection

Use bridged networking  
Give the guest operating system direct access to an external Ethernet network. The guest must have its own IP address on the external network.

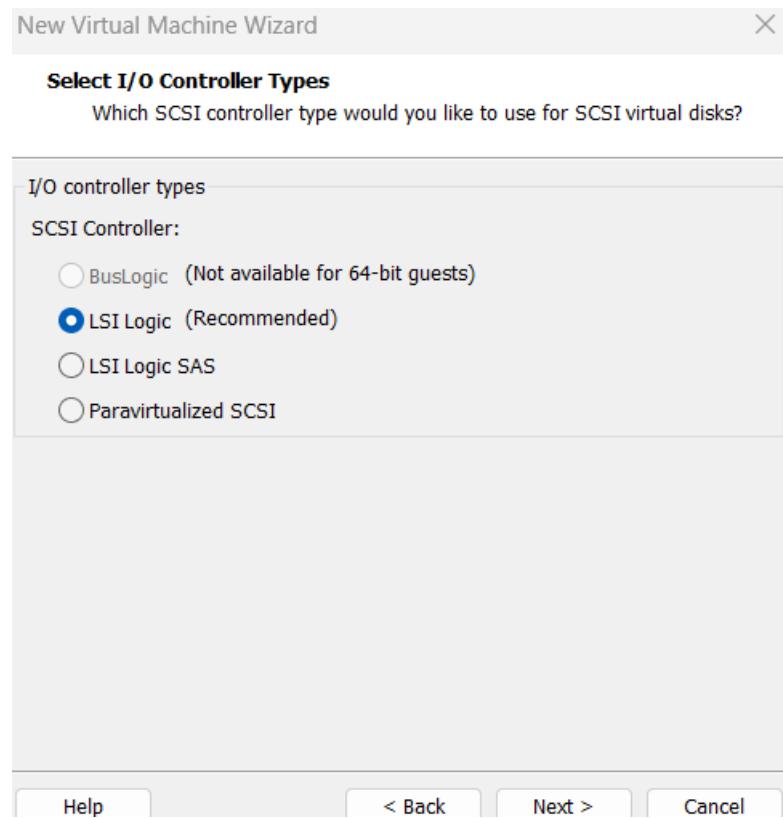
Use network address translation (NAT)  
Give the guest operating system access to the host computer's dial-up or external Ethernet network connection using the host's IP address.

Use host-only networking  
Connect the guest operating system to a private virtual network on the host computer.

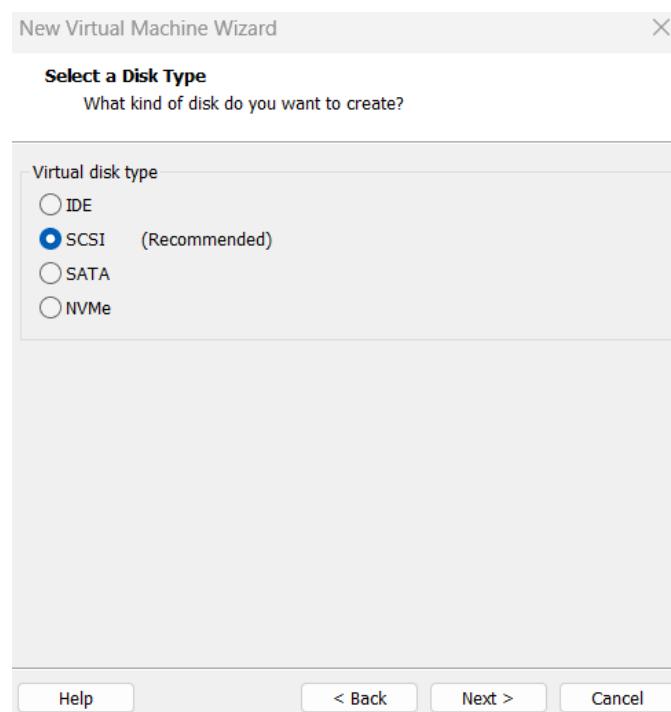
Do not use a network connection

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

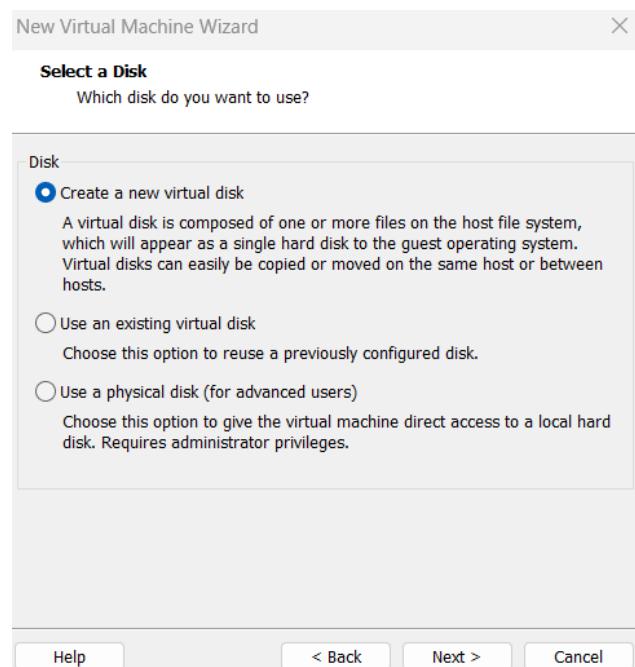
Sélection du contrôleur SCSI recommandé pour assurer la compatibilité avec l'OS 64 bits.



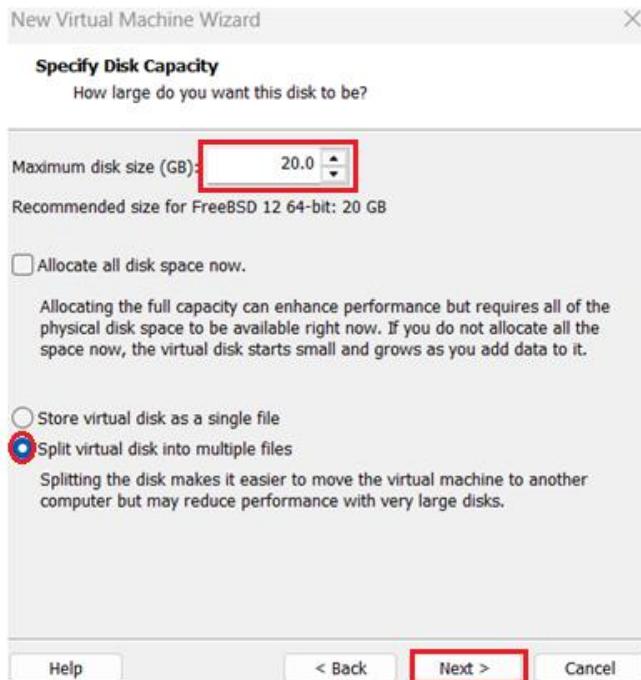
Choix du type de disque virtuel : SCSI, recommandé pour ses performances et sa compatibilité.



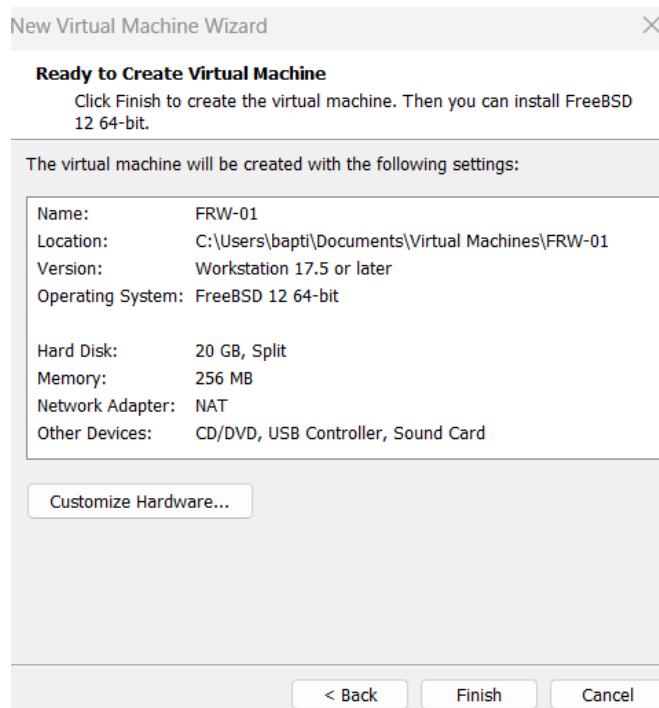
Création d'un nouveau disque virtuel.



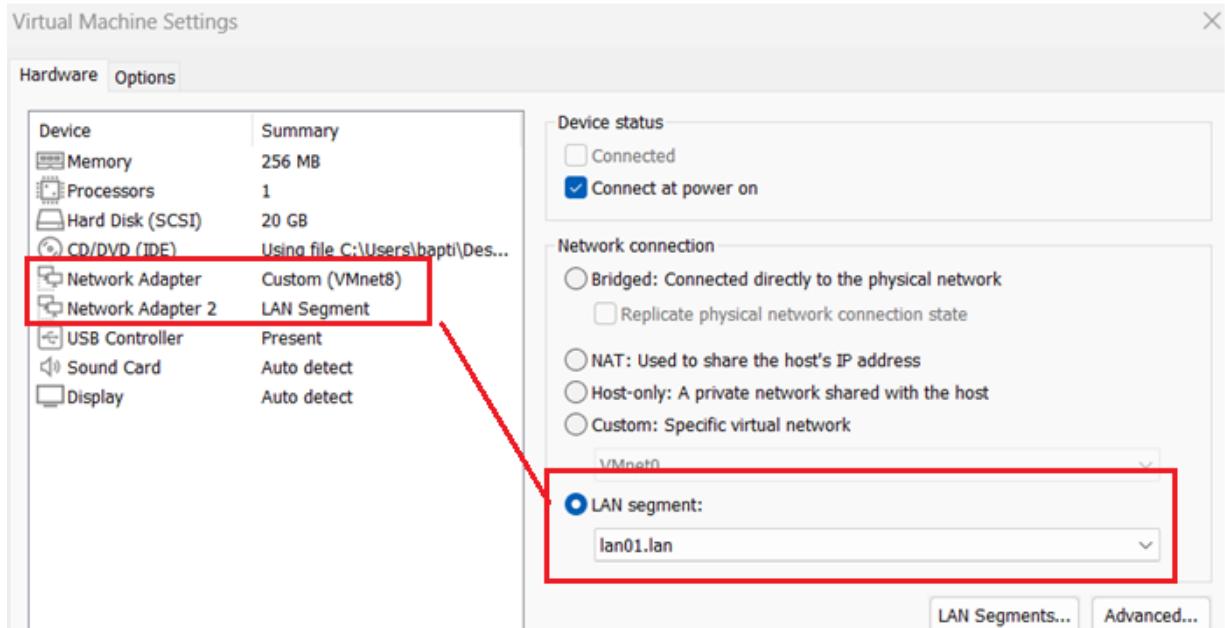
Définition de la taille du disque virtuel à 20 Go, en le scindant en plusieurs fichiers.



Récapitulatif de la configuration avant la création de la VM : tout est prêt, **Finish**.



## Configuration FRW-01 et FRW-02

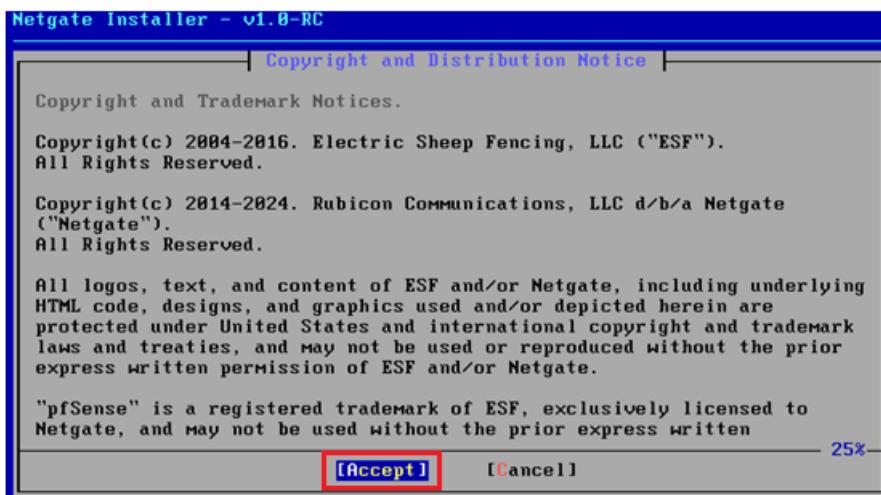


On démarre les deux pare-feux pfSense pour procéder à leur installation

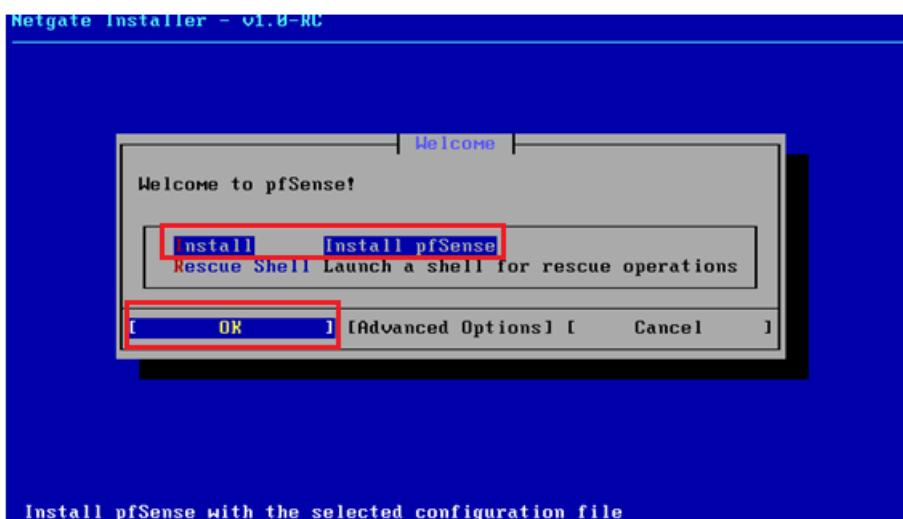
[Installation du système FreeBSD pour pfSense](#)



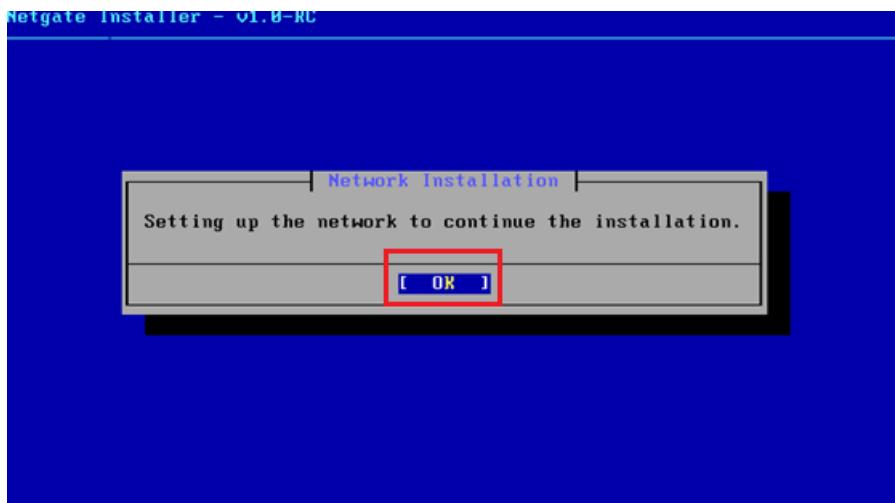
À l'écran des conditions d'utilisation, appuyez sur la touche [ENTRÉE] pour accepter et poursuivre l'installation.



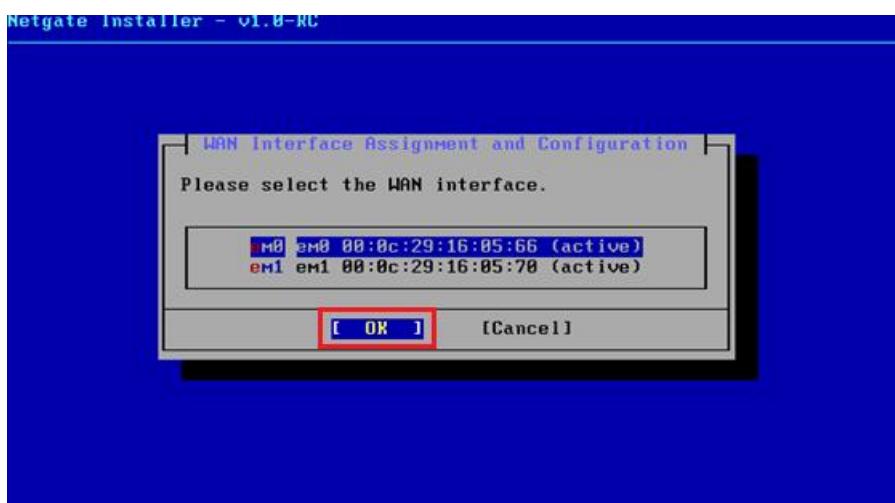
Sélectionnez « Install » à l'aide des flèches directionnelles, puis appuyez sur la touche [ENTRÉE].



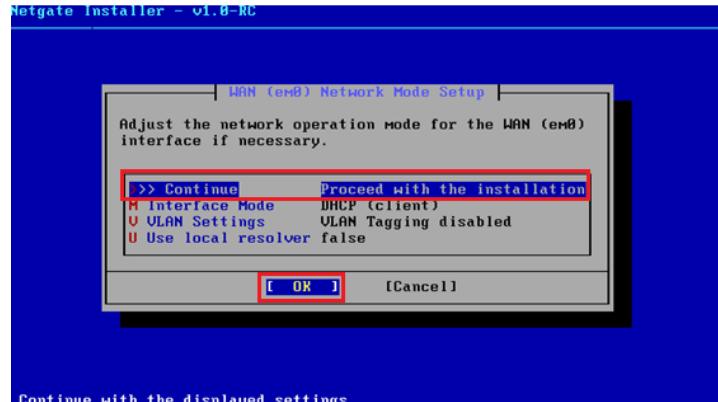
À cette étape, appuyer sur la touche [ENTRÉE] pour permettre à pfSense de configurer automatiquement la connexion réseau et accéder à Internet afin de poursuivre l'installation.



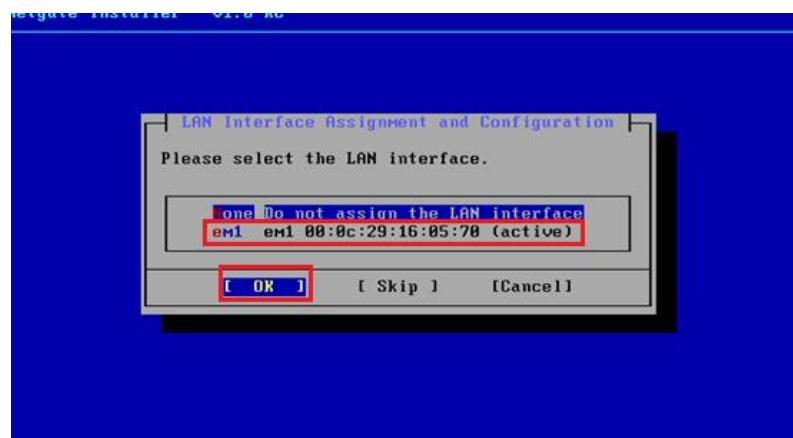
Sélectionnez l'interface em0, pour configurer le WAN puis appuyez sur [ENTRÉE].



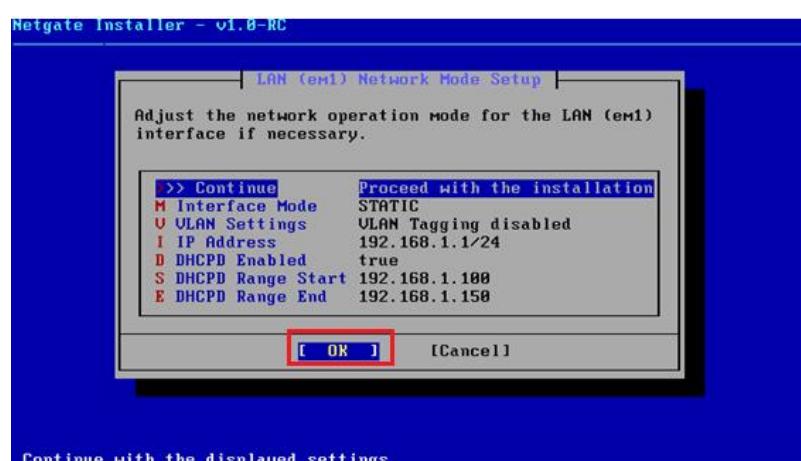
Sélectionnez « Continue » pour poursuivre l'installation et appuyez sur [ENTRÉE].



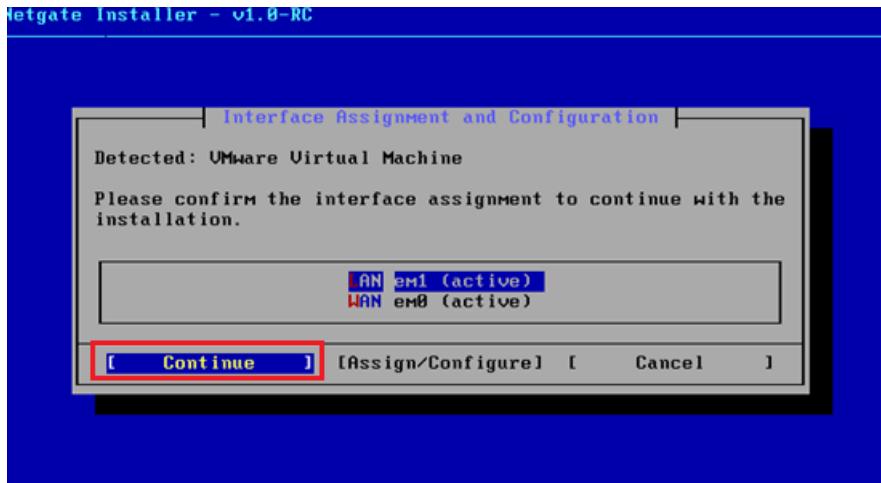
Sélectionnez em1 comme interface LAN, puis validez avec [ENTRÉE].



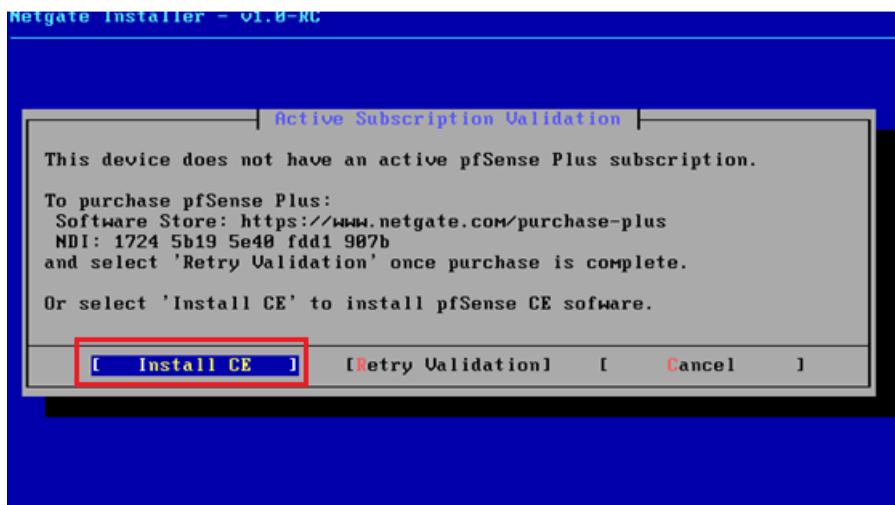
Laissez les paramètres proposés par défaut puis validez avec [ENTRÉE] pour continuer l'installation.



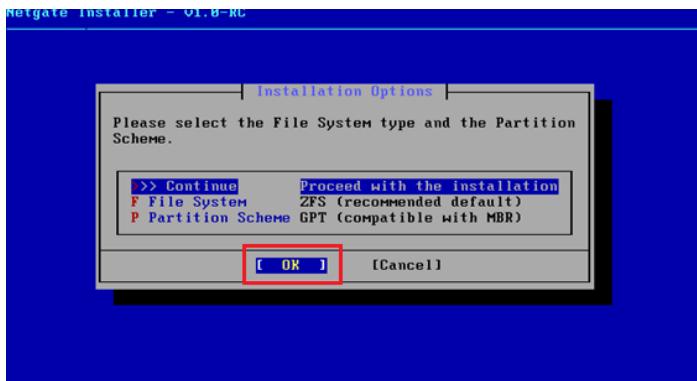
Confirmez l'assignation des interfaces en appuyant sur [ENTRÉE] pour continuer.



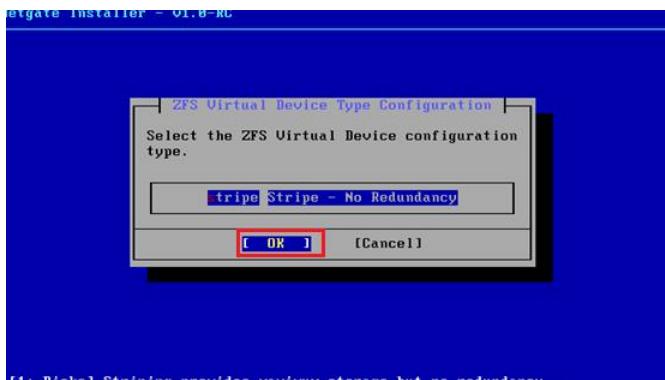
Sélectionnez "Install CE" pour lancer l'installation de la version gratuite de pfSense.



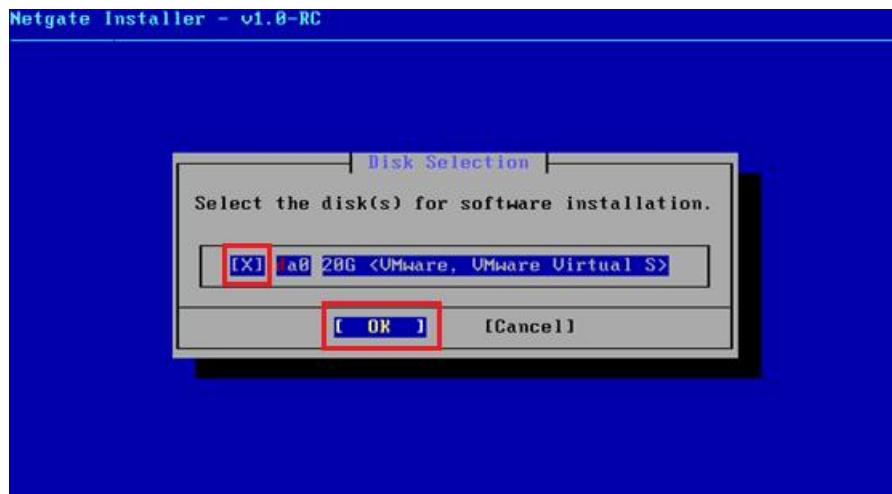
Appuie sur [ENTRÉE] pour continuer l'installation avec ces paramètres recommandés.



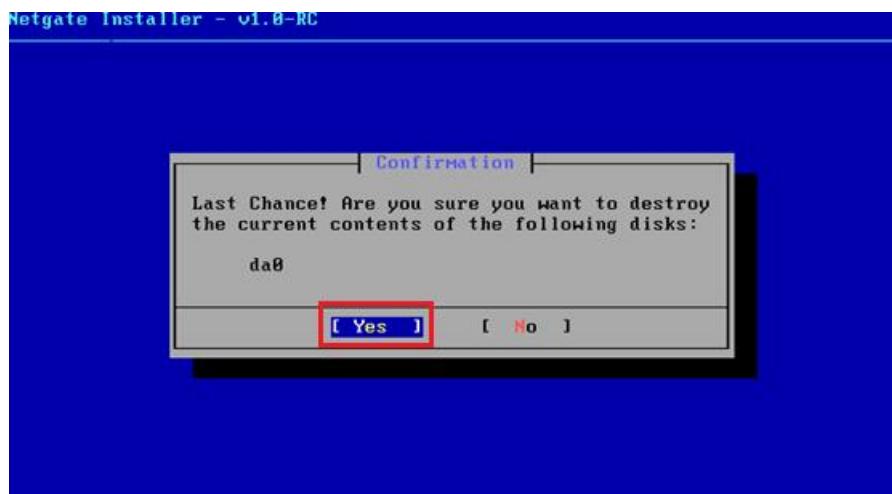
Sélectionnez Stripe – No Redundancy puis validez en appuyant sur [ENTRÉE].



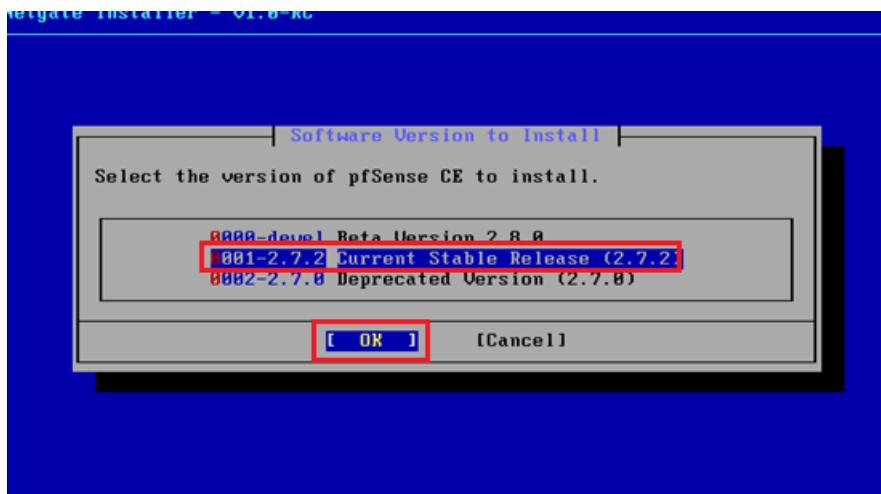
Sélectionnez le disque proposé avec la barre d'espace pour l'installation (ici, le disque de 20 Go), puis appuyez sur [ENTRÉE].



Appuyez simplement sur la touche [ENTRÉE] pour valider l'étape et poursuivre l'installation.

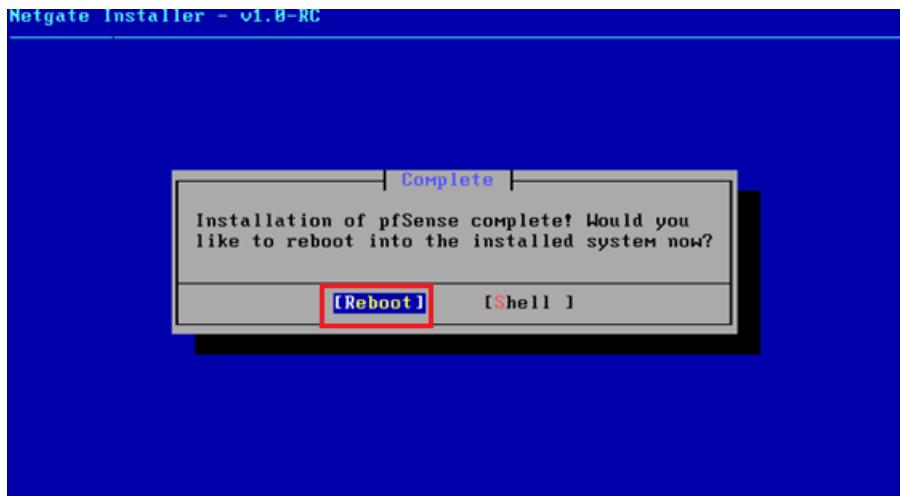


Sélectionnez la version 2.7.2 Current Stable Release, puis appuyez sur [ENTRER] pour continuer l'installation.



*Puis patientez...*

Après l'apparition du message confirmant la fin de l'installation, cliquez sur **[Reboot]** pour redémarrer le système.



Votre installation est prête.

À présent, nous allons procéder à la configuration réseau de pfSense afin de permettre l'accès à son interface web, indispensable pour les prochaines opérations.

Même opération pour FRW-02.

## Configuration du pare-feu principal (FRW-01)

Le pare-feu principal FRW-01 a été configuré avec les paramètres suivants :

- **Interface WAN** : attribution de l'adresse IP via **DHCP**
- **Interface LAN** : adresse IP statique **192.168.100.253/24**

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.47.133/24
LAN (lan)      -> em1      -> v4: 192.168.100.253/24

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

Enter an option: ■
```

## Configuration du pare-feu secondaire (FRW-02)

Le pare-feu secondaire FRW-02 a été configuré avec les paramètres suivants :

- **Interface WAN** : attribution de l'adresse IP via **DHCP**
- **Interface LAN** : adresse IP statique **192.168.100.252/24**

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.47.134/24
LAN (lan)      -> em1      -> v4: 192.168.100.252/24

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

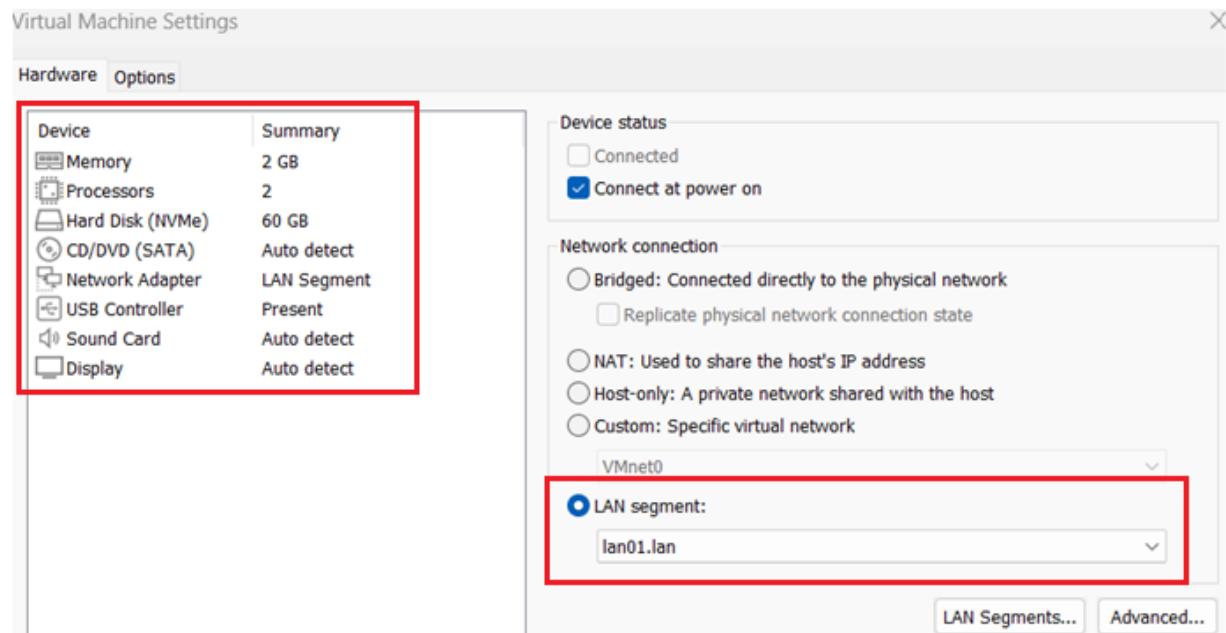
Enter an option: ■
```

On procède à la configuration des serveurs **SRV-AD-01** et **SRV-AD-02**, qui permettront notamment d'accéder aux interfaces web des pare-feux **pfSense**.

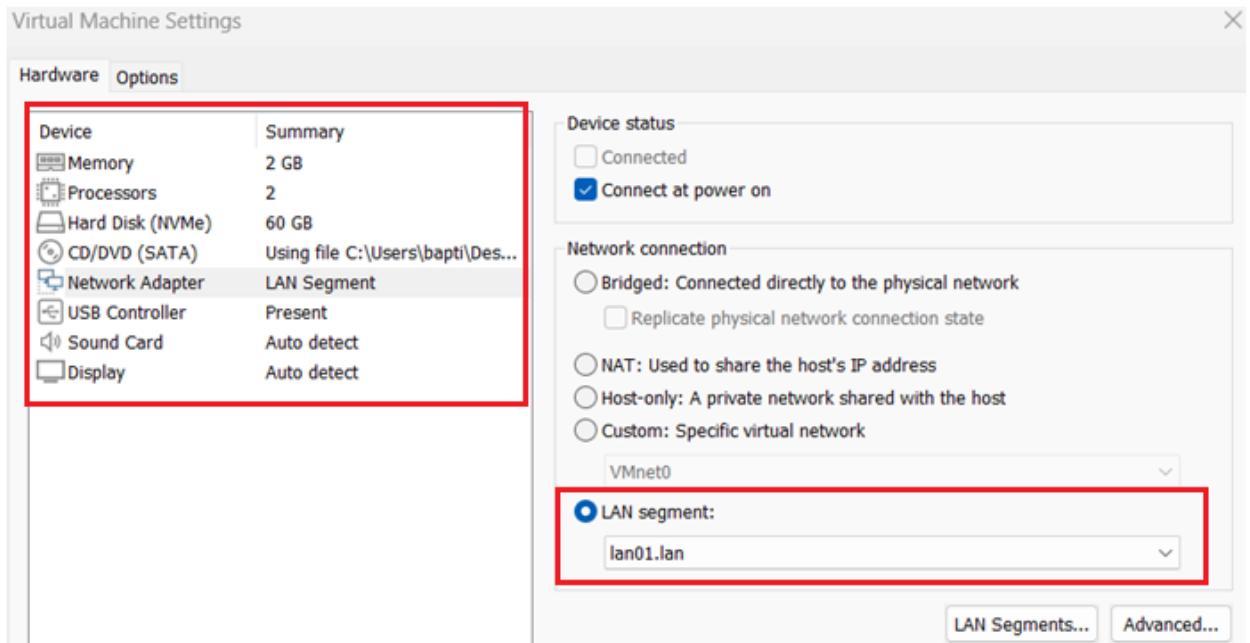
## Prérequis

- **2 machines virtuelles (VM)**
  - **Configuration :**
    - 2 Go de mémoire vive
    - 2 processeurs
    - 1 disque dur de 60 Go
    - 1 carte réseau (LAN)
- **Système d'exploitation : Windows Server 2019**

## Configuration SRV-AD-01 :

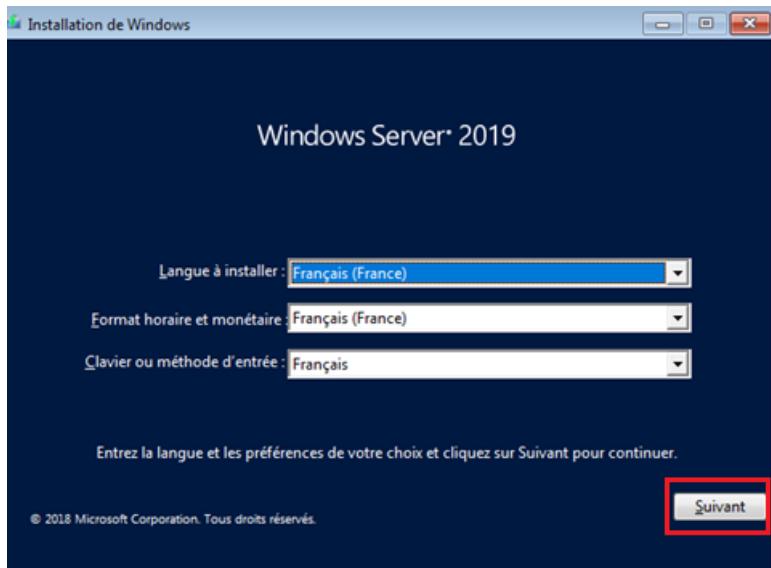


### Configuration de SRV-AD-02 :

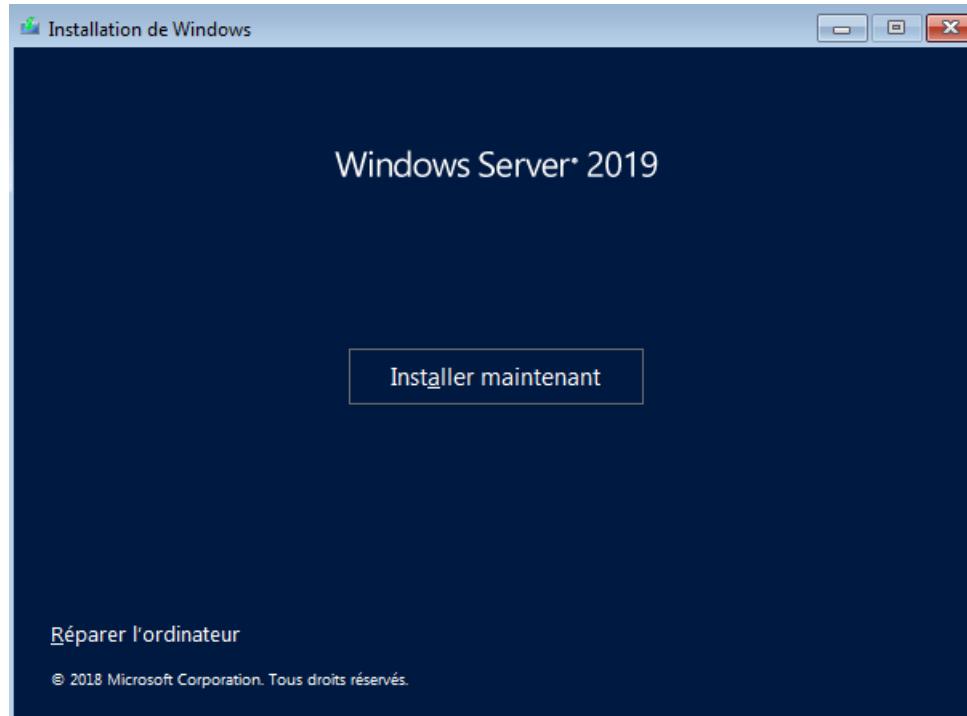


On peut dans un premier temps démarrer les deux serveurs pour procéder à l'installation de base de Windows Server 2019.

