

« We must do what nobody doing for you... »



Sujet : Documentation technique « Mewpipe »

Auteurs : Valentin Duhamel, Clément Delain,
Valentin Lecorps, Samuel Lioult, André Douglas
Djomgoue Katchieu

Date : 26/06/15

Propriétaire : Société 4 Highway

Table des matières

1.	Veille technologique.....	5
A.	Technologies imposées	5
a)	Architecture trois-tiers.....	5
b)	Repository.....	5
B.	Choix technologiques	5
a)	Virtualisation.....	5
b)	RéPLICATION / BACKUP	5
c)	Pare-feux / Firewall.....	6
d)	Téléphonie IP	6
2.	Architecture Réseaux et Systèmes.....	7
A.	Préambule	7
B.	Partie réseau	7
a)	Installation de la première machine PfSense (NYFW1).....	7
b)	Création du cluster PfSense	12
c)	Instanciation du VPN entre New-York et Dallas.....	21
C.	Installation et configuration du Contrôleur de domaine DC1.....	26
a)	Prérequis.....	26
b)	Pré-configuration	26
c)	Ajout et configuration du rôle AD DS.....	29
D.	Installation et configuration de VMWare vCenter	33
a)	Introduction	33
b)	Installation	33
E.	Installation et configuration d'un ESXi	40
a)	Introduction	40
b)	Installation	40
c)	Configuration de l'ESXi.....	40
F.	Création du cluster d'ESXi sur vCenter.....	43
a)	Introduction	43
b)	Création du datacenter	43
c)	Ajout des hôtes au datacenter.....	44
d)	Création et configuration du cluster	46
e)	Activation de la haute disponibilité au niveau du cluster	47
G.	Installation et configuration d'un serveur WEB IIS (NYFE1).....	52
a)	Introduction	52

b)	Création de la machine virtuelle	52
c)	Installation du système d'exploitation.....	57
d)	Installation du rôle IIS	59
e)	Accès à la console d'administration du IIS et test du site web par défaut	65
H.	Installation et configuration d'un serveur WEB Back-End (NYBE1).....	67
I.	Installation et configuration d'un serveur de Base de données (NYBDD1).....	67
J.	Création des machines NYFE2, NYBE2 et NYBDD2 attachées à NYESX2	67
K.	Load-balancing et Fail-Over des serveurs WEB (Front-end).....	67
a)	Création du pool de load-balancing	67
b)	Instanciation du serveur virtuel	69
c)	Vérification.....	70
L.	Clustering des serveurs de l'architecture trois-tiers	72
M.	Déploiement du site Web MEWPIPE.....	84
a)	Installation de MongoDB avec réplication de BDD	84
b)	Installation du serveur node	93
c)	Mise en place du front-end sur nos serveurs NYFE1 et NYFE2	101
N.	Mise en place d'un stockage iSCSI sur un réseau dédié pour les VMs	109
a)	Contexte.....	109
b)	Principe et application	109
c)	Configuration	110
O.	Repository Linux.....	134
a)	Introduction	134
b)	Création du repository Linux.....	134
c)	Installation de Veeam	134
d)	Ajout du repository	139
e)	Ajout du vCenter	145
f)	Création d'un job de sauvegarde	148
P.	Mise en place du système de téléphonie IP	154
a)	Création de la machine virtuelle et installation d'Asterisk	154
b)	Configuration d'Asterisk	155
Q.	Création d'un job de réplication des machines virtuelles	164
R.	Gestion des cas de pannes	169
a)	Introduction	169
b)	Equipements réseaux.....	169
c)	Load-balancing web des routeurs / pare-feux	171

d)	Panne serveur	172
e)	Panne datacenter.....	174

1. Veille technologique

A. Technologies imposées

a) Architecture trois-tiers

Conformément au cahier des charges, l'architecture trois-tiers sera implémentée sur des technologies **Microsoft Windows Server** dans sa version 2012 R2.

Distribution sous licence



b) Repository

La sauvegarde des machines virtuelles doit être assurée sur un repository **Linux**. Le système d'exploitation de ce dernier sera un Debian dans sa version 8.

Distribution OpenSource



B. Choix technologiques

a) Virtualisation

Pour la virtualisation de nos serveurs, notre équipe a choisi les produits **VMWare vSphere**. Notre choix s'est rapidement effectué du fait que VMWare est le leader sur le marché de la virtualisation. De plus, notre ingénieur système a plus de connaissances dans la virtualisation VMWare que dans la virtualisation Microsoft (Hyper-V) qui était notre second choix.

Logiciel sous licence



b) RéPLICATION / Backup

Afin d'assurer la réPLICATION des machines virtuelles, du datacenter de New-York au datacenter de Dallas et pour effectuer les sauvegardes journalières des machines virtuelles sur le repository Linux, notre équipage a retenu la technologie **Veeam**. Veeam est un applicatif souple et facile à prendre en main.

De plus, Veeam réduit la complexité au maximum en s'intégrant directement dans la couche de virtualisation VMWare. Le choix était donc évident, après avoir choisi la technologie VMWare vSphere pour la virtualisation, Veeam s'imposait pour la réPLICATION et le backup des machines virtuelles.

Logiciel sous licence



c) Pare-feux / Firewall

La virtualisation des routeurs étant imposée, nous avons choisi la distribution **PfSense** pour assurer les fonctions de routeurs et de pare-feux. PfSense a l'avantage d'être une distribution souple et consommant peu de ressources tout en assurant un très grand nombre de fonctionnalités. En effet, il permet d'assurer haute disponibilité et confidentialité tout en étant facilement administrable.

Distribution Open source



d) Téléphonie IP

Pour la téléphonie IP, notre équipe a retenu la technologie **Asterisk**. Celui-ci à l'avantage d'être un logiciel OpenSource et donc d'éviter le coût énorme d'une mise en place d'un système PBX. Il utilise des connexions à large bande pour connecter le réseau téléphonique au réseau mondial de la téléphonie traditionnelle. Les appels peuvent encore être émis et reçus de la même manière qu'ils le sont avec un système PBX traditionnel. Ce qui permet ainsi de mutualiser les infrastructures téléphonique et informatique.

Logiciel OpenSource



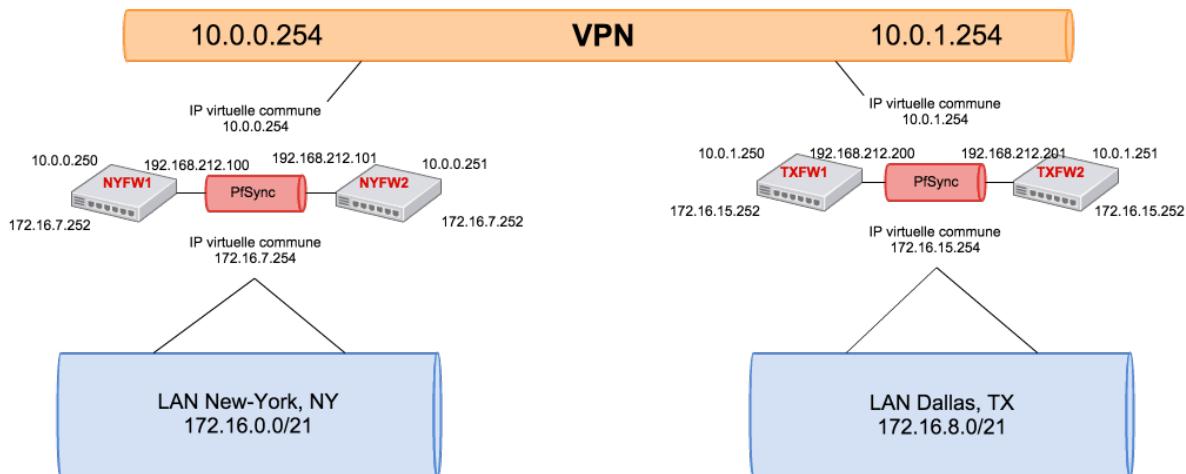
2. Architecture Réseaux et Systèmes

A. Préambule

Il se peut qu'il y ait certains décalages entre les adresses IP renseignées sur le schéma et celles qui vont apparaître sur les screenshots d'installation. Cela est dû au fait, que l'adressage et le plan réseau ont évolué plusieurs fois ce qui crée un décalage entre l'architecture actuelle et celle présente durant la prise des screenshots.

B. Partie réseau

Voici un schéma résumant l'architecture à réaliser pour le projet Mewpipe :



Pour la maquette, nous avons choisi d'utiliser les technologies PfSense pour le routage et toutes les règles de firewall.

Nous allons donc créer 4 machines virtuelles embarquant le système d'exploitation de PfSense pour les utiliser comme routeur/firewall.

Un cluster PfSense sera alors instancié pour chaque datacenter. Un VPN entre les deux clusters PfSense assurera la sécurité des flux transitant entre nos deux datacenters.

a) Installation de la première machine PfSense (NYFW1)

i. Prérequis

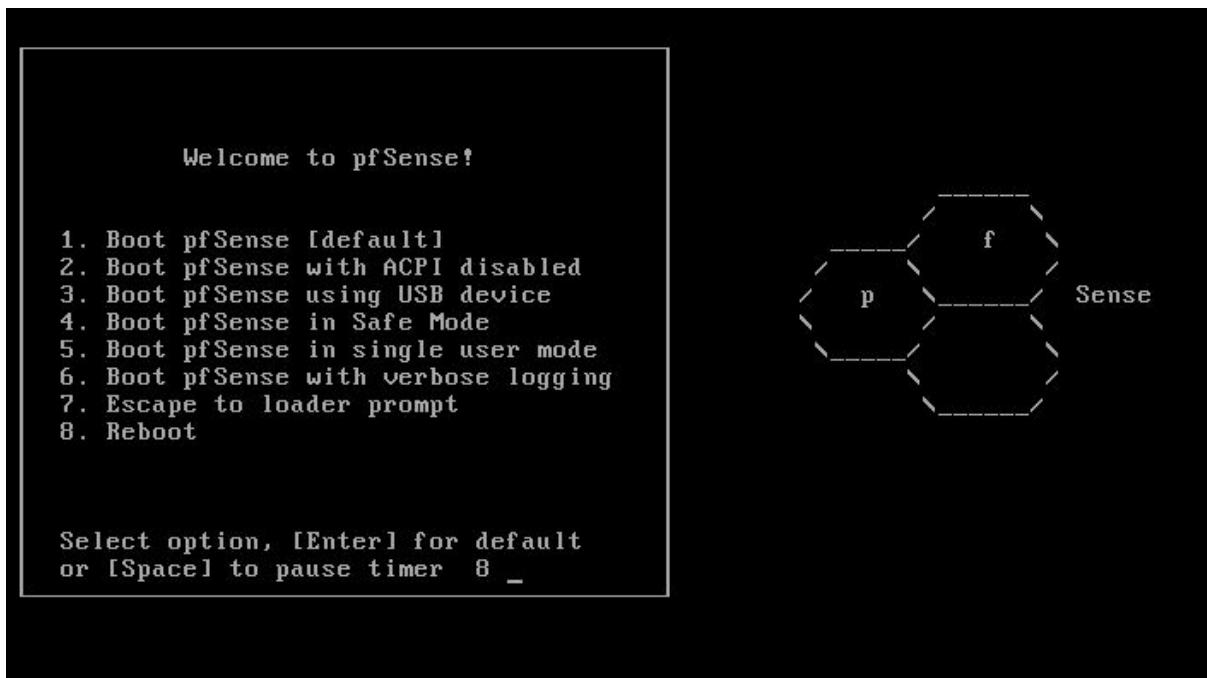
Performance : Ces systèmes d'exploitations n'étant pas gourmands, nous avons opté pour 512Mo de RAM, 1 cœur de processeur et 8Go d'espace disque.

Réseau : 3 cartes réseaux sont nécessaires :

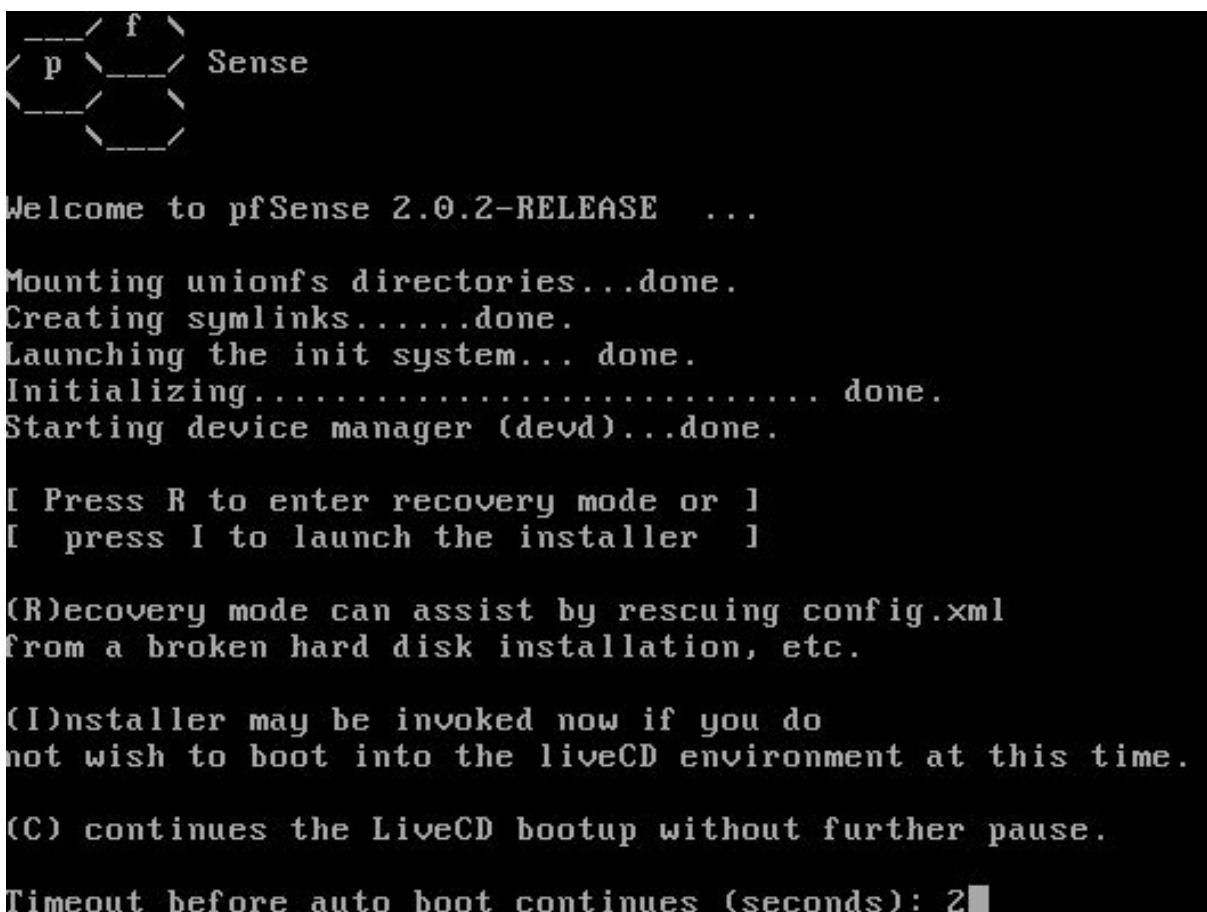
- LAN : 172.16.0.0/21
- WAN : 10.0.0.0/24
- PFSYNC: 192.168.212.0/24 (Pour la liaison PfSync)

ii. Installation du système d'exploitation

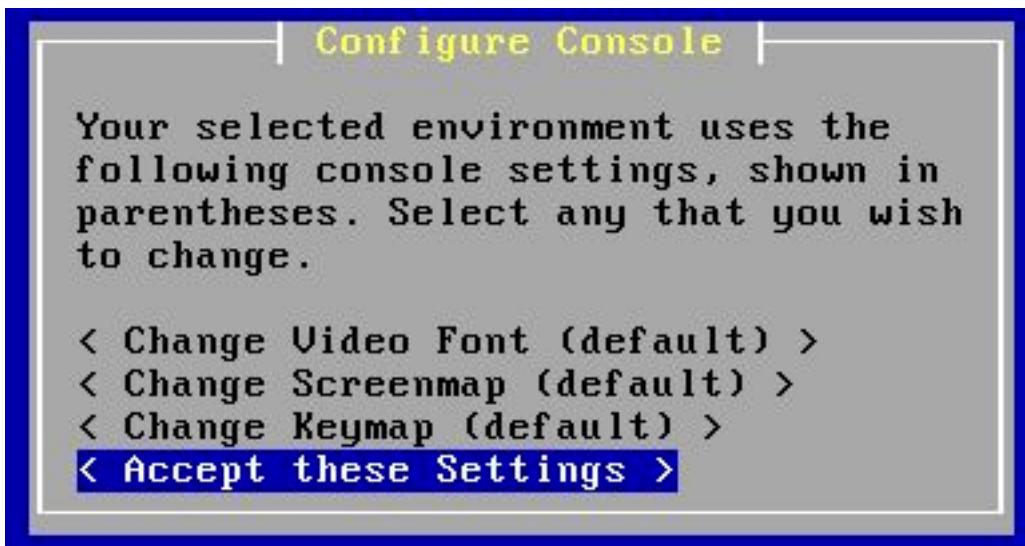
Une fois l'ISO monté, un menu de boot apparaît. Selon les besoins on peut choisir de démarrer PfSense avec certaines options activées. Si aucune touche n'est appuyée, PfSense bootera avec les options par défauts (choix 1) au bout de 8 secondes.



Appuyons sur **Entrée** pour booter avec les options par défaut :



Appuyer rapidement sur la touche “I” afin de démarrer l’installation :



L'installation démarre, dès le premier écran nous pouvons régler différents paramètres notamment la police d'écriture et l'encodage des caractères. Ces options sont utiles pour des cas bien particuliers. Nous n'y toucherons donc pas. On sélectionne **Accept these Settings** :



On choisit **Quick/Easy Install** pour procéder à l'installation rapide.

Le message qui suit, nous informe que le disque dur sera formaté et toutes les données présentes dessus seront effacées. On sélectionne **OK** et on continue.

L'installation débute et copie les fichiers nécessaires sur le disque dur, nous devons par la suite choisir quel type de kernel nous voulons installer, étant sur un ordinateur nous choisissons le **Standard Kernel**.

Une fois l'installation terminée, le système devra rebooter.

iii. Première configuration

Lors du premier démarrage de Pfsense, il faut configurer les différentes interfaces (WAN, LAN, DMZ, etc.). Pfsense nous affiche nos différentes cartes réseaux avec leur adresse MAC, ce qui nous permet de les différencier :

```
Welcome to pfSense 2.0.2-RELEASE ...  
No core dumps found.  
Creating symlinks.....done.  
External config loader 1.0 is now starting... ad0s1b  
Launching the init system... done.  
Initializing..... done.  
Starting device manager (devd)...done.  
Loading configuration.....done.  
  
Network interface mismatch -- Running interface assignment option.  
  
Valid interfaces are:  
em0  08:00:27:f2:97:f0  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4  
em1  08:00:27:1c:11:e3  (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.4  
  
Do you want to set up VLANs first?  
  
If you are not going to use VLANs, or only for optional interfaces, you should  
say no here and use the webConfigurator to configure VLANs later, if required.  
  
Do you want to set up VLANs now [y:n]? █
```

La première étape de configuration concerne l'utilisation des VLANs, pour l'instant ce qui nous importe est la configuration de base de Pfsense, nous appuyons donc sur la touche **N** :

```
If you do not know the names of your interfaces, you may choose to use  
auto-detection. In that case, disconnect all interfaces now before  
hitting 'a' to initiate auto detection.  
  
Enter the WAN interface name or 'a' for auto-detection: █
```

PfSense nous demande alors d'entrer le nom de l'interface WAN, dans notre cas il s'agit d'**em1**.

Il faut ensuite entrer le nom de l'interface LAN, **em0** dans le cas présent.

PfSense nous propose alors d'entrer une interface optionnelle, cela nous importe peu pour l'instant, on appuie alors sur **Entrée** :

```
Enter the Optional 1 interface name or 'a' for auto-detection  
(or nothing if finished): █
```

Un récapitulatif et une demande de confirmation apparaisse alors, on confirme par **Y** :

```
The interfaces will be assigned as follows:  
  
WAN  -> em1  
LAN  -> em0  
  
Do you want to proceed [y:n]? █
```

Une fois la configuration terminée, le menu de la console de Pfsense apparaît. Celui-ci est utile dans le cas de tâches administratives, comme l'oubli du mot de passe de l'interface web. Néanmoins la plupart des options présentes dans ce menu sont également disponibles via l'interface web.

