
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

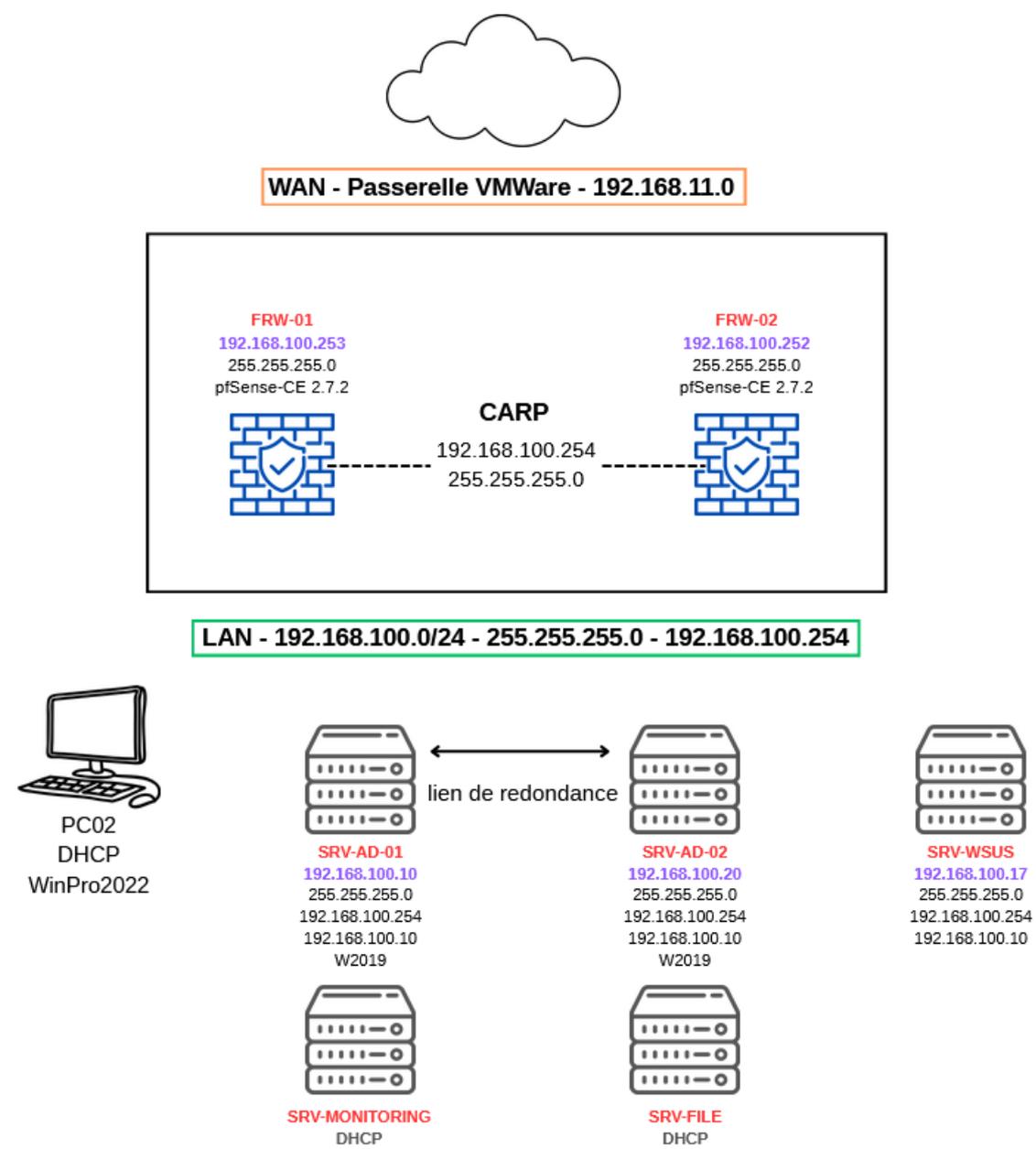
Zabbix – Solution de supervision et de monitoring

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)

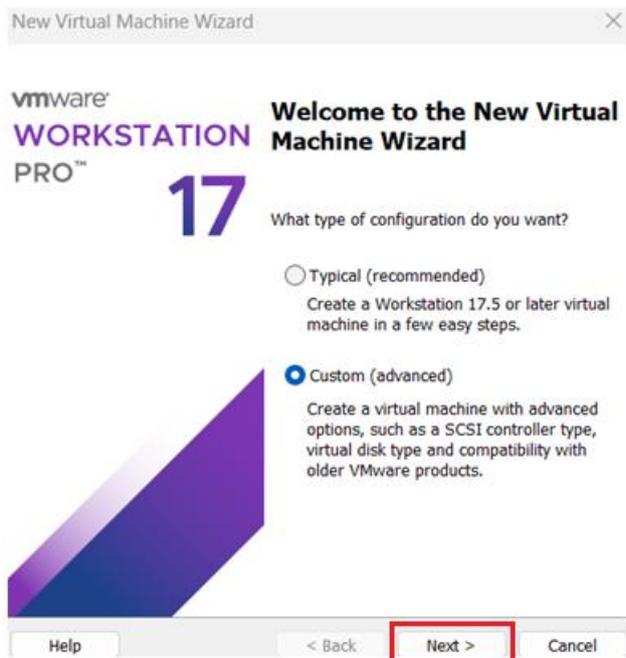
Prérequis de création des machines virtuelles :

2 machines virtuelles (VM)

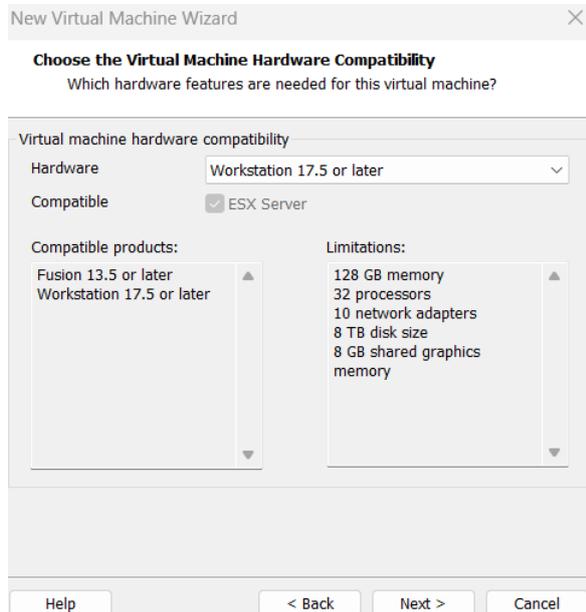
- Configuration :
 - 256 Mo de RAM
 - 1 processeur
 - 1 disque dur de 20 Go
 - 2 cartes réseau (1 en NAT, 1 en réseau interne (LAN))

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.



New Virtual Machine Wizard

Choose the Virtual Machine Hardware Compatibility
Which hardware features are needed for this virtual machine?

Virtual machine hardware compatibility

Hardware: Workstation 17.5 or later

Compatible: ESX Server

Compatible products:

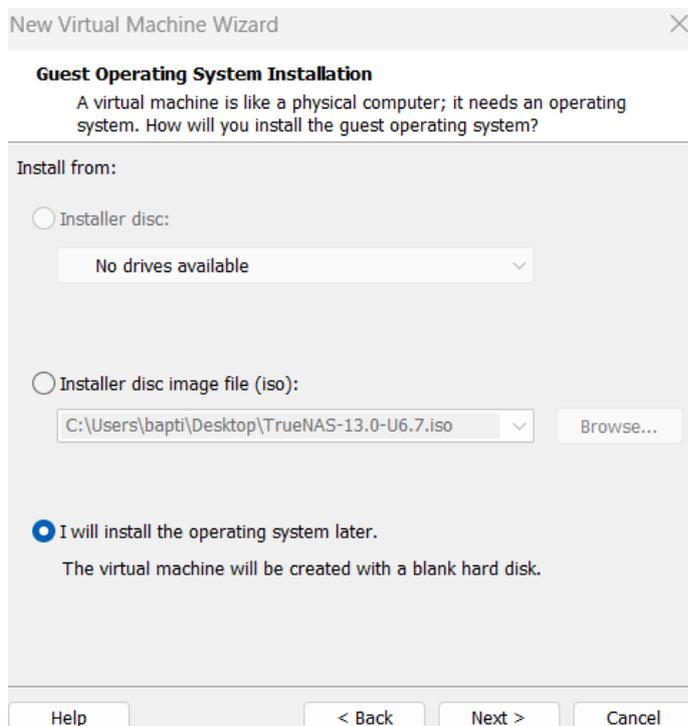
- Fusion 13.5 or later
- Workstation 17.5 or later

Limitations:

- 128 GB memory
- 32 processors
- 10 network adapters
- 8 TB disk size
- 8 GB shared graphics memory

Buttons: Help, < Back, Next >, Cancel

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



New Virtual Machine Wizard

Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

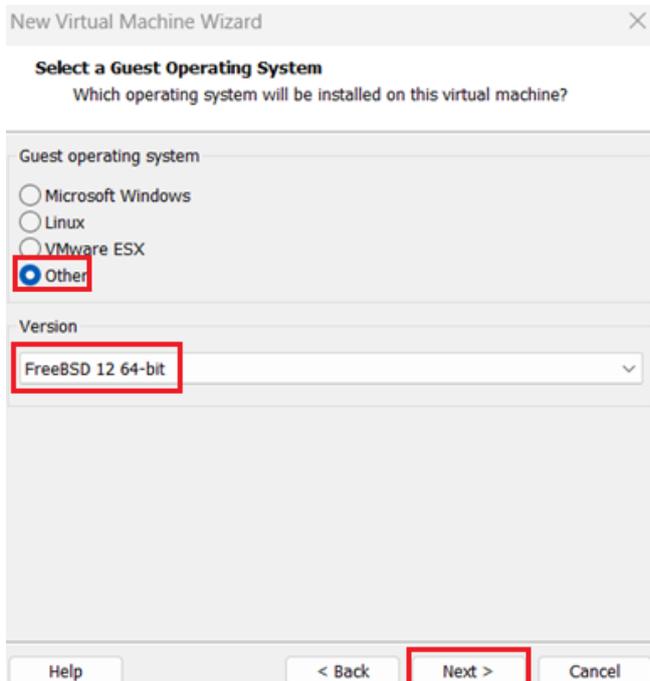
Installer disc:
No drives available

Installer disc image file (iso):
C:\Users\bapti\Desktop\TrueNAS-13.0-U6.7.iso Browse...

I will install the operating system later.
The virtual machine will be created with a blank hard disk.

Buttons: Help, < Back, Next >, Cancel

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



New Virtual Machine Wizard

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system

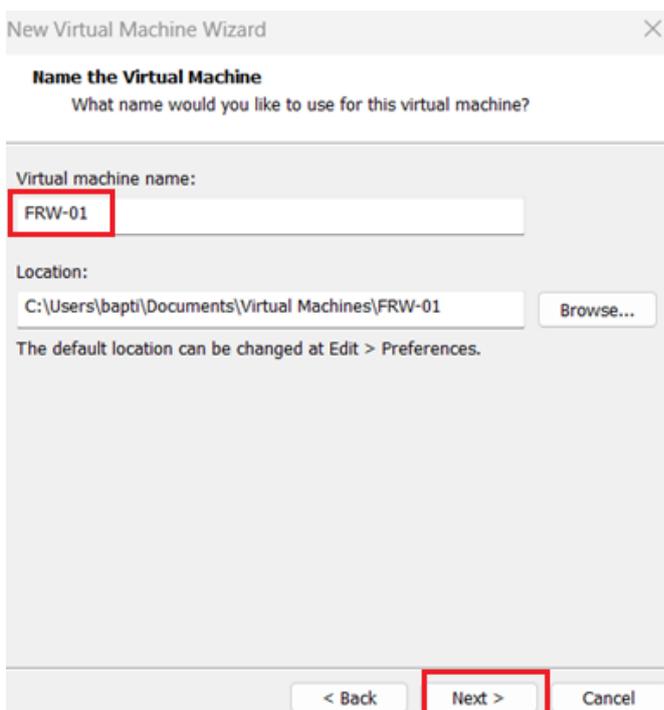
- Microsoft Windows
- Linux
- VMware ESX
- Other

Version

FreeBSD 12 64-bit

Help < Back Next > Cancel

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



New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:

FRW-01

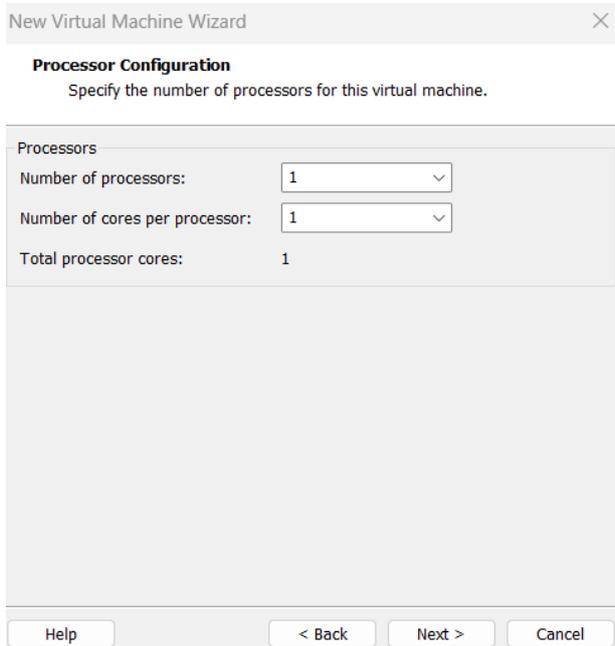
Location:

C:\Users\bapti\Documents\Virtual Machines\FRW-01 Browse...

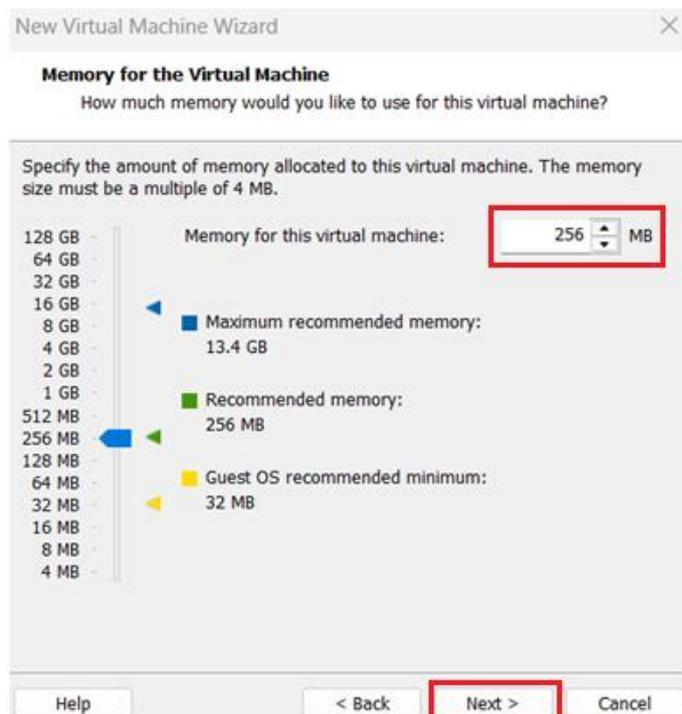
The default location can be changed at Edit > Preferences.

< Back Next > Cancel

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 ✕

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.

New Virtual Machine Wizard ×

Select I/O Controller Types
Which SCSI controller type would you like to use for SCSI virtual disks?

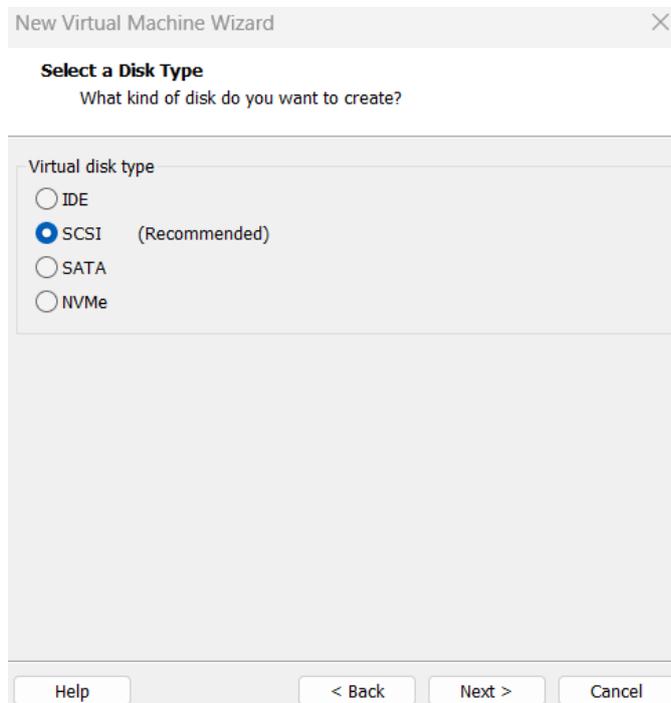
I/O controller types

SCSI Controller:

- BusLogic (Not available for 64-bit guests)
- LSI Logic (Recommended)
- LSI Logic SAS
- Paravirtualized SCSI

Help < Back Next > Cancel

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



New Virtual Machine Wizard

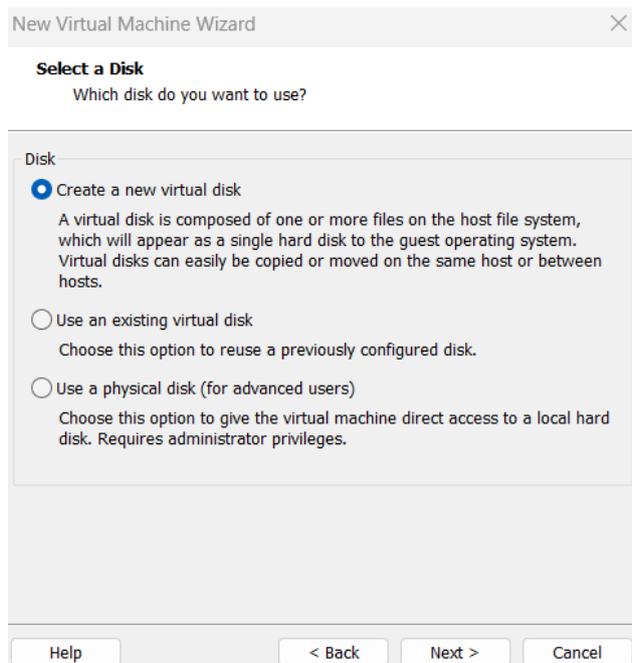
Select a Disk Type
What kind of disk do you want to create?

Virtual disk type

- IDE
- SCSI (Recommended)
- SATA
- NVMe

Buttons: Help, < Back, Next >, Cancel

Création d'un nouveau disque virtuel.



New Virtual Machine Wizard

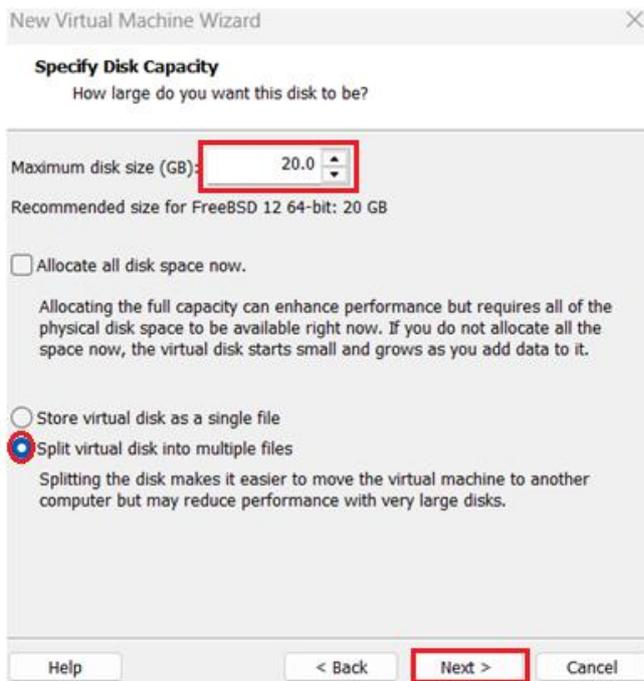
Select a Disk
Which disk do you want to use?

Disk

- Create a new virtual disk
A virtual disk is composed of one or more files on the host file system, which will appear as a single hard disk to the guest operating system. Virtual disks can easily be copied or moved on the same host or between hosts.
- Use an existing virtual disk
Choose this option to reuse a previously configured disk.
- Use a physical disk (for advanced users)
Choose this option to give the virtual machine direct access to a local hard disk. Requires administrator privileges.

Buttons: Help, < Back, Next >, Cancel

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



New Virtual Machine Wizard

Specify Disk Capacity
How large do you want this disk to be?

Maximum disk size (GB):

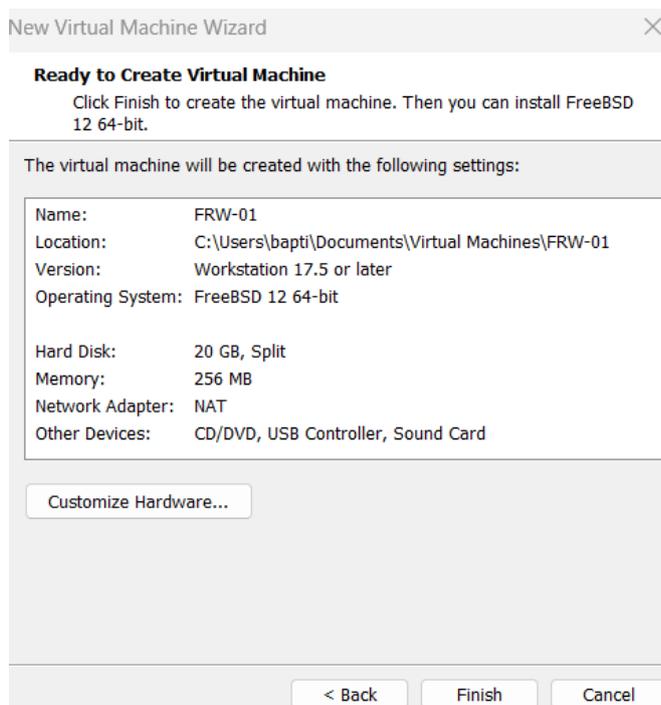
Recommended size for FreeBSD 12 64-bit: 20 GB

Allocate all disk space now.
Allocating the full capacity can enhance performance but requires all of the physical disk space to be available right now. If you do not allocate all the space now, the virtual disk starts small and grows as you add data to it.

Store virtual disk as a single file
 Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help < Back **Next >** Cancel

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



New Virtual Machine Wizard

Ready to Create Virtual Machine
Click Finish to create the virtual machine. Then you can install FreeBSD 12 64-bit.

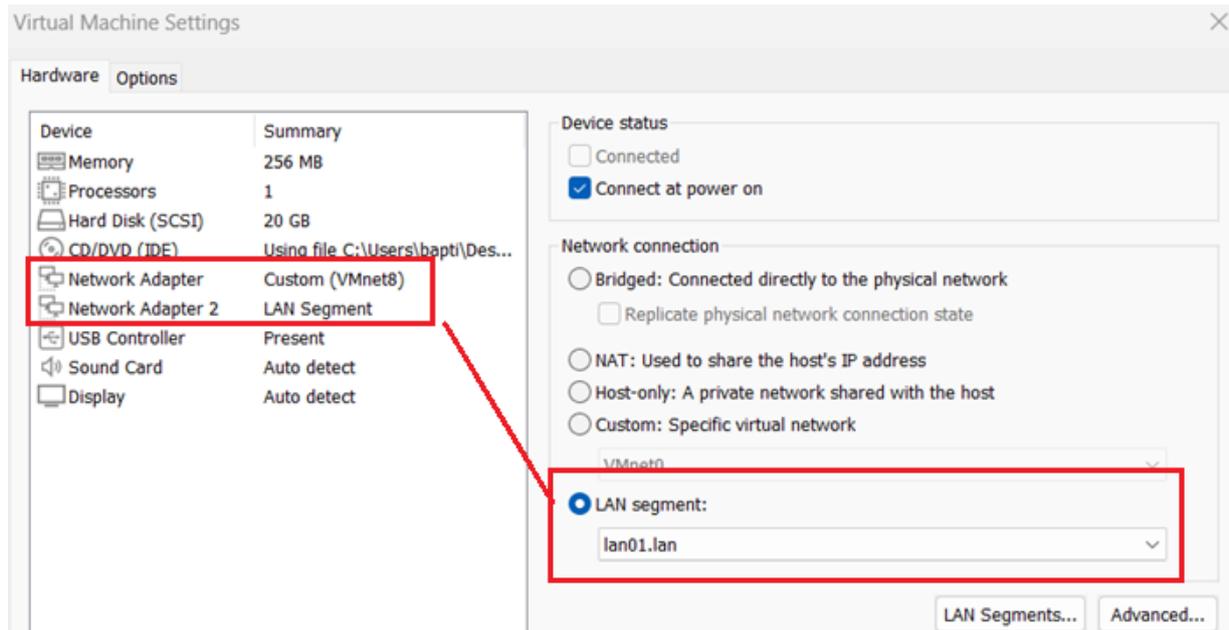
The virtual machine will be created with the following settings:

Name:	FRW-01
Location:	C:\Users\bapti\Documents\Virtual Machines\FRW-01
Version:	Workstation 17.5 or later
Operating System:	FreeBSD 12 64-bit
Hard Disk:	20 GB, Split
Memory:	256 MB
Network Adapter:	NAT
Other Devices:	CD/DVD, USB Controller, Sound Card

Customize Hardware...

< Back Finish Cancel

Configuration FRW-01 et FRW-02

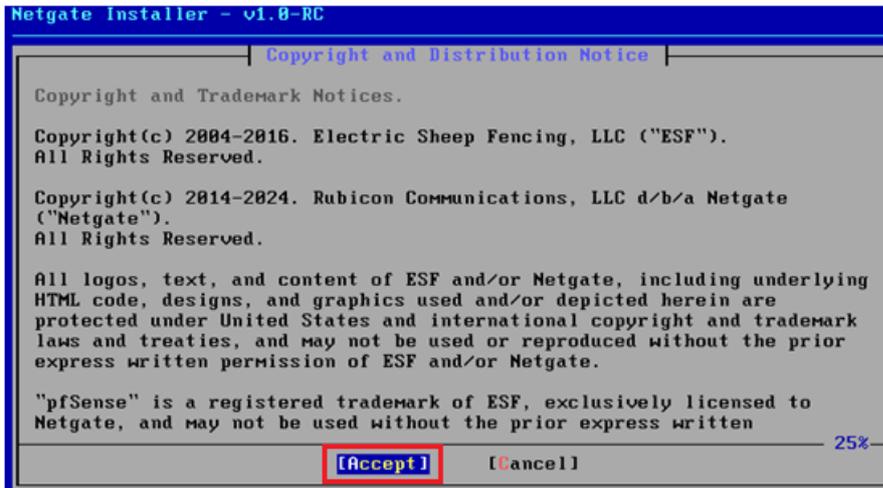


On démarre les deux pare-feux pfSense pour procéder à leur installation

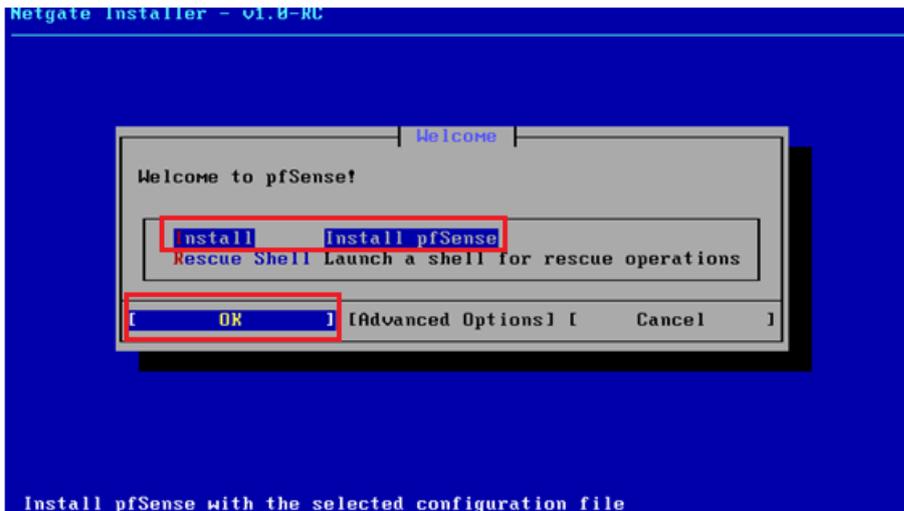
Installation du système FreeBSD pour pfSense



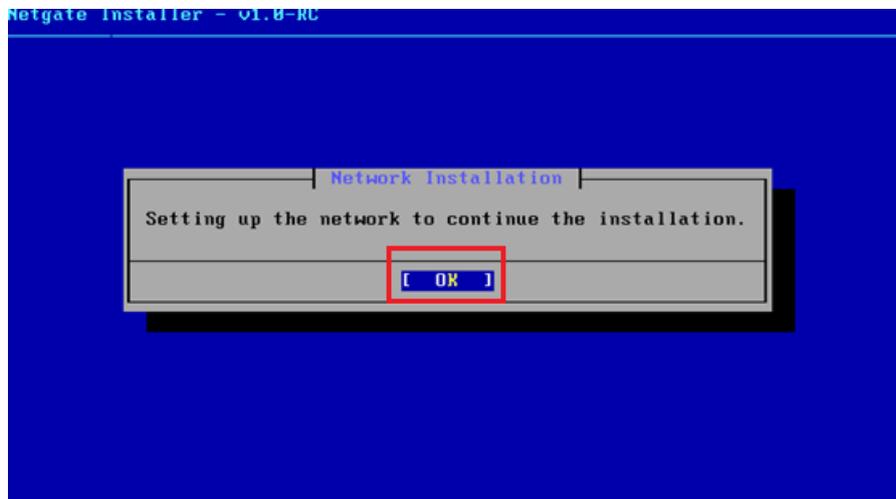
À l'écran des conditions d'utilisation, appuyez sur la touche [ENTRÉE] pour accepter et poursuivre l'installation.



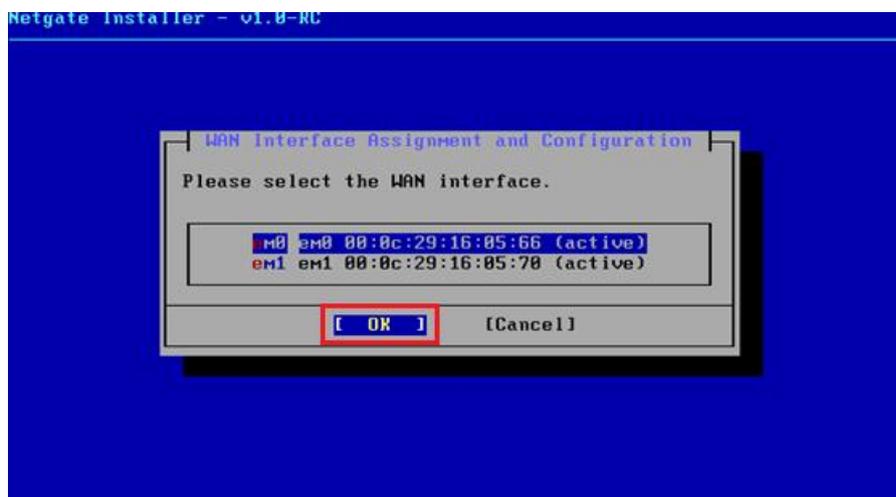
Sélectionnez « Install » à l'aide des flèches directionnelles, puis appuyez sur la touche [ENTRÉE].



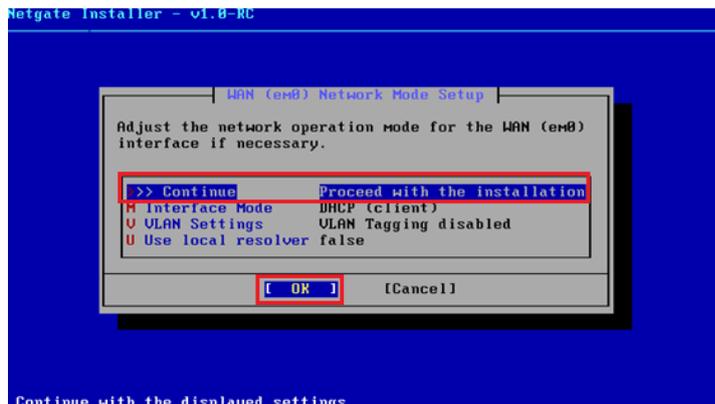
À cette étape, appuyer sur la touche [ENTRÉE] pour permettre à pfSense de configurer automatiquement la connexion réseau et accéder à Internet afin de poursuivre l'installation.



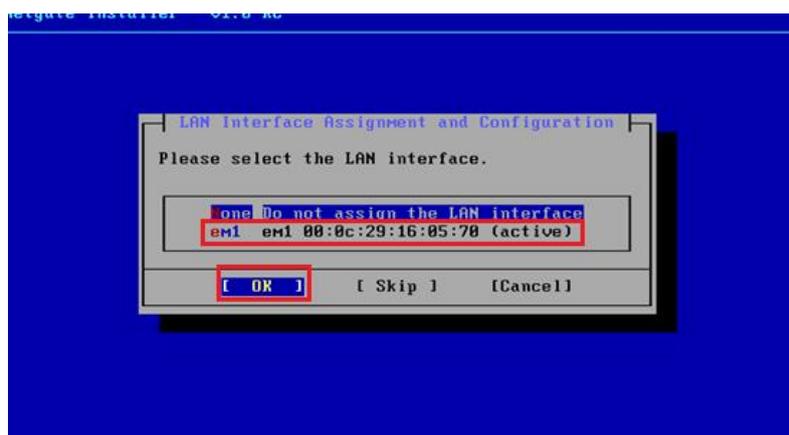
Sélectionnez l'interface em0, pour configurer le WAN puis appuyez sur [ENTRÉE].



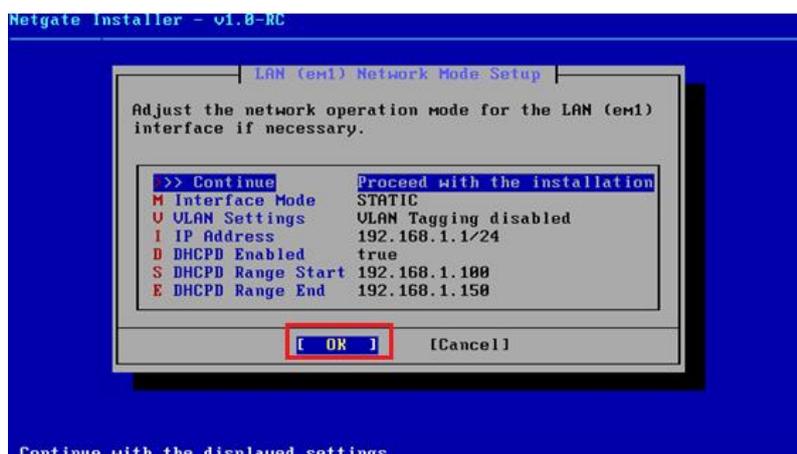
Sélectionnez « Continue » pour poursuivre l'installation et appuyez sur [ENTRÉE].



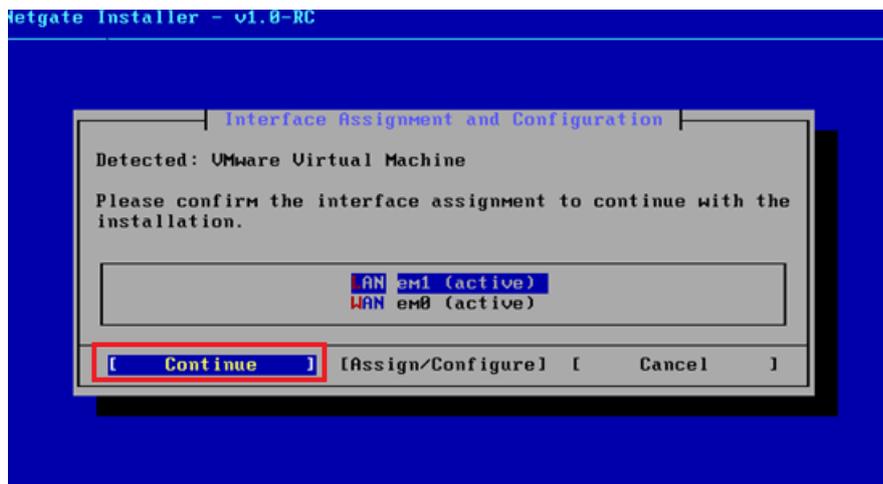
Sélectionnez em1 comme interface LAN, puis validez avec [ENTRÉE].



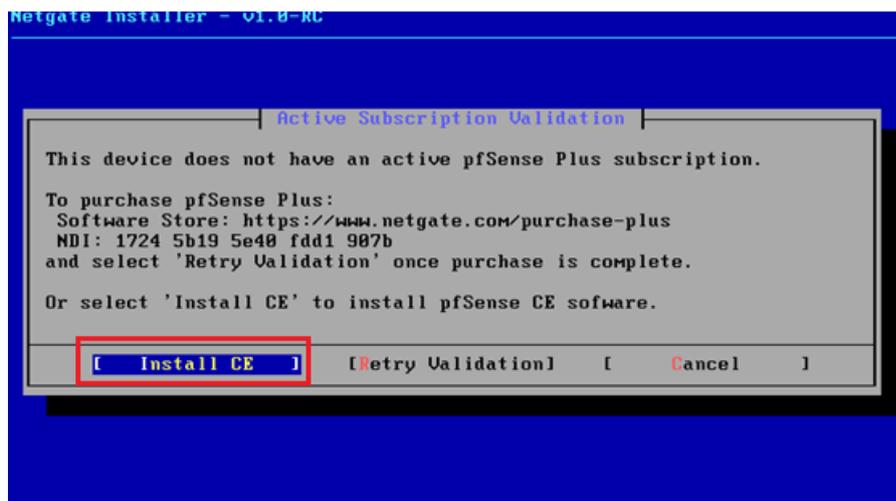
Laissez les paramètres proposés par défaut puis validez avec [ENTRÉE] pour continuer l'installation.