Dans un premier temps, choisissez les paramètres de langue, de format horaire et de clavier selon vos préférences, puis cliquez sur **Suivant** pour lancer l'installation de Windows Server 2019.

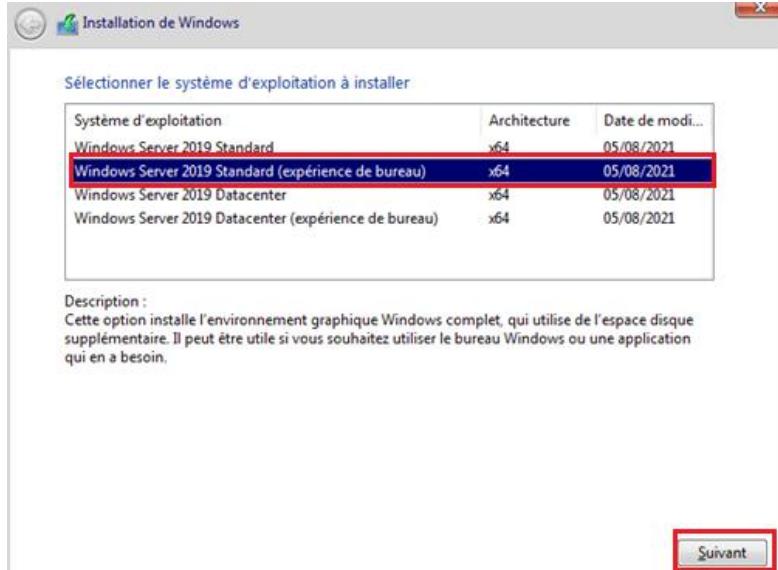


Cliquez sur **Installer maintenant** pour lancer l'installation de Windows Server 2019.

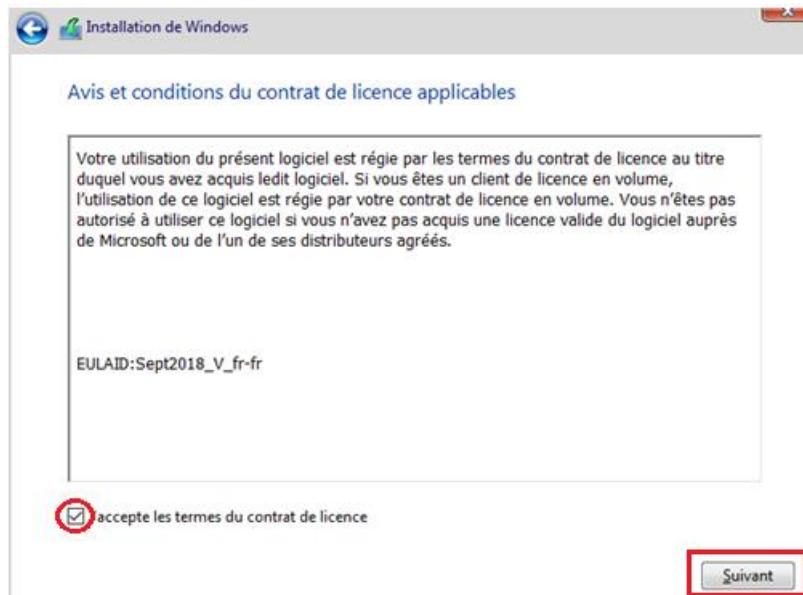


*Patinez...*

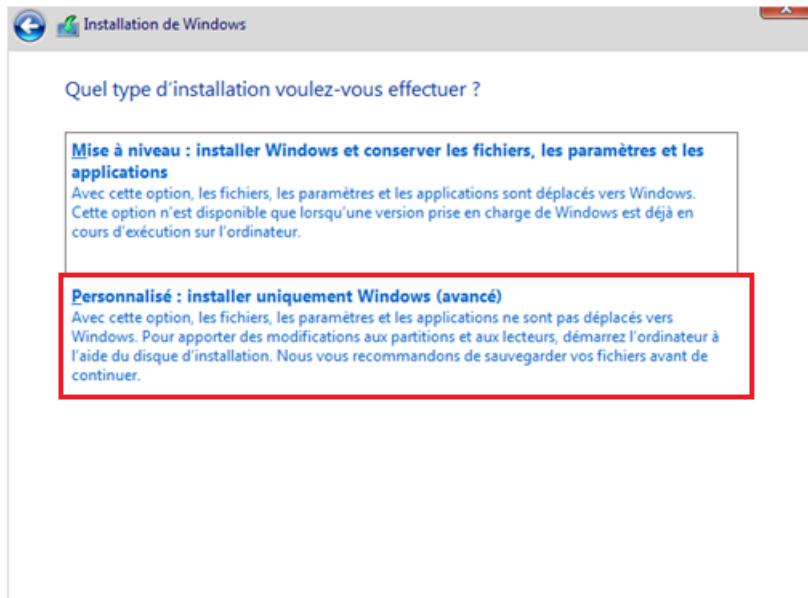
Sélectionnez **Windows Server 2019 Standard (expérience de bureau)**, puis cliquez sur **Suivant** pour bénéficier de l'interface graphique complète.



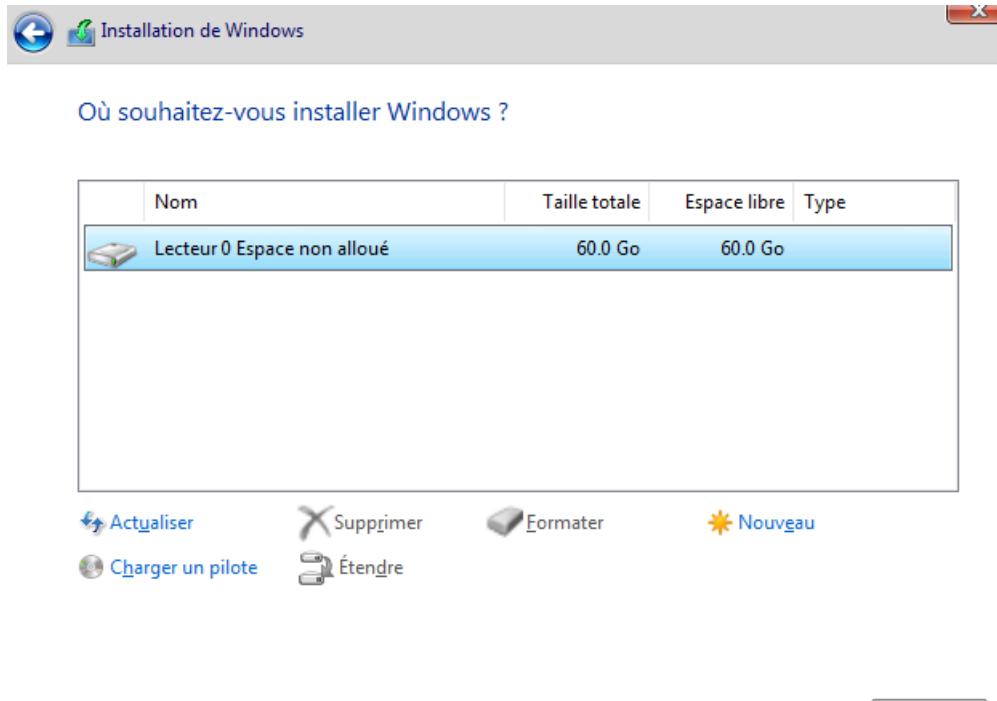
Cochez "J'accepte les termes du contrat de licence", puis cliquez sur **Suivant** pour continuer l'installation.



Sélectionnez "**Personnalisé : installer uniquement Windows (avancé)**", afin de procéder à une installation propre du système d'exploitation.

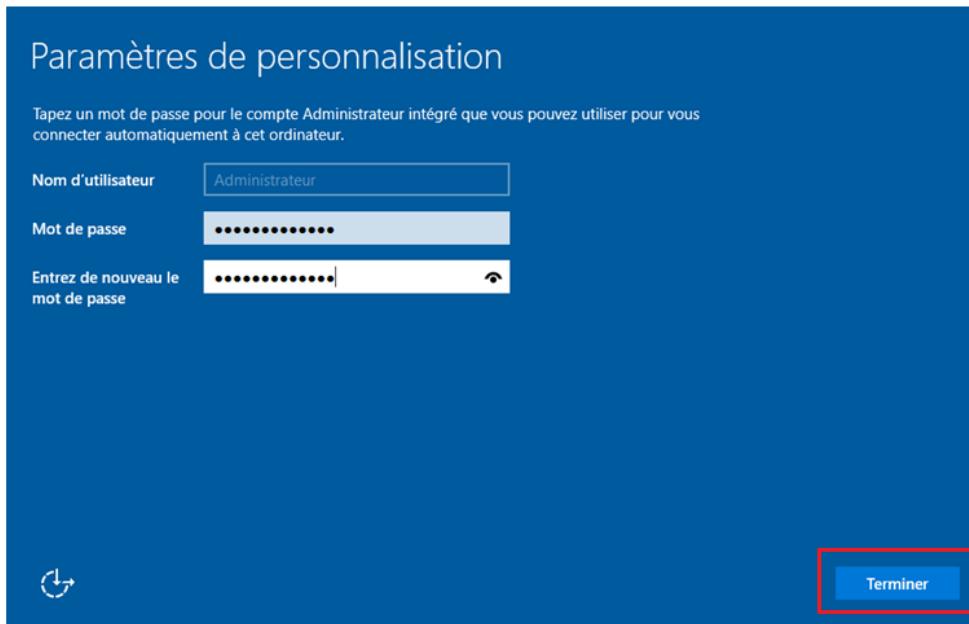


Choisissez le lecteur avec l'espace non alloué, puis cliquez sur **Suivant** pour lancer l'installation de Windows Server 2019.



*Patientez...*

Définissez un mot de passe pour le compte **Administrateur**, confirmez-le dans le champ en dessous, puis cliquez sur **Terminer** pour finaliser la configuration.

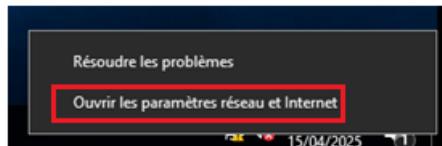


Vous êtes désormais connecté à votre environnement Windows Server.

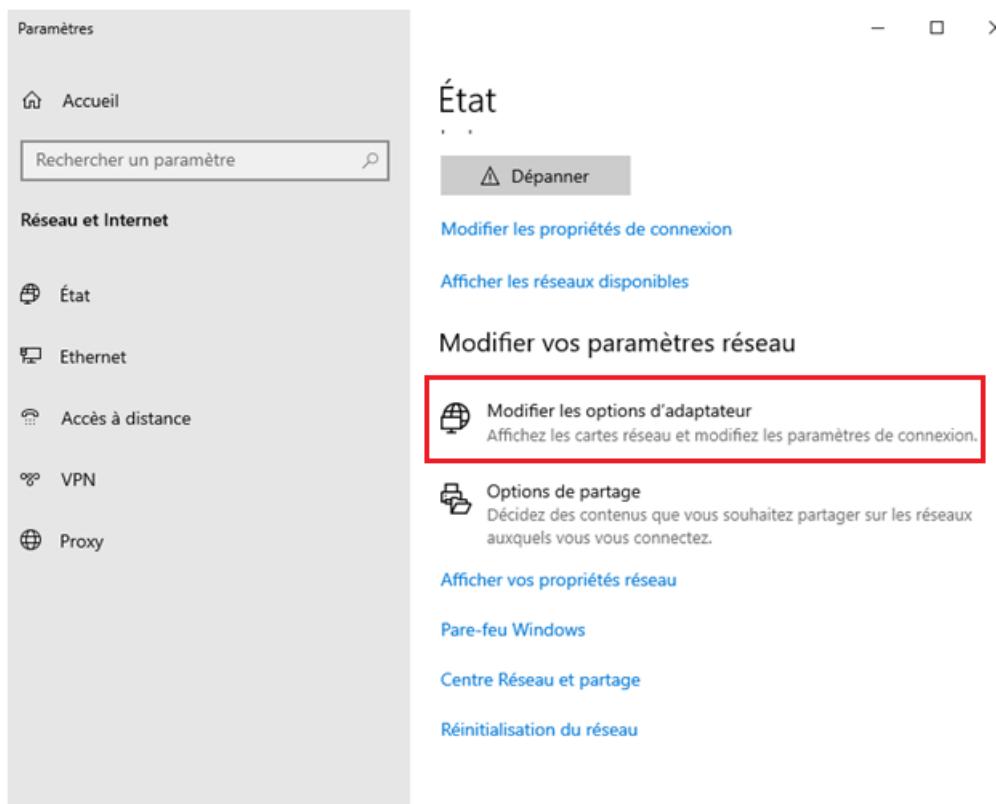
On va maintenant configurer les paramètres réseau de chaque serveur.

Effectuez un clic droit sur l'icône réseau en bas à droite, puis cliquez sur "**Ouvrir les paramètres réseau et Internet**" afin d'accéder aux options de configuration de l'adresse IP.

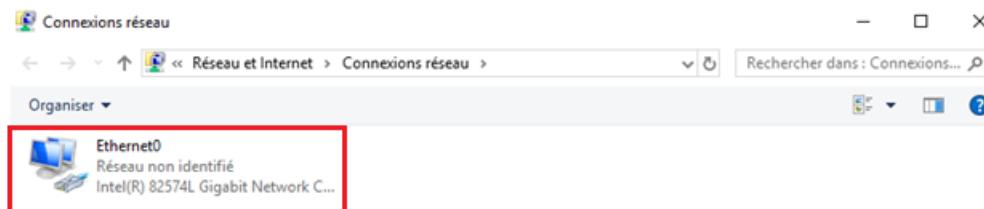




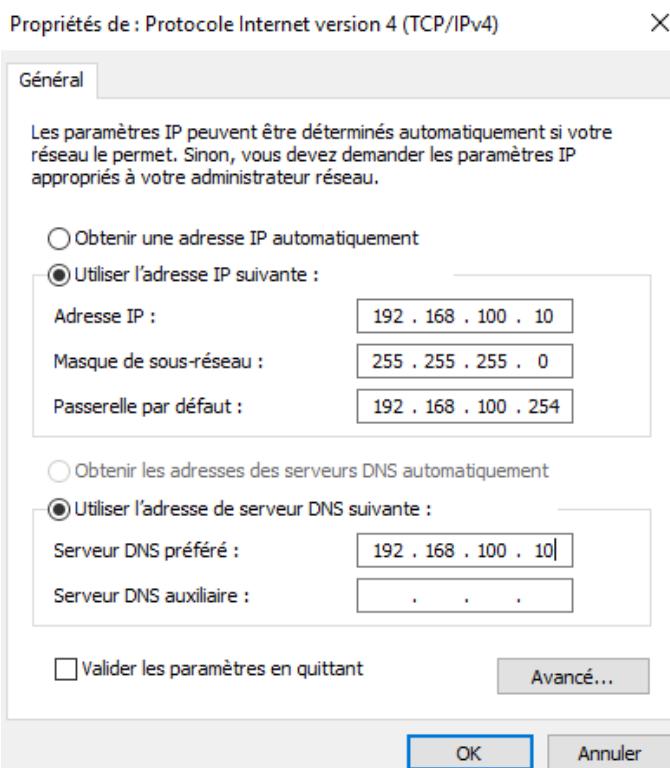
Cliquez sur "Modifier les options d'adaptateur".



Clic droit sur Ethernet0 > Propriétés > Protocole IPv4 attribué



STG-AD-01



## SRV-AD-02

Propriétés de : Protocole Internet version 4 (TCP/IPv4) X

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :	192 . 168 . 100 . 20
Masque de sous-réseau :	255 . 255 . 255 . 0
Passerelle par défaut :	192 . 168 . 100 . 254

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :	192 . 168 . 100 . 10
Serveur DNS auxiliaire :	. . .

Valider les paramètres en quittant Avancé...

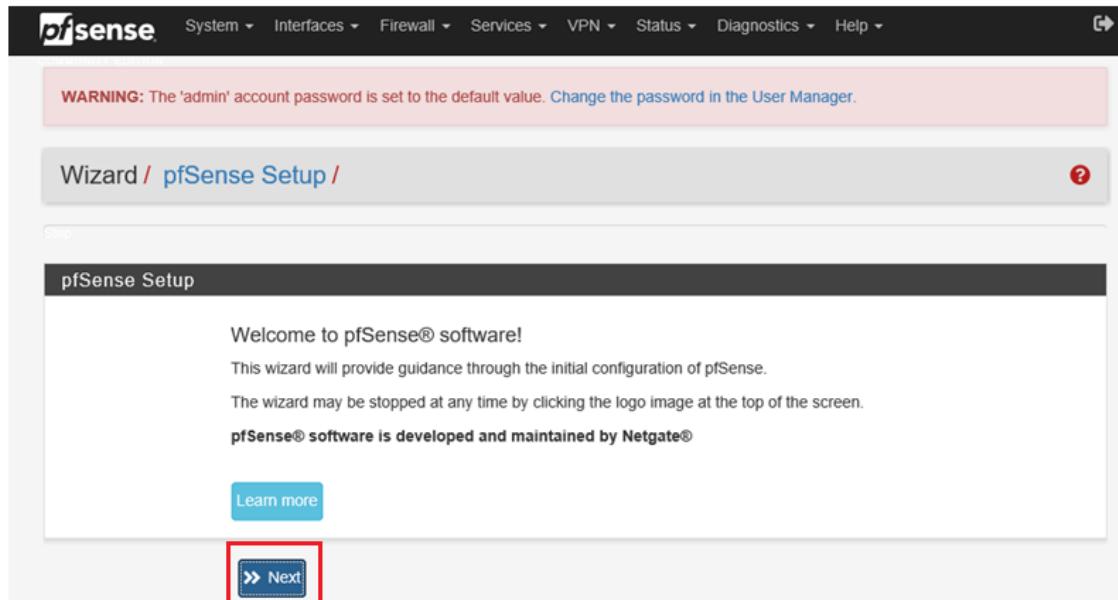
OK Annuler

## 2.2) Configuration d'un CARP

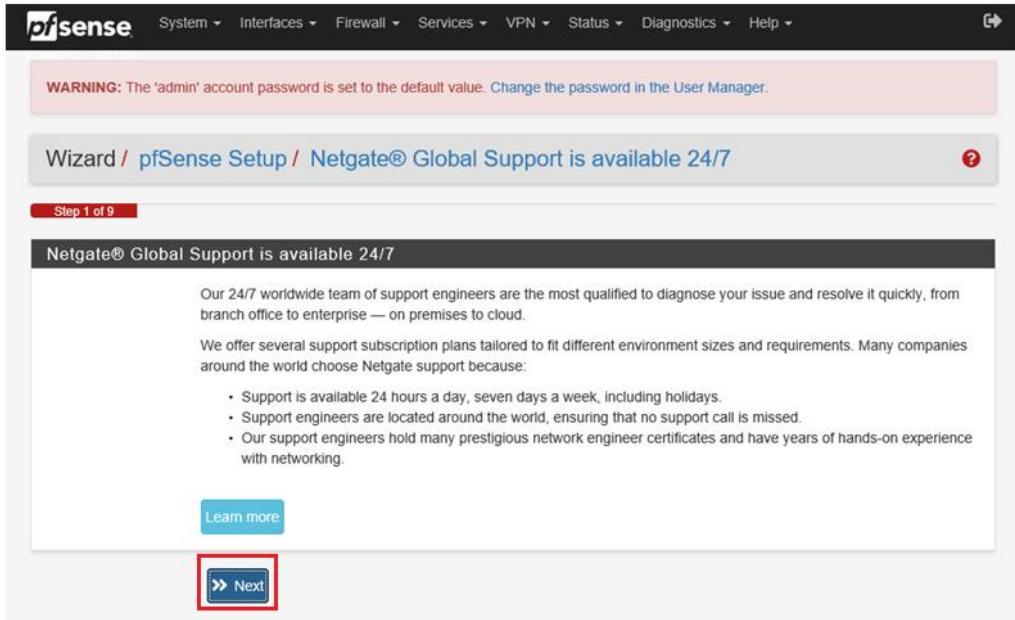
Pour configurer le CARP depuis FRW-01, accéder à l'interface web du pare-feu via l'adresse :

👉 <http://192.168.100.253/>

Une fois connecté à l'interface web de pfSense, une configuration initiale du pare-feu vous sera proposée. Cliquez simplement sur "**Next**" pour poursuivre.



Le message d'information concernant le support 24/7 de Netgate apparaît ensuite. Cliquez sur "Next" pour continuer.



**pfSense** System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

**Wizard / pfSense Setup / Netgate® Global Support is available 24/7**

**Step 1 of 9**

**Netgate® Global Support is available 24/7**

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise — on premises to cloud.

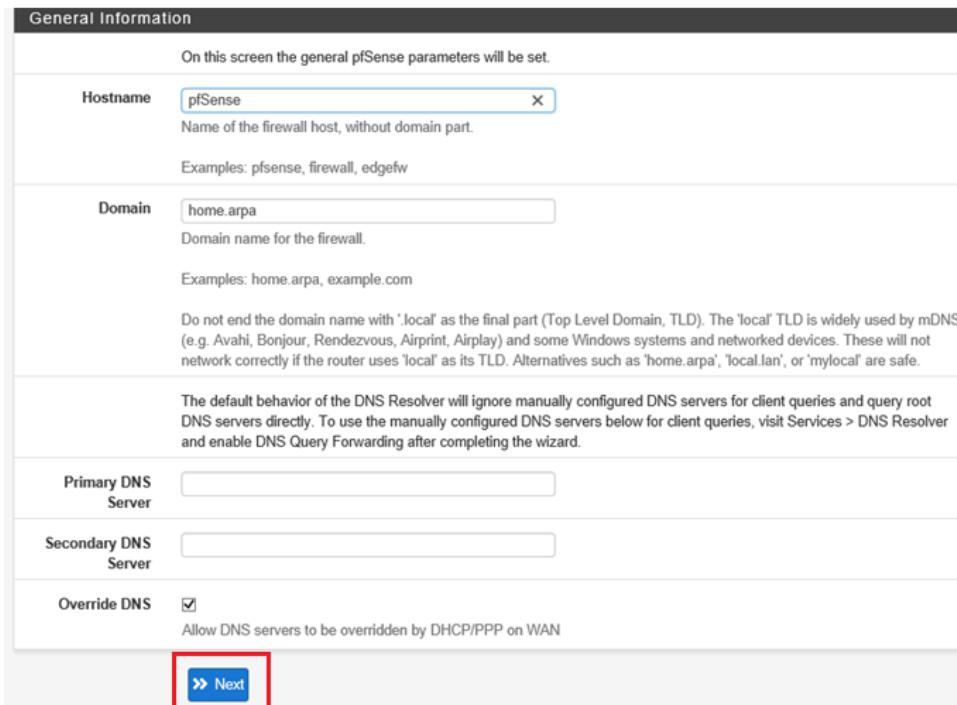
We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

**>> Next**

Vous pouvez modifier ici le nom d'hôte du routeur si nécessaire, puis cliquez sur "Next" pour poursuivre.



**General Information**

On this screen the general pfSense parameters will be set.

<b>Hostname</b>	<input type="text" value="pfSense"/> <a href="#">X</a>
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
<b>Domain</b>	<input type="text" value="home.arpa"/>
Domain name for the firewall.	
Examples: home.arpa, example.com	
Do not end the domain name with 'local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
<b>Primary DNS Server</b>	<input type="text"/>
<b>Secondary DNS Server</b>	<input type="text"/>
<b>Override DNS</b>	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	

**>> Next**

Choisissez le fuseau horaire approprié, ici **Europe/Paris**, afin d'éviter toute désynchronisation du pare-feu avec les machines du réseau LAN. Un mauvais paramètre horaire pourrait entraîner des dysfonctionnements au niveau du routage et des services réseau.

**Time Server Information**

Please enter the time, date and time zone.

Time server hostname	2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.	
Timezone	Europe/Paris
<b>&gt;&gt; Next</b>	

Cliquez sur **Next** pour poursuivre la configuration.

L'adresse IP LAN du pare-feu primaire est configurée en 192.168.100.253 avec un masque /24, conformément au plan d'adressage, **Next**.

**Configure LAN Interface**

On this screen the Local Area Network information will be configured.

LAN IP Address	192.168.100.253
Type dhcp if this interface uses DHCP to obtain its IP address.	
Subnet Mask	24
<b>&gt;&gt; Next</b>	

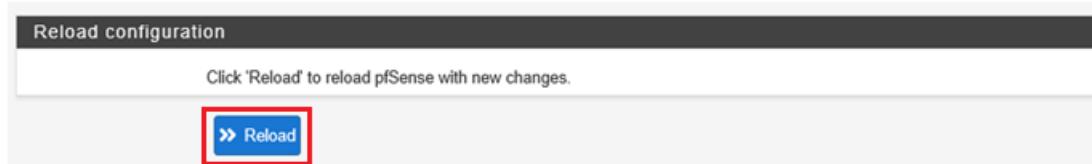
Modifiez impérativement le mot de passe administrateur pour sécuriser le routeur, puis cliquez sur **Next**. Pensez à enregistrer ce mot de passe dans un gestionnaire comme KeePass si plusieurs personnes doivent y accéder.

**Set Admin WebGUI Password**

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password	*****
Admin Password AGAIN	*****
<b>&gt;&gt; Next</b>	

Cliquez sur **Reload** et patientez le temps que les configurations s'appliquent.



*Patinez, puis **Finish** pour confirmer et quittez la configuration globale du routeur.*

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the best things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short anonymous survey.

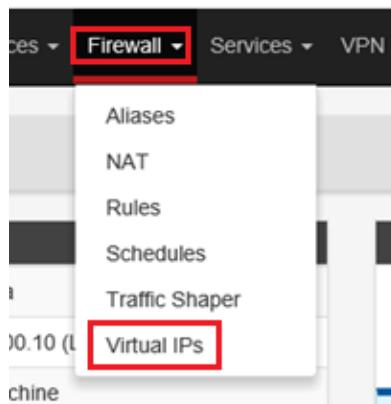
[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers

**Finish**

Depuis le tableau de bord, aller dans le menu **Firewall** puis sélectionner **Virtual IPs**.



Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
				<b>+ Add</b>

Une fois dans l'onglet *Virtual IPs*, sélectionner le type **CARP**, renseigner les paramètres nécessaires puis cliquer sur *Save* pour valider la configuration.

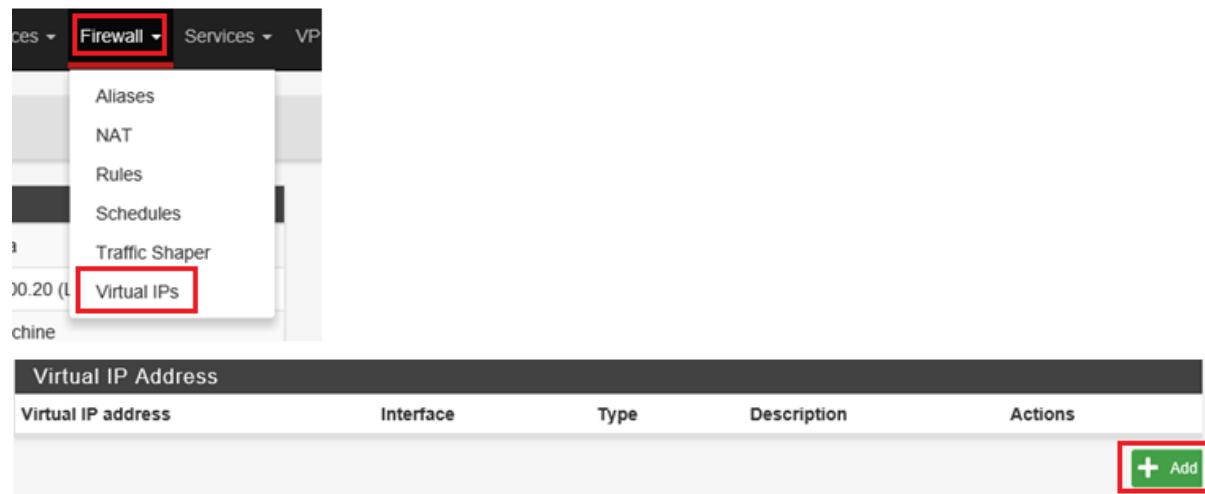
**Edit Virtual IP**

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	LAN			
Address type	Single address			
Address(es)	192.168.100.254 / 24			
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP	****		****	
Password	Enter the VHID group password.			
VHID Group	1			
Enter the VHID group that the machines will share.				
Advertising frequency	1	0	Base	Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	LAN CARP			
A description may be entered here for administrative reference (not parsed).				
<b>Save</b>				

Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
192.168.100.254/24 (vhid: 1)	LAN	CARP	LAN CARP	 

La configuration du CARP sur le pare-feu secondaire **FRW-02** s'effectue de la même manière que sur FRW-01.

Accéder à l'interface web via l'adresse : <http://192.168.100.252/>, puis aller dans **Firewall > Virtual IPs**.



The screenshot shows the 'Virtual IP Address' configuration page. At the top, there is a navigation bar with tabs: 'Services', 'Firewall' (which is selected and highlighted with a red box), 'Services', and 'VP'. Below the navigation bar is a sidebar with links: 'Aliases', 'NAT', 'Rules', 'Schedules', 'Traffic Shaper', and 'Virtual IPs' (which is also highlighted with a red box). The main area is titled 'Virtual IP Address' and contains a table with columns: 'Virtual IP address', 'Interface', 'Type', 'Description', and 'Actions'. In the 'Actions' column, there is a green button with a white plus sign and the word 'Add' (also highlighted with a red box).

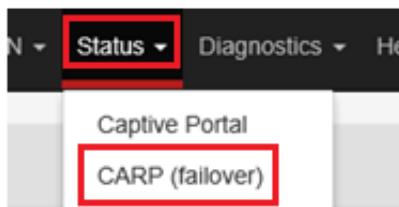
Dans Virtual IPs, sélectionner le type "CARP" et renseigner les paramètres indiqués ci-dessous, puis cliquer sur "Save".

**Edit Virtual IP**

Type	<input type="radio"/> IP Alias	<input checked="" type="radio"/> CARP	<input type="radio"/> Proxy ARP	<input type="radio"/> Other
Interface	LAN			
Address type	Single address			
Address(es)	192.168.100.254		/ 24	v
The mask must be the network's subnet mask. It does not specify a CIDR range.				
Virtual IP Password	****	****	Enter the VHID group password. Confirm	
VHID Group	1			
Enter the VHID group that the machines will share.				
Advertising frequency	1	0	v	
Base Skew				
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.				
Description	LAN CARP			
A description may be entered here for administrative reference (not parsed).				
<input type="button" value="Save"/>				

<b>Virtual IP Address</b>				
Virtual IP address	Interface	Type	Description	Actions
192.168.100.254/24 (vhid: 1)	LAN	CARP	LAN CARP	 

Pour vérifier le bon fonctionnement du CARP, se rendre dans l'interface web de chaque pare-feu, puis accéder à : **Status > CARP (failover)**.



À ce stade, le pare-feu **FRW-01** apparaît en tant que « **MASTER** ».

Status / CARP

CARP Maintenance

ⓘ Temporarily Disable CARP  ⚡ Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.100.254/24	LAN CARP	▶ MASTER

State Synchronization Status

State Creator Host IDs:

- 8a698ec8 (This node)

ⓘ

When state synchronization is enabled and functioning properly the list of state creator host IDs will be identical on each node participating in state synchronization.

The state creator host ID for this node can be set to a custom value under System > High Avail Sync. If the state creator host ID has recently changed, the old ID will remain until all states using the old ID expire or are removed.

Le pare-feu FRW-02 est quant à lui en position « BACKUP ».

Status / CARP

CARP Maintenance

ⓘ Temporarily Disable CARP  ⚡ Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
LAN@1	192.168.100.254/24	LAN CARP	<span> ⚡ BACKUP</span>

State Synchronization Status

State Creator Host IDs:

- 64b2f289 (This node)

ⓘ

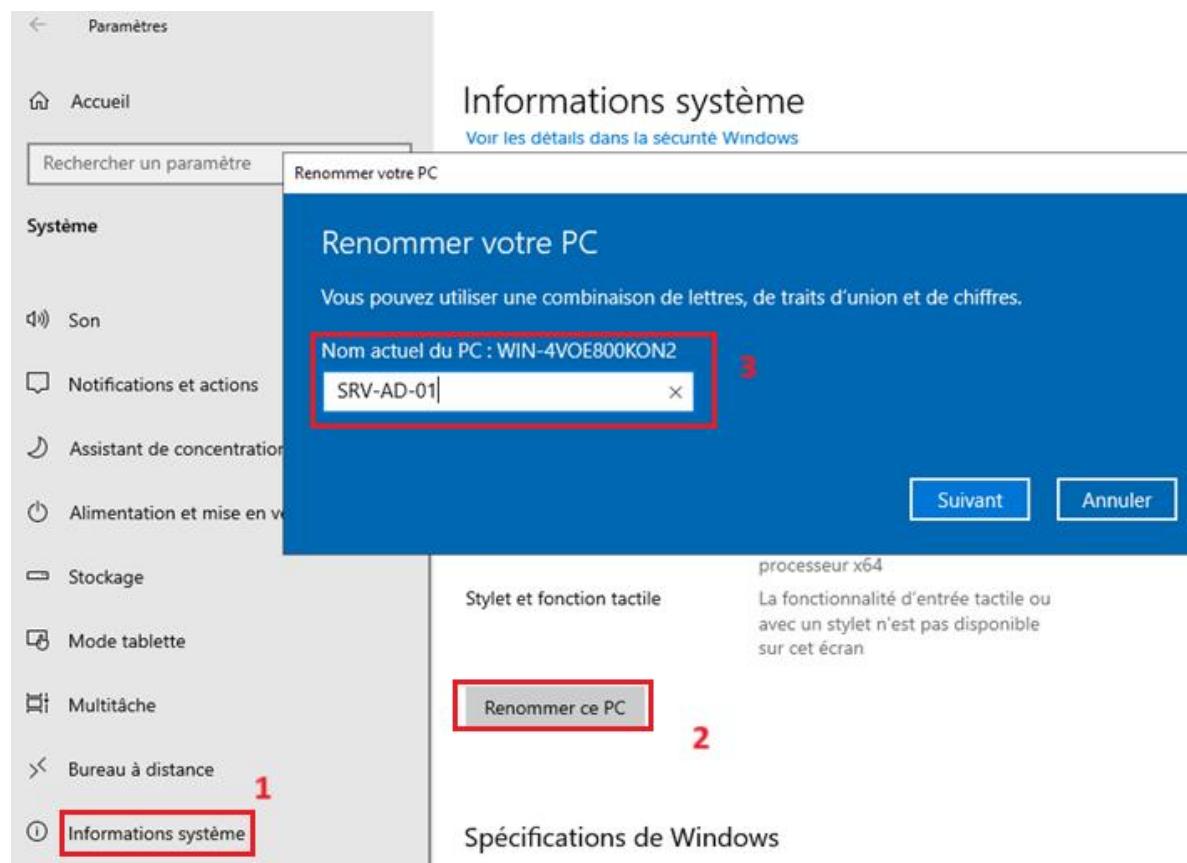
When state synchronization is enabled and functioning properly the list of state creator host IDs will be identical on each node participating in state synchronization.

The state creator host ID for this node can be set to a custom value under System > High Avail Sync. If the state creator host ID has recently changed, the old ID will remain until all states using the old ID expire or are removed.

## Active Directory – Service d'annuaire

### 2.3) Déploiement de l'Active Directory sur deux contrôleurs de domaine (SRV-AD-01 & SRV-AD-02)

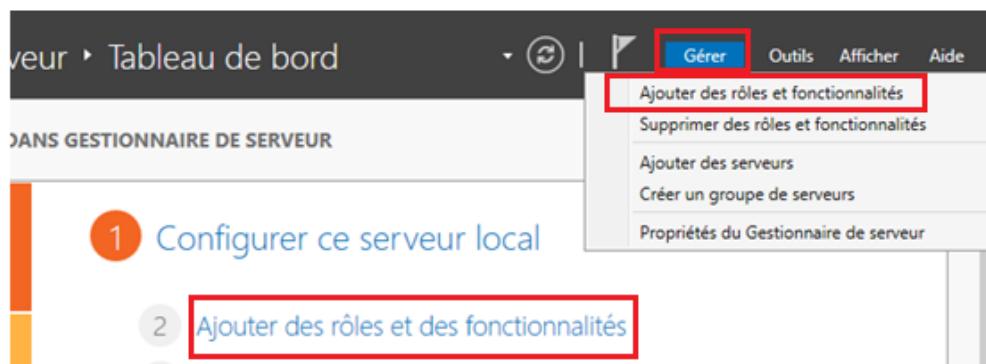
Tout d'abord, pensez à renommer votre machine avec le nom défini dans le plan, en accédant à **Paramètres > Système > Informations système**, puis en cliquant sur **Renommer ce PC**.



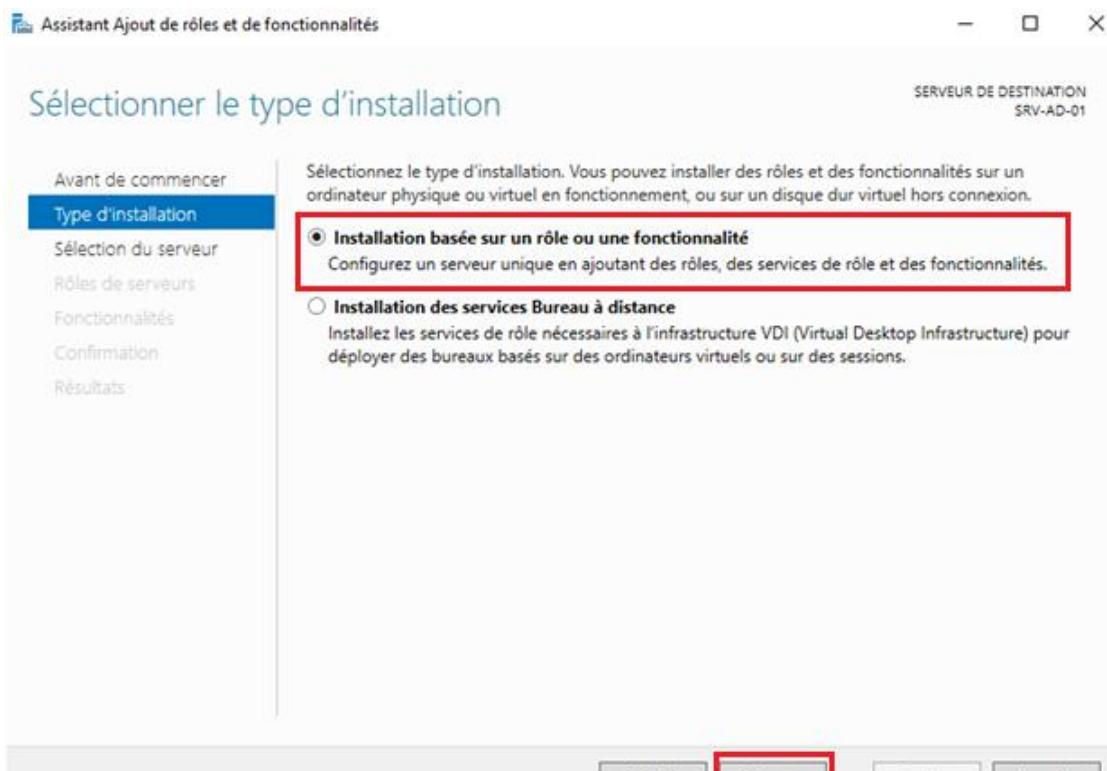
Une fois le nom modifié, redémarrez la machine pour que le changement soit pris en compte.