On va alors configurer les adresses IP de notre PfSense pour pouvoir avoir accès à son interface Web, pour cela entrer le choix **2** dans la console :

```
Réduire -> em1
LAN -> em0

Do you want to proceed [y:n]?y

Writing configuration...done.
One moment while we reload the settings... done!
*** Welcome to pfSense 2.2.2-RELEASE-cdrom (amd64) on pfSense ***

WAN (wan)      -> em1      -> v4/DHCP4: 10.19.19.250/22
LAN (lan)      -> em0      -> v4: 172.16.7.152/21
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) pfSense Developer Shell
4) Reset to factory defaults   13) Upgrade 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

99) Install pfSense to a hard drive, etc.

Enter an option: 2
```

Pfsense nous demande quelle interface nous souhaitons configurer, nous commençons par la LAN, option **2** et on entre l'adresse IP :

```
Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.7.252
```

Il faut ensuite entrer le masque de sous-réseau en notation CIDR puis entrer la passerelle par défaut de la LAN :

```
Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.7.252

Subnet Masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 21

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 172.16.7.254
```

Une adresse IPv6 nous est ensuite demandée, nous n'en mettons pas volontairement, ensuite nous choisissons de ne pas activer la fonction serveur DHCP sur le LAN en répondant par **N** :

```

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n

Please wait while the changes are saved to LAN...
  Reloading filter...
  Reloading routing configuration...
  DHCPD...

The IPv4 LAN address has been set to 172.16.7.252/21
You can now access the webConfigurator by opening the following URL in your web
browser:
      http://172.16.7.252/
Press <ENTER> to continue.

```

PfSense nous indique alors que nous avons accès à l'interface Web d'administration à l'adresse IP renseignée pour l'interface LAN :

System Information	
Name	pfSense.localdomain
Version	2.2.2-RELEASE (amd64) built on Mon Apr 13 20:10:22 CDT 2015 FreeBSD 10.1-RELEASE-p9
Platform	cdrom
CPU Type	Intel(R) Core(TM) i7-3740QM CPU @ 2.70GHz Current: 336 MHz, Max: 2693 MHz
Uptime	03 Hours 07 Minutes 34 Seconds

Interfaces	
WAN (DHCP)	1000baseT <full-duplex> 10.0.0.136
LAN	1000baseT <full-duplex> 172.16.7.252
PFSYNC	1000baseT <full-duplex> 10.19.19.247

De la même manière, nous configurons l'interface WAN avec pour adresse IP : 10.0.0.250.

iv. Installation du second PfSense (NYFW2)

On reproduit les étapes précédentes pour le second routeur avec pour adresse IP LAN : 172.16.7.253 et adresse IP WAN : 10.0.0.251

b) Création du cluster PfSense

i. Contexte

La tolérance de panne est un processus visant à assurer une disponibilité constante et continue d'éléments réseaux. Dans le cas présent, le fail-over va nous permettre de faire travailler nos deux PfSense derrière une IP virtuelle unique. Le principe est alors que si l'un des Pfsenses tombe, un autre est présent pour prendre le trafic à sa place et ce de manière invisible pour l'utilisateur car la même IP virtuelle sera toujours utilisée.

ii. Protocole CARP

Le protocole CARP (Common address redundancy protocol) est le protocole utilisé par Pfsense pour la mise en place d'un Fail-over. CARP est un protocole travaillant sur les couches 2 et 3 du modèle OSI. Dans son fonctionnement, on met dans un groupe plusieurs hôtes (groupe de redondance) qui partageront alors une même adresse IP et auront une adresse MAC dite "virtuelle".

Derrière cette adresse IP qui sera virtuelle se cacheront deux ou plusieurs hôtes parmi un maître qui prendra et traitera l'intégralité des requêtes en destination de l'IP virtuelle. Les hôtes du réseaux communiqueront entre eux afin de vérifier que le maître est toujours actif, s'il vient à tomber, l'hôte désigné comme esclave prendra le relais afin d'accueillir et de traiter le trafic en destination de l'adresse IP Virtuelle.

CARP est une alternative sécurisée aux protocoles HSRP ou VRRP car il implémente le SHA1-HMAC lors de ses échanges (appelé advertisement). Ceci bloquant, s'ils sont interceptés par un pirate, leur lecture et leur compréhension qui pourrait révéler des informations importantes sur le réseau.

iii. PfSync

Avec CARP nous avons vu ce qui allait permettre à nos hôtes de se répartir les tâches dans le Fail-Over, Pfsense utilise également le protocole PfSync dans son processus de mise en place du Fail-Over.

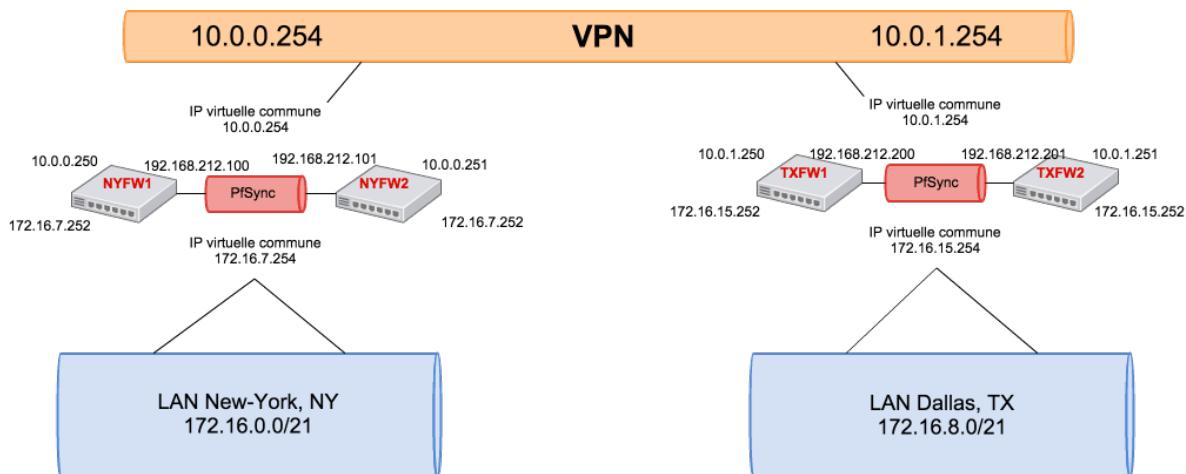
PfSync est un protocole utilisé pour synchroniser plusieurs machines exécutant le firewall Packet Filter, implémenté dans Pfsense.

Plus précisément, c'est par ce protocole que nous allons pouvoir gérer plusieurs hôtes via une seule interface, il fera en sorte par exemple de diffuser les états de connexion (fermée, ouverte, établies,...) entre le routeur maître et les routeurs esclaves permettant ainsi une reprise des états de connexions en cas de panne du maître et de reprise de l'esclave.

PfSync est un des composants essentiels de la mise en place d'une haute disponibilité sous Pfsense.

iv. Configuration

Nous allons donc maintenant passer à la configuration du cluster Pfsense. Pour rappel, nous allons implémenter toute la partie gauche du schéma suivant :

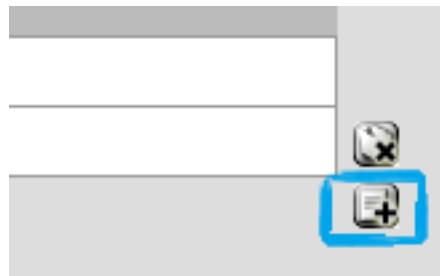


Nous devons commencer par ajouter une interface PfSync à nos Pfsenses. (C'est pour cela que nous avions décidé de dédier deux interfaces pour le WAN).

On se rend donc sur l'interface d'administration de notre Pfsense 1 (NYFW1), il faut alors aller dans **Interfaces** puis **assign** :



On va alors cliquer sur le petit formulaire avec un + qui va nous permettre d'ajouter une interface :

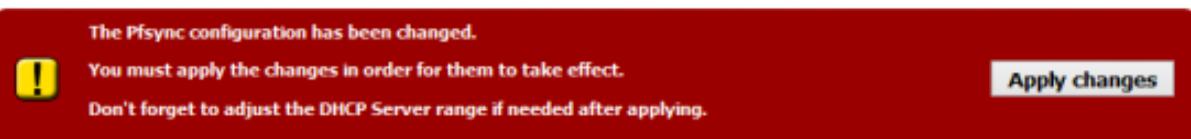


Une fois cette opération effectuée, on pourra voir notre nouvelle interface (nommée "OPT1"), il faudra alors l'assigner à notre interface restante. Une fois la sélection faite, il faut cliquer sur "Save" en bas du tableau.

Nous allons ensuite cliquer sur le nom de notre interface OPT1 pour la configurer. On va commencer par cocher la case **Enable Interface**, puis nous allons saisir le champ **Description**, sélectionner **Static IPv4** dans **IPv4 Configuration Type** et saisir l'IPv4 de notre interface dans la section **Static IPv4 Configuration** :

General configuration	
<input type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable Interface
Description	<input type="text"/> Pfsync Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC address	<input type="text"/> Insert my location This field can be used to modify ("spoof") the MAC address of (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
MTU	<input type="text"/> If you leave this field blank, the adapter's default MTU will be used in all circumstances.
MSS	<input type="text"/> If you enter a value in this field, then MSS clamping for TCP connections (header size) will be in effect.
Speed and duplex	<input type="button"/> Advanced - Show advanced option
Static IPv4 configuration	
IPv4 address	<input type="text"/> 10.0.0.252 / 16
IPv4 Upstream Gateway	<input type="text"/> None - or add a new one . If this interface is an Internet connection, select an existing Gateway. On local LANs the upstream gateway should be "none".

On validera en cliquant sur **Save** en bas de page. Par sécurité, Pfsense nous demande d'appliquer les changements, on cliquera donc sur **Apply changes** :



Cette procédure de création d'adresse est à répéter sur le deuxième Pfsense (NYFW2) en adaptant l'IP bien entendu (10.0.0.253).

Maintenant que nos interfaces dédiées Pfsync sont prêtes, il va falloir les utiliser. On va pour cela aller dans **Firewall** puis dans **Virtual IPs** et enfin sélectionner l'onglet **CARP settings**.

Sur le maître et sur l'esclave, nous cocherons **Synchronize States**. On va ensuite sélectionner **PFSYNC** comme interface de synchronisation (**Synchronize interface**), pour avoir un peu plus de sécurité, nous pourrons renseigner l'IP de l'interface Pfsync de l'hôte d'en face pour éviter les envois en multicast dans **pfsync Synchronize Peer IP**.

Pour le bloc XMLRPC Sync, on va cocher pour les deux hôtes les cases suivantes :

- Synchronize Firewall Schedules
- Synchronize rules
- Synchronize NAT
- Synchronize aliases
- Synchronize load balancer
- Synchronize IPsec
- Synchronize Static Routes
- Synchronize Virtual IPs
- Synchronize traffic shaper(queues)
- Synchronize traffic shaper(limiter)
- Synchronize traffic shaper(layer7)

Cela va permettre au maître d'envoyer les informations de routages, de filtrage et de translation à son esclave afin qu'il les récupère en direct et en état si celui-ci a un dysfonctionnement.

Enfin, uniquement sur le Maître, nous allons renseigner l'IP de l'interface pfsync de l'esclave dans **Synchronize Config to IP** ainsi que le login et mot de passe. Étant donné que c'est le maître qui se synchronise vers l'esclave et non l'inverse, ce dernier paramétrage n'est pas à effectuer sur l'esclave :

System: High Availability Sync

State Synchronization Settings (pfsync)

Synchronize States pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
NOTE: Clicking save will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface If Synchronize States is enabled, it will utilize this interface for communication.
NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best.
NOTE: You must define a IP on each machine participating in this failover group.
NOTE: You must have an IP assigned to the interface on any participating sync nodes.

pfsync Synchronize Peer IP Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP Enter the IP address of the firewall to which the selected configuration sections should be synchronized.
NOTE: XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username Enter the webConfigurator username of the system entered above for synchronizing your configuration.
NOTE: Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System Password Enter the webConfigurator password of the system entered above for synchronizing your configuration.
NOTE: Do not use the Synchronize Config to IP and password option on backup cluster members!

Nous allons maintenant passer à la création de notre IP virtuelle, dans notre cas ce sera 172.16.7.254/21. La configuration n'est à effectuer que sur le maître du cluster qui, via le lien pfsync établi précédemment, va ensuite diffuser la configuration à ses esclaves.

On va aller dans **Firewall** puis dans **Virtual IPs** et on va cliquer sur le petit + à droite du tableau pour créer notre adresse IP virtuelle :

Virtual IP address	Interface	Type	Description

Note:
The virtual IP addresses defined on this page may be used in NAT mappings.
You can check the status of your CARP Virtual IPs and interfaces [here](#).

Ici, nous allons devoir choisir le protocole de synchronisation que nous souhaitons utiliser, **CARP** dans notre cas. Puis l'interface coté interface virtuelle, c'est à dire sur quel réseau va se situer l'IP virtuelle que nous souhaitons affecter au cluster, nous allons partir sur l'IP 172.16.7.254 qui sera donc du coté LAN, on sélectionnera donc **LAN** puis on saisira l'adresse IP virtuelle de notre cluster. On saisira également un mot de passe qui permettra de sécuriser les échanges ainsi qu'un numéro VHID (Virtual Host Identifier). On pourra également spécifier les valeurs de temps de synchronisation :



Firewall: Virtual IP Address: Edit

Edit Virtual IP	
Type	<input type="radio"/> IP Alias <input checked="" type="radio"/> CARP <input type="radio"/> Proxy ARP <input type="radio"/> Other
Interface	LAN
IP Address(es)	Type: <input type="button" value="Single address"/> Address: <input type="text" value="172.16.7.254"/> /21 <small>This must be a CIDR range.</small>
Virtual IP Password	<input type="password" value="*****"/> Enter the VHID group password.
VHID Group	1 <input type="button" value="▼"/> Enter the VHID group that the machines will share
Advertising Frequency	Base: <input type="button" value="1"/> Skew: <input type="button" value="0"/>
Description	<input type="text" value="IP virtuelle cluster LAN"/> You may enter a description here for your reference (not parsed).
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

On oubliera pas de sauvegarder en cliquant sur **Save** et d'appliquer nos modifications avec le bouton **Apply**.

Par défaut, des règles sont mises en place pour bloquer certains trafics, étant donné que les liens PfSync sont des interfaces uniquement dédiées à ce protocole, il ne sert à rien de mettre de filtrage particulier dessus.

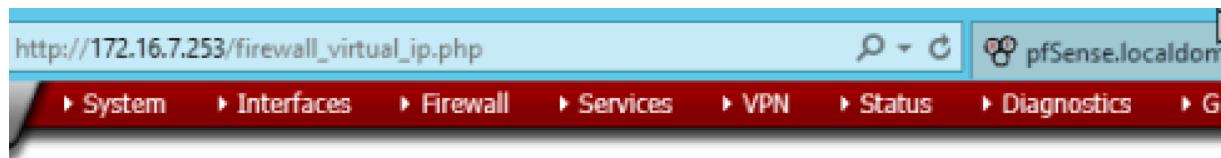
On va donc se rendre dans **Firewall** puis dans **Rules** et on ira sélectionner l'interface **PfSync** sur les deux hôtes :

Floating	WAN	LAN	PFSYNC						
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
No rules are currently defined for this interface									
All incoming connections on this interface will be blocked until you add pass rules.									
Click the button to add a new rule.									

On va ajouter une règle permettant de tout laisser passer, il faudra pour cela simplement s'assurer de sélectionner **Pass** dans le premier champ puis dans le bas du formulaire sélectionner **any** au niveau des ports :

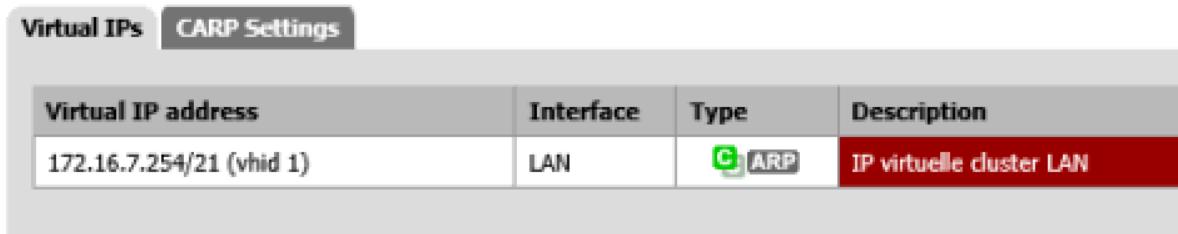
Destination port range	from: <input type="text" value="any"/> <input type="button" value="..."/> to: <input type="text" value="any"/> <input type="button" value="..."/>
Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port	
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	 You may enter a description here for your reference.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Une fois que ces deux règles seront en place, les hôtes vont commencer à échanger sur leurs états et le maître va envoyer la configuration à son esclave. On pourra donc, sur cet esclave, aller voir si les configurations faites sur le maître sont présentes. On va par exemple aller dans **Firewall** puis dans **Virtual IP** pour voir que l'esclave a bien la configuration de l'IP virtuelle que nous avons configurée sur le maître :



The screenshot shows the pfSense web interface. The URL in the address bar is http://172.16.7.253/firewall_virtual_ip.php. The navigation bar at the top includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and General. The Firewall link is currently selected.

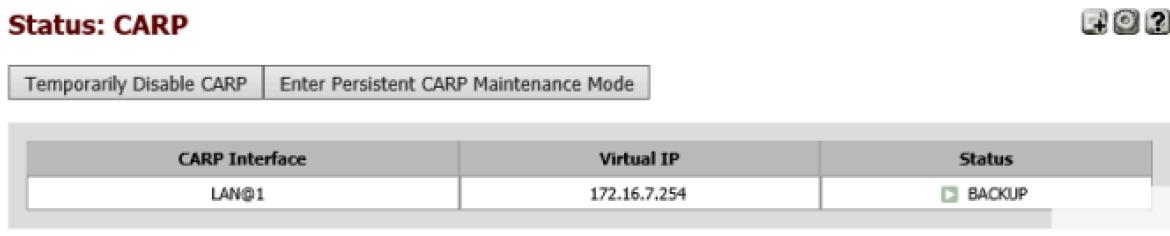
Firewall: Virtual IP Addresses



The screenshot shows the 'Virtual IPs' tab selected in the Firewall settings. A table lists a single virtual IP entry:

Virtual IP address	Interface	Type	Description
172.16.7.254/21 (vhid 1)	LAN	CARP	IP virtuelle cluster LAN

Dans un second temps, on pourra sur le maître et sur l'esclave (aussi appelé **backup** dans pfsense) aller dans **Status** puis dans **CARP (Fail-Over)** pour voir que les rôles sont bien affectés, par exemple l'aperçu que l'on aura sur l'esclave :



The screenshot shows the 'Status: CARP' tab selected. It displays the status of the CARP interface:

CARP Interface	Virtual IP	Status
LAN@1	172.16.7.254	BACKUP

Enfin, nous pouvons faire un test fonctionnel, nous allons pinguer l'IP virtuelle du cluster puis couper le Maître pour voir que l'IP virtuelle répond toujours et que l'esclave a bien pris le relais du cluster :

```
C:\Users\Administrateur>ping 172.16.7.254 -t

Envoi d'une requête 'Ping' à 172.16.7.254 avec 32 octets
Réponse de 172.16.7.254 : octets=32 temps<1ms TTL=64
Délai d'attente de la demande dépassé.
Réponse de 172.16.7.254 : octets=32 temps<1ms TTL=64
Réponse de 172.16.7.254 : octets=32 temps<1ms TTL=64
```

On voit donc la perte d'un paquet ICMP qui correspond au temps que le cluster met à réagir pour réaffecter le rôle de maître à l'esclave qui va alors gérer le trafic en attendant le retour du maître.

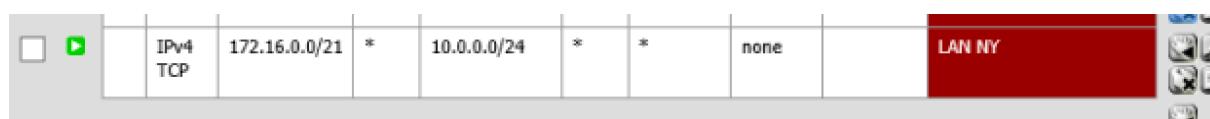
On va faire de même pour attribuer une adresse IP virtuelle partagée dans le réseau WAN :

Firewall: Virtual IP Addresses

VIRTUAL IPs	CARP Settings		
Virtual IP address	Interface	Type	Description
172.16.7.254/21 (vhid 1)	LAN	CARP	IP virtuelle cluster LAN
10.0.0.254/24 (vhid 2)	WAN	CARP	IP virtuelle cluster WAN
Notes:			

Pour que LAN puisse communiquer avec le WAN nous devons créer une règle autorisant les flux.

Pour cela allons dans **Firewall** puis **Rules** enfin on clique sur l'onglet **LAN**. On souhaite autoriser les flux provenant de notre LAN en destination du WAN, ce qui donne :



Et pour le test :

```
C:\Users\Administrateur>ping 10.0.0.254 -t

Envoi d'une requête 'Ping' à 10.0.0.254 avec 32 octets
Réponse de 10.0.0.254 : octets=32 temps<1ms TTL=64
Délai d'attente de la demande dépassé.
Réponse de 10.0.0.254 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.254 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.254 : octets=32 temps<1ms TTL=64
```

Notre datacenter de New-York communique désormais avec le réseau WAN uniquement via l'adresse IP 172.16.7.254 et sort via l'adresse 10.0.0.254.