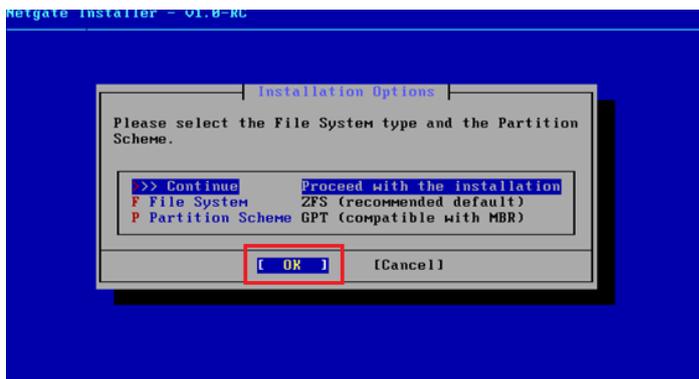
Confirmez l'assignation des interfaces en appuyant sur [ENTRÉE] pour continuer.



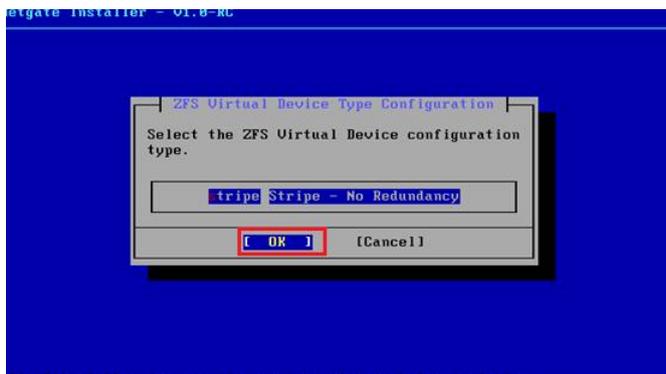
Sélectionnez "Install CE" pour lancer l'installation de la version gratuite de pfSense.



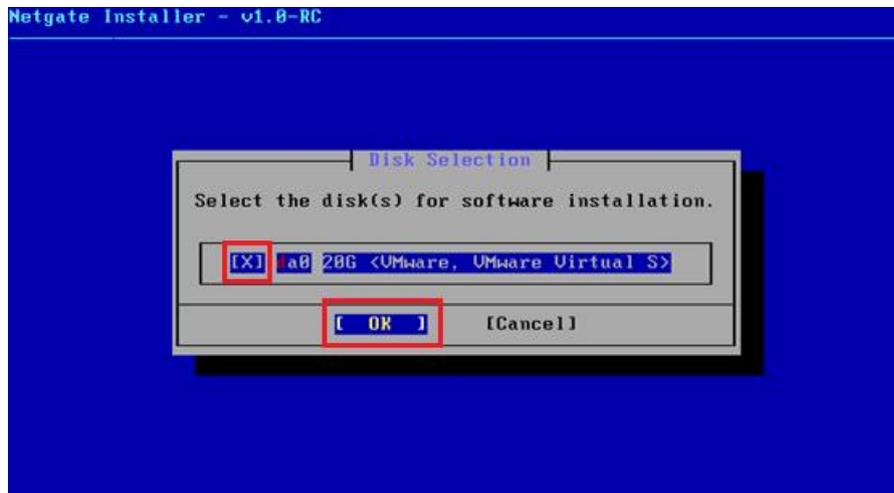
Appuie sur [ENTRÉE] pour continuer l'installation avec ces paramètres recommandés.



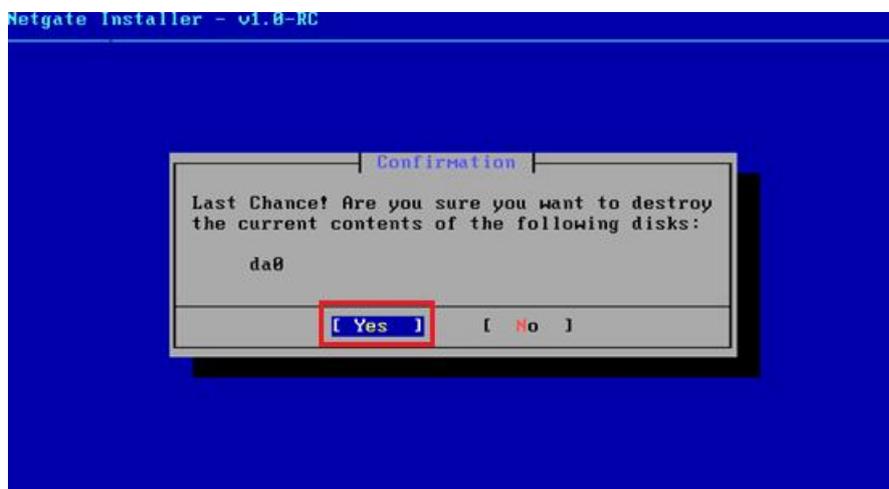
Sélectionnez Stripe – No Redundancy puis validez en appuyant sur [ENTRÉE].



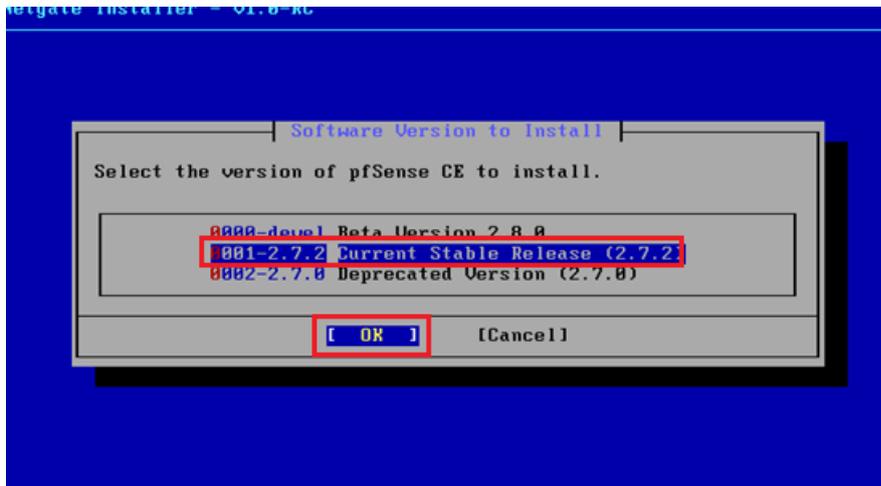
Sélectionnez le disque proposé avec la barre d'espace pour l'installation (ici, le disque de 20 Go), puis appuyez sur [ENTRÉE].



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

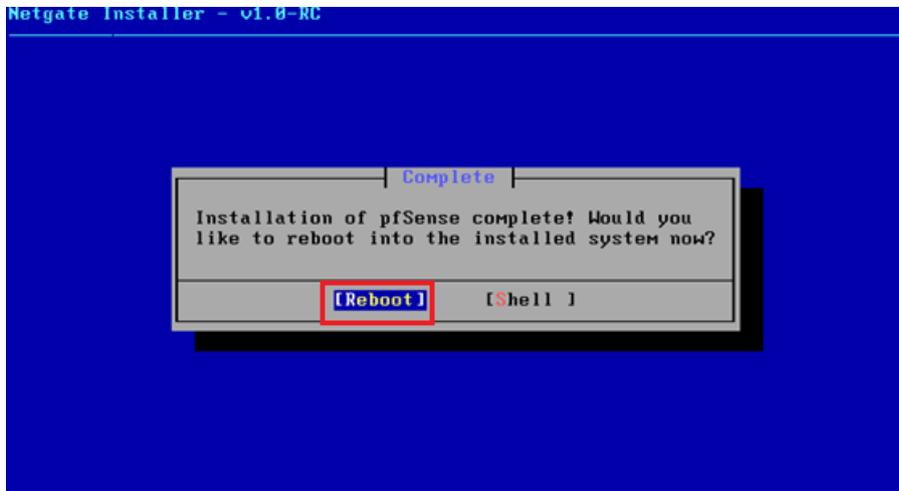


Sélectionnez la version 2.7.2 Current Stable Release, puis appuyez sur [ENTRER] pour continuer l'installation.