## Installation de l'Active Directory sur SRV-AD-01

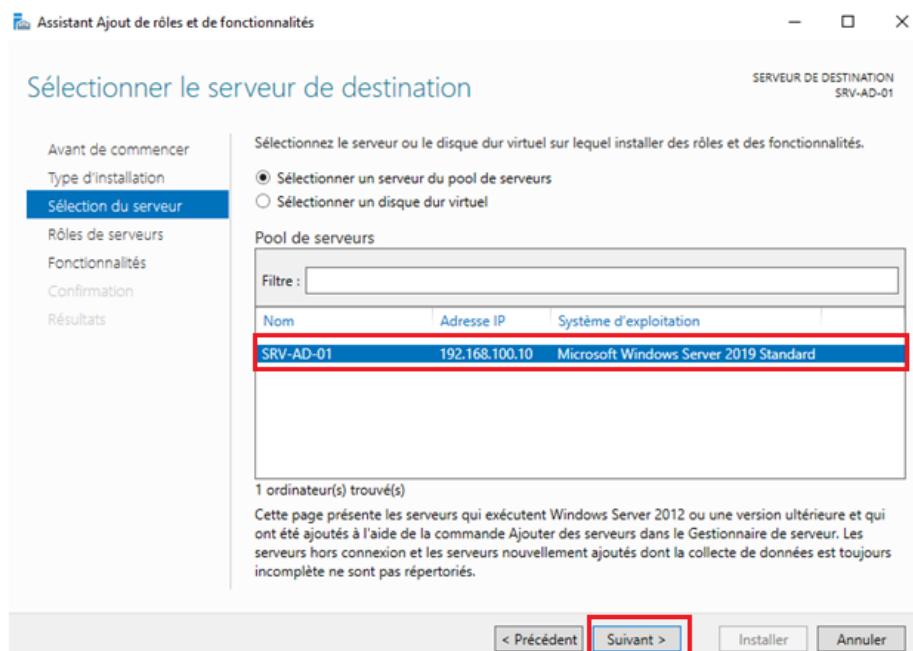
Accéder à **Gérer > Ajouter des rôles et fonctionnalités**, puis cliquer directement sur **Suivant** pour lancer l'installation.



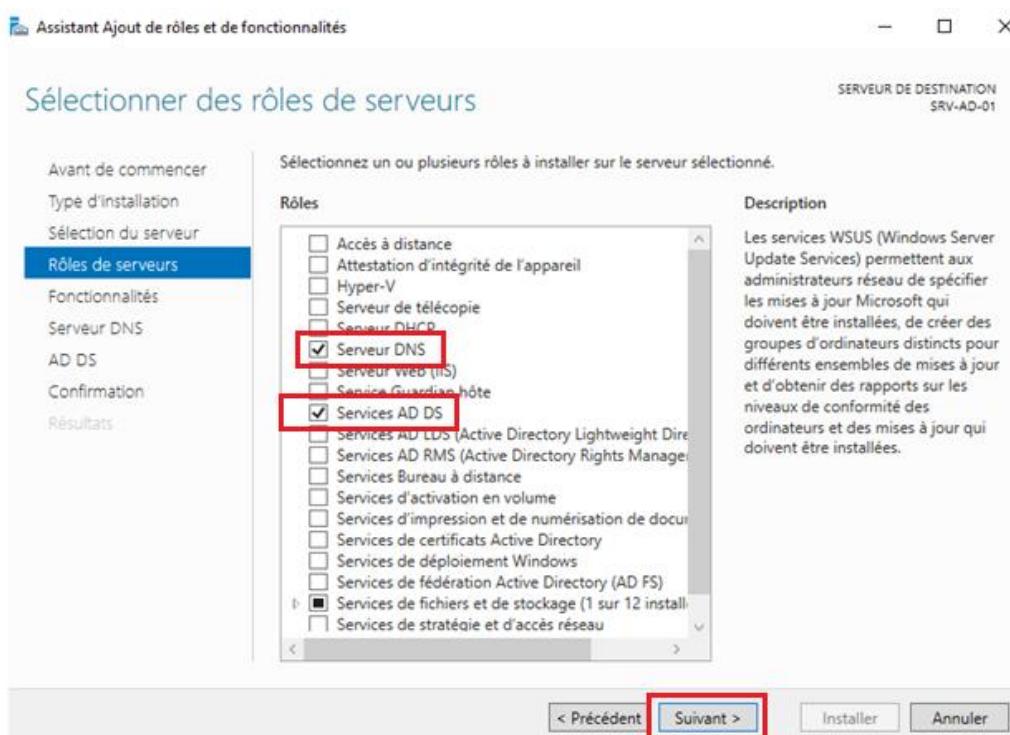
Cocher "**Installation basée sur un rôle ou une fonctionnalité**", puis cliquer sur **Suivant**.



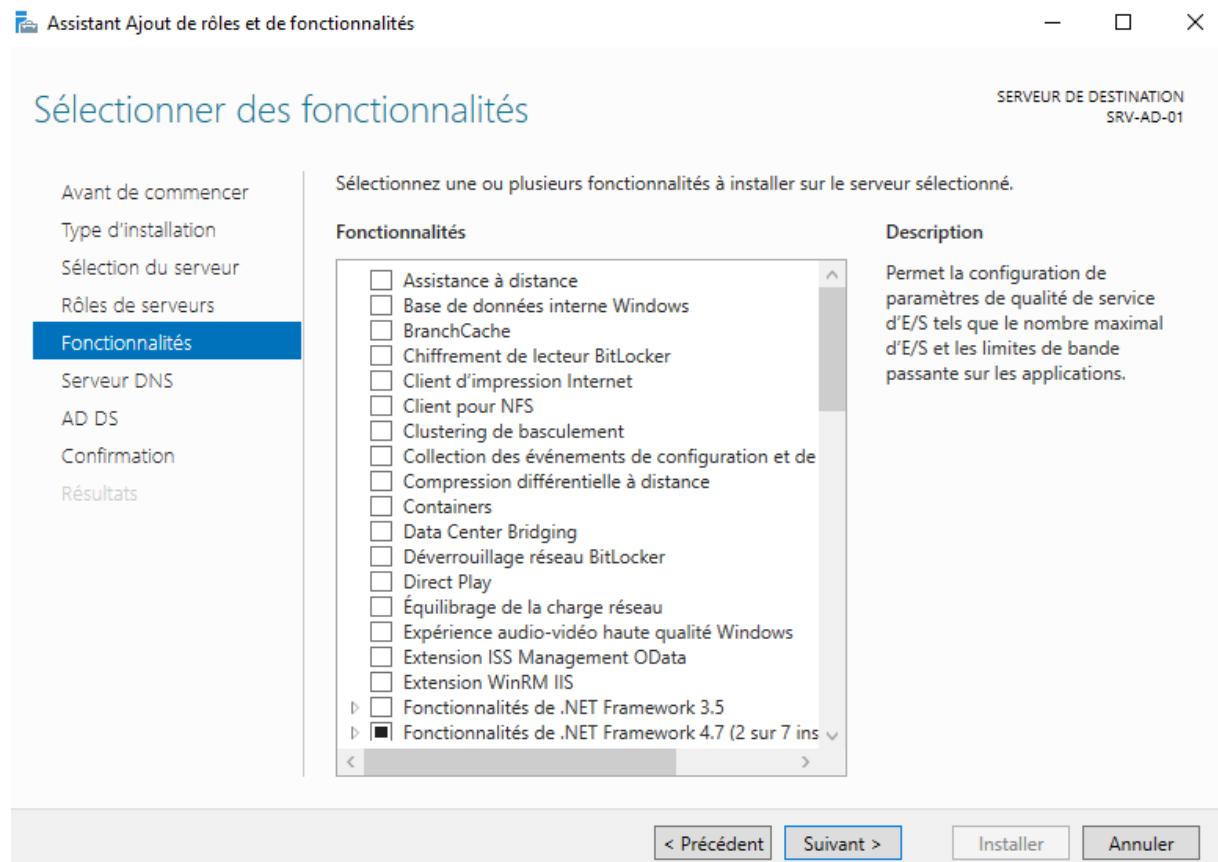
Sélectionner le serveur SRV-AD-01 dans la liste, puis cliquer sur **Suivant**.



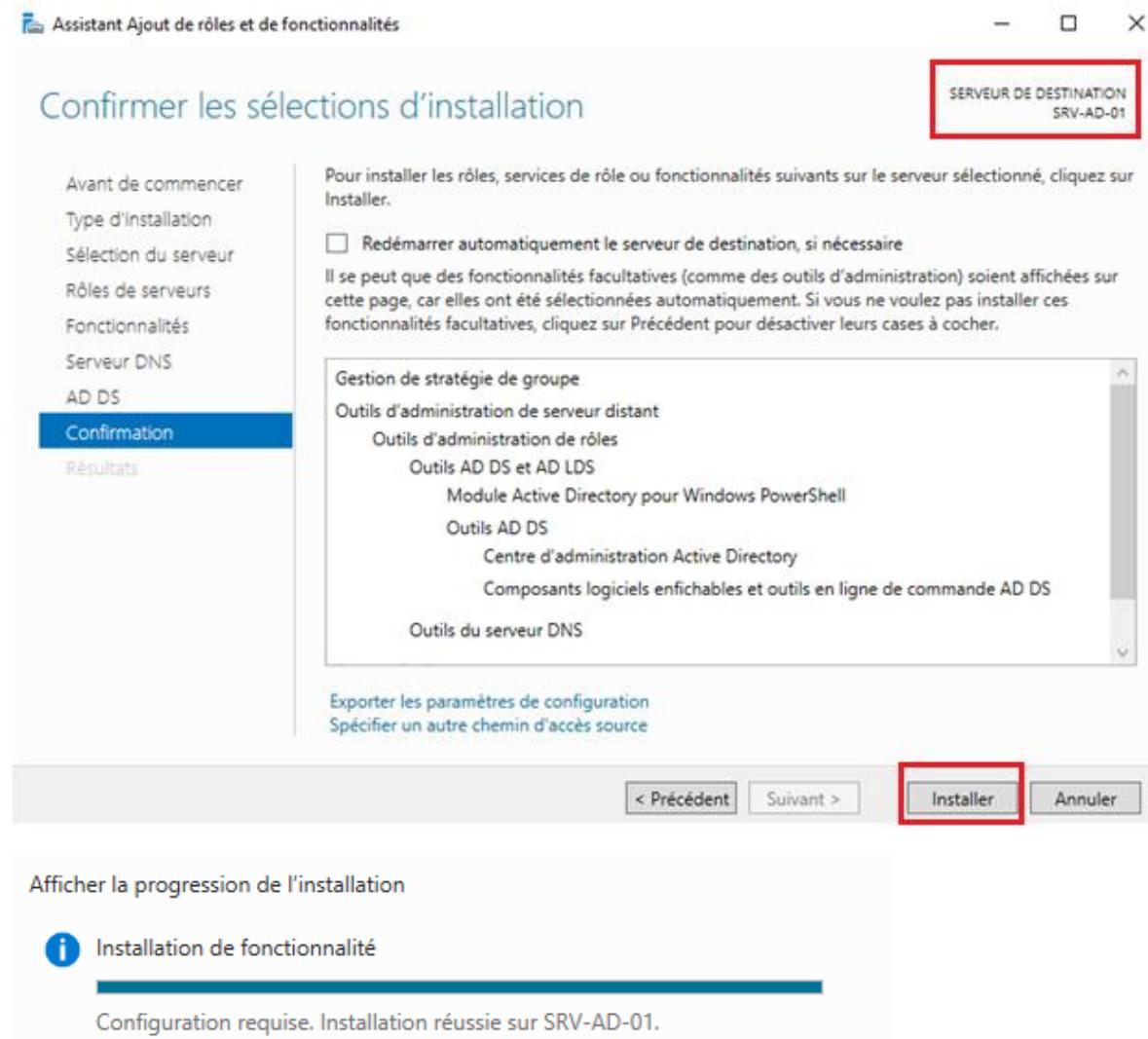
Cocher les rôles **Services AD DS** et **Serveur DNS**, puis cliquer sur **Suivant**.



Ne rien cocher ici, cliquer simplement sur **Suivant**.

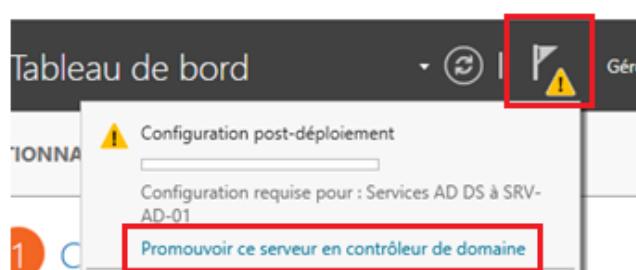


Continuer en cliquant sur **Suivant** jusqu'à apercevoir le bouton **Installer**, puis lancer l'installation.

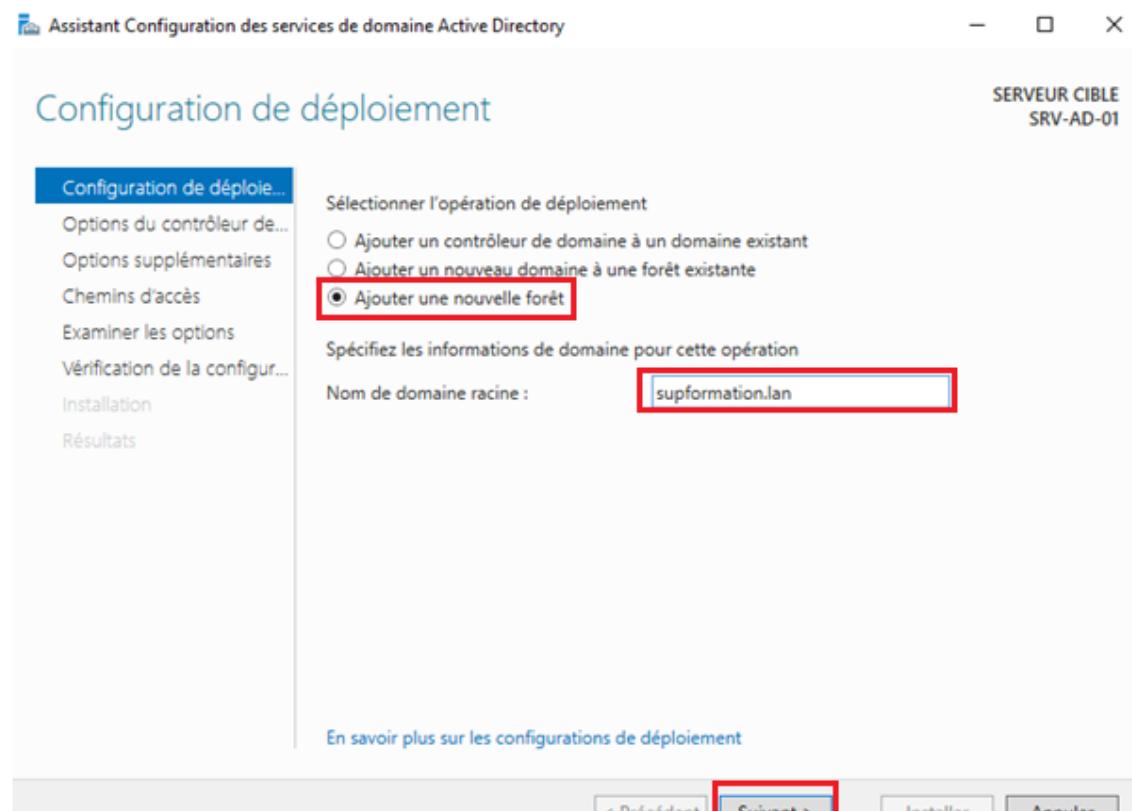


## Configuration de l'Active Directory sur le serveur SRV-AD-01

Une fois l'installation terminée, cliquer sur l'icône d'alerte puis sur « Promouvoir ce serveur en contrôleur de domaine ».



Cocher « Ajouter une nouvelle forêt », entrer le nom de domaine supformation.lan, puis cliquer sur Suivant.



Définir et confirmer un mot de passe pour le mode de restauration DSRM, puis cliquer sur Suivant.

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :  ······

Confirmer le mot de passe :  ······

Aucune configuration pour les options DNS, cliquer sur **Suivant**.

Assistant Configuration des services de domaine Active Directory

SERVEUR CIBLE  
SRV-AD-01

Options DNS

⚠ Il est impossible de créer une délégation pour ce serveur DNS car la zone parente faisant autorité est intro... [Afficher plus](#) ×

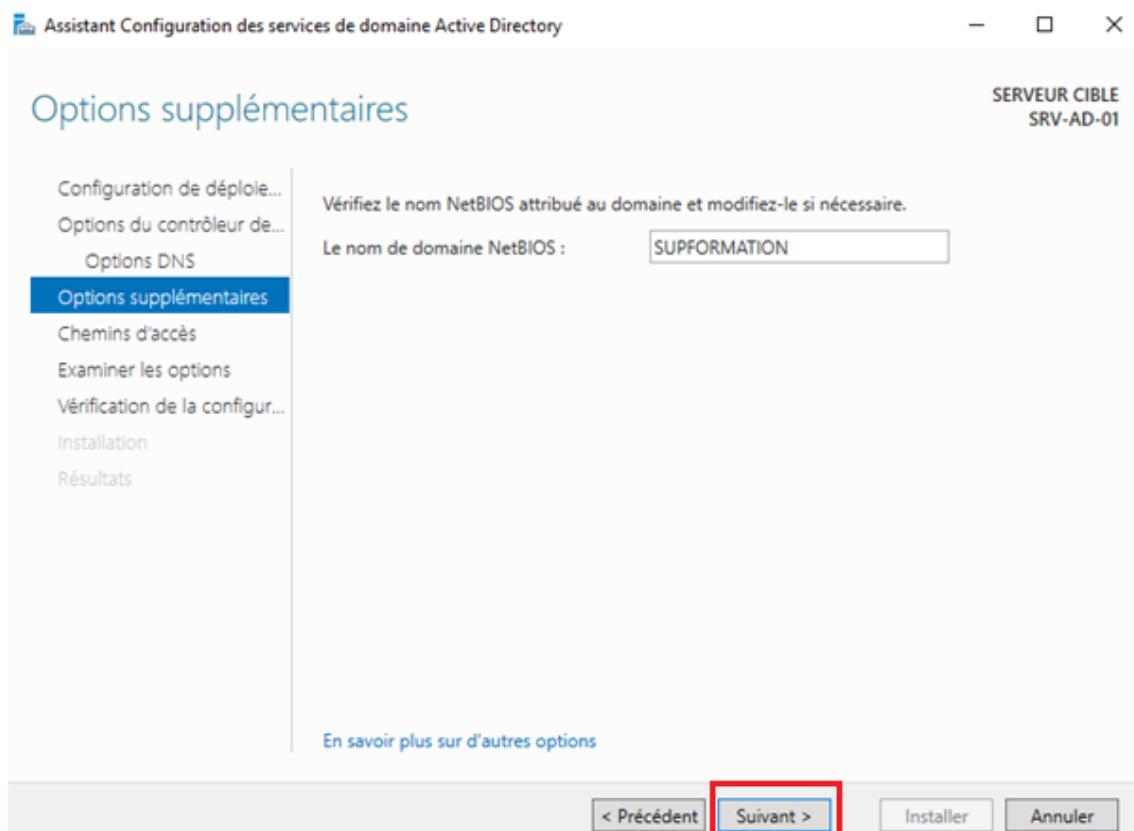
Configuration de déploie...  
Options du contrôleur de...  
**Options DNS**  
Options supplémentaires  
Chemins d'accès  
Examiner les options  
Vérification de la configur...  
Installation  
Résultats

Spécifier les options de délégation DNS  
 Créer une délégation DNS

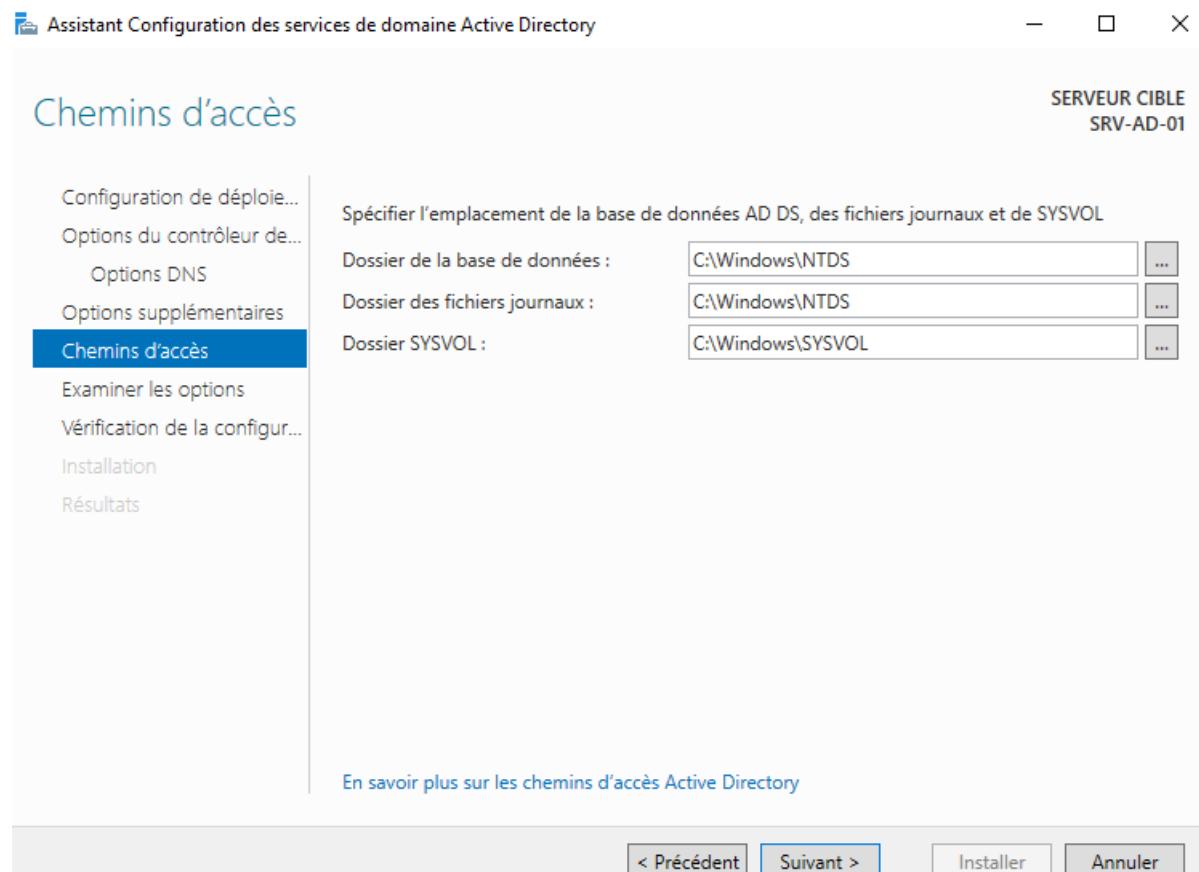
[En savoir plus sur la délégation DNS](#)

[< Précédent](#) Suivant > [Installer](#) [Annuler](#)

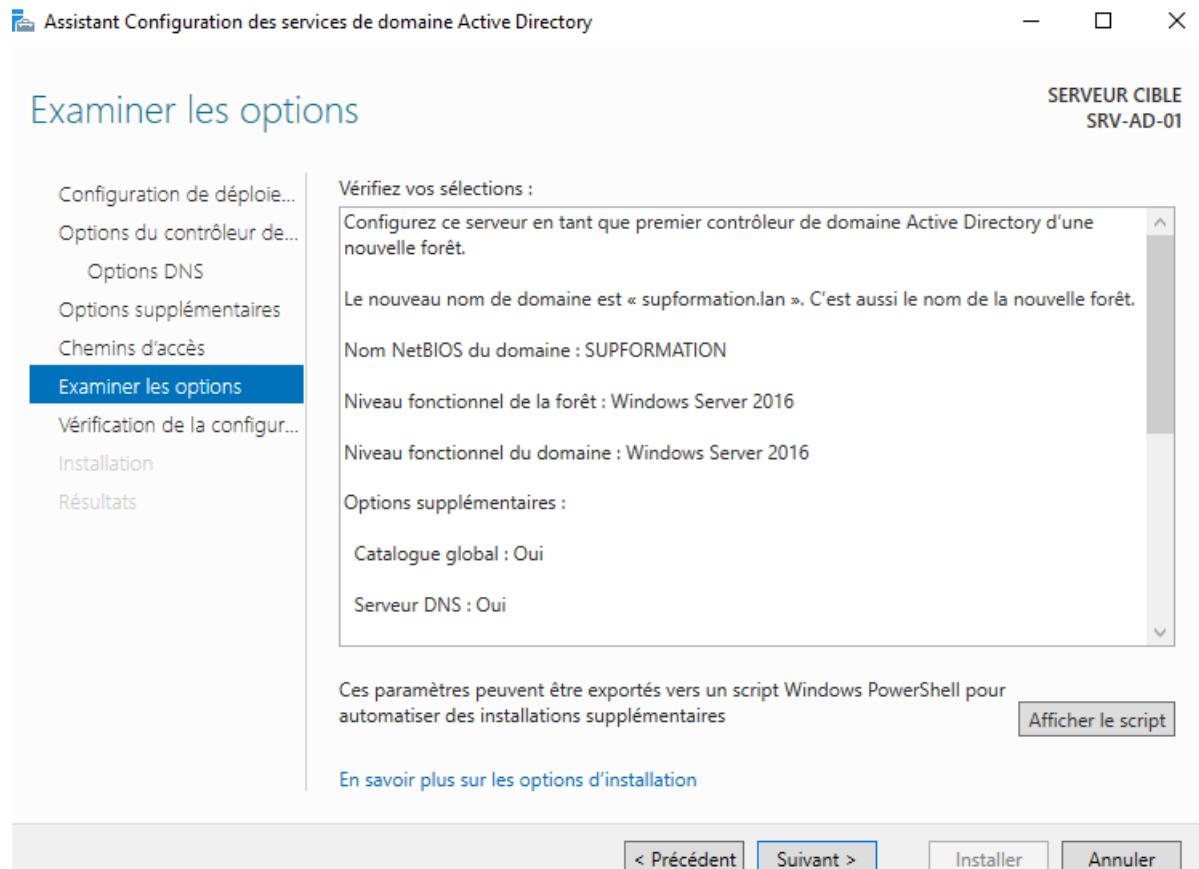
Vérifier que le nom NetBIOS correspond bien, puis cliquer sur **Suivant**.



Laisser les chemins d'accès par défaut puis cliquer sur **Suivant**.



Cliquer sur **Suivant**, puis sur **Installer** pour lancer l'installation. Patientez jusqu'à la fin du processus.



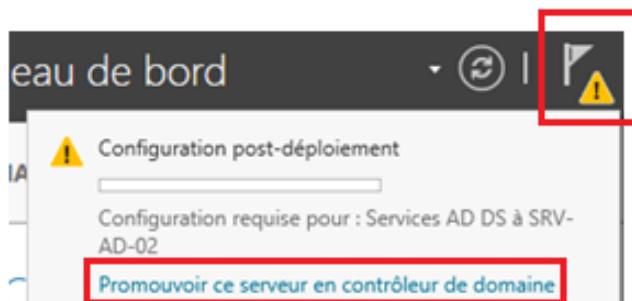
## Installation de l'Active Directory sur le SRV-AD-02

Concernant l'installation de l'Active Directory sur le serveur secondaire, la procédure reste identique à celle du serveur primaire. Seule la configuration diffère légèrement.

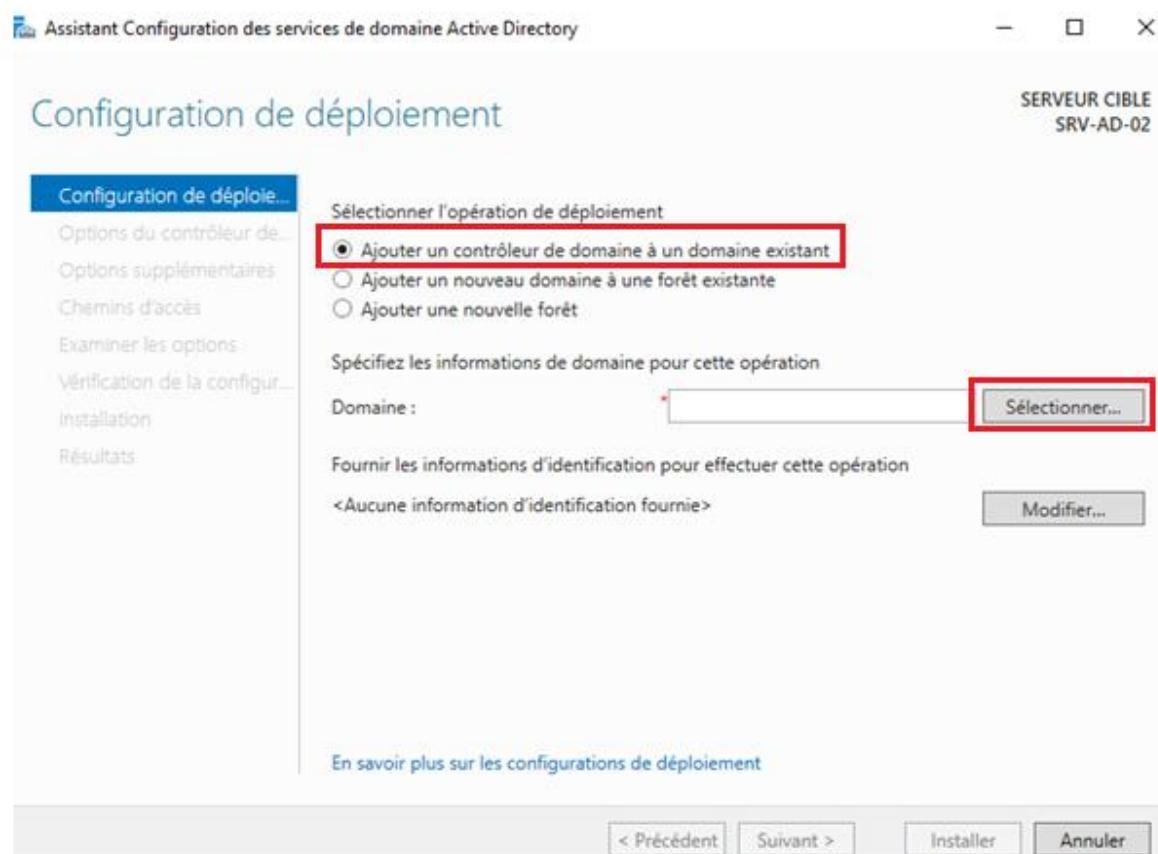


## Configuration de l'Active Directory sur le SRV-AD-02

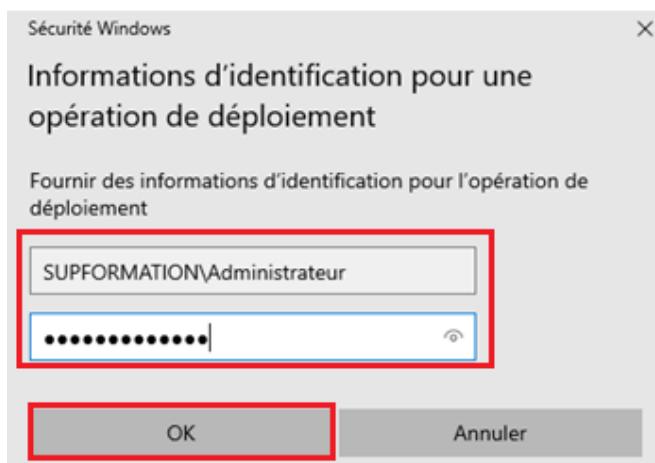
Clique sur l'icône d'avertissement, puis sélectionne « **Promouvoir ce serveur en contrôleur de domaine** » pour lancer l'assistant de configuration.



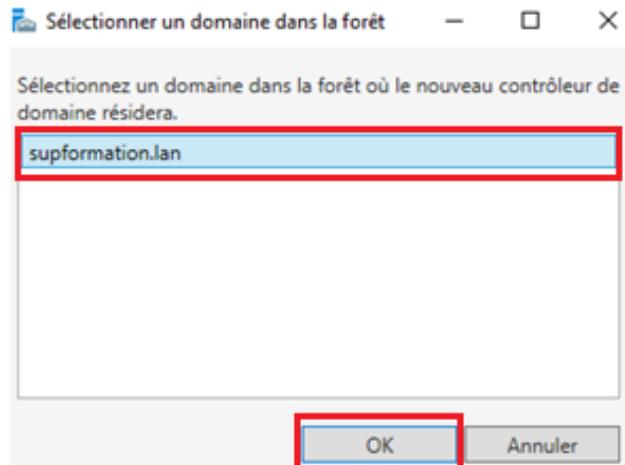
Cocher « Ajouter un contrôleur de domaine à un domaine existant », cliquer sur « Sélectionner... ».



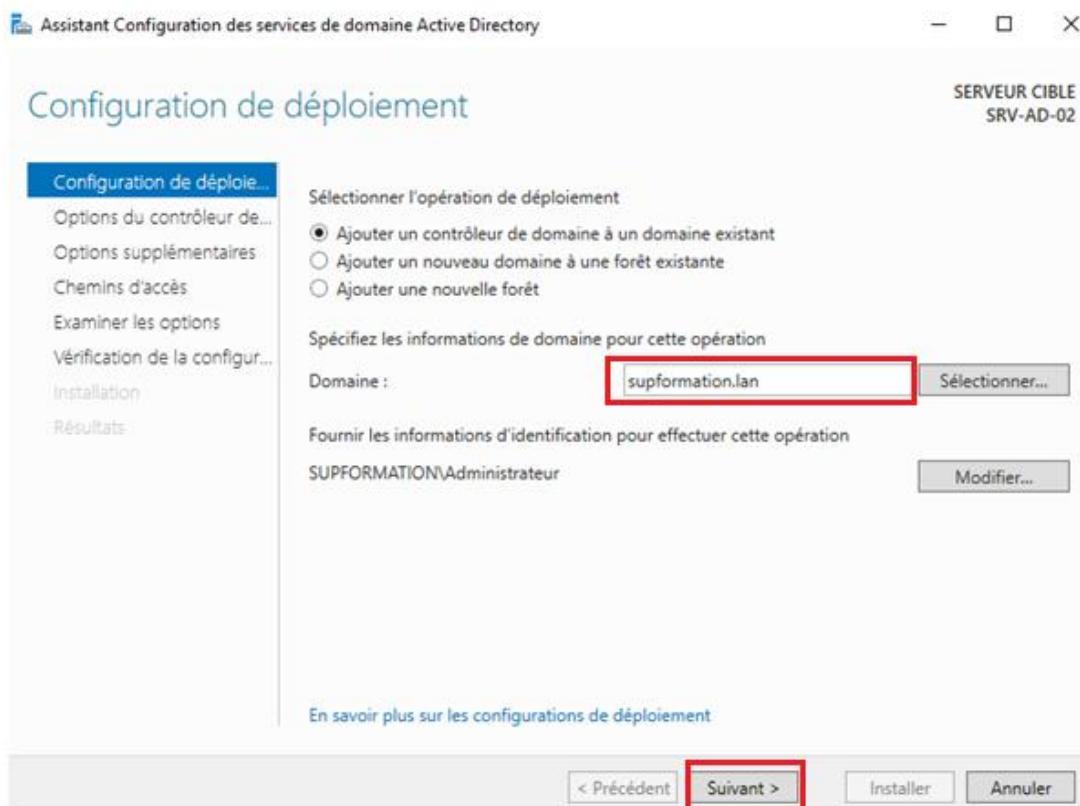
Renseigne les identifiants de l'administrateur du domaine puis clique sur OK pour valider.



Selectionne le domaine **supformation.lan**, puis clique sur **OK** pour continuer l'intégration du contrôleur secondaire.



Une fois le domaine sélectionné, clique sur **Suivant** pour poursuivre la configuration.



Assistant Configuration des services de domaine Active Directory

Configuration de déploiement SERVEUR CIBLE SRV-AD-02

Configuration de déplo...

- Options du contrôleur de...
- Options supplémentaires
- Chemins d'accès
- Examiner les options
- Vérification de la config...
- Installation
- Résultats

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine : supformation.lan Sélectionner...

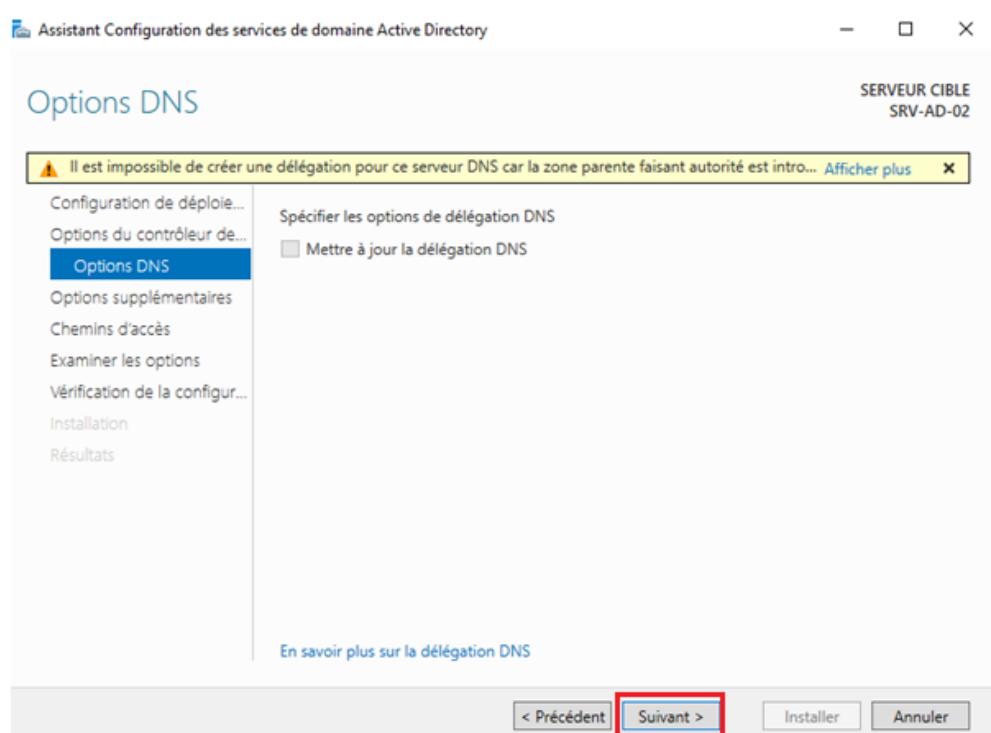
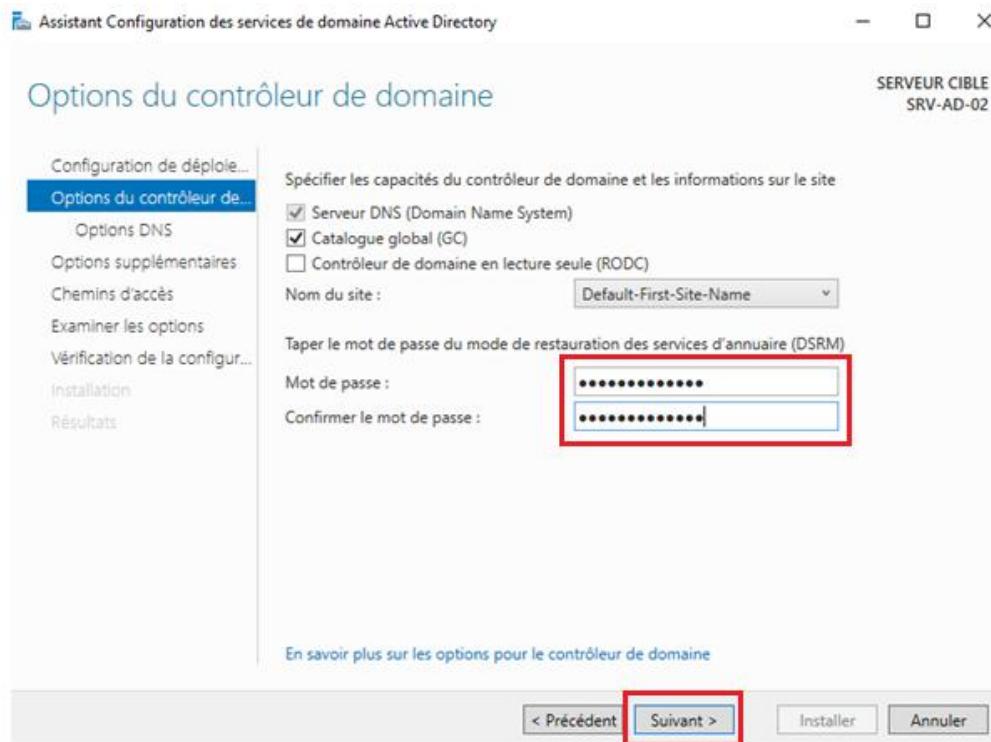
Fournir les informations d'identification pour effectuer cette opération

SUPERFORMATION\Administrateur Modifier...