La prochaine étape consiste à créer ce même cluster pour le datacenter de Texas avec pour réseau LAN 172.16.8.0/21 et pour réseau WAN 10.0.1.0/24.

Nos deux clusters PfSense créés, il va maintenant falloir les faire communiquer ensemble. Cela va se faire via un VPN et c'est l'objectif du prochain point.

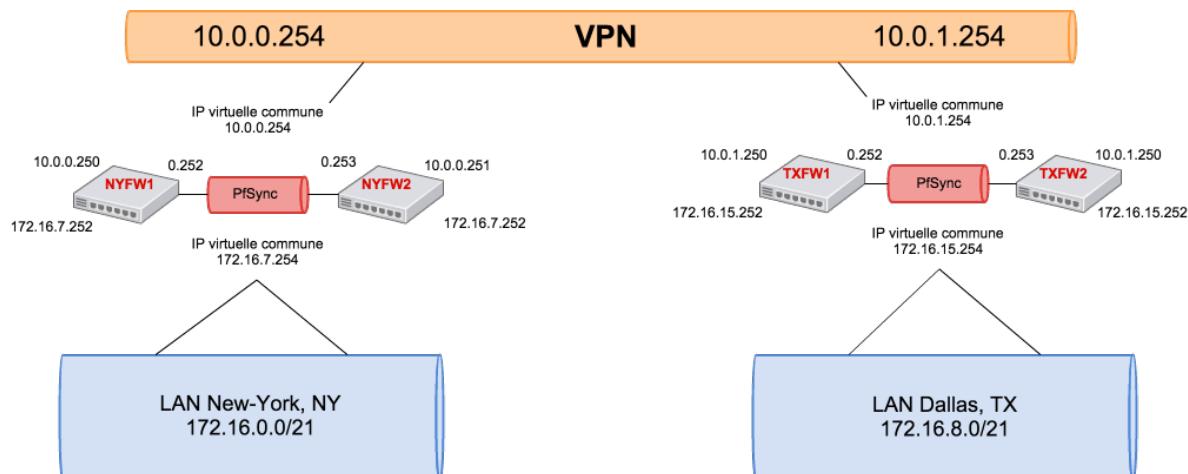
c) Instanciation du VPN entre New-York et Dallas

i. Introduction

Un VPN (Virtual Private Network) va nous permettre de faire communiquer nos deux sites distants, à savoir New-York et Dallas. Le VPN à l'avantage de sécuriser les flux le traversant à l'aide d'un chiffrement.

Nous allons ici utiliser IPSec (Internet Protocol Security) qui est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau. Il se caractérise comme étant un standard ouvert travaillant sur la couche 3 et supportant de nombreux algorithmes de chiffrement et d'authentification.

Pour rappel, le VPN s'établira entre nos deux IPs virtuels WAN de nos clusters PfSense :



ii. Configuration

On commence donc par accéder à l'interface d'administration de notre premier PfSense (NYFW1). On se rend directement dans le menu **VPN** puis dans **IPsec** :



On va commencer par cocher la case **Enable IPsec** qui se situe dans le cadre puis sur **Save**. On va ensuite cliquer sur le + pour ajouter une nouvelle configuration IPsec à ce tableau :

VPN: IPsec



Tunnels Mobile clients Pre-Shared Keys

Enable IPsec

Save

Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
<input type="text"/>				

On commence par remplir l'IP de notre partenaire VPN. Étant sur mon Pfsense 10.0.0.254, je mets l'IP 10.0.1.254. On peut également y mettre une description :

Internet Protocol	IPv4 <input type="button" value="▼"/>	Select the Internet Protocol family from this dropdown.
Interface	WAN <input type="button" value="▼"/>	Select the interface for the local endpoint of this phase1 entry.
Remote gateway	<input type="text"/> 10.0.1.254	Enter the public IP address or host name of the remote gateway
Description	<input type="text"/> VPN TO DALLAS <input type="button" value="x"/>	You may enter a description here for your reference (not parsed).

Voici le reste de la configuration a appliqué :

Phase 1 proposal (Authentication)	
Authentication method	<input type="button" value="Mutual PSK"/> Must match the setting chosen on the remote side.
Negotiation mode	<input type="button" value="Aggressive"/> Aggressive is more flexible, but less secure.
My identifier	<input type="button" value="My IP address"/>
Peer identifier	<input type="button" value="Peer IP address"/>
Pre-Shared Key	<input type="text" value="mewpipevpnaccess"/> Input your Pre-Shared Key string.
Phase 1 proposal (Algorithms)	
Encryption algorithm	<input type="button" value="AES"/> <input type="button" value="256 bits"/>
Hash algorithm	<input type="button" value="SHA1"/> Must match the setting chosen on the remote side.
DH key group	<input type="button" value="2 (1024 bit)"/> Must match the setting chosen on the remote side.
Lifetime	<input type="text" value="28800"/> seconds
Advanced Options	
Disable Rekey	<input type="checkbox"/> Whether a connection should be renegotiated when it is about to expire.
Responder Only	<input type="checkbox"/> Enable this option to never initiate this connection from this side, only receive connections.
NAT Traversal	<input type="button" value="Auto"/> Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP) with clients that are behind restrictive firewalls.
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD <input type="text" value="10"/> seconds Delay between requesting peer acknowledgement.
	<input type="text" value="5"/> retries Number of consecutive failures allowed before disconnect.
<input type="button" value="Save"/>	

Nous avons juste passé le mode de négociation en **Aggressive** et entré la **Pre-Shared Key**.

On fini par cliquer sur **Save** puis sur **Apply changes** sur la page suivante. On va alors cliquer sur le + présent en dessous de la première ligne du tableau qui se situe sur la page :

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description
V1	WAN 10.0.1.254	aggressive	AES (256 bits)	SHA1	VPN TO DALLAS
+ - Show 0 Phase-2 entries					

On arrive sur une nouvelle page de configuration sur laquelle nous allons remplir le champ **Remote Network** dans lequel nous allons mettre la plage IP du LAN distant :

Disabled		<input type="checkbox"/> Disable this phase2 entry Set this option to disable this phase2 entry without removing it from the list.
Mode	Tunnel IPv4	
Local Network	Type:	LAN subnet
	Address:	/ 128
	In case you need NAT/BINAT on this network specify the address to be translated	
	Type:	None
	Address:	/ 0
Remote Network	Type:	Network
	Address:	172.16.8.0 / 21
Description	LAN DALLAS	
	You may enter a description here for your reference (not parsed).	

On clique sur **Save** puis sur **Apply changes** sur la page suivante. Si on redéveloppe le tableau principal avec le +, nous aurons quelque chose qui ressemble à cela :

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description												
V1	WAN 10.0.1.254	aggressive	AES (256 bits)	SHA1	VPN TO DALLAS												
<table border="1"> <tr> <th>Mode</th> <th>Local Subnet</th> <th>Remote Subnet</th> <th>P2 Protocol</th> <th>P2 Transforms</th> <th>P2 Auth Methods</th> </tr> <tr> <td>tunnel</td> <td>LAN</td> <td>172.16.8.0/21</td> <td>ESP</td> <td>AES (auto)</td> <td>SHA1</td> </tr> </table>						Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	tunnel	LAN	172.16.8.0/21	ESP	AES (auto)	SHA1
Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods												
tunnel	LAN	172.16.8.0/21	ESP	AES (auto)	SHA1												

Nous avons donc un résumé de notre configuration VPN. Il faut maintenant effectuer exactement la même configuration du coté de notre deuxième Pfsense en adaptant bien entendu les IP et les plages IP précisées et ne cochant la case “Enable Pfsense” **uniquement après avoir saisi les configurations**.

Sur nos deux routeurs, on va alors aller dans **Firewall** puis **rules** pour aller dans l’onglet **IPsec** et cliquer sur le + à droite du tableau pour ajouter une règle qui va autoriser tous les flux à arriver depuis l’interface :

[Edit Firewall rule](#)

Action	<input type="button" value="Pass"/> <input type="button" value="Block"/> <input type="button" value="Reject"/> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="IPsec"/> <input type="button" value="Ethernet"/> <input type="button" value="Loopback"/> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<input type="button" value="IPv4"/> <input type="button" value="IPv6"/> Select the Internet Protocol version this rule applies to
Protocol	<input type="button" value="TCP"/> <input type="button" value="UDP"/> <input type="button" value="ICMP"/> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify TCP here.</p>
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="button" value="any"/> / <input type="button" value="Custom"/> Address: <input type="text" value="192.168.1.100"/> / <input type="button" value="Custom"/> <input type="button" value="Advanced"/> - Show source port range
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <input type="button" value="any"/> / <input type="button" value="Custom"/> Address: <input type="text" value="192.168.1.100"/> / <input type="button" value="Custom"/>
Destination port range	from: <input type="button" value="any"/> / <input type="button" value="Custom"/> to: <input type="button" value="any"/> / <input type="button" value="Custom"/> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	 <input type="text" value="VPN"/> You may enter a description here for your reference.
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Une fois ces deux configurations faites, on peut attendre une bonne minute que les pare-feux négocient la construction du VPN.

C. Installation et configuration du Contrôleur de domaine DC1

a) Prérequis

Nous avons choisi les technologies Microsoft pour déployer notre contrôleur de domaine. Le système d'exploitation Windows Server 2012 R2 – DataCenter est ainsi utilisé. Ce step-by-step part du principe que le système d'exploitation est déjà installé et prêt à être utilisé.

b) Pré-configuration

Avant de se lancer dans la configuration de notre contrôleur de domaine, nous allons d'abord changer son hostname et lui adresser une adresse IP fixe sur le réseau dédié aux serveurs.

i. Changement du Hostname

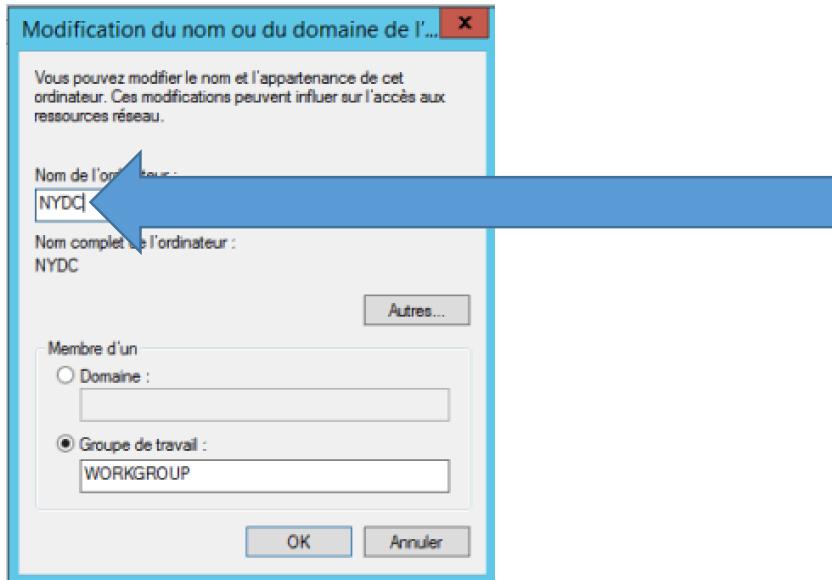
Pour cela, cliquer sur **Configurer ce serveur local** dans la console de Gestionnaire de serveur :



Cliquer ensuite sur le nom de l'ordinateur :



Cliquer sur **Modifier...** et changer le nom du serveur, dans notre cas il s'appelle NYDC :



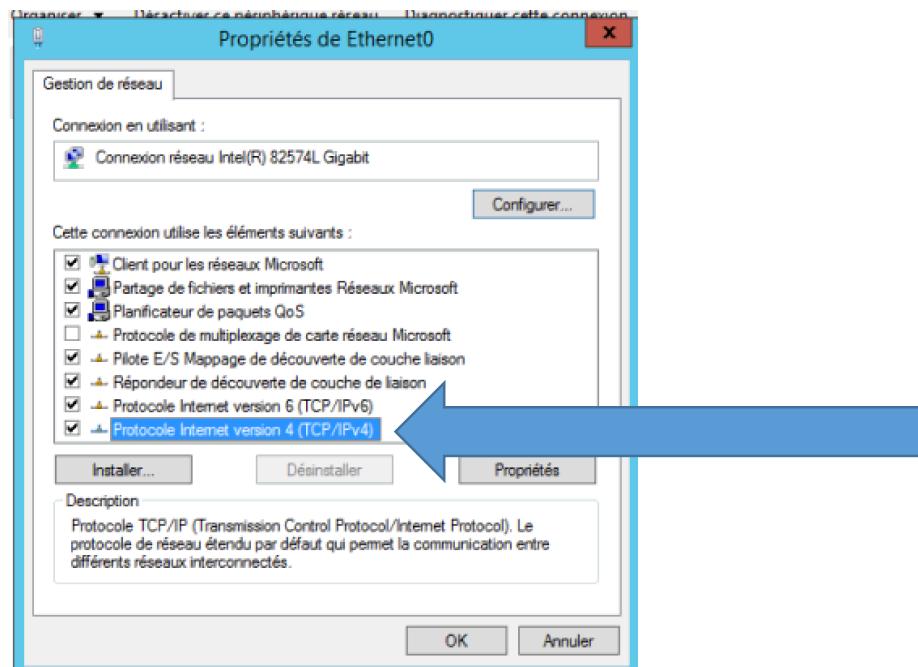
Enfin, cliquer sur **OK**, un message apparaît vous signalant que vous devez redémarrer le serveur pour que les changements soient pris en compte, valider et cliquer sur **Redémarrer maintenant**

ii. Changement de l'adresse IP

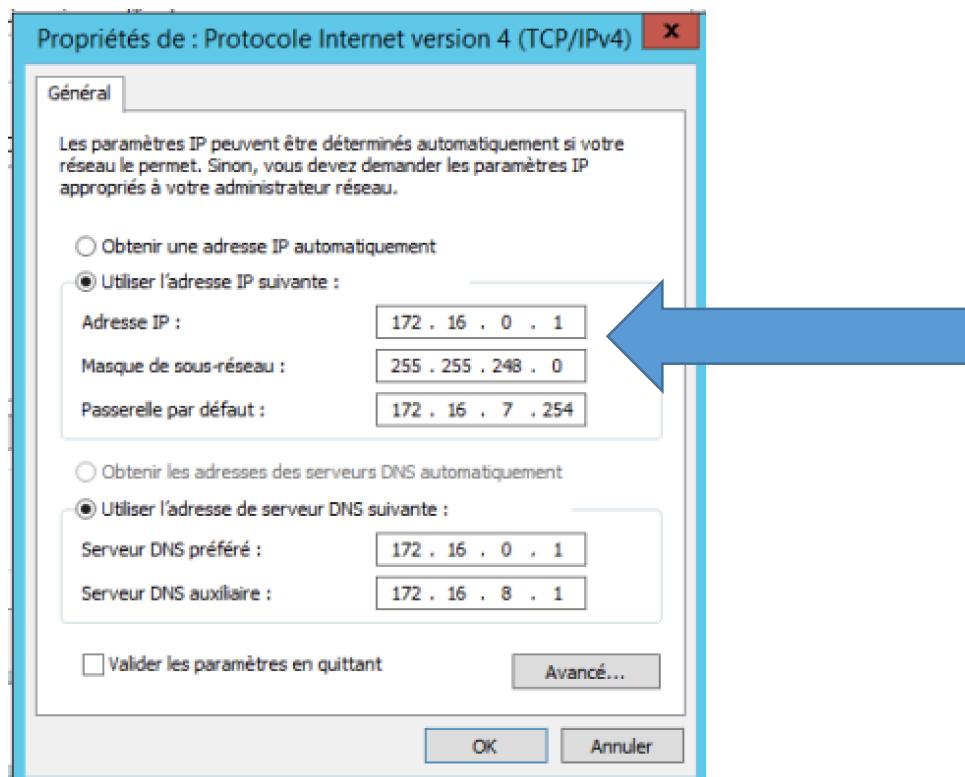
Tous serveur doit posséder une adresse IP fixe afin d'être continuellement joignable. Pour cela, cliquer sur **Configurer ce serveur local** dans la console de Gestionnaire de serveur, puis sur **Adresse IPv4...** :



Effectuer un clic-droit sur votre carte réseau, puis cliquer sur **Propriétés**, pour enfin double-cliquer sur **Protocole Internet version 4** :



Renseigner alors les informations adéquates :



Enfin, si tout est correctement configuré, on obtient ceci :



c) Ajout et configuration du rôle AD DS

Dans le gestionnaire de serveur, cliquer sur **Ajouter des rôles et des fonctionnalités** :

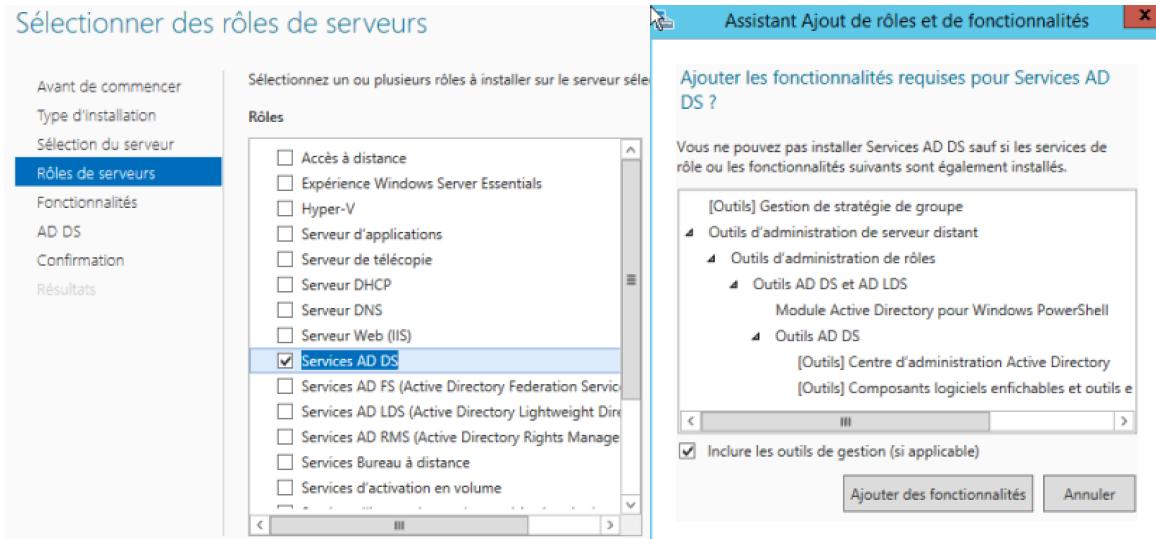
1 Configurer ce serveur local

2 Ajouter des rôles et des fonctionnalités

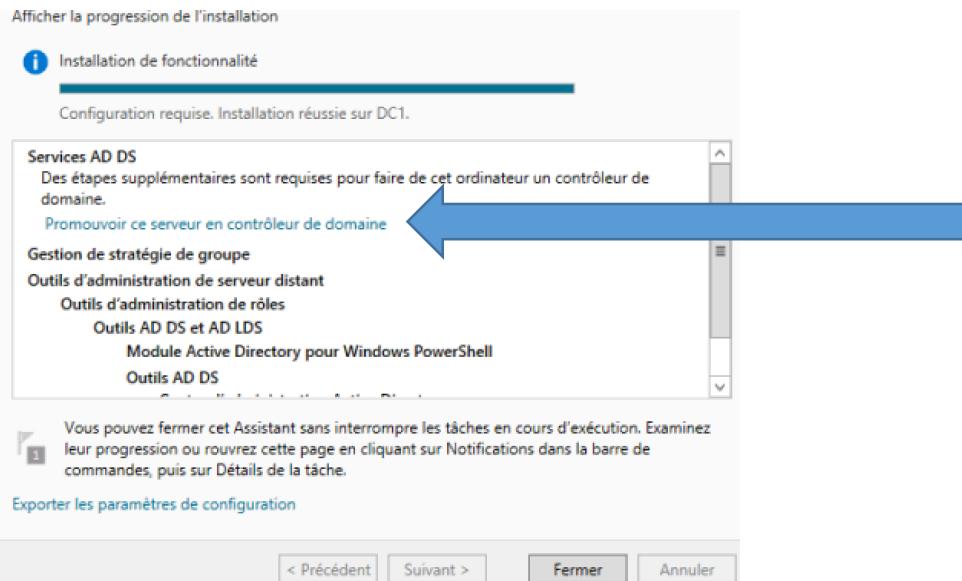
3 Ajouter d'autres serveurs à gérer

4 Créer un groupe de serveurs

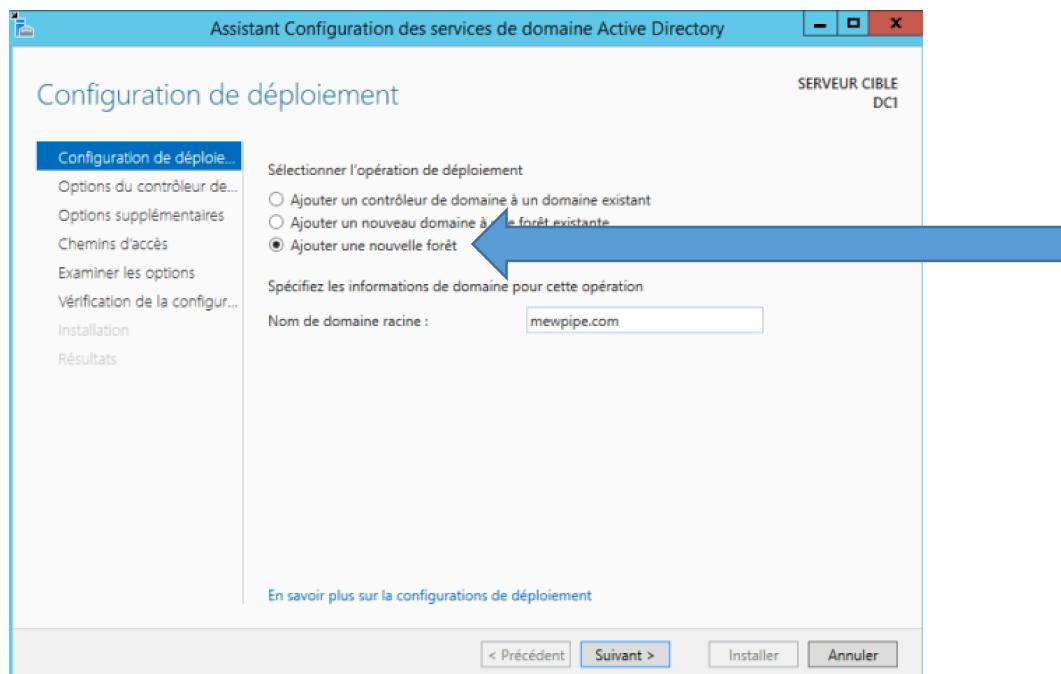
Cliquer sur **Suivant** jusqu'à la sélection de rôles. Ici, cocher la case AD DS (Active Directory Domain Services), l'assistant nous propose alors d'ajouter les fonctionnalités correspondantes, cliquer sur **OK** :