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

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

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

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

Enter an option: █

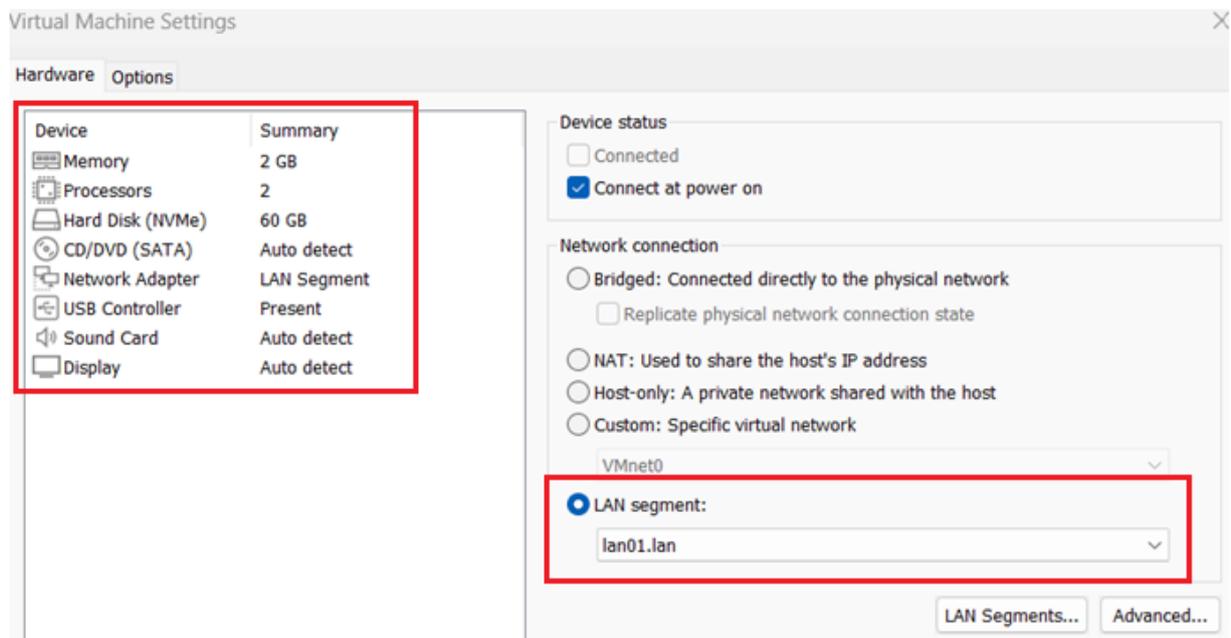
```

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 :



The screenshot shows the 'Virtual Machine Settings' window for a VM named 'SRV-AD-01'. The 'Hardware' tab is selected, and the 'Options' sub-tab is active. A red box highlights the hardware configuration table on the left, and another red box highlights the network connection settings on the right.

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status

- Connected
- Connect at power on

Network connection

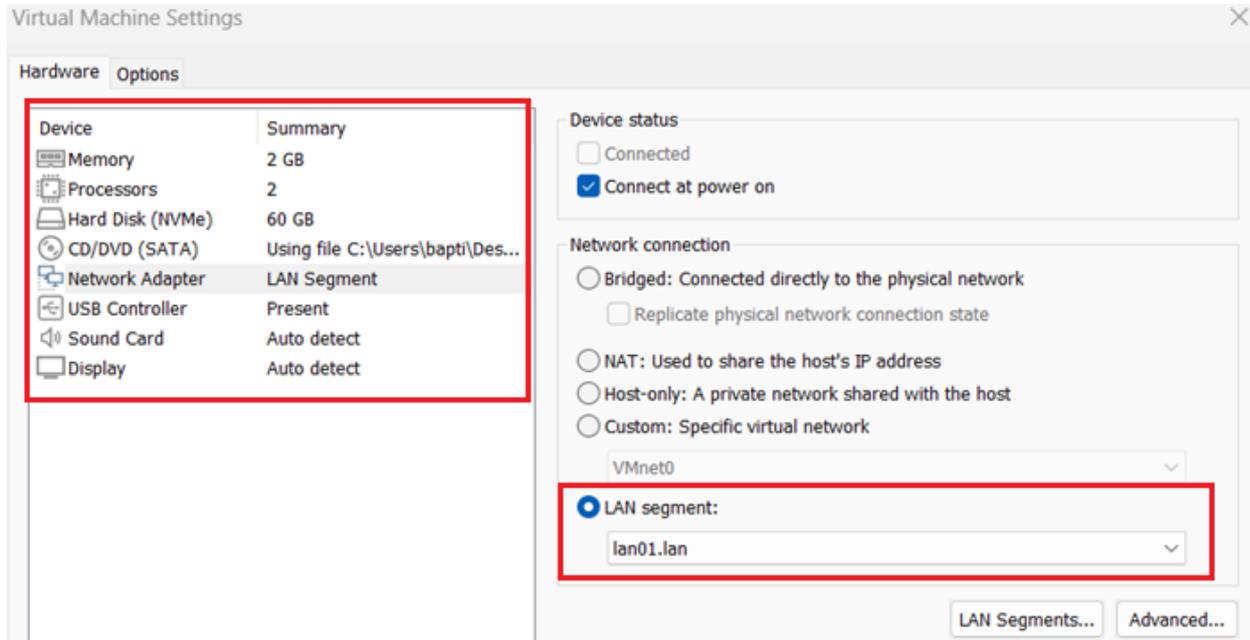
- Bridged: Connected directly to the physical network
 - Replicate physical network connection state
- NAT: Used to share the host's IP address
- Host-only: A private network shared with the host
- Custom: Specific virtual network

VMnet0

LAN segment:
lan01.lan

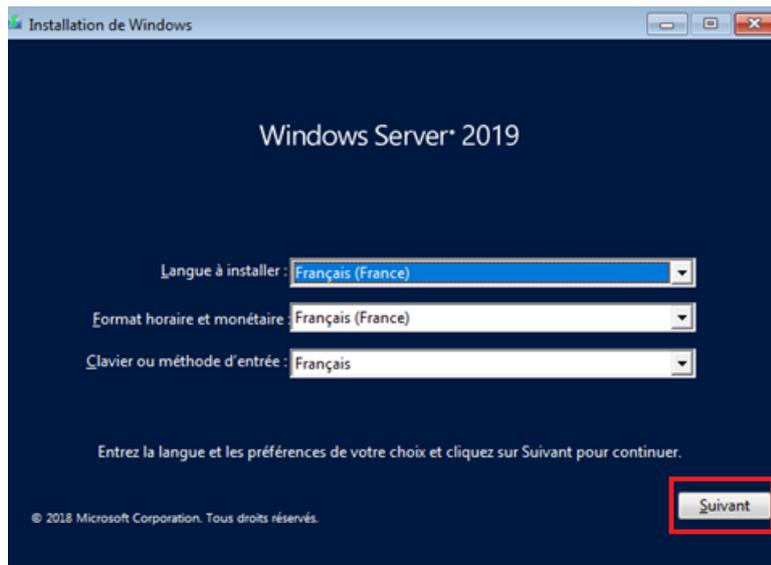
LAN Segments... Advanced...

Configuration de SRV-AD-02 :

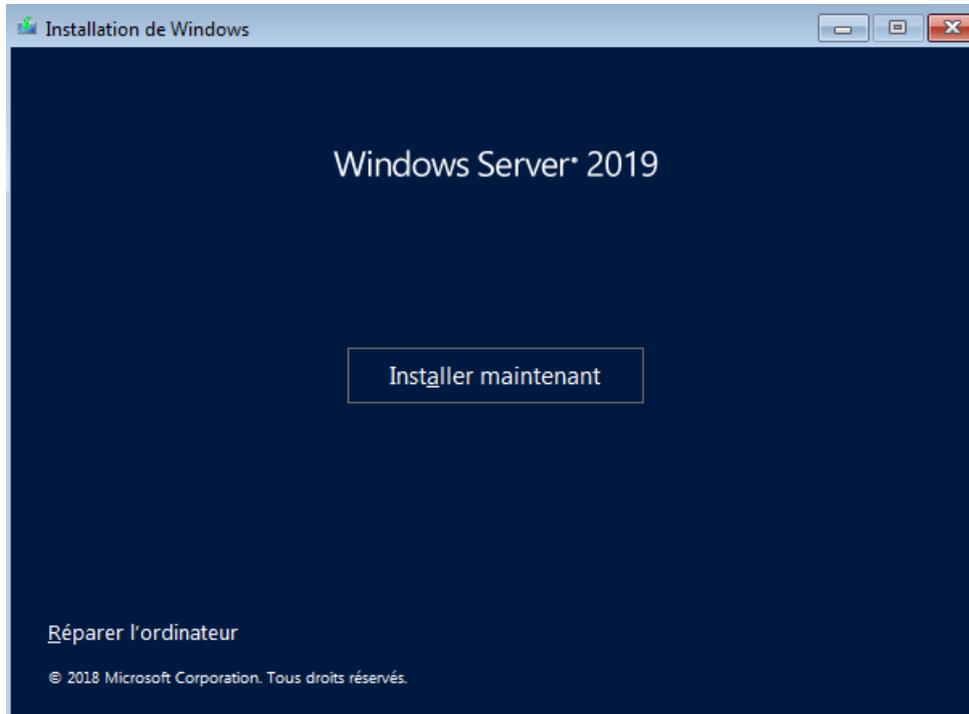


On peut dans un premier temps démarrer les deux serveurs pour procéder à l'installation de base de Windows Server 2019.

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.

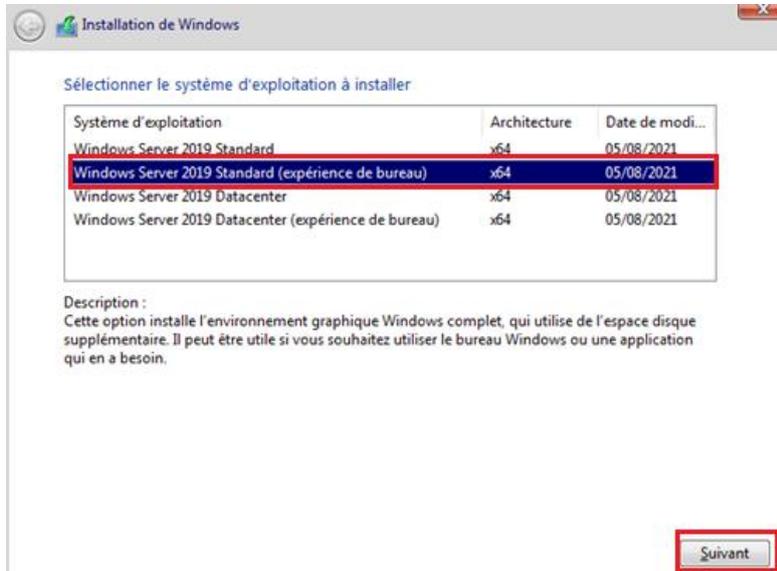


Cliquez sur **Installer maintenant** pour lancer l'installation de Windows Server 2019.

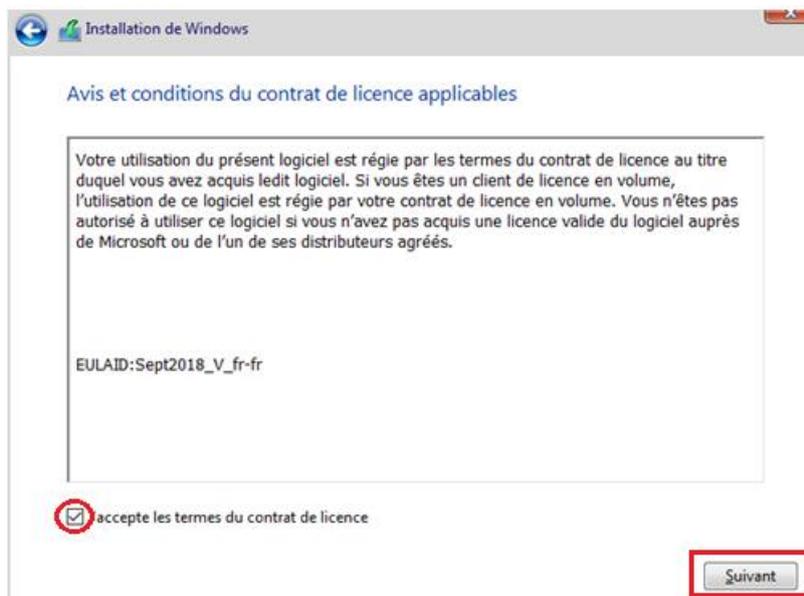


Patientez...

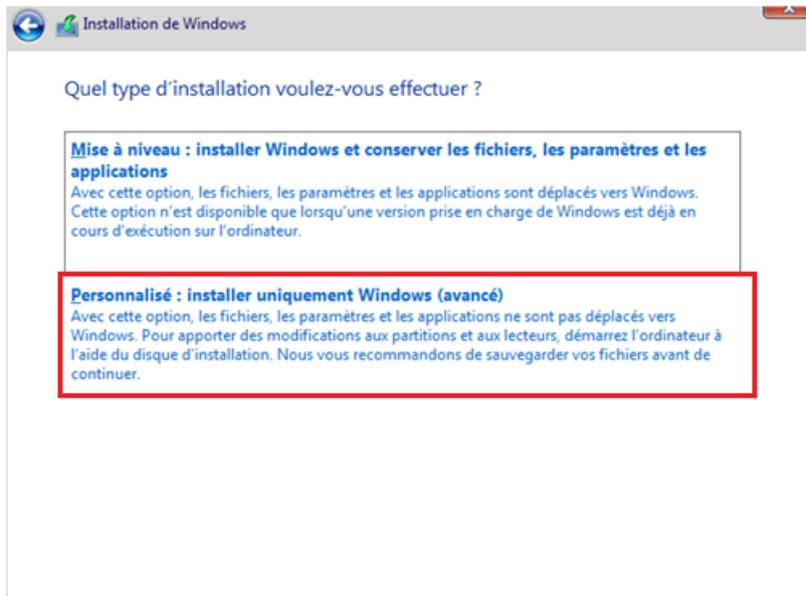
Sélectionnez **Windows Server 2019 Standard (expérience de bureau)**, puis cliquez sur **Suivant** pour bénéficier de l'interface graphique complète.



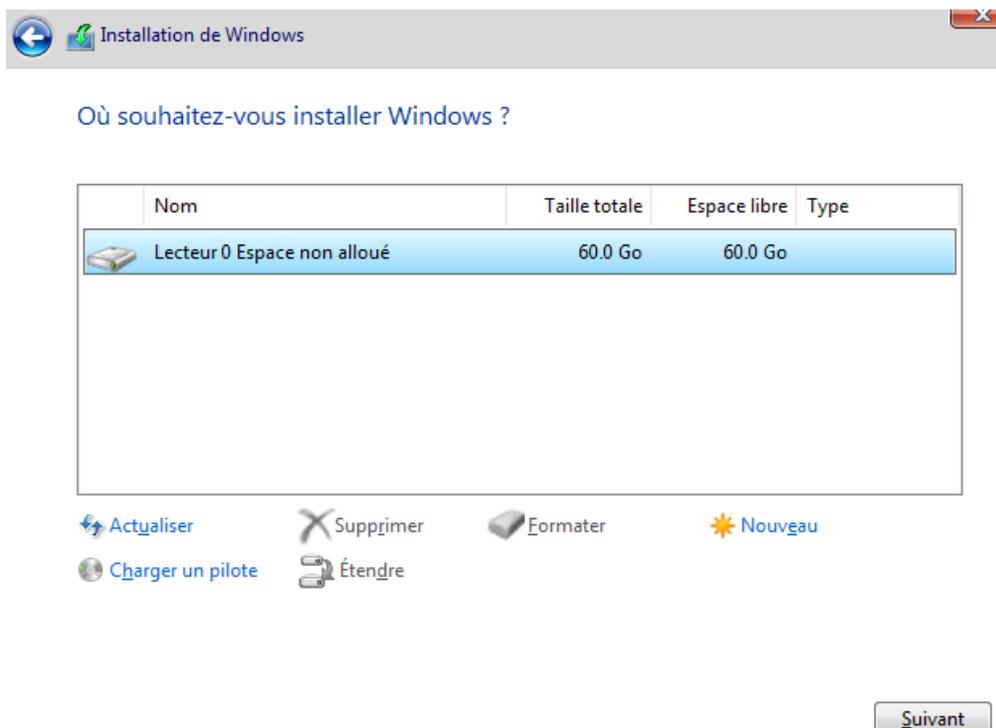
Cochez "J'accepte les termes du contrat de licence", puis cliquez sur **Suivant** pour continuer l'installation.



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

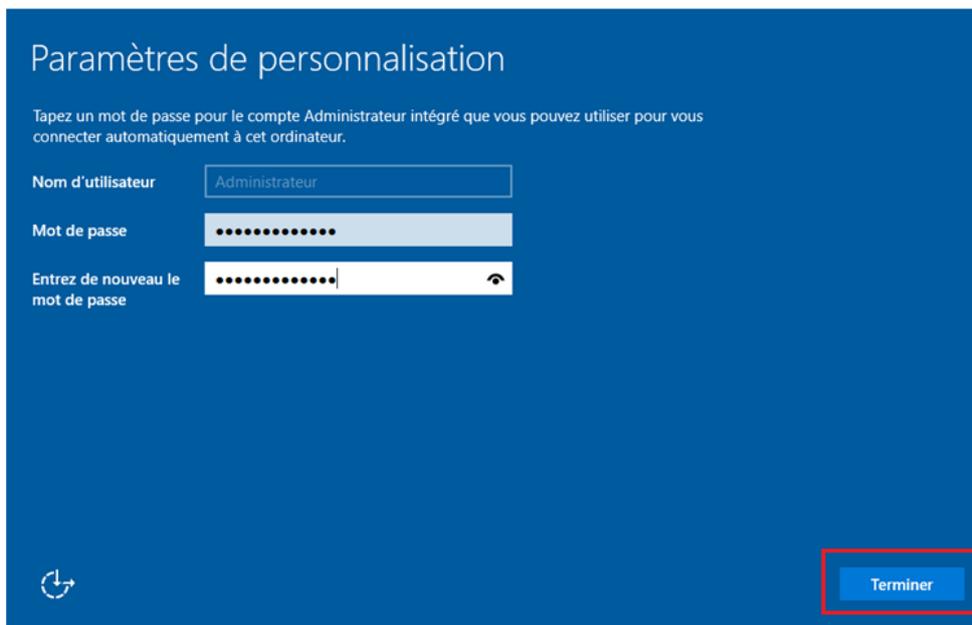


Choisissez le lecteur avec l'espace non alloué, puis cliquez sur **Suivant** pour lancer l'installation de Windows Server 2019.



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.



Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

Nom d'utilisateur

Mot de passe

Entrez de nouveau le mot de passe 

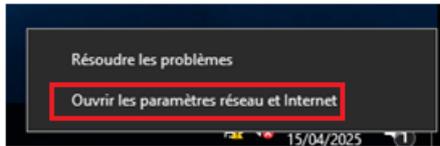
 Terminer

Vous êtes désormais connecté à votre environnement Windows Server.

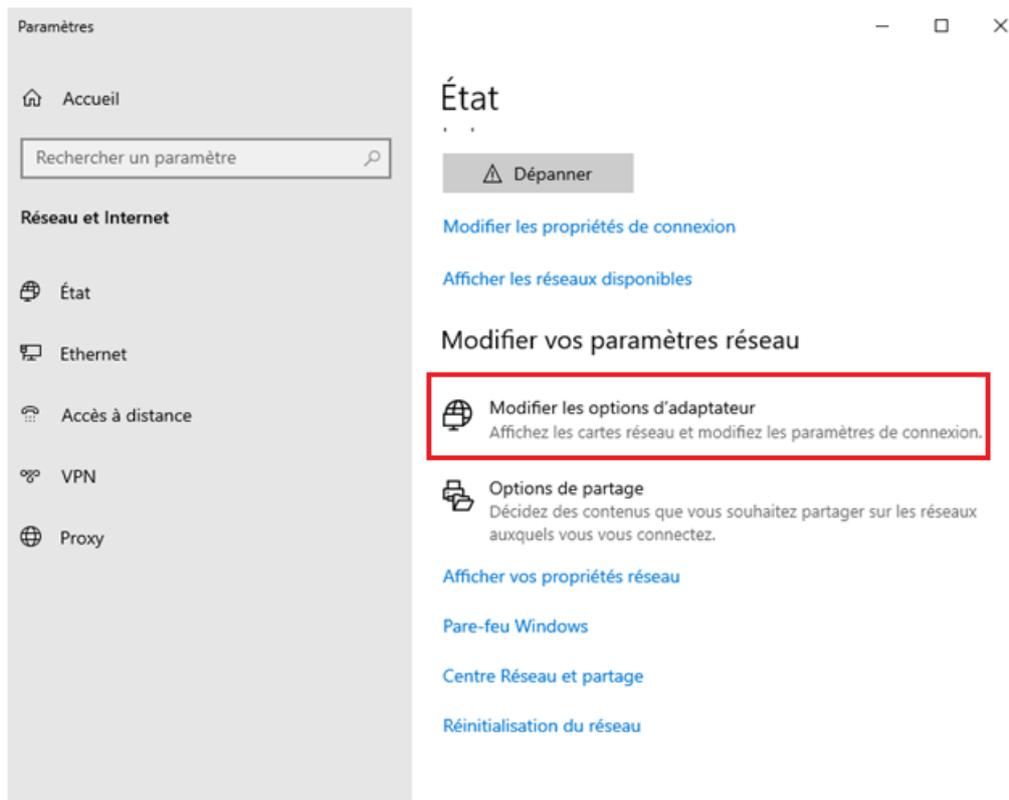
On va maintenant configurer les paramètres réseau de chaque serveur.

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.

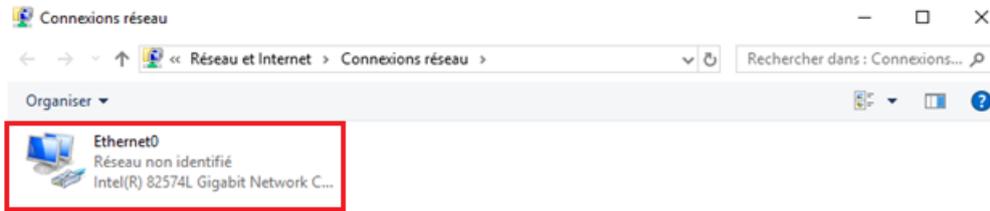




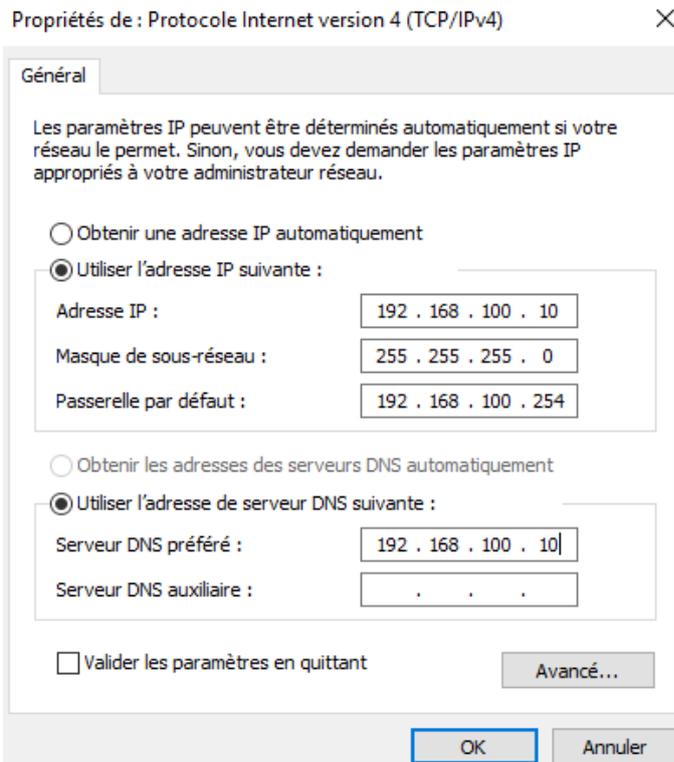
Cliquez sur "Modifier les options d'adaptateur".



Clic droit sur Ethernet0 > Propriétés > Protocole IPv4 attribue



STG-AD-01



SRV-AD-02

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

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...

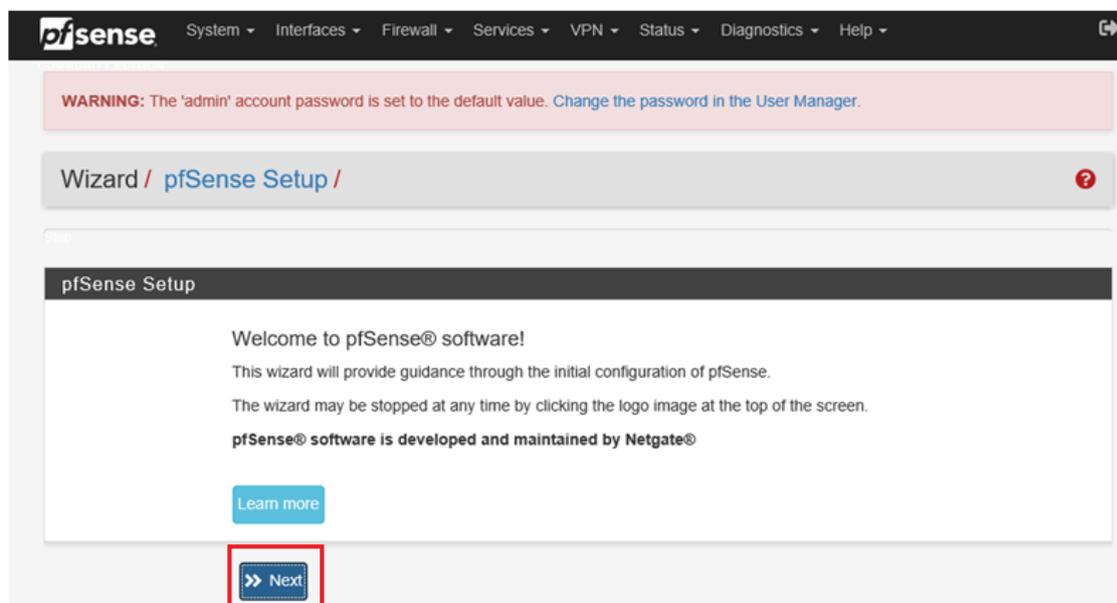
OK Annuler

2.2) Configuration d'un CARP

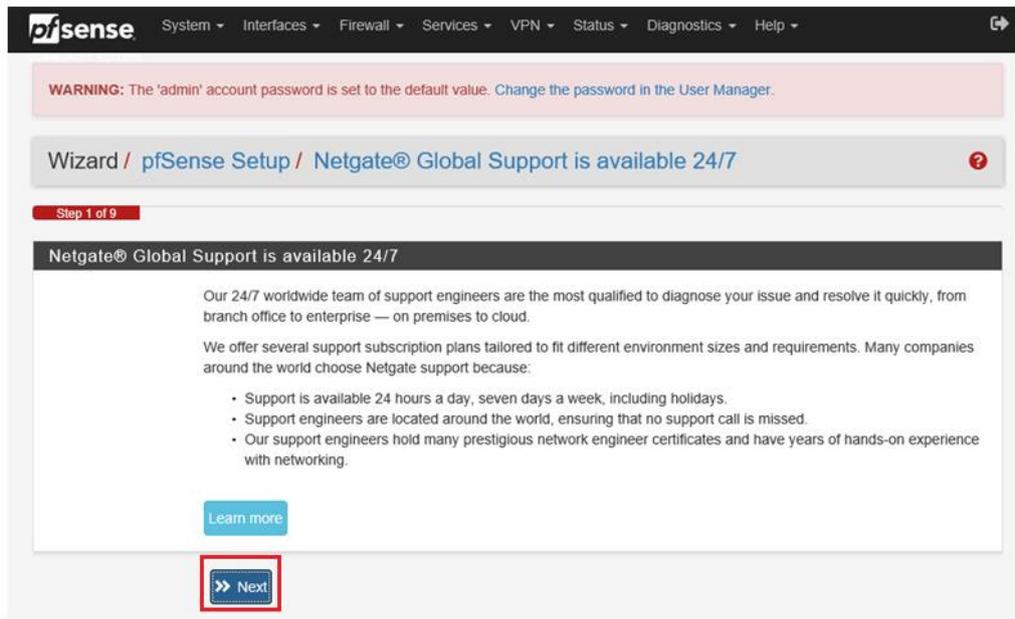
Pour configurer le CARP depuis **FRW-01**, accéder à l'interface web du pare-feu via l'adresse :

☞ <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.

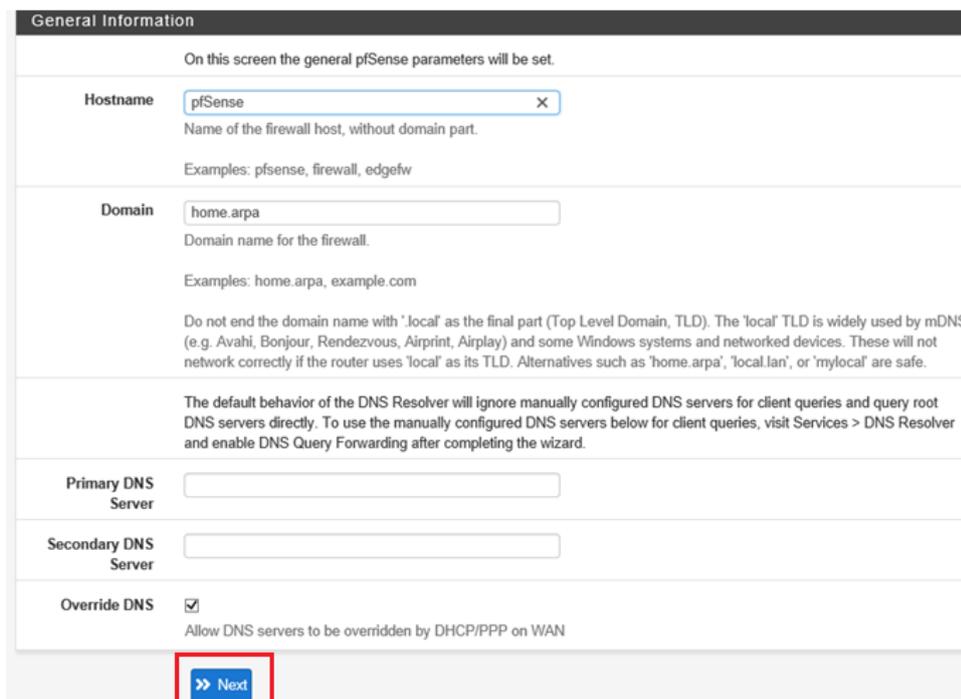


Le message d'information concernant le support 24/7 de Netgate apparaît ensuite. Cliquez sur "Next" pour continuer.



The screenshot shows the pfSense web interface. At the top, there is a navigation menu with items like System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the breadcrumb trail reads "Wizard / pfSense Setup / Netgate® Global Support is available 24/7". The main content area is titled "Netgate® Global Support is available 24/7" and contains text about their 24/7 support team and a list of reasons why companies choose their support. A "Learn more" button is present, and a "Next" button is highlighted with a red box.

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

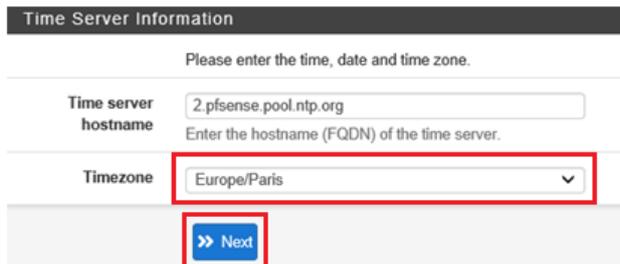


The screenshot shows the "General Information" configuration page in pfSense. It contains the following fields and options:

- Hostname:** A text input field containing "pfSense". Below it, a note says "Name of the firewall host, without domain part." and "Examples: pfsense, firewall, edgefw".
- Domain:** A text input field containing "home.arpa". Below it, a note says "Domain name for the firewall." and "Examples: home.arpa, example.com".
- Primary DNS Server:** An empty text input field.
- Secondary DNS Server:** An empty text input field.
- Override DNS:** A checkbox that is checked. Below it, a note says "Allow DNS servers to be overridden by DHCP/PPP on WAN".

A "Next" button is highlighted with a red box at the bottom of the page.

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.

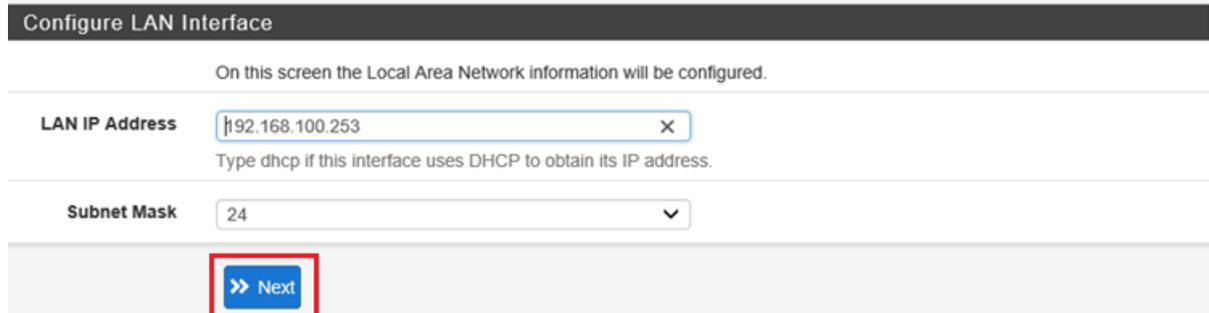
Time server hostname: 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone: Europe/Paris

Next

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

Next

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

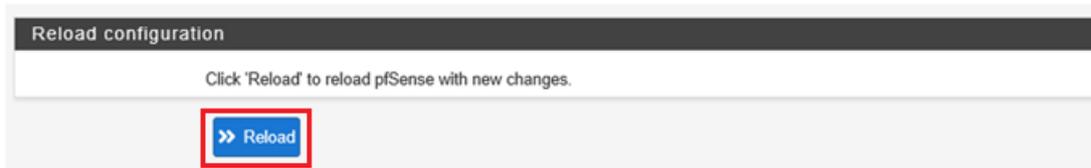
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password:

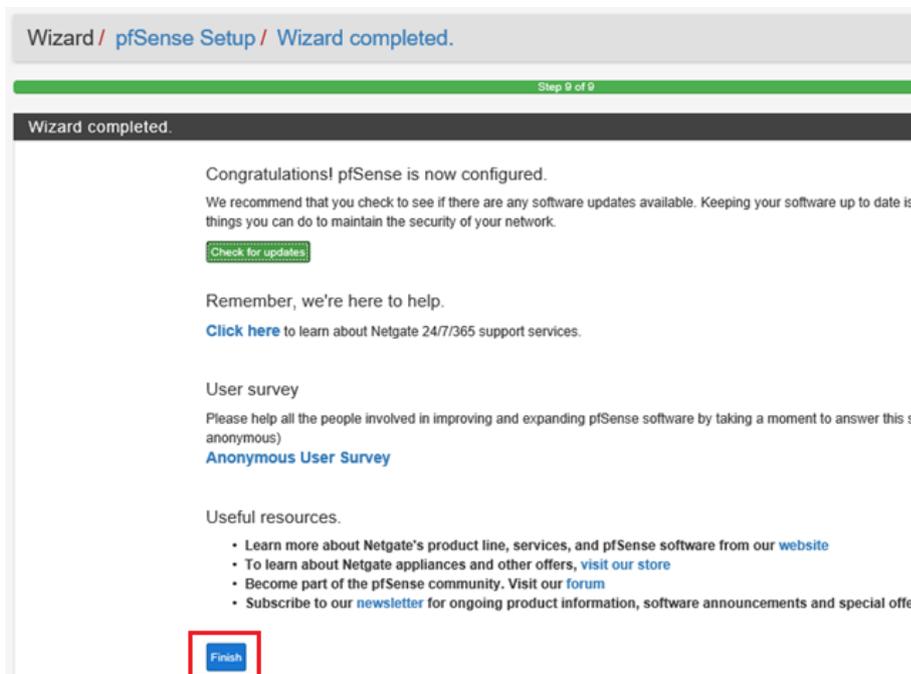
Admin Password AGAIN:

Next

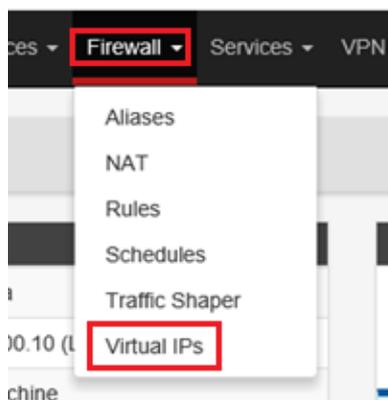
Cliquez sur **Reload** et patientez le temps que les configurations s'appliquent.



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



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



Virtual IP Address				
Virtual IP address	Interface	Type	Description	Actions
				+ Add

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 IP Alias **CARP** Proxy ARP 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. Confirm

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.

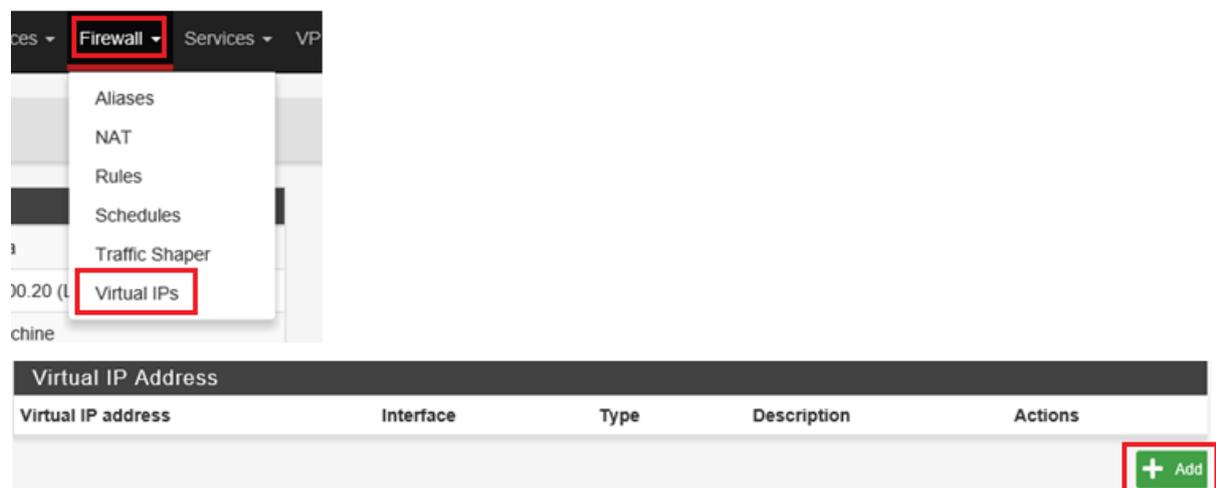
Description LAN CARP
A description may be entered here for administrative reference (not parsed).

[Save](#)

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**.



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

Edit Virtual IP

Type IP Alias **CARP** Proxy ARP 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. Confirm

VHID Group 1
Enter the VHID group that the machines will share.

Advertising frequency 1 (Base) 0 (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).

Virtual IP Address				
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)

i

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	⏸ BACKUP

State Synchronization Status

State Creator Host IDs:

- 64b2f289 (This node)

i

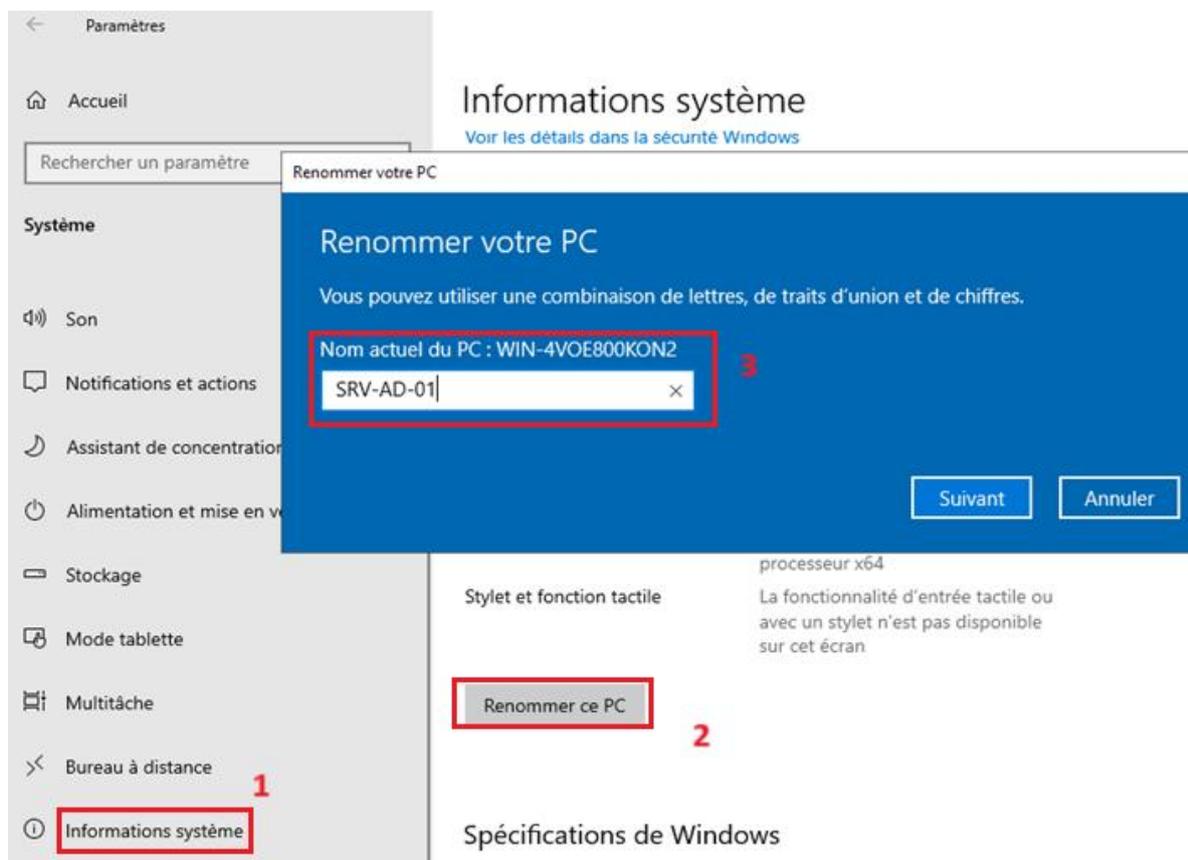
When state synchronization is enabled and functioning properly the list of state creator host IDs will be identical on each node participating in state synchronization.

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)

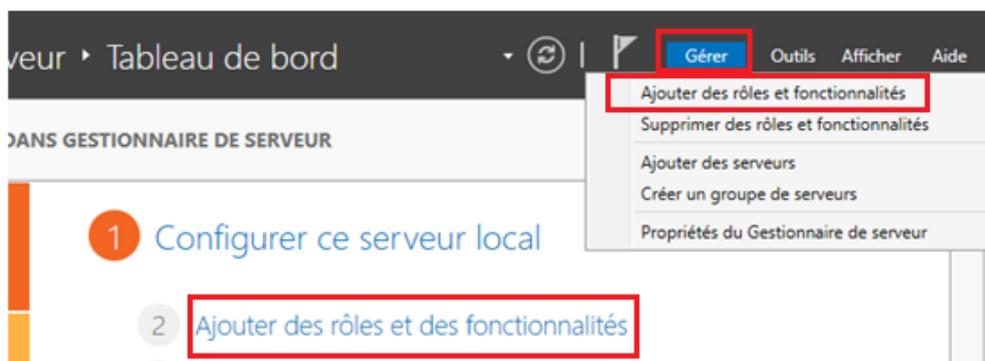
Tout d’abord, pensez à renommer votre machine avec le nom défini dans le plan, en accédant à **Paramètres > Système > Informations système**, puis en cliquant sur **Renommer ce PC**.



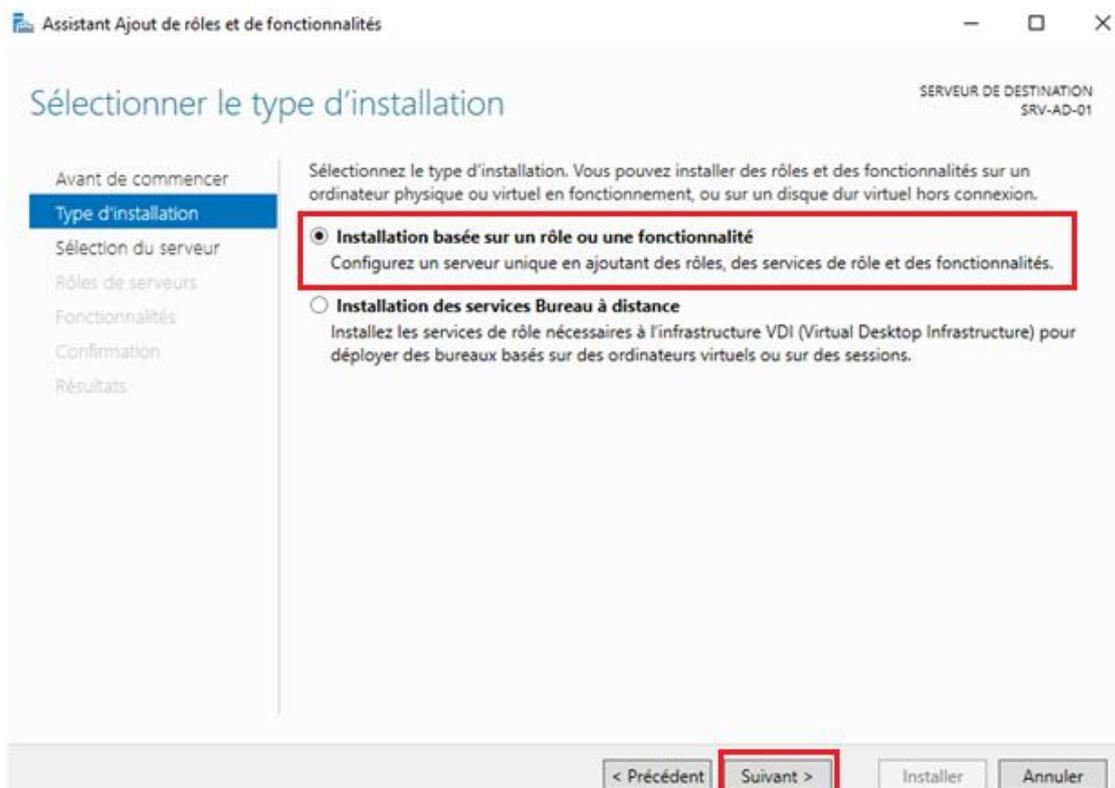
Une fois le nom modifié, redémarrez la machine pour que le changement soit pris en compte.

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