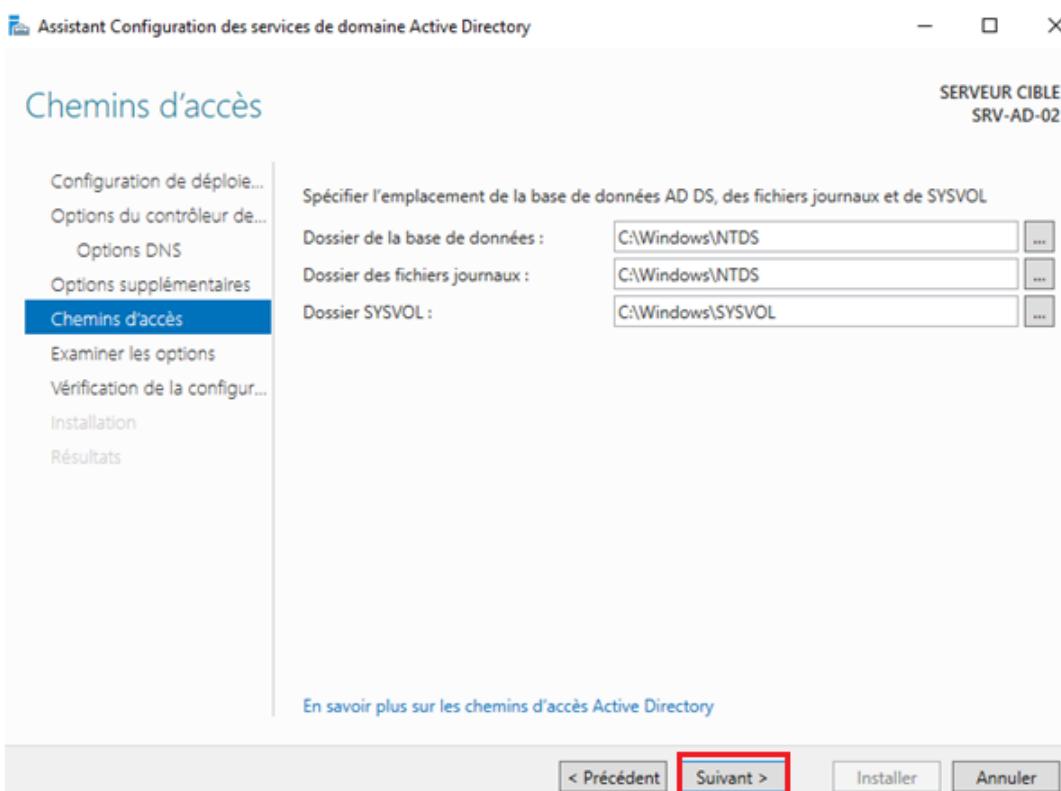
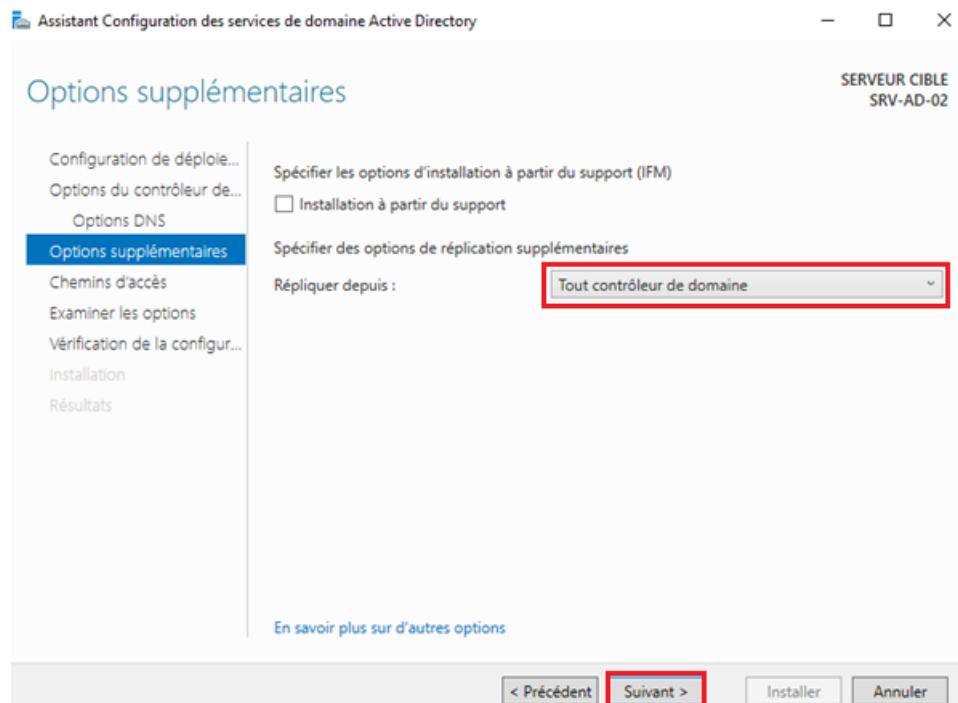
En savoir plus sur les configurations de déploiement

< Précédent Suivant > Installer Annuler

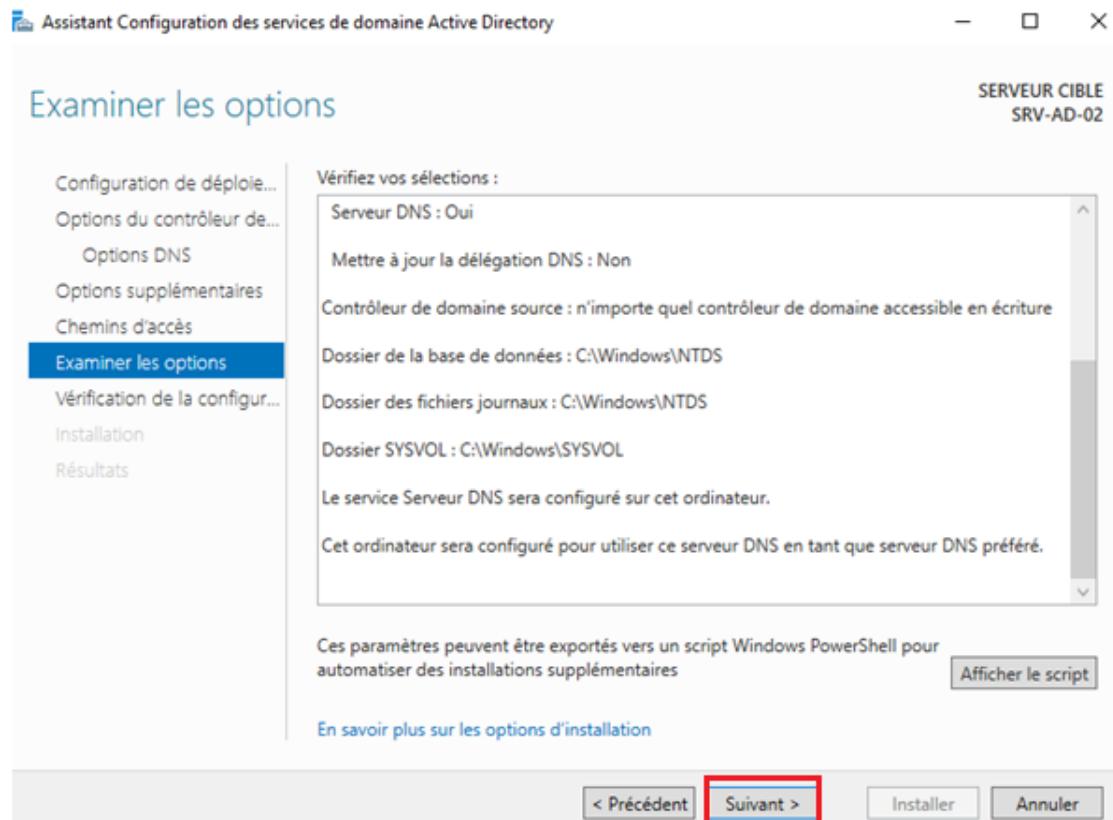
Saisis le mot de passe DSRM comme précédemment, puis clique sur **Suivant** pour continuer l'installation.



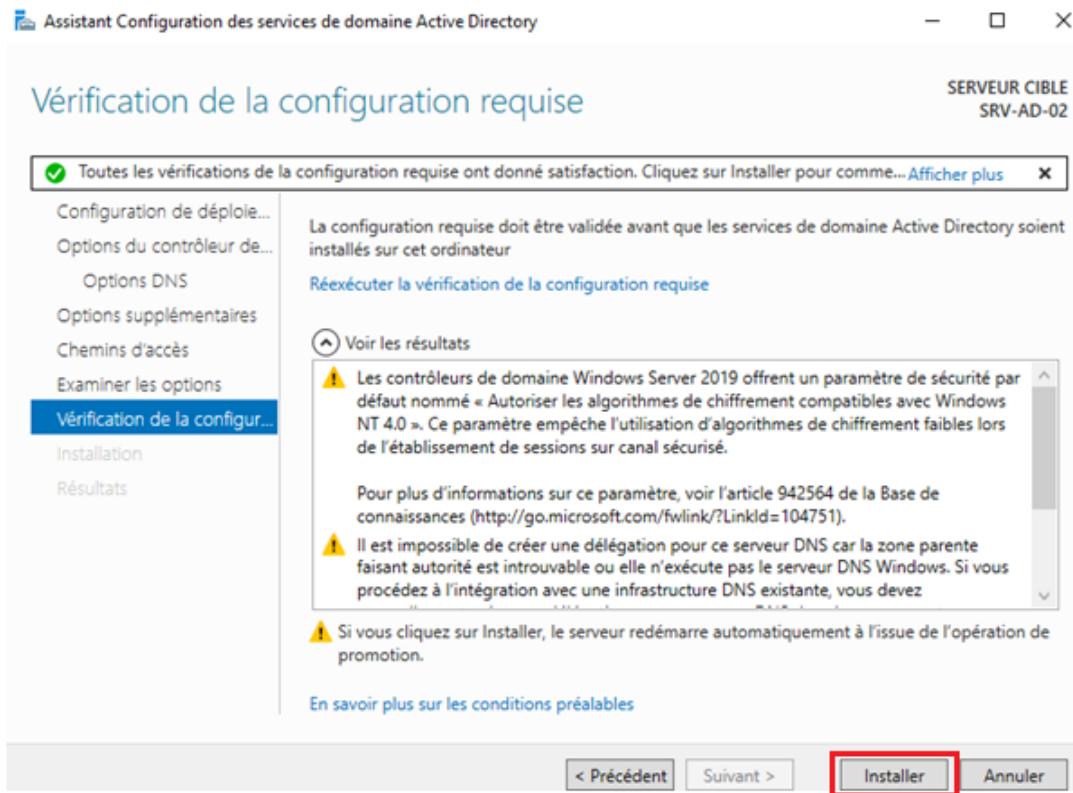
Laisse l'option par défaut « **Tout contrôleur de domaine** », puis cliquer sur **Suivant**.



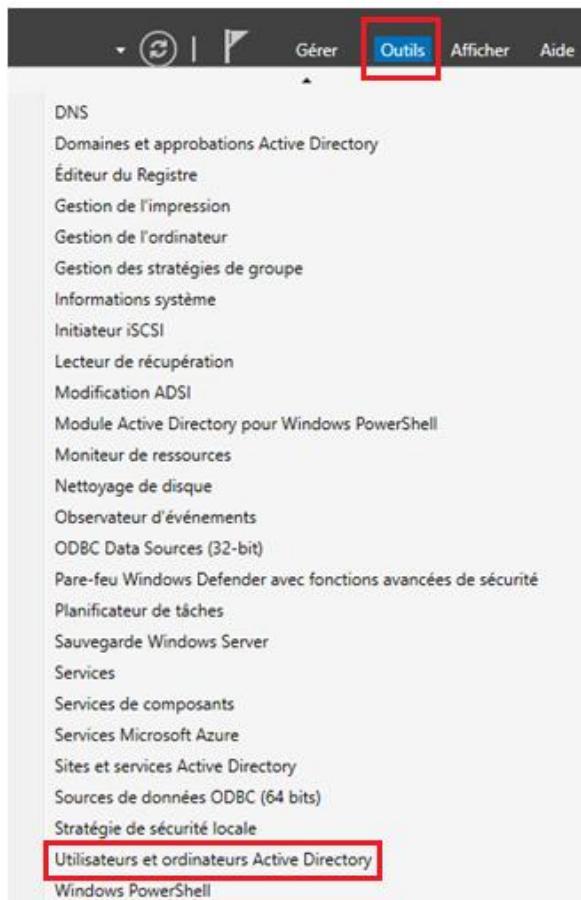
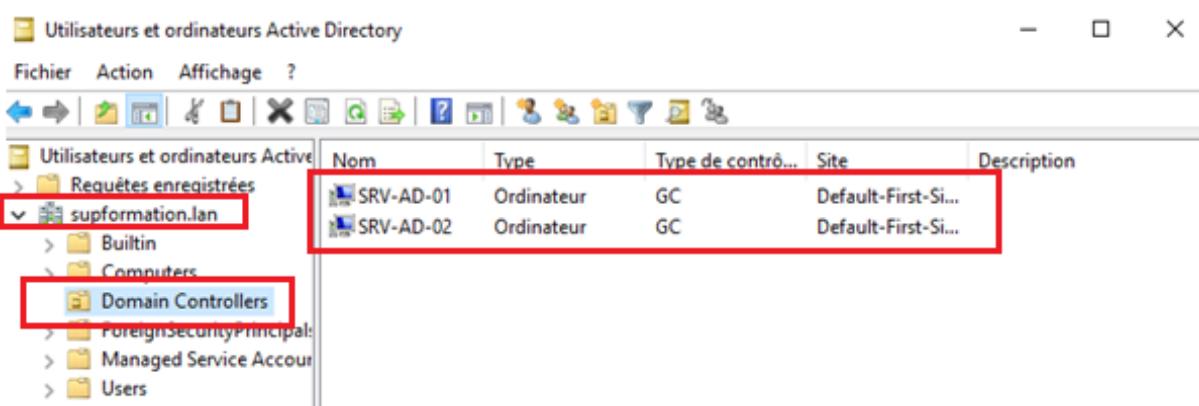
Ceci est un récapitulatif des paramètres choisis. Vérifiez que tout est correct, puis cliquez sur **Suivant**.



Tous les prérequis ont été validés. Cliquez sur "Installer" pour lancer la configuration du serveur secondaire.



Afin de vérifier la bonne jonction du serveur secondaire au domaine, ouvrir le **Gestionnaire de serveur**, puis accéder à **Outils > Utilisateurs et ordinateurs Active Directory**.

Nom	Type	Type de contrôleur	Site	Description
SRV-AD-01	Ordinateur	GC	Default-First-Site...	
SRV-AD-02	Ordinateur	GC	Default-First-Site...	

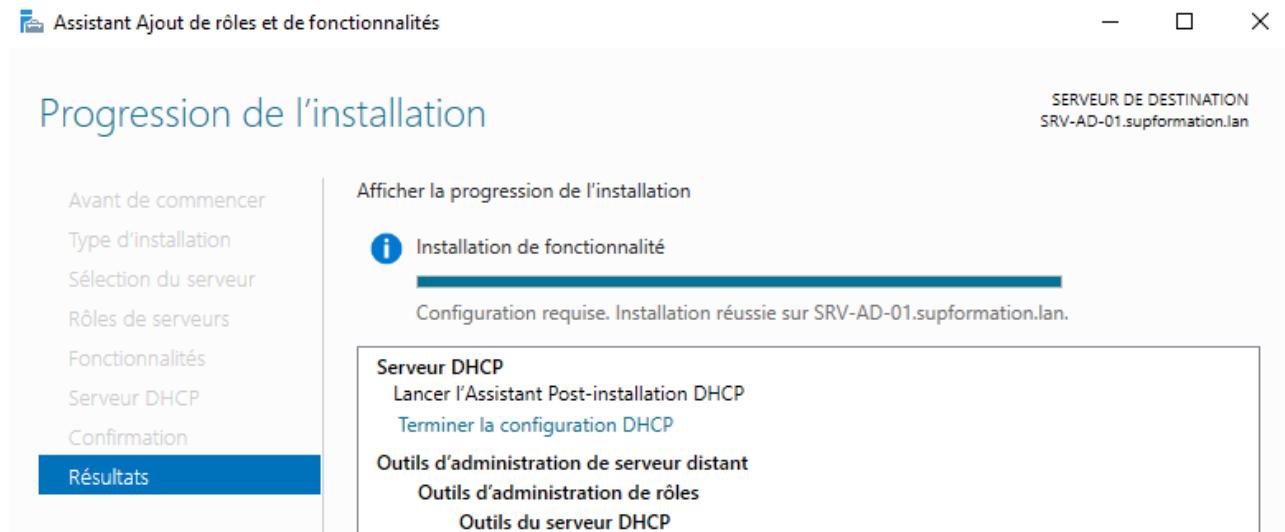
## DHCP – Dynamic Host Configuration Protocol

### 2.4) Installation et configuration du service DHCP avec basculement sur les serveurs SRV-AD-01 et SRV-AD-02

L'installation du rôle DHCP sur le serveur primaire SRV-AD-01 se déroule comme suit :

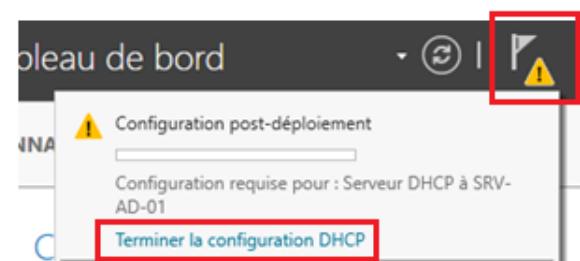
Accéder à **Ajouter des rôles et fonctionnalités**, puis cliquer successivement sur **Suivant** jusqu'à l'étape de sélection du serveur. Sélectionner le serveur concerné, cliquer sur **Suivant**, cocher **Serveur DHCP**, puis cliquer sur **Suivant**.

Continuer avec **Suivant** jusqu'à l'étape **Installer**. Lancer l'installation et cliquer sur **Fermer** une fois celle-ci terminée.



Une fois le rôle DHCP installé, une alerte apparaît dans le tableau de bord.

Cliquez sur "**Terminer la configuration DHCP**" pour finaliser l'installation via l'assistant prévu à cet effet.



**Assistant Configuration post-installation DHCP**

- □ ×

**Description****Description**

Autorisation

Résumé

Les étapes suivantes seront effectuées pour configurer le serveur DHCP sur l'ordinateur cible :

Créez les groupes de sécurité suivants pour la délégation de l'administration du serveur DHCP.

- Administrateurs DHCP
- Utilisateurs DHCP

Autorisez le serveur DHCP sur l'ordinateur cible (s'il appartient au domaine).

&lt; Précédent

**Suivant >**

Valider

Annuler

**Assistant Configuration post-installation DHCP**

- □ ×

**Autorisation****Description**

Autorisation

Résumé

Spécifiez les informations d'identification à utiliser pour autoriser ce serveur DHCP dans les services AD DS.

- Utiliser les informations d'identification de l'utilisateur suivant

Nom d'utilisateur :

- Utiliser d'autres informations d'identification

Nom d'utilisateur :

- Ignorer l'autorisation AD

&lt; Précédent

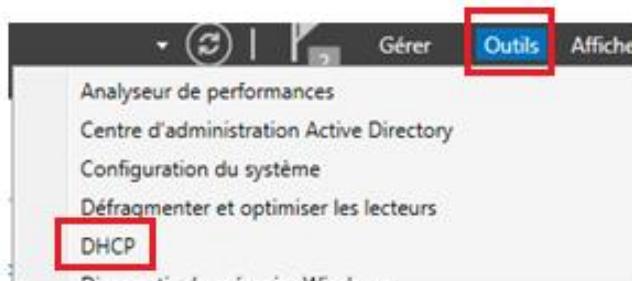
Suivant &gt;

**Valider**

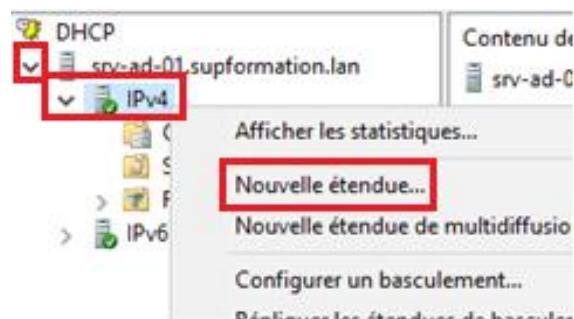
Annuler

## Configuration du protocole DHCP sur le serveur SRV-AD-01

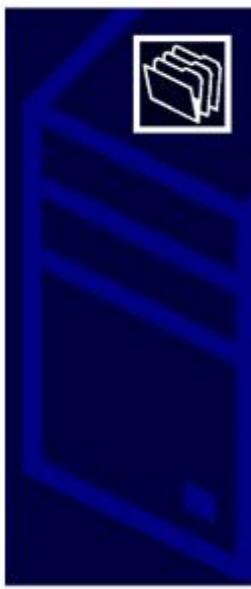
Se rendre dans la console **DHCP** depuis le **Gestionnaire de serveurs** afin de débuter la configuration du service.



Dans la console DHCP, effectuer un clic droit sur "IPv4" puis sélectionner "Nouvelle étendue..." afin de créer une plage d'adresses à distribuer.



Assistant Nouvelle étendue



## Assistant Nouvelle étendue

Cet Assistant vous permet de paramétrer une étendue pour distribuer des adresses IP aux ordinateurs sur le réseau.

Cliquez sur Suivant pour continuer.

< Précédent **Suivant >** Annuler

Commencez par définir le nom de l'étendue ainsi qu'une description (facultative mais utile pour la traçabilité), puis cliquez sur **Suivant**.

Assistant Nouvelle étendue

### Nom de l'étendue

Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.



Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.

Nom :

Description :

< Précédent **Suivant >** Annuler

Définir ici une plage d'adresses IP allant de 192.168.100.100 à 192.168.100.150, avec un masque de sous-réseau en /24, afin de distribuer dynamiquement les adresses aux clients.

Assistant Nouvelle étendue

**Plage d'adresses IP**

Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début :	192 . 168 . 100 . 100
Adresse IP de fin :	192 . 168 . 100 . 150

Paramètres de configuration qui se propagent au client DHCP.

Longueur :	24
Masque de sous-réseau :	255 . 255 . 255 . 0

< Précédent **Suivant >** Annuler

Aucune exclusion n'est nécessaire, cliquer directement sur **Suivant**.

Assistant Nouvelle étendue

**Ajout d'exclusions et de retard**

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCPOFFER.

Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début :	Adresse IP de fin :	Ajouter
Plage d'adresses exclue :		Supprimer
Retard du sous-réseau en millisecondes :		

0

< Précédent **Suivant >** Annuler

Par défaut, la durée du bail DHCP est de 8 jours, ce qui convient à la plupart des environnements de bureau. Cliquer sur Suivant pour continuer.

Assistant Nouvelle étendue

**Durée du bail**

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.



La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours :      Heures :      Minutes :

< Précédent  Annuler

Cocher « Oui, je veux configurer ces options maintenant », puis cliquer sur **Suivant** pour continuer la configuration de l'étendue DHCP.

Assistant Nouvelle étendue

**Configuration des paramètres DHCP**

Vous devez configurer les options DHCP les plus courantes pour que les clients puissent utiliser l'étendue.



Lorsque les clients obtiennent une adresse, ils se voient attribuer des options DHCP, telles que les adresses IP des routeurs (passerelles par défaut), des serveurs DNS, et les paramètres WINS pour cette étendue.

Les paramètres que vous sélectionnez maintenant sont pour cette étendue et ils remplaceront les paramètres configurés dans le dossier Options de serveur pour ce serveur.

Voulez-vous configurer les options DHCP pour cette étendue maintenant ?

- Oui, je veux configurer ces options maintenant  
 Non, je configurerais ces options ultérieurement

< Précédent **Suivant >**

Annuler

Indique l'adresse IP de la passerelle par défaut, ici **192.168.100.254**, afin que les clients puissent communiquer avec les autres équipements du réseau, puis clique sur **Ajouter**, puis **Suivant**.

Assistant Nouvelle étendue

**Routeur (passerelle par défaut)**

Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.



Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

< Précédent  Annuler

Assistant Nouvelle étendue

**Nom de domaine et serveurs DNS**

DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.



Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

Nom du serveur :

Répondre

Adresse IP :

192.168.100.10  
192.168.100.10

Ajouter

Supprimer

Monter

Descendre

< Précédent

**Suivant >**

Annuler

Aucun serveur WINS n'étant utilisé, laisse vide et clique sur **Suivant**.

Assistant Nouvelle étendue

**Serveurs WINS**

Les ordinateurs fonctionnant avec Windows peuvent utiliser les serveurs WINS pour convertir les noms NetBIOS d'ordinateurs en adresses IP.



Entrer les adresses IP ici permet aux clients Windows d'interroger WINS avant d'utiliser la diffusion pour s'enregistrer et résoudre les noms NetBIOS.

Nom du serveur :

Résoudre

Adresse IP :

Ajouter  
Supprimer  
Monter  
Descendre

Pour modifier ce comportement pour les clients DHCP Windows, modifiez l'option 046, type de nœud WINS/NBT, dans les options de l'étendue.

< Précédent

**Suivant >**

Annuler

Coche « Oui, je veux activer cette étendue maintenant », puis clique sur **Suivant**.

Assistant Nouvelle étendue

**Activer l'étendue**

Les clients ne peuvent obtenir des baux d'adresses que si une étendue est activée.



Voulez-vous activer cette étendue maintenant ?

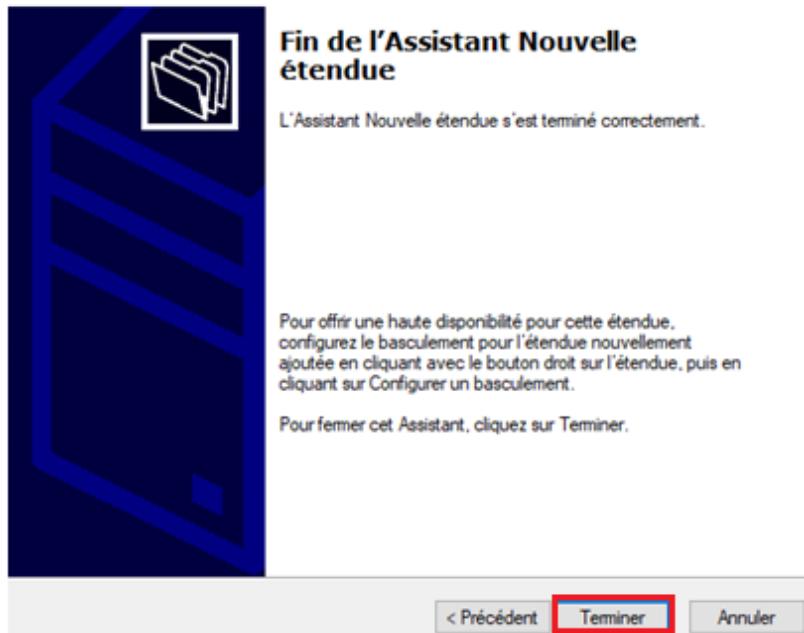
Oui, je veux activer cette étendue maintenant

Non, j'activerai cette étendue ultérieurement

< Précédent

**Suivant >**

Annuler

**Assistant Nouvelle étendue**


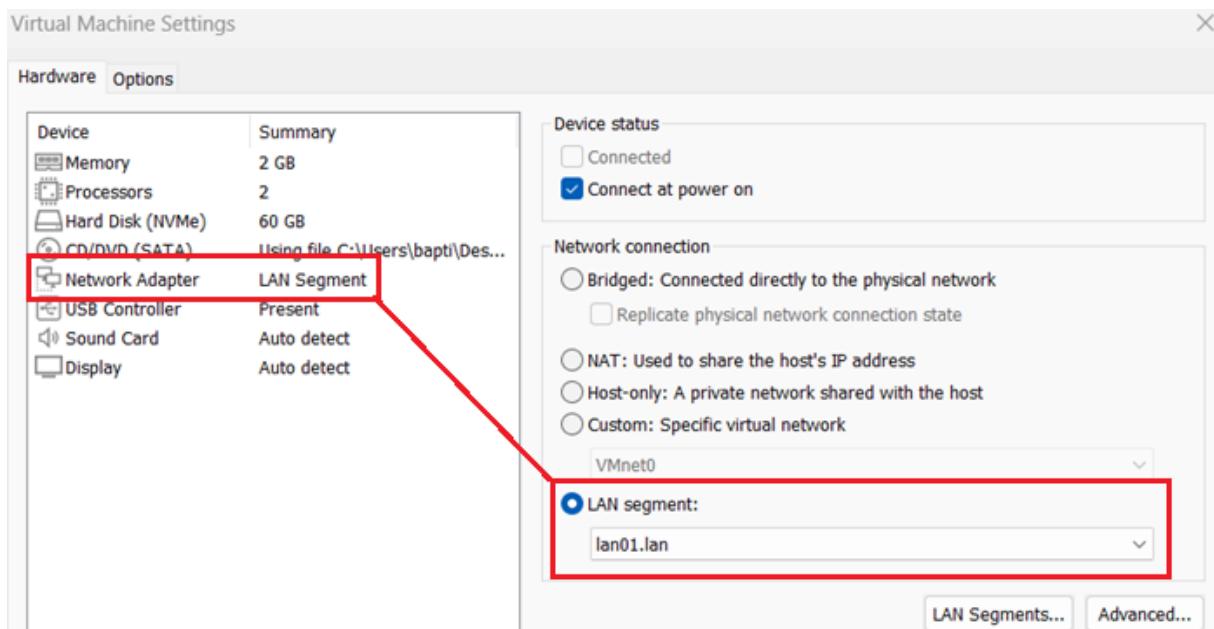
Contenu du serveur DHCP	État
<ul style="list-style-type: none"> <li>Options de serveur</li> <li>Étendue [192.168.100.0] supformation_ét... ** Actif **</li> <li>Stratégies</li> <li>Filtres</li> </ul>	

**DHCP**

- srv-ad-01.supformation.lan
  - IPv4
    - Options de serveur
    - Étendue [192.168.100.0] supformation\_étendue
      - Pool d'adresses
      - Baux d'adresses
      - Réservations
      - Options d'étendue
      - Stratégies
    - Stratégies
    - Filtres
  - IPv6

## 2.5) Test du fonctionnement DHCP sur un poste client

On va en profiter pour créer et démarrer la VM *USER-Test*, qui servira à vérifier le bon fonctionnement du DHCP configuré sur nos serveurs, soit **PC01** dans notre tableau d'adressage.



Une fois l'installation terminée, profitez-en pour renommer directement la machine en **PC01**, afin de rester cohérent avec votre plan de nommage.

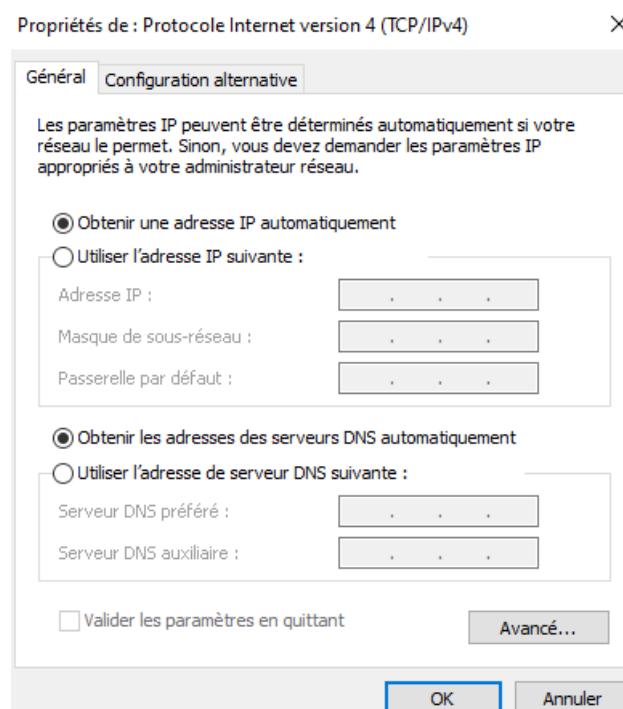
Sur PC01 :

```
C:\Users\Administrateur>ipconfig /all
```

## Configuration IP de Windows

```
Nom de l'hôte . . . . . : PC01
Suffixe DNS principal . . . . . :
Type de noeud. . . . . : Hybride
Routage IP activé . . . . . : Non
Proxy WINS activé . . . . . : Non
Liste de recherche du suffixe DNS.: supformation.lan
```

## Carte Ethernet Ethernet0 :



Depuis les baux d'adresses de **SRV-AD-01** du DHCP :

	Adresse IP du client	Nom	Expiration du bail	Type	ID unique	Actions
	192.168.100.100	PC01.supformation...	10/05/2025 19:28:17	DHCP	000c29ea6	Baux d'adresses

Actions menu:

- Autres actions ▾

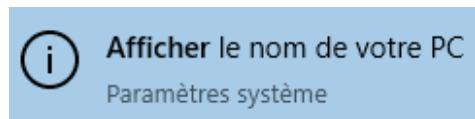
Left sidebar (DHCP interface):

- DHCP
- srv-ad-01.supformation.lan
  - IPv4
    - Options de serveur
    - Étendue [192.168.100.0] supfo
      - Pool d'adresses
      - Baux d'adresses
    - Réservations
      - Options d'étendue
      - Stratégies
    - Stratégies
    - Filtres
  - IPv6
    - Options de serveur

## 2.6) Ajout des clients Windows au domaine supformation.lan

Le poste **PC01** étant bien configuré en DHCP, nous allons maintenant l'ajouter au domaine **supformation.lan**.

Dans la barre de recherche Windows, tapez "**Afficher le nom de votre PC**" puis appuyez sur **Entrée**.



Puis cliquez sur **Paramètres avancés du système**.

**Paramètres associés**

Gestionnaire de périphériques

Bureau à distance

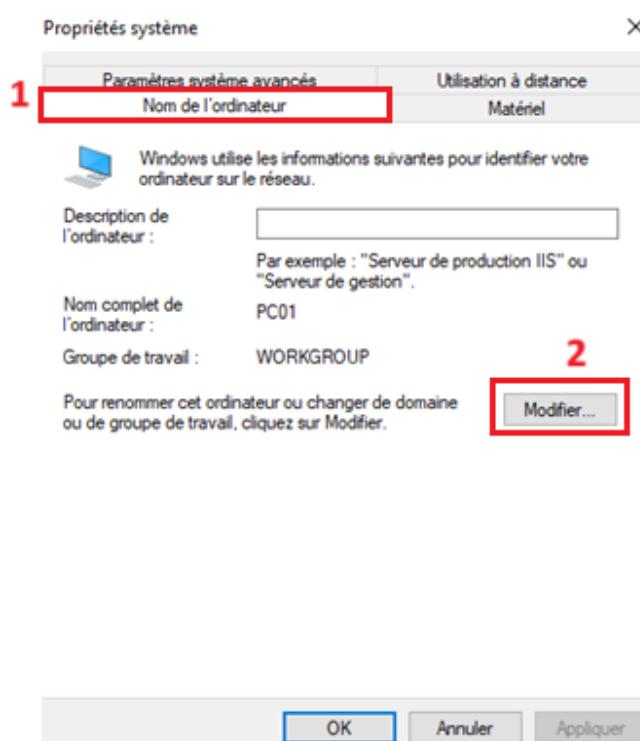
Protection du système

**Paramètres avancés du système**

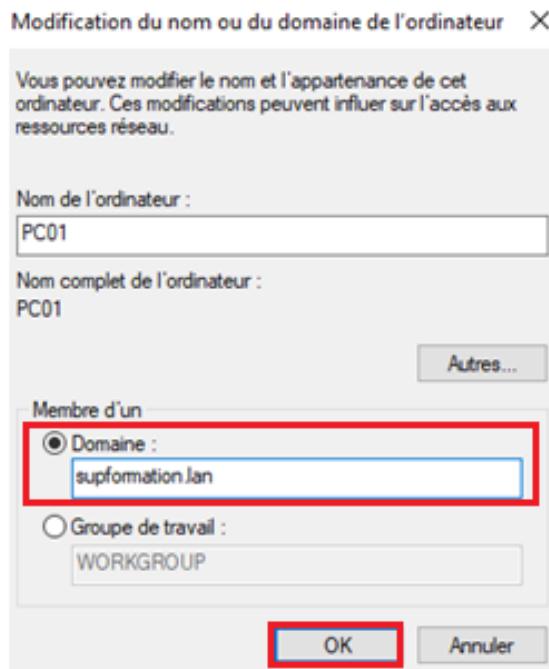
Renommer ce PC (avancé)

Paramètres graphiques

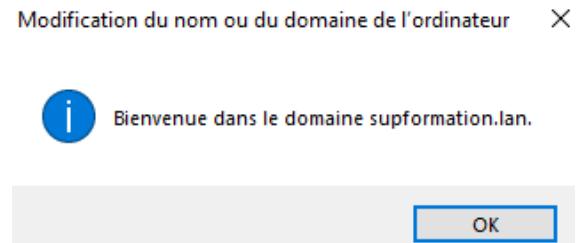
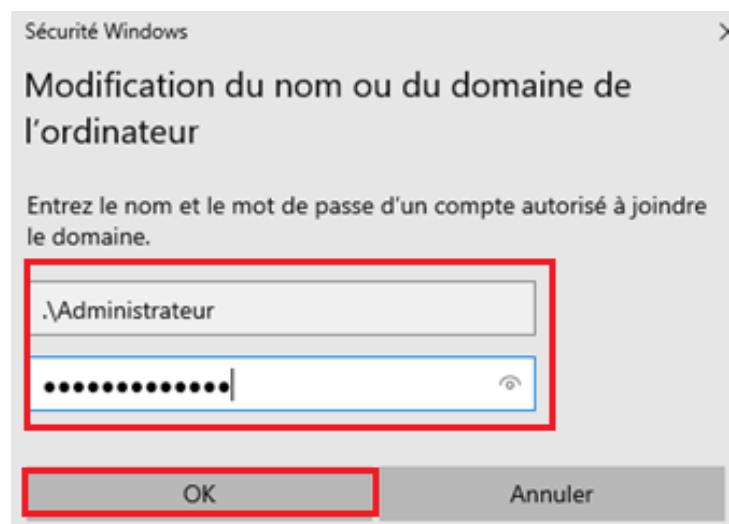
Dans l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier** pour l'ajouter au domaine.



Cochez **Domaine**, entrez supformation.lan, puis cliquez sur **OK** pour lancer la jonction.



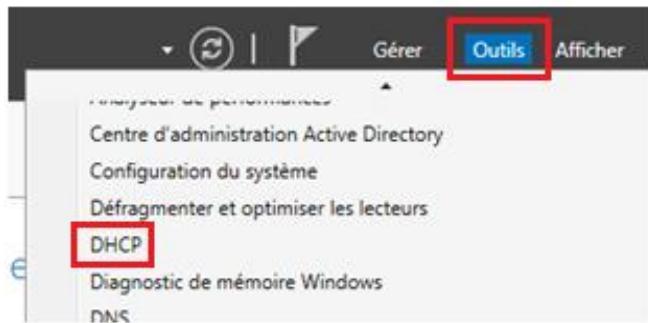
Indiquez un compte autorisé pour joindre le domaine, comme Administrateur du domaine, puis cliquez sur **OK**.



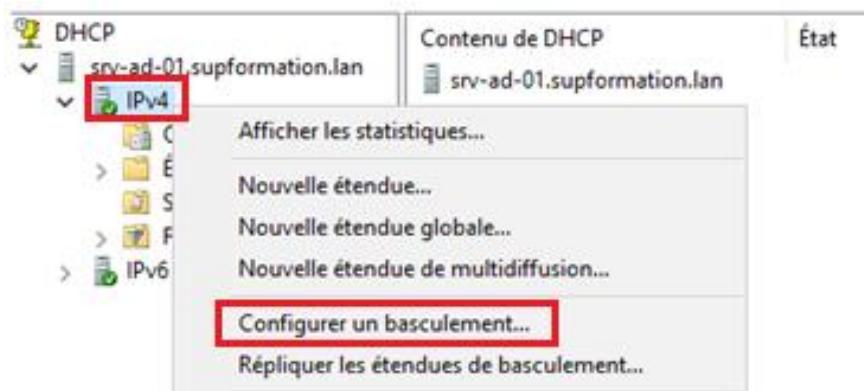
Le message confirme que l'ordinateur a bien rejoint le domaine supformation.lan. Vous pouvez maintenant redémarrer le poste pour finaliser l'intégration.

## Configuration du basculement du DHCP sur le serveur SRV-AD-01

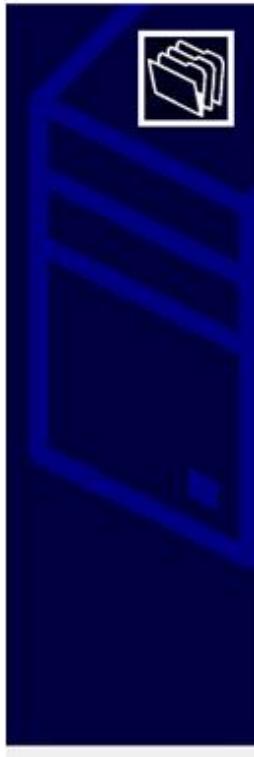
Ouvrir la console via Outils > DHCP depuis le Gestionnaire de serveur.



Faites un clic droit sur IPv4, puis sélectionnez **Configurer un basculement...** pour démarrer l'assistant.