Enfin cliquer sur **Suivant**, puis sur **Installer**. L'assistant installe alors le rôle AD DS sur votre serveur. Une fois que l'installation est complète, cliquer sur **Promouvoir ce serveur en contrôleur de domaine** :

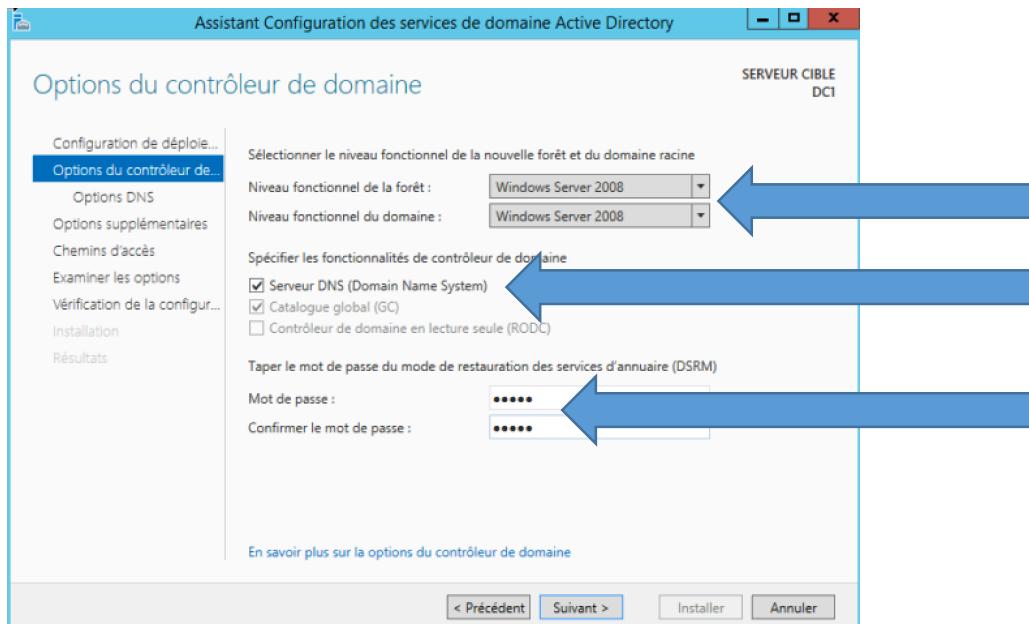


Une nouvelle fenêtre apparaît. Sélectionner la case **Ajouter une nouvelle forêt**, et entrer le nom de votre forêt (nom de domaine racine) :



Cliquer alors sur **Suivant**. Il faut ensuite sélectionner le niveau fonctionnel de la forêt, en laissant Windows Server 2012, vous ne pourrez pas faire fonctionner de serveur Windows Server 2008 dessus. Pour avoir plus de marge, nous choisissons de mettre Windows Server 2008 pour le niveau fonctionnel de la forêt.

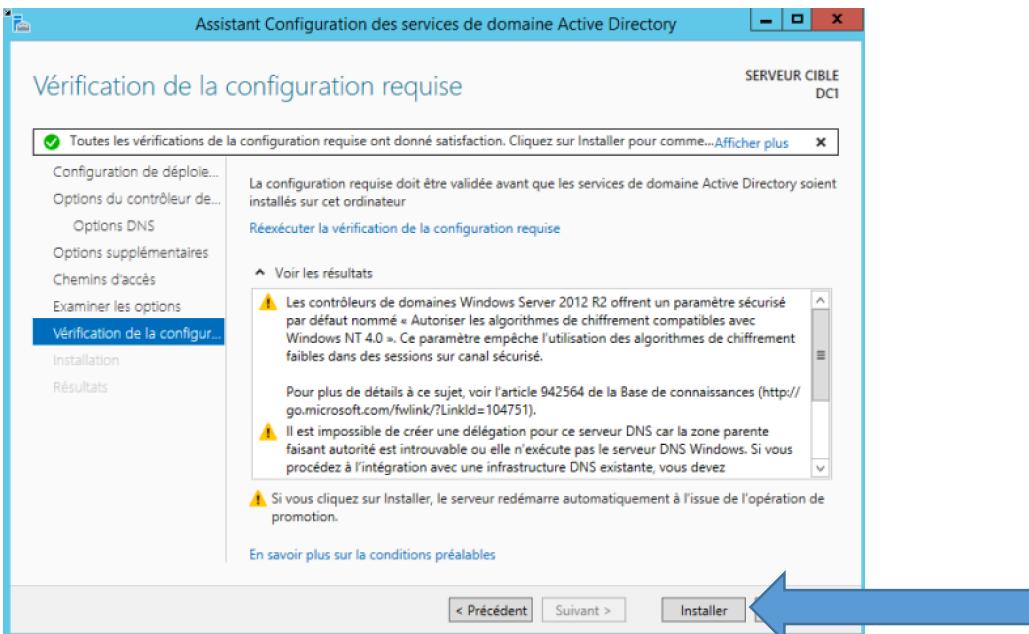
Laisser également la case Serveur DNS cochée puisqu'il faut que notre contrôleur de domaine fasse aussi serveur DNS, enfin, renseigner un mot de passe et cliquer sur **Suivant** :



L'avertissement est tout à fait normal étant donné que nous n'avons pas encore de zone parente, cliquer alors sur **Suivant**. Il vous faut alors confirmer le nom NetBios de votre machine. Cliquer sur **Suivant**.

Vient alors le choix des chemins d'accès, laisser les valeurs par défaut et cliquer sur **Suivant**.

Un récapitulatif de notre installation apparaît, si tout est OK, cliquer sur **Suivant**. L'assistant va alors vérifier la configuration. Si cette dernière est validée, cliquer sur **Installer** :



Le serveur doit alors redémarrer...

Suite au redémarrage, on s'aperçoit que notre serveur est désormais dans le domaine que nous venons de configurer :



Dans le gestionnaire de serveur, on remarque que nous ne sommes plus dans le domaine WORKGROUP mais dans notre domaine et que 2 nouveaux services sont venus se greffés :

 A screenshot of the Windows Server Manager interface. On the left, a navigation pane lists "Tableau de bord", "Serveur local" (which is selected and highlighted in blue), "Tous les serveurs", "AD DS", "DNS", and "Services de fichiers et d...". A large blue arrow points from the left towards the "Serveur local" item. On the right, a "PROPRIÉTÉS" (Properties) window is open for the server "Pour NYDC". It displays the following information:

Nom de l'ordinateur	NYDC
Domaine	mewpipe.com
Pare-feu Windows	Public : Inactif
Gestion à distance	Activé
Bureau à distance	Désactivé
Association de cartes réseau	Désactivé
Ethernet0	172.16.0.1, Compatible IPv6

 A second blue arrow points from the right side of the "Domaine" row towards the "mewpipe.com" value.

D. Installation et configuration de VMWare vCenter

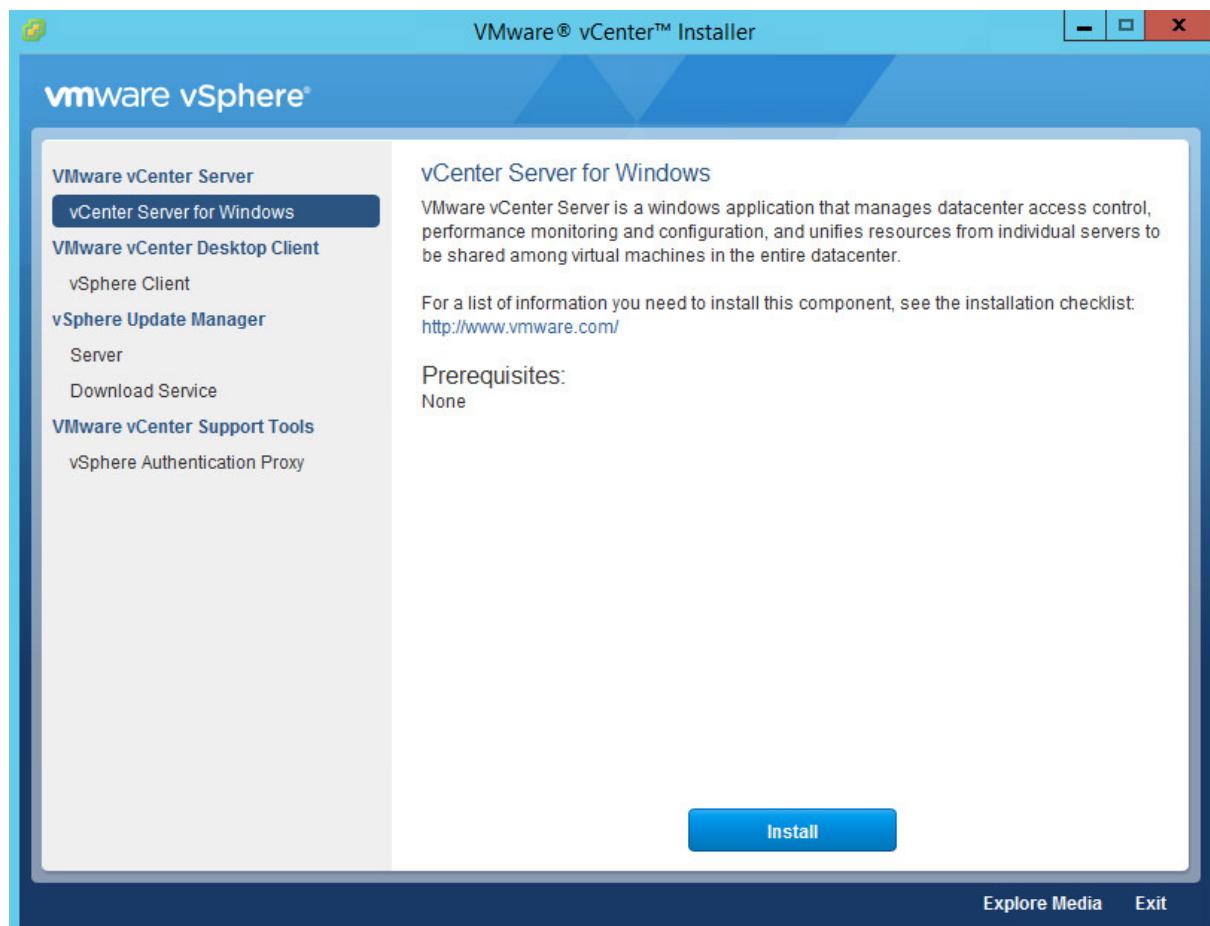
a) Introduction

Dans cette partie, nous allons installer et configurer VMWare vCenter sur une machine Windows Server 2012 R2 Datacenter. La machine est préconfigurée :

- Elle possède une IP fixe,
- elle est intégrée au domaine **mewpipe.com**,
- son hostname a été changé,
- le composant **Fonctionnalités de .NET Framework 3.5** a été ajouté,
- les mises à jours importantes ont été effectué.

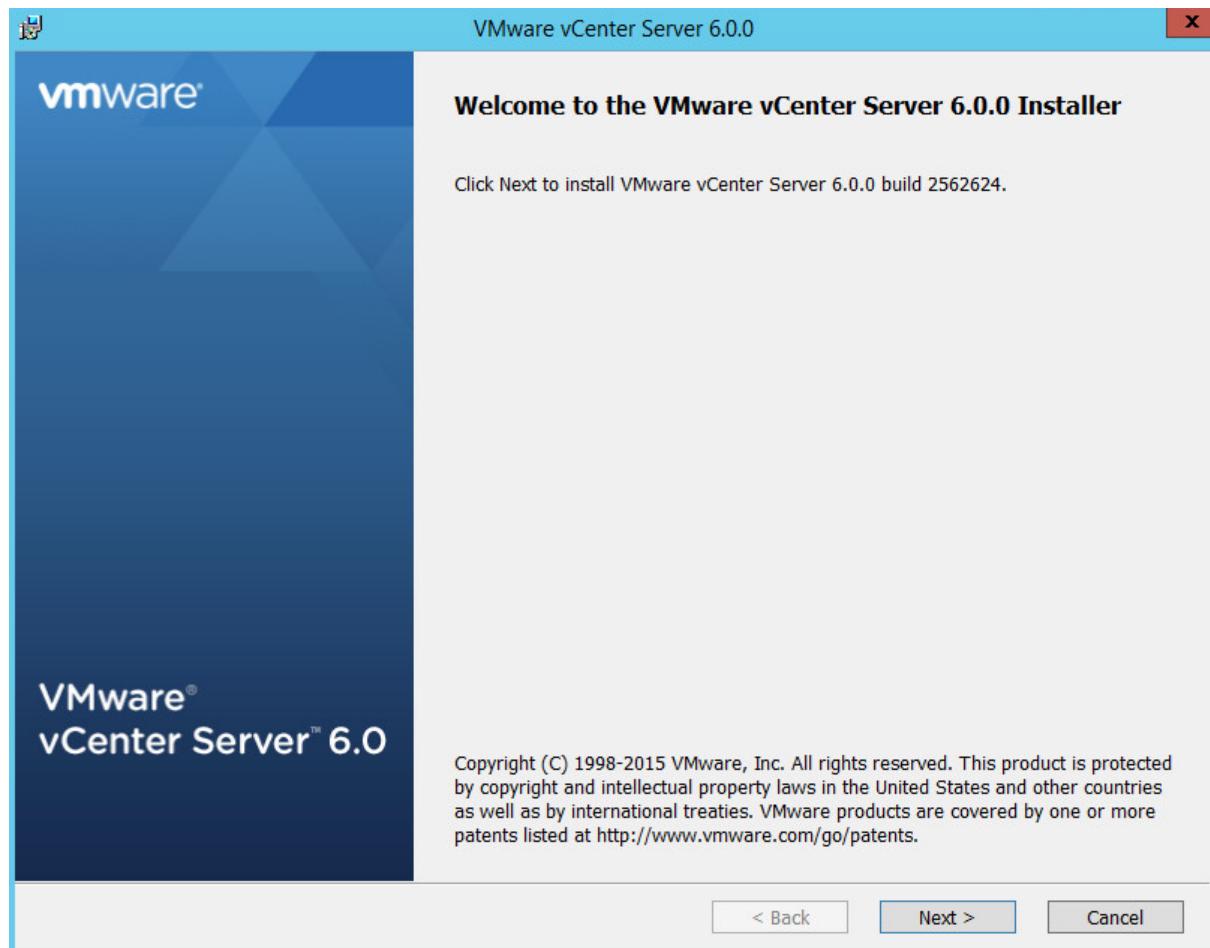
b) Installation

Nous lançons l'exécution de vCenter sur notre machine. Nous arrivons alors sur l'interface suivante :

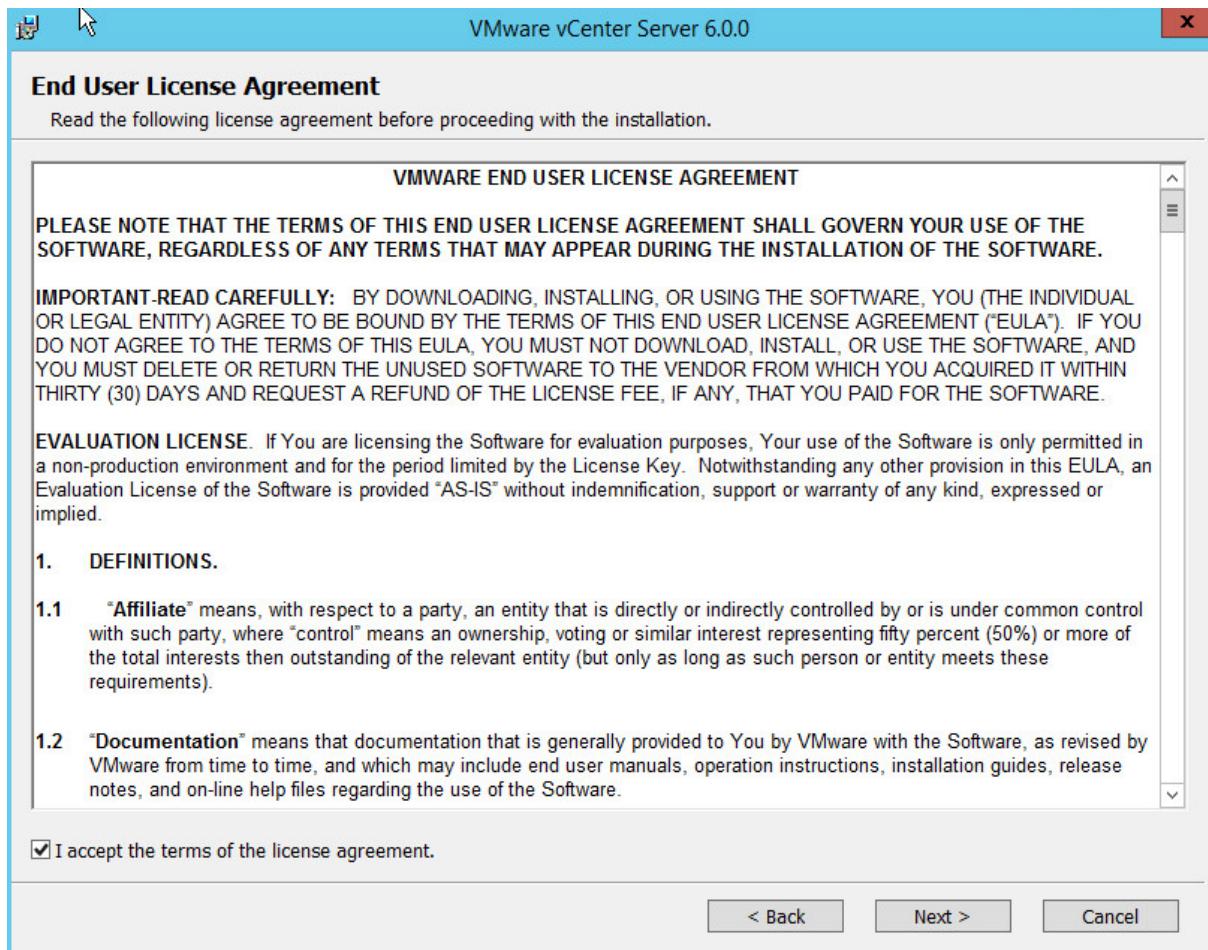


Nous sélectionnons vCenter Server for Windows, puis nous cliquons sur **Install**.