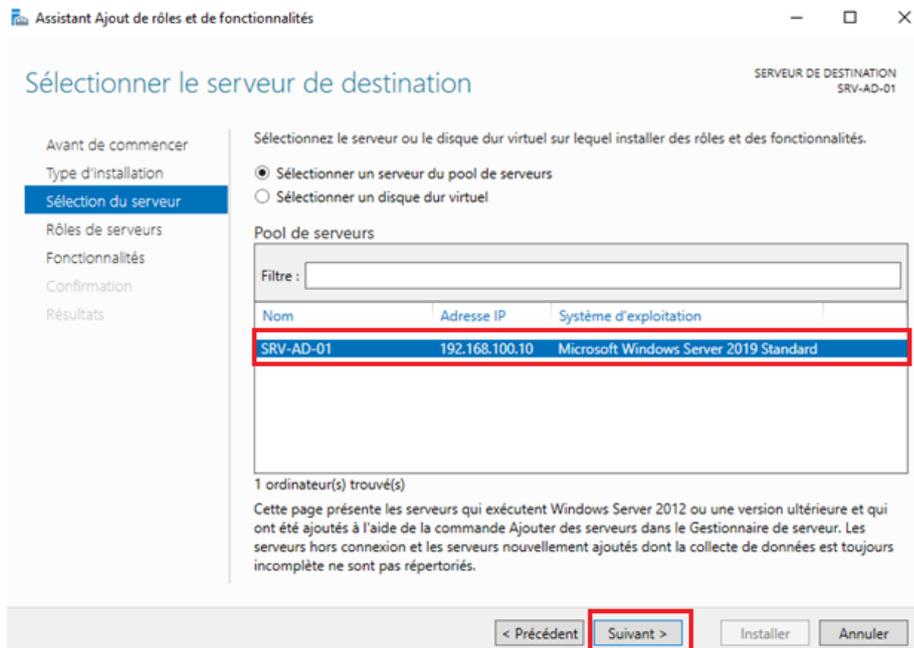
Accéder à **Gérer > Ajouter des rôles et fonctionnalités**, puis cliquer directement sur **Suivant** pour lancer l'installation.



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**.



Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER LE SERVEUR DE DESTINATION

SÉLECTIONNER LE SERVEUR DE DESTINATION SRV-AD-01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs

Sélectionner un disque dur virtuel

Pool de serveurs

Filter :

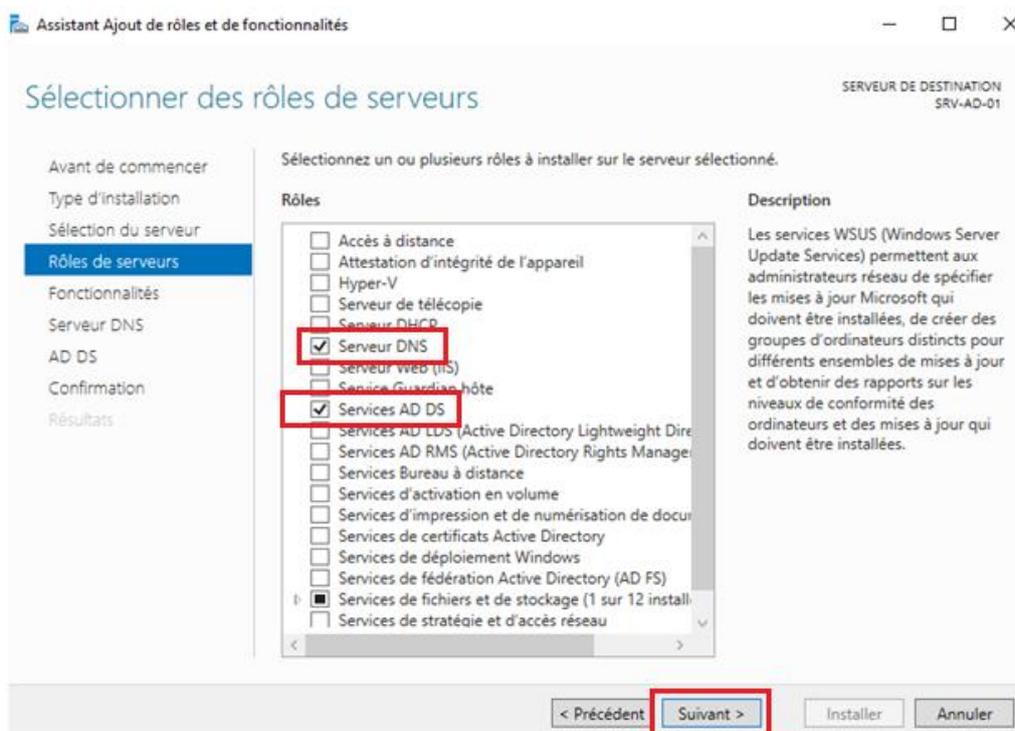
Nom	Adresse IP	Système d'exploitation
SRV-AD-01	192.168.100.10	Microsoft Windows Server 2019 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent **Suivant >** Installer Annuler

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



Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES RÔLES DE SERVEURS

SÉLECTIONNER DES RÔLES DE SERVEURS SRV-AD-01

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Serveur DNS

AD DS

Confirmation

Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

- Accès à distance
- Attestation d'intégrité de l'appareil
- Hyper-V
- Serveur de télécopie
- Serveur DHCP
- Serveur DNS**
- Serveur web (IIS)
- Service Guardian hôte
- Services AD DS**
- Services AD LDS (Active Directory Lightweight Directory Services)
- Services AD RMS (Active Directory Rights Management Services)
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de documents
- Services de certificats Active Directory
- Services de déploiement Windows
- Services de fédération Active Directory (AD FS)
- Services de fichiers et de stockage (1 sur 12 installés)
- Services de stratégie et d'accès réseau

Description

Les services WSUS (Windows Server Update Services) permettent aux administrateurs réseau de spécifier les mises à jour Microsoft qui doivent être installées, de créer des groupes d'ordinateurs distincts pour différents ensembles de mises à jour et d'obtenir des rapports sur les niveaux de conformité des ordinateurs et des mises à jour qui doivent être installées.

< Précédent **Suivant >** Installer Annuler

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

Assistant Ajout de rôles et de fonctionnalités

SÉLECTIONNER DES FONCTIONNALITÉS

SERVEUR DE DESTINATION
SRV-AD-01

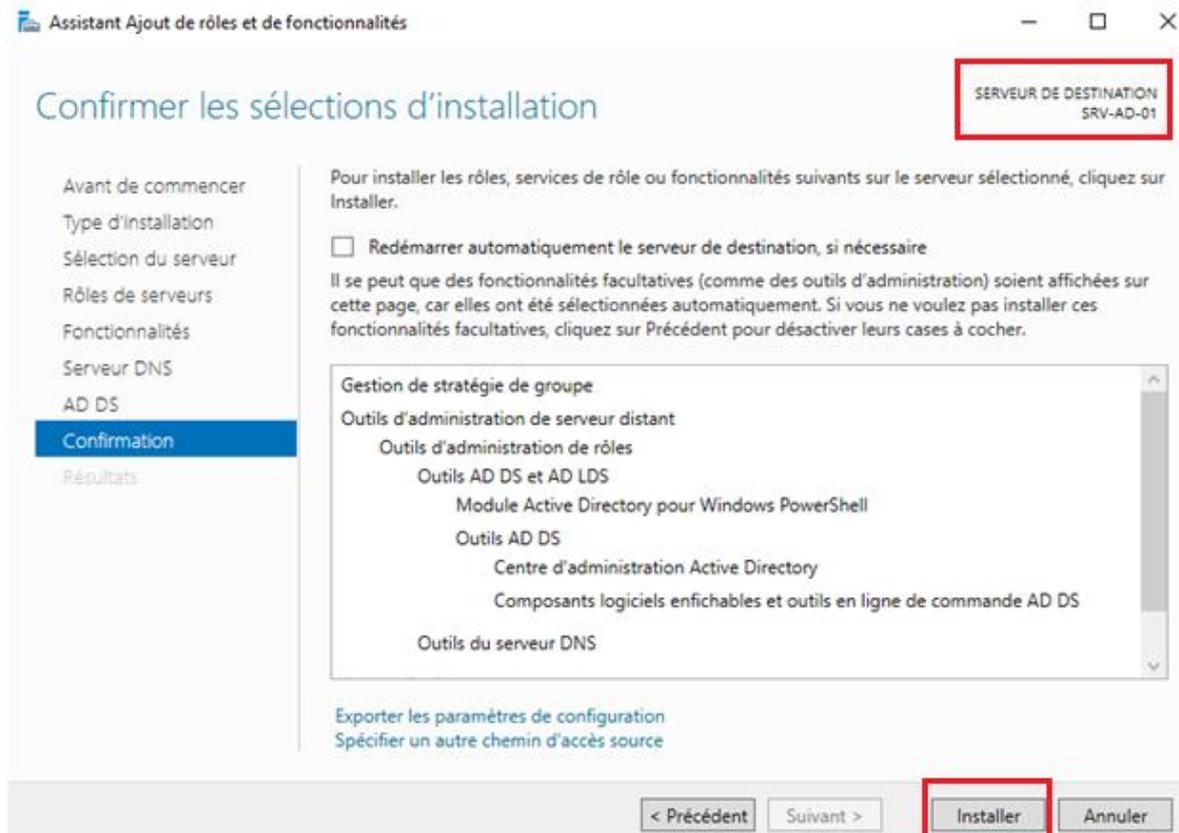
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DNS
AD DS
Confirmation
Résultats

Sélectionnez une ou plusieurs fonctionnalités à installer sur le serveur sélectionné.

Fonctionnalités	Description
<input type="checkbox"/> Assistance à distance	
<input type="checkbox"/> Base de données interne Windows	
<input type="checkbox"/> BranchCache	
<input type="checkbox"/> Chiffrement de lecteur BitLocker	
<input type="checkbox"/> Client d'impression Internet	
<input type="checkbox"/> Client pour NFS	
<input type="checkbox"/> Clustering de basculement	
<input type="checkbox"/> Collection des événements de configuration et de	
<input type="checkbox"/> Compression différentielle à distance	
<input type="checkbox"/> Containers	
<input type="checkbox"/> Data Center Bridging	
<input type="checkbox"/> Déverrouillage réseau BitLocker	
<input type="checkbox"/> Direct Play	
<input type="checkbox"/> Équilibrage de la charge réseau	
<input type="checkbox"/> Expérience audio-vidéo haute qualité Windows	
<input type="checkbox"/> Extension ISS Management OData	
<input type="checkbox"/> Extension WinRM IIS	
▸ <input type="checkbox"/> Fonctionnalités de .NET Framework 3.5	
▸ <input checked="" type="checkbox"/> Fonctionnalités de .NET Framework 4.7 (2 sur 7 ins	Permet la configuration de paramètres de qualité de service d'E/S tels que le nombre maximal d'E/S et les limites de bande passante sur les applications.

< Précédent **Suivant >** Installer Annuler

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



Assistant Ajout de rôles et de fonctionnalités

Confirmer les sélections d'installation

SERVER DE DESTINATION
SRV-AD-01

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DNS
AD DS
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

- Gestion de stratégie de groupe
- Outils d'administration de serveur distant
 - Outils d'administration de rôles
 - Outils AD DS et AD LDS
 - Module Active Directory pour Windows PowerShell
 - Outils AD DS
 - Centre d'administration Active Directory
 - Composants logiciels enfichables et outils en ligne de commande AD DS
 - Outils du serveur DNS

Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source

< Précédent Suivant > **Installer** Annuler

Afficher la progression de l'installation



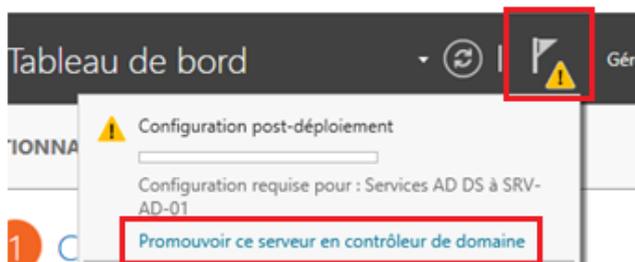
Installation de fonctionnalité



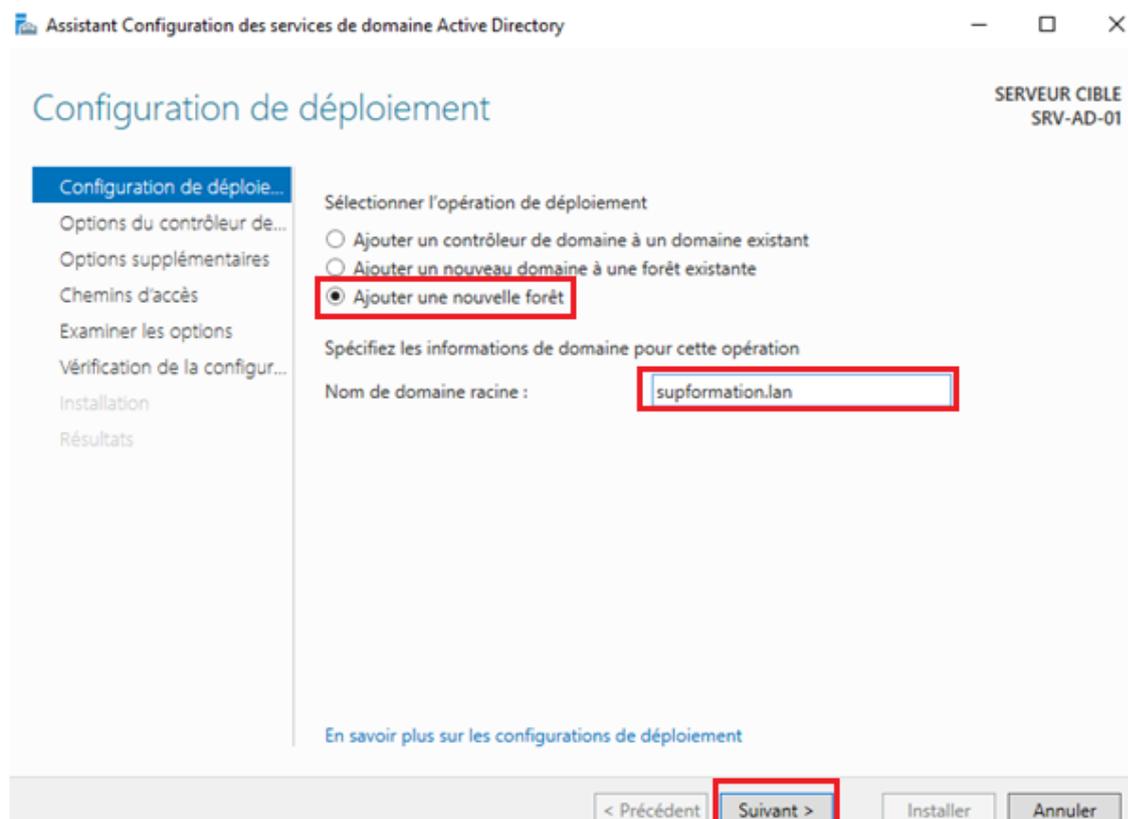
Configuration requise. Installation réussie sur SRV-AD-01.

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**.



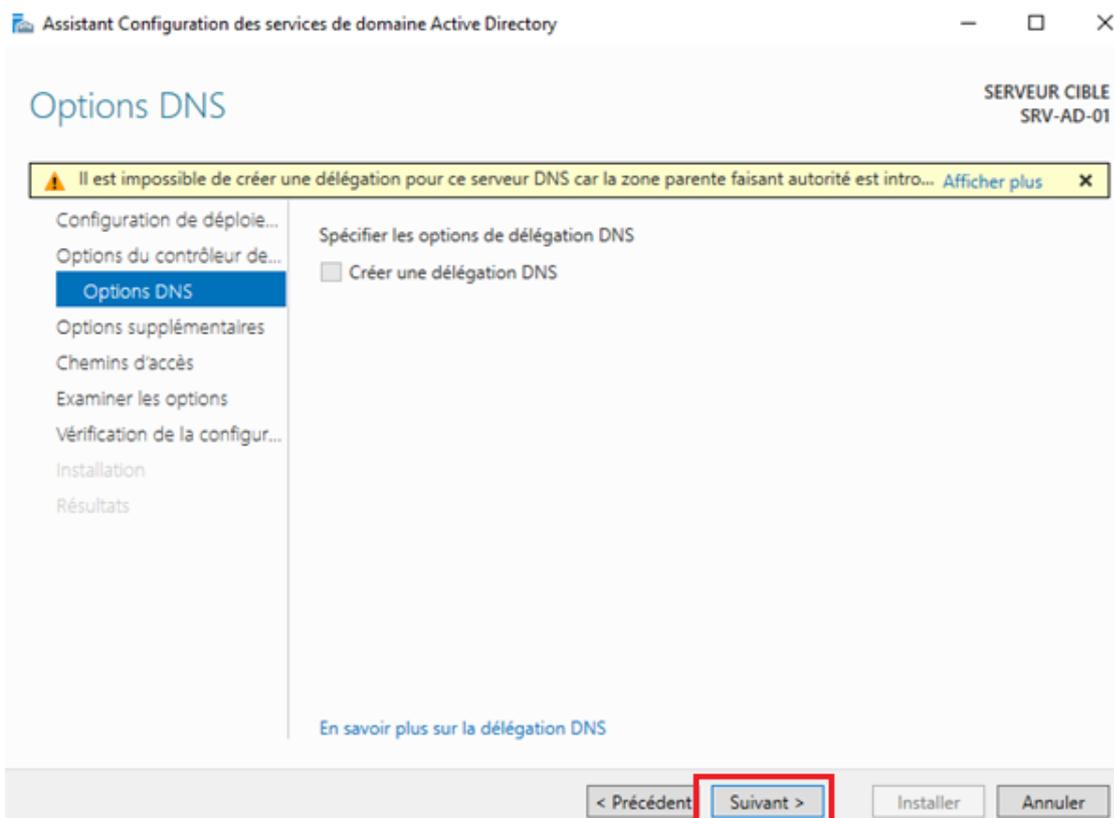
Définir et confirmer un mot de passe pour le mode de restauration DSRM, puis cliquer sur Suivant.

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

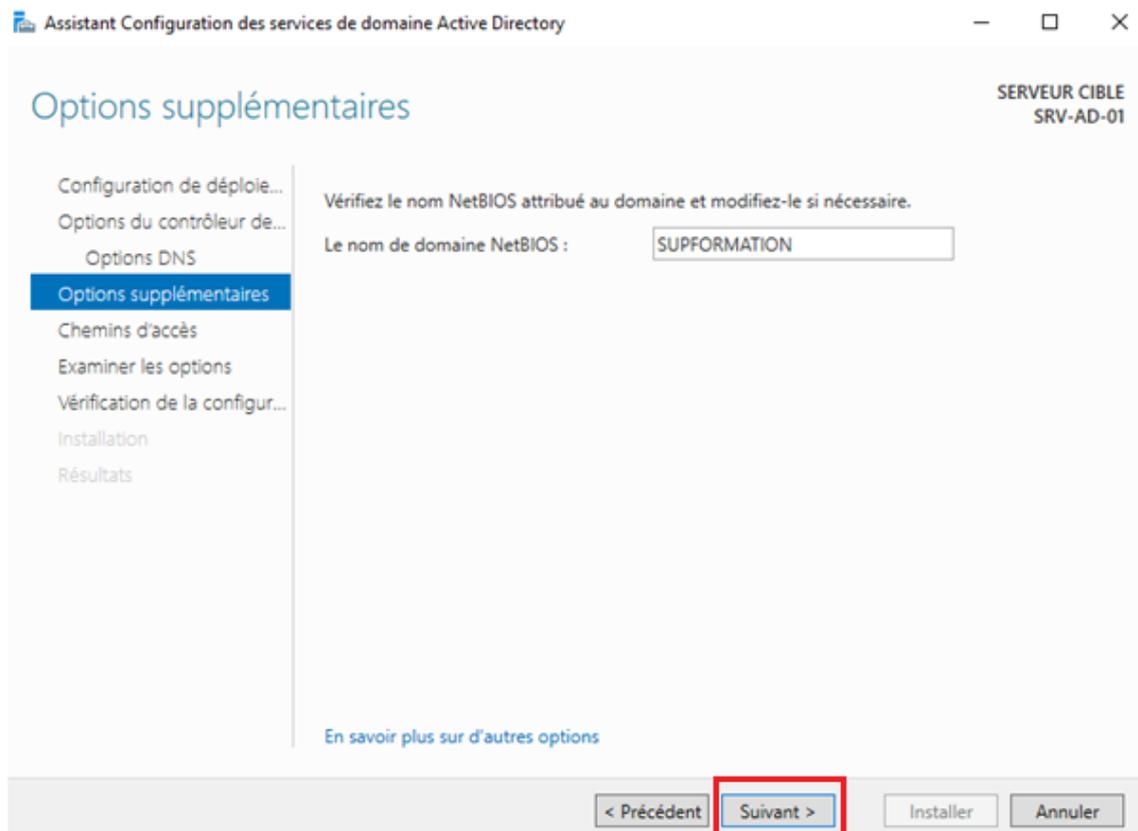
Mot de passe :

Confirmer le mot de passe :

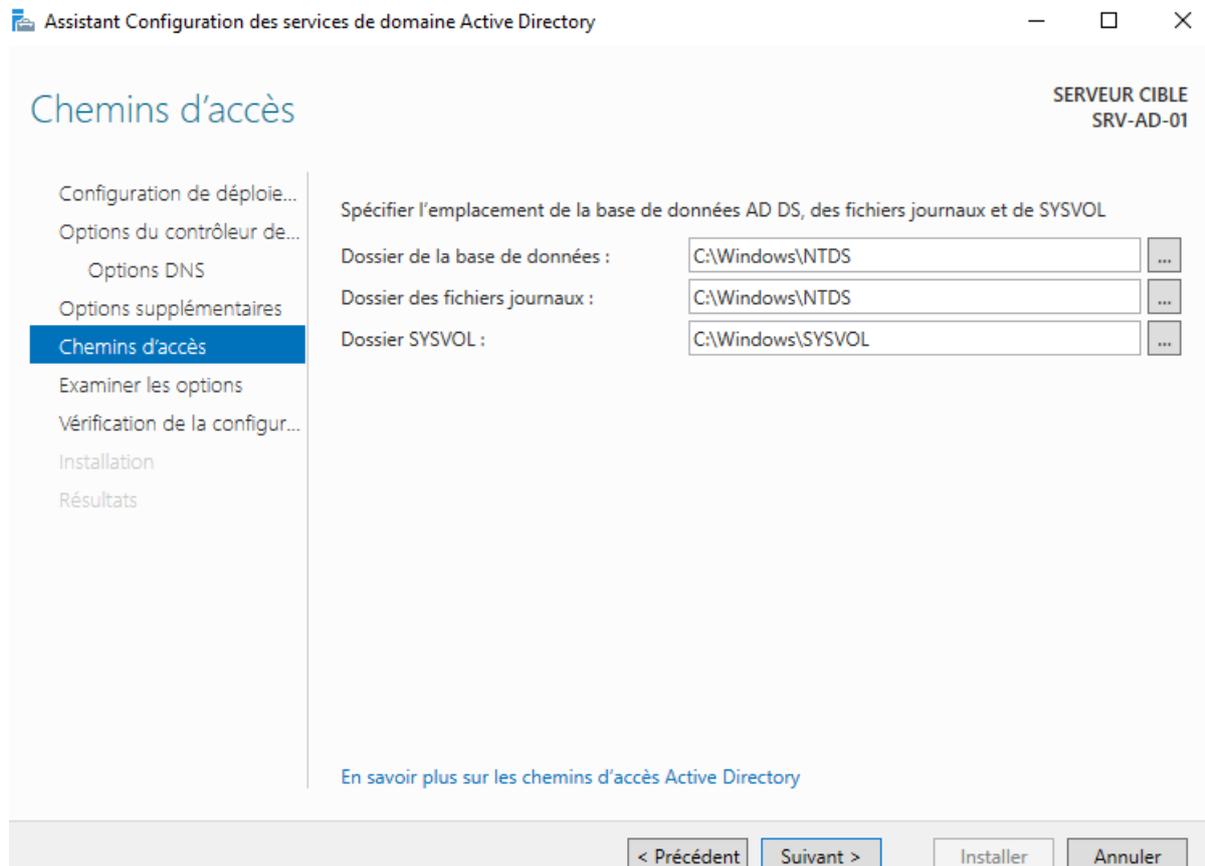
Aucune configuration pour les options DNS, cliquer sur **Suivant**.



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

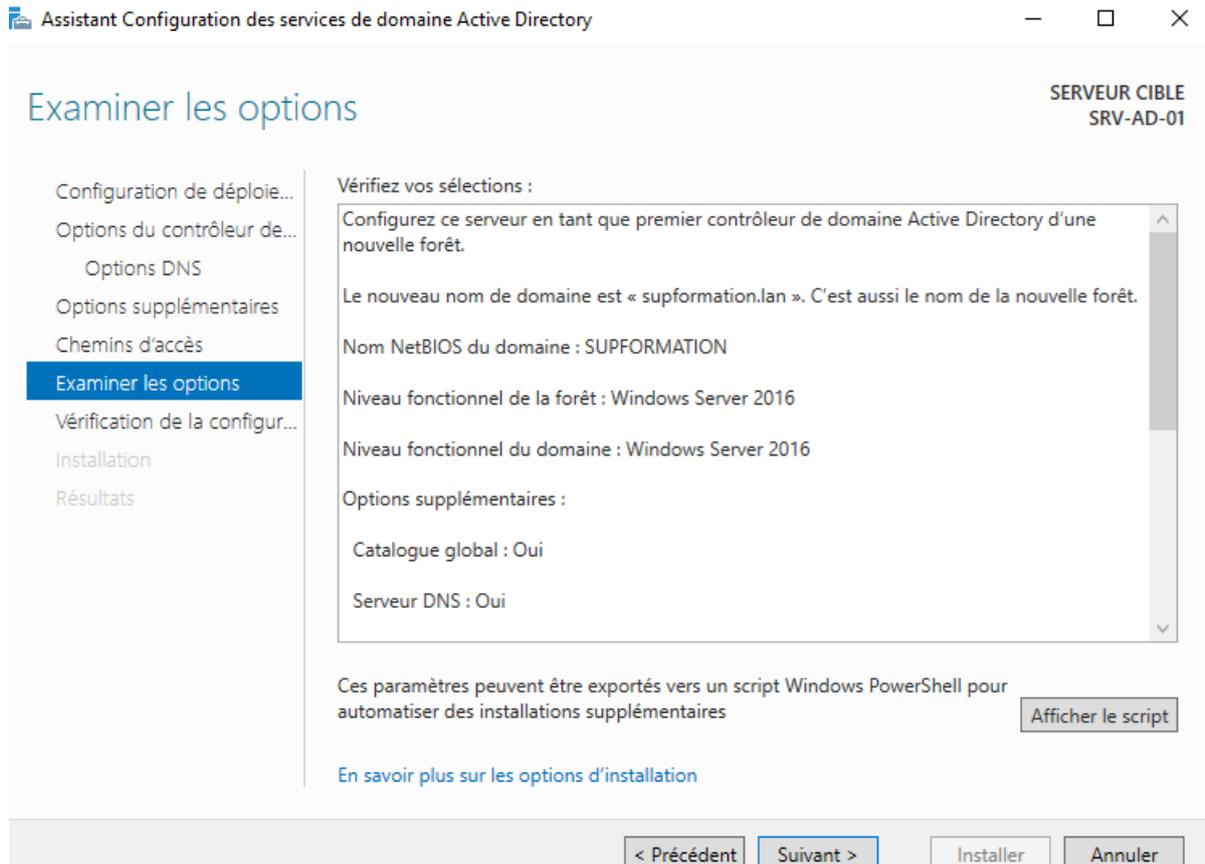


Laisser les chemins d'accès par défaut puis cliquer sur **Suivant**.



The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar includes window control buttons. The main window has a left sidebar with a menu: 'Configuration de déploie...', 'Options du contrôleur de...', 'Options DNS', 'Options supplémentaires', 'Chemins d'accès' (highlighted in blue), 'Examiner les options', 'Vérification de la configur...', 'Installation', and 'Résultats'. The main area is titled 'Chemins d'accès' and 'SERVEUR CIBLE SRV-AD-01'. It contains the instruction 'Spécifier l'emplacement de la base de données AD DS, des fichiers journaux et de SYSVOL'. Below this are three input fields: 'Dossier de la base de données : C:\Windows\NTDS', 'Dossier des fichiers journaux : C:\Windows\NTDS', and 'Dossier SYSVOL : C:\Windows\SYSVOL'. Each field has a browse button ('...'). At the bottom, there are four buttons: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

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



Assistant Configuration des services de domaine Active Directory

SERVER CIBLE
SRV-AD-01

Examiner les options

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

Vérifiez vos sélections :

Configurez ce serveur en tant que premier contrôleur de domaine Active Directory d'une nouvelle forêt.

Le nouveau nom de domaine est « supformation.lan ». C'est aussi le nom de la nouvelle forêt.

Nom NetBIOS du domaine : SUPFORMATION

Niveau fonctionnel de la forêt : Windows Server 2016

Niveau fonctionnel du domaine : Windows Server 2016

Options supplémentaires :

Catalogue global : Oui

Serveur DNS : Oui

Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires [Afficher le script](#)

[En savoir plus sur les options d'installation](#)

< Précédent **Suivant >** Installer Annuler

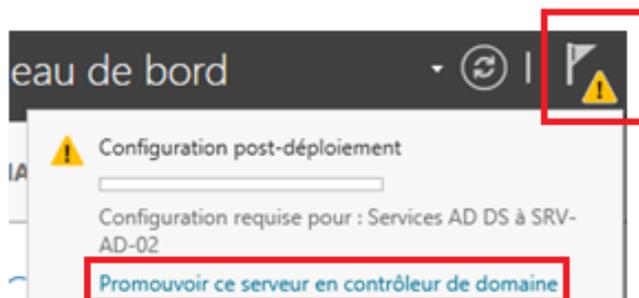
Installation de l'Active Directory sur le SRV-AD-02

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.

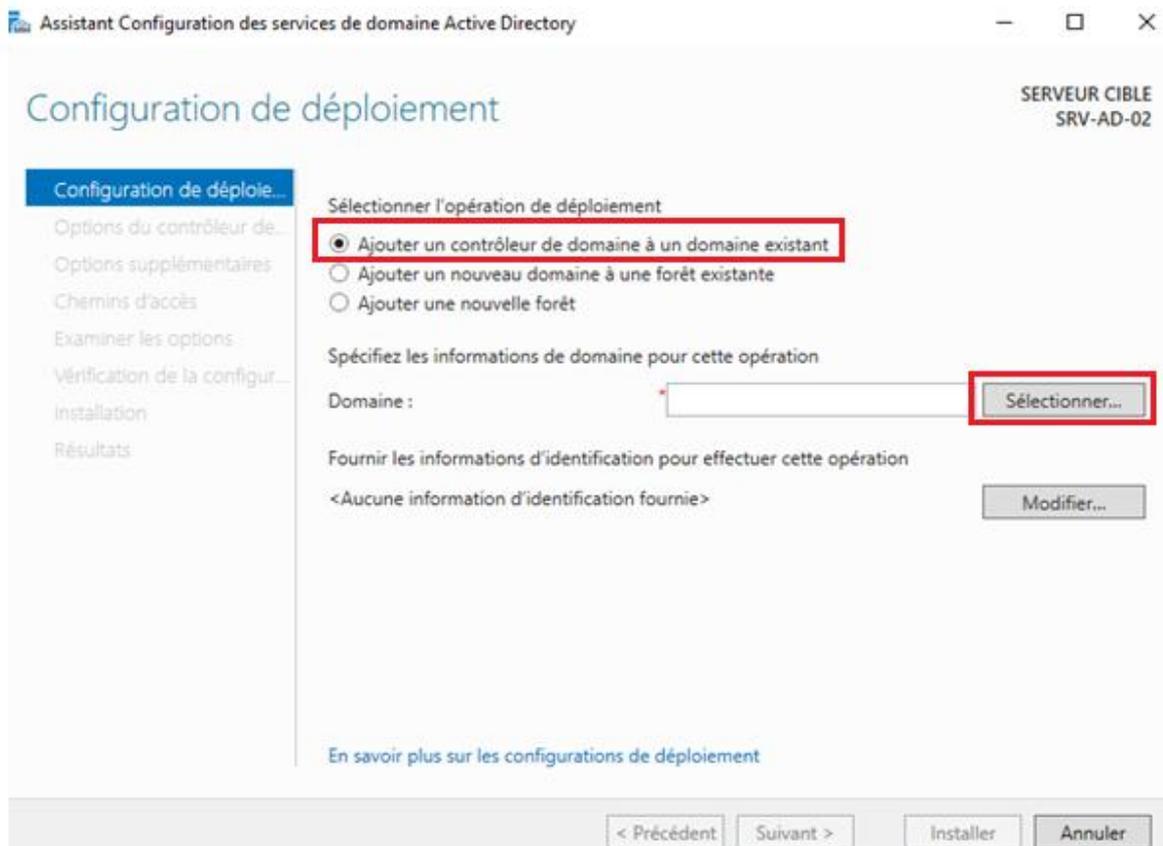