Configurer un basculement



Introduction au basculement DHCP

Le basculement DHCP permet la haute disponibilité des services DHCP en synchronisant les informations des deux d'adresses IP entre deux serveurs DHCP. Le basculement DHCP fournit également un équilibrage de charge en matière de requêtes DHCP.

Cet Assistant vous guide tout au long de la configuration du basculement DHCP. Sélectionnez dans la liste suivante les étendues disponibles pouvant être configurées pour une haute disponibilité. Les étendues déjà configurées pour une haute disponibilité ne figurent pas dans la liste ci-dessous.

Etendues disponibles :  Sélectionner tout

192.168.100.0

< Précédent **Suivant >** Annuler

Depuis SRV-AD-01, ajoute SRV-AD-02 comme serveur partenaire pour le basculement DHCP, puis clique sur **Suivant**.

Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement



Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire :

Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

**Ajouter un serveur**

Ajouter un serveur

?

X

Sélectionnez un serveur que vous voulez ajouter à votre console.

Ce serveur :

**Parcourir...**

Ce serveur DHCP autorisé :

Nom	Adresse IP
srv-ad-01.supformation.lan	192.168.100.10
srv-ad-02.supformation.lan	192.168.100.20

OK

Annuler

Sélectionnez un ordinateur

X

Sélectionnez le type de cet objet :

un ordinateur

**Types d'objets...**

À partir de cet emplacement :

supformation.lan

**Emplacements...**

Entrez le nom de l'objet à sélectionner ([exemples](#)) :

**srv**

**Vérifier les noms**

**Avancé...**

**OK**

Annuler

**Noms multiples trouvés**
X

Plusieurs objets correspondent au nom d'objet suivant : "srv". Sélectionnez un nom dans la liste ou cliquez sur Annuler pour entrer un nouveau nom.

**Noms correspondants :**

Nom	Description	Dossier
SRV-AD-01		supformation lan/Domain Contr...
<b>SRV-AD-02</b>		supformation lan/Domain Contr...


**Configurer un basculement**
**Spécifier le serveur partenaire à utiliser pour le basculement**


Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire



Réutiliser les résultats de basculement (éventuellement configurés avec ce serveur [le cas échéant]).

Coche l'option *Équilibrage de charge*, laisse la répartition à 50/50 et désactive l'authentification du message. Clique sur **Suivant**.

Configurer un basculement

Créer une relation de basculement



Créer une relation de basculement avec le partenaire srv-ad-02

Nom de la relation :

Délai de transition maximal du client (MCLT) :  heures  minutes

Mode :

Pourcentage d'équilibrage de charge

Serveur local :	<input type="text" value="50"/> %
Serveur partenaire :	<input type="text" value="50"/> %

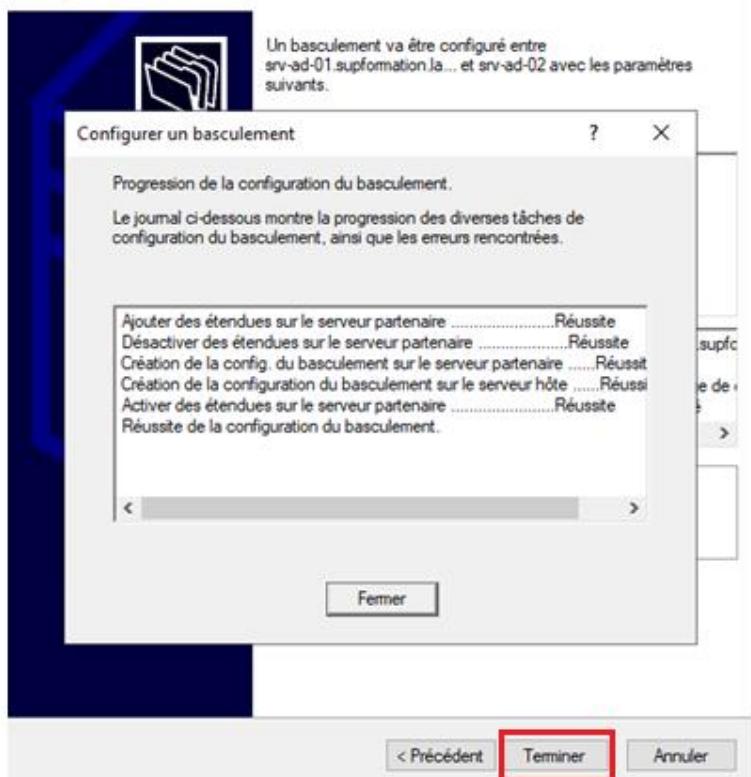
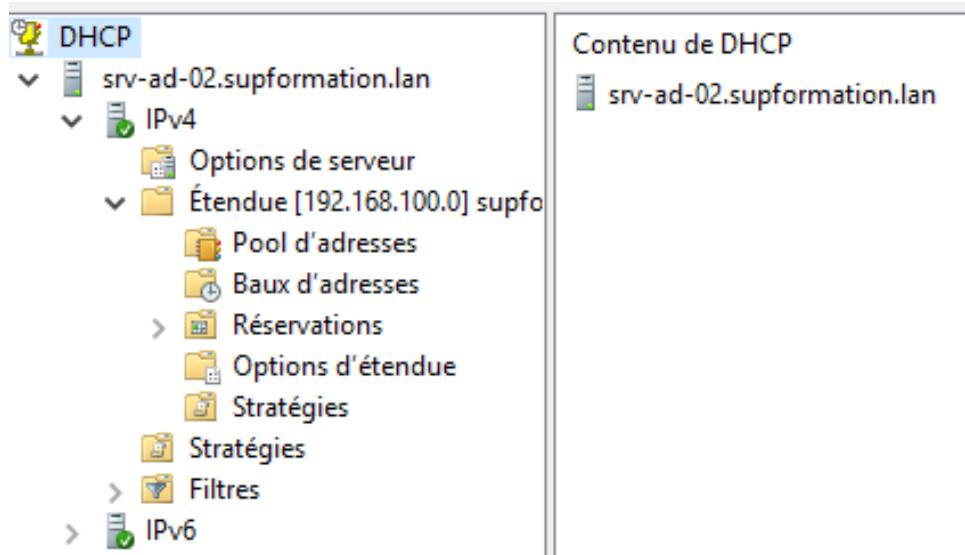
Intervalle de basculement d'état :  minutes

Activer l'authentification du message

Secret partagé :

[< Précédent](#) [Suivant >](#) [Annuler](#)

Configurer un basculement

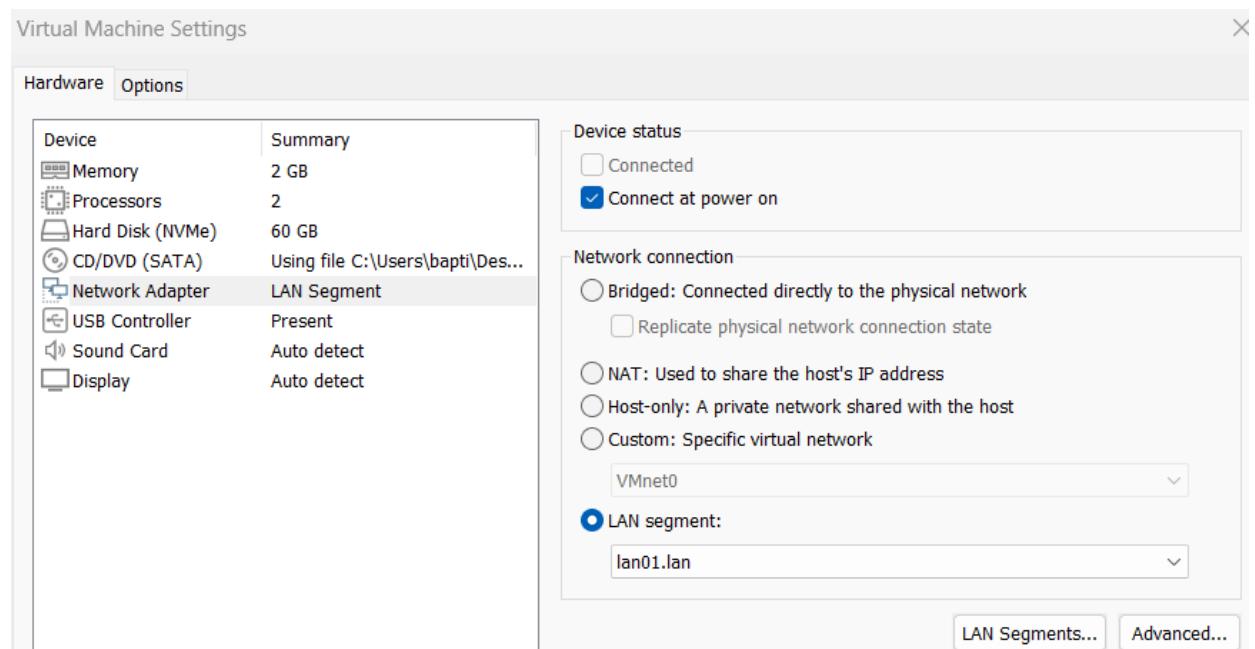
The screenshot shows the Windows Server Management Console for DHCP. On the left, the navigation pane shows a tree structure under "DHCP". The path selected is "srv-ad-02.supformation.lan > IPv4 > Étendue [192.168.100.0] supfo". The right pane is titled "Contenu de DHCP" and displays the selected scope: "srv-ad-02.supformation.lan".

## Serveur WSUS

### 2.7) Installation et configuration du service WSUS

Nous allons créer la machine virtuelle **SRV-WSUS**, dédiée au rôle *Windows Server Update Services*, afin d'optimiser les performances, garantir une meilleure lisibilité de l'infrastructure et respecter les bonnes pratiques d'isolement des rôles ; cette VM sera configurée selon les caractéristiques définies dans notre tableau d'adressage, puis jointe au domaine **supformation.lan**.

En entreprise, il est recommandé d'ajouter un second disque dédié au serveur WSUS afin de stocker efficacement toutes les mises à jour sans saturer le disque principal du système.



Propriétés de : Protocole Internet version 4 (TCP/IPv4) X**Général**

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :

192 . 168 . 100 . 17

Masque de sous-réseau :

255 . 255 . 255 . 0

Passerelle par défaut :

192 . 168 . 100 . 254

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

192 . 168 . 100 . 10

Serveur DNS auxiliaire :

. . .

Valider les paramètres en quittant

Avancé...

OK

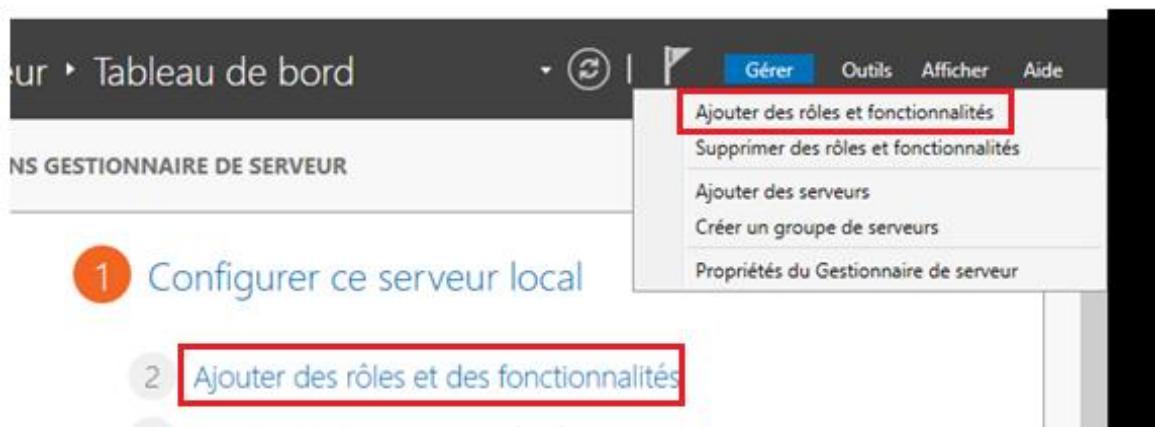
Annuler

Modification du nom ou du domaine de l'ordinateur X

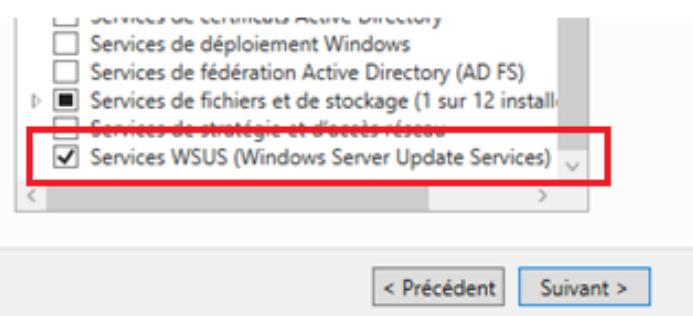
Bienvenue dans le domaine supformation.lan.

OK

Sur le serveur SRV-WSUS, ouvrir le **Gestionnaire de serveur**, puis cliquer sur **Ajouter des rôles et des fonctionnalités**.



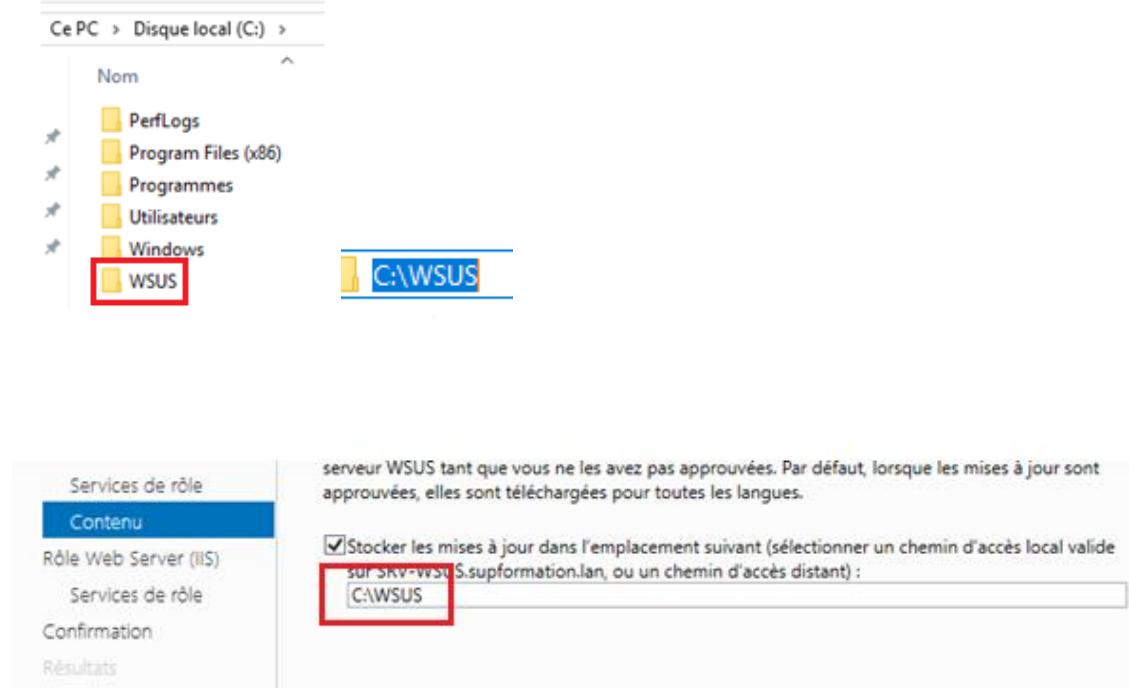
Passer les premiers écrans en cliquant sur **Suivant**, puis cocher la fonctionnalité « **Services WSUS (Windows Server Update Services)** ».



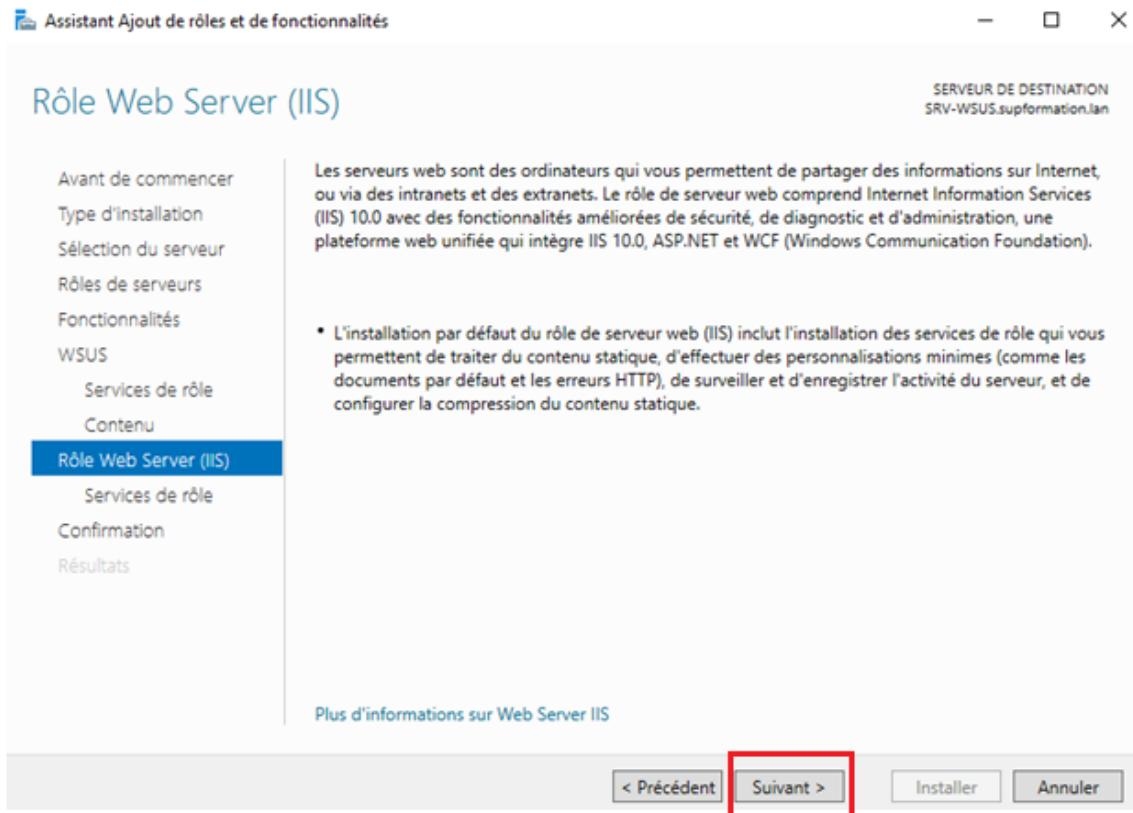
**Suivant** à plusieurs reprises, coche ensuite les services de rôle « **WID Connectivity** » et « **WSUS Services** », puis clique sur **Suivant**.

- 
- WID Connectivity**
  - WSUS Services**
  - SQL Server Connectivity

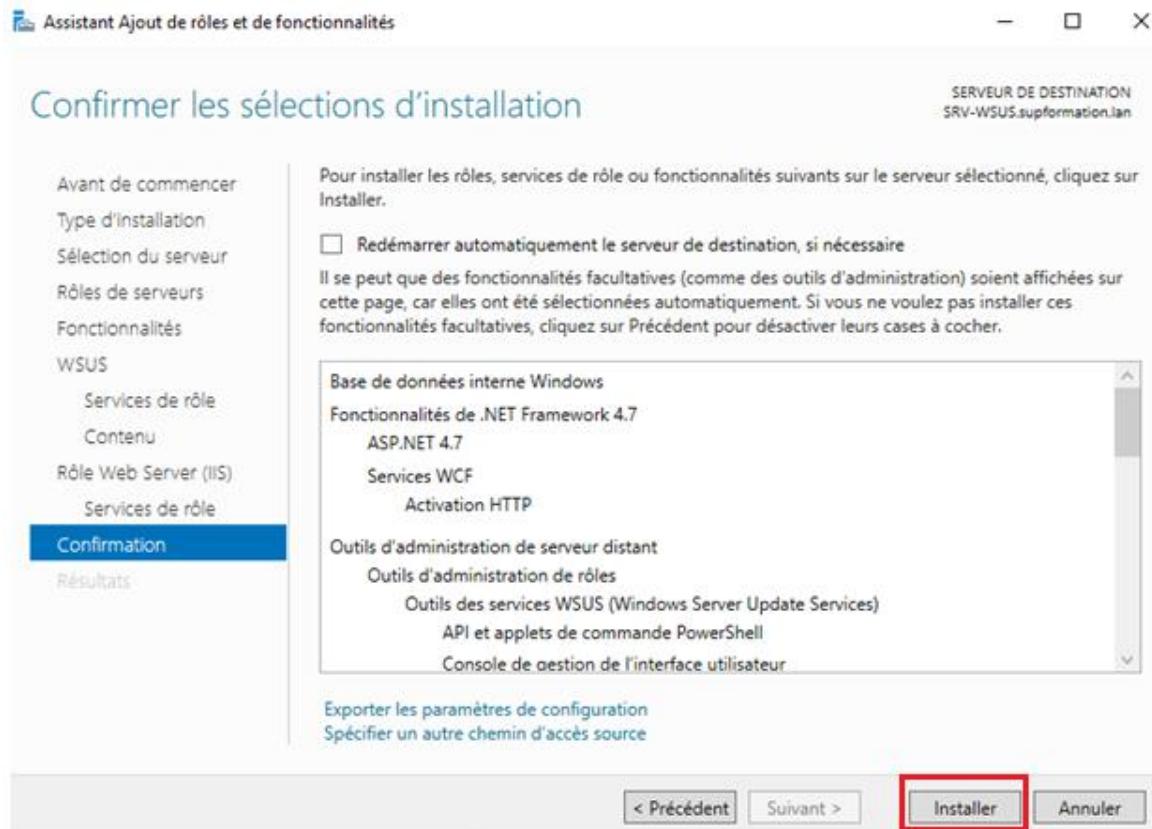
Ici, ne disposant que d'un seul disque, nous créons un dossier dédié sur celui-ci, par exemple C:\WSUS, puis nous l'indiquons comme chemin de stockage avant de cliquer sur **Suivant**.



Le rôle **Web Server (IIS)** est requis pour WSUS car il sert à distribuer les mises à jour aux clients via http, donc **Suivant**.



Cliquez sur **Installer** afin de lancer le processus d'installation des rôles sélectionnés, puis sur **Fermer** une fois l'installation complétée.



#### Afficher la progression de l'installation

##### Installation de fonctionnalité

Configuration requise. Installation réussie sur SRV-WSUS.supformation.lan.

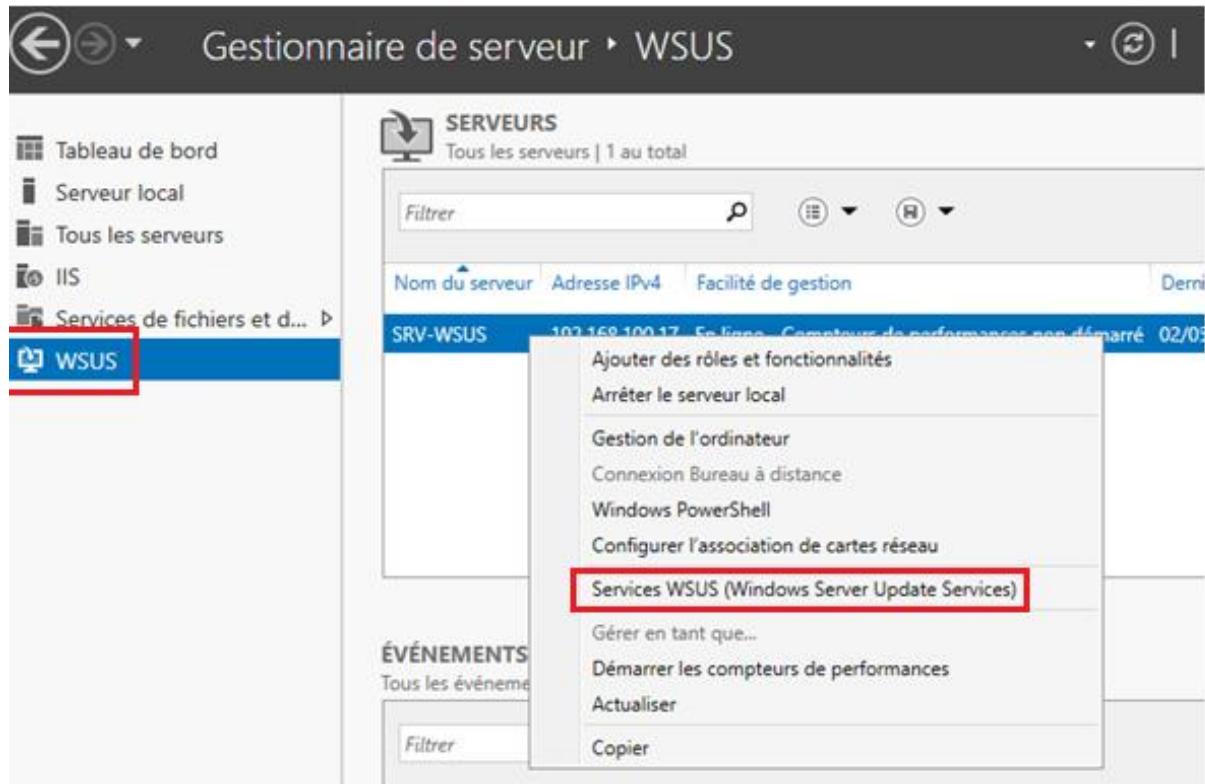
## Configuration du service WSUS

Après l'installation, une alerte apparaît dans le Gestionnaire de serveur, cliquer sur "**Lancer les tâches de post-installation**" pour finaliser le déploiement du service WSUS.

Le rôle WSUS est désormais installé, mais il n'est pas encore opérationnel.

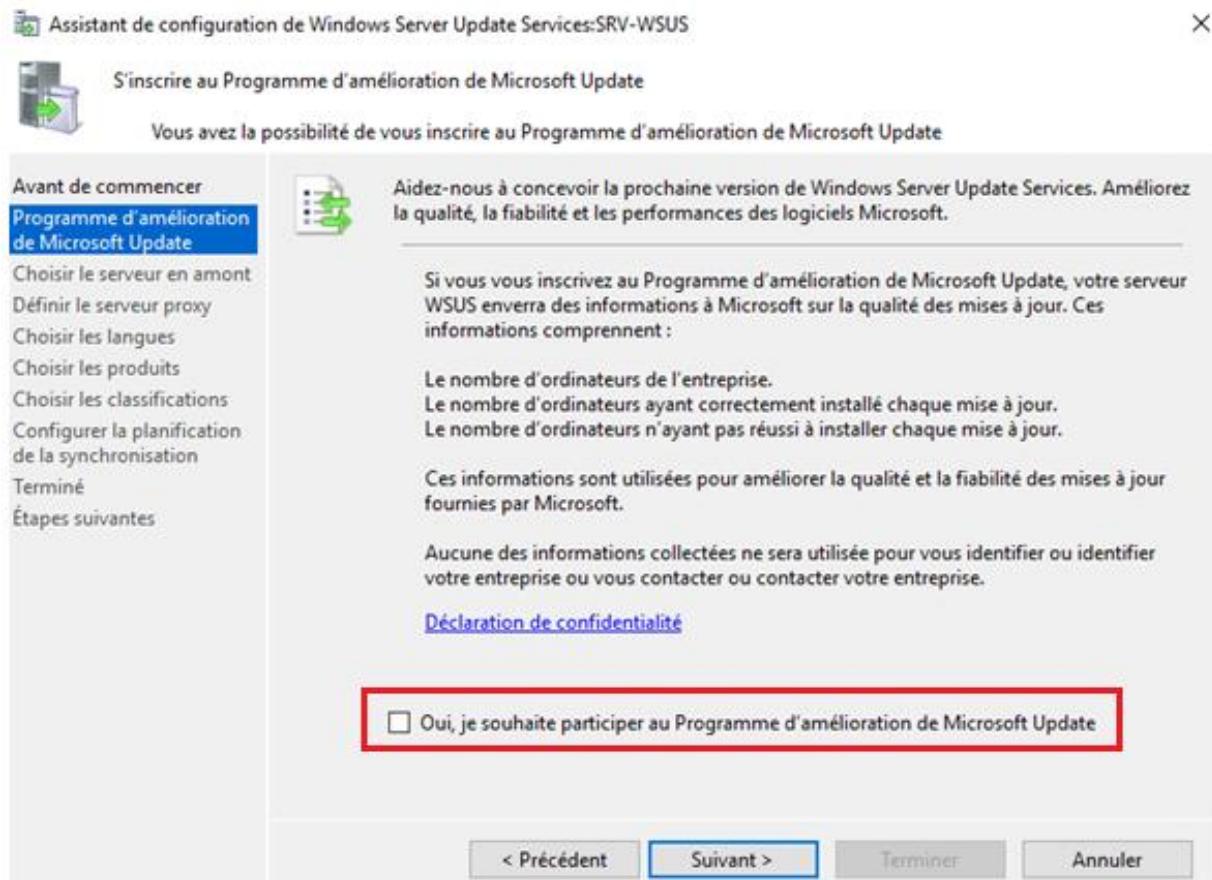
Il est nécessaire de procéder à sa configuration initiale ainsi qu'à une première synchronisation avec les serveurs de Microsoft.

Pour cela, ouvrir le **Gestionnaire de serveur**, cliquer sur **WSUS** dans le menu de gauche, puis effectuer un **clic droit** sur le nom du serveur et sélectionner **Service WSUS**.

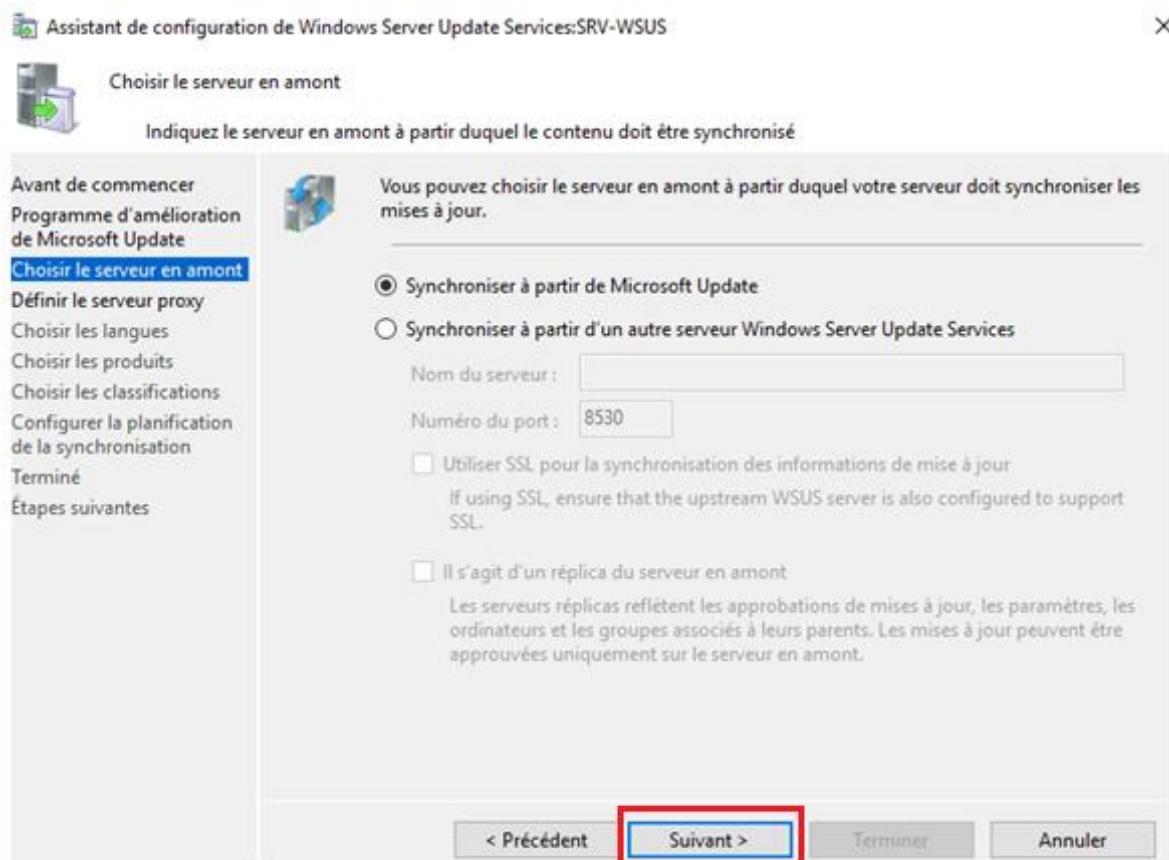


L'assistant de configuration s'ouvre automatiquement. Cliquer sur **Suivant** pour commencer.

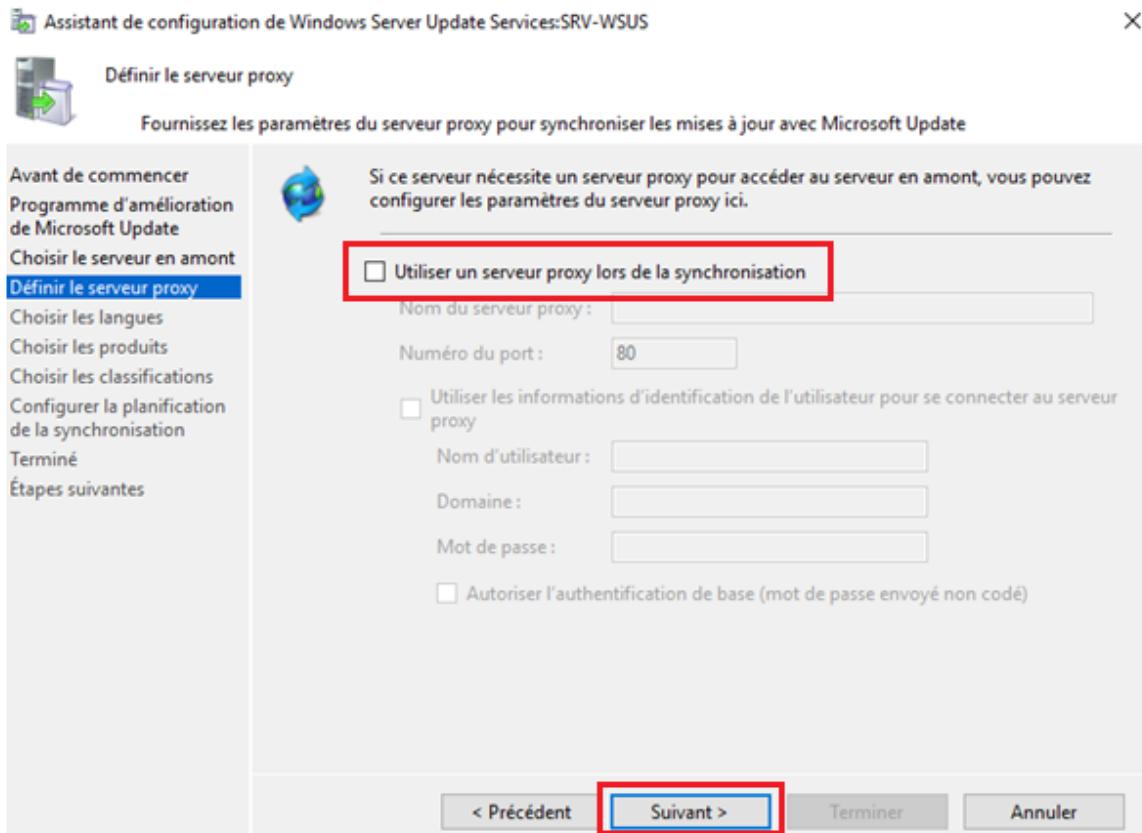
À l'étape de collecte de données, ne pas cocher la case si l'on ne souhaite pas envoyer d'informations à Microsoft, puis cliquer sur **Suivant**.



Ne disposant que d'un seul serveur WSUS, laisser l'option « **Synchroniser à partir de Microsoft Update** » cochée, puis cliquer sur **Suivant**.

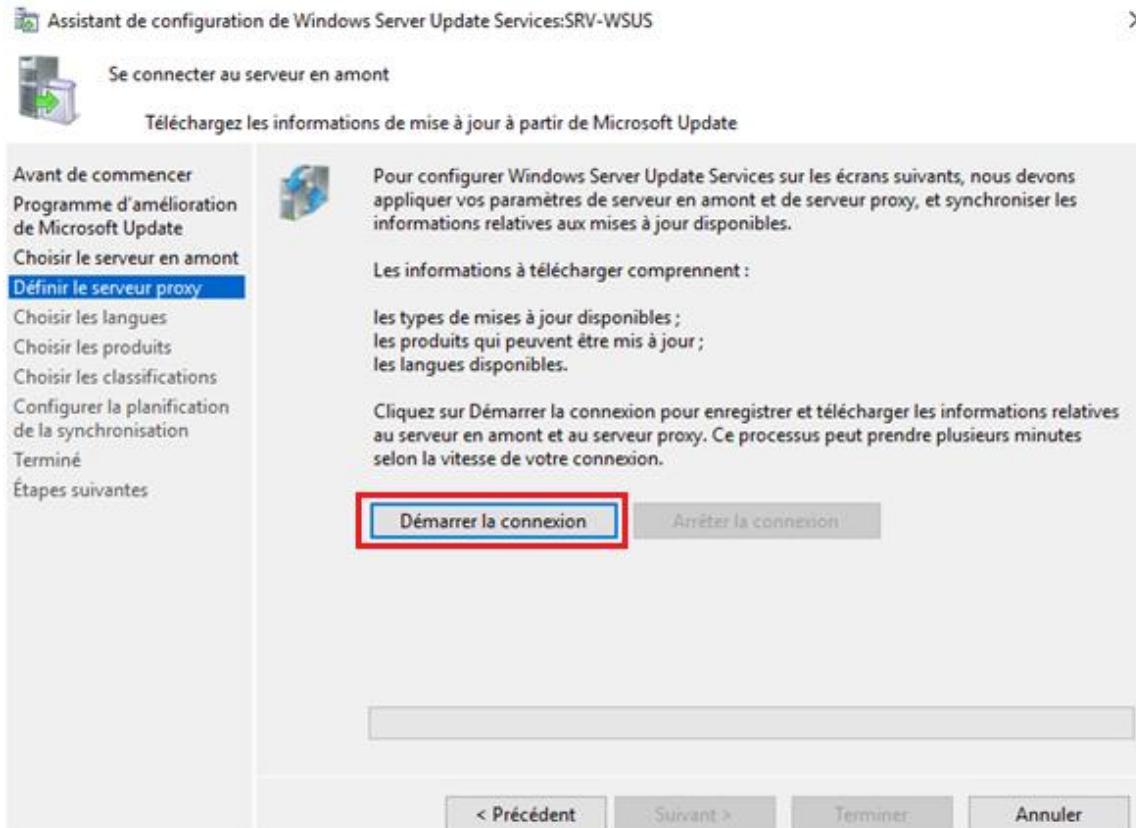


Indiquer si une connexion via un serveur proxy est nécessaire pour accéder à Internet.  
Dans notre cas, aucun proxy n'est requis, cliquer donc sur **Suivant**.



Cette étape permet d'initier la première synchronisation avec les serveurs Microsoft Update afin de récupérer la liste des types de mises à jour disponibles.

Cliquer sur **Démarrer la connexion** pour lancer le processus.

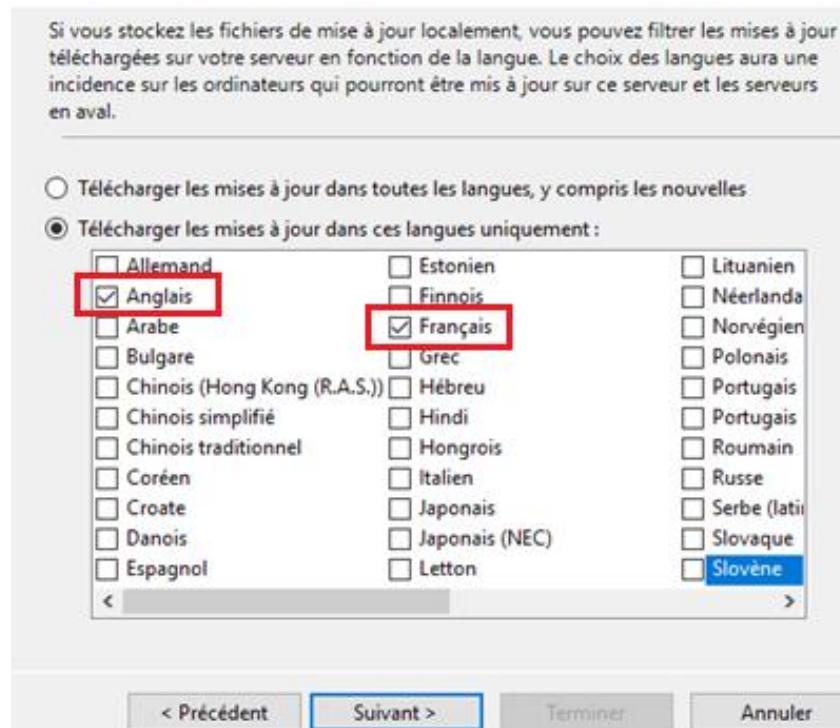


⚠ Cette étape peut être particulièrement longue et durer plusieurs dizaines de minutes.  
Une fois la connexion établie, cliquer sur **Suivant**.