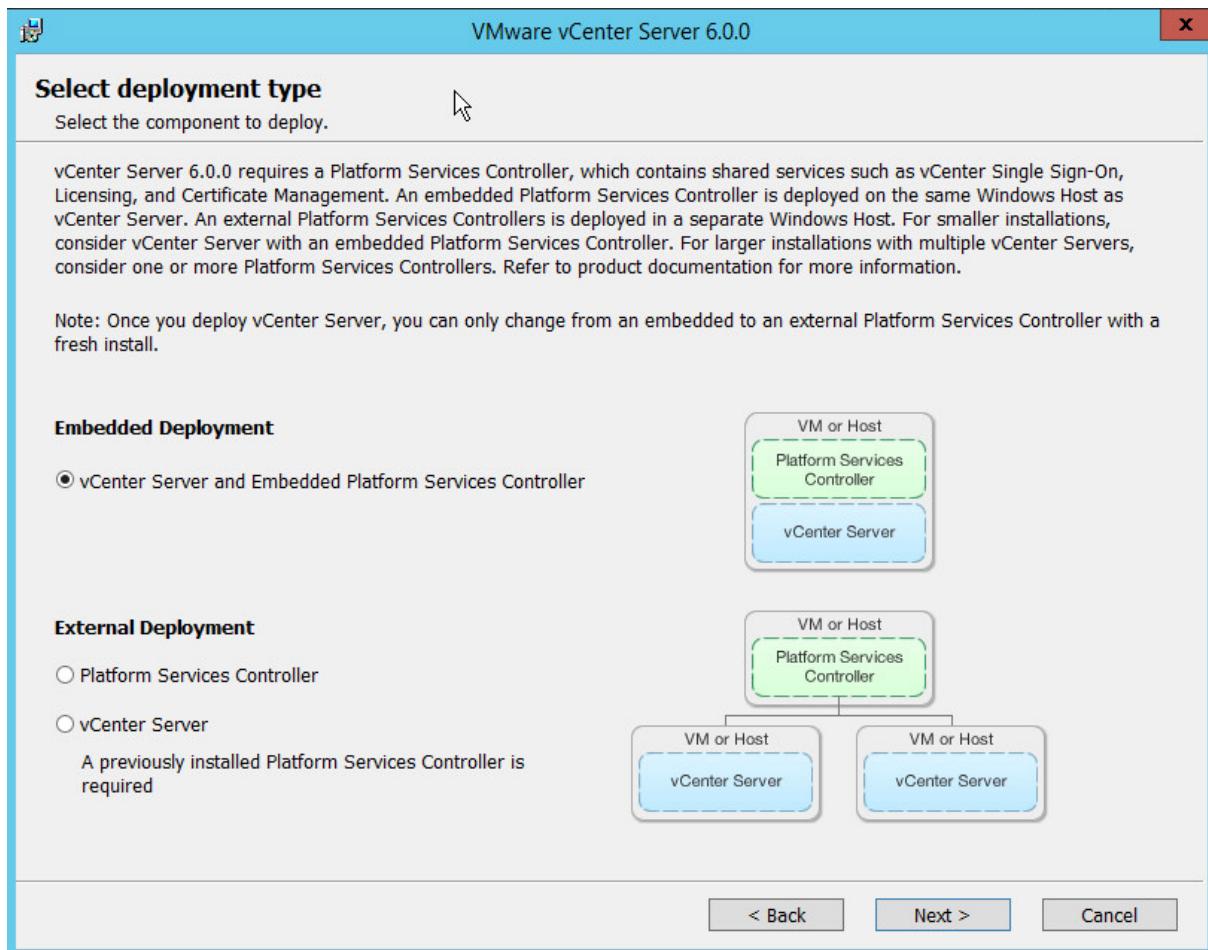
Cliquer alors sur **Next** :



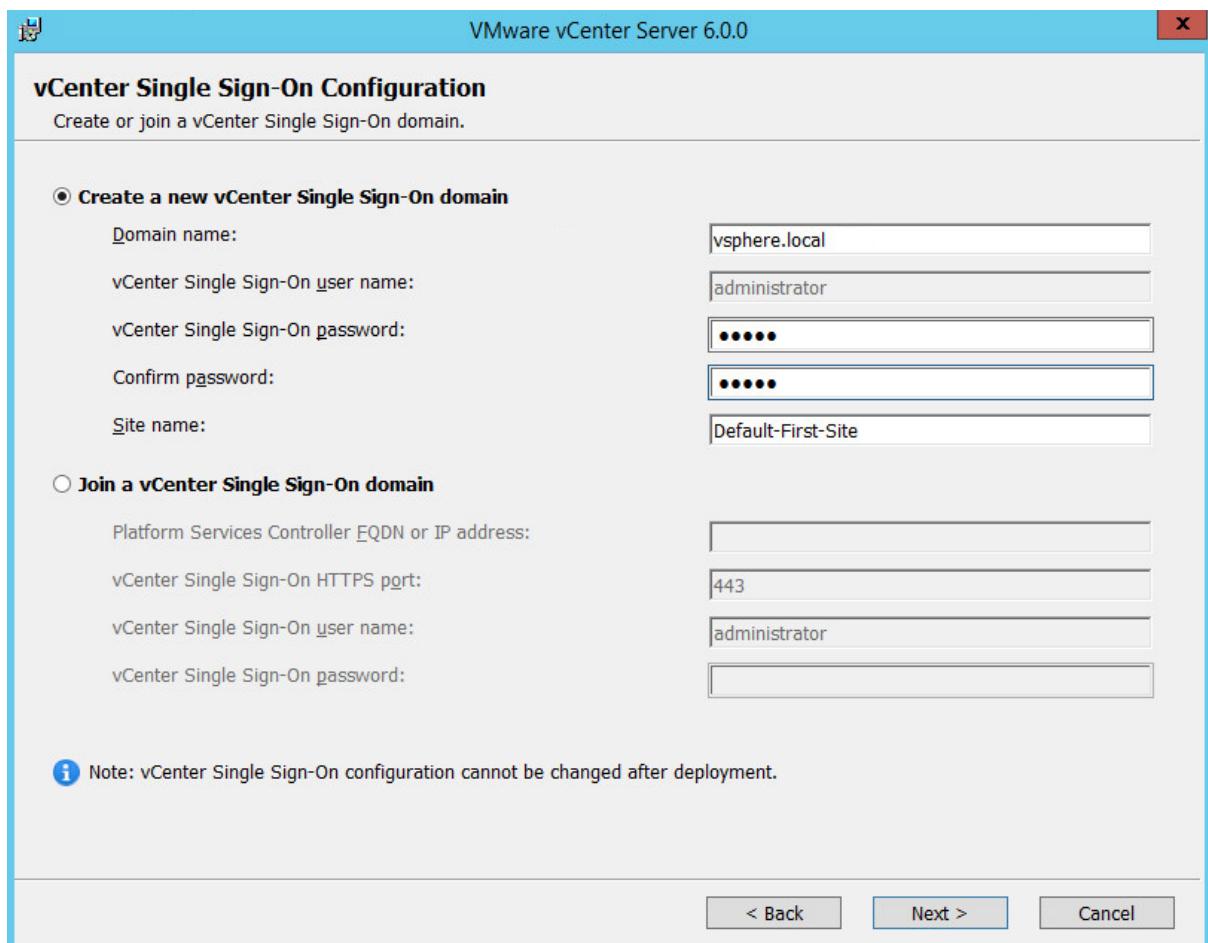
Accepter les licences et cliquer sur **Next** :



Ensuite, nous devons choisir entre installer le PSC (Platform Services Controller) avec le vCenter interne ou externe. Ici, nous choisissons de l'installer avec le vCenter en interne :



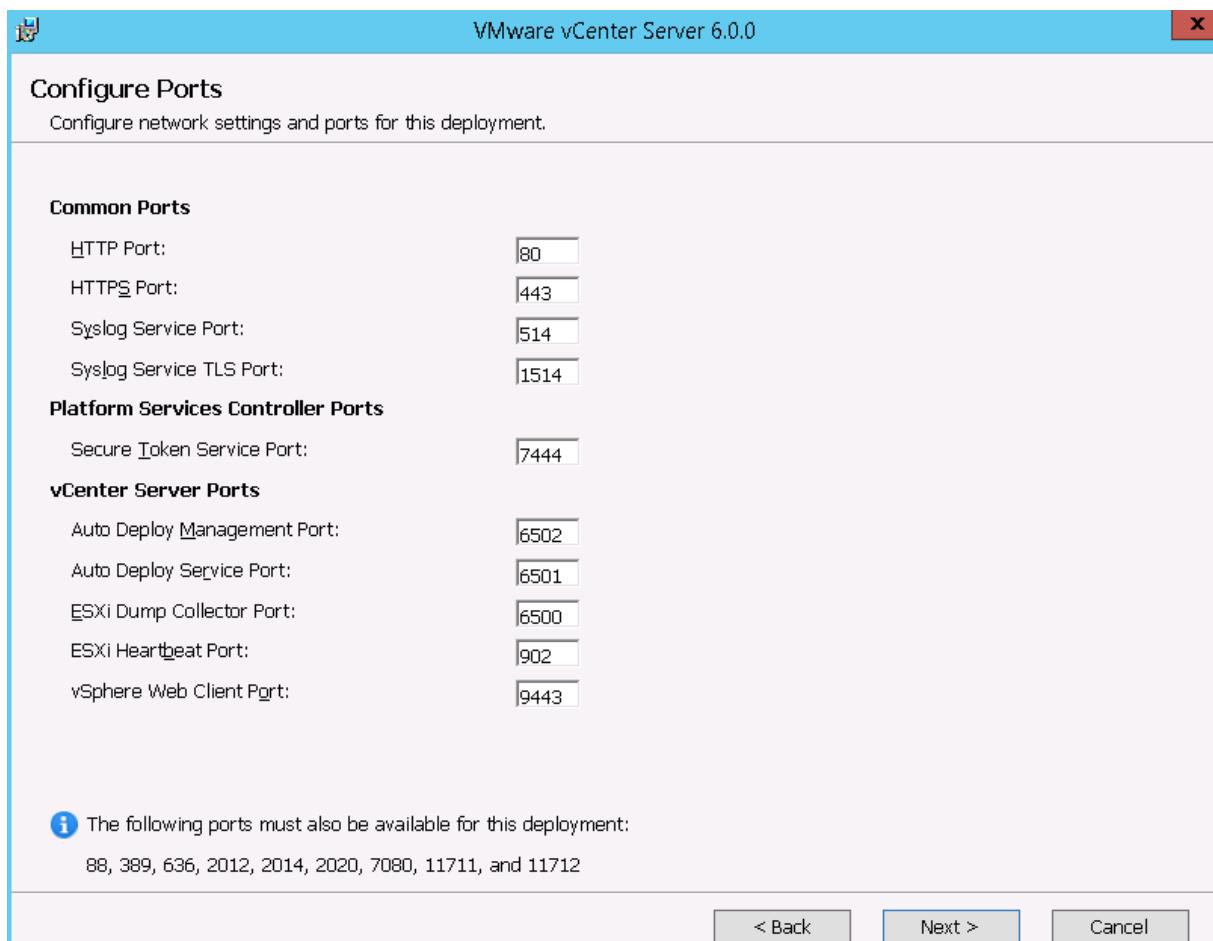
L'installeur récupère alors le nom FQDN de notre machine et nous l'indique, cliquer alors sur **Next**. Ensuite, nous avons deux options, soit rejoindre ou créer un domaine SSO (Single Sign-On). Comme nous n'avons pas de domaine existant, nous choisissons d'en créer un, puis on clique sur **Next** :



Encore, une fois deux options s'offrent à nous, pour exécuter l'instance vCenter, nous pouvons choisir entre utiliser le compte local Système Windows ou choisir un compte du domaine. Ici, nous optons pour se connecter avec le compte local Système.

On clique sur **Next**, vient alors le choix de la base de données, choisir une existante ou utiliser la base de données intégrée de vCenter. Dans notre cas, nous choisissons d'utiliser la base de données intégrée.

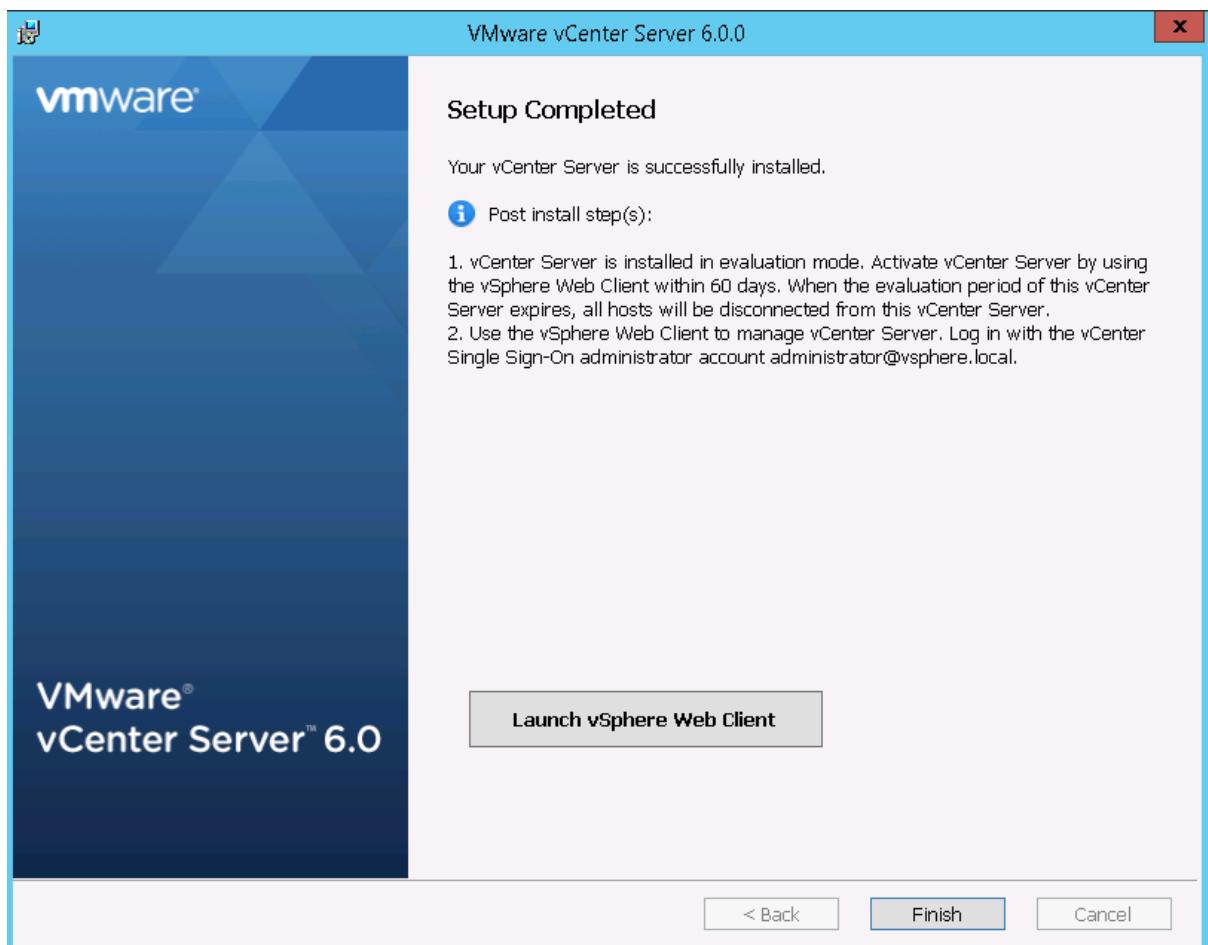
On cliquer sur **Next**, l'installeur nous indique les différents ports utilisés par vCenter, on laisse toutes les valeurs par défaut et on clique sur **Next** :



Il faut ensuite choisir le dossier d'installation, on laisse par défaut, on clique sur **Next**.

Le wizard nous fait alors un résumé avant l'installation, après vérification, cliquer sur **Install**.

L'installation est terminée, notre vCenter est désormais prêt à être utilisé, on peut alors se connecter au client Web de vCenter :



E. Installation et configuration d'un ESXi

a) Introduction

Ici, nous installons un ESXi dans sa version 6.0. L'ESXi sera amené à virtualiser notre infrastructure trois-tiers (Front-end, back-end et base de données). Ainsi, nous créons une nouvelle VM, avec pour configuration 4Go de RAM, 2 cœurs de processeurs et un espace disque de 40Go.

b) Installation

Nous lançons l'installation de l'ESXi, la VM boot alors sur l'iso... Une message de bienvenue apparaît alors, on appuie sur la touche **Entrée**.

Il faut ensuite accepter les conditions générales d'utilisation en pressant la touche **F11**.

La machine nous demande ensuite sur quel disque installer le système, on choisit notre disque de 40Go et on valide avec la touche **Entrée**, puis on choisit notre langue.

Il faut maintenant entrer un nouveau mot de passe pour l'accès à l'administration de notre nouveau ESXi. Enfin, il faut confirmer l'installation en pressant la touche **F11**.

Une fois l'installation terminée, l'ESXi devra redémarrer, pour cela presser la touche **Entrée**.

Une fois redémarré, nous arrivons sur cette interface :



On peut voir la configuration de notre ESXi ainsi que ses adresses IPv4 et IPv6. On remarque d'emblée que l'adresse IPv4 est en DHCP, or, un serveur possède toujours une adresse IP fixe. On va alors entrer dans la configuration de notre ESXi.

c) Configuration de l'ESXi

Nous allons modifier l'adresse IPv4, pour cela, appuyer sur la touche **F2** pour entrer dans l'interface de configuration. Il faut alors rentrer le mot de passe que nous avions rentré à l'installation.

Avec les flèches nous allons nous rendre sur **Configure Management Network** pour modifier notre adresse IP :

System Customization	Configure Management Network
Configure Password Configure Lockdown Mode Configure Management Network Restart Management Network Test Management Network Network Restore Options Configure Keyboard Troubleshooting Options View System Logs View Support Information Reset System Configuration	<p>Hostname: localhost</p> <p>IPv4 Address: 172.16.4.5</p> <p>Network identity acquired from DHCP server 172.16.7.254</p> <p>IPv6 Addresses: fe80::20c:29ff:feb:8290/64</p> <p>To view or modify this host's management network setting detail, press <Enter>.</p>

On descend alors sur **IPv4 Configuration** et presse la touche **Entrée** :

Configure Management Network	IPv4 Configuration
Network Adapters VLAN (optional) IPv4 Configuration IPv6 Configuration DNS Configuration Custom DNS Suffixes	<p>Automatic</p> <p>IPv4 Address: 172.16.4.5 Subnet Mask: 255.255.248.0 Default Gateway: 172.16.0.2</p> <p>This host can obtain an IPv4 parameters automatically if your network includes a DHCP server. If it does not, the following settings must be specified:</p>

Dans les options, on se déplace maintenant sur **Set static IPv4 address...** et on presse la barre d'espace pour valider notre choix. On va ensuite choisir notre configuration et on la valide avec la touche **Entrée** :

IPv4 Configuration	
This host can obtain network settings automatically if your network includes a DHCP server. If it does not, the following settings must be specified:	
<input type="checkbox"/> Disable IPv4 configuration for management network <input type="checkbox"/> Use dynamic IPv4 address and network configuration <input checked="" type="checkbox"/> Set static IPv4 address and network configuration:	
IPv4 Address	[172.16.4.12]
Subnet Mask	[255.255.248.0]
Default Gateway	[172.16.0.2]
<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel	

Nous allons ensuite modifier notre configuration DNS, pour cela aller sur **DNS Configuration** et presser la touche **Entrée**, on arrive alors sur cette interface :

DNS Configuration

This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.

- () Obtain DNS server addresses and a hostname automatically
- (o) Use the following DNS server addresses and hostname:

Primary DNS Server	[172.16.0.2]
Alternate DNS Server	[]
Hostname	[localhost]

<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

On va alors entrer l'adresse IP de notre serveur DNS et changer le hostname de notre ESXi et valider avec la touche Entrée :

DNS Configuration

This host can only obtain DNS settings automatically if it also obtains its IP configuration automatically.

- () Obtain DNS server addresses and a hostname automatically
- (o) Use the following DNS server addresses and hostname:

Primary DNS Server	[172.16.4.1]
Alternate DNS Server	[]
Hostname	[NYESX2_]

<Up/Down> Select <Space> Mark Selected <Enter> OK <Esc> Cancel

Ensuite, on presse la touche Esc pour retourner au menu principal. L'ESXi nous demande alors si on veut appliquer les changements effectués, on valide alors avec la touche Y. La configuration est alors enregistrée, notre ESXi est désormais prêt à être intégrer dans notre vCenter et prêt à travailler.

F. Création du cluster d'ESXi sur vCenter

a) Introduction

Toutes les manipulations effectuées ici, sont exécutées sous le client vSphere VMWare. Le client Web de vCenter permet de faire exactement les mêmes choses.