Configuration de l'Active Directory sur le SRV-AD-02

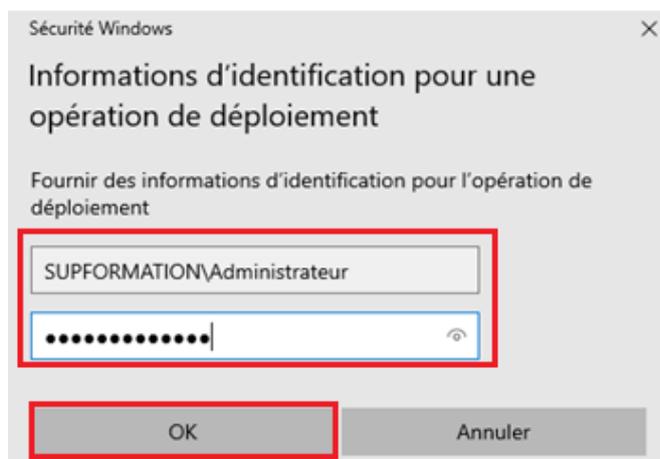
Clique sur l'icône d'avertissement, puis sélectionne « **Promouvoir ce serveur en contrôleur de domaine** » pour lancer l'assistant de configuration.



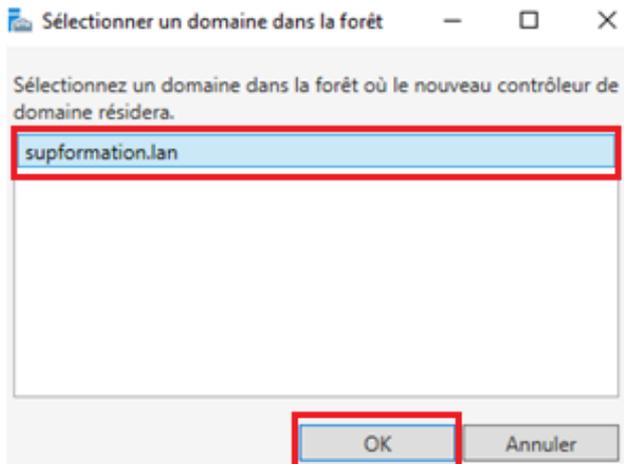
Coche « **Ajouter un contrôleur de domaine à un domaine existant** », clique sur « **Sélectionner...** ».



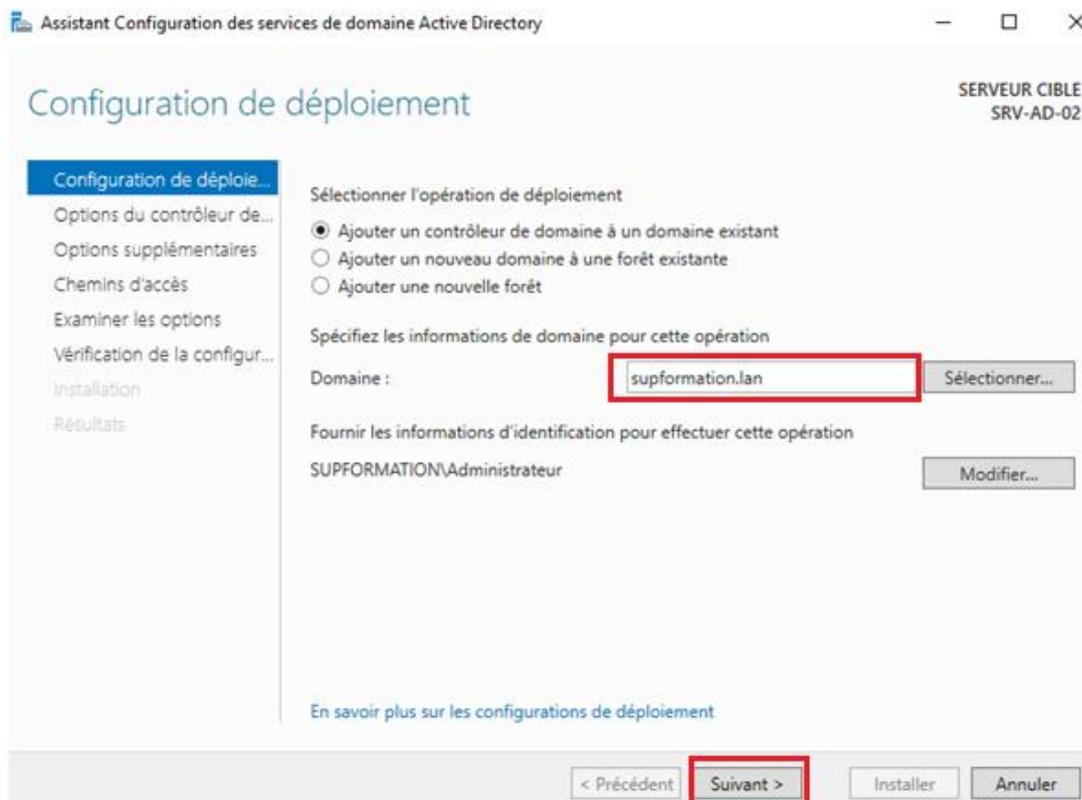
Renseigne **les identifiants de l'administrateur du domaine** puis clique sur **OK** pour valider.



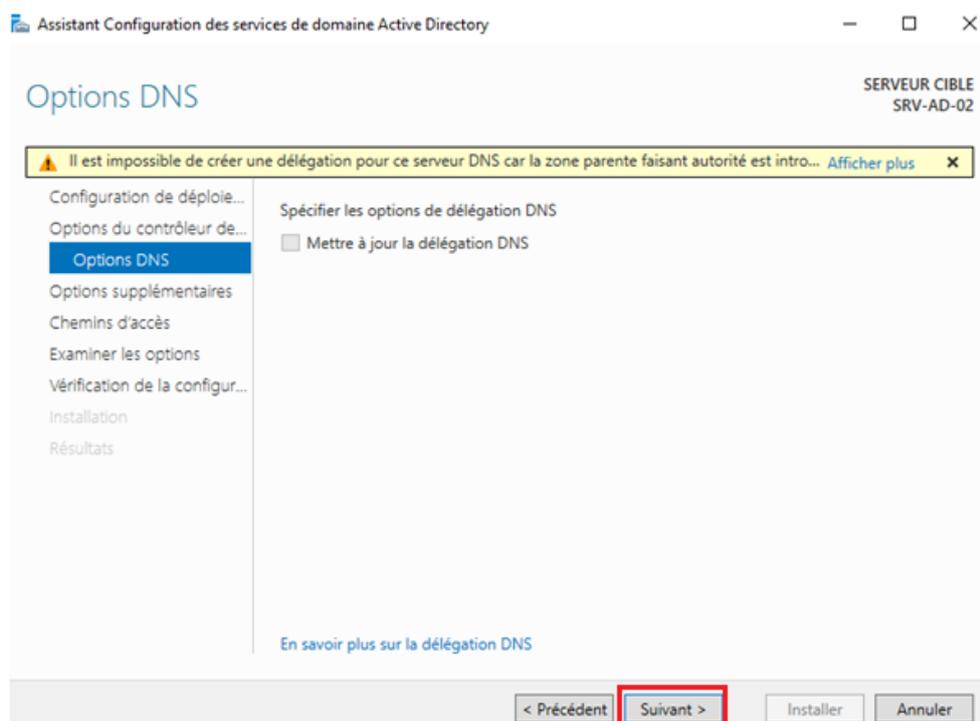
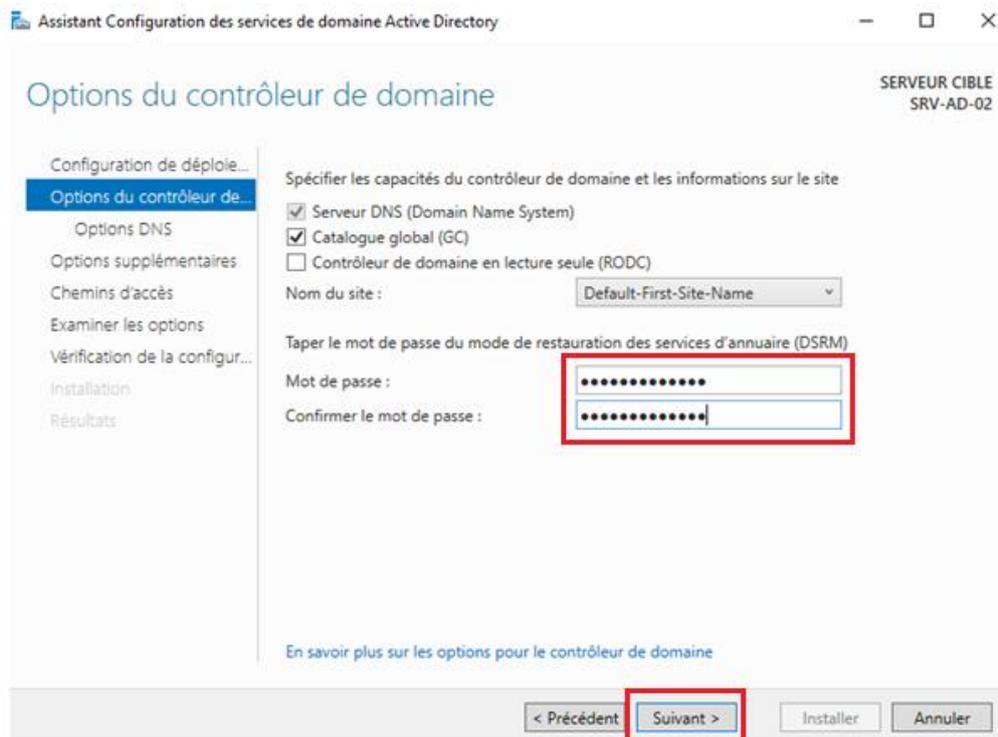
Sélectionne le domaine **supformation.lan**, puis clique sur **OK** pour continuer l'intégration du contrôleur secondaire.



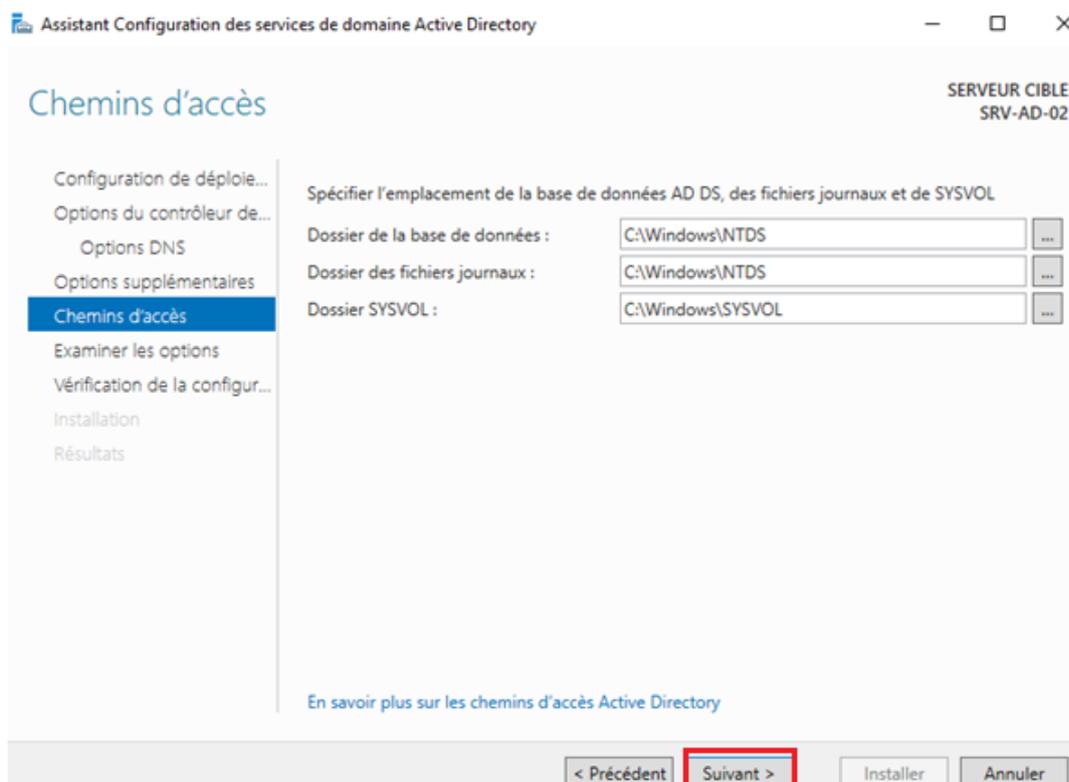
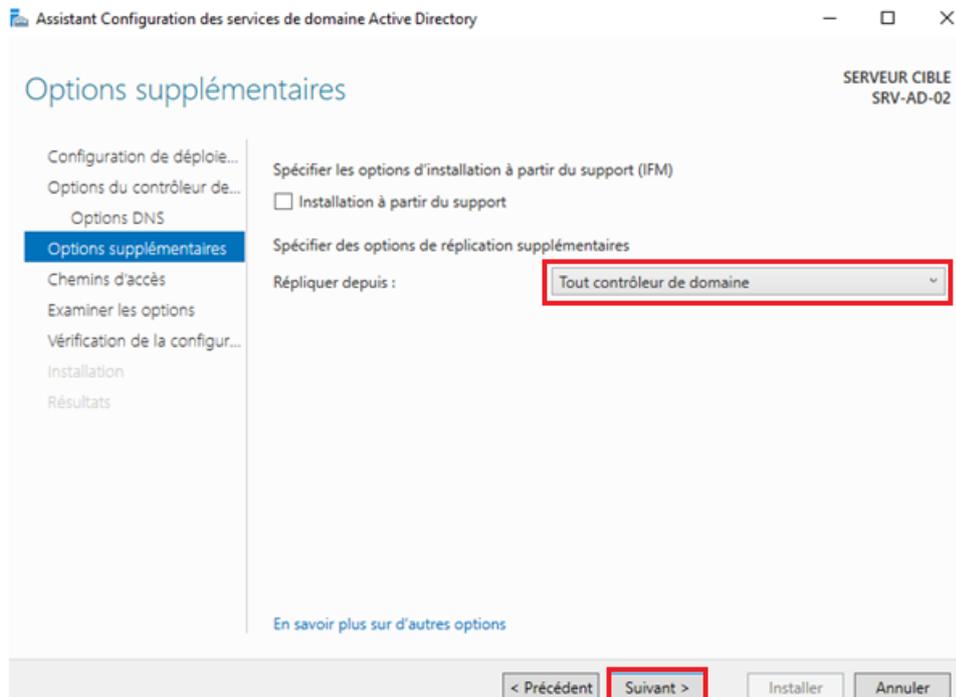
Une fois le domaine sélectionné, clique sur **Suivant** pour poursuivre la configuration.



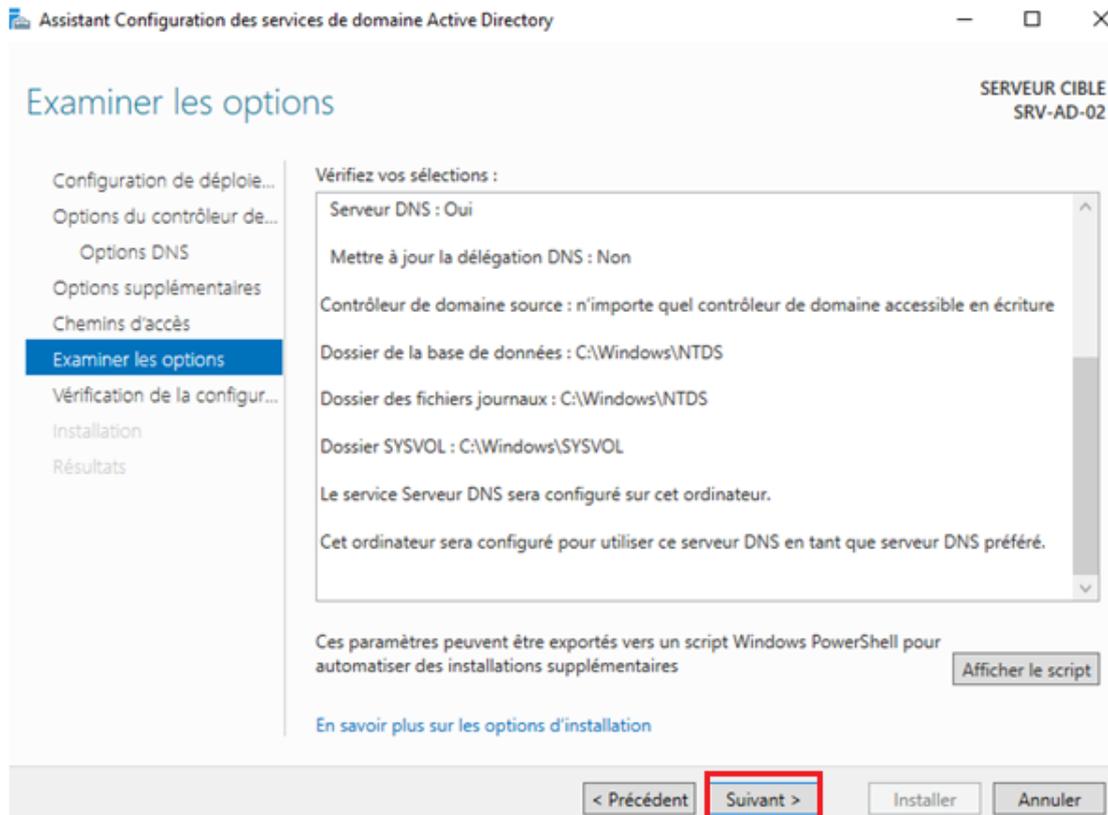
Saisi le mot de passe DSRM comme précédemment, puis clique sur **Suivant** pour continuer l'installation.



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

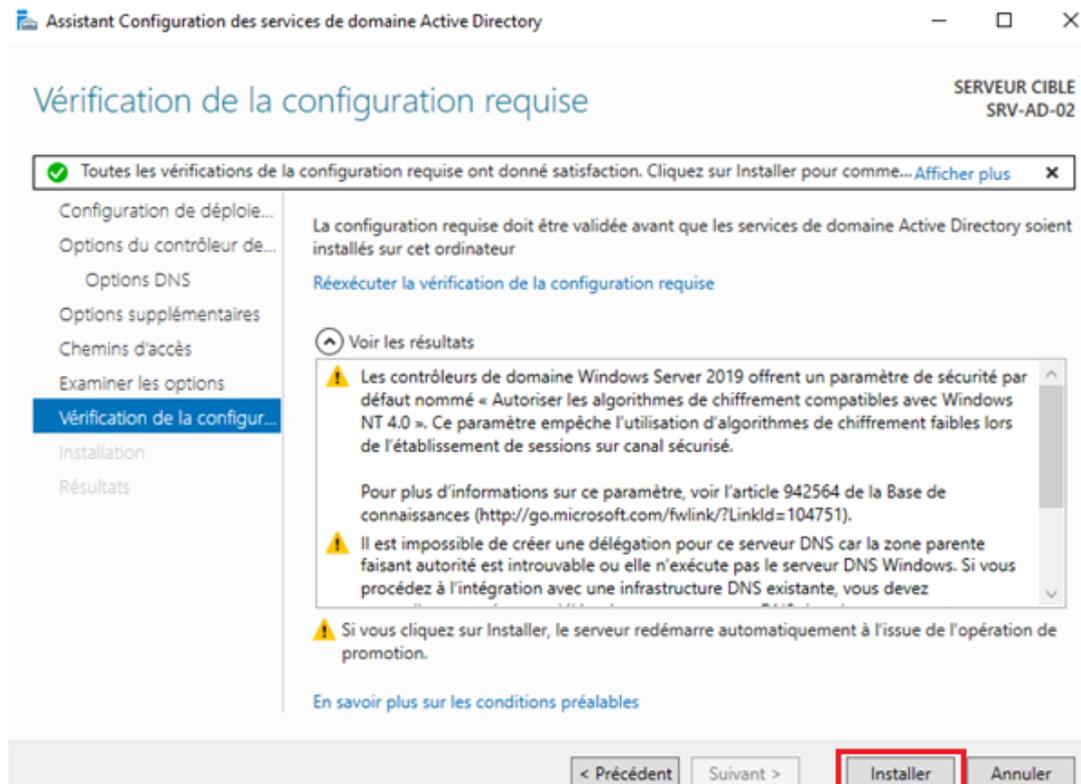


Ceci est un récapitulatif des paramètres choisis. Vérifie que tout est correct, puis clique sur **Suivant**.

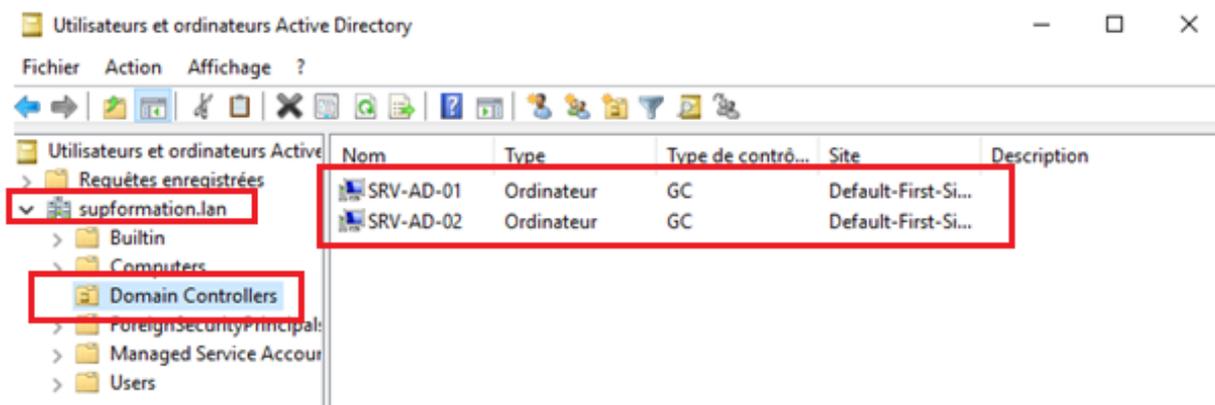
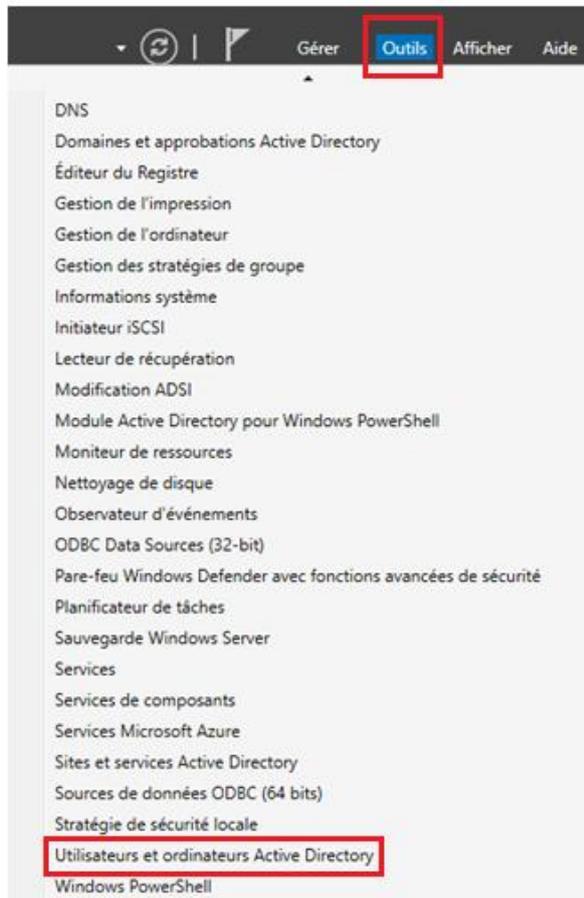


The screenshot shows the 'Assistant Configuration des services de domaine Active Directory' window. The title bar reads 'Assistant Configuration des services de domaine Active Directory'. The main window title is 'Examiner les options'. In the top right corner, it says 'SERVEUR CIBLE SRV-AD-02'. On the left, there is a navigation pane with the following items: 'Configuration de déploiement...', 'Options du contrôleur de domaine...', 'Options DNS', 'Options supplémentaires', 'Chemins d'accès', 'Examiner les options' (highlighted in blue), 'Vérification de la configuration...', 'Installation', and 'Résultats'. The main area is titled 'Vérifiez vos sélections :'. It contains a list of selected options: 'Serveur DNS : Oui', 'Mettre à jour la délégation DNS : Non', 'Contrôleur de domaine source : n'importe quel contrôleur de domaine accessible en écriture', 'Dossier de la base de données : C:\Windows\NTDS', 'Dossier des fichiers journaux : C:\Windows\NTDS', and 'Dossier SYSVOL : C:\Windows\SYSVOL'. Below this list, it states: 'Le service Serveur DNS sera configuré sur cet ordinateur.' and 'Cet ordinateur sera configuré pour utiliser ce serveur DNS en tant que serveur DNS préféré.'. At the bottom of the main area, there is a note: 'Ces paramètres peuvent être exportés vers un script Windows PowerShell pour automatiser des installations supplémentaires' and a button 'Afficher le script'. Below the main area, there is a link: 'En savoir plus sur les options d'installation'. At the bottom of the window, there are four buttons: '< Précédent', 'Suivant >' (highlighted with a red box), 'Installer', and 'Annuler'.

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**.



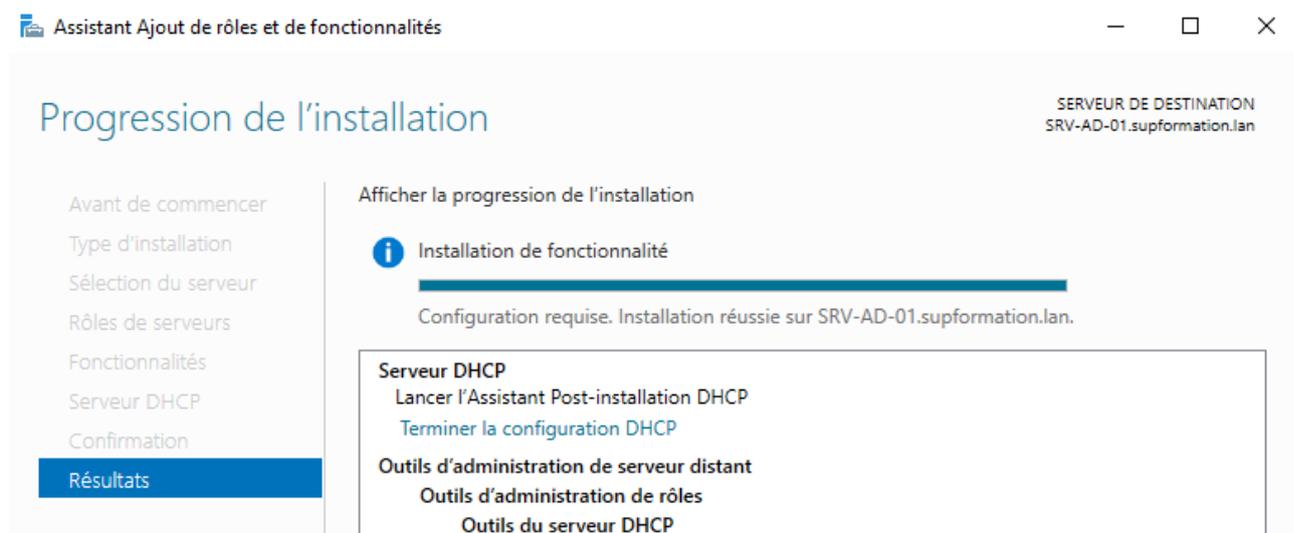
DHCP – Dynamic Host Configuration Protocol

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 :

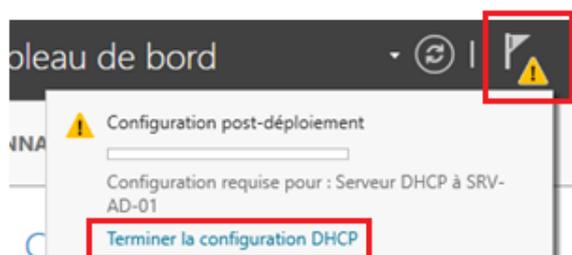
Accéder à **Ajouter des rôles et fonctionnalités**, puis cliquer successivement sur **Suivant** jusqu'à l'étape de sélection du serveur. Sélectionner le serveur concerné, cliquer sur **Suivant**, cocher **Serveur DHCP**, puis cliquer sur **Suivant**.

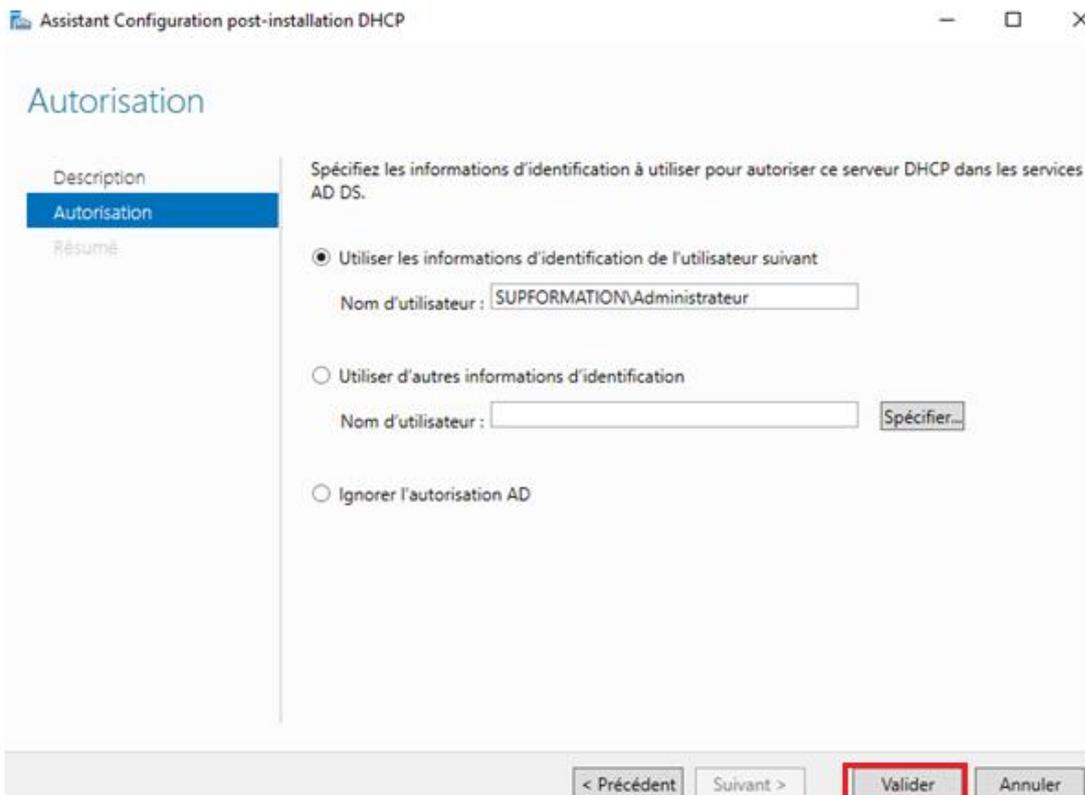
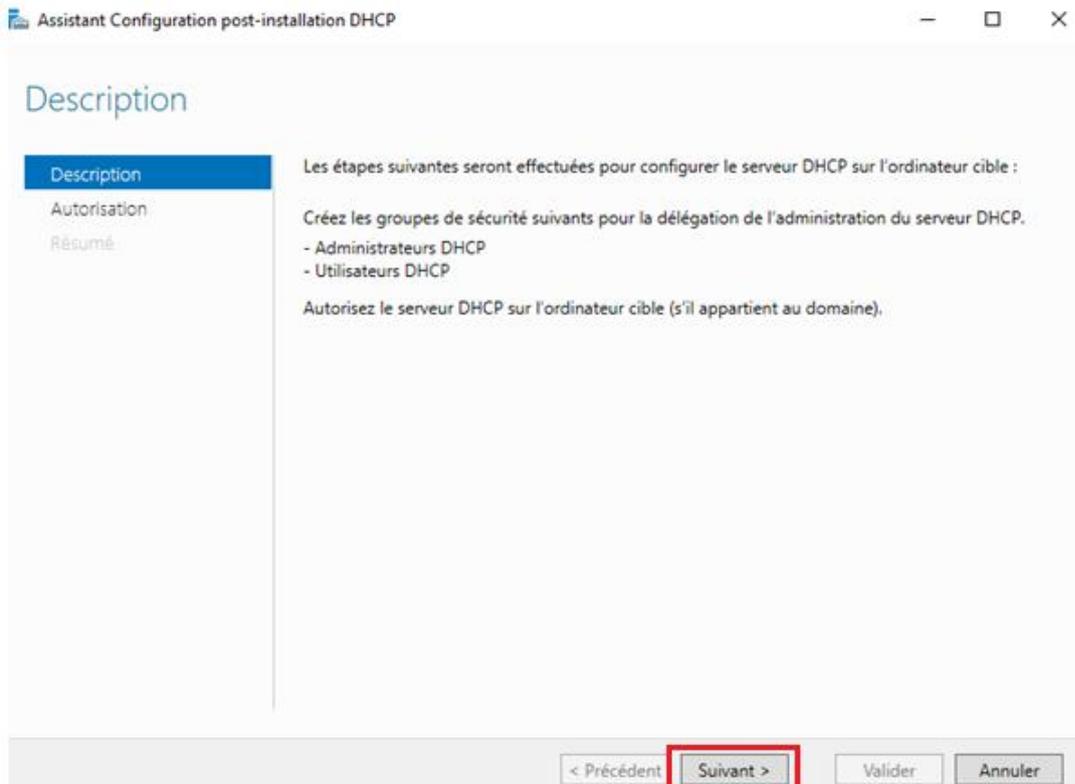
Continuer avec **Suivant** jusqu'à l'étape **Installer**. Lancer l'installation et cliquer sur **Fermer** une fois celle-ci terminée.



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

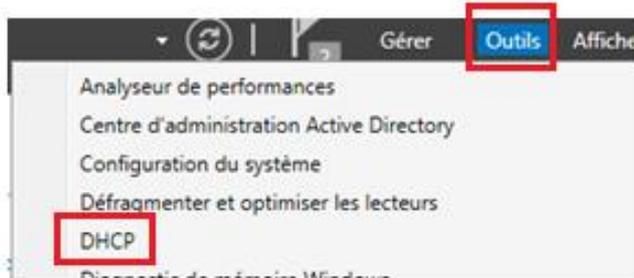
Cliquez sur **Terminer la configuration DHCP** pour finaliser l'installation via l'assistant prévu à cet effet.



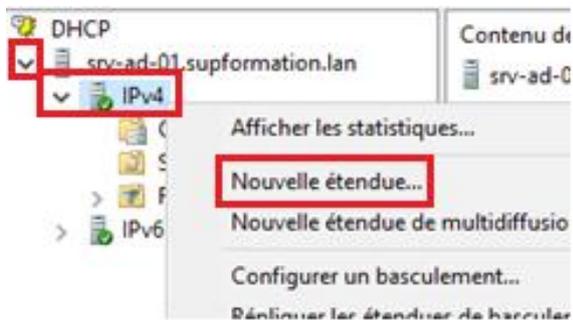


Configuration du protocole DHCP sur le serveur SRV-AD-01

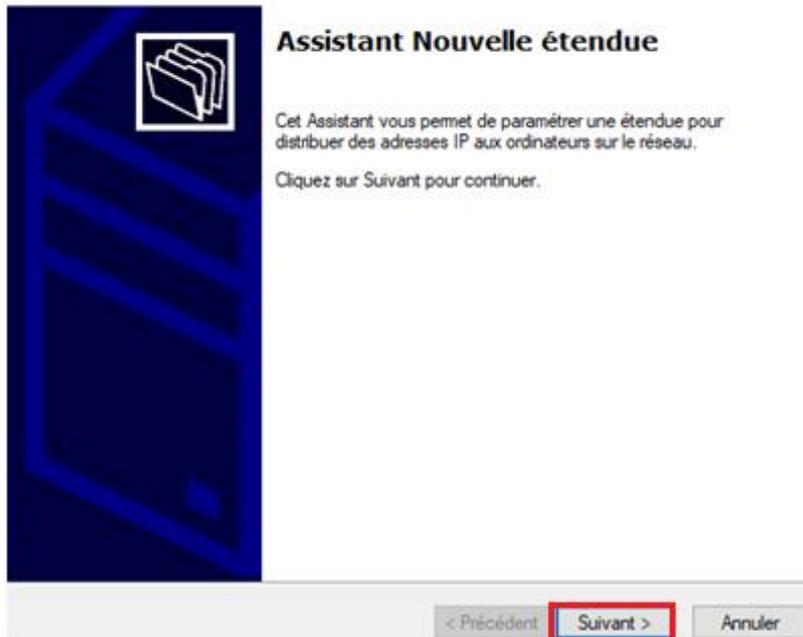
Se rendre dans la console **DHCP** depuis le **Gestionnaire de serveurs** afin de débiter la configuration du service.



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

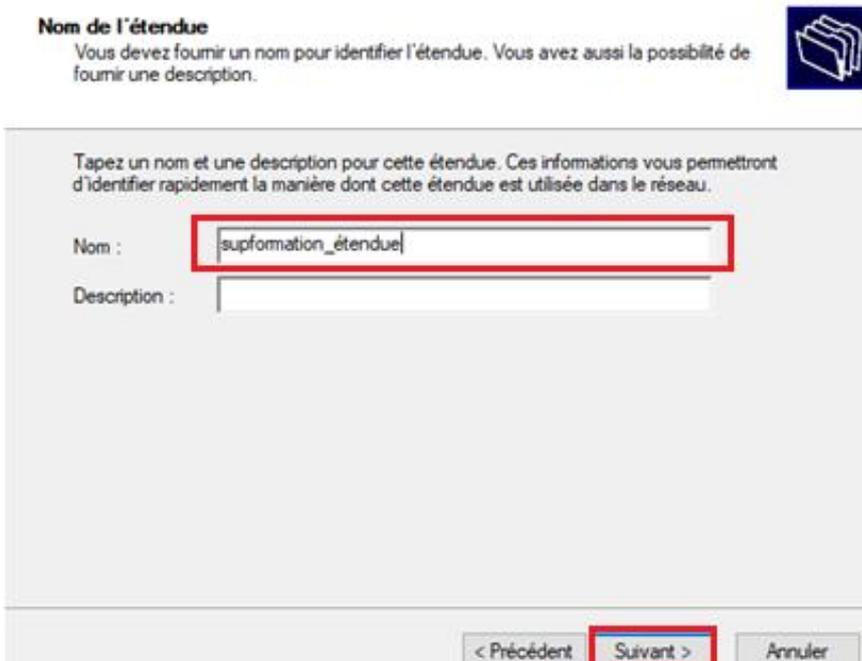


Assistant Nouvelle étendue



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



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 :

Adresse IP de fin :

Paramètres de configuration qui se propagent au client DHCP.

Longueur :

Masque de sous-réseau :

< 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 DHCP OFFER.



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 :

Plage d'adresses exclue :

Retard du sous-réseau en millisecondes :

< 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 :

8	0	0
---	---	---

< Précédent

Suivant >

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 configurerai 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 :

<input type="text" value="."/> <input type="text" value="."/> <input type="text" value="."/> <input type="text" value="192.168.100.254"/>	<input type="button" value="Ajouter"/> <input type="button" value="Supprimer"/> <input type="button" value="Monter"/> <input type="button" value="Descendre"/>
--	---

< Précédent **Suivant >** 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 :

Adresse IP :

Ajouter

Résoudre

192.168.100.10
192.168.100.10

Supprimer

Monter

Descendre

< Précédent

Suivant >

Annuler

Aucun serveur WINS n'étant utilisé, laissez vide et cliquez 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 : Adresse IP :

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

Cochez « **Oui, je veux activer cette étendue maintenant** », puis cliquez sur **Suivant**.

Assistant Nouvelle étendue

Activer l'étendue

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



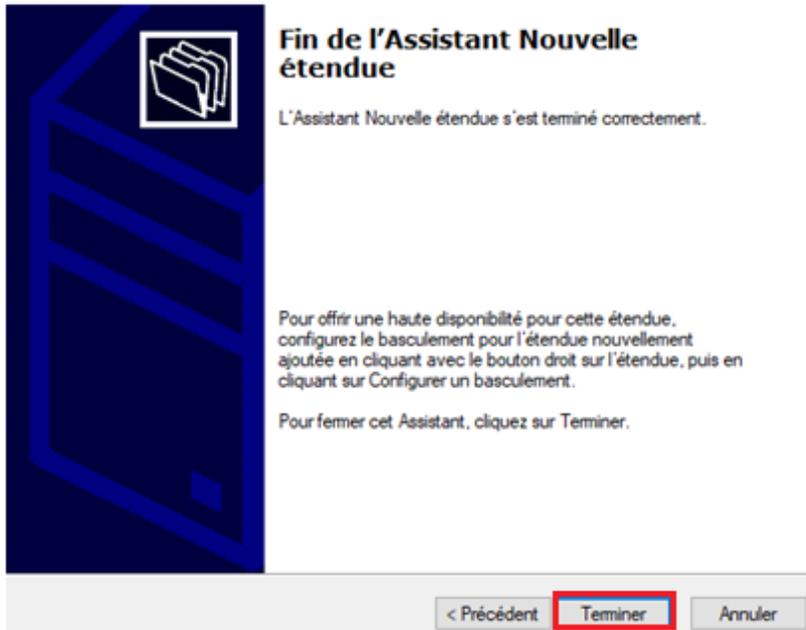
Voulez-vous activer cette étendue maintenant ?

Oui, je veux activer cette étendue maintenant

Non, j'activerai cette étendue ultérieurement

< Précédent **Suivant >** Annuler

Assistant Nouvelle étendue



Fin de l'Assistant Nouvelle étendue

L'Assistant Nouvelle étendue s'est terminé correctement.

Pour offrir une haute disponibilité pour cette étendue, configurez le basculement pour l'étendue nouvellement ajoutée en cliquant avec le bouton droit sur l'étendue, puis en cliquant sur Configurer un basculement.

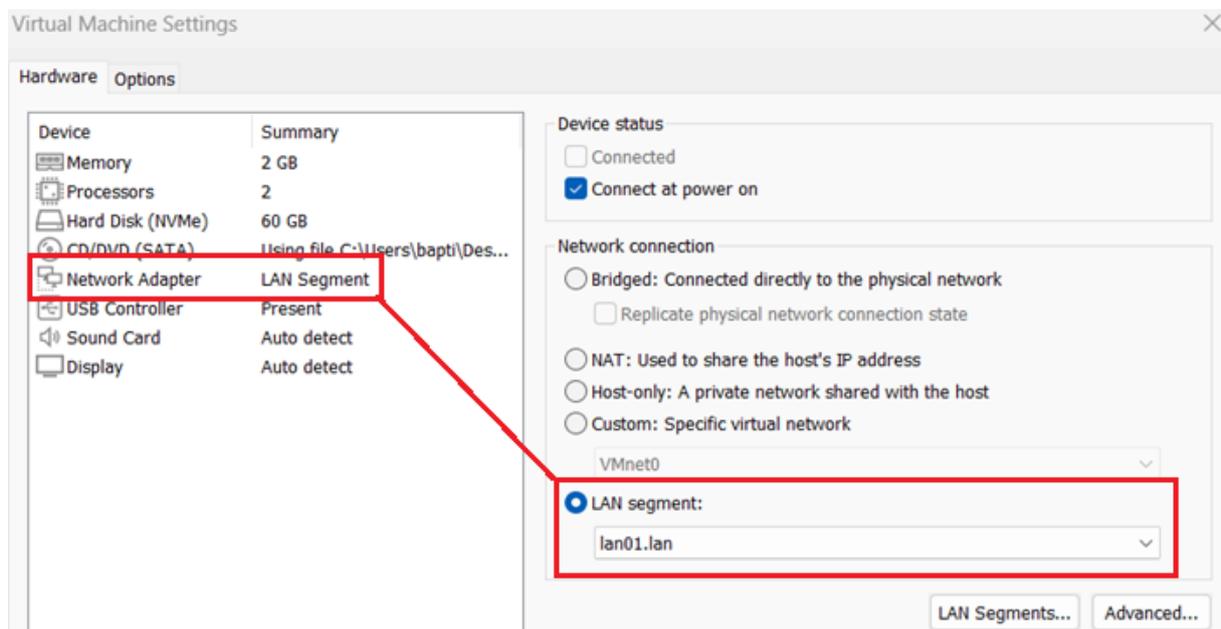
Pour fermer cet Assistant, cliquez sur Terminer.

< Précédent **Terminer** Annuler

Contenu du serveur DHCP		État
<ul style="list-style-type: none"> DHCP <ul style="list-style-type: none"> srv-ad-01.supformation.lan <ul style="list-style-type: none"> IPv4 <ul style="list-style-type: none"> Options de serveur <ul style="list-style-type: none"> Étendue [192.168.100.0] supformation_étendue <ul style="list-style-type: none"> Pool d'adresses Baux d'adresses Réservations Options d'étendue Stratégies Stratégies Filtres IPv6 	<ul style="list-style-type: none"> Options de serveur Étendue [192.168.100.0] supformation_ét... ** Actif ** Stratégies Filtres 	

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 :

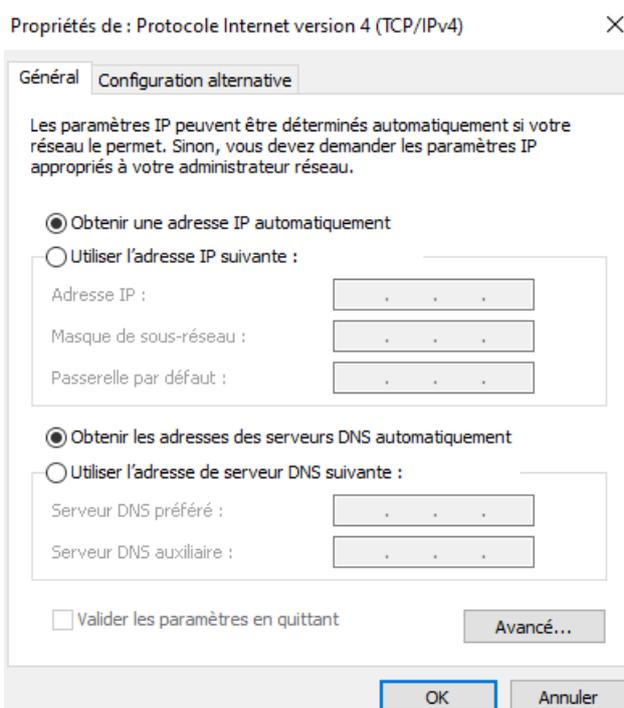
```
C:\Users\Administrateur>ipconfig /all