Sélectionner les langues des mises à jour.

L'**anglais** est activé par défaut et ne peut pas être désélectionné.

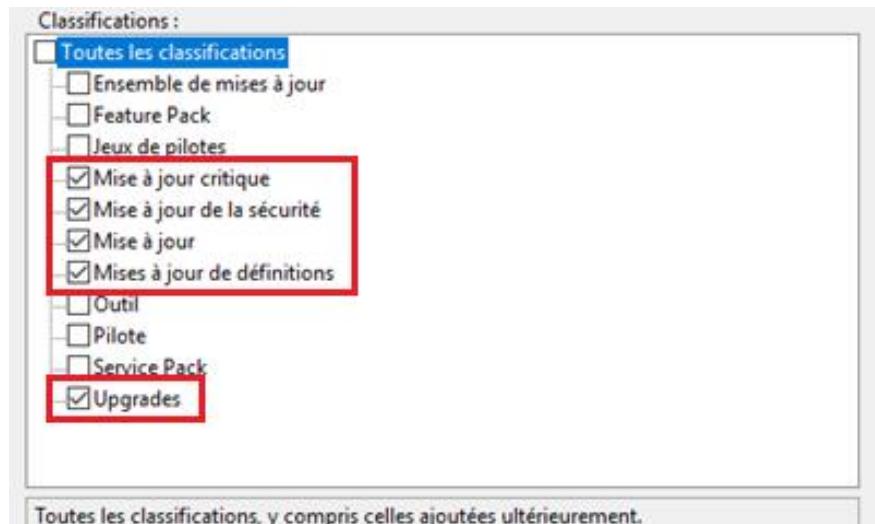
Cocher **français** en complément, puis cliquer sur **Suivant**.



À l'étape de sélection des produits, une liste complète des produits Microsoft est proposée. Cocher uniquement ceux nécessaires ; dans notre cas, « **Windows 10, version 1903 and later** », puis cliquer sur **Suivant**.



Cette étape concerne les **classifications**, c'est-à-dire les types de mises à jour que le serveur WSUS devra gérer.



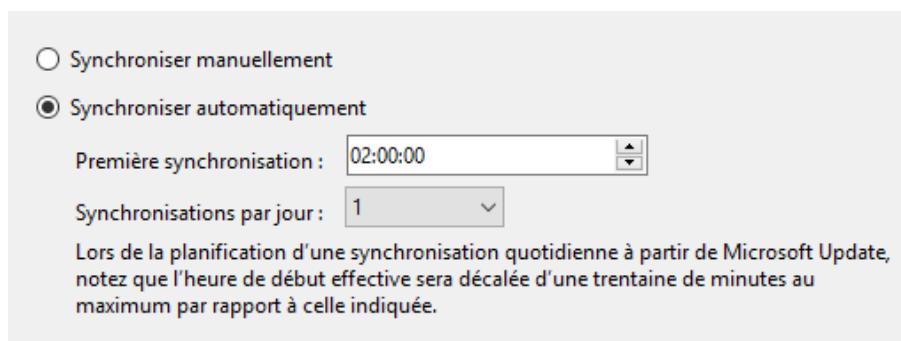
Jusqu'à présent, nous avons défini les besoins de l'infrastructure.

Nous passons maintenant à la configuration de la **synchronisation**, qui permettra au serveur WSUS de se connecter aux serveurs Microsoft pour récupérer les mises à jour disponibles.

Commencer par sélectionner le **mode de synchronisation** souhaité.

- **Synchronisation manuelle** : les mises à jour devront être lancées manuellement.
- **Synchronisation automatique** : permet de planifier des synchronisations à intervalles réguliers.

Dans notre cas, nous optons pour une **synchronisation automatique**, puis cliquer sur **Suivant**.



Synchroniser manuellement

Synchroniser automatiquement

Première synchronisation : 02:00:00

Synchronisations par jour : 1

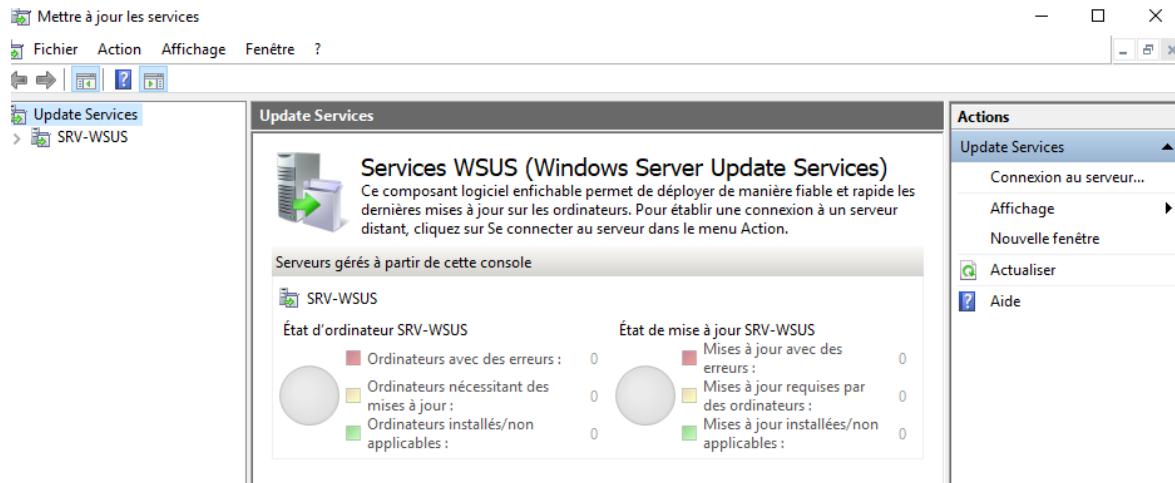
Lors de la planification d'une synchronisation quotidienne à partir de Microsoft Update, notez que l'heure de début effective sera décalée d'une trentaine de minutes au maximum par rapport à celle indiquée.

La configuration du serveur WSUS est maintenant terminée.

Cocher l'option « **Commencer la synchronisation initiale** », puis cliquer sur **Terminer**.

Cette synchronisation peut être particulièrement longue, selon les produits sélectionnés.

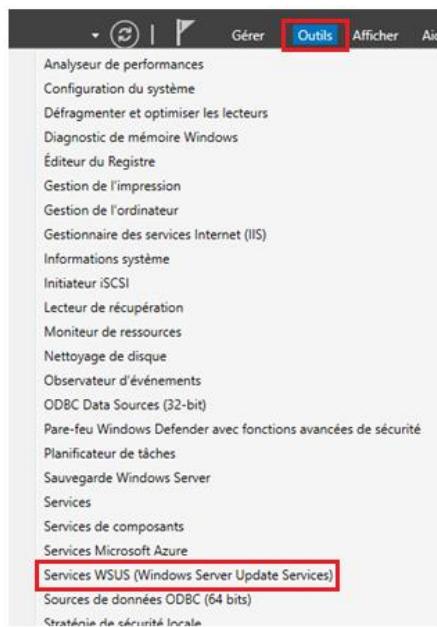
Dans notre cas, elle est estimée à **environ 1h30**.



### Aperçu de la console d'administration du Serveur WSUS

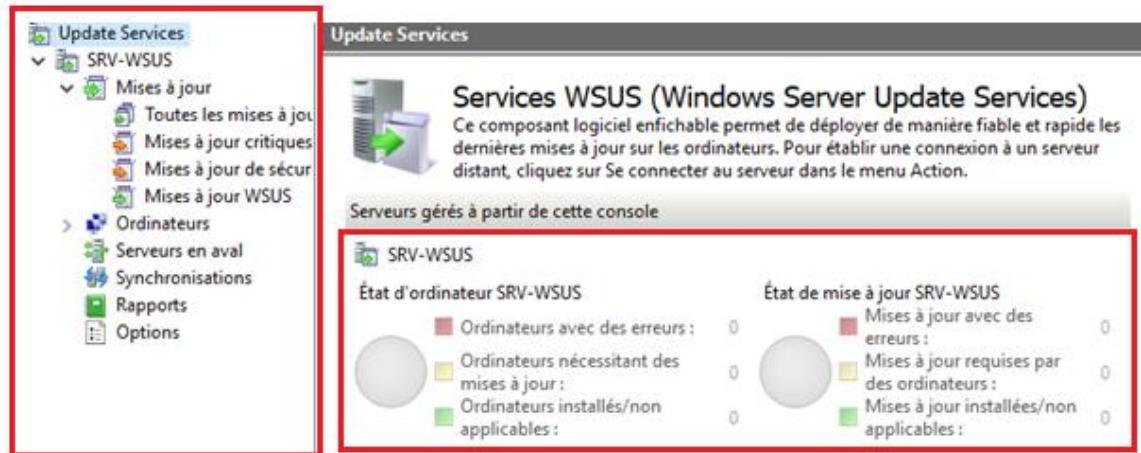
Pour accéder à la console d'administration de WSUS, ouvrir le **Gestionnaire de serveur**, puis cliquer sur **Outils**.

Dans la liste, sélectionner **Service WSUS**.



Voici l'aperçu de la console WSUS :

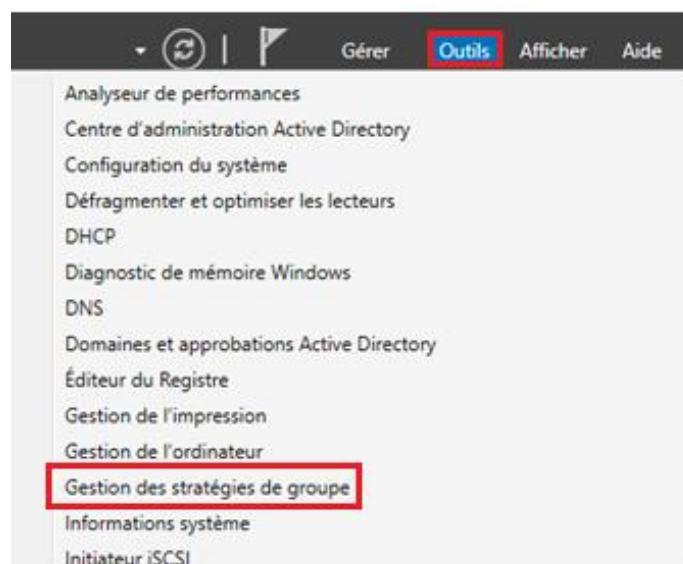
1. Un volet latéral regroupant l'ensemble des **catégories** de gestion.
2. Un tableau de bord affichant l'**état des ordinateurs** recensés et celui des **mises à jour disponibles**.



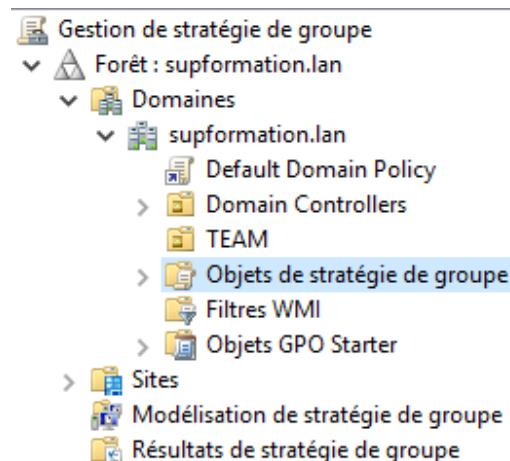
## GPO – Gestion des stratégies de groupe

### 2.8) Mise en place de GPO de sécurité et de gestion des utilisateurs

Gestionnaire de serveur sur ton contrôleur de domaine, Outils -> Gestion de stratégie de groupe (ou *Group Policy Management* en anglais).



Dans la console de gestion des stratégies de groupe, déplier les éléments afin d'afficher l'arborescence suivante :



Effectuer un clic droit sur l'unité d'organisation (UO) ciblée, puis sélectionner :

**« Crée un objet GPO dans ce domaine et le lier ici... »**

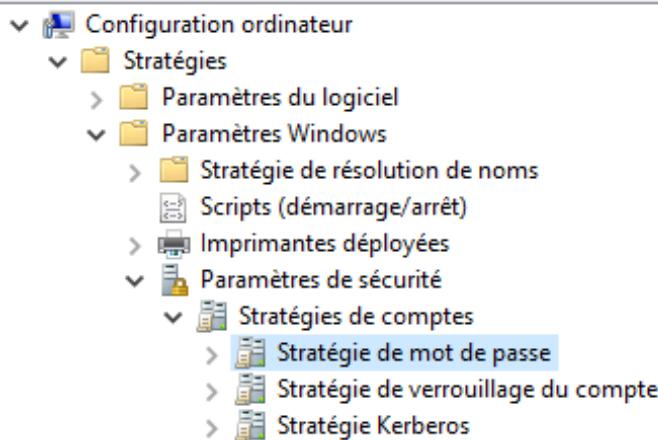
Nommer cet objet de stratégie de groupe « Mot de passe », puis cliquer sur OK.



Effectuer un clic droit sur la GPO nouvellement créée, puis cliquer sur « Modifier » afin d'ouvrir l'éditeur de gestion des stratégies de groupe.



Déplier : Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégies de mot de passe.



Définir les paramètres suivants selon les besoins de l'organisation :

Stratégie	Paramètres de stratégie
[] Audit de la longueur minimale du mot de passe	Non défini
[] Conserver l'historique des mots de passe	Non défini
[] Durée de vie maximale du mot de passe	180 jours
[] Durée de vie minimale du mot de passe	30 jours
[] Enregistrer les mots de passe en utilisant un chiffrement rév...	Non défini
[] Le mot de passe doit respecter des exigences de complexité	Activé
[] Longueur minimale du mot de passe	12 caractère(s)

### Interdire le panneau de configuration pour les utilisateurs

Dans l'arborescence, faire un clic droit sur l'UO ciblée, puis sélectionner « **Créer un objet GPO dans ce domaine et le lier ici...** »

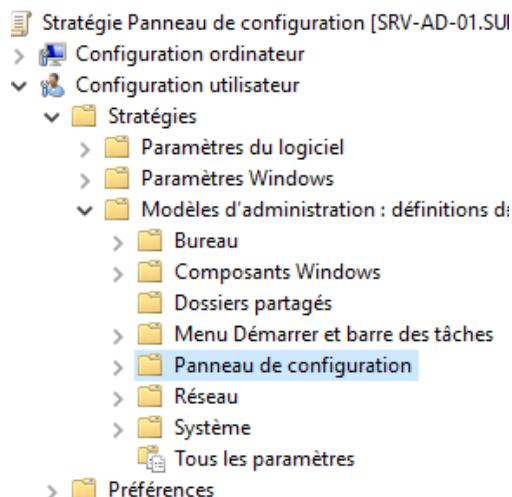
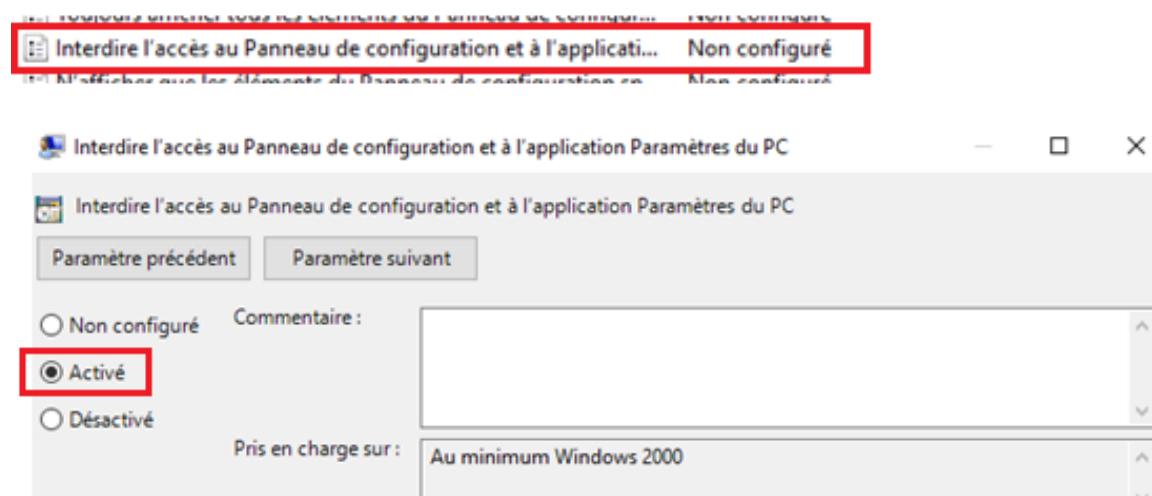
Nommer la GPO « Panneau de configuration », puis cliquer sur OK.

Ensuite, faire un **clic droit sur la GPO** nouvellement créée, puis sélectionner **Modifier**.



Déplier les menus jusqu'à obtenir l'arborescence suivante :

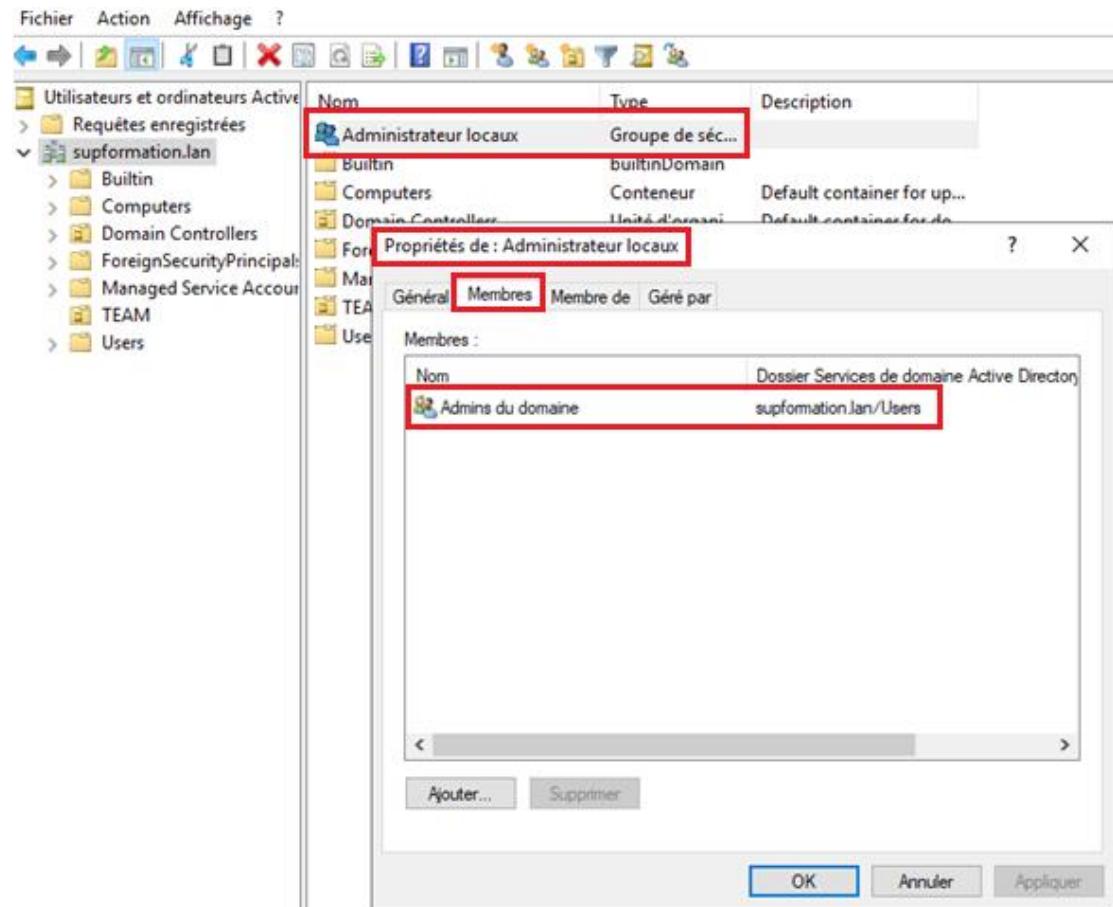
**Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration**

Paramètre	Valeur
Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC	Activé
Masquer les éléments du Panneau de configuration spécifiés	Non configuré
Toujours afficher tous les éléments du Panneau de config...	Non configuré
Interdire l'accès au Panneau de configuration et à l'applicati...	Activé
N'afficher que les éléments du Panneau de configuration sp...	Non configuré
Visibilité de la page des paramètres	Non configuré

## Ajouter un administrateur local sur les postes membres du domaine

**Prérequis :** Créer un groupe de sécurité dans l'Active Directory nommé « **Administrateur locaux** » et y ajouter le **compte Administrateur du domaine**.



The screenshot shows the Windows Server Management Console (ADUC). On the left, the navigation pane displays the structure of the Active Directory, including 'Utilisateurs et ordinateurs Active', 'Requêtes enregistrées', and a expanded 'supformation.lan' container with subfolders like 'BuiltIn', 'Computers', 'Domain Controllers', etc. In the center, a properties dialog box for the 'Administrateurs locaux' security group is open. The 'Membres' tab is selected, showing a list of members. One member, 'Admins du domaine', is highlighted with a red box. At the bottom of the dialog, there are buttons for 'Ajouter...' (Add...), 'Supprimer' (Delete), 'OK', 'Annuler' (Cancel), and 'Appliquer' (Apply).

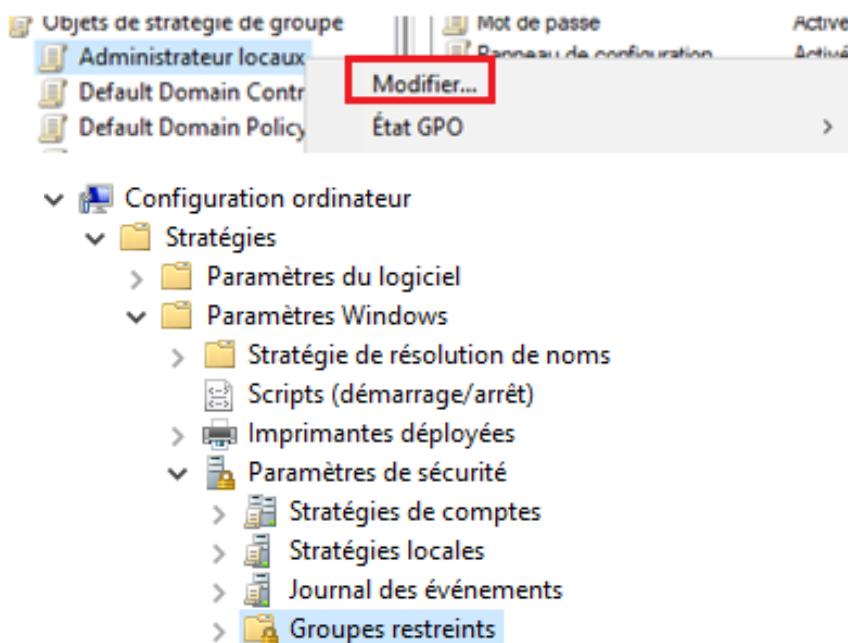
Effectuer le procédé habituel : clic droit sur l'unité d'organisation (UO) concernée, puis sélectionner « **Créer un objet GPO dans ce domaine et le lier ici...** ».

Nommer cette GPO « **Administrateurs locaux** ».

Ensuite, faire un **clic droit** sur la GPO nouvellement créée et cliquer sur **Modifier**.

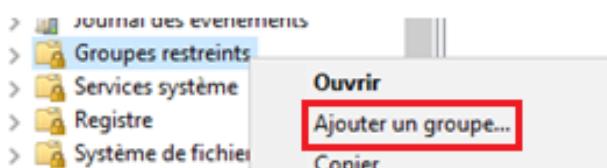
Déplier les menus suivants dans l'éditeur de stratégie de groupe :

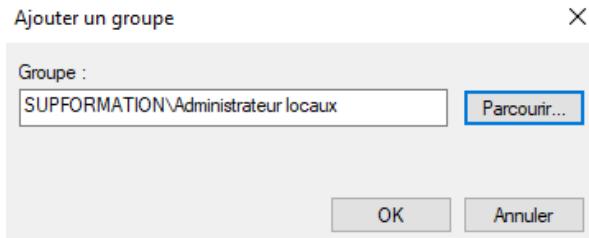
**Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Groupes restreint**



Dans **Groupes restreints**, faire un clic droit puis sélectionner « **Ajouter un groupe...** ».

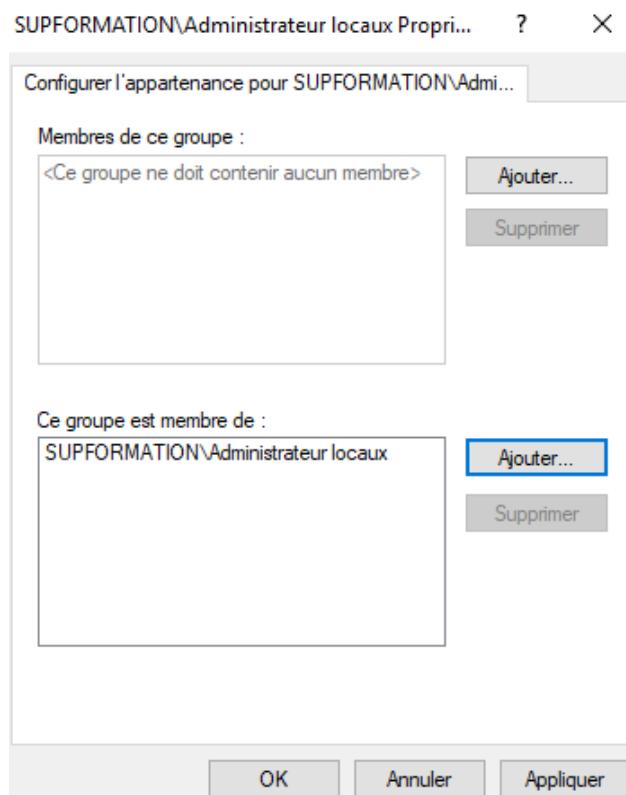
Utiliser le bouton **Parcourir** pour rechercher dans l'Active Directory et sélectionner le groupe « **Administrateur locaux** » préalablement créé à cet effet.



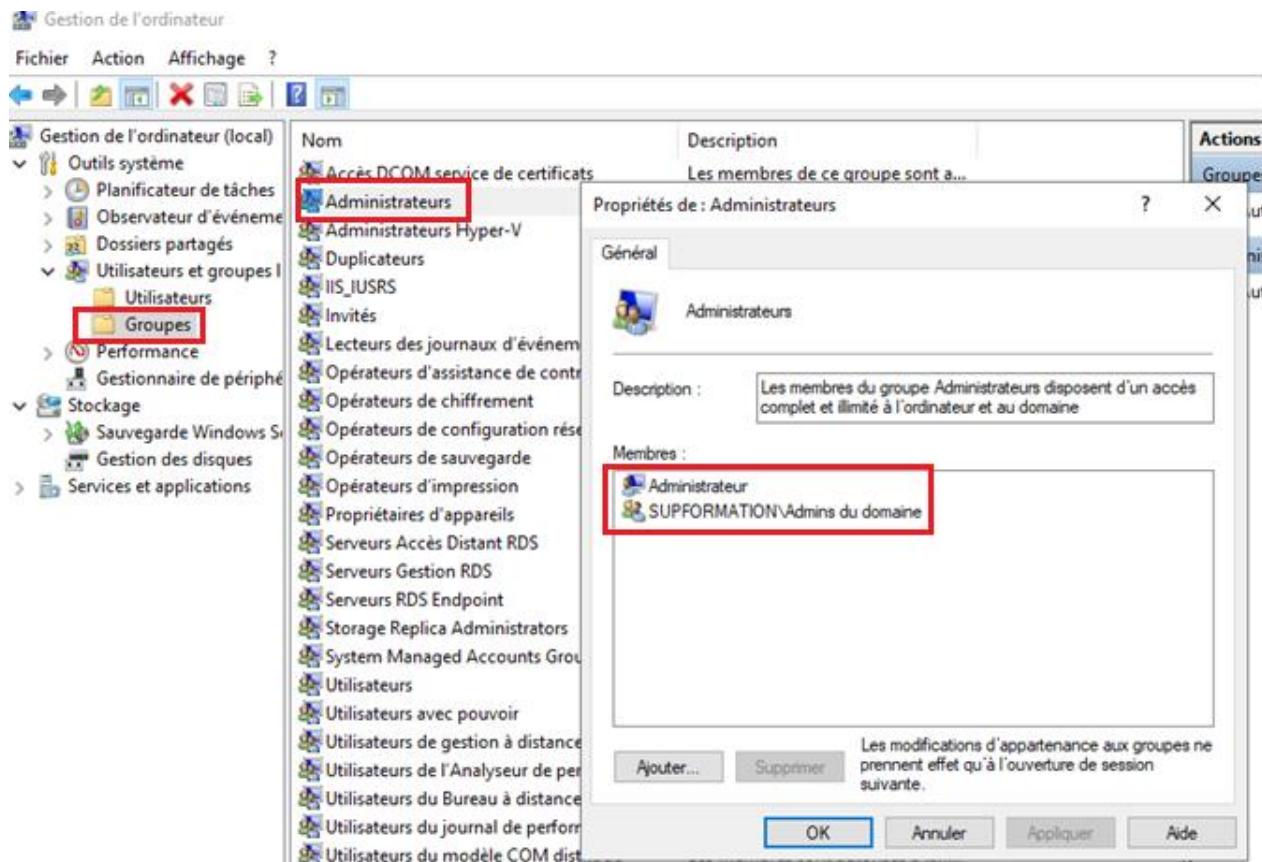


Dans la fenêtre **Configurer l'appartenance**, ajouter dans « **Ce groupe est membre de** » le groupe **Administrateurs**, afin que les membres du groupe « Administrateurs locaux » soient reconnus comme administrateurs **locaux** sur les postes clients du domaine.

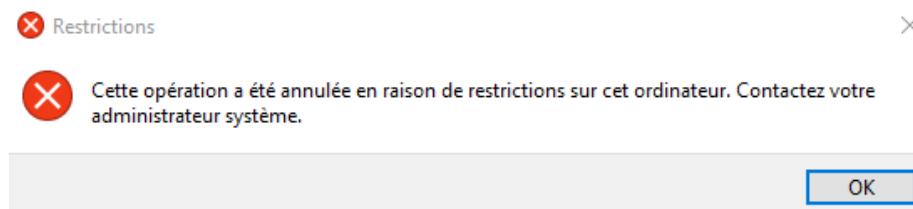
Puis cliquer sur **Appliquer** et **OK**.



Pour vérifier la bonne application de la GPO sur les postes clients, se connecter en tant qu'utilisateur, exécuter deux fois la commande **gpupdate /force**, redémarrer deux fois, puis vérifier que le groupe « Administrateur locaux » est bien présent dans la Gestion de l'ordinateur.



L'accès au panneau de configuration :



## 2.9) Déploiement de GPO pour l'environnement de travail

Lier les postes clients au serveur WSUS via une stratégie de groupe (GPO)

Créer et lier une nouvelle GPO à l'UO cible, **clic droit > Modifier**, puis naviguer dans les paramètres comme suit :

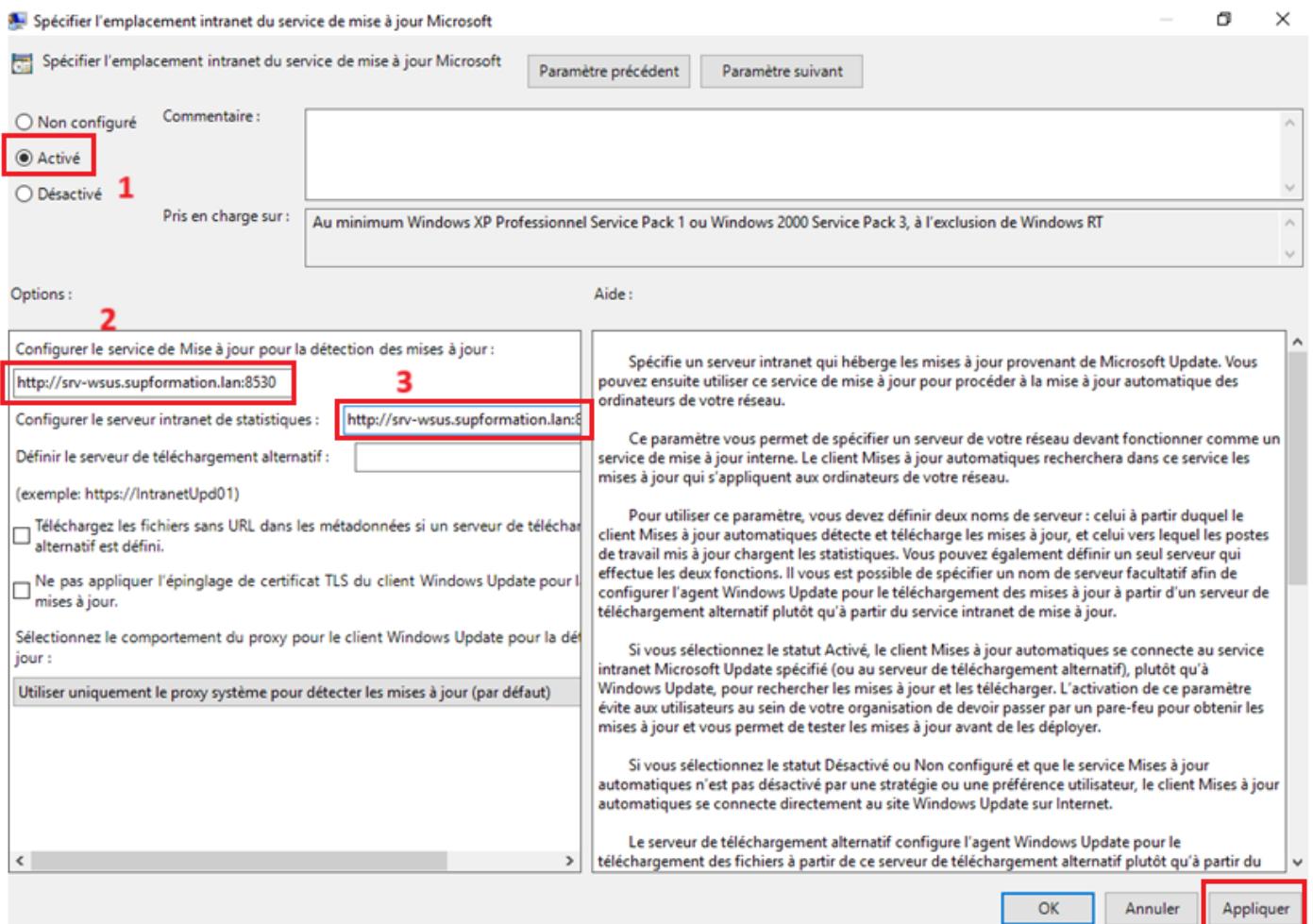


Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update

## Activation du paramètre "Spécifier l'emplacement intranet du service de mise à jour Microsoft"

1. Activer le paramètre.
2. Renseigner l'adresse du serveur WSUS comme source pour la détection des mises à jour.
3. Utiliser également cette adresse pour les statistiques.

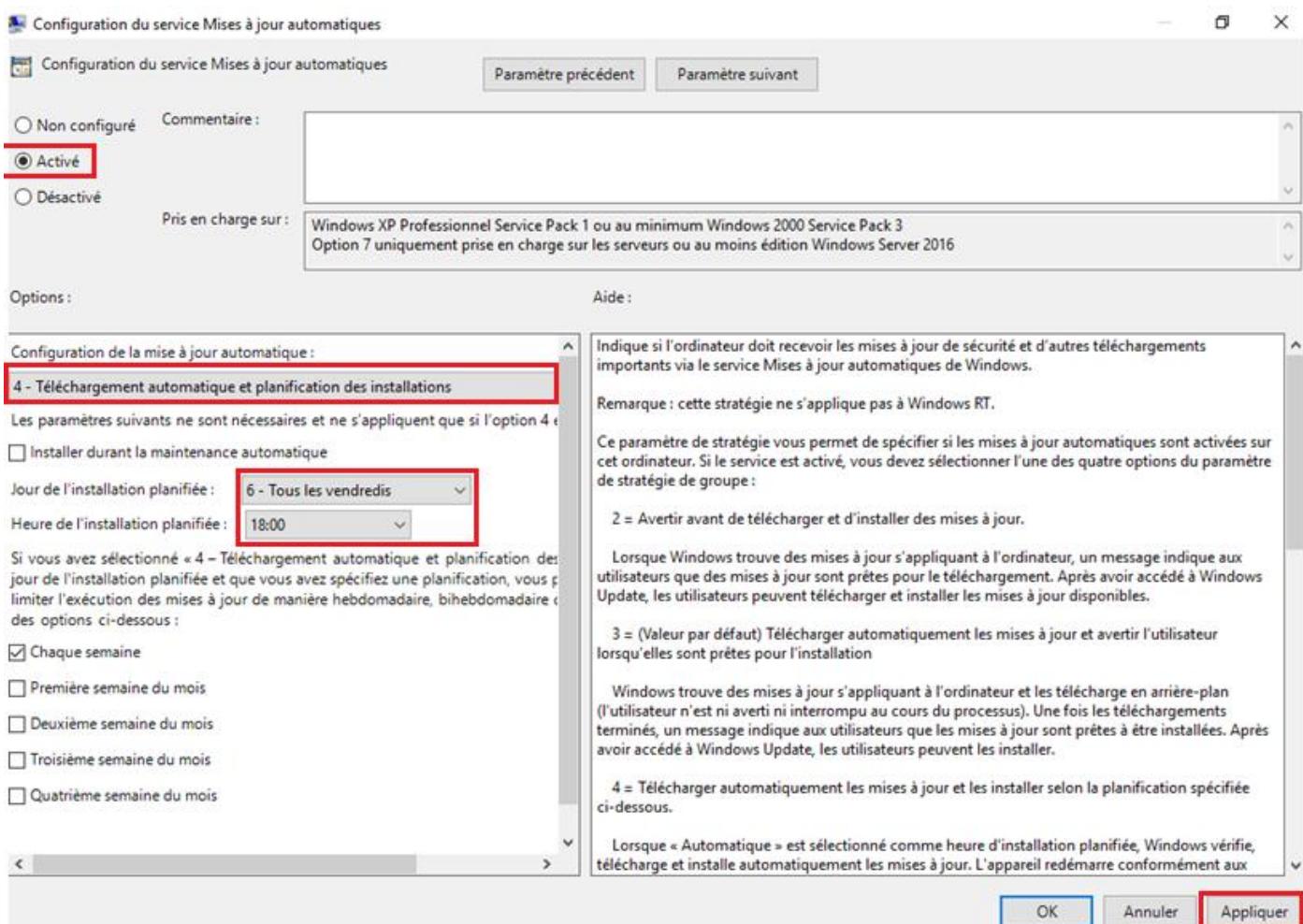
Une fois le paramétrage effectué, cliquer sur **Appliquer** puis **OK**.



Activer le paramètre « Configuration du service Mises à jour automatiques » puis renseigner les options suivantes :

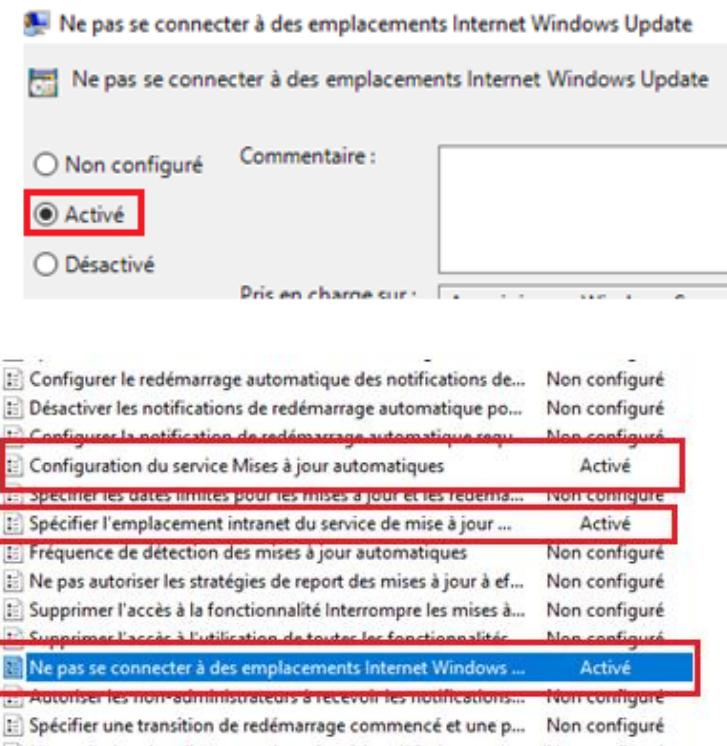
1. Activer le paramètre
2. Choisir « 4 – Téléchargement automatique et planification des installations »
3. Définir le jour de l'installation
4. Définir l'heure souhaitée

Terminer par **Appliquer** puis **OK**.



Activer simplement le paramètre « **Ne pas se connecter à des emplacements Internet Windows Update** ».

Une fois activé, cliquer sur **Appliquer** puis **OK**.