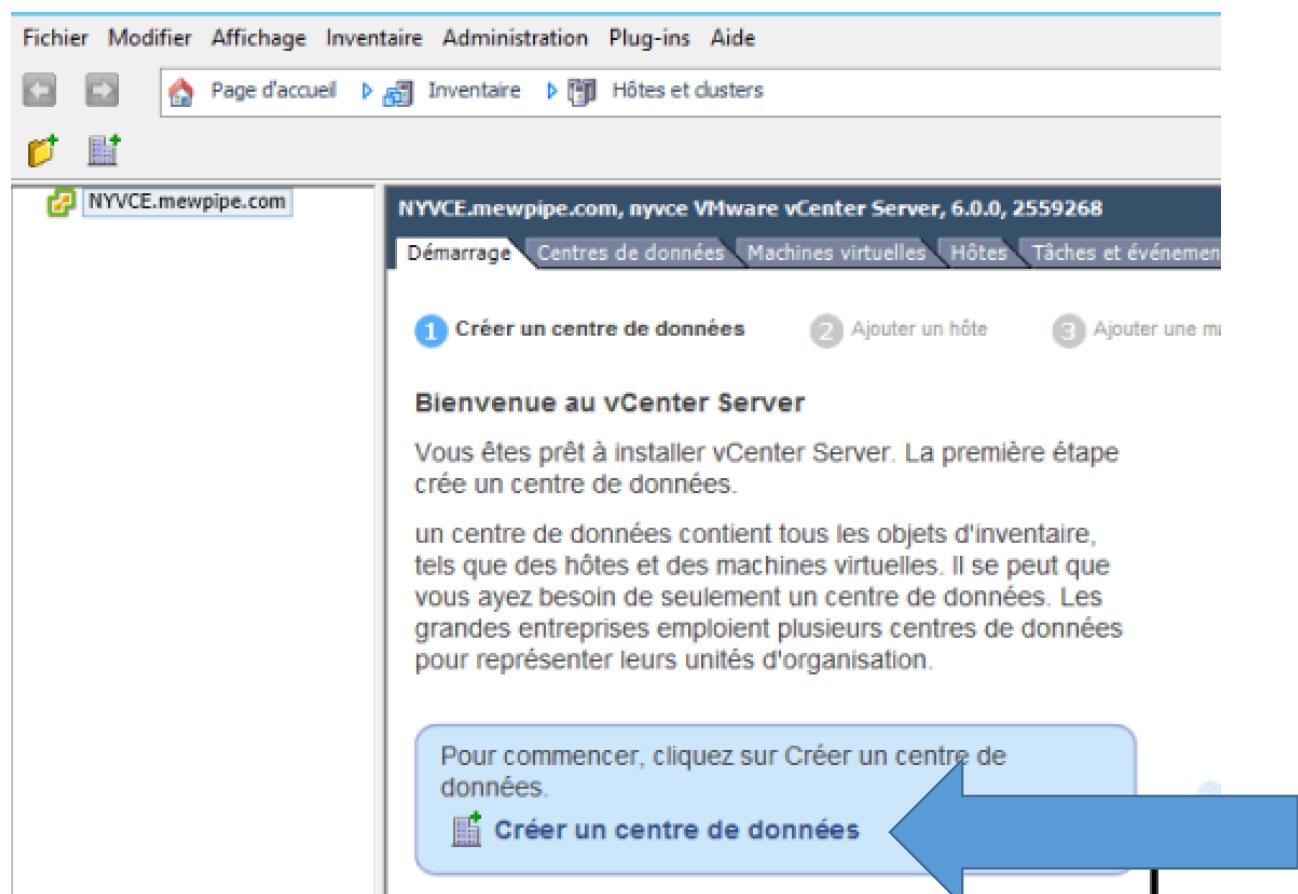
Pour résumé, nous avons :

- Notre vCenter : NYVCE.mewpipe.com (172.16.4.10)
- ESXi : NYESX1.mewpipe.com (172.16.4.11)
- ESXi : NYESX2.mewpipe.com (172.16.4.12)

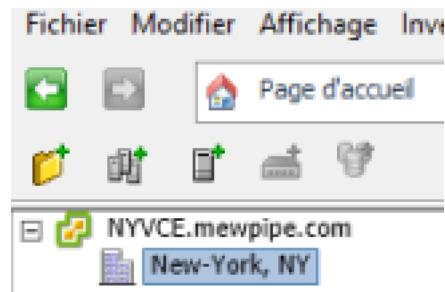
Le but étant de créer un cluster de nos deux ESXi via le vCenter.

b) Création du datacenter

Dans notre client vSphere, nous allons commencer par créer un DataCenter. Pour cela, on va cliquer sur **Créer un centre de données** :



On renseigne un nom, notre Datacenter est alors créé :



c) Ajout des hôtes au datacenter

L'étape suivante consiste à ajouter nos deux ESXi dans notre nouveau datacenter, pour cela on va cliquer sur **Ajouter un hôte** :

The screenshot shows the 'Ajouter un hôte' (Add Host) wizard in step 2. The title bar says 'Ajouter un hôte'. The left sidebar shows the datacenter 'New-York, NY' with its sub-site 'New-York, NY'. The main content area has three numbered steps: 1. Créer un centre de données, 2. Ajouter un hôte (which is active), and 3. Ajouter une machine virtuelle. Step 2 is titled 'Ajouter un hôte' and contains the following text:

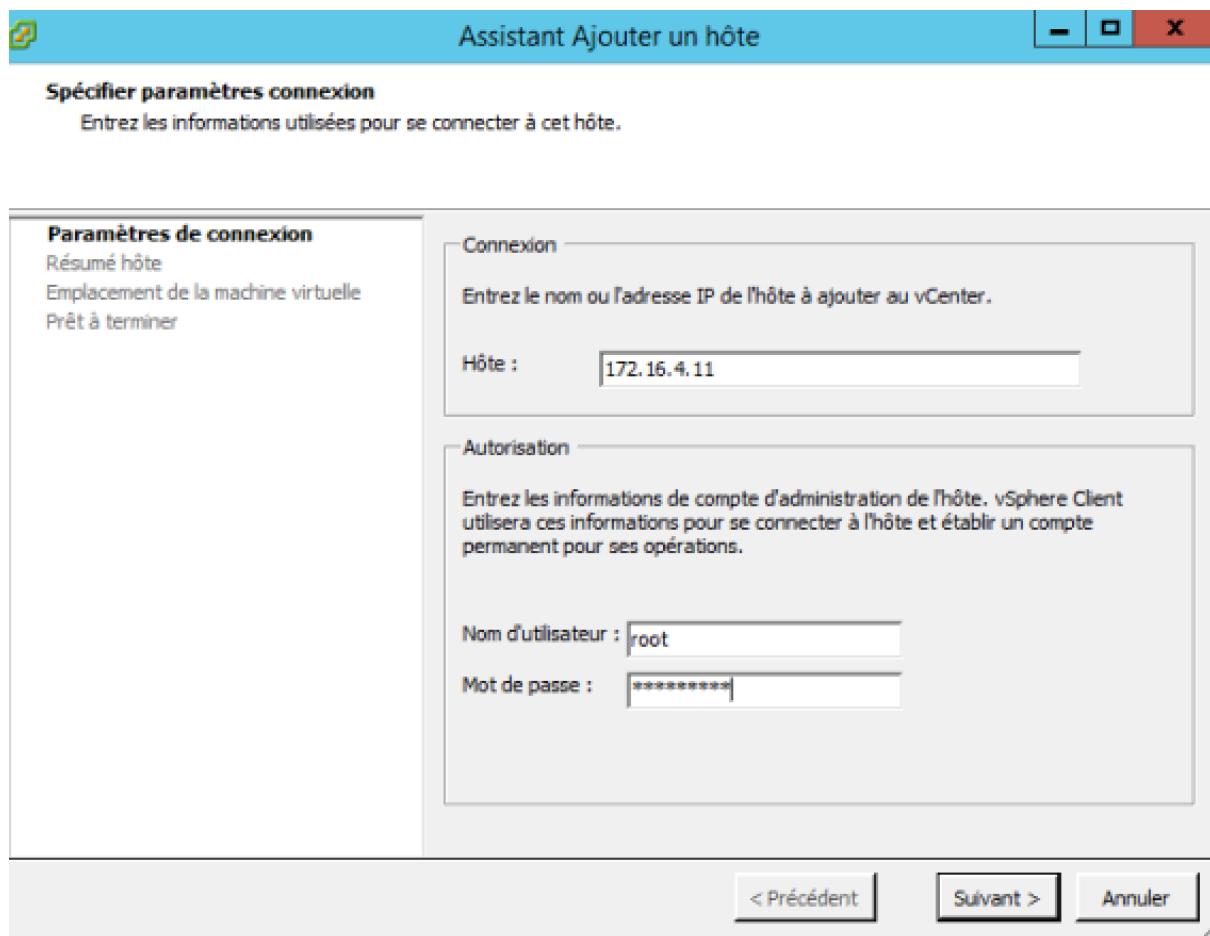
Un hôte est un ordinateur qui emploie un logiciel de virtualisation, comme ESX ou ESXi, pour exécuter des machines virtuelles. L'ajout d'un hôte à l'inventaire le place sous l'administration de vCenter Server.

Vous avez besoin d'un ordinateur exécutant le logiciel ESX ou ESXi. Si vous n'avez pas le logiciel ESX ou ESXi, visitez le [site Web de VMware](#) pour plus d'informations sur ce produit.

Pour ajouter un hôte, vous devez connaître son emplacement sur le réseau et le compte administratif (en général administrateur ou racine).

A blue callout bubble points to the 'Ajouter un hôte' button with the text: 'Pour continuer la configuration de vCenter Server, cliquez sur Ajouter un hôte.'

Vient alors s'ouvrir un wizard, il faut entrer l'adresse IP de notre premier ESX, ainsi que les identifiants pour s'y connecter :

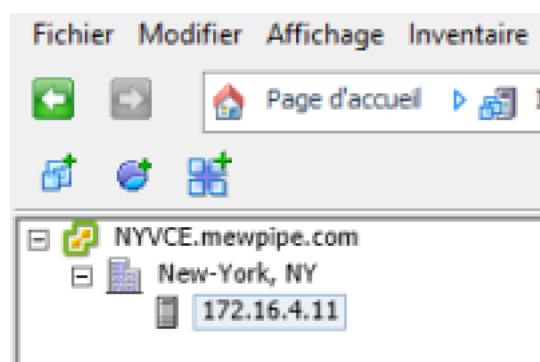


Nous pouvons alors cliquer sur **Suivant**, une alerte sécurité apparaît nous demandant si nous souhaitons poursuivre la connexion, cliquons sur **Oui**.

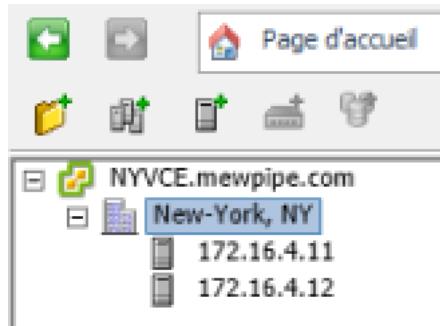
Nous pouvons ensuite passer le résumé de l'hôte, pour la licence, laisser en version d'évaluation, contentons-nous de cliquer sur **Suivant**.

L'assistant nous demande alors où intégrer cet hôte, il a choisi pour nous le datacenter récemment créé, cliquons alors sur **Suivant**, puis sur **Terminer**.

Après un petit temps de synchronisation, notre premier ESXi apparaît dans notre datacenter :



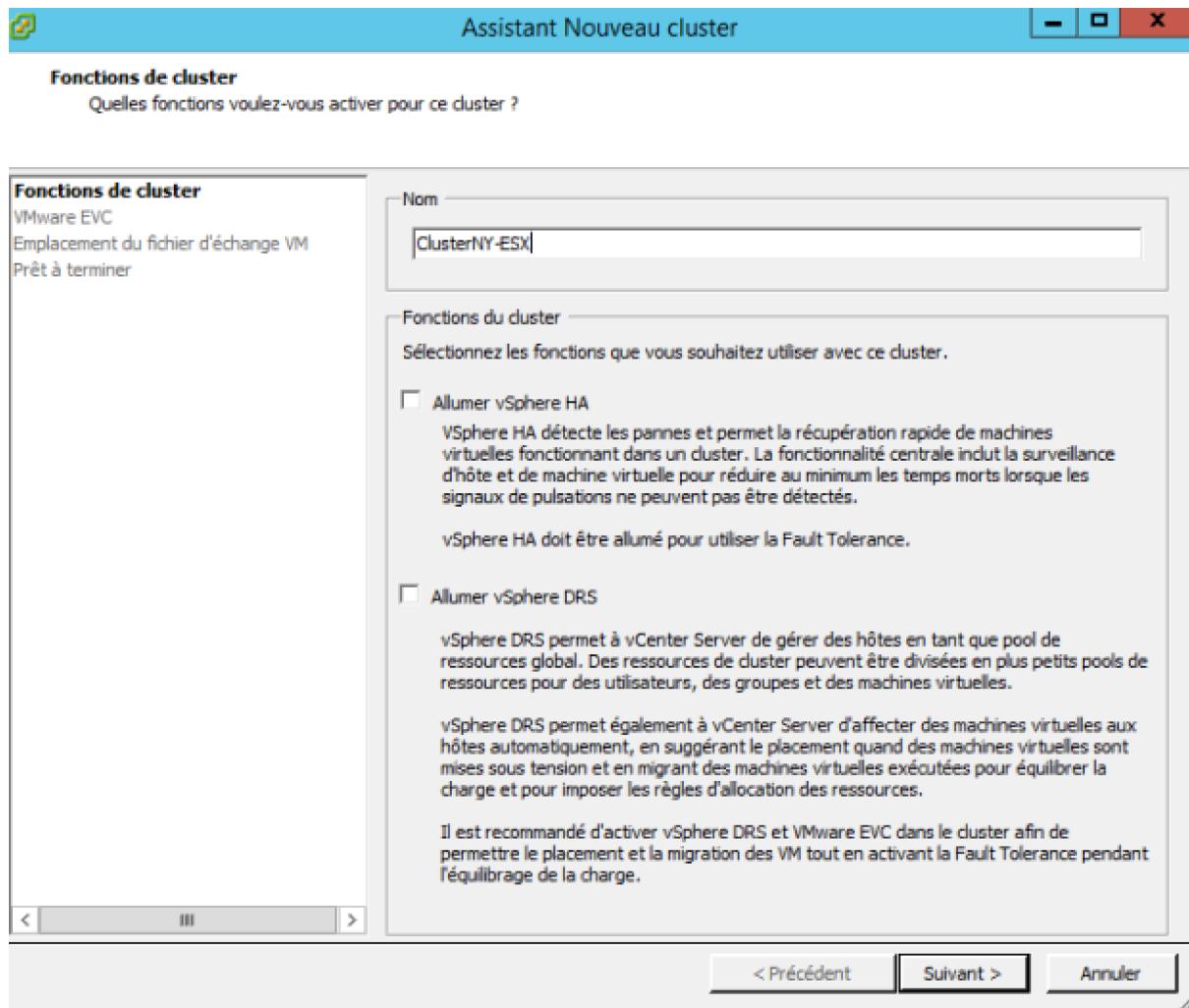
Nous faisons de même pour notre deuxième ESXi, nous obtenons alors le résultat suivant :



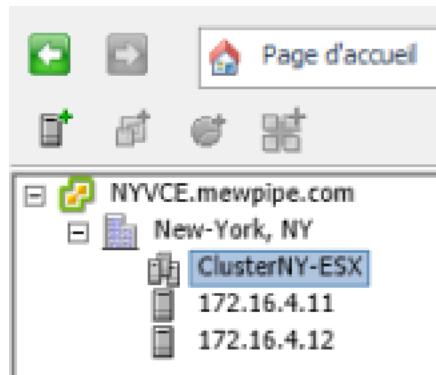
Nos deux ESXi sont alors intégrés à notre datacenter mais ne forme pas encore pour autant un cluster.

d) Création et configuration du cluster

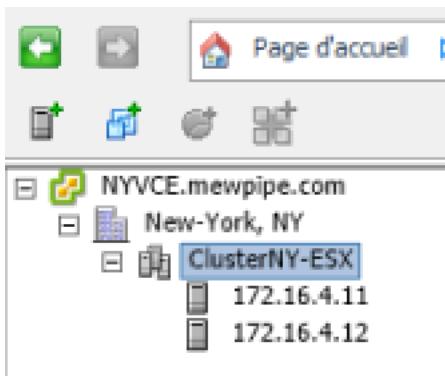
Nous allons maintenant créer notre cluster. Pour cela, effectuer un clic-droit sur le datacenter et cliquer sur **Créer un nouveau cluster**, s'ouvre alors une nouvelle fenêtre, dans laquelle on va renseigner le nom de notre nouveau cluster :



Nous n'allumons pas vSphere HA et DRS pour le moment, on clique sur suivant, on laisse l'EVC désactivé également. Enfin, on choisit de stocker le fichier d'échange dans le même répertoire que la machine virtuelle pour le moment, puis on clique sur **Terminer**. Notre nouveau cluster est alors créé :



Pour intégrer nos ESXi au nouveau cluster il suffit de les faire glisser dans ce dernier, nous obtenons alors le résultat suivant :

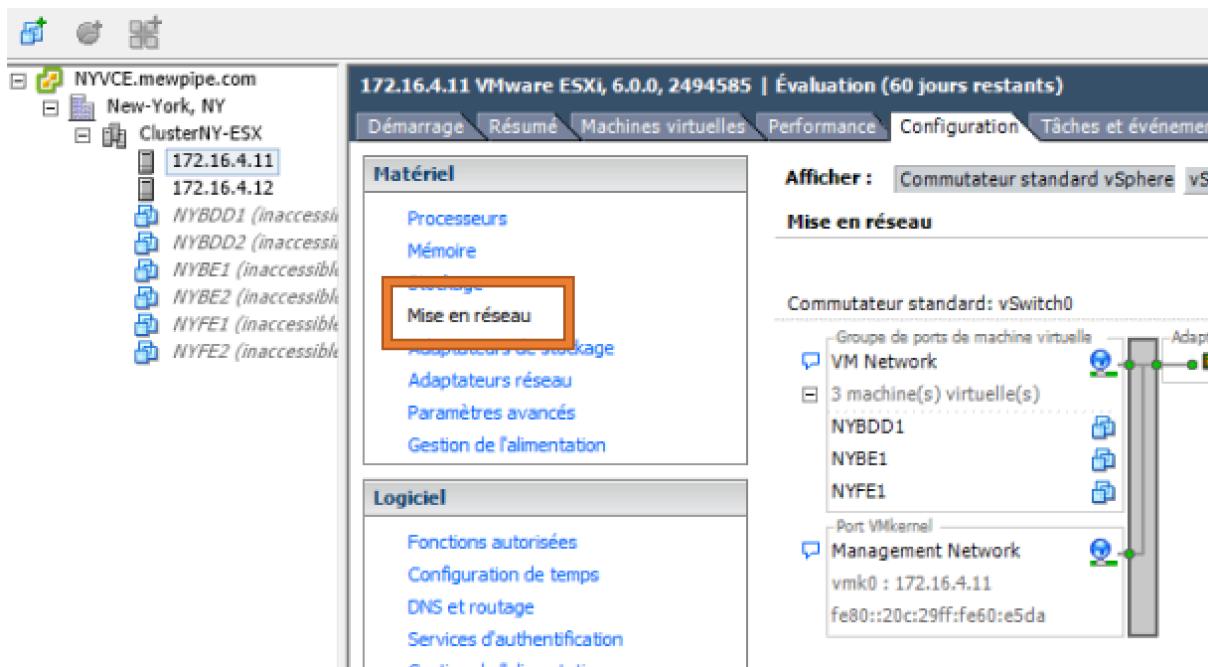


Notre ESXi forment alors un cluster.

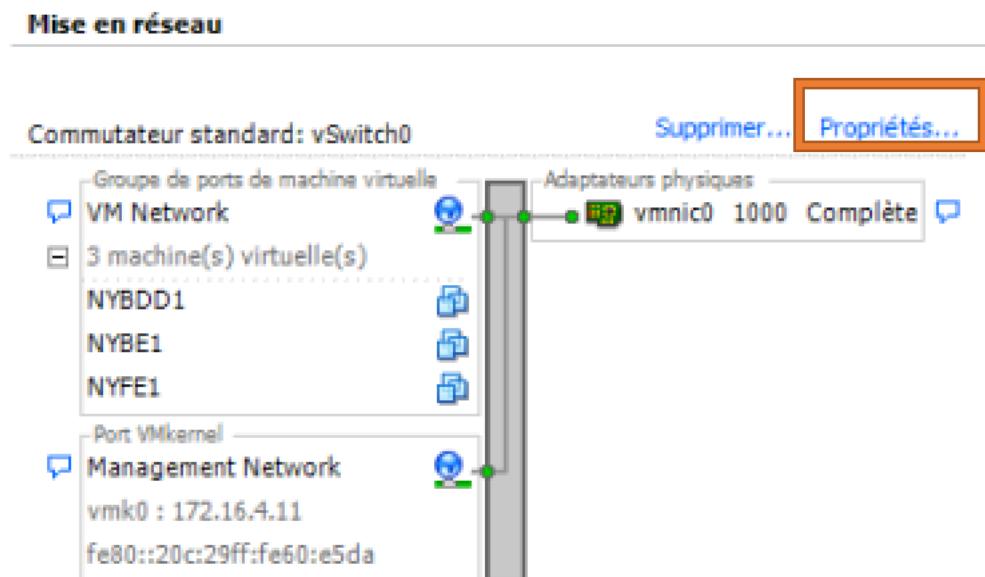
e) Activation de la haute disponibilité au niveau du cluster

Afin d'assurer la haute disponibilité dans notre cluster, nous allons devoir activer la **HA** au sein de ce dernier. Pour cela, on va au préalable activer le **vMotion** sur les réseaux de management des VMS de nos ESXi afin de pouvoir effectuer des migrations de machines virtuelles à chaud.