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 :

Suffixe DNS propre à la connexion. . . : supformation.lan
Description. . . . . : Intel(R) 82574L Gigabit Network Connection
Adresse physique . . . . . : 00-0C-29-EA-68-47
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::f9f4:6a82:f023:c488%10(préféré)
Adresse IPv4. . . . . : 192.168.100.100(préféré)
Masque de sous-réseau. . . . . : 255.255.255.0
Bail obtenu. . . . . : vendredi 2 mai 2025 19:55:06
Bail expirant. . . . . : samedi 10 mai 2025 19:55:05
Passerelle par défaut. . . . . : 192.168.100.254
Serveur DHCP . . . . . : 192.168.100.20
IAID DHCPv6 . . . . . : 100666409
DUID de client DHCPv6. . . . . : 00-01-00-01-2F-A6-BE-32-00-0C-29-EA-68-47
Serveurs DNS. . . . . : 192.168.100.10
                                192.168.100.20
NetBIOS sur Tcpip. . . . . : Activé
```



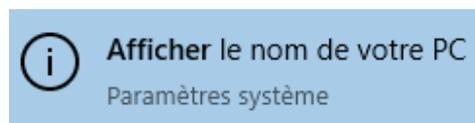
Depuis les baux d'adresses de **SRV-AD-01** du DHCP :

	Adresse IP du client	Nom	Expiration du bail	Type	ID unique	Actions
<ul style="list-style-type: none"> ▼ DHCP ▼ srv-ad-01.supformation.lan <ul style="list-style-type: none"> ▼ IPv4 <ul style="list-style-type: none"> Options de serveur ▼ Étendue [192.168.100.0] supfoi <ul style="list-style-type: none"> Pool d'adresses Baux d'adresses > Réservations Options d'étendue Stratégies Stratégies > Filtres ▼ IPv6 <ul style="list-style-type: none"> Options de serveur 	192.168.100.100	PC01.supformation...	10/05/2025 19:28:17	DHCP	000c29ea6	<ul style="list-style-type: none"> Baux d'adresses ▲ Autres actions ▶

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

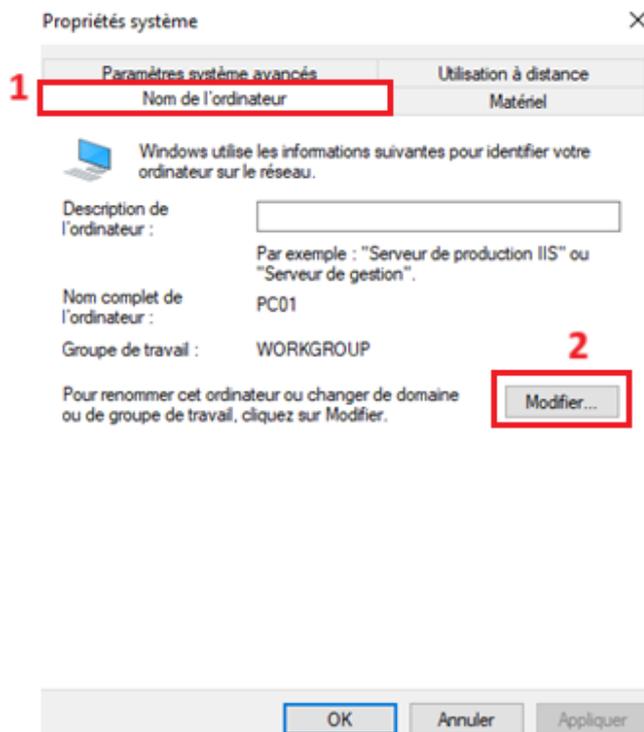
Protection du système

Paramètres avancés du système

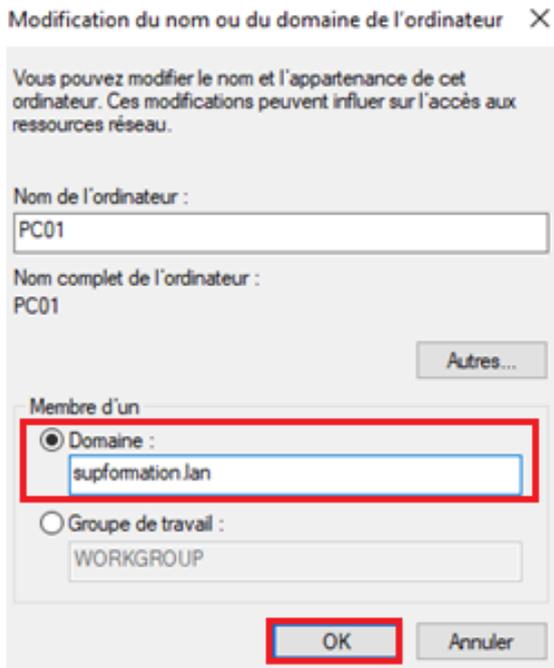
Renommer ce PC (avancé)

Paramètres graphiques

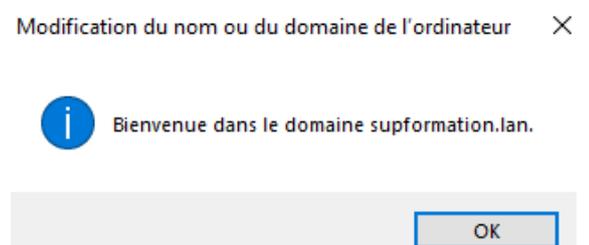
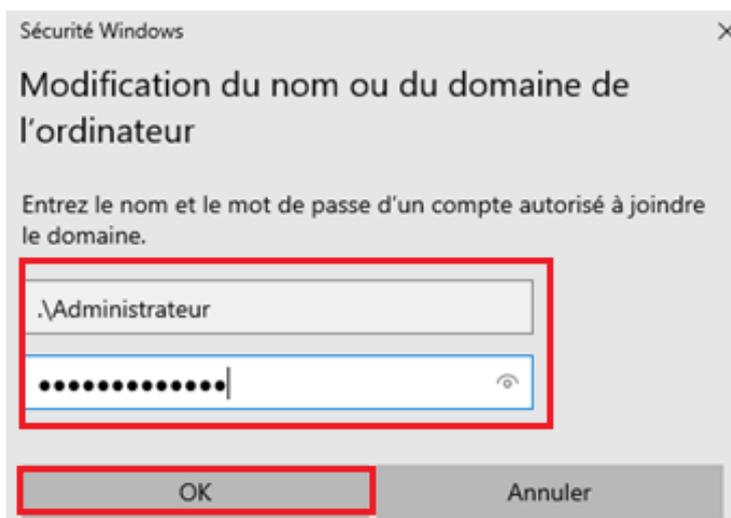
Dans l'onglet **Nom de l'ordinateur**, cliquez sur **Modifier** pour l'ajouter au domaine.



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



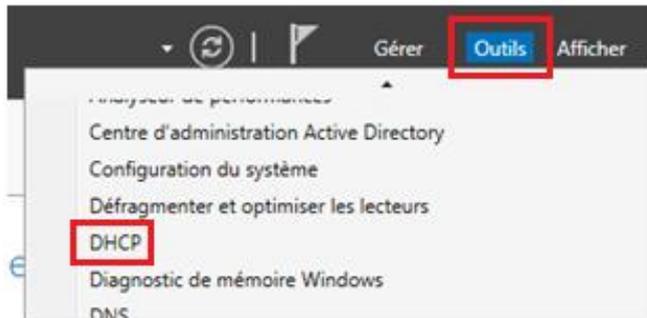
Indiquez un compte autorisé pour joindre le domaine, comme Administrateur du domaine, puis cliquez sur **OK**.



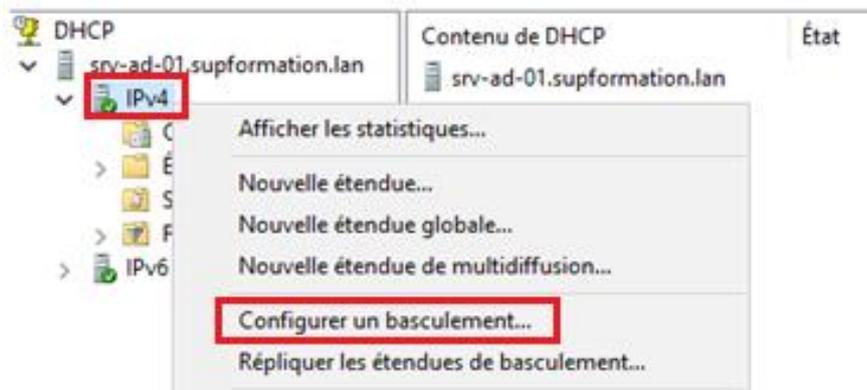
Le message confirme que l'ordinateur a bien rejoint le domaine supformation.lan. Vous pouvez maintenant redémarrer le poste pour finaliser l'intégration.

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

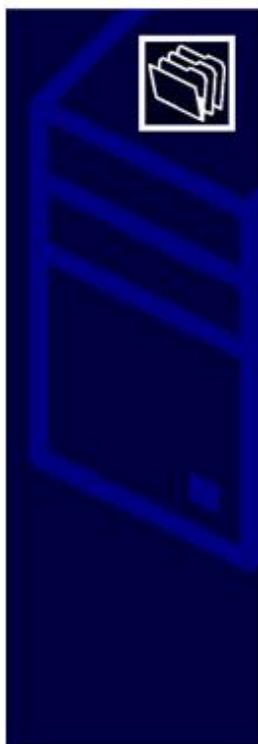
Ouvrir la console via **Outils** > **DHCP** depuis le **Gestionnaire de serveur**.



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 baux 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.

Étendues disponibles : Sélectionner tout

192.168.100.0

< Précédent **Suivant >** Annuler

Depuis SRV-AD-01, ajoutez **SRV-AD-02** comme serveur partenaire pour le basculement DHCP, puis cliquez 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 : **Ajouter un serveur**

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

< Précédent Suivant > Annuler

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 :

Types d'objets...

À partir de cet emplacement :

Emplacements...

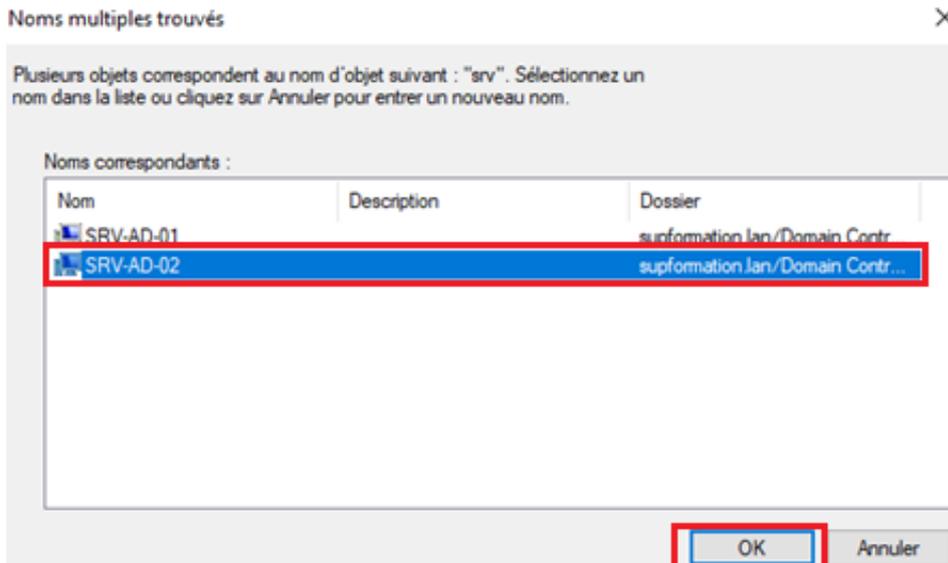
Entrez le nom de l'objet à sélectionner (exemples) :

Vérifier les noms

Avancé...

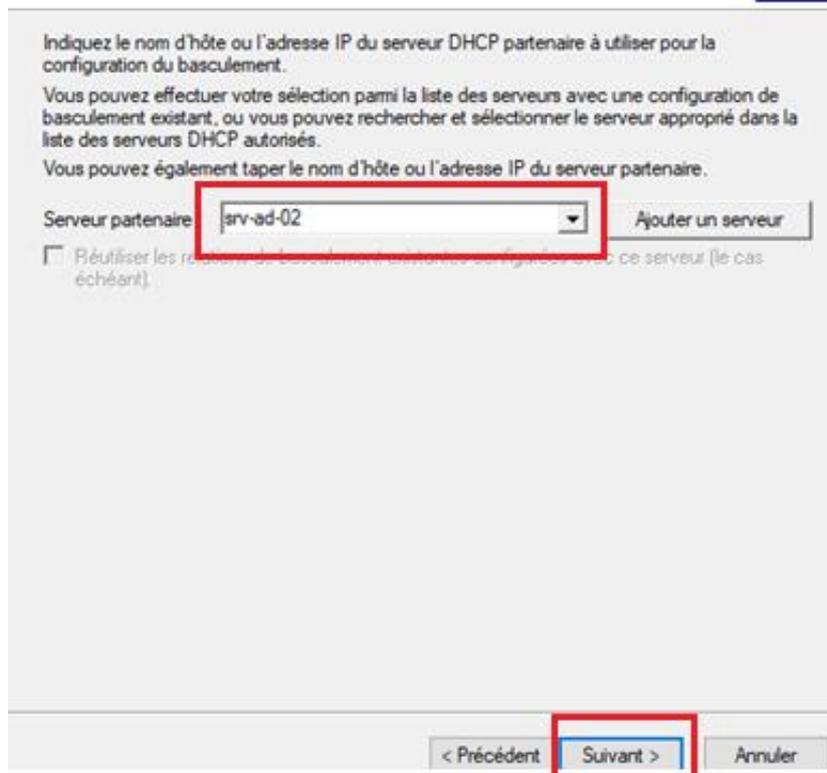
OK

Annuler



Configurer un basculement

Spécifier le serveur partenaire à utiliser pour le basculement



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 : %

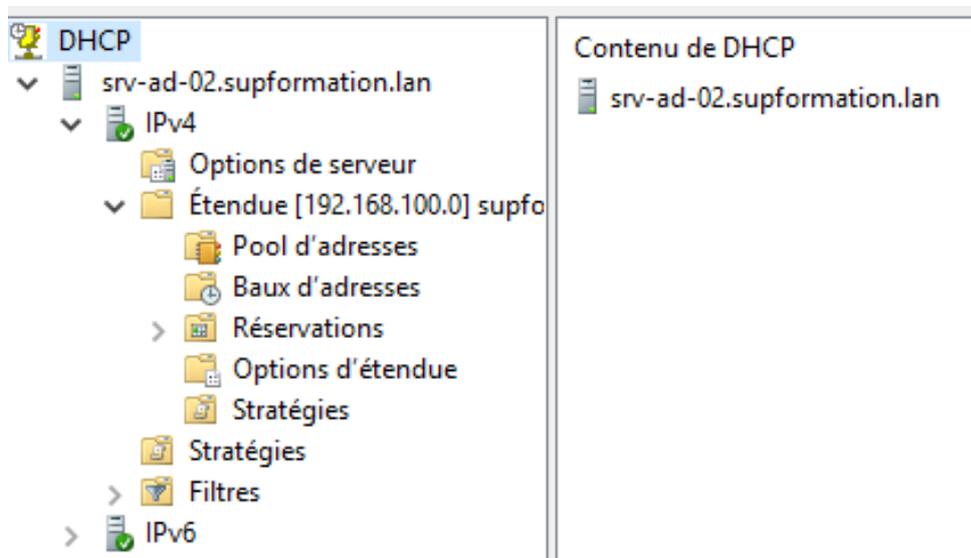
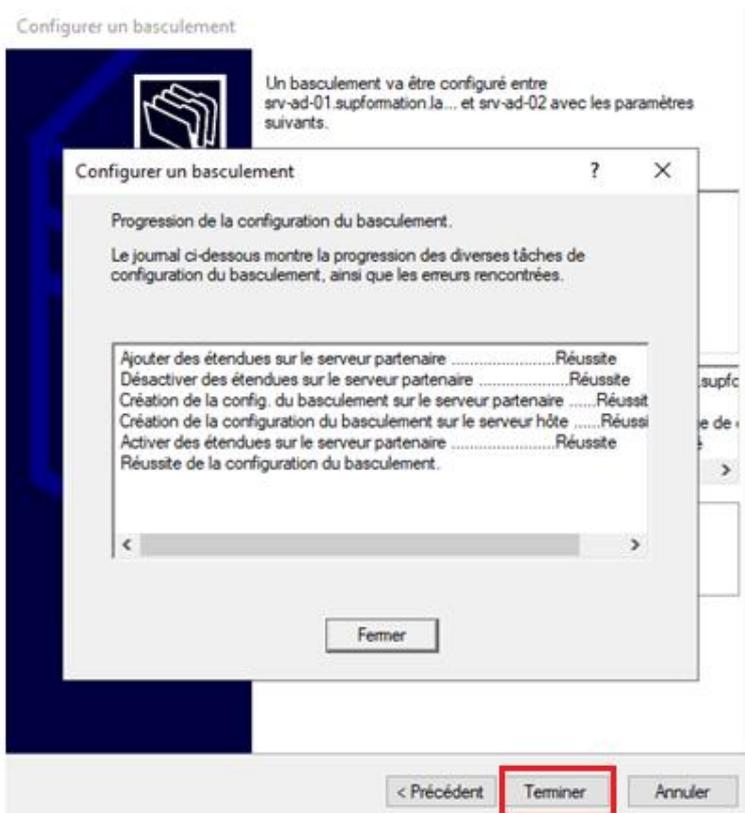
Serveur partenaire : %

Intervalle de basculement d'état : minutes

Activer l'authentification du message

Secret partagé :

< Précédent **Suivant** > Annuler

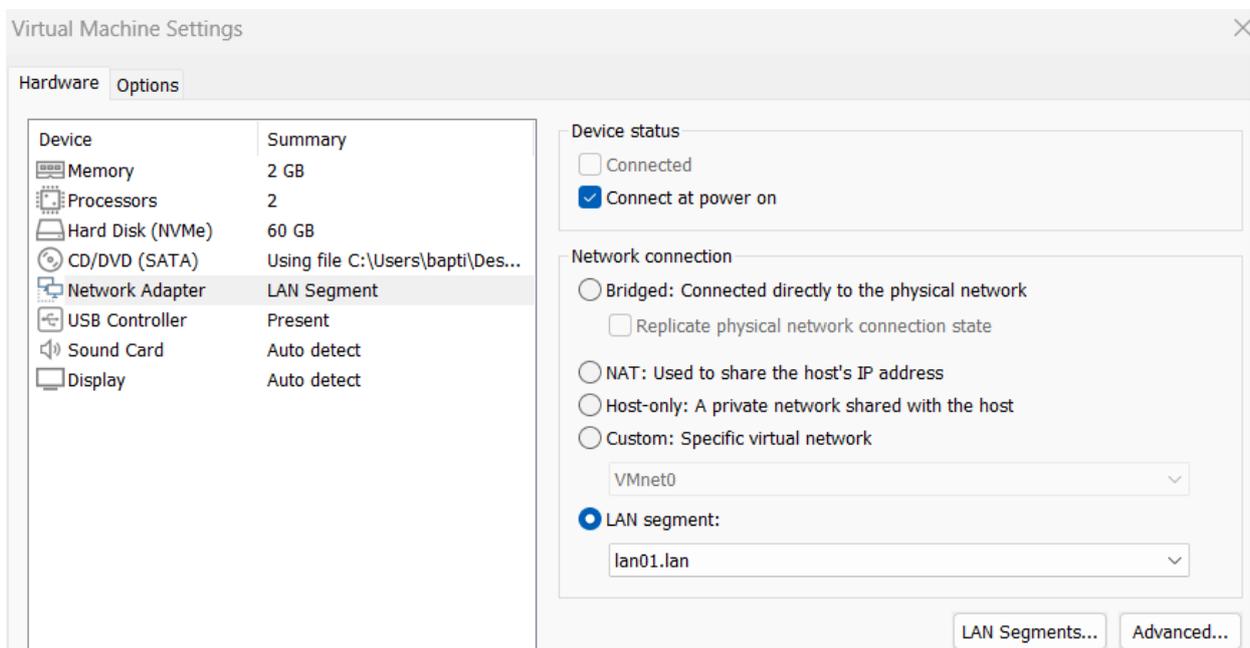


Serveur WSUS

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 :

Masque de sous-réseau :

Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

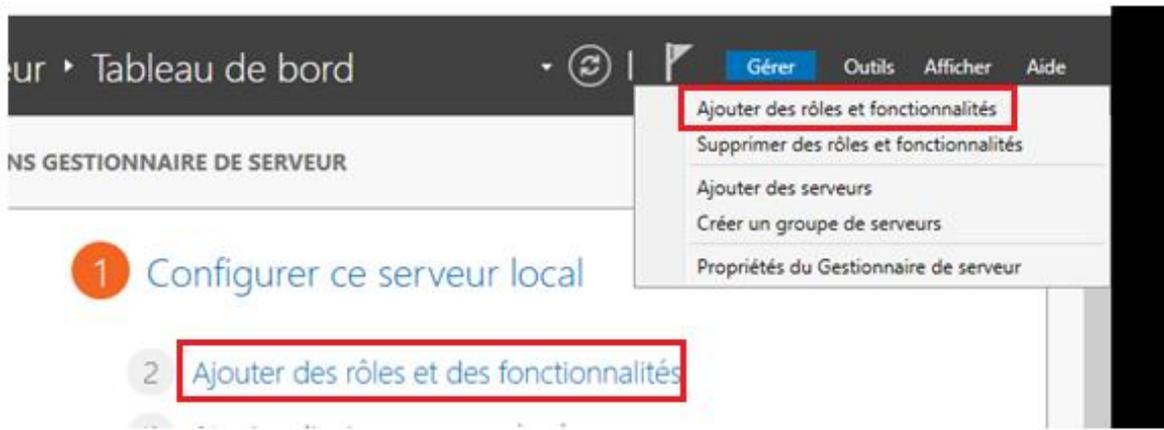
Valider les paramètres en quittant

Modification du nom ou du domaine de l'ordinateur X

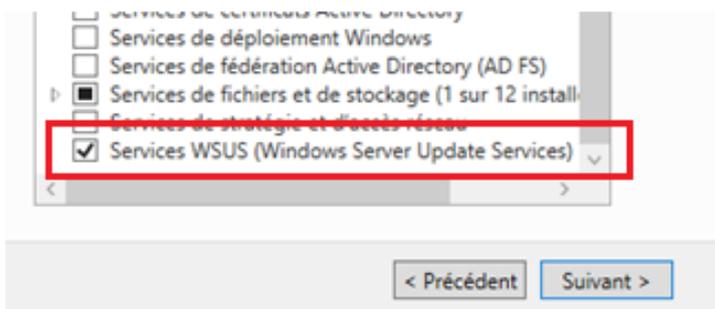


Bienvenue dans le domaine supformation.lan.

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



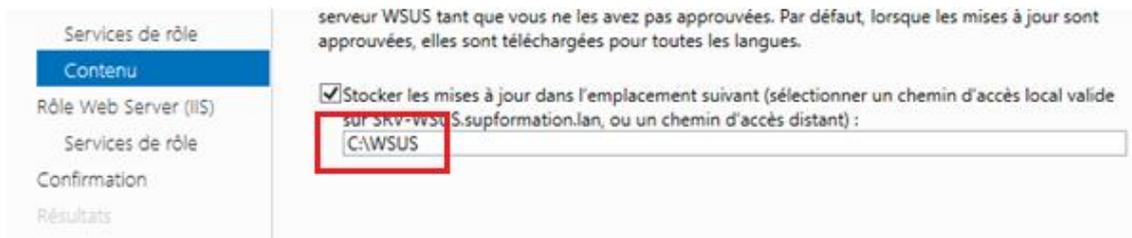
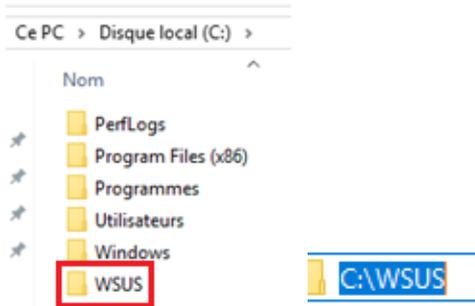
Passer les premiers écrans en cliquant sur **Suivant**, puis cocher la fonctionnalité « **Services WSUS (Windows Server Update Services)** ».



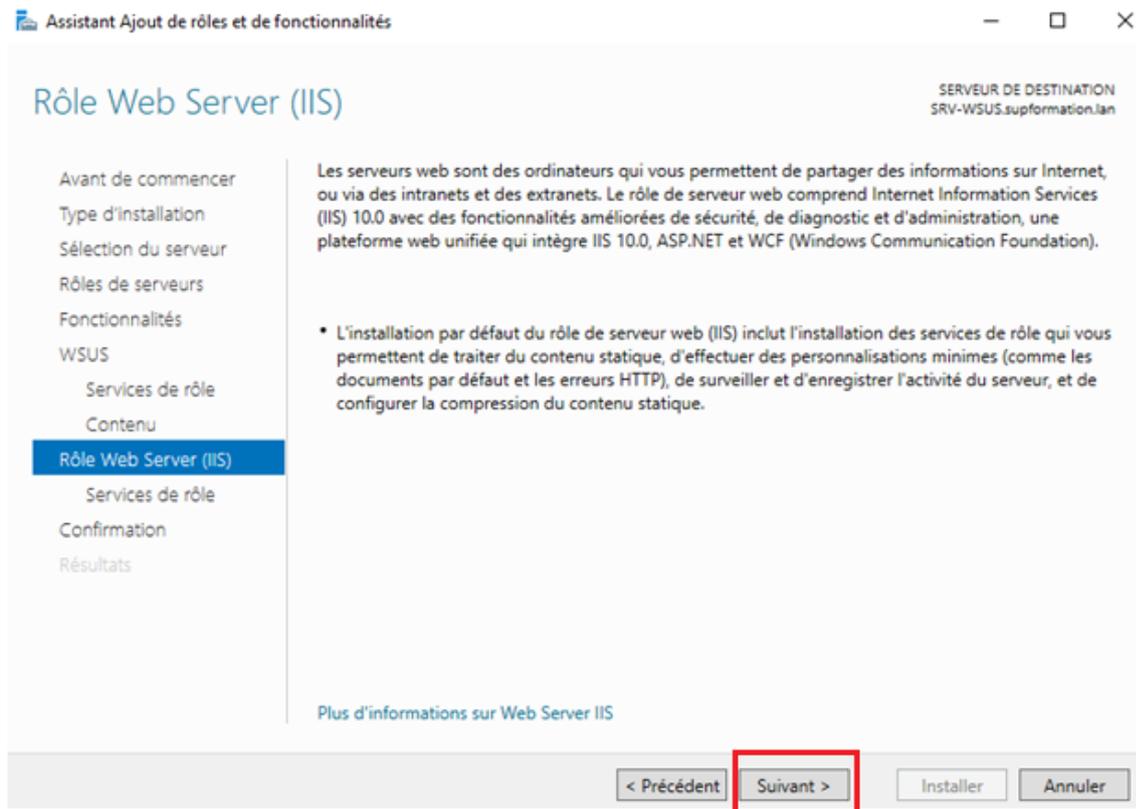
Suivant à plusieurs reprises, coche ensuite les services de rôle « **WID Connectivity** » et « **WSUS Services** », puis clique sur **Suivant**.

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

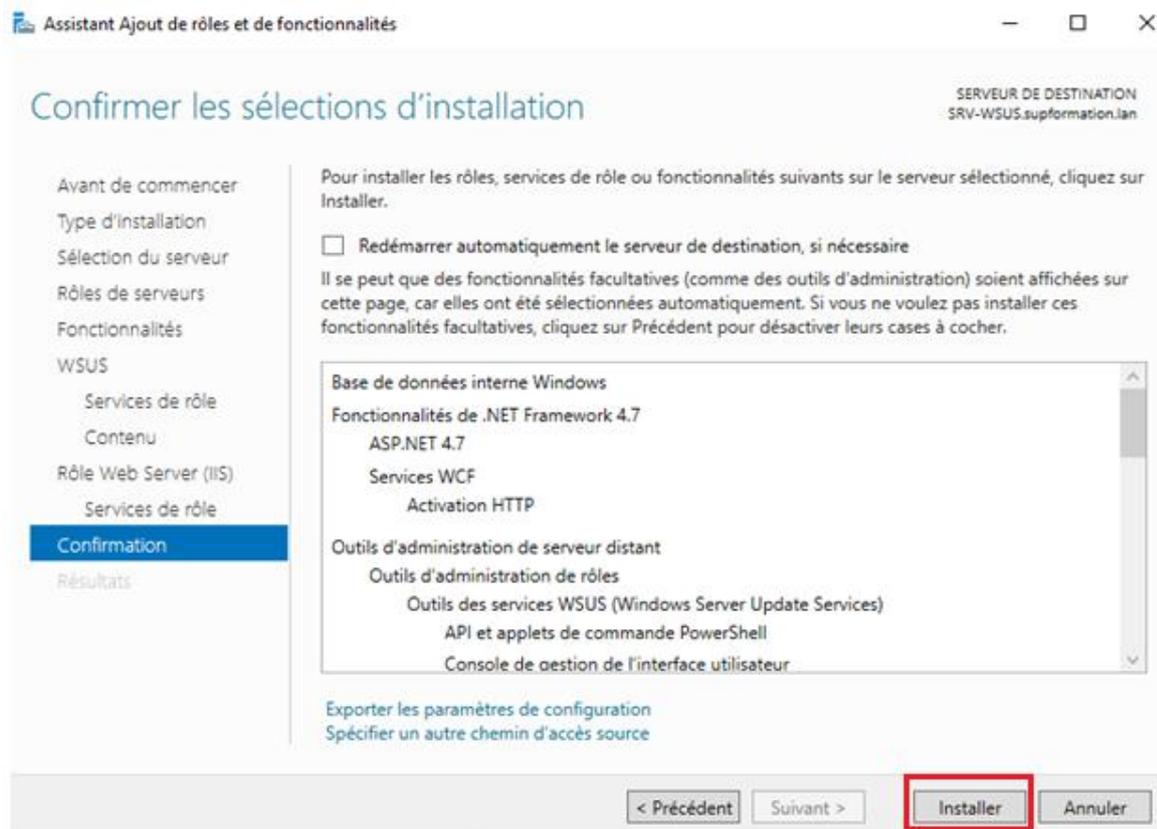
Ici, ne disposant que d'un seul disque, nous créons un dossier dédié sur celui-ci, par exemple C:\WSUS, puis nous l'indiquons comme chemin de stockage avant de cliquer sur **Suivant**.



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.



Assistant Ajout de rôles et de fonctionnalités

CONFIRMER LES SÉLECTIONS D'INSTALLATION

SERVEUR DE DESTINATION
SRV-WSUS.supformation.lan

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

- Base de données interne Windows
- Fonctionnalités de .NET Framework 4.7
 - ASP.NET 4.7
 - Services WCF
 - Activation HTTP
- Outils d'administration de serveur distant
 - Outils d'administration de rôles
 - Outils des services WSUS (Windows Server Update Services)
 - API et applets de commande PowerShell
 - Console de gestion de l'interface utilisateur

Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source

< Précédent Suivant > **Installer** Annuler

Afficher la progression de l'installation

i Installation de fonctionnalité

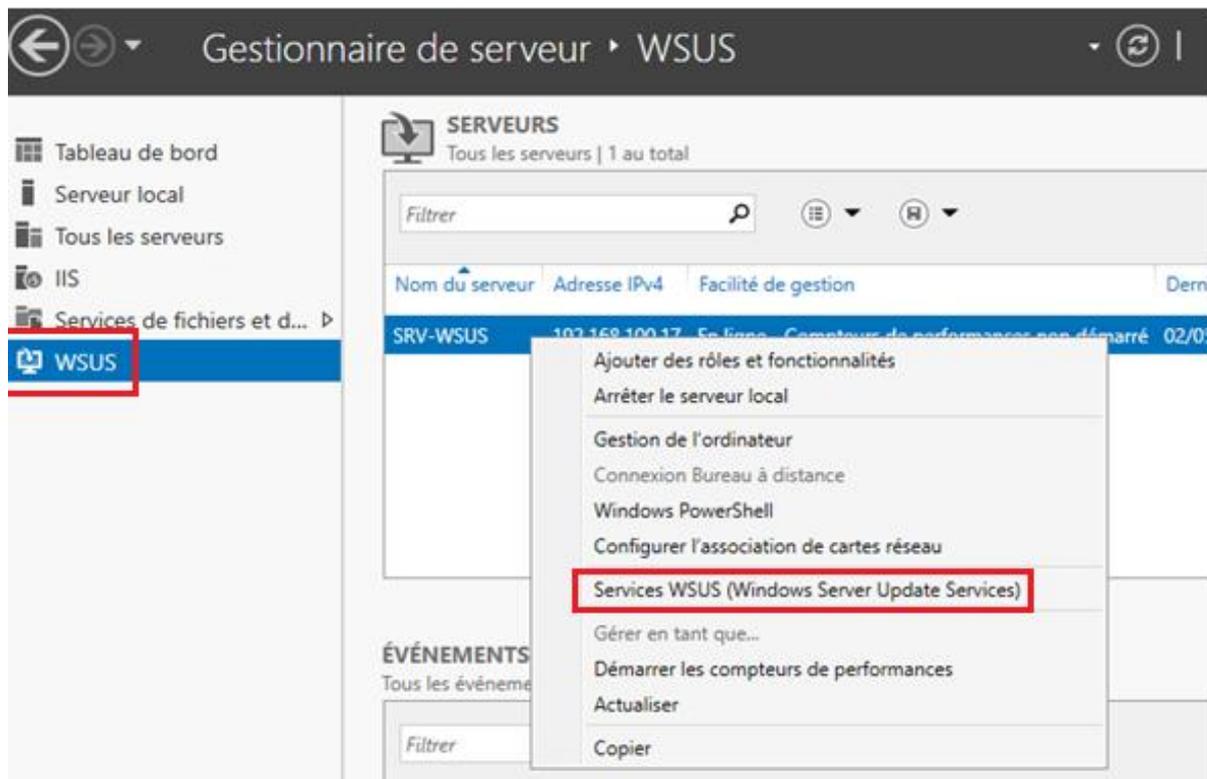
Configuration requise. Installation réussie sur SRV-WSUS.supformation.lan.

Configuration du service WSUS

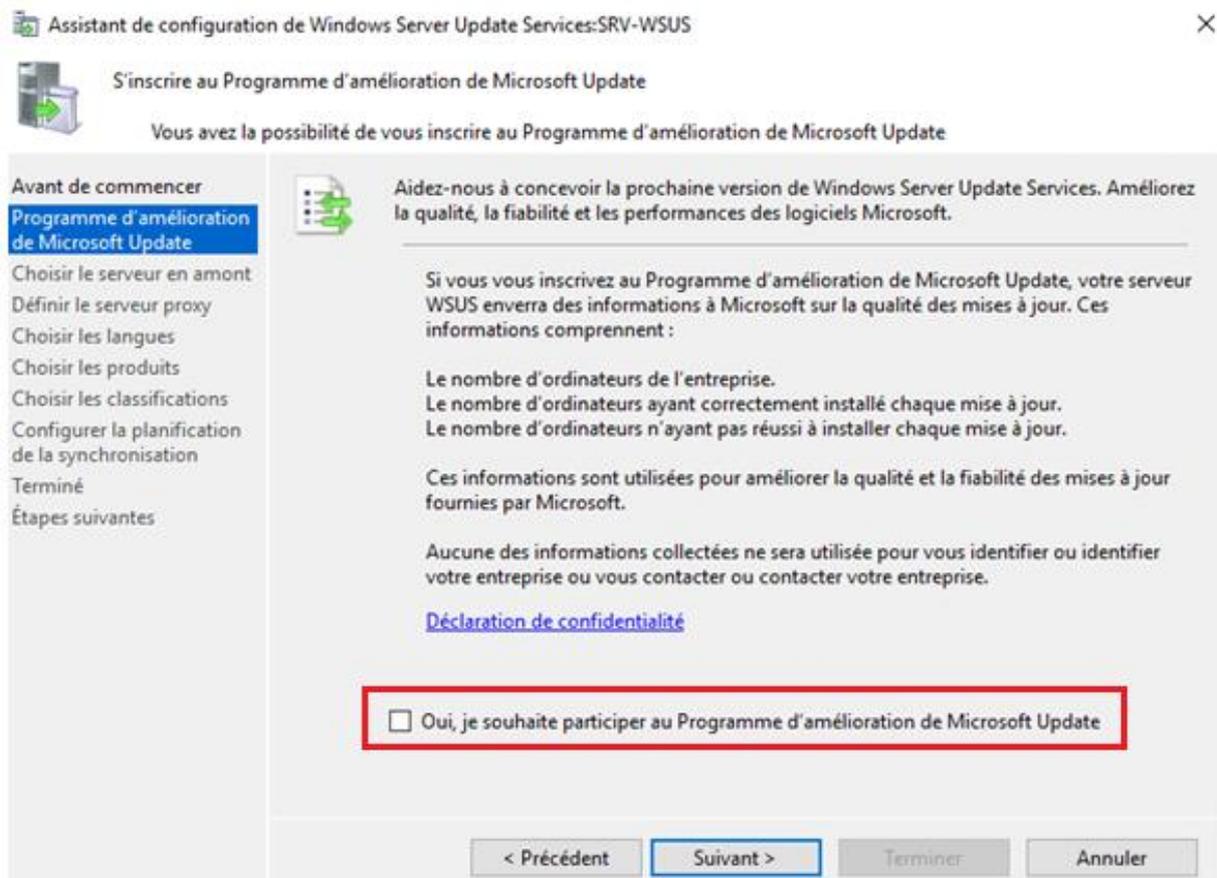
Après l'installation, une alerte apparaît dans le Gestionnaire de serveur, cliquer sur "**Lancer les tâches de post-installation**" pour finaliser le déploiement du service WSUS.

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.

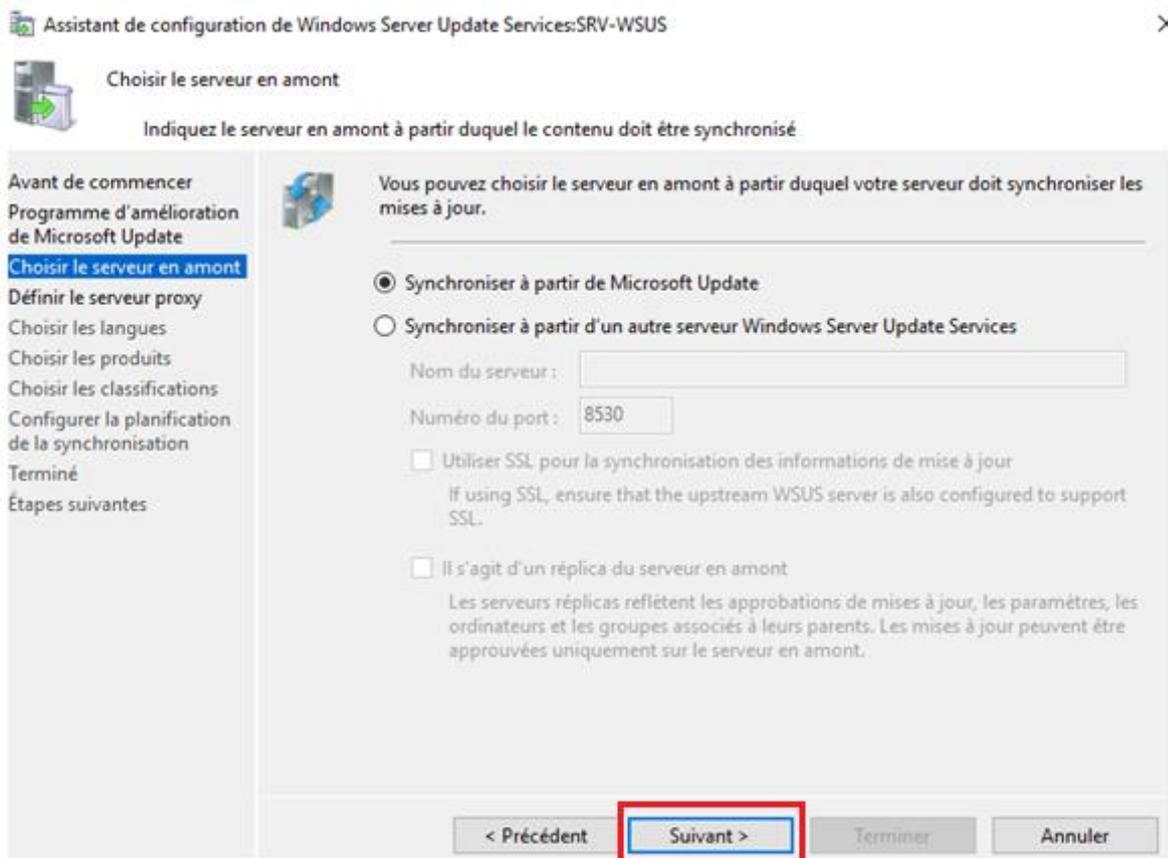
Pour cela, ouvrir le **Gestionnaire de serveur**, cliquer sur **WSUS** dans le menu de gauche, puis effectuer un **clic droit** sur le nom du serveur et sélectionner **Service WSUS**.



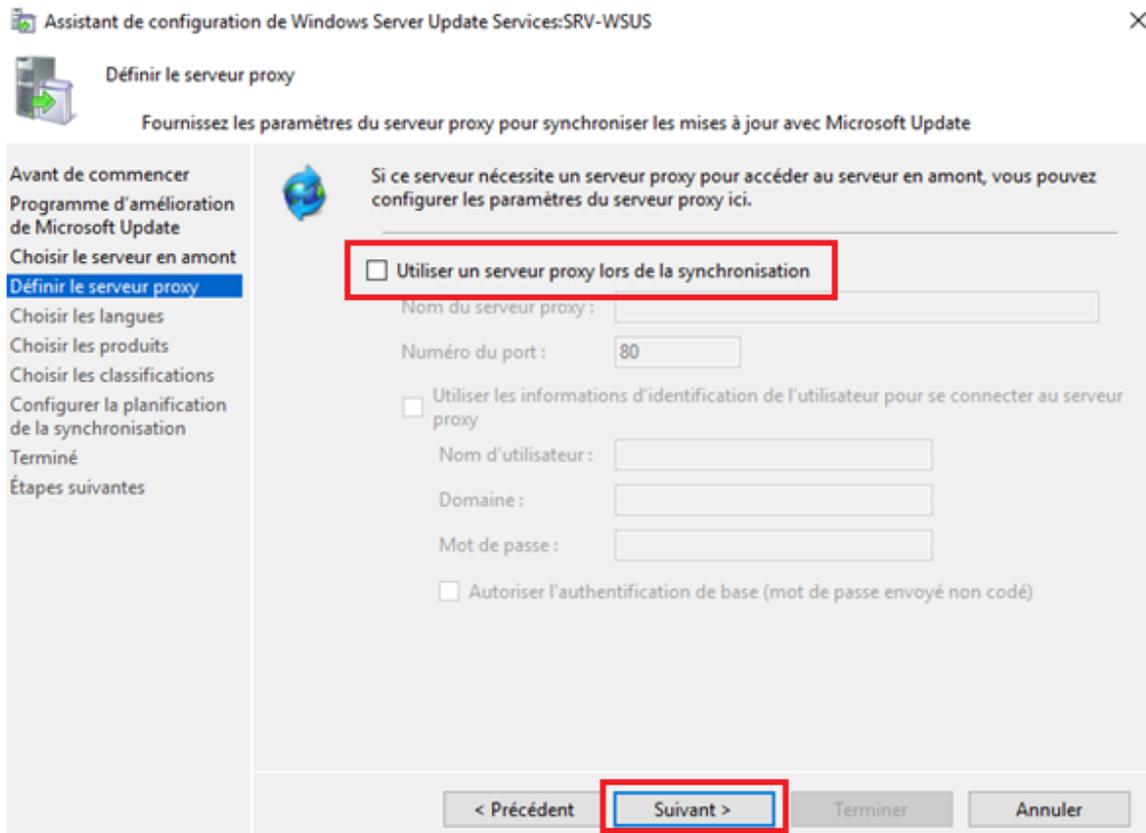
L'assistant de configuration s'ouvre automatiquement. Cliquer sur **Suivant** pour commencer.
À l'étape de collecte de données, ne pas cocher la case si l'on ne souhaite pas envoyer d'informations à Microsoft, puis cliquer sur **Suivant**.



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**.



Assistant de configuration de Windows Server Update Services:SRV-WSUS

Définir le serveur proxy

Fournissez les paramètres du serveur proxy pour synchroniser les mises à jour avec Microsoft Update

Avant de commencer
Programme d'amélioration de Microsoft Update
Choisir le serveur en amont
Définir le serveur proxy
Choisir les langues
Choisir les produits
Choisir les classifications
Configurer la planification de la synchronisation
Terminé
Étapes suivantes

Si ce serveur nécessite un serveur proxy pour accéder au serveur en amont, vous pouvez configurer les paramètres du serveur proxy ici.

Utiliser un serveur proxy lors de la synchronisation

Nom du serveur proxy :

Numéro du port :

Utiliser les informations d'identification de l'utilisateur pour se connecter au serveur proxy

Nom d'utilisateur :

Domaine :

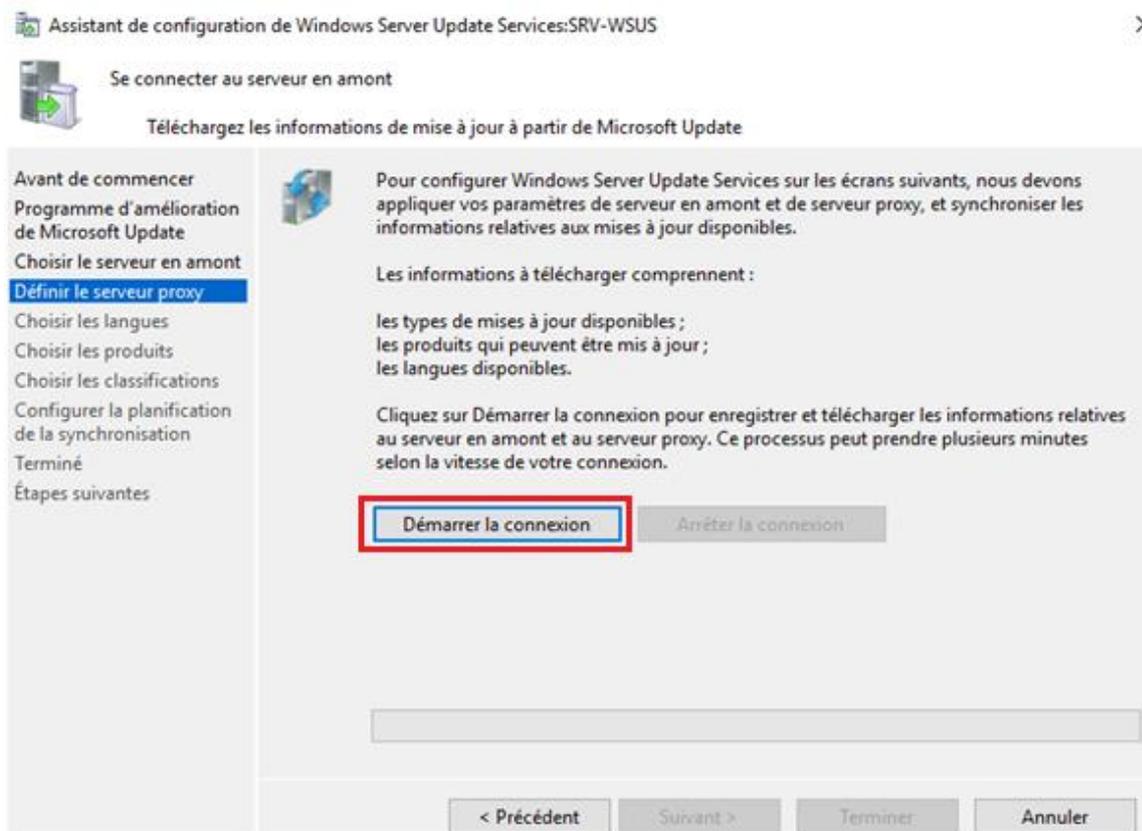
Mot de passe :

Autoriser l'authentification de base (mot de passe envoyé non codé)

< Précédent **Suivant >** Terminer Annuler

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**.

Si vous stockez les fichiers de mise à jour localement, vous pouvez filtrer les mises à jour téléchargées sur votre serveur en fonction de la langue. Le choix des langues aura une incidence sur les ordinateurs qui pourront être mis à jour sur ce serveur et les serveurs en aval.

Télécharger les mises à jour dans toutes les langues, y compris les nouvelles
 Télécharger les mises à jour dans ces langues uniquement :

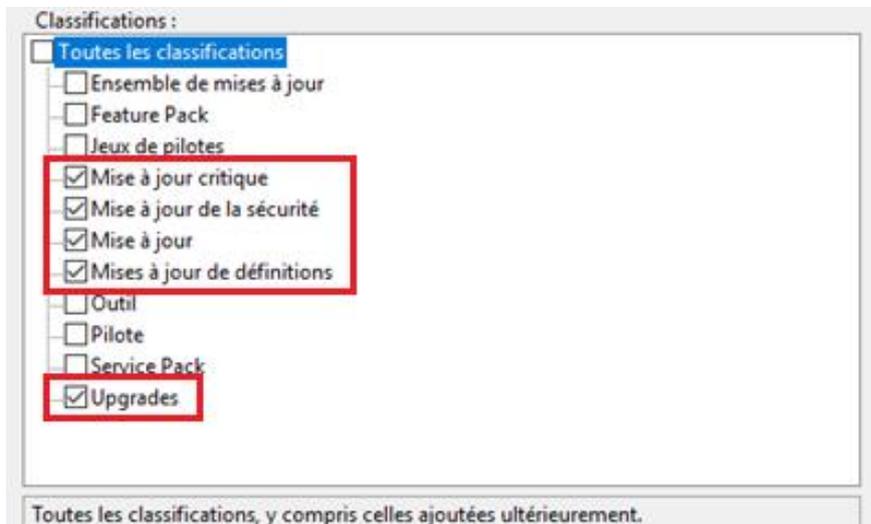
<input type="checkbox"/> Allemand	<input type="checkbox"/> Estonien	<input type="checkbox"/> Lituanien
<input checked="" type="checkbox"/> Anglais	<input type="checkbox"/> Finnois	<input type="checkbox"/> Néerlandais
<input type="checkbox"/> Arabe	<input checked="" type="checkbox"/> Français	<input type="checkbox"/> Norvégien
<input type="checkbox"/> Bulgare	<input type="checkbox"/> Grec	<input type="checkbox"/> Polonais
<input type="checkbox"/> Chinois (Hong Kong (R.A.S.))	<input type="checkbox"/> Hébreu	<input type="checkbox"/> Portugais
<input type="checkbox"/> Chinois simplifié	<input type="checkbox"/> Hindi	<input type="checkbox"/> Portugais
<input type="checkbox"/> Chinois traditionnel	<input type="checkbox"/> Hongrois	<input type="checkbox"/> Roumain
<input type="checkbox"/> Coréen	<input type="checkbox"/> Italien	<input type="checkbox"/> Russe
<input type="checkbox"/> Croate	<input type="checkbox"/> Japonais	<input type="checkbox"/> Serbe (lati)
<input type="checkbox"/> Danois	<input type="checkbox"/> Japonais (NEC)	<input type="checkbox"/> Slovaque
<input type="checkbox"/> Espagnol	<input type="checkbox"/> Letton	<input type="checkbox"/> Slovène

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**.

<input type="checkbox"/> Visual Studio 2022
<input checked="" type="checkbox"/> Windows 10, version 1903 and later
<input type="checkbox"/> Windows Server 2016 for RS4

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



The screenshot shows the 'Classifications' window in WSUS. It contains a list of classification categories with checkboxes. The following categories are checked and highlighted with red boxes:

- Toutes les classifications
- Mise à jour critique
- Mise à jour de la sécurité
- Mise à jour
- Mises à jour de définitions
- Upgrades

Other categories like 'Ensemble de mises à jour', 'Feature Pack', 'Jeux de pilotes', 'Outil', 'Pilote', and 'Service Pack' are unchecked. A footer note reads: 'Toutes les classifications, y compris celles ajoutées ultérieurement.'

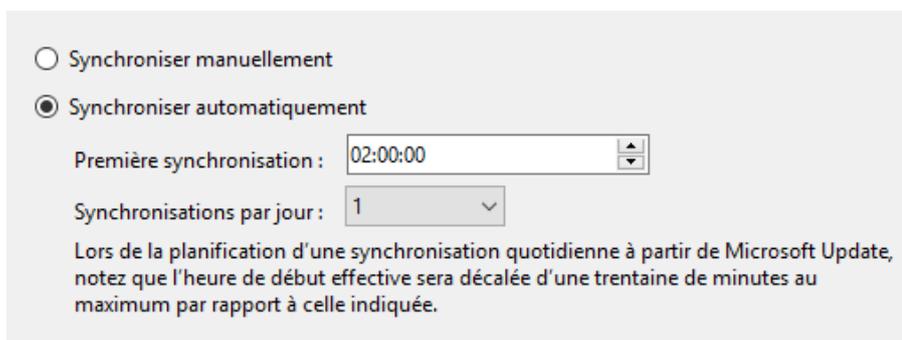
Jusqu'à présent, nous avons défini les besoins de l'infrastructure.

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**.



The screenshot shows the 'Synchronisation' configuration window. Two radio buttons are present:

- Synchroniser manuellement
- Synchroniser automatiquement

Below the radio buttons, there are two input fields:

- Première synchronisation : 02:00:00
- Synchronisations par jour : 1

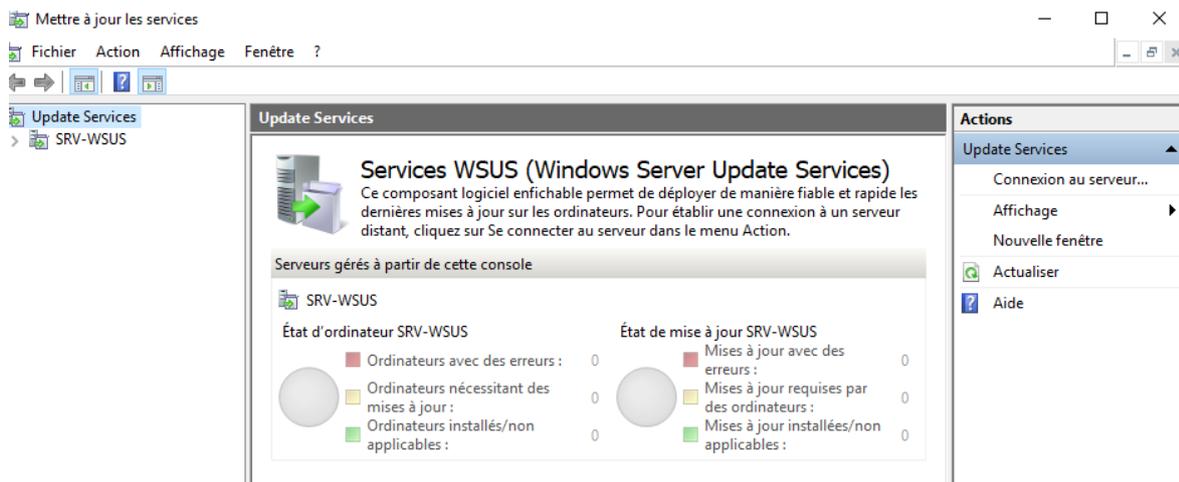
A note at the bottom states: 'Lors de la planification d'une synchronisation quotidienne à partir de Microsoft Update, notez que l'heure de début effective sera décalée d'une trentaine de minutes au maximum par rapport à celle indiquée.'

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.

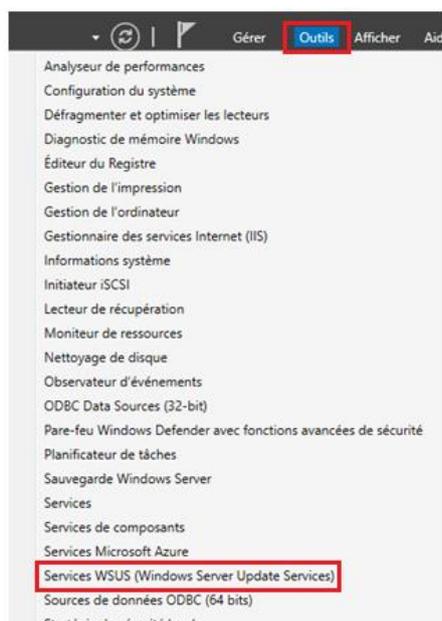
Dans notre cas, elle est estimée à **environ 1h30**.



Aperçu de la console d'administration du Serveur WSUS

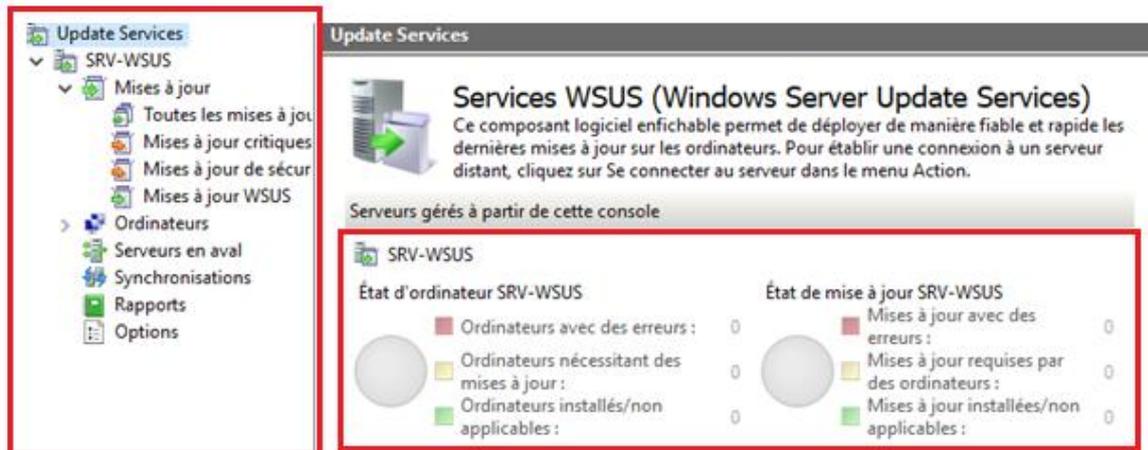
Pour accéder à la console d'administration de WSUS, ouvrir le **Gestionnaire de serveur**, puis cliquer sur **Outils**.