La GPO est désormais prête

## Information – Faire remonter un poste dans la console WSUS

Pour que le serveur ou client apparaisse dans la console WSUS, suivre les étapes suivantes :

1. Ouvrir l'invite de commandes sur la machine concernée.
2. Exécuter la commande : gpupdate /force pour forcer l'application de la GPO.
3. Redémarrer la machine.
4. Aller dans Paramètres > Mises à jour et sécurité.

Si la GPO est bien appliquée, Windows Update indiquera qu'un serveur intranet est utilisé pour la détection des mises à jour :

## Windows Update

\*Votre organisation gère certains paramètres

[Afficher les stratégies de mise à jour configurées](#)

En cliquant sur « **Afficher les stratégies de mise à jour configurées** », on peut visualiser les paramètres définis par la GPO appliquée.

### Stratégies définies sur votre appareil

Télécharger automatiquement les mises à jour et m'avertir lorsqu'elles sont prêtes à être installées

Source : Administrateur

Type : Stratégie de groupe

Définir les options de mise à jour automatique

Source : Administrateur

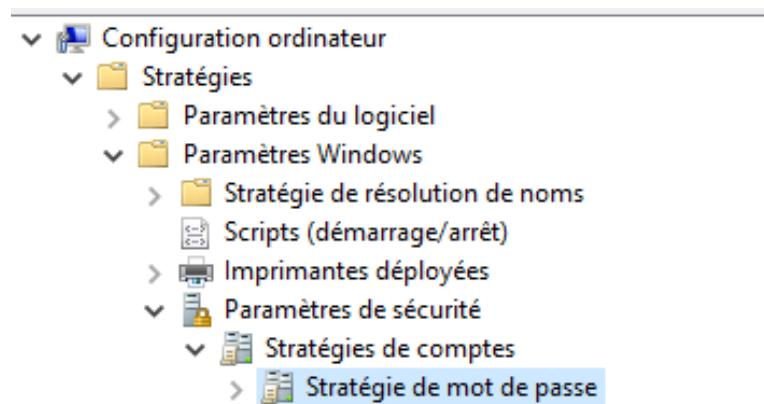
Type : Stratégie de groupe

## Mise en place d'une politique de mot de passe complexe pour le service IT

Créer une GPO nommée « **MDP Admins** » sur l'UO ciblée, puis l'éditer.

Chemin à suivre :

Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de mot de passe.



Le service informatique disposant de droits étendus, il est essentiel de renforcer la sécurité de leurs accès, notamment en imposant une complexité accrue des mots de passe.

Définir alors les contraintes suivantes :

 Durée de vie maximale du mot de passe	92 jours
 Durée de vie minimale du mot de passe	1 jours
 Enregistrer les mots de passe en utilisant un chiffrement rév...	Non défini
 Le mot de passe doit respecter des exigences de complexité	Activé
 Longueur minimale du mot de passe	14 caractère(s)

## Configuration du mappage de lecteurs réseau

Depuis l'UO Cible, clic droit > *Créer un objet GPO dans ce domaine et le lier ici...*

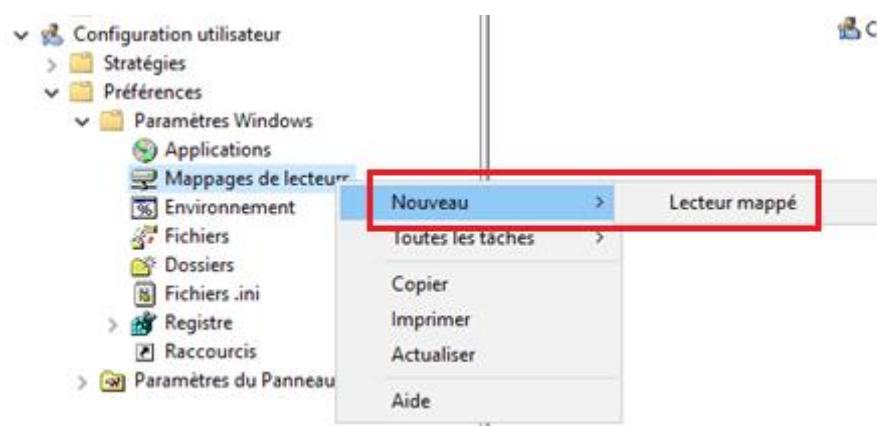
Nommer la GPO **ADM\_MAPPAGE**, puis clic droit dessus > **Modifier**

Parcours à suivre :

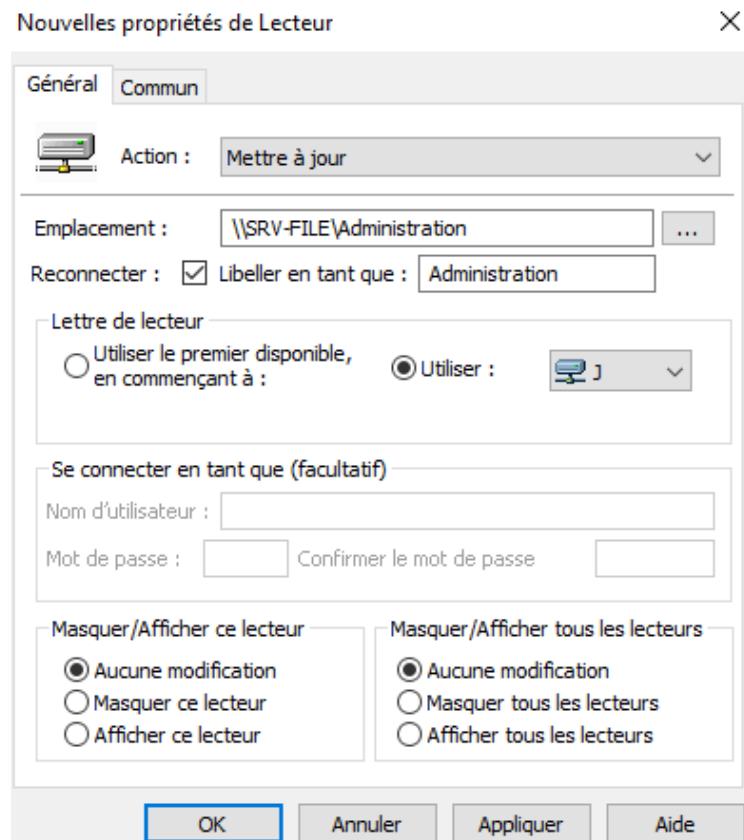
Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteur



Dans la section **Mappages de lecteur**, clic droit > **Nouveau > Lecteur mappé**.



Dans la configuration du lecteur réseau, il suffit d'indiquer l'emplacement du partage, un nom lisible pour l'utilisateur et une lettre pour le lecteur. Aucun réglage n'est nécessaire dans l'onglet « Commun ». Cette méthode sera reprise pour les autres services.



## Installation d'un .MSI

Cette procédure peut être utilisée pour l'installation de n'importe quel fichier .MSI. Dans notre cas, il s'agit d'installer l'agent **Zabbix**, un outil de supervision qui permet de surveiller l'état des machines (CPU, RAM, services, etc.) depuis un serveur central.

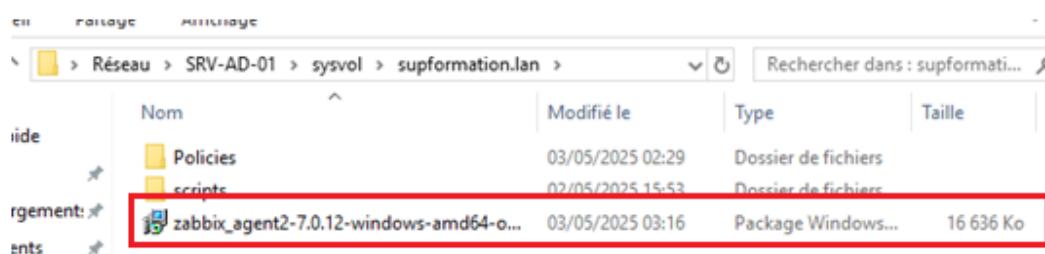
Commencer par télécharger l'agent compatible avec votre environnement (système, architecture, version) depuis le site officiel :

[https://www.zabbix.com/download\\_agents](https://www.zabbix.com/download_agents)

OS DISTRIBUTION	OS VERSION	HARDWARE	ZABBIX VERSION	ENCRYPTION	PACKAGING
Windows	Any	amd64	7.2	OpenSSL	MSI
Linux		i386	7.0 LTS	No encryption	Archive
macOS			6.2		
AIX			6.0 LTS		
FreeBSD			5.4		
OpenBSD			5.2		
Solaris			5.0 LTS		
			4.4		
			4.2		
			4.0 LTS		
			3.0 LTS		

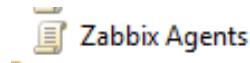
Une fois l'agent Zabbix téléchargé, il faut le placer dans un répertoire accessible à tous les postes du domaine.

Dans notre cas, un dossier partagé a été créé dans **SYSVOL**, à la racine du domaine, afin de centraliser l'accès au fichier d'installation.



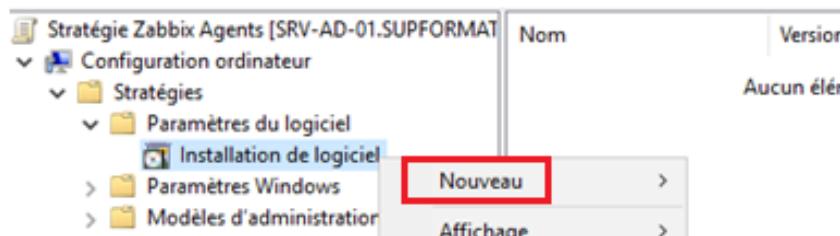
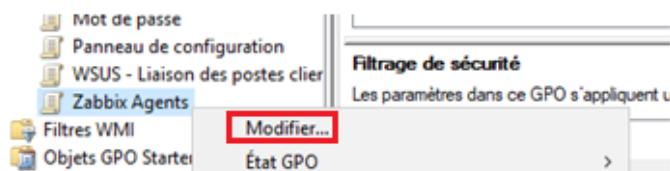
L'agent ayant été déposé, ouvrez le **Gestionnaire de stratégie de groupe**.

Créez une nouvelle GPO, que nous nommerons dans notre cas : « **Zabbix Agents** ».

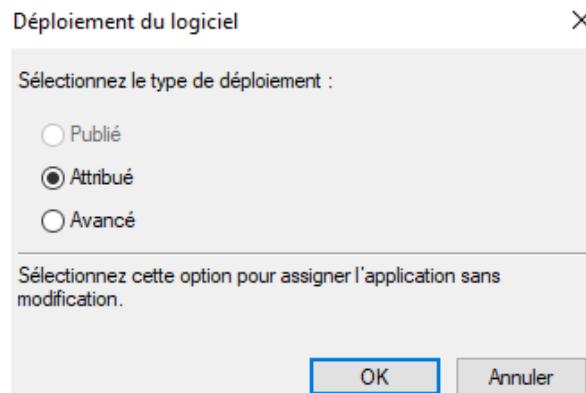


Une fois la GPO créée, cliquez sur "Modifier", puis accédez à : Configuration de l'ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel.

Ensuite, faites un clic droit dans le panneau de droite et sélectionnez **Nouveau > Package...**

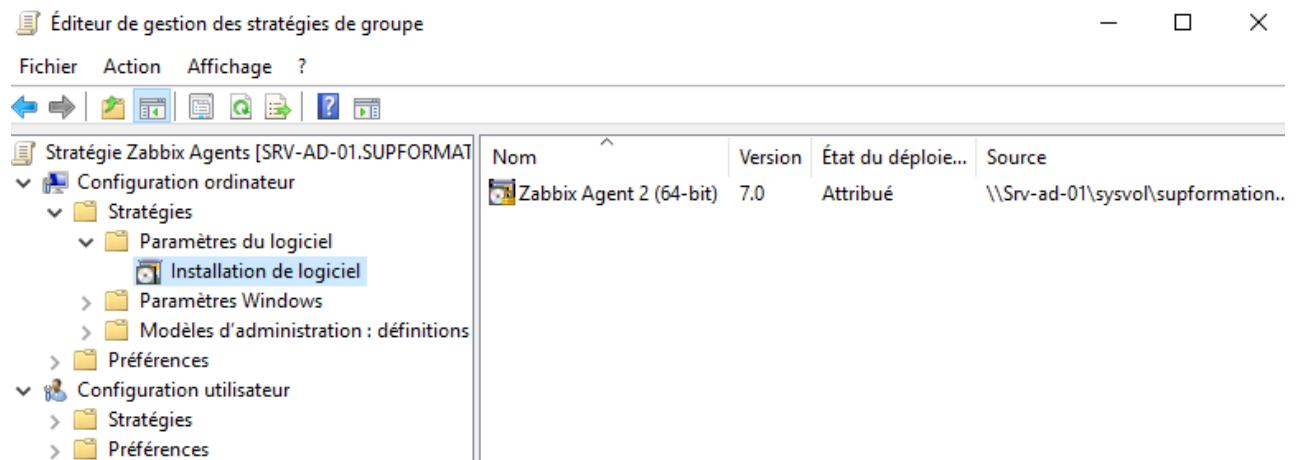


Renseignez ensuite le chemin UNC du répertoire contenant le fichier de l'agent, sélectionnez le fichier MSI, puis cliquez sur "Ouvrir".  
 Cochez l'option "**Attribué**", puis validez en cliquant sur "OK".



Une fois l'ajout effectué, le package apparaîtra dans la section d'installation des logiciels. Il ne reste plus qu'à lier la GPO à l'unité d'organisation (UO) contenant les serveurs Windows.

**L'agent Zabbix sera alors automatiquement installé sur les serveurs de l'UO.** En cas de non-installation, exécutez la commande gpupdate /force pour forcer l'application de la stratégie.



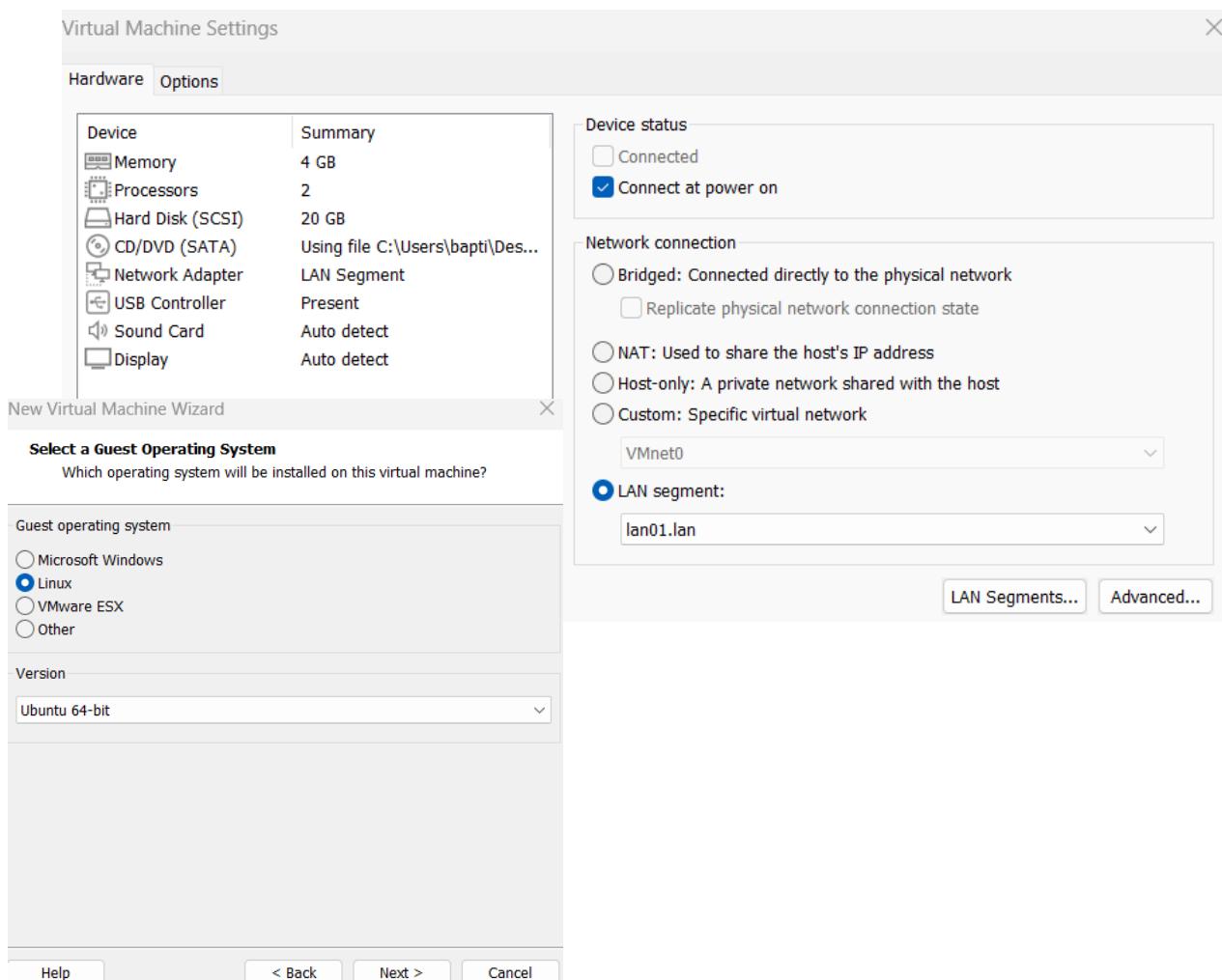
Nom	Version	État du déploiement	Source
Zabbix Agent 2 (64-bit)	7.0	Attribué	\\\Srv-ad-01\sysvol\supformation..

## Configuration des serveurs Linux

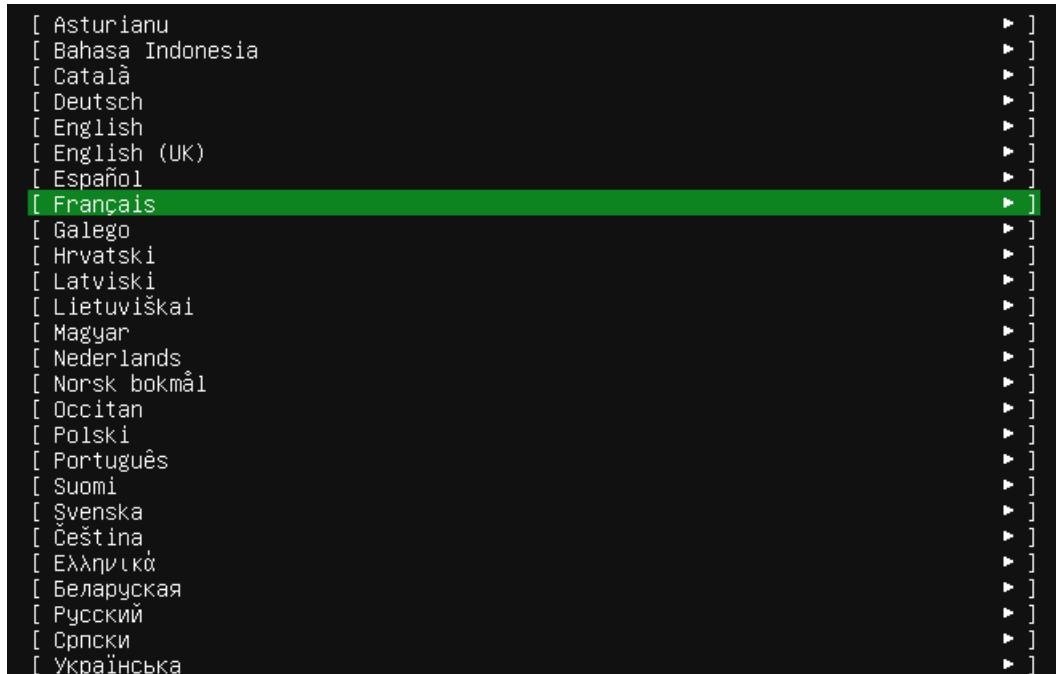
### Samba (serveur de fichiers)

### 3.0) Intégration d'un serveur Samba au domaine et mise en place de partages réseau accessibles depuis Windows

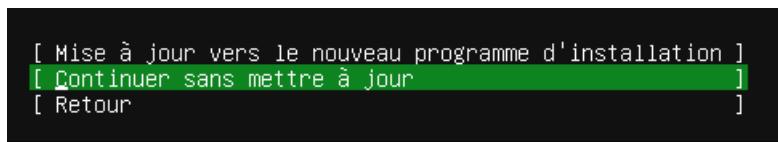
Nous allons utiliser la machine **SRV-FILE** (Ubuntu 22.04) comme serveur de fichiers, en y déployant le service Samba et en l'intégrant au domaine Active Directory.



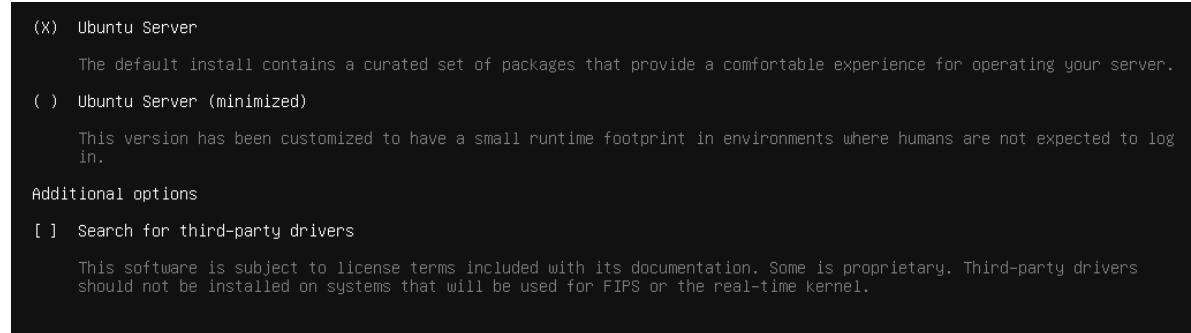
Lors du démarrage de l'installateur Ubuntu Server, sélectionnez la langue souhaitée à l'aide des flèches du clavier, puis validez avec **Entrée**. Dans notre cas, nous choisissons "**Français**".



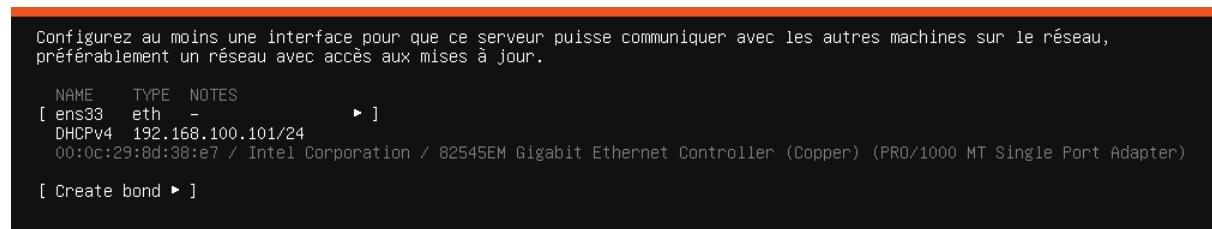
Lorsque l'installateur propose une mise à jour, sélectionnez l'option "**Continuer sans mettre à jour**" afin de démarrer immédiatement l'installation avec la version actuelle.



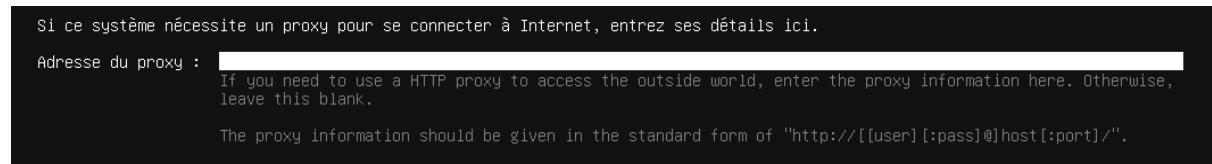
Sélectionnez "**Ubuntu Server**" (option par défaut) afin d'installer l'environnement standard avec l'ensemble des paquets nécessaires pour un usage classique



Le serveur est configuré en DHCP afin de simplifier l'installation. Si besoin, l'adresse IP pourra être fixée ultérieurement.



Aucune configuration de proxy n'est requise dans notre environnement.



- Laisse l'option "Utiliser un disque entier" sélectionnée ✓
- Laisse cochée "Set up this disk as an LVM group" ✓
- **Ne coche pas** l'option de chiffrement avec LUKS (sauf si tu veux du chiffrement, ce qui n'est pas utile ici)

Puis tu continues avec "**Entrée**" ou descends jusqu'à "**Terminé**" (qui viendra après confirmation).

```
Configure a guided storage layout, or create a custom one:

(X) Utiliser un disque entier
    [ /dev/sda local disk 20.000G ▾ ]
[X] Set up this disk as an LVM group
    [ ] Encrypt the LVM group with LUKS

        Phrase de passe :

        Confirmez la phrase de passe :

    [ ] Also create a recovery key
        The key will be stored as ~/recovery-key.txt in the live system and will be
        copied to /var/log/installer/ in the target system.
```

La configuration est confirmée en sélectionnant l'option "Terminé"

```
SOMMAIRE DU SYSTÈME DE FICHIERS

POINT DE MONTAGE      TAILLE     TYPE     TYPE DE PÉRIPHÉRIQUE
[ /                   10.000G   new ext4   nouveau LVM logical volume    ▶ ]
[ /boot                1.771G   new ext4   nouveau partition de disque local ▶ ]

DISQUES DISPONIBLES

PÉRIPHÉRIQUE          TYPE           TAILLE
[ ubuntu-vg (nouveau)  LVM volume group  18.222G ▶ ]
espace libre           8.222G        ▶

[ Create software RAID (md) ▶ ]
[ Create volume group (LVM) ▶ ]

PÉRIPHÉRIQUES UTILISÉS

PÉRIPHÉRIQUE          TYPE           TAILLE
[ ubuntu-vg (nouveau)  LVM volume group  18.222G ▶ ]
ubuntu-lv              nouveau, to be formatted as ext4, mounted at /
                           10.000G ▶

[ /dev/sda               disque local    20.000G ▶ ]
partition 1             nouveau, BIOS grub spacer  1.000M ▶
partition 2             nouveau, to be formatted as ext4, mounted at /boot  1.771G ▶
partition 3             nouveau, PV of LVM volume group ubuntu-vg  18.222G ▶

[ Terminé ] (highlighted)
[ Rétablir ]
[ Retour ]
```

Le compte administrateur anadmin a été créé avec les droits sudo. Le nom d'hôte de la machine a été défini sur **srv-file**, conformément au plan d'adressage.

Enter the username and password you will use to log in to the system. You can configure SSH access on a later screen, but a password is still needed for sudo.

Votre nom : admin

Your servers name: srv-file  
The name it uses when it talks to other computers.

Choisir un nom d'utilisateur : anadmin

Choisir un mot de passe : \*\*\*\*\*

Confirmer votre mot de passe: \*\*\*\*\*

Le serveur OpenSSH est installé afin de permettre un accès distant sécurisé. L'authentification par mot de passe est activée pour l'utilisateur anadmin.

OpenSSH configuration

You can choose to install the OpenSSH server package to enable secure remote access to your server.

[X] Installer le serveur OpenSSH

[X] Autoriser l'authentification par mot de passe via SSH

[ Import SSH key ▶ ]

AUTHORIZED KEYS

No authorized key

Aucun paquet snap supplémentaire n'a été sélectionné à cette étape. Les composants nécessaires seront installés manuellement après l'installation selon les besoins.

```
These are popular snaps in server environments. Select or deselect with SPACE, press ENTER to see more details of the package, publisher and versions available.

[ ] microk8s canonical✓ Kubernetes for workstations and appliances
[ ] nextcloud nextcloud✓ Nextcloud Server - A safe home for all your data
[ ] wekan xet7 Open-Source kanban
[ ] kata-containers katacontainers✓ Build lightweight VMs that seamlessly plug into the containers ecosystem
[ ] docker canonical✓ Docker container runtime
[ ] canonical-livepatch canonical✓ Canonical Livepatch Client
[ ] rocketchat-server rocketchat✓ Rocket.Chat server
[ ] mosquitto mosquitto✓ Eclipse Mosquitto MQTT broker
[ ] etcd canonical✓ Resilient key-value store by CoreOS
[ ] powershell canonical✓ PowerShell for every system!
[ ] sabnzbd safihre SABnzbd
[ ] wormhole snapcrafters.wget get things from one computer to another, safely
[ ] aws-cli aws✓ Universal Command Line Interface for Amazon Web Services
[ ] google-cloud-sdk google-cloud-sdk✓ Google Cloud SDK
[ ] sicli softlayer Python based SoftLayer API Tool.
[ ] doctl digitalocean✓ The official DigitalOcean command line interface
[ ] postgresql10 cmd✓ PostgreSQL is a powerful, open source object-relational database system.
[ ] heroku heroku✓ CLI client for Heroku
[ ] keepalived keepalived-project✓ High availability VRRP/BFD and load-balancing for Linux
[ ] prometheus canonical✓ The Prometheus monitoring system and time series database
```

Installation complete!

Une fois l'installation terminée, vous pouvez redémarrer le système afin de finaliser le déploiement et accéder à votre nouveau serveur.

## Ajout du serveur samba au domaine

Avant d'ajouter le serveur Samba au domaine, commencez par mettre à jour la machine en exécutant les commandes suivantes :

```
anadmin@srv-file:~$ sudo apt update && sudo apt upgrade
```

```
Préparation du dépaquetage de .../06-open-iscsi_2.1.5-1ubuntu1.1_amd64.deb ...
Dépaquetage de open-iscsi (2.1.5-1ubuntu1.1) sur (2.1.5-1ubuntu1) ...
Préparation du dépaquetage de .../07-distro-info-data_0.52ubuntu0.9_all.deb ...
Dépaquetage de distro-info-data (0.52ubuntu0.9) sur (0.52ubuntu0.7) ...
Préparation du dépaquetage de .../08-ubuntu-pro-client-110n_35.1ubuntu0~22.04_amd64.deb ...
Dépaquetage de ubuntu-pro-client-110n (35.1ubuntu0~22.04) sur (33.2~22.04) ...
Préparation du dépaquetage de .../09-ubuntu-pro-client_35.1ubuntu0~22.04_amd64.deb ...
```

```
Progression : [ 28%] [#####.....]
```

Patiencez...

Ensuite, installez les paquets nécessaires à l'intégration du serveur Samba au domaine à l'aide de la commande suivante :

```
anadmin@srv-file:~$ sudo apt install samba krb5-user winbind libpam-winbind libnss-winbind smbclient
```

Poursuivre en configurant Kerberos dans le fichier /etc/krb5.conf.

Kerberos joue un rôle central dans l'intégration du serveur au domaine Active Directory. Il fournit un mécanisme d'authentification sécurisé permettant à l'AD de valider les identifiants des utilisateurs. La configuration correcte de ce service est donc essentielle.

```
anadmin@srv-file:~$ sudo nano /etc/krb5.conf_
```

Le fichier /etc/krb5.conf a été configuré pour intégrer le domaine SUPFORMATION.LAN, avec le contrôleur srv-ad-01.supformation.lan défini comme KDC et serveur Kerberos.

```
GNU nano 6.2                               /etc/krb5.conf
[libdefaults]
default_realm = SUPFORMATION.LAN
dns_lookup_realm = false
dns_lookup_kdc = true

[realms]
SUPFORMATION.LAN = {
kdc = srv-ad-01.supformation.lan
admin_server = srv-ad-01.supformation.lan
}

[domain_realms]
.supformation.lan = SUPFORMATION.LAN
supformation.lan = SUPFORMATION.LAN
```

Passons maintenant à la configuration de Samba en accédant au fichier de configuration suivant :

```
anadmin@srv-file:~$ sudo nano /etc/samba/smb.conf
```

Mettre votre mot de passe admin puis **ENTER**.

Correction de la configuration Samba pour intégrer le serveur au domaine Active Directory SUPFORMATION.LAN en mode sécurité ADS.

```
GNU nano 6.2                               /etc/samba/smb.conf *
[global]
workgroup = SUPFORMATION
security = ADS
realm = SUPFORMATION.LAN

domain master = no
local master = no
preferred master = no

idmap config * :_backend = tdb
idmap config * : range = 10000-20000

template shell = /bin/bash

winbind use default domain = true
winbind offline logon = false
winbind nss info = rfc2307
winbind enum users = yes
winbind enum groups = yes

[homes]
```

comment = Home Directories  
browseable = no  
writable = yes

Validation de la configuration Samba réussie avec testparm : le serveur est prêt à rejoindre le domaine en tant que membre (ROLE\_DOMAIN\_MEMBER).

```
anadmin@srv-file:~$ sudo testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed

Server role: ROLE_DOMAIN_MEMBER

Press enter to see a dump of your service definitions
```

Résultat du fichier **smb.conf** une fois correctement configuré et validé via testparm.

```
# Global parameters
[global]
    domain master = No
    local master = No
    preferred master = No
    realm = SUPFORMATION.LAN
    security = ADS
    template shell = /bin/bash
    winbind enum groups = Yes
    winbind enum users = Yes
    winbind nss info = rfc2307
    winbind use default domain = Yes
    workgroup = SUPFORMATION
    idmap config * : range = 10000-20000
    idmap config * : backend = tdb

[homes]
    browseable = No
    comment = Home Directories
    read only = No
```

Création du fichier **user.map** pour mapper l'utilisateur root local à l'administrateur AD.

```
anadmin@srv-file:~$ sudo nano /etc/samba/user.map
```

Dans le fichier fraîchement créé, y renseigner la ligne suivante :

```
GNU nano 6.2
!root = SUPFORMATION\Administrateur
```

Il ne reste plus qu'à rejoindre le domaine SUPFORMATION à l'aide de la commande suivante, qui nécessite le mot de passe du compte Administrateur du domaine :

```
anadmin@srv-file:~$ sudo net ads join -U Administrateur
Password for [SUPFORMATION\Administrateur]:
```

```
using short domain name -- SUPFORMATION
Joined 'SRV-FILE' to dns domain 'supformation.lan'
No PDC domain configured for srv-file. Unable to re-
```

Une fois lié au domaine, configurer Winbind en modifiant le fichier /etc/nsswitch.conf afin d'intégrer la résolution des utilisateurs et groupes du domaine.

```
anadmin@srv-file:~$ sudo nano /etc/nsswitch.conf
```

Faire la configuration ci-dessous dans le fichier /etc/nsswitch.conf pour activer la résolution des utilisateurs et groupes du domaine via Winbind.

```
GNU nano 6.2                               /etc/nsswitch.conf *
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference` and `info` packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      compat winbind
group:       compat winbind
shadow:      compat_
gsnauow:    tries

hosts:        files dns
networks:     files

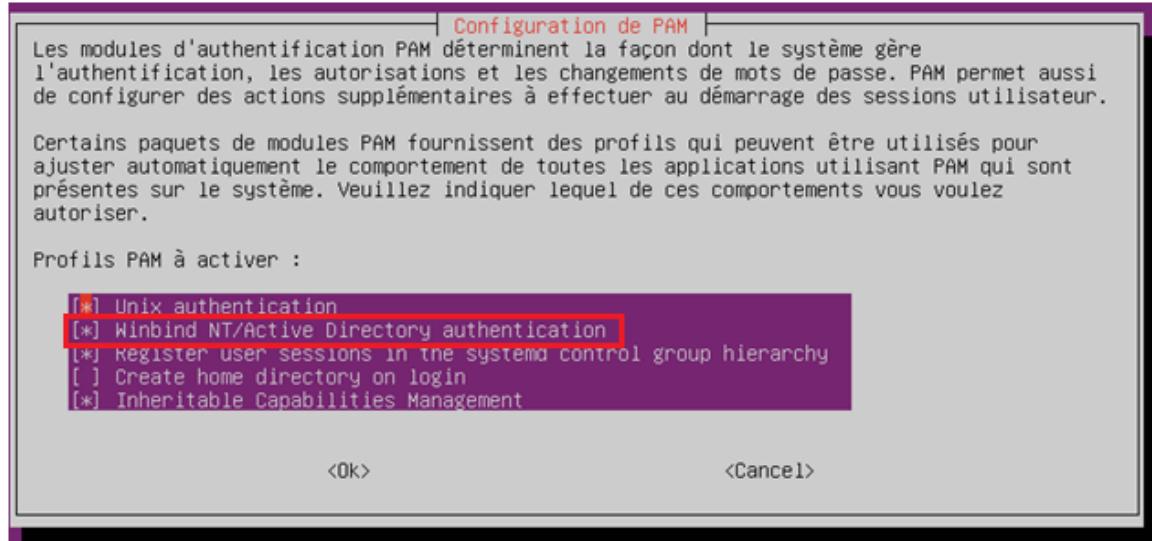
protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
```

Pour finir, il faudra configurer PAM afin de permettre l'authentification des utilisateurs du domaine sur le système.

```
anadmin@srv-file:~$ sudo pam-auth-update
```

Et cocher la case suivante si ce n'est pas déjà fait : "**Winbind NT/Active Directory authentication**".



Pour s'assurer que les configurations sont bien prises en compte, redémarrer les services suivants :

```
anadmin@srv-file:~$ sudo systemctl restart smbd winbind_
```

Une petite vérification afin de s'assurer que la liaison au domaine est bien fonctionnelle peut être effectuée avec les commandes suivantes :

```
anadmin@srv-file:~$ wbinfo -g
ordinateurs du domaine
contrôleurs de domaine
administrateurs du schéma
administrateurs de l'entreprise
éditeurs de certificats
admins du domaine
utilisateurs du domaine
invités du domaine
propriétaires créateurs de la stratégie de groupe
serveurs ras et ias
groupe de réplication dont le mot de passe rodc est autorisé
groupe de réplication dont le mot de passe rodc est refusé
contrôleurs de domaine en lecture seule
contrôleurs de domaine d'entreprise en lecture seule
contrôleurs de domaine clonables
protected users
administrateurs clés
administrateurs clés enterprise
dnsadmins
dnsupdateproxy
utilisateurs dhcp
administrateurs dhcp
administrateur locaux
```

```
anadmin@srv-file:~$ wbinfo -u
administrateur
invité
krbtgt
baptiste
```

Comme vu ci-dessus, les groupes ainsi que les utilisateurs présents dans le domaine sont désormais visibles depuis le serveur Samba, confirmant le bon fonctionnement de l'intégration.

## Créer un partage avec Samba

Débuter en créant le répertoire dans lequel le partage se trouvera avec la commande suivante :

```
anadmin@srv-file:~$ mkdir -p /srv/DATAS_
```

Refus de permission lors de la création du dossier, ce qui a nécessité l'utilisation de sudo, puis une vérification avec ls -ld a confirmé que le dossier /srv/DATA a bien été créé avec les droits par défaut.

```
anadmin@srv-file:~$ mkdir -p /srv/DATAS
mkdir: cannot create directory '/srv/DATAS': Permission denied
anadmin@srv-file:~$ sudo mkdir -p /srv/DATA
anadmin@srv-file:~$ ls -ld /srv/DATA
ls: command not found
anadmin@srv-file:~$ ls -ld /srv/DATA
drwxr-xr-x 2 root root 4096 mai 3 15:02 /srv/DATA
```

Une fois le dossier créé, on lui attribue le propriétaire root et le groupe IT du domaine Active Directory afin de contrôler les accès.

```
anadmin@srv-file:~$ sudo chown -R root:supformation\\IT /srv/DATA
```

Il faudra également appliquer les permissions 2770 au répertoire afin de garantir un contrôle d'accès strict.

```
anadmin@srv-file:~$ sudo chmod -R 2770 /srv/DATA_
```

Il est maintenant possible de déclarer le partage Samba en éditant le fichier de configuration /etc/samba/smb.conf à l'aide de la commande ci-dessous.

```
anadmin@srv-file:~$ sudo nano /etc/samba/smb.conf
```

Ajouter la configuration ci-dessous dans le fichier smb.conf pour définir le partage Samba.  
Adapter le nom du partage, le chemin et les groupes selon les besoins :

```
[DATA]
comment = Partage de données IT
path = /srv/DATA
guest ok = no
writable = yes
write list = @SUPFORMATION\IT
browseable = yes
valid users = @SUPFORMATION\IT_
```

Redémarrer les services Samba afin d'appliquer les modifications apportées au fichier smb.conf.

```
anadmin@srv-file:~$ sudo systemctl restart smbd nmbd winbind
```

Les services Samba ont été redémarrés avec succès, et les droits sur le répertoire /srv/DATA confirment que le groupe IT dispose des permissions de lecture et d'écriture, avec héritage activé grâce au setgid.

```
anadmin@srv-file:~$ sudo systemctl restart smbd nmbd winbind
anadmin@srv-file:~$ ls -ld /srv/DATA
drwxrws--- 2 root it 4096 mai 3 15:02 /srv/DATA
```

N'oubliez pas de renseigner une adresse IPv4 statique pour votre machine, **basée sur le plan d'adressage défini dans votre infrastructure**, afin d'éviter tout conflit ou perte de connectivité liée au DHCP.