Après avoir sélectionné notre premier ESXi, on se rend dans l'onglet **Configuration**, puis on clique sur le lien **Mise en réseau** du panel **Matériel** :



On clique alors sur les **Propriétés** de notre commutateur standard **vSwitch0** :



On va alors sélectionner notre **Management Network** et cliquer sur **Modifier** :

vSwitch0 propriétés

Ports	Adaptateurs réseau
Configuration	Résumé
vSwitch	120 ports
VM Network	Groupe de ports...
Management Network	vMotion et port...

Propriétés port

Étiquette réseau : Management Network
 ID VLAN : Aucun (0)
 vMotion : Activé
 Enregistrement de Fault Tolerance : Désactivé
 Trafic gestion : Activé
 Liaison port iSCSI : Désactivé

Paramètres carte réseau

Adresse MAC : 00:0c:29:60:e5:da
 MTU : 1500

Paramètres IP

Adresse IP : 172.16.4.11
 Masque de sous-réseau : 255.255.248.0

[Afficher le tableau de roulement](#)

Paramètres IPv6

Adresses IPv6 : fe80::20c:29ff:fe60:e5da/64

[Afficher le tableau de roulement](#)

Règles pertinentes

(Aucune)

Ajouter... **Modifier...** Supprimer

Dans l'onglet **Général**, nous allons cocher la case **vMotion** :

Général | Paramètres IP | Sécurité | Formation du trafic | Association de cartes réseau

Propriétés port

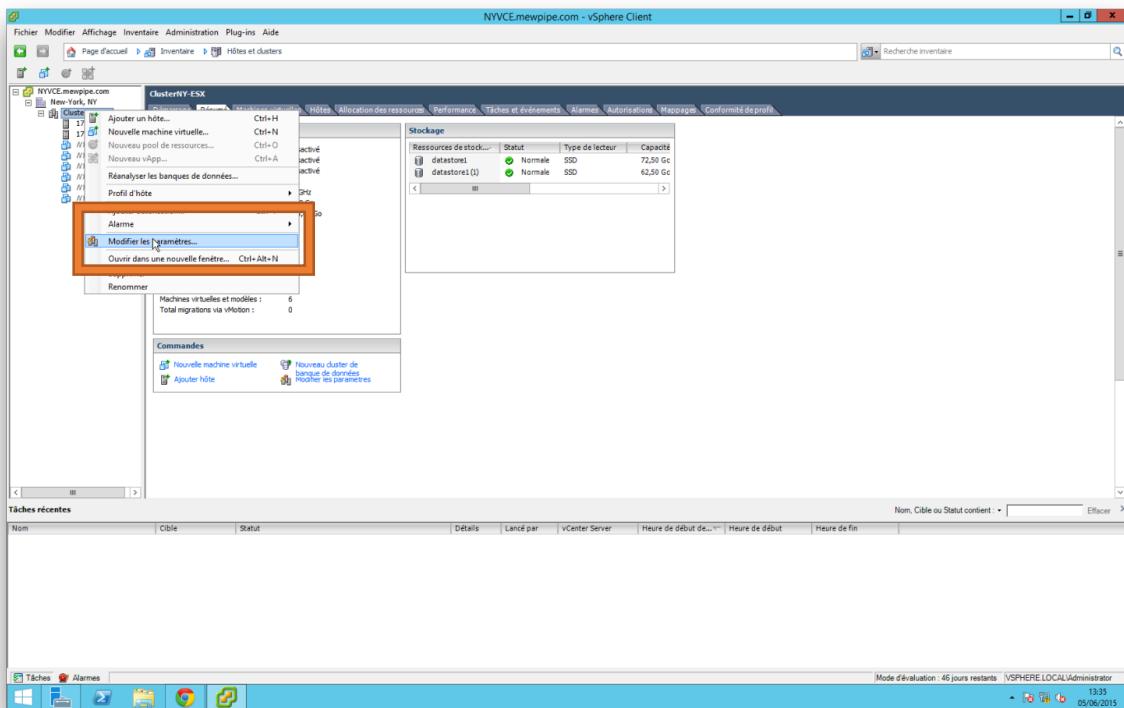
Étiquette réseau : Management Network
 ID VLAN (facultatif) : Aucun (0)
vMotion : Activé

Enregistrement de Fault Tolerance : Activé
 Trafic gestion : Activé
 Liaison port iSCSI : Activé

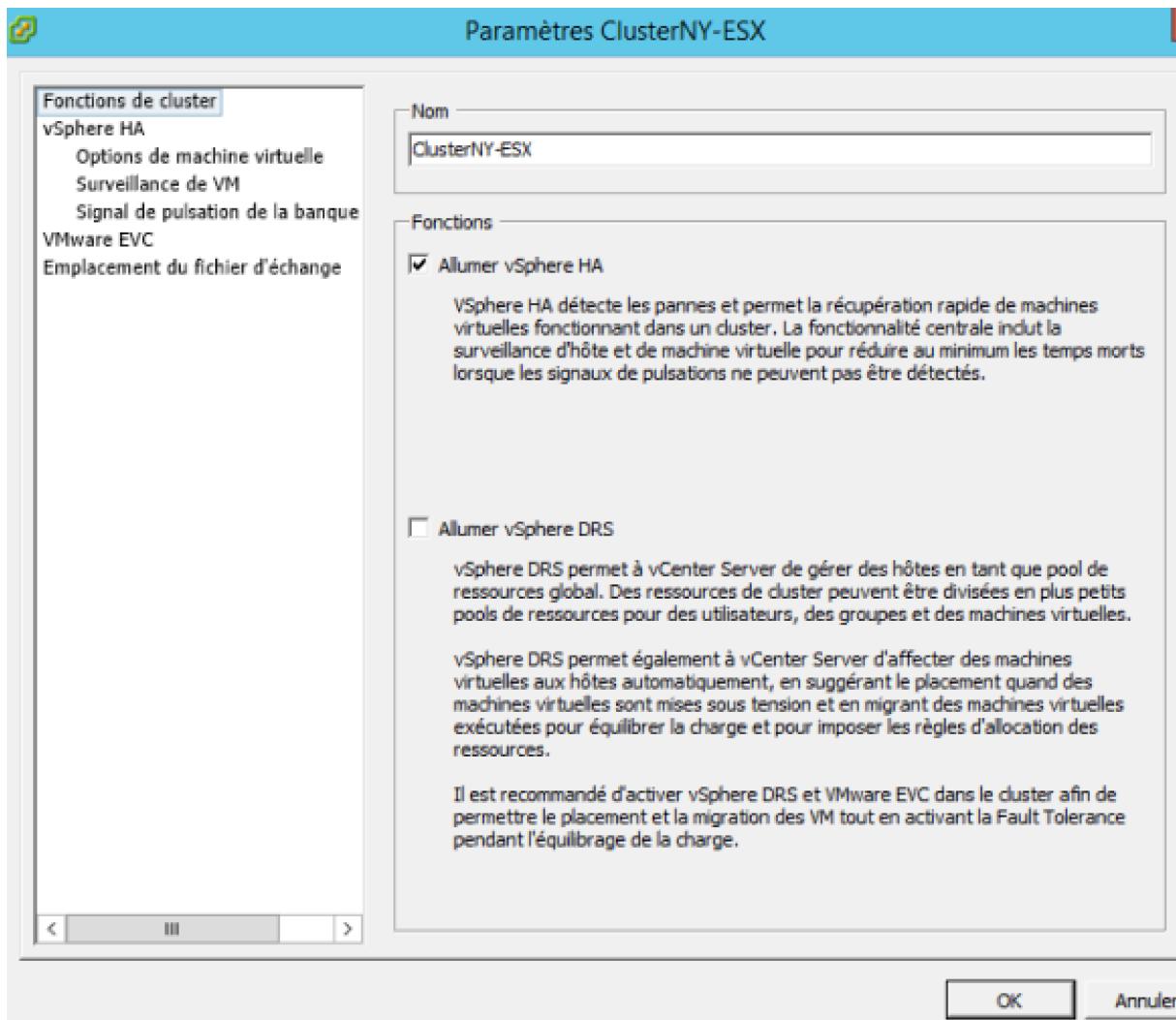
Paramètres de carte réseau

MTU : 1500

Il nous faut maintenant la haute disponibilité sur notre cluster. Pour cela, on effectue clic-droit sur notre cluster, pour enfin cliquer sur **Modifier les paramètres...** :



On va alors cocher la case **Allumer vSphere HA** :



Enfin, on vérifie dans l'onglet **Signal de pulsation de la banque de données** que notre banque de données est bien sélectionné. On peut ensuite valider en cliquant sur **OK**.

On peut alors voir la progression de la configuration sur nos ESXi en bas de l'interface :

Nom	Cible	Statut	Détails	Lancé par	vCenter Server
Configuration de vSphere HA	172.16.4.11	52%	En attente ...	Système	NYVCE.mewpi...
Configuration de vSphere HA	172.16.4.12	52%	En attente ...	Système	NYVCE.mewpi...
Reconfigurer cluster	ClusterNY-ESX	Terminé	VSPHERE.LO...	NYVCE.mewpi...	

Une fois terminé :

Tâches récentes						
Nom	Cible	Statut	Détails	Lancé par	vCenter Server	Heure de début de...
Configuration de vSphere HA	172.16.4.11	Terminé	Système	NYVCE.mewpi...	05/06/2015 13:39:54	
Configuration de vSphere HA	172.16.4.12	Terminé	Système	NYVCE.mewpi...	05/06/2015 13:39:54	
Reconfigurer cluster	ClusterNY-ESX	Terminé	VSPHERE.LO...	NYVCE.mewpi...	05/06/2015 13:39:53	

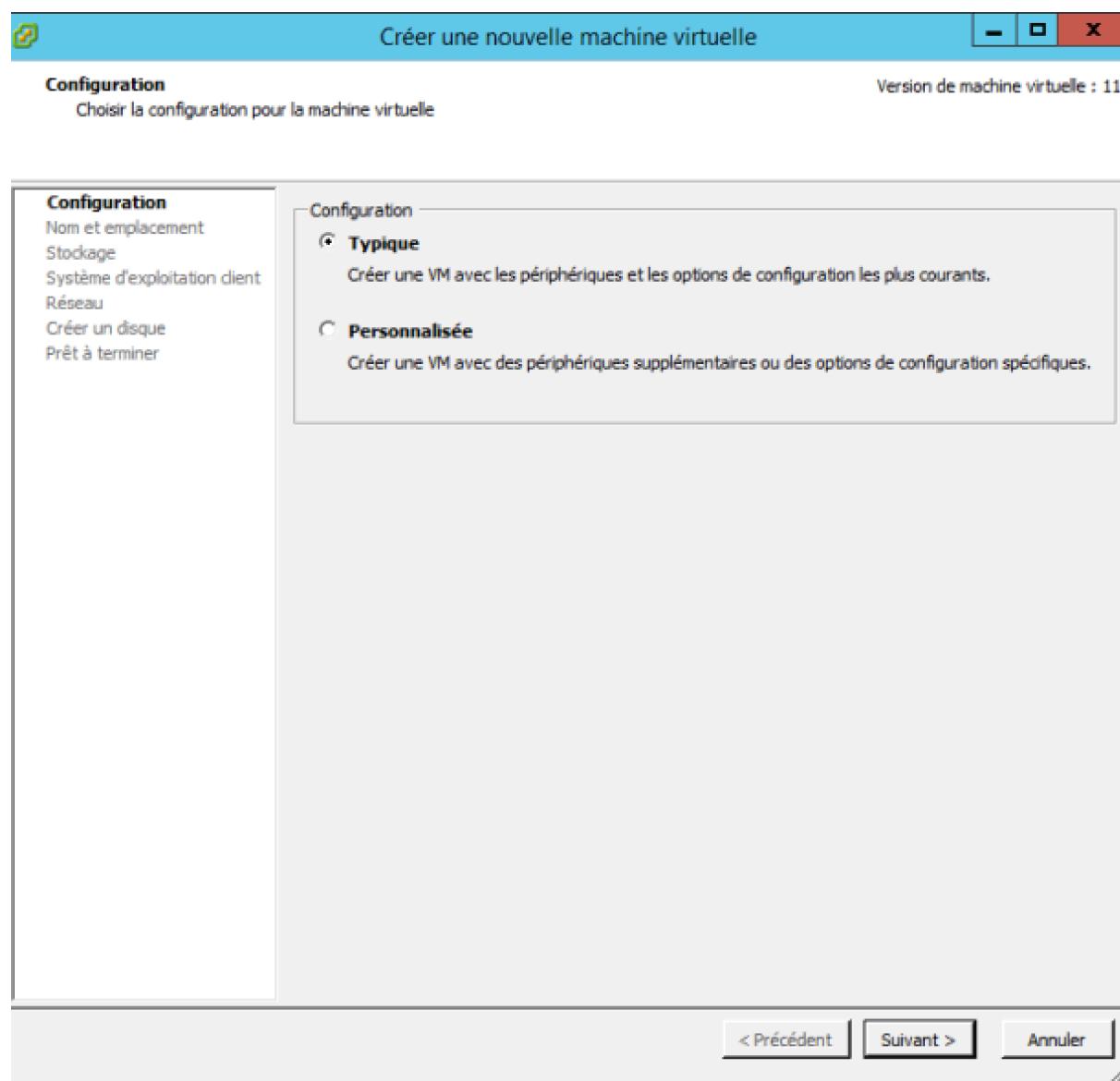
G. Installation et configuration d'un serveur WEB IIS (NYFE1)

a) Introduction

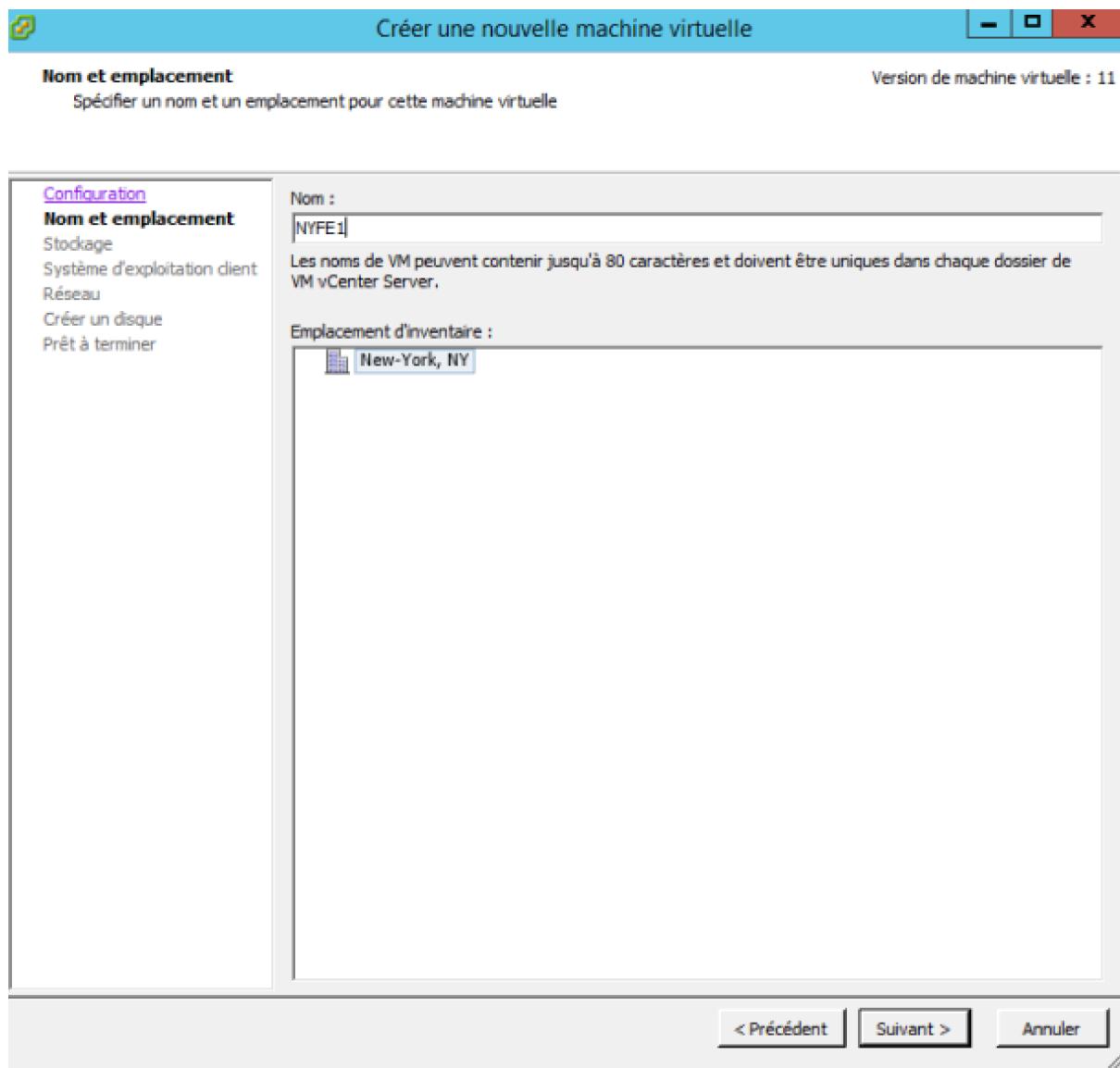
Comme indiqué dans le cahier des charges, l'architecture du site web doit être en trois-tiers (Front-end, back-end, et base de données) et doit être entièrement virtualisée. Nous allons donc créer une nouvelle machine virtuelle Windows Server 2012 R2 Datacenter dans notre ESXi1 (NYESX1.mewpipe.com). Il faudra ensuite installer le rôle IIS dans notre nouveau server WEB qui fera office de front-end dans notre architecture.

b) Création de la machine virtuelle

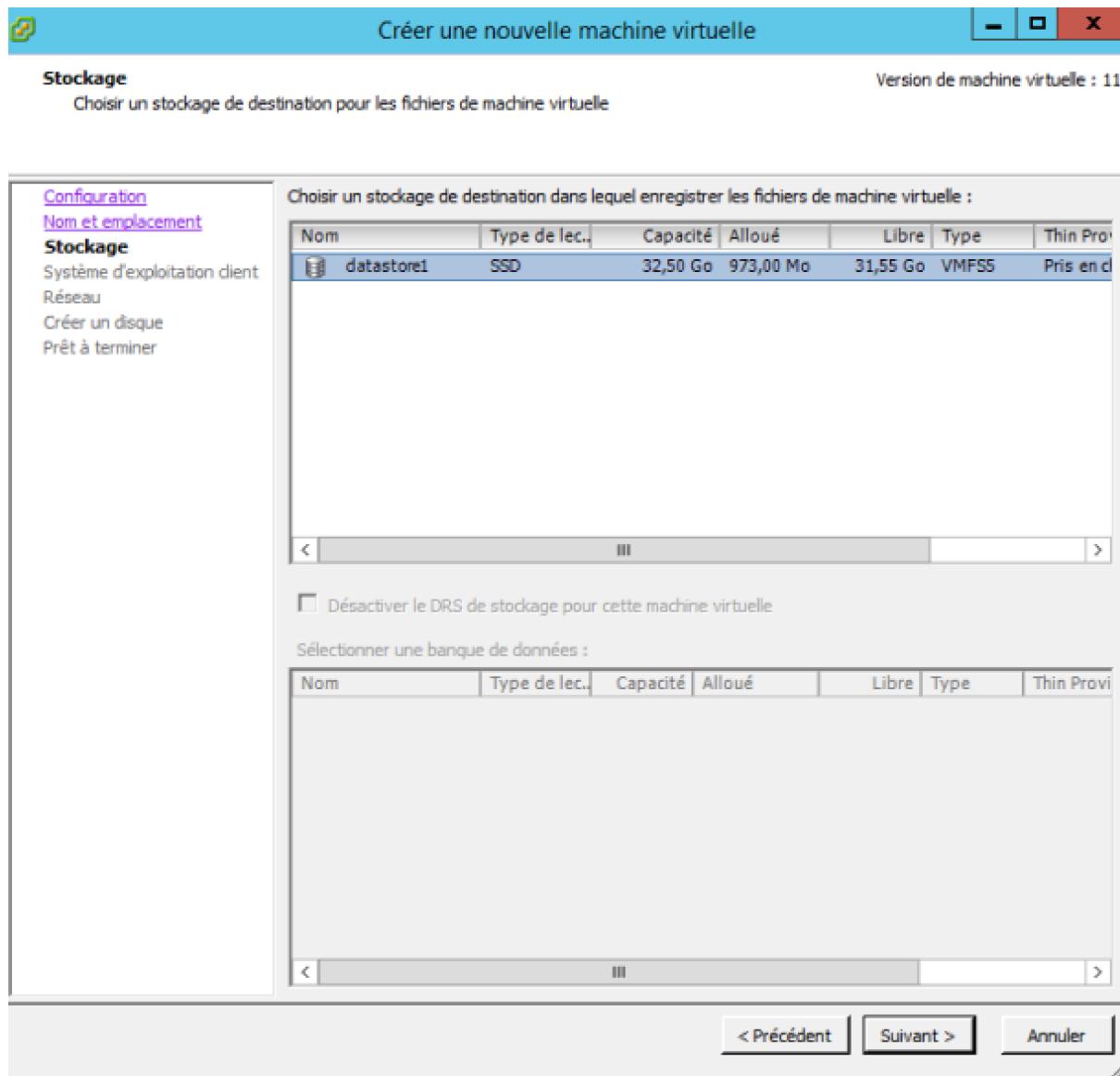
Afin de créer notre nouvelle VM, effectuer un clic-droit sur l'ESXi1 et cliquer sur **Nouvelle machine virtuelle...** S'ouvre alors une nouvelle fenêtre, laisser la configuration en **Typique** et on clique sur **Suivant :**