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



Voici l'aperçu de la console WSUS :

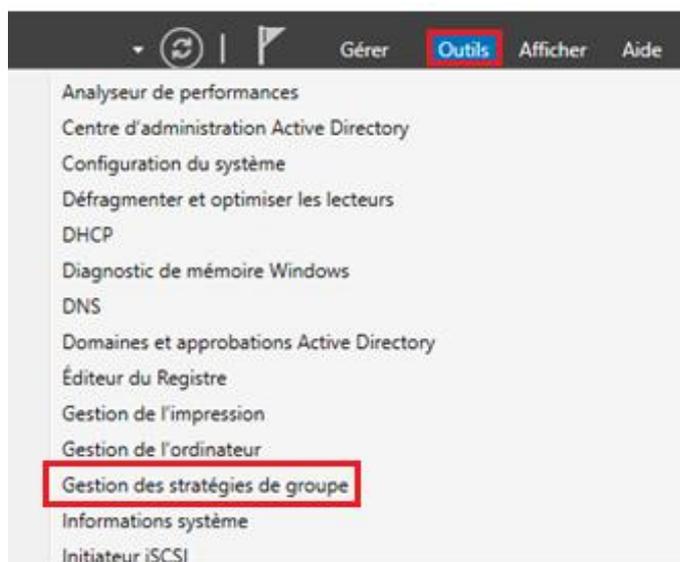
1. Un volet latéral regroupant l'ensemble des **catégories** de gestion.
2. Un tableau de bord affichant l'**état des ordinateurs** recensés et celui des **mises à jour disponibles**.



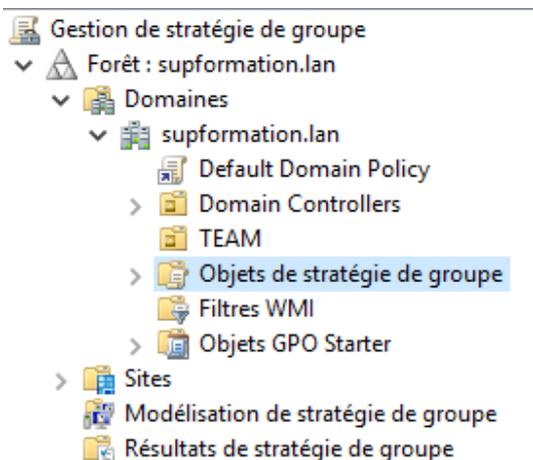
GPO – Gestion des stratégies de groupe

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 :

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

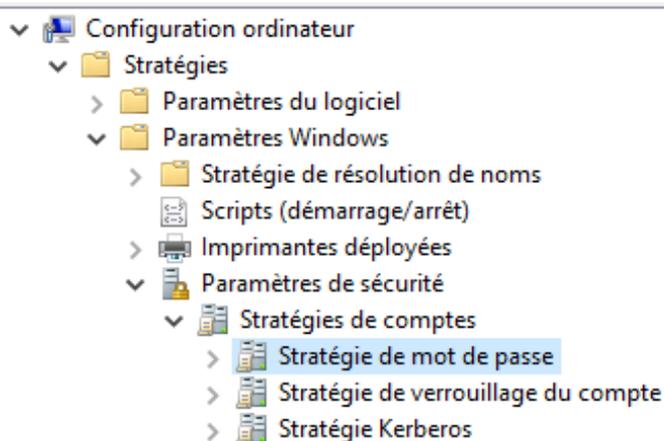
Nommer cet objet de stratégie de groupe « Mot de passe », puis cliquer sur **OK**.



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

- Stratégie Panneau de configuration [SRV-AD-01.SUI]
 - > Configuration ordinateur
 - > Configuration utilisateur
 - ▼ Stratégies
 - > Paramètres du logiciel
 - > Paramètres Windows
 - ▼ Modèles d'administration : définitions d:
 - > Bureau
 - > Composants Windows
 - > Dossiers partagés
 - > Menu Démarrer et barre des tâches
 - > **Panneau de configuration**
 - > Réseau
 - > Système
 - > Tous les paramètres
 - > Préférences

Interdire l'accès au Panneau de configuration et à l'applicati...	Non configuré
N'afficher que les éléments du Panneau de configuration sp...	Non configuré

Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC

Paramètre précédent Paramètre suivant

Non configuré Commentaire :

Activé

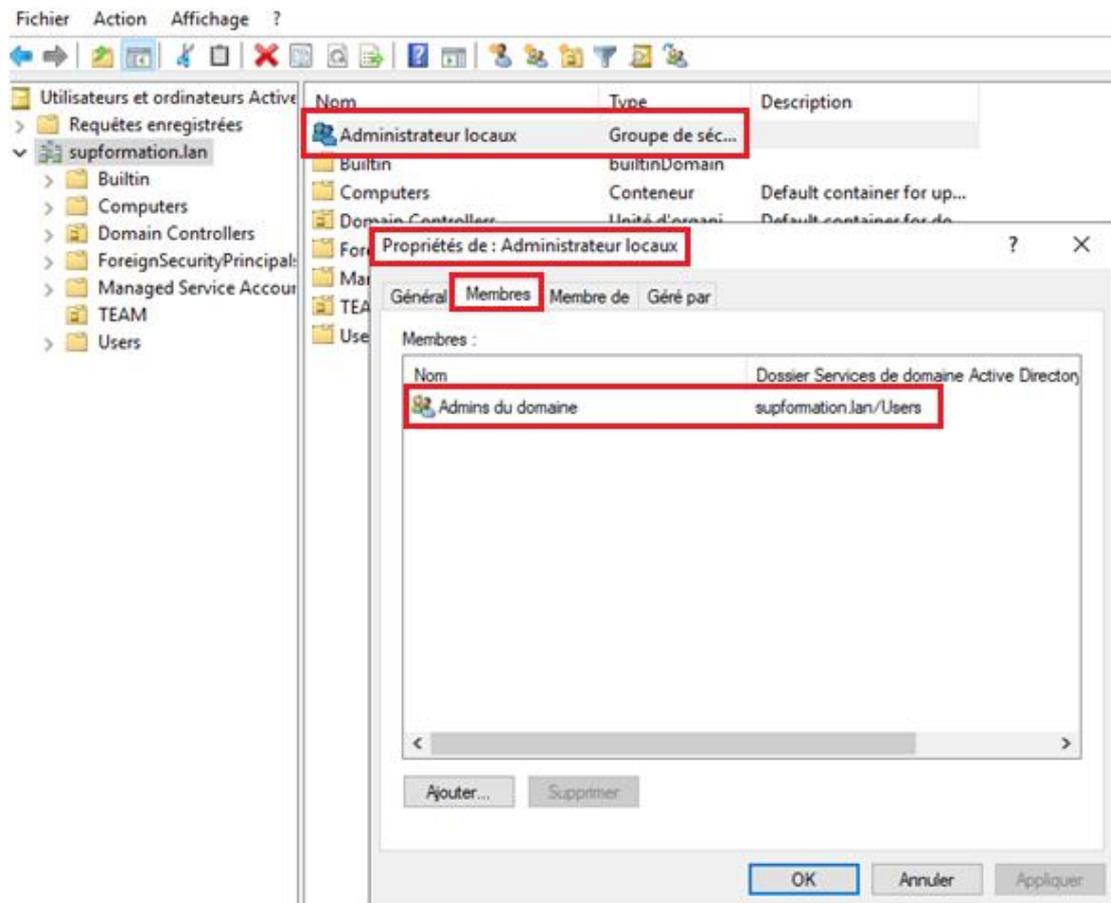
Désactivé

Pris en charge sur : Au minimum Windows 2000

Masquer les éléments du Panneau de configuration spécifiés	Non configuré
Toujours afficher tous les éléments du Panneau de configur...	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**.



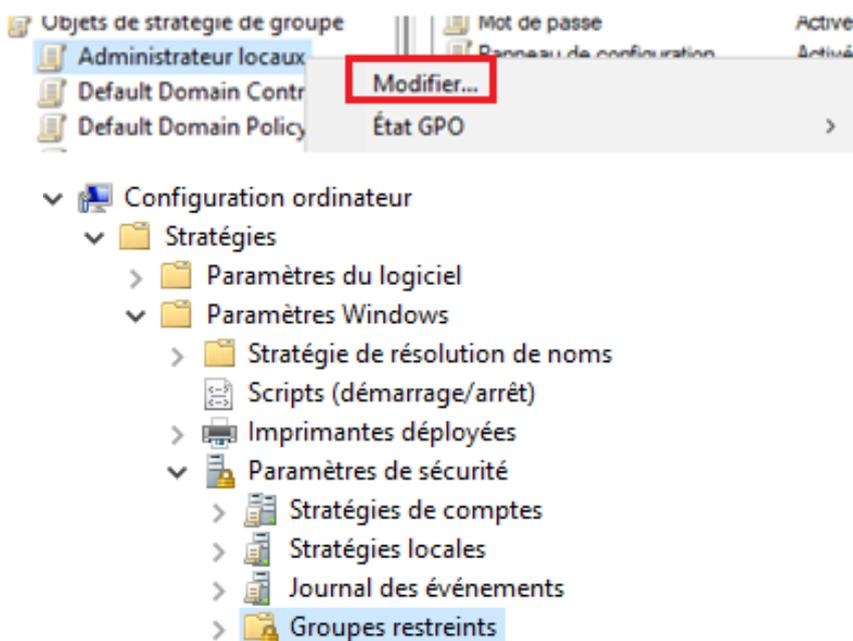
Effectuer le procédé habituel : clic droit sur l'**unité d'organisation (UO)** concernée, puis sélectionner « **Créer un objet GPO dans ce domaine et le lier ici...** ».

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

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

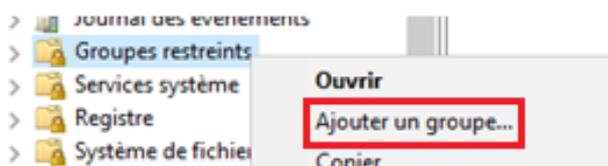
Déplier les menus suivants dans l'éditeur de stratégie de groupe :

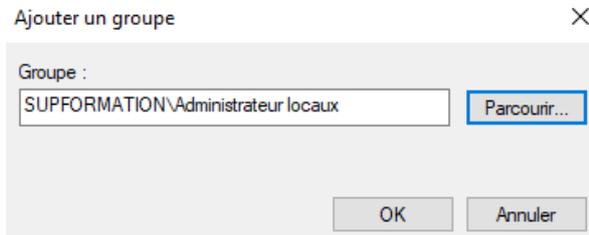
Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Groupes restreint



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

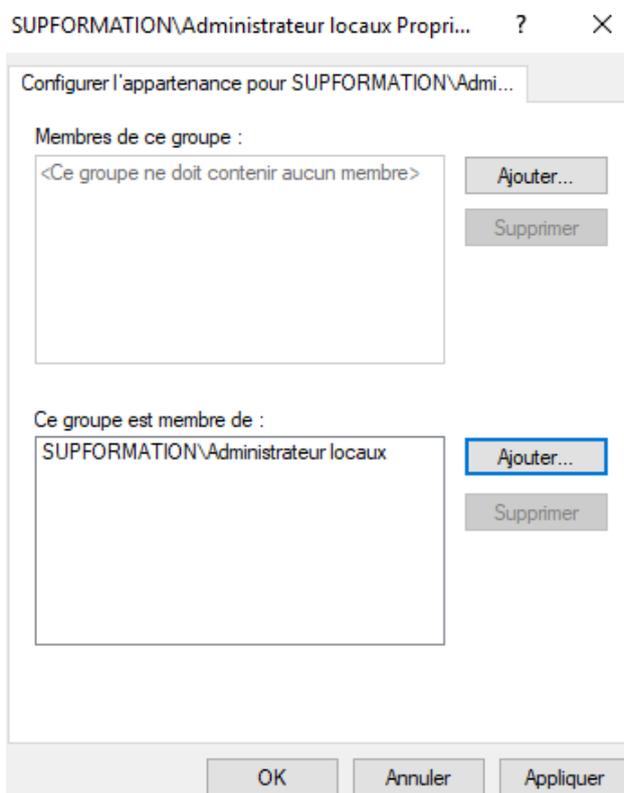
Utiliser le bouton **Parcourir** pour rechercher dans l'Active Directory et sélectionner le groupe « **Administrateur locaux** » préalablement créé à cet effet.



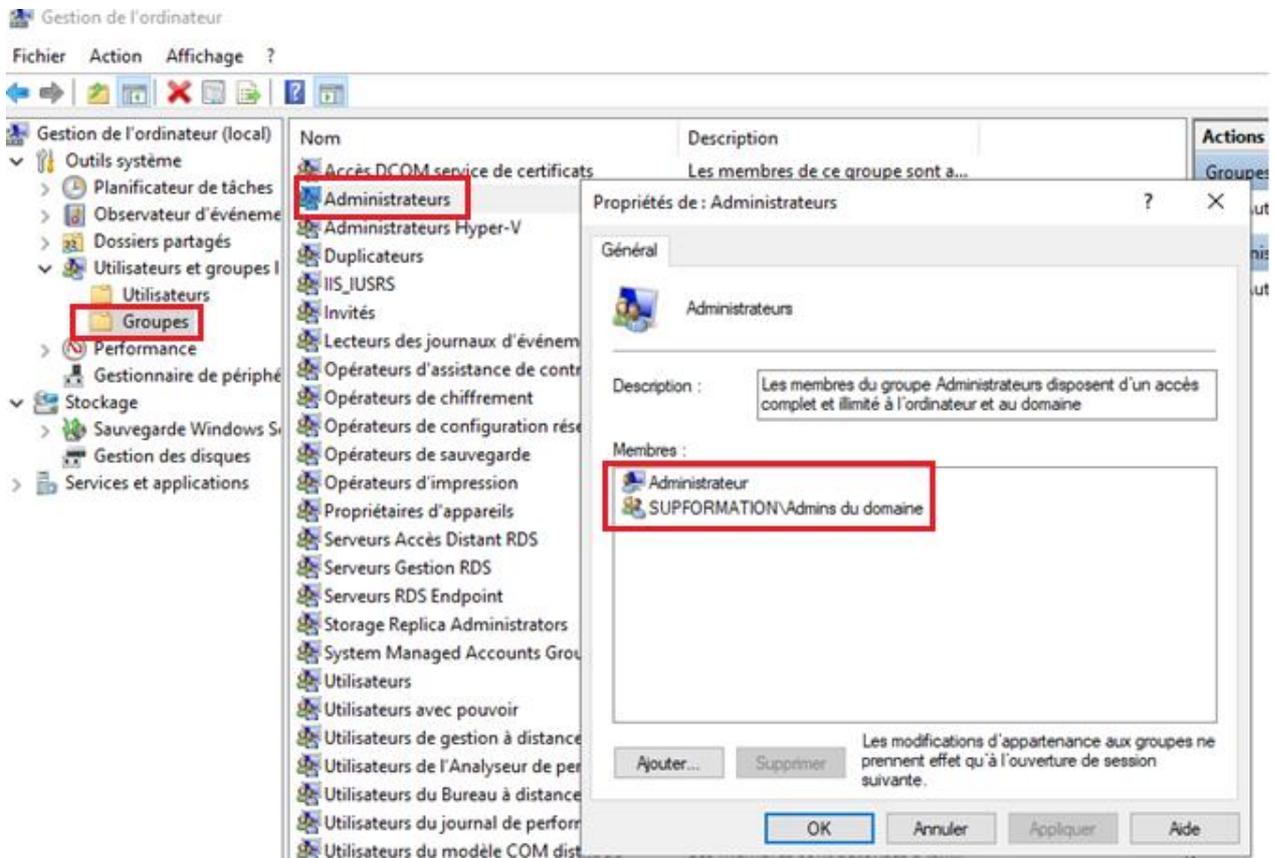


Dans la fenêtre **Configurer l'appartenance**, ajouter dans « **Ce groupe est membre de** » le groupe **Administrateurs**, afin que les membres du groupe « Administrateurs locaux » soient reconnus comme administrateurs **locaux** sur les postes clients du domaine.

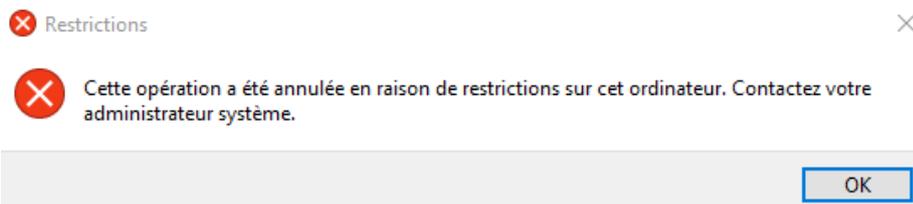
Puis cliquer sur **Appliquer** et **OK**.



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'OU cible, **clic droit** > **Modifier**, puis naviguer dans les paramètres comme suit :

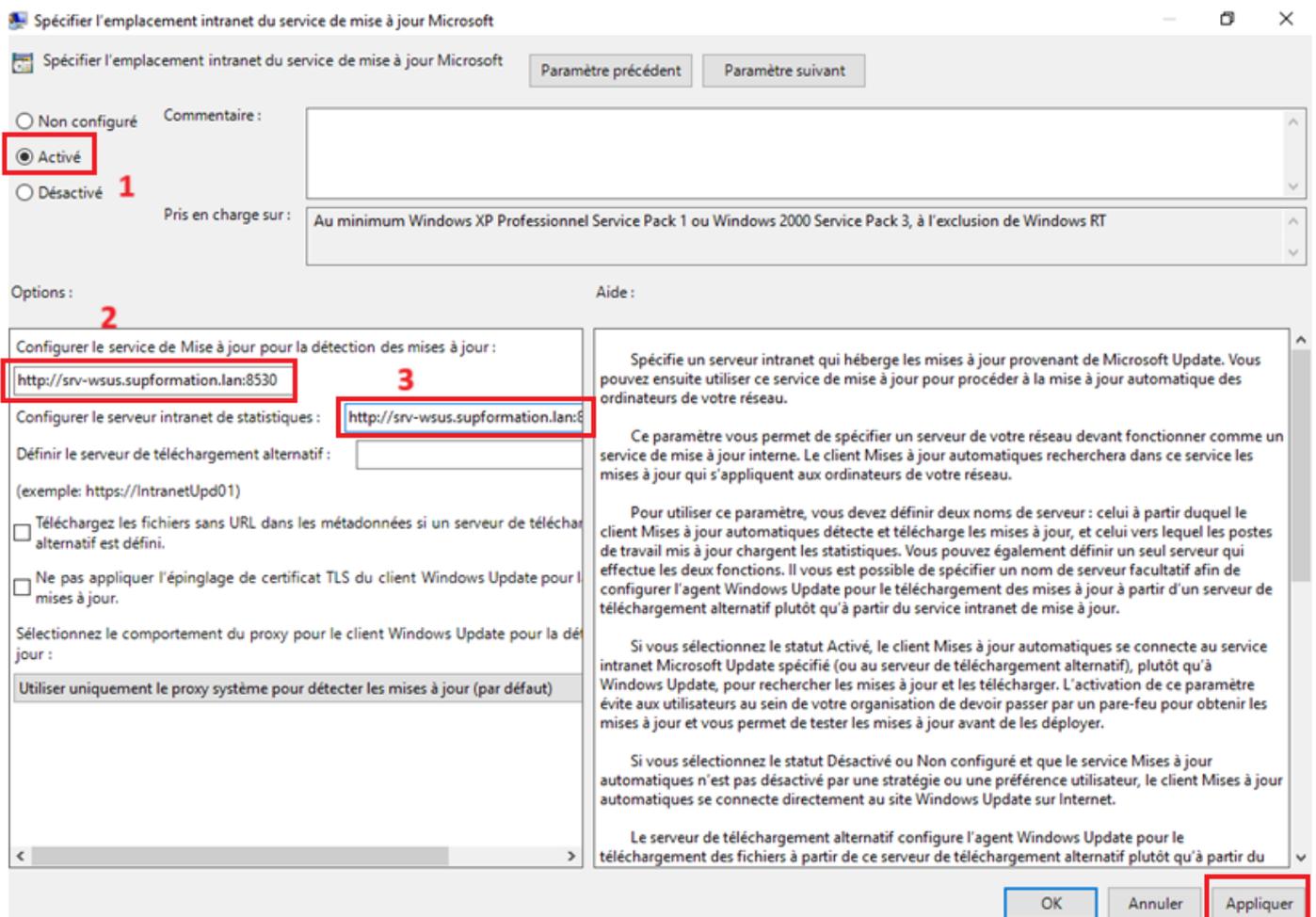


Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Windows Update

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**.



Spécifier l'emplacement intranet du service de mise à jour Microsoft

Paramètre précédent Paramètre suivant

Non configuré Commentaire :

Activé 1

Désactivé 1

Pris en charge sur : Au minimum Windows XP Professionnel Service Pack 1 ou Windows 2000 Service Pack 3, à l'exclusion de Windows RT

Options : 2

Aide :

Configurer le service de Mise à jour pour la détection des mises à jour :

3

Configurer le serveur intranet de statistiques :

Définir le serveur de téléchargement alternatif :

(exemple: https://IntranetUpd01)

Téléchargez les fichiers sans URL dans les métadonnées si un serveur de téléchargement alternatif est défini.

Ne pas appliquer l'épinglage de certificat TLS du client Windows Update pour les mises à jour.

Sélectionnez le comportement du proxy pour le client Windows Update pour la détection :

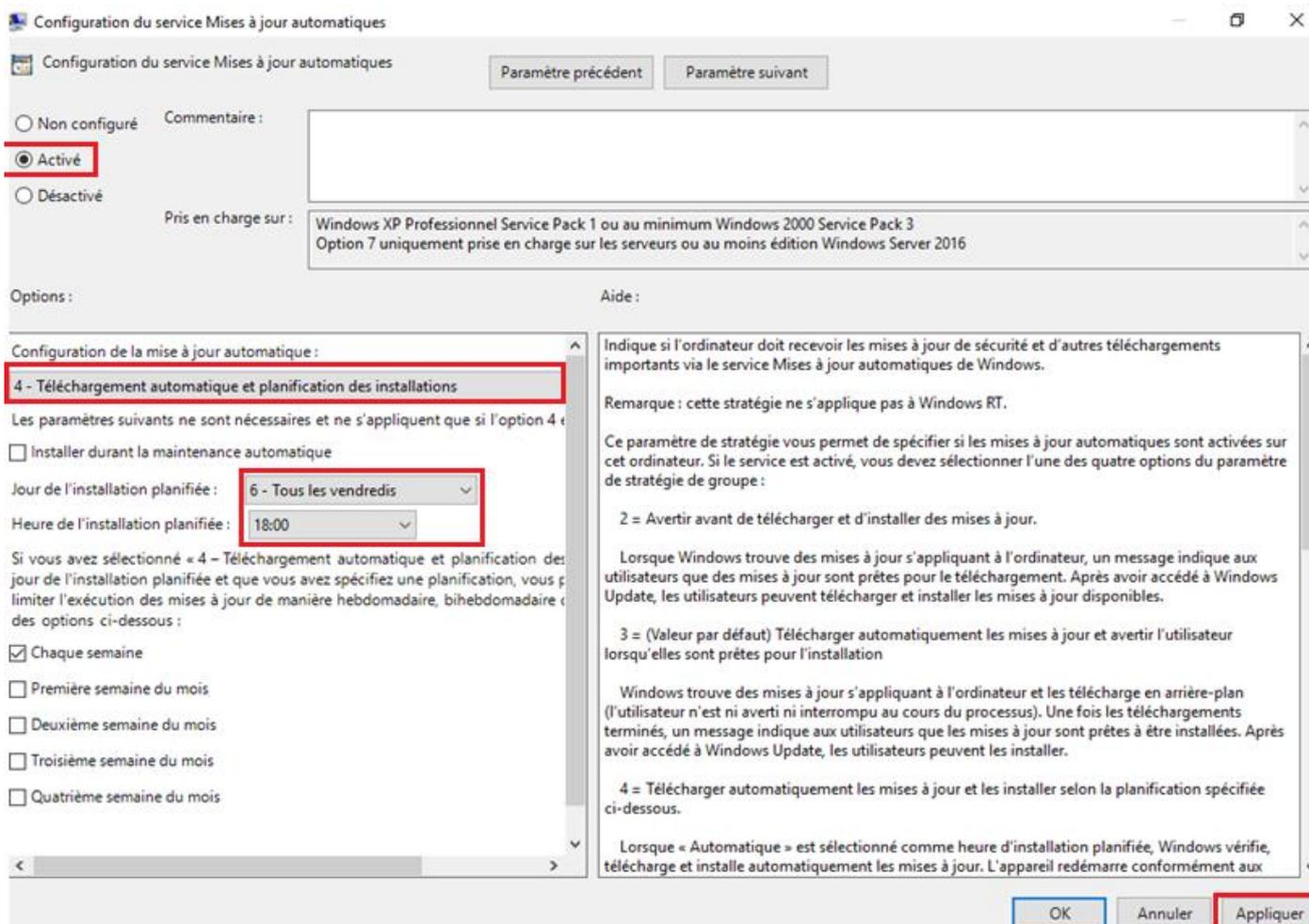
Utiliser uniquement le proxy système pour détecter les mises à jour (par défaut)

OK Annuler **Appliquer**

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**.



Configuration du service Mises à jour automatiques

Configuration du service Mises à jour automatiques

Paramètre précédent Paramètre suivant

Non configuré Commentaire :

Activé

Désactivé

Pris en charge sur : Windows XP Professionnel Service Pack 1 ou au minimum Windows 2000 Service Pack 3
Option 7 uniquement prise en charge sur les serveurs ou au moins édition Windows Server 2016

Options : Aide :

Configuration de la mise à jour automatique :

4 - Téléchargement automatique et planification des installations

Les paramètres suivants ne sont nécessaires et ne s'appliquent que si l'option 4 est sélectionnée :

Installer durant la maintenance automatique

Jour de l'installation planifiée : 6 - Tous les vendredis

Heure de l'installation planifiée : 18:00

Si vous avez sélectionné « 4 - Téléchargement automatique et planification des installations », vous pouvez limiter l'exécution des mises à jour de manière hebdomadaire, bihebdomadaire ou mensuelle en choisissant une des options ci-dessous :

Chaque semaine

Première semaine du mois

Deuxième semaine du mois

Troisième semaine du mois

Quatrième semaine du mois

Indique si l'ordinateur doit recevoir les mises à jour de sécurité et d'autres téléchargements importants via le service Mises à jour automatiques de Windows.

Remarque : cette stratégie ne s'applique pas à Windows RT.

Ce paramètre de stratégie vous permet de spécifier si les mises à jour automatiques sont activées sur cet ordinateur. Si le service est activé, vous devez sélectionner l'une des quatre options du paramètre de stratégie de groupe :

2 = Avertir avant de télécharger et d'installer des mises à jour.

Lorsque Windows trouve des mises à jour s'appliquant à l'ordinateur, un message indique aux utilisateurs que des mises à jour sont prêtes pour le téléchargement. Après avoir accédé à Windows Update, les utilisateurs peuvent télécharger et installer les mises à jour disponibles.

3 = (Valeur par défaut) Télécharger automatiquement les mises à jour et avertir l'utilisateur lorsqu'elles sont prêtes pour l'installation

Windows trouve des mises à jour s'appliquant à l'ordinateur et les télécharge en arrière-plan (l'utilisateur n'est ni averti ni interrompu au cours du processus). Une fois les téléchargements terminés, un message indique aux utilisateurs que les mises à jour sont prêtes à être installées. Après avoir accédé à Windows Update, les utilisateurs peuvent les installer.

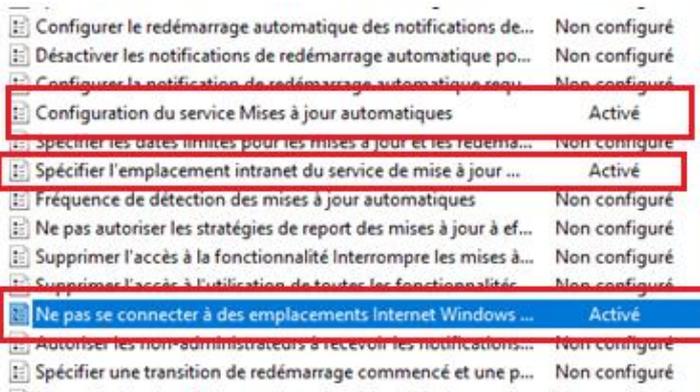
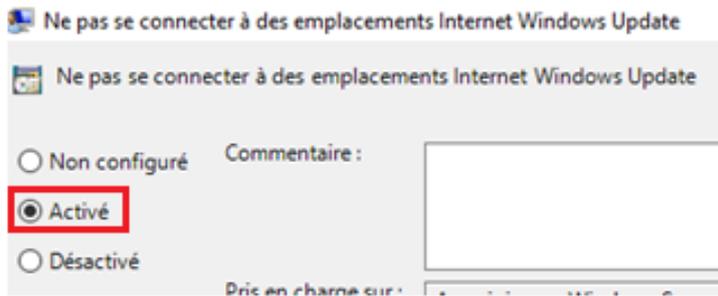
4 = Télécharger automatiquement les mises à jour et les installer selon la planification spécifiée ci-dessous.

Lorsque « Automatique » est sélectionné comme heure d'installation planifiée, Windows vérifie, télécharge et installe automatiquement les mises à jour. L'appareil redémarre conformément aux

OK Annuler **Appliquer**

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

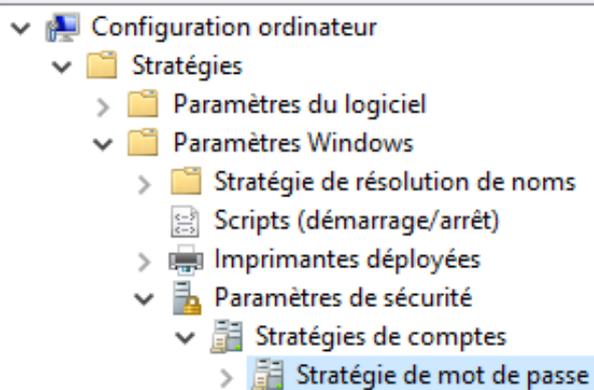
Type : Stratégie de groupe

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...*

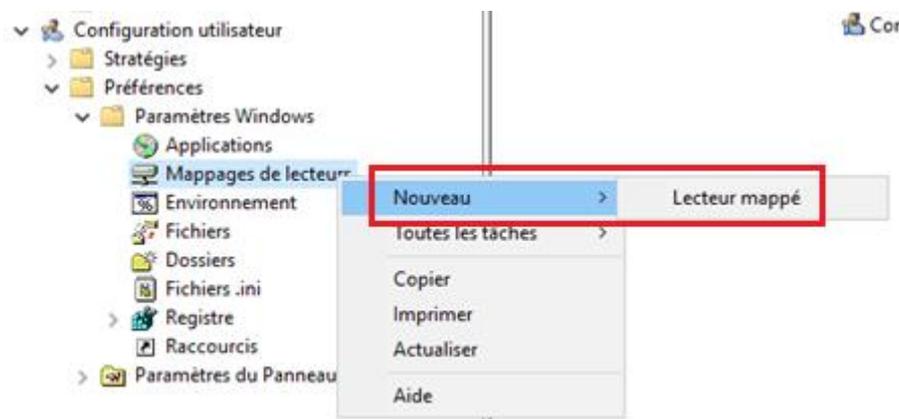
Nommer la GPO **ADM_MAPPAGE**, puis clic droit dessus > **Modifier**

Parcours à suivre :

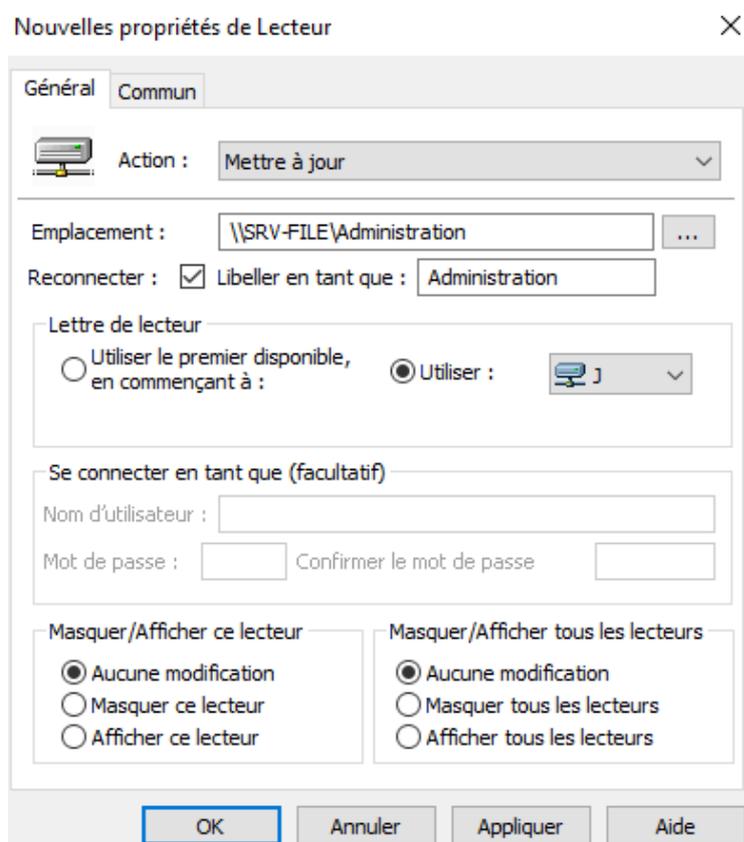
Configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteur



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.



The image shows a Windows dialog box titled "Nouvelles propriétés de Lecteur" (New Network Drive Properties) with a close button (X) in the top right corner. The dialog has two tabs: "Général" (selected) and "Commun".

Under the "Général" tab, there is a section for "Action" with a dropdown menu set to "Mettre à jour". Below this is the "Emplacement" field containing the path "\\SRV-FILE\Administration" and a browse button (...). The "Reconnecter" checkbox is checked, and the "Libeller en tant que" field is set to "Administration".

The "Lettre de lecteur" section has two radio buttons: "Utiliser le premier disponible, en commençant à :" (unselected) and "Utiliser :" (selected). The "Utiliser :" dropdown menu is set to "J".

The "Se connecter en tant que (facultatif)" section has fields for "Nom d'utilisateur :", "Mot de passe :", and "Confirmer le mot de passe".

At the bottom, there are two sections for visibility: "Masquer/Afficher ce lecteur" and "Masquer/Afficher tous les lecteurs". Both sections have three radio buttons: "Aucune modification" (selected), "Masquer ce lecteur" (unselected), and "Afficher ce lecteur" (unselected).

At the bottom of the dialog are four buttons: "OK", "Annuler", "Appliquer", and "Aide".

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.

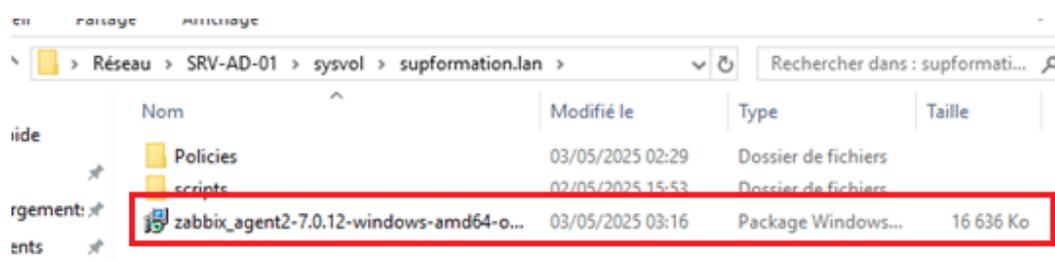
Commencer par télécharger l'agent compatible avec votre environnement (système, architecture, version) depuis le site officiel :

https://www.zabbix.com/download_agents

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		

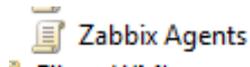
Une fois l'agent Zabbix téléchargé, il faut le placer dans un répertoire accessible à tous les postes du domaine.

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.



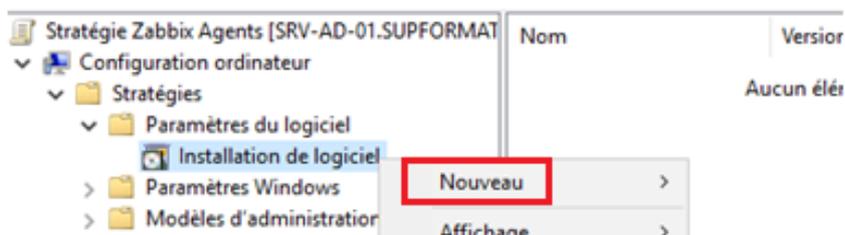
L'agent ayant été déposé, ouvrez le **Gestionnaire de stratégie de groupe**.

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



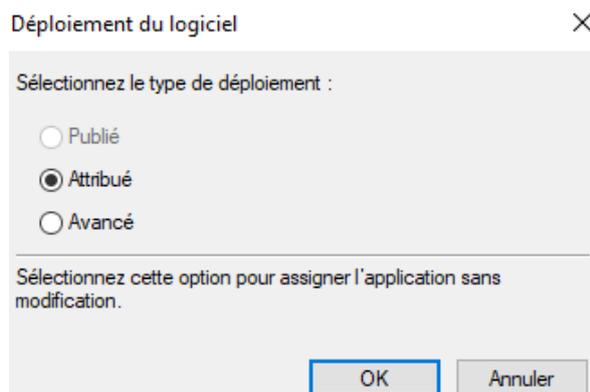
Une fois la GPO créée, cliquez sur **"Modifier"**, puis accédez à : **Configuration de l'ordinateur > Stratégies > Paramètres du logiciel > Installation de logiciel**.

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



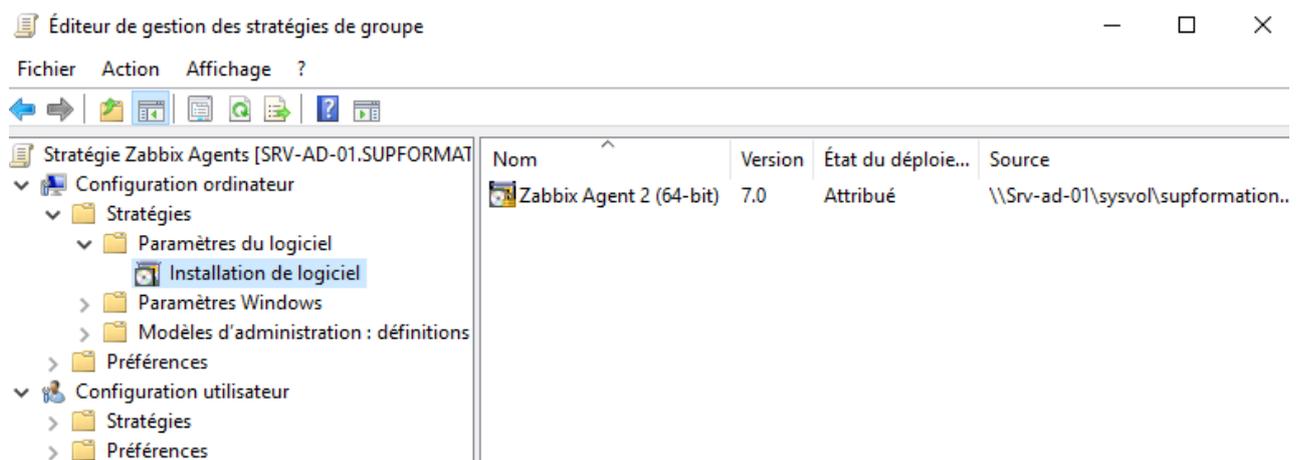
Renseignez ensuite le chemin UNC du répertoire contenant le fichier de l'agent, sélectionnez le fichier MSI, puis cliquez sur "Ouvrir".

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.

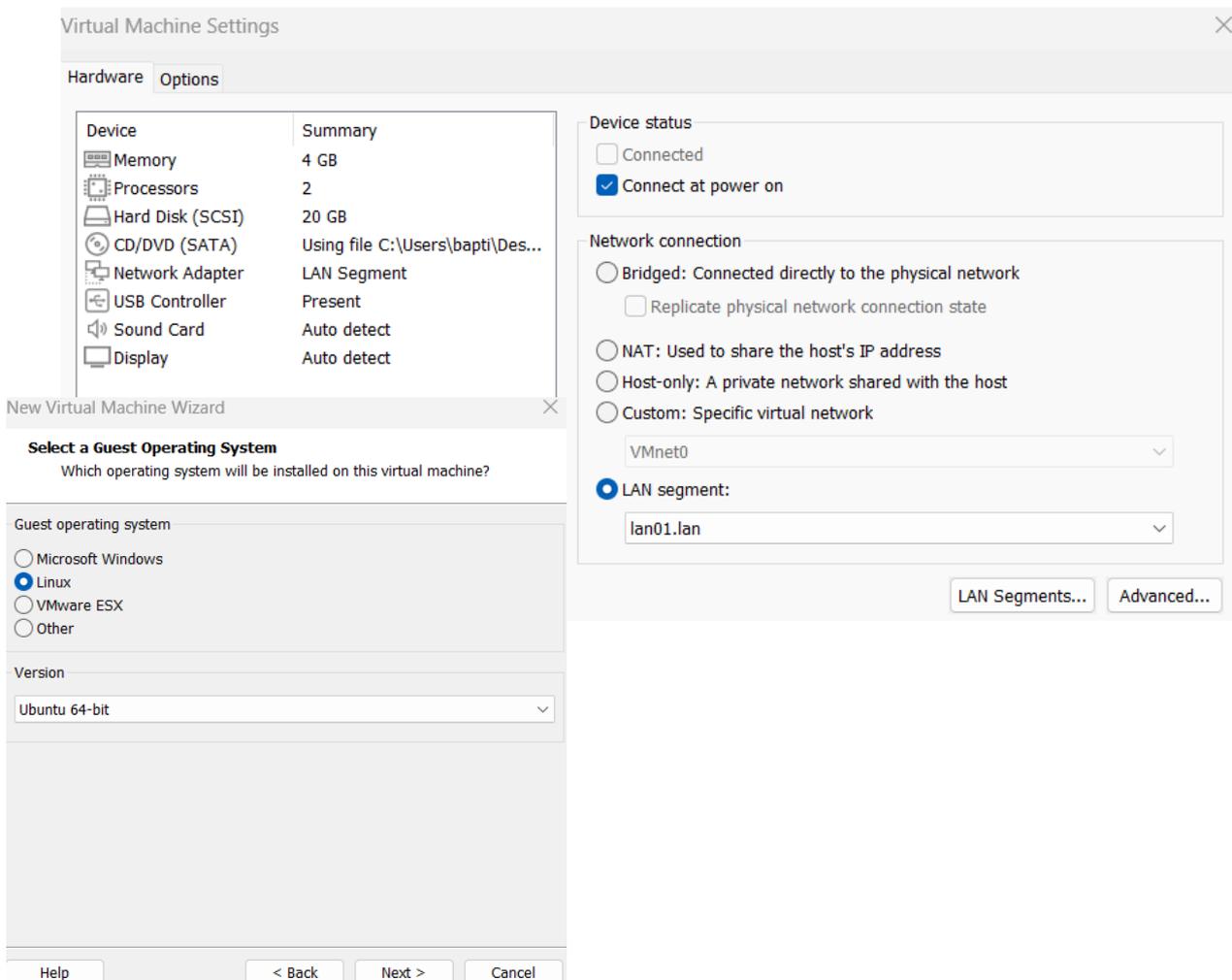


Configuration des serveurs Linux

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.



The image shows two overlapping windows from a virtualization software interface. The background window is 'Virtual Machine Settings' with the 'Options' tab selected. The foreground window is 'New Virtual Machine Wizard'.

Virtual Machine Settings - Options Tab:

Device	Summary
Memory	4 GB
Processors	2
Hard Disk (SCSI)	20 GB
CD/DVD (SATA)	Using file C:\Users\bapti\Des...
Network Adapter	LAN Segment
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Device status:

- Connected
- Connect at power on

Network connection:

- Bridged: Connected directly to the physical network
 - Replicate physical network connection state
- NAT: Used to share the host's IP address
- Host-only: A private network shared with the host
- Custom: Specific virtual network
 - VMnet0
- LAN segment:
 - lan01.lan

Buttons: LAN Segments..., Advanced...

New Virtual Machine Wizard:

Select a Guest Operating System
Which operating system will be installed on this virtual machine?

Guest operating system:

- Microsoft Windows
- Linux
- VMware ESX
- Other

Version:

Ubuntu 64-bit

Buttons: Help, < Back, Next >, Cancel

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**".