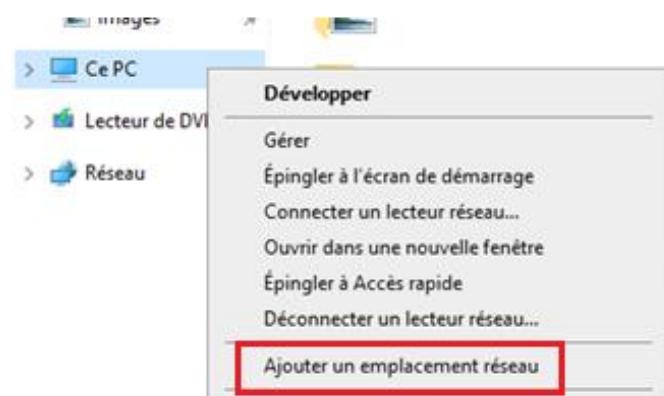
```
# network: {config: disabled}

network:
  version: 2
  ethernets:
    ens33:
      dhcp4: false
      addresses:
        - 192.168.100.18/24
      gateway4: 192.168.100.254
      nameservers:
        addresses:
          - 8.8.8.8
          - 1.1.1.1
```

### Accès au partage Samba depuis le client Windows

Se rendre sur le poste client Windows avec un compte appartenant au groupe de sécurité défini lors de la création du partage Samba, puis ouvrir l'explorateur de fichiers.

Dans l'explorateur, faire un clic droit sur **Ce PC**, puis sélectionner **Ajouter un emplacement réseau**.



Suivant > Suivant puis renseigner l'adresse réseau du partage Samba, en utilisant l'adresse IP actuelle du serveur (même en DHCP), par exemple : \\192.168.100.101\DATA\ dans notre cas.

Adresse réseau ou Internet :

Parcourir...

[Voir des exemples](#)

Un nom par défaut sera attribué au raccourci réseau ; vous pouvez le modifier selon votre besoin, puis cliquer sur **Suivant**.

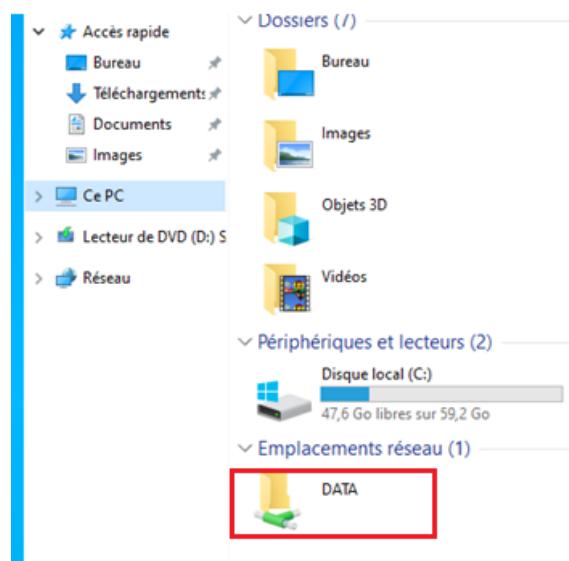
Entrez le nom de cet emplacement réseau :

Entrez le nom de cet emplacement réseau :

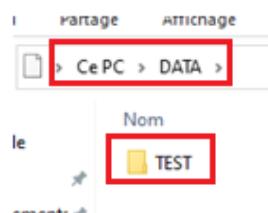
Suivant      Annuler

L'emplacement réseau sera ajouté avec succès.

Reprendons maintenant depuis le début en retournant à l'accueil de l'explorateur de fichiers.

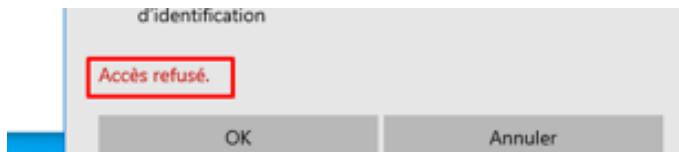


Se rendre dans le partage DATA, puis effectuer un test en créant un fichier pour vérifier les droits d'écriture.



Et si l'on souhaite être pointilleux, il est possible de tester l'accès avec un utilisateur qui ne fait pas partie du groupe de sécurité : l'accès au partage devra alors être refusé.

Il ne reste plus qu'à reproduire cette méthode pour mettre en place les autres partages selon les besoins.



## Serveur de monitoring

### Zabbix – Solution de supervision et de monitoring

#### 3.1) Installation de Zabbix et déploiement des agents sur les machines Windows et Ubuntu

C'est à ce moment que la VM **SRV-MONITORING**, basée sur Ubuntu 22.04, entre en jeu. Elle devra disposer d'un accès à Internet pendant l'installation de la solution Zabbix.

#### Installation de Zabbix

En premier lieu, mettre à jour les paquets logiciels installés sur le système en exécutant la commande suivante :

```
sudo apt update && sudo apt upgrade -y
```

Une fois le système mis à jour, commencer par installer le référentiel officiel de Zabbix à l'aide des commandes suivantes :

```
 wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.4-1+ubuntu22.04_all.deb
```

```
 sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
```

```
 sudo apt update
```

Poursuivre en installant le serveur Zabbix, son interface web (frontend) ainsi que l'agent, à l'aide de la commande suivante :

```
 sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
```

```
 Paramétrage de php8.1-readline (8.1.2-1ubuntu2.21) ...
Creating config file /etc/php/8.1/mods-available/readline.ini with new version
Paramétrage de apache2-data (2.4.52-1ubuntu4.14) ...
Paramétrage de zabbix-agent (1:6.4.21-1+ubuntu22.04) ...
Created symlink /etc/systemd/system/multi-user.target.wants/zabbix-agent.service → /lib/systemd/system/zabbix-agent.service.
Paramétrage de mailcap (3.70+nmu1ubuntu1) ...
Paramétrage de libopenipmi0 (2.0.29-0.1ubuntu6) ...
Paramétrage de fping (5.1-1) ...
Paramétrage de php8.1-opcache (8.1.2-1ubuntu2.21) ...
Progression : [ 74%] [########################################.....]
```

Maintenant, créer une base de données initiale pour Zabbix ainsi qu'un utilisateur dédié avec les droits nécessaires.

MariaDB a été installée sur la machine à l'aide de la commande suivante :

```
 sudo apt install mariadb-server -y
```

Puis,

```
 sudo mysql -uroot -p
```

Votre mot de passe, puis :

```
CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
```

```
CREATE USER zabbix@localhost IDENTIFIED BY 'UnMotDePasseFortIci';
```

```
GRANT ALL PRIVILEGES ON zabbix.* TO zabbix@localhost;
```

```
SET GLOBAL log_bin_trust_function_creators = 1;
```

```
QUIT;
```

```
MariaDB [(none)]> CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin; CREATE USER zabbix@localhost IDENTIFIED BY 'UnMotDePasseFortIci'; GRANT ALL PRIVILEGES ON zabbix.* TO zabbix@localhost; SET GLOBAL log_bin_trust_function_creators = 1; QUIT;
Query OK, 1 row affected (0,001 sec)

Query OK, 0 rows affected (0,001 sec)

Query OK, 0 rows affected (0,001 sec)

Query OK, 0 rows affected (0,000 sec)

Bye
```

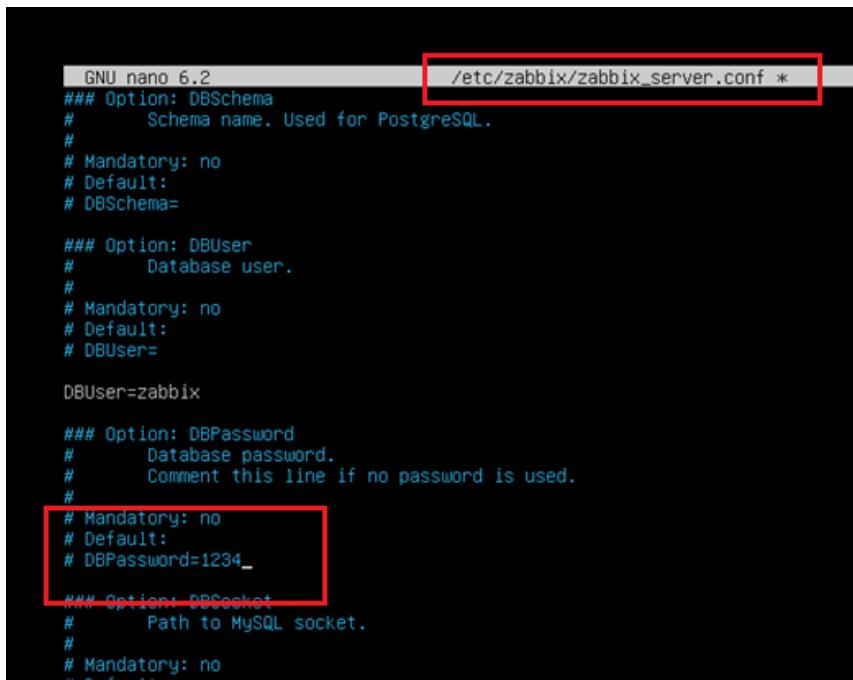
Sur le serveur Zabbix, importer les données initiales dans la base de données à l'aide de la commande ci-dessous, puis saisir le mot de passe défini précédemment pour l'utilisateur zabbix lorsque cela est demandé.

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix
```

Désactiver l'option log\_bin\_trust\_function\_creators en se reconnectant à MariaDB avec les droits root et en exécutant la commande suivante.

```
mysql -uroot -p  
SET GLOBAL log_bin_trust_function_creators = 0;  
QUIT;
```

Maintenant, configurer la base de données pour le serveur Zabbix en renseignant les informations de connexion dans le fichier de configuration prévu à cet effet.



```
GNU nano 6.2 /etc/zabbix/zabbix_server.conf *  
### Option: DBSchema  
# Schema name. Used for PostgreSQL.  
#  
# Mandatory: no  
# Default:  
# DBSchema=  
  
### Option: DBUser  
# Database user.  
#  
# Mandatory: no  
# Default:  
# DBUser=  
  
DBUser=zabbix  
  
### Option: DBPassword  
# Database password.  
# Comment this line if no password is used.  
#  
# Mandatory: no  
# Default:  
# DBPassword=1234_  
  
### Option: DBSocket+  
# Path to MySQL socket.  
#  
# Mandatory: no  
# Default:
```

Démarrer les processus du serveur et de l'agent Zabbix avec la commande suivante, puis les activer au démarrage du système :

```
sudo systemctl restart zabbix-server zabbix-agent apache2
```

```
sudo systemctl enable zabbix-server zabbix-agent apache2
```

La suite de la configuration s'effectue depuis l'interface web du serveur Zabbix.

L'URL par défaut est : <http://<adresse-ip-du-serveur>/zabbix>

Lors de l'accès à l'interface, la première page affichée permet de sélectionner la langue.  
Choisir la langue souhaitée, puis cliquer sur **Prochaine étape**.



The screenshot shows the Zabbix 6.4 installation welcome screen. At the top, it says "ZABBIX". On the left, there's a sidebar with links: Bienvenue, Vérification des prérequis, Configurer la connexion à la base de données, Paramètres, Résumé pré-installation, and Installer. The main area says "Bienvenue dans Zabbix 6.4". Below that, it says "Langage par défaut" followed by a dropdown menu set to "Français (fr\_FR)". To the right of the dropdown is an "i" icon. At the bottom, there are two buttons: "Retour" and "Prochaine étape", with "Prochaine étape" highlighted by a red box.

À cette étape, une vérification automatique des prérequis est effectuée. Il suffit de cliquer sur 'Prochaine étape' pour continuer.

**ZABBIX**

### Vérification des prérequis

	Valeur actuelle	Requis
Bienvenue	Version de PHP	8.1.2-1ubuntu2.21
Vérification des prérequis	7.4.0	OK
Configurer la connexion à la base de données	Option PHP "memory_limit"	128M
	Option PHP "post_max_size"	16M
Paramètres	Option PHP "upload_max_filesize"	2M
Résumé pré-installation	Option PHP "max_execution_time"	300
Installer	Option PHP "max_input_time"	300
	support de bases de données par PHP	MySQL
	bcmath pour PHP	sur
	mbstring pour PHP	sur
	Option PHP "mbstring.func_overload"	inactif
		inactif

[Retour](#) [Prochaine étape](#)

Renseigner les paramètres de connexion à la base de données comme ci-dessous, puis cliquer sur '**Prochaine étape**'. Le mot de passe à saisir correspond à celui défini lors de la création de la base de données initiale sur le serveur Zabbix.



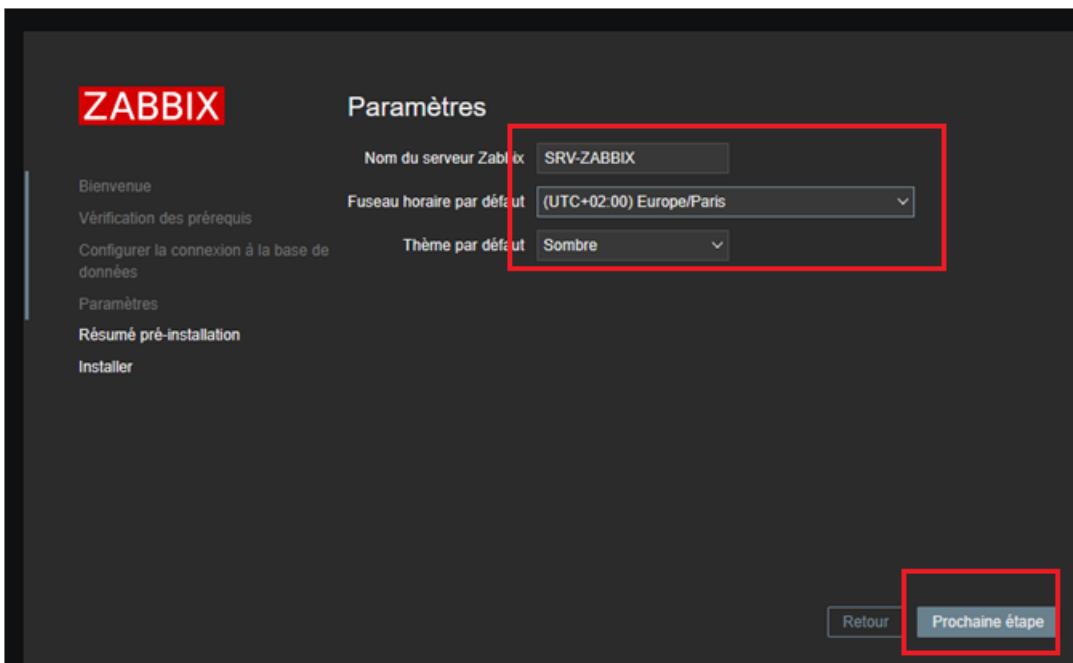
The screenshot shows the 'Configurer la connexion à la base de données' (Configure database connection) step of the Zabbix installation wizard. The left sidebar lists steps: Bienvenue, Vérification des prérequis, Configurer la connexion à la base de données, Paramètres, Résumé pré-installation, and Installer. The main area has the following fields:

- Type de base de données: MySQL (selected)
- Hôte base de données: localhost
- Port de la base de données: 0 (0 - utiliser le port par défaut)
- Nom de la base de données: zabbix
- Stocker les informations d'identification dans:
  - Texte brut (selected)
  - Coffre HashiCorp
  - Coffre CyberArk
- Utilisateur: zabbix
- Mot de passe: (redacted)

Below these fields, a note states: 'Chiffrement TLS de la base de données' followed by a detailed explanation: 'La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Unix) ou de la mémoire partagée (Windows).'. At the bottom right are 'Retour' and 'Prochaine étape' buttons, with 'Prochaine étape' being highlighted with a red box.

Ci-contre, renseigner les éléments suivants :

1. Le nom du serveur Zabbix,
  2. Le fuseau horaire,
  3. Le thème de l'interface.
- Puis cliquer sur **Prochaine étape** pour continuer.



ZABBIX

Paramètres

Bienvenue Vérification des prérequis Configurer la connexion à la base de données Paramètres Résumé pré-installation Installer

Nom du serveur Zabbix : SRV-ZABBIX

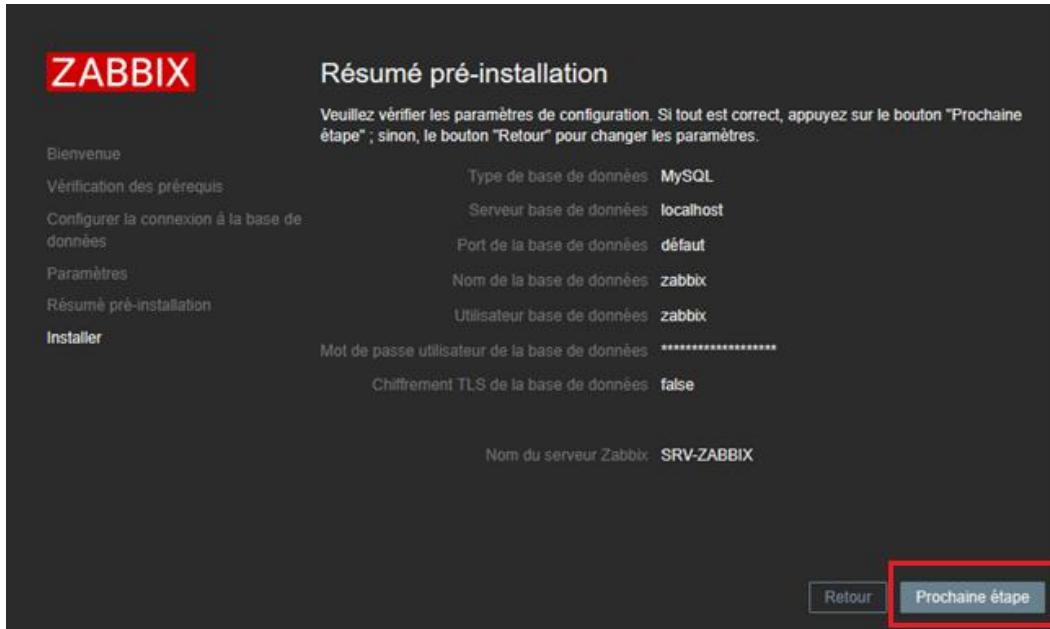
Fuseau horaire par défaut : (UTC+02:00) Europe/Paris

Thème par défaut : Sombre

Retour Prochaine étape

Ici, l'avant-dernière étape présente un récapitulatif de la configuration réalisée.

Vérifier les informations, puis cliquer sur **Prochaine étape** pour finaliser l'installation."

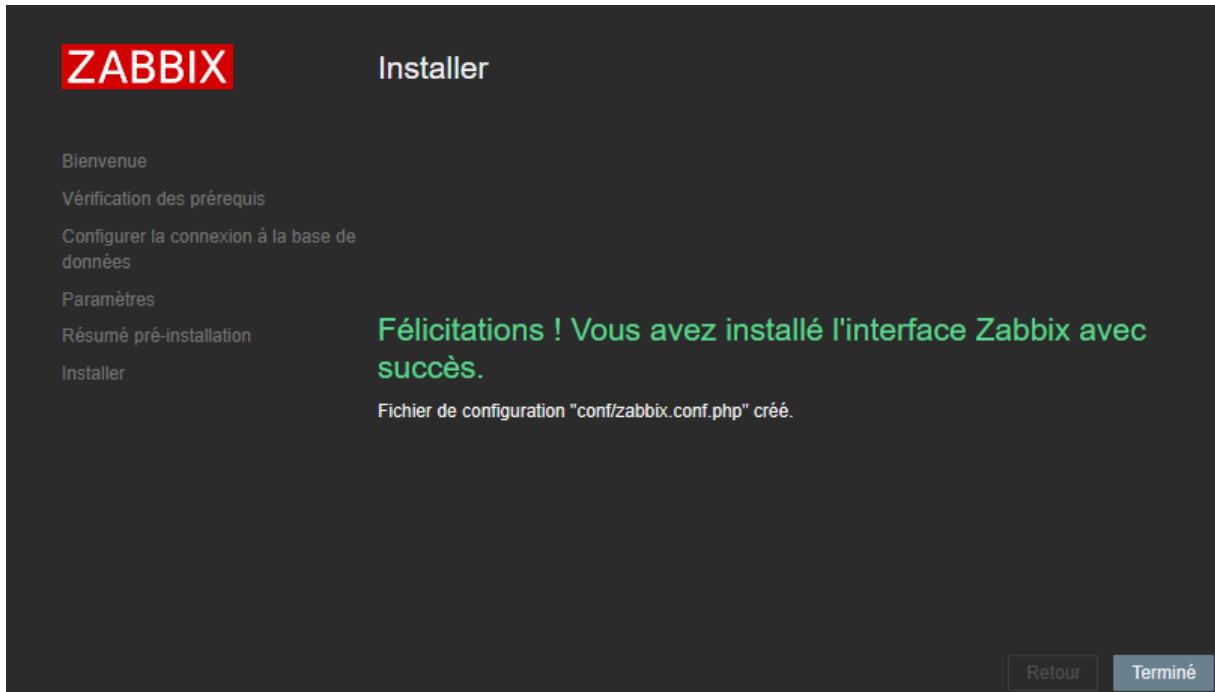


**ZABBIX** Résumé pré-installation

Veuillez vérifier les paramètres de configuration. Si tout est correct, appuyez sur le bouton "Prochaine étape" ; sinon, le bouton "Retour" pour changer les paramètres.

Bienvenue	Type de base de données	MySQL
Vérification des prérequis	Serveur base de données	localhost
Configurer la connexion à la base de données	Port de la base de données	défaut
Paramètres	Nom de la base de données	zabbix
Résumé pré-installation	Utilisateur base de données	zabbix
Installer	Mot de passe utilisateur de la base de données	*****
	Chiffrement TLS de la base de données	false

Nom du serveur Zabbix: SRV-ZABBIX



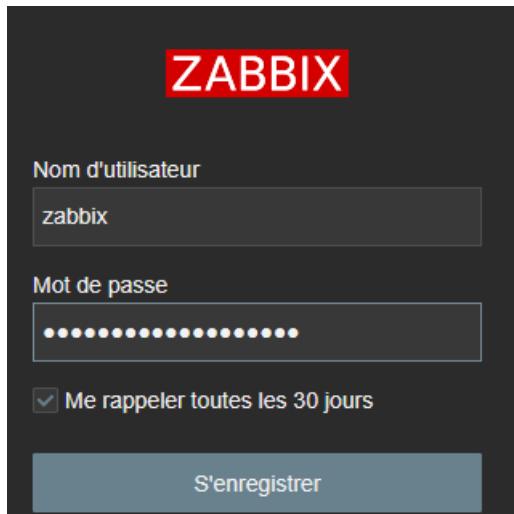
**ZABBIX** Installer

Bienvenue  
Vérification des prérequis  
Configurer la connexion à la base de données  
Paramètres  
Résumé pré-installation  
Installer

**Félicitations ! Vous avez installé l'interface Zabbix avec succès.**

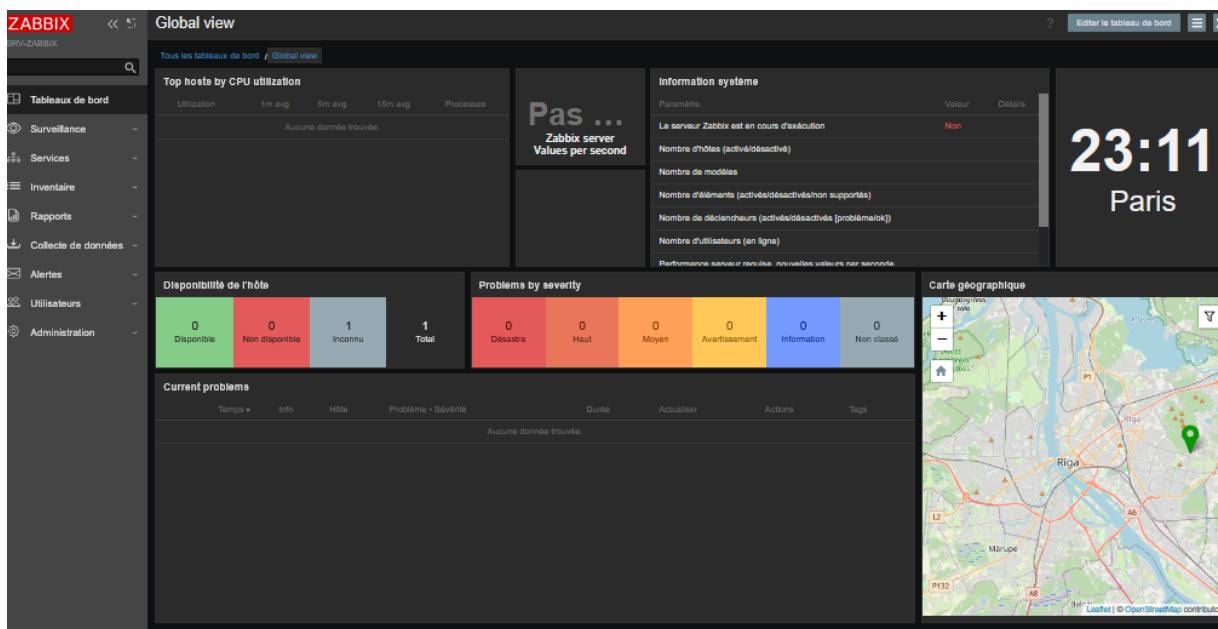
Fichier de configuration "conf/zabbix.conf.php" créé.

Nous pouvons désormais établir une première connexion à l'interface web de Zabbix.

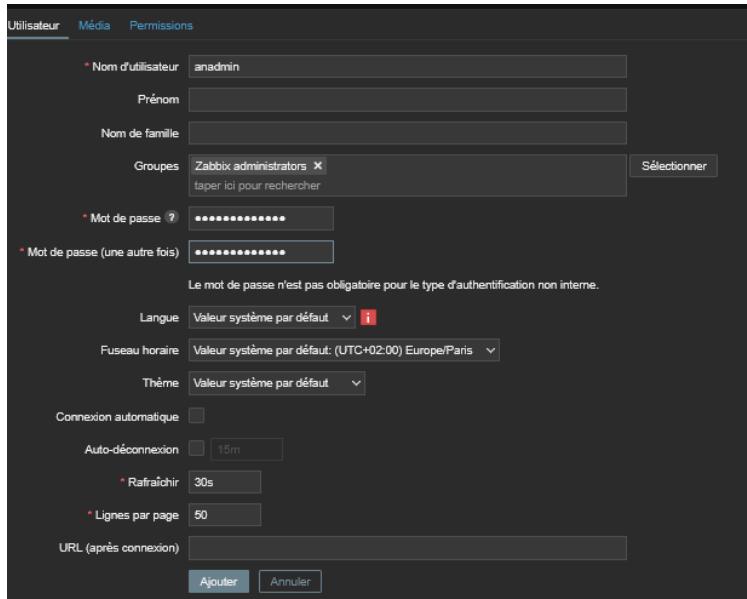


The screenshot shows the Zabbix registration page. It has a dark background with red and white text. The title 'ZABBIX' is at the top. Below it is a 'Nom d'utilisateur' field containing 'zabbix', a 'Mot de passe' field filled with dots, and a checked 'Me rappeler toutes les 30 jours' checkbox. At the bottom is a blue 'S'enregistrer' button.

Une fois connecté à l'interface Zabbix, l'outil de supervision offre une vue centralisée riche en informations via son tableau de bord.



L'une des premières actions à réaliser est la création d'un nouvel utilisateur avec les droits « Administrateurs », en se rendant dans : Utilisateurs > Utilisateurs > Créer un utilisateur.  
 Dans notre cas, l'utilisateur **anadmin** a été créé.

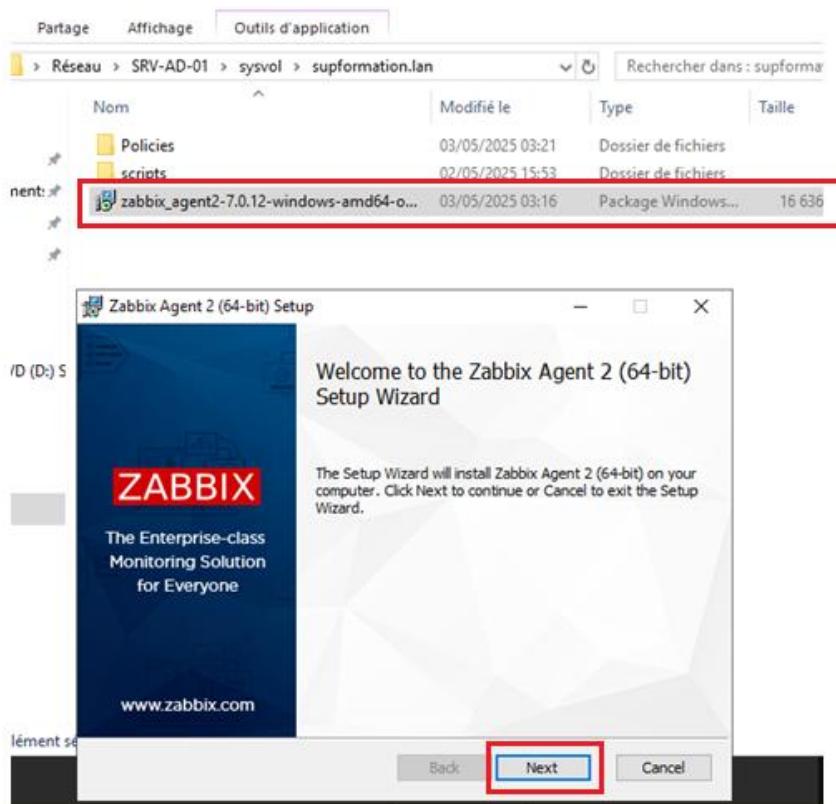


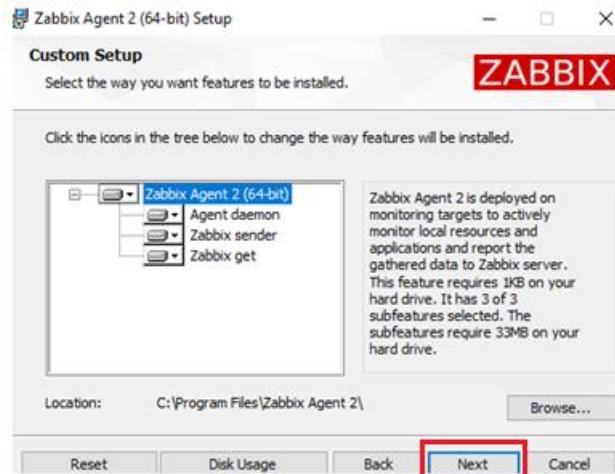
The screenshot shows the 'Utilisateur' creation form. The user 'anadmin' has been entered. The 'Groupes' field contains 'Zabbix administrators'. The 'Rôle utilisateur' dropdown is set to 'Super admin role'. Other fields like 'Prénom', 'Nom de famille', and 'Mot de passe' are also filled out. The 'Ajouter' button is visible at the bottom.

Nom d'utilisateur	Prénom	Nom de famille	Rôle utilisateur	Groupes	Est connecté ?	Connexion	Accès à l'interface	Accès API	Mode debug	État
Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Oui (03/05/2025 23:18:13)	Ok	Interne	Activé	Désactivé	Activé
anadmin			Super admin role	Zabbix administrators	Non	Ok	Valeur système par défaut	Activé	Désactivé	Activé
guest			Guest role	Disabled, Guests, Internal	Non	Ok	Interne	Désactivé	Désactivé	Désactivé

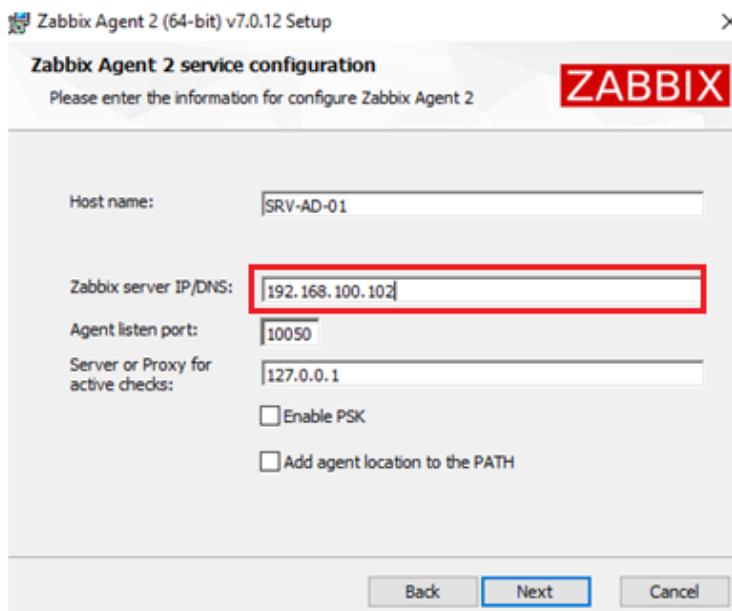
### 3.2) Configuration des agents dans la console d'administration Zabbix

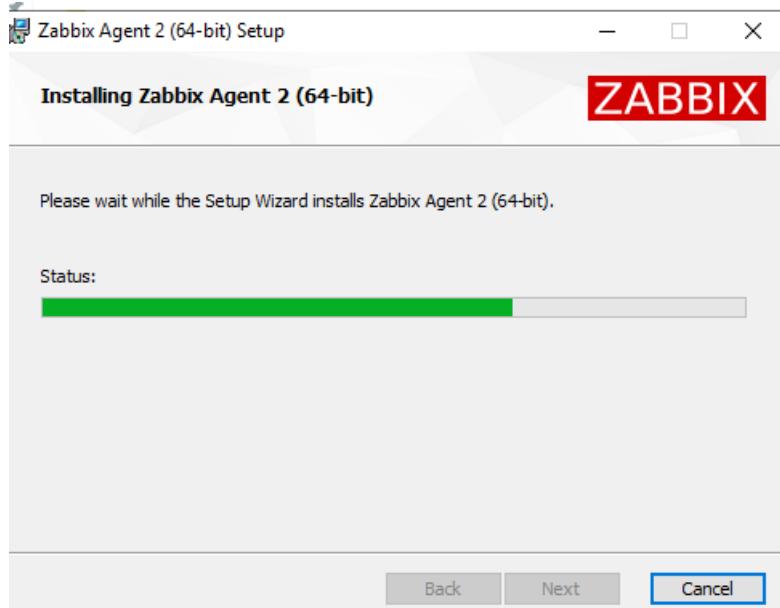
Pour procéder à l'installation de l'agent Zabbix sur les machines à superviser, commencer par récupérer l'installateur précédemment déposé sur le partage réseau.





Dans cette étape, renseigner l'adresse IP du serveur Zabbix (dans notre cas **192.168.100.102**) afin que l'agent puisse communiquer avec lui.





## Installation d'un agent zabbix sur une machine Ubuntu

Commencer par se rendre sur la page suivante :

[https://www.zabbix.com/fr/download?zabbix=6.4&os\\_distribution=ubuntu&os\\_version=22.04&components=agent&db=&ws=](https://www.zabbix.com/fr/download?zabbix=6.4&os_distribution=ubuntu&os_version=22.04&components=agent&db=&ws=)

Une fois sur cette page, sélectionner les informations correspondant à votre environnement.

VERSION DE ZABBIX	OS DISTRIBUTION	VERSION DU SYSTÈME D'EXPLOITATION	ZABBIX COMPONENT	BASE DE DONNÉES	SERVEUR WEB
6.4	Alma Linux	22.04 (Jammy)	Server, Frontend, Agent	---	---
6.0 LTS	CentOS	20.04 (Focal)	Proxy		
5.0 LTS	Debian	18.04 (Bionic)	Agent		
7.0 PRE-RELEASE	OpenSUSE Leap	16.04 (Xenial)	Agent 2		
	Oracle Linux	14.04 (Trusty)	Java Gateway		
	Raspberry Pi OS		Web Service		
	Red Hat Enterprise Linux				
	Rocky Linux				
	SUSE Linux Enterprise Server				
	Ubuntu				
	Ubuntu (arm64)				

En fonction des informations sélectionnées, la configuration proposée variera. Dans notre cas, voici celle à appliquer :

```
# wget https://repo.zabbix.com/zabbix/6.4/ubuntu/pool/main/z/zabbix-release/zabbix-release\_6.4-1+ubuntu22.04\_all.deb
```

```
# sudo dpkg -i zabbix-release_6.4-1+ubuntu22.04_all.deb
```

```
# sudo apt update  
sudo apt install zabbix-agent2
```

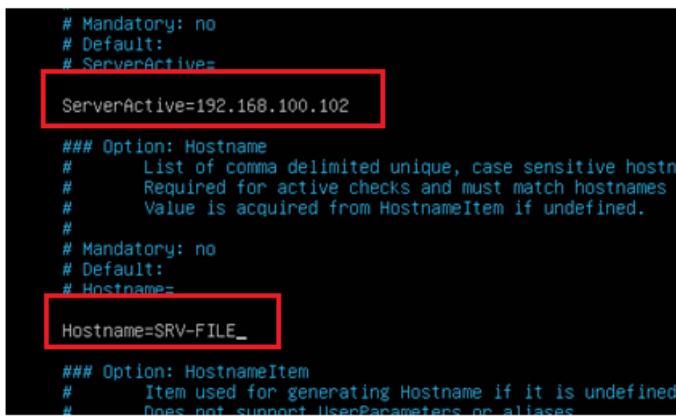
L'agent a bien été installé.

Une fois l'agent installé, exécuter la commande suivante pour accéder au fichier de configuration de l'agent Zabbix :

```
sudo nano /etc/zabbix/zabbix_agent2.conf
```

Dans le fichier de configuration, modifier les variables ServerActive et Hostname de manière à obtenir ce qui suit :

- ServerActive = adresse IP du serveur Zabbix
- Hostname = nom de l'hôte sur lequel l'agent est installé



```
# Mandatory: no
# Default:
# ServerActive=
ServerActive=192.168.100.102

### Option: Hostname
#      List of comma delimited unique, case sensitive hostnames
#      Required for active checks and must match hostnames
#      Value is acquired from HostnameItem if undefined.
#
# Mandatory: no
# Default:
# Hostname=
Hostname=SRV-FILE_

### Option: HostnameItem
#      Item used for generating Hostname if it is undefined
#      Does not support UserParameters or aliases
```

Pour finaliser la configuration de l'agent, redémarrer puis activer le service Zabbix Agent avec les commandes suivantes :

```
sudo systemctl restart zabbix-agent
```

```
sudo systemctl enable zabbix-agent
```

```
anadmin@srv-file:~$ sudo systemctl restart zabbix-agent
anadmin@srv-file:~$ sudo systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-
install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent

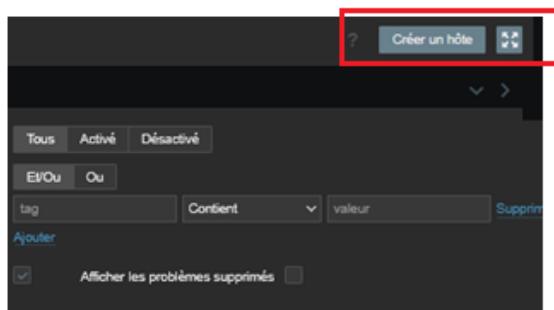
```

## Configuration de l'agent sur la console d'administration zabbix

Commencer par se rendre dans la console d'administration Zabbix. Dans le bandeau de gauche, déplier le menu "**Surveillance**", puis cliquer sur "**Hôtes**" pour accéder à la gestion des permissions.



Ici, cliquer sur "**Créer un hôte**" pour ajouter une nouvelle machine à superviser.



Ici, définir une configuration similaire à celle-ci-dessous :

1. **Nom de l'hôte** : indiquer le nom exact de la machine sur laquelle l'agent Zabbix a été installé,
2. **Modèle et Groupe d'hôtes** : sélectionner un modèle (ex. Linux by Zabbix agent) et un groupe d'hôtes approprié,
3. **Adresse IP** : renseigner l'IP de l'hôte,
4. **Description** : ajouter une description pour contextualiser la supervision.

Enfin, cliquer sur "Ajouter".

**Nouvel hôte**

Hôte	IPMI	Tags	Macros	Inventaire	Chiffrement	Table de correspondance
* Nom de l'hôte	SRV-AD-01					
Nom visible	SRV-AD-01					
Modèles	Windows by Zabbix agent <input type="button" value="Sélectionner"/>	taper ici pour rechercher				
* Groupes d'hôtes	Virtual machines <input type="button" value="Sélectionner"/>	taper ici pour rechercher				
Interfaces	Type adresse IP	Nom DNS	Connexion à	Port	Défaut	
	Agent 192.168.100.10		IP	DNS	10050	<input checked="" type="radio"/> Supprimer
<input type="button" value="Ajouter"/> <b>Description</b> : Contrôleur de domaine 1						
Surveillé via le proxy: <input type="button" value="pas de proxy"/> <input checked="" type="checkbox"/> Activé						
<input type="button" value="Ajouter"/> <input type="button" value="Annuler"/>						

## Retourner dans la sous-catégorie Hôtes.

Ici, retrouvez l'ensemble des hôtes configurés et vus par Zabbix.

L'hôte **SRV-AD-01**, tout juste ajouté, sera disponible et configurable dans cet espace.

Cliquer sur **Tableau de bord** pour obtenir plus de détails concernant cet hôte.



Ci-dessous, l'interface Zabbix affiche le comportement :