```
[ Asturianu ]
[ Bahasa Indonesia ]
[ Català ]
[ Deutsch ]
[ English ]
[ English (UK) ]
[ Español ]
[ Français ]
[ Galego ]
[ Hrvatski ]
[ Latviski ]
[ Lietuviškai ]
[ Magyar ]
[ Nederlands ]
[ Norsk bokmål ]
[ Occitan ]
[ Polski ]
[ Português ]
[ Suomi ]
[ Svenska ]
[ Čeština ]
[ Ελληνικά ]
[ Беларуская ]
[ Русский ]
[ Српски ]
[ Українська ]
```

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.

```
[ Mise à jour vers le nouveau programme d'installation ]
[ Continuer sans mettre à jour ]
[ Retour ]
```

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

```
(X) Ubuntu Server
    The default install contains a curated set of packages that provide a comfortable experience for operating your server.

( ) Ubuntu Server (minimized)
    This version has been customized to have a small runtime footprint in environments where humans are not expected to log in.

Additional options

[ ] Search for third-party drivers

    This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers should not be installed on systems that will be used for FIPS or the real-time kernel.
```

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

```
Configurez au moins une interface pour que ce serveur puisse communiquer avec les autres machines sur le réseau,
préférentiellement un réseau avec accès aux mises à jour.

NAME     TYPE  NOTES
[ ens33  eth   -      ▶ ]
DHCPv4   192.168.100.101/24
00:0c:29:8d:38:e7 / Intel Corporation / 82545EM Gigabit Ethernet Controller (Copper) (PRO/1000 MT Single Port Adapter)

[ Create bond ▶ ]
```

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

```
Si ce système nécessite un proxy pour se connecter à Internet, entrez ses détails ici.

Adresse du proxy : 
If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise,
leave this blank.

The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".
```

- 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 18.225G ▶

[ Terminé ]
[ 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.

```
ssh 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
[ ] mosquito         mosquito✓    Eclipse Mosquitto MQTT broker
[ ] etcd             canonical✓   Resilient key-value store by CoreOS
[ ] powershell      canonical✓   PowerShell for every system!
[ ] sabnzbd          safihre     SABnzbd
[ ] wormhole         snapcrafters 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
[ ] slicli           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) 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%] [#####.....]
```

Patientez...

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_realm]
.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 DNS 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_
gshadow:        files

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
```


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-ld: 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 smb 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 smb 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.

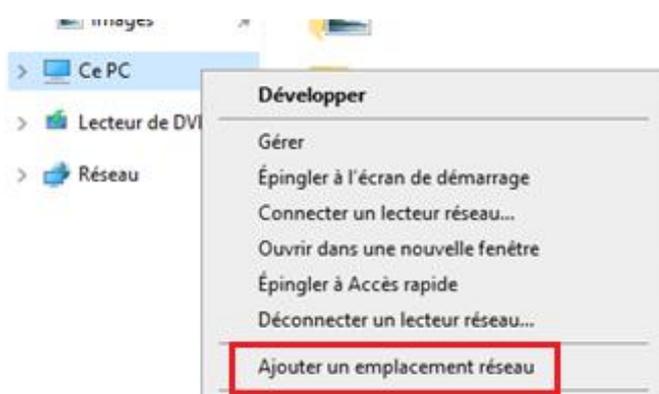
```
# network: {config: disabled}

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 :

[Voir des exemples](#)

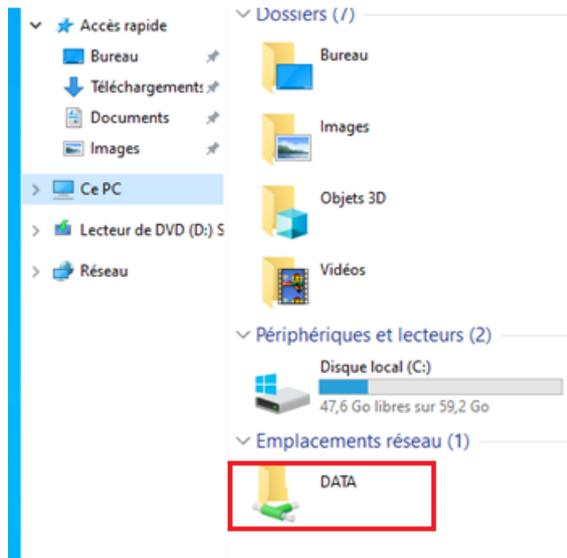
Un nom par défaut sera attribué au raccourci réseau ; vous pouvez le modifier selon votre besoin, puis cliquer sur **Suivant**.

Entrez le nom de cet emplacement réseau :

Entrez le nom de cet emplacement réseau :

L'emplacement réseau sera ajouté avec succès.

Reprenons 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+nmubuntu1) ...
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
```

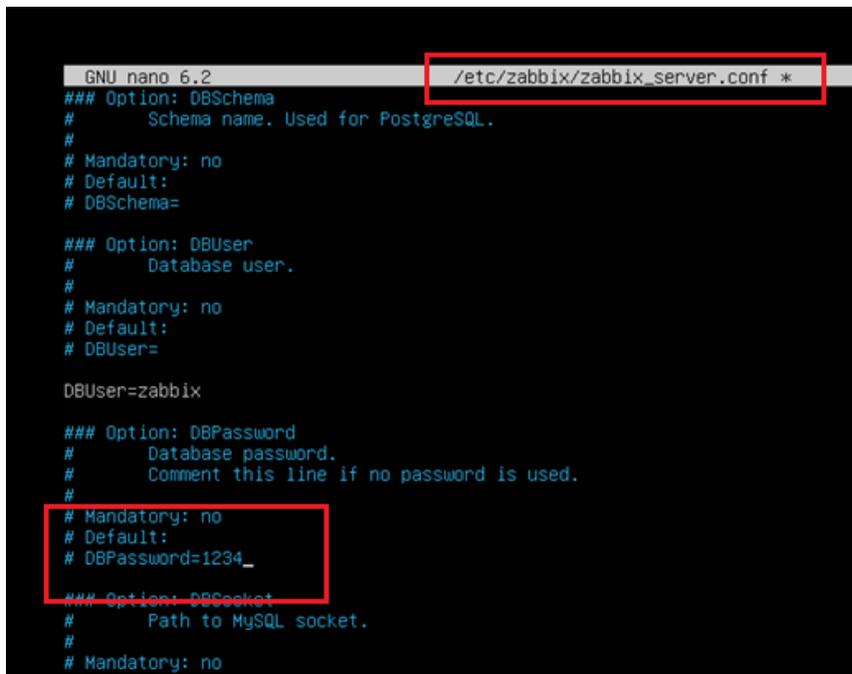
Désactiver l'option `log_bin_trust_function_creators` en se reconnectant à MariaDB avec les droits root et en exécutant la commande suivante.

```
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.

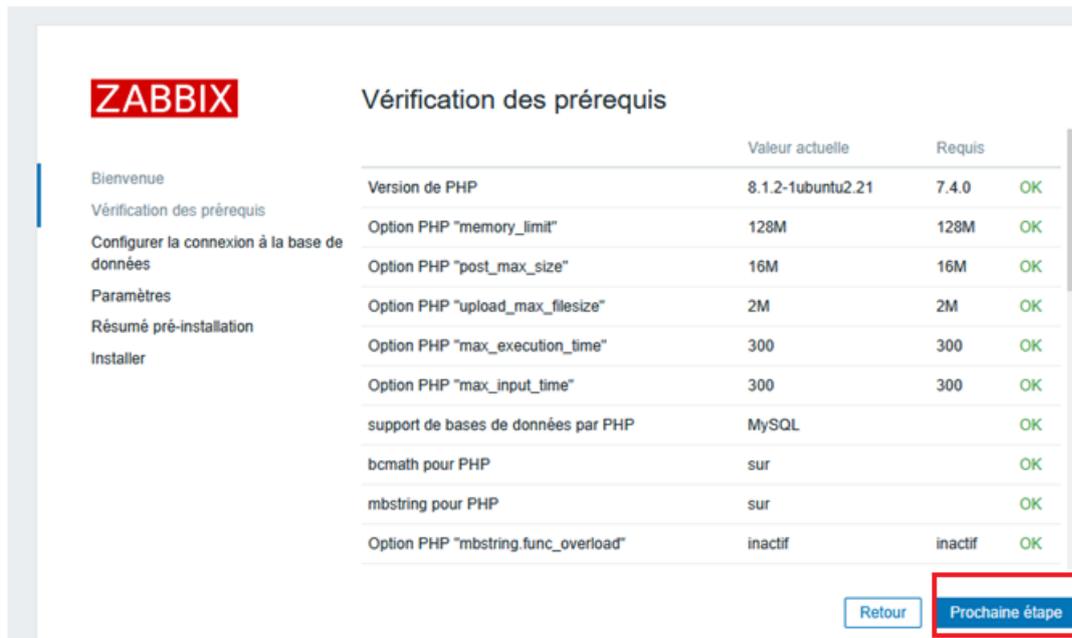
L'URL par défaut est : <http://<adresse-ip-du-serveur>/zabbix>

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**.



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	
Version de PHP	8.1.2-1ubuntu2.21	7.4.0	OK
Option PHP "memory_limit"	128M	128M	OK
Option PHP "post_max_size"	16M	16M	OK
Option PHP "upload_max_filesize"	2M	2M	OK
Option PHP "max_execution_time"	300	300	OK
Option PHP "max_input_time"	300	300	OK
support de bases de données par PHP	MySQL		OK
bcmath pour PHP	sur		OK
mbstring pour PHP	sur		OK
Option PHP "mbstring.func_overload"	inactif	inactif	OK

[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.



ZABBIX

Configurer la connexion à la base de données

Veillez créer la base de données manuellement et configurer les paramètres de connexion. Appuyez sur le bouton "Prochaine étape" quand c'est fait.

Type de base de données:

Hôte base de données:

Port de la base de données: 0 - utiliser le port par défaut

Nom de la base de données:

Stocker les informations d'identification dans: Texte brut Coffre HashiCorp Coffre CyberArk

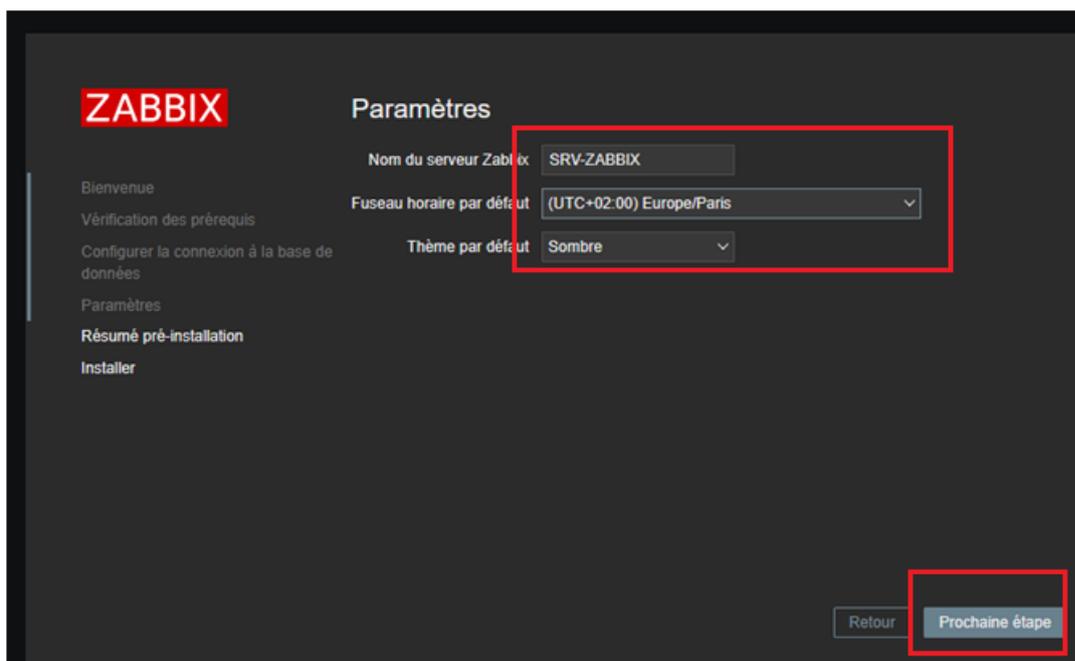
Utilisateur:

Mot de passe:

Chiffrement TLS de la base de données: La connexion ne sera pas chiffrée car elle utilise un fichier socket (sous Linux) ou de la mémoire partagée (Windows).

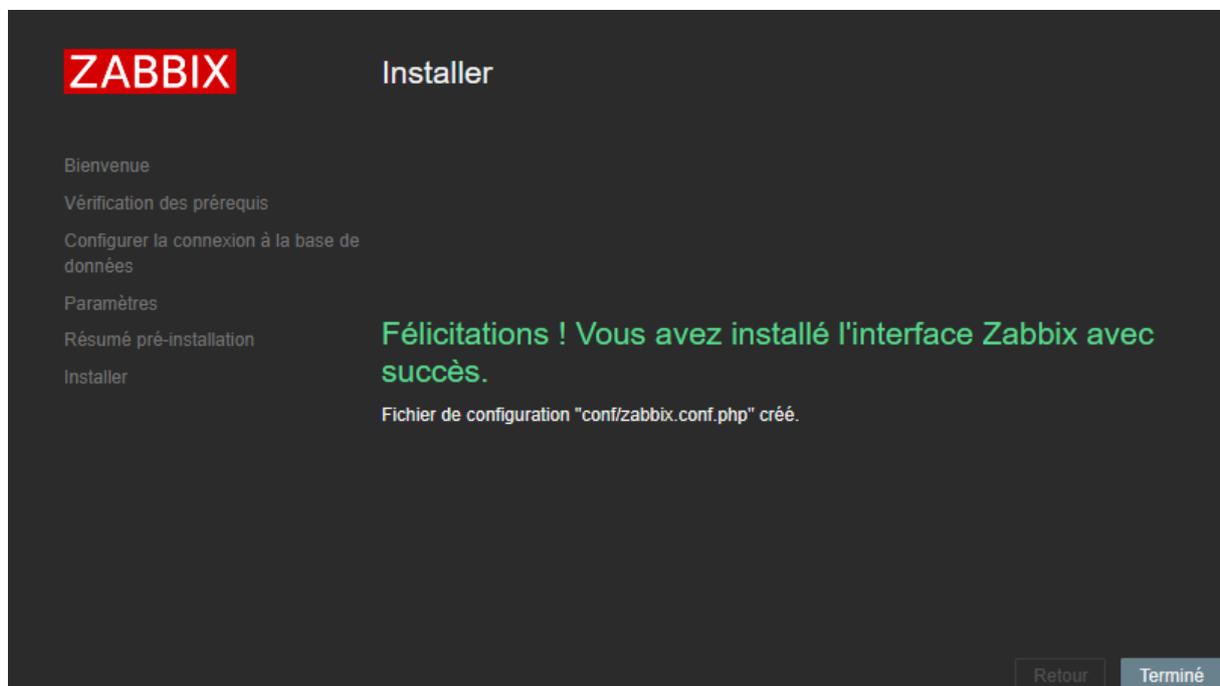
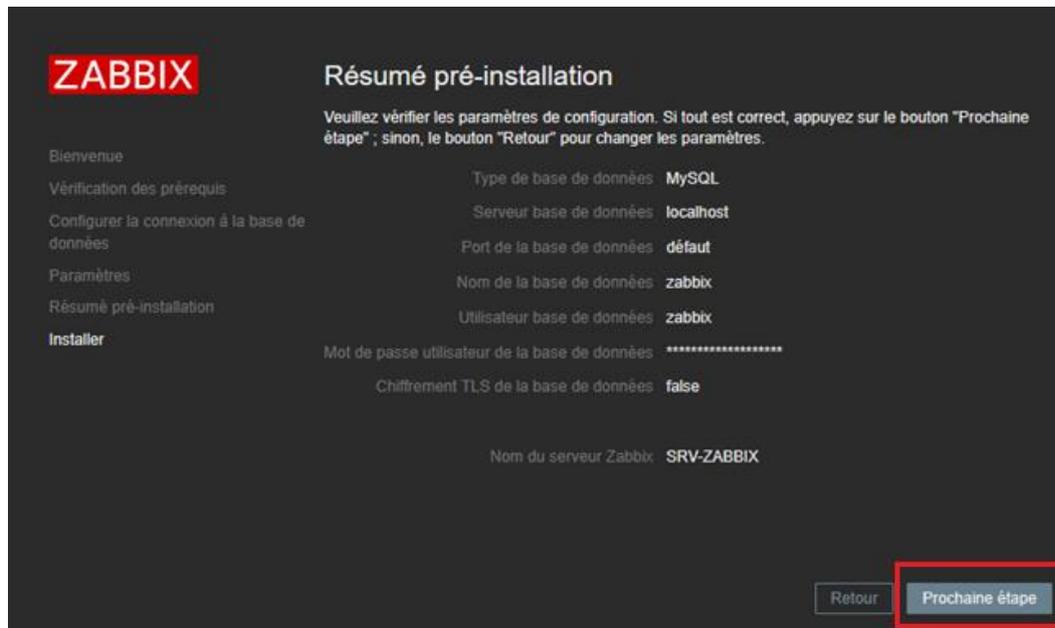
Ci-contre, renseigner les éléments suivants :

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

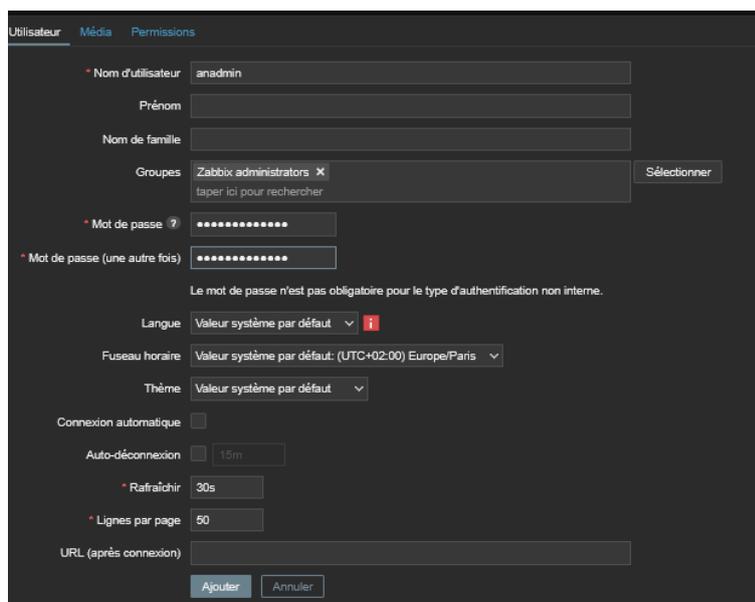


The screenshot shows the Zabbix installation configuration interface. On the left, a sidebar contains the following menu items: **ZABBIX**, Bienvenue, Vérification des prérequis, Configurer la connexion à la base de données, Paramètres, Résumé pré-installation, and Installer. The main area is titled "Paramètres" and contains three configuration fields: "Nom du serveur Zabbix" with the value "SRV-ZABBIX", "Fuseau horaire par défaut" with the value "(UTC+02:00) Europe/Paris", and "Thème par défaut" with the value "Sombre". A red box highlights these three fields. At the bottom right, there are two buttons: "Retour" and "Prochaine étape", with the latter also highlighted by a red box.

Ici, l'avant-dernière étape présente un récapitulatif de la configuration réalisée. Vérifier les informations, puis cliquer sur **Prochaine étape** pour finaliser l'installation."



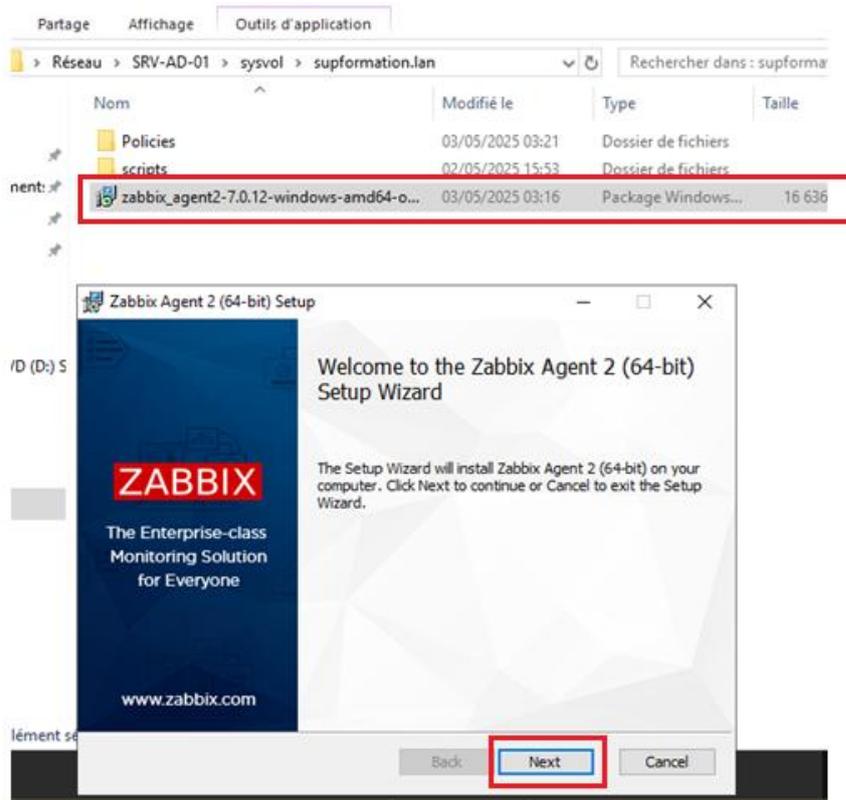
L'une des premières actions à réaliser est la création d'un nouvel utilisateur avec les droits « Administrateurs », en se rendant dans : Utilisateurs > Utilisateurs > Créer un utilisateur. Dans notre cas, l'utilisateur **anadmin** a été créé.

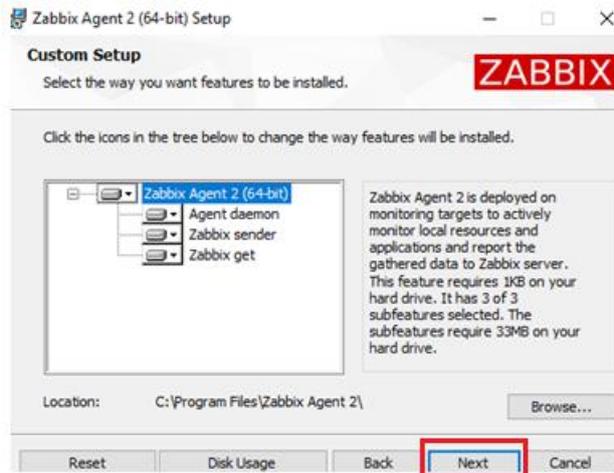


<input type="checkbox"/>	Nom d'utilisateur	Prénom	Nom de famille	Rôle utilisateur	Groupes	Est connecté ?	Connexion	Accès à l'interface	Accès API	Mode debug	État
<input type="checkbox"/>	Admin	Zabbix	Administrator	Super admin role	Internal, Zabbix administrators	Oui (03/05/2025 23:18:13)	Ok	Interne	Activé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

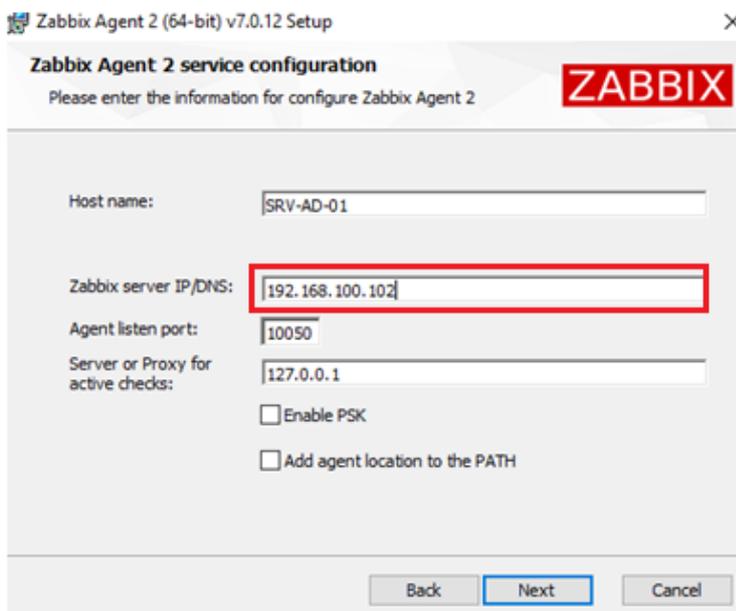
3.2) Configuration des agents dans la console d'administration Zabbix

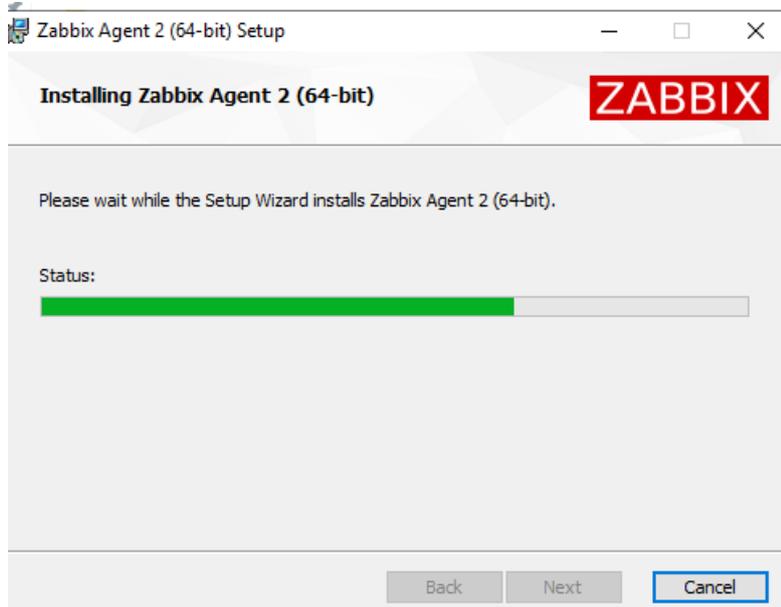
Pour procéder à l'installation de l'agent Zabbix sur les machines à superviser, commencer par récupérer l'installateur précédemment déposé sur le partage réseau.





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=

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
```

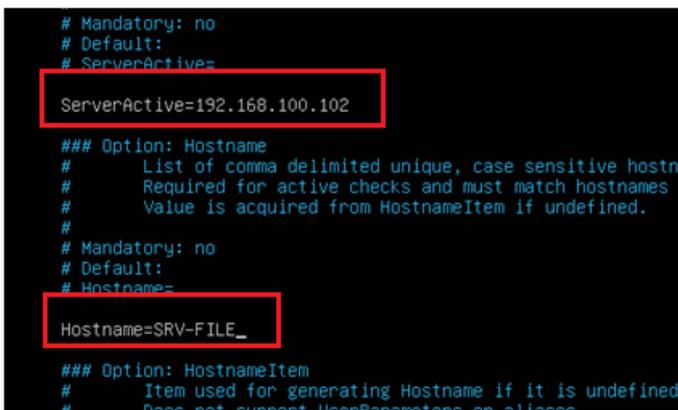
L'agent a bien été installé.

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
```

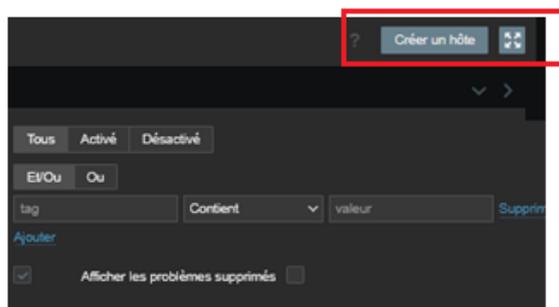
```
anadmin@srv-file:~$ sudo systemctl restart zabbix-agent
anadmin@srv-file:~$ sudo systemctl enable zabbix-agent
Synchronizing state of zabbix-agent.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable zabbix-agent
```

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.



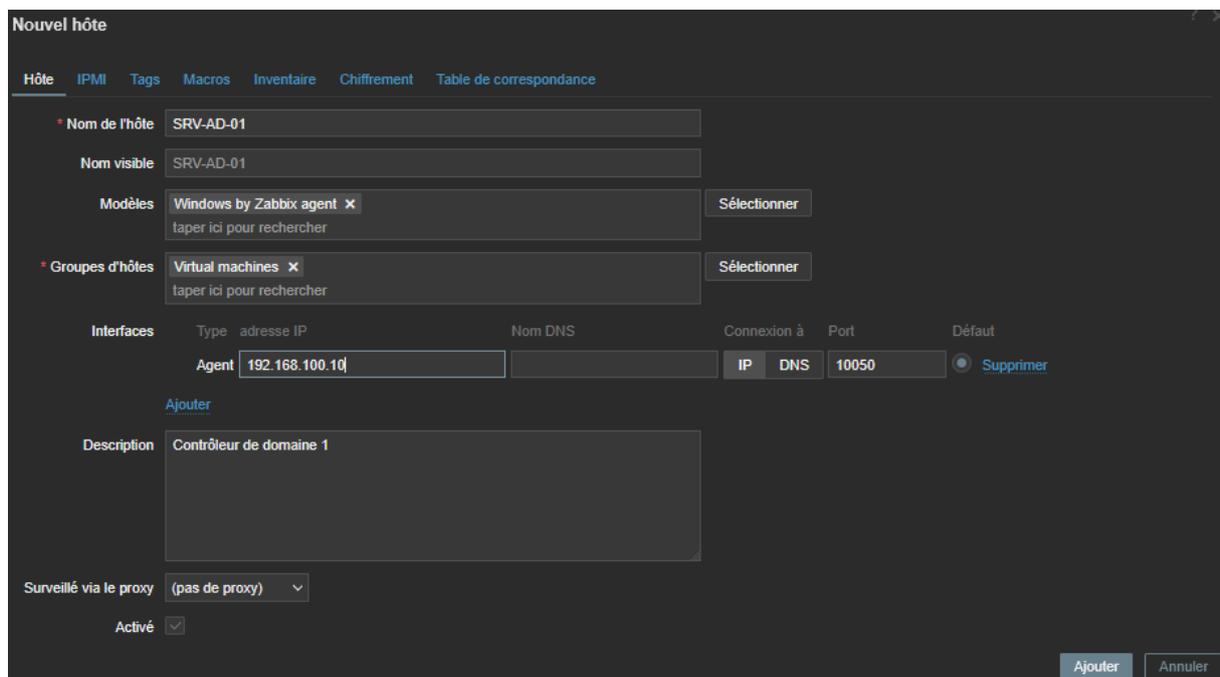
Ici, cliquer sur **"Créer un hôte"** pour ajouter une nouvelle machine à superviser.



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".



The screenshot shows the 'Nouvel hôte' (New host) configuration form in Zabbix. The form is titled 'Nouvel hôte' and has a dark theme. It contains several sections:

- Hôte** (Host):
 - Nom de l'hôte** (Host name): SRV-AD-01
 - Nom visible** (Visible name): SRV-AD-01
 - Modèles** (Templates): Windows by Zabbix agent (selected), with a 'Sélectionner' button and a search prompt.
 - Groupes d'hôtes** (Host groups): Virtual machines (selected), with a 'Sélectionner' button and a search prompt.
- Interfaces** (Interfaces):
 - Table with columns: Type, adresse IP, Nom DNS, Connexion à, Port, Défaut.
 - Row 1: Agent, 192.168.100.10, (empty), IP, DNS, 10050, (radio selected) Supprimer.
- Description** (Description): Contrôleur de domaine 1
- Surveillé via le proxy** (Monitored via proxy): (pas de proxy) (dropdown)
- Activé** (Enabled):

At the bottom right, there are 'Ajouter' (Add) and 'Annuler' (Cancel) buttons.

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 :