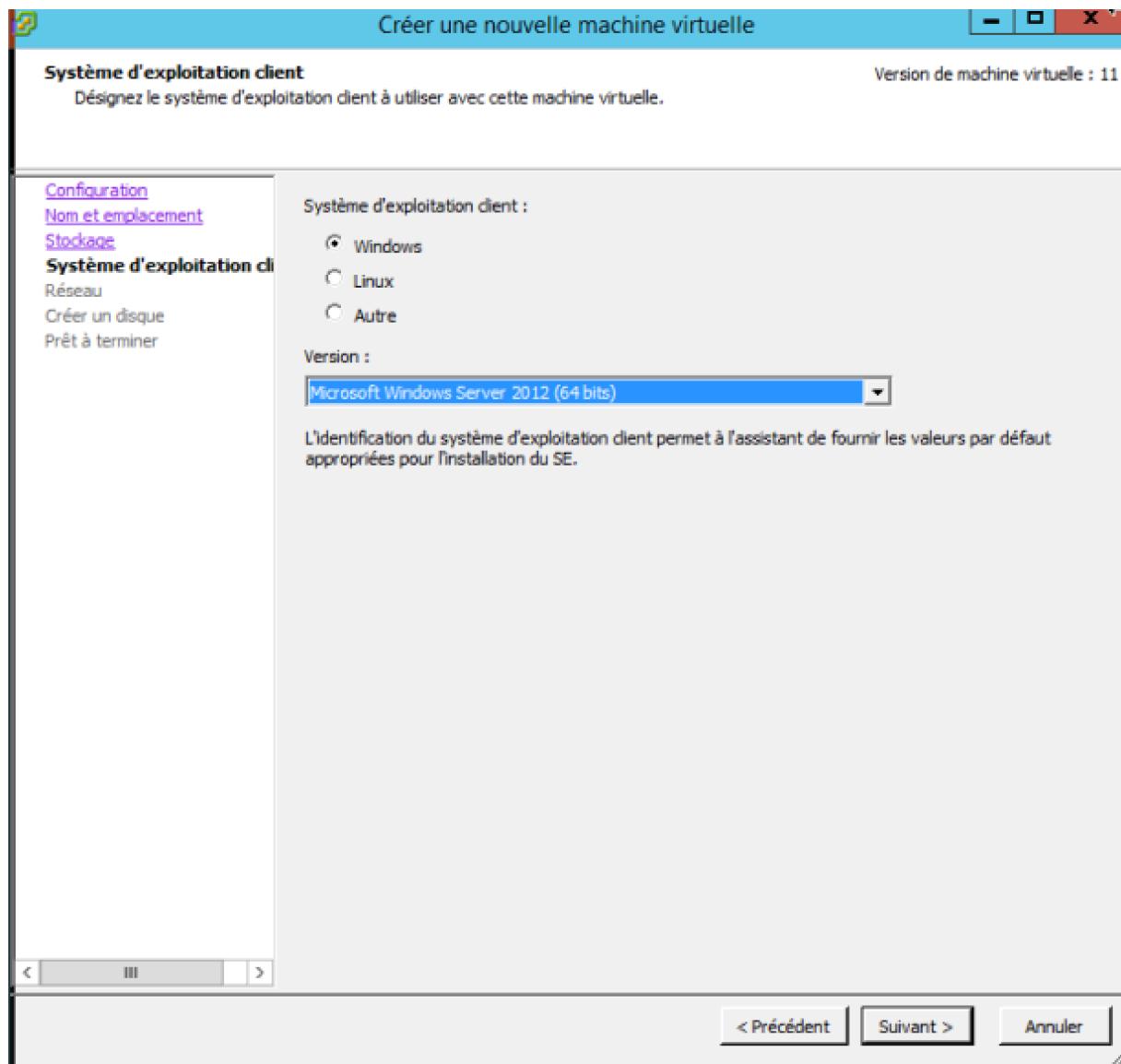
On renseigne ensuite un nom à notre nouvelle machine, l'assistant nous l'a placée dans notre datacenter, c'est parfait, on continue en cliquant sur **Suivant :**



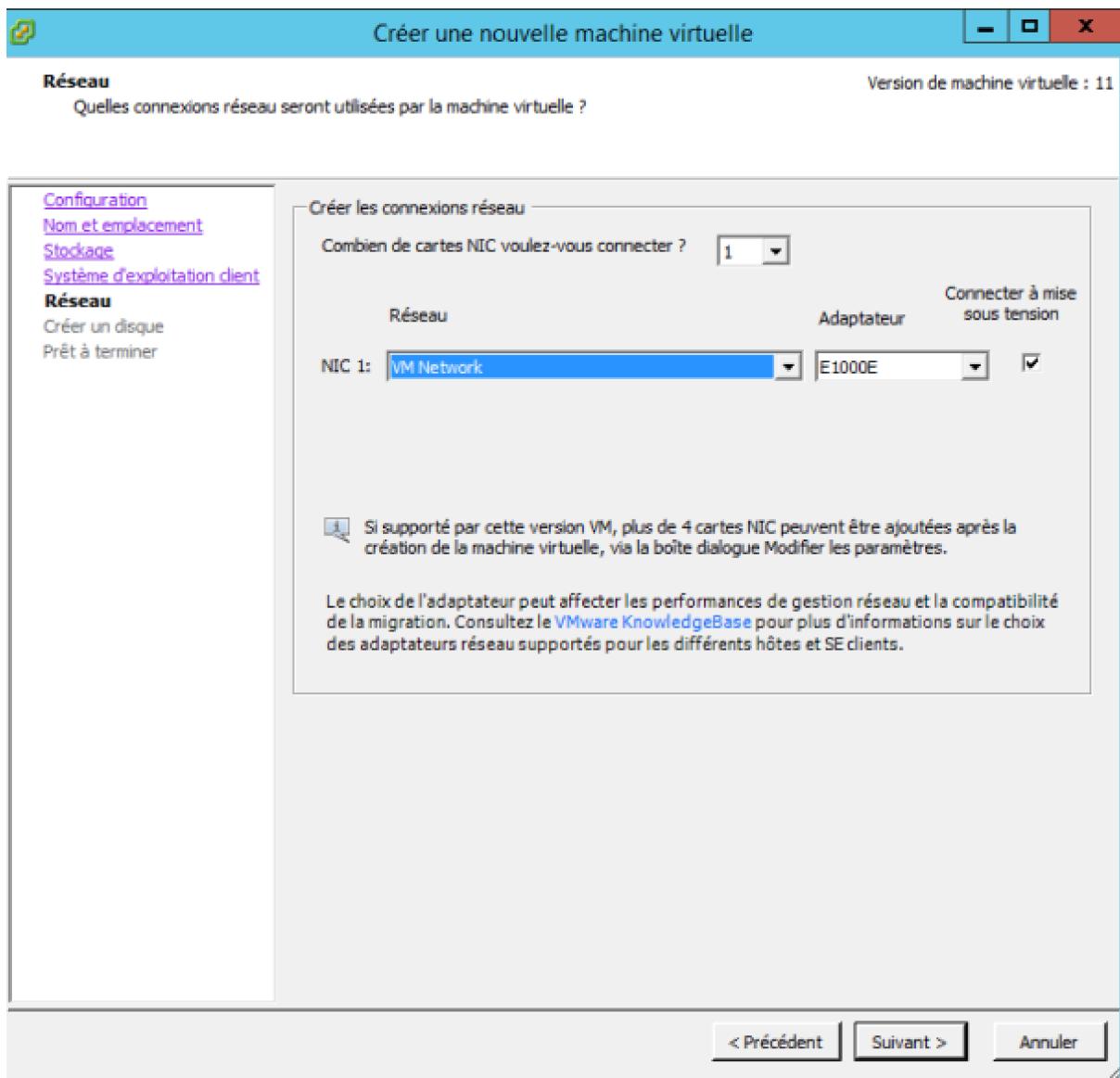
Pour le moment, on laisse le stockage des fichiers de la VM dans le datastore par défaut et on clique sur **Suivant** :



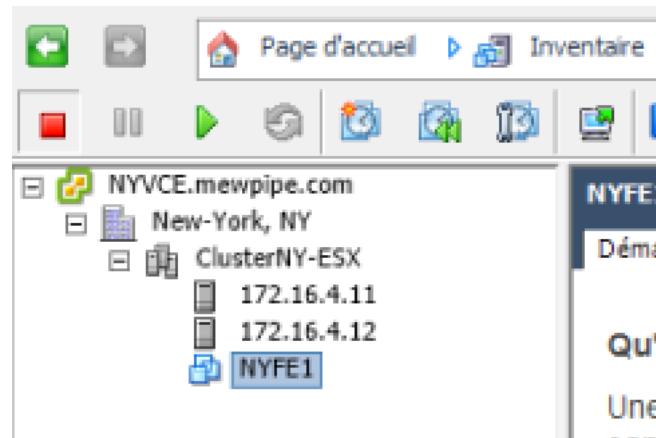
On spécifie le système d'exploitation que l'on utilisera sur notre VM, dans notre cas on indique **Microsoft Windows Server 2012 (64 bits)** et on clique sur **Suivant** :



On lui connecte un adaptateur réseau, on laisse par défaut et on clique sur **Suivant** :



On arrive à la création de notre disque. Dans notre cas, on choisit un disque d'une taille de 20Go en **Thin provision**, on clique ensuite sur **suivant**, on a alors droit à un résumé de la configuration de la machine virtuelle qu'on s'apprête à créer, on peut alors cliquer sur **Terminer**. On obtient alors le résultat suivant :

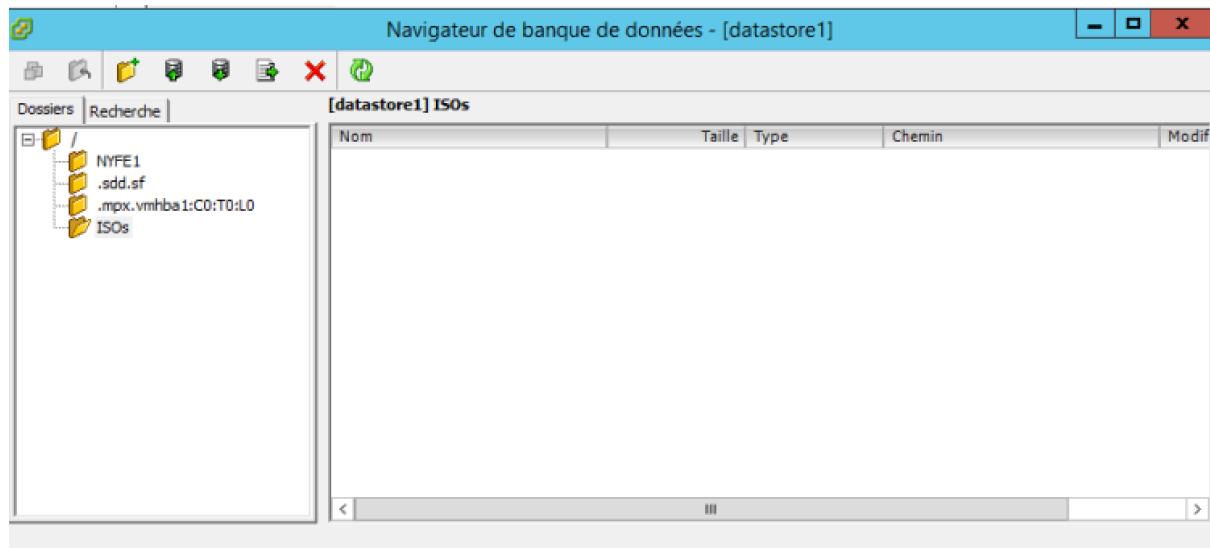


Notre machine virtuelle est désormais créée, il va maintenant falloir la faire démarrer sur l'ISO d'un Windows Server 2012 pour installer le système d'exploitation de ce dernier.

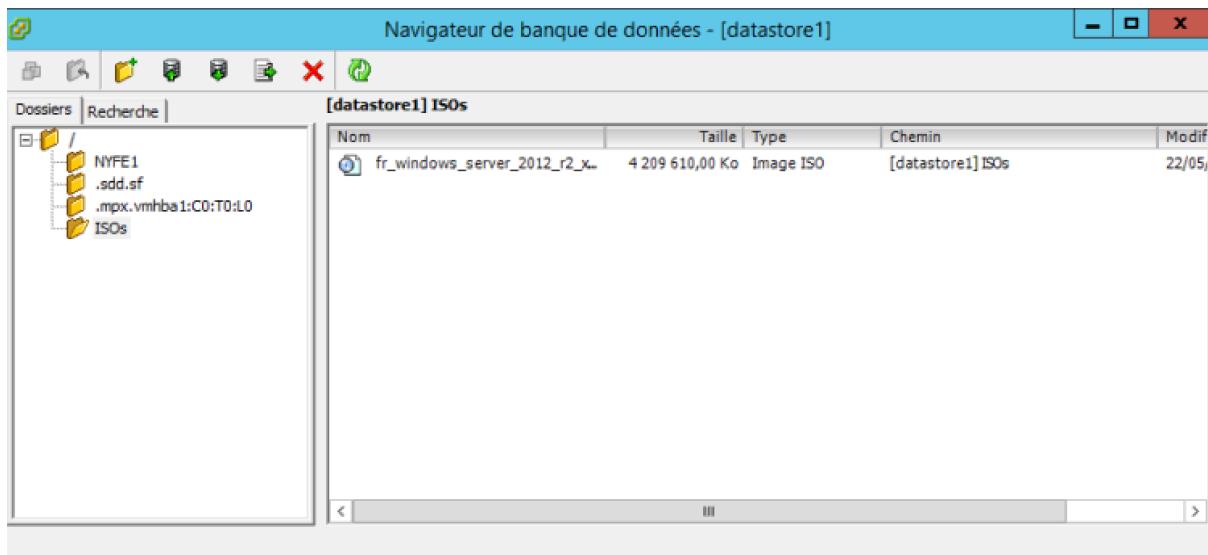
c) Installation du système d'exploitation

Pour installer notre système d'exploitation, il faut que notre ISO soit stockée sur le datastore de notre ESXi1. Pour cela, il faut aller l'uploader dedans.

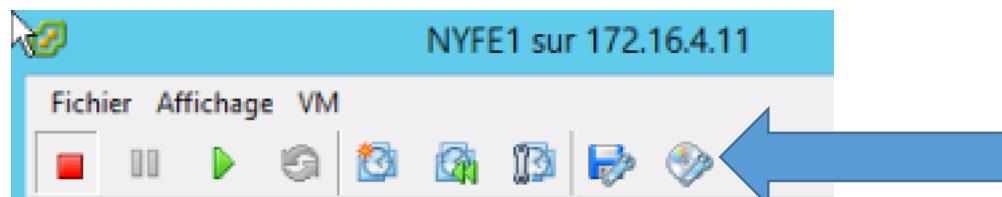
Cliquer sur l'ESXi1, puis se rendre dans l'onglet **Configuration**, enfin effectuer un clic-droit sur le datastore et cliquer sur **Parcourir la banque de données...**. Nous arrivons alors dans notre datastore :



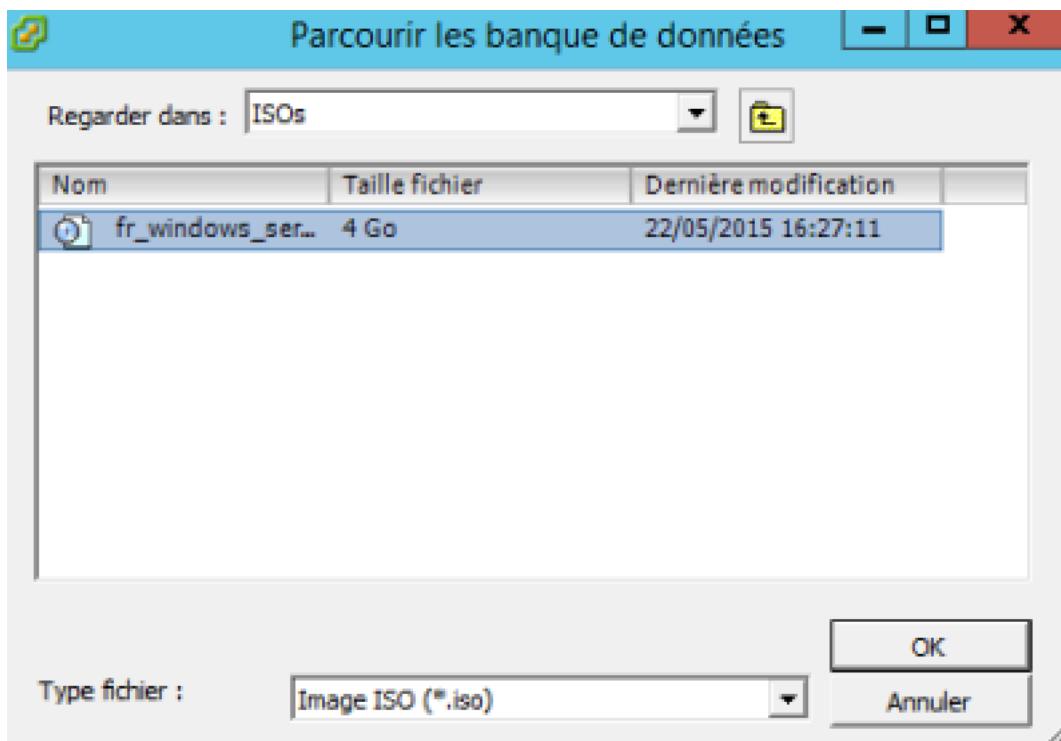
Comme on peut le voir, nous avons déjà créé un dossier **ISOs** pour stocker nos différentes ISOs. Se rendre dans ce dossier et cliquer sur l'icône **Télécharger fichiers vers cette BD**, vous pouvez alors chercher votre ISO et l'uploader sur votre datastore :



Effectuons alors un clic-droit sur notre nouvelle machine et cliquons sur **Ouvrir la console**. La console de la machine vient alors s'ouvrir, il faut ensuite sur **Connecter / déconnecter les périphériques CD/DVD de la machine** pour pouvoir booter la VM sur notre ISO :



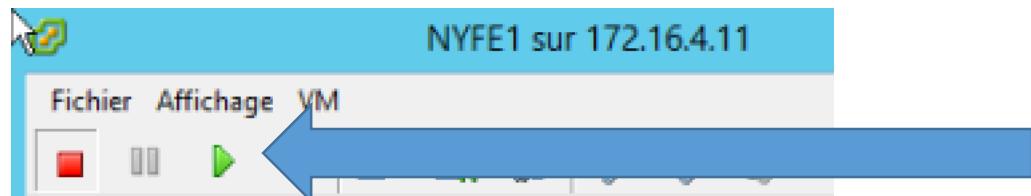
Puis cliquer sur **Connexion à une image ISO sur une banque de données**, puis en allant dans notre **datastore1** puis dans notre dossier **ISOs**, on peut aller chercher notre ISO :



Arrivé à ce niveau, il faut penser à configurer les performances de notre machine pour en pas qu'elle soit trop gourmande à son démarrage.

On peut ensuite cliquer sur **Connecter le CD/DVD**.

Nous pouvons alors lancer l'exécution de notre machine virtuelle en cliquant sur la petite flèche verte :



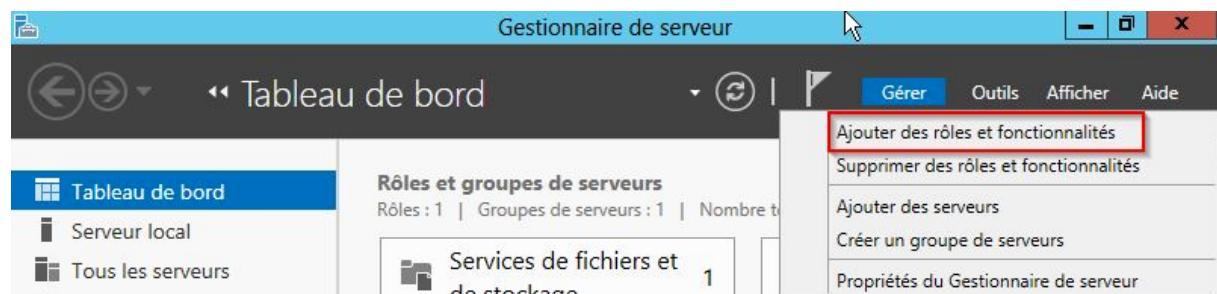
L'installation du système d'exploitation se fait alors normalement comme on a pu le voir dans la partie **1.B** de ce document.

Il faut ensuite changer le hostname de la machine, lui définir une adresse IP fixe et l'intégrer dans notre domaine comme on a pu le voir dans les parties **1.B.a) et 1.B.b)**.

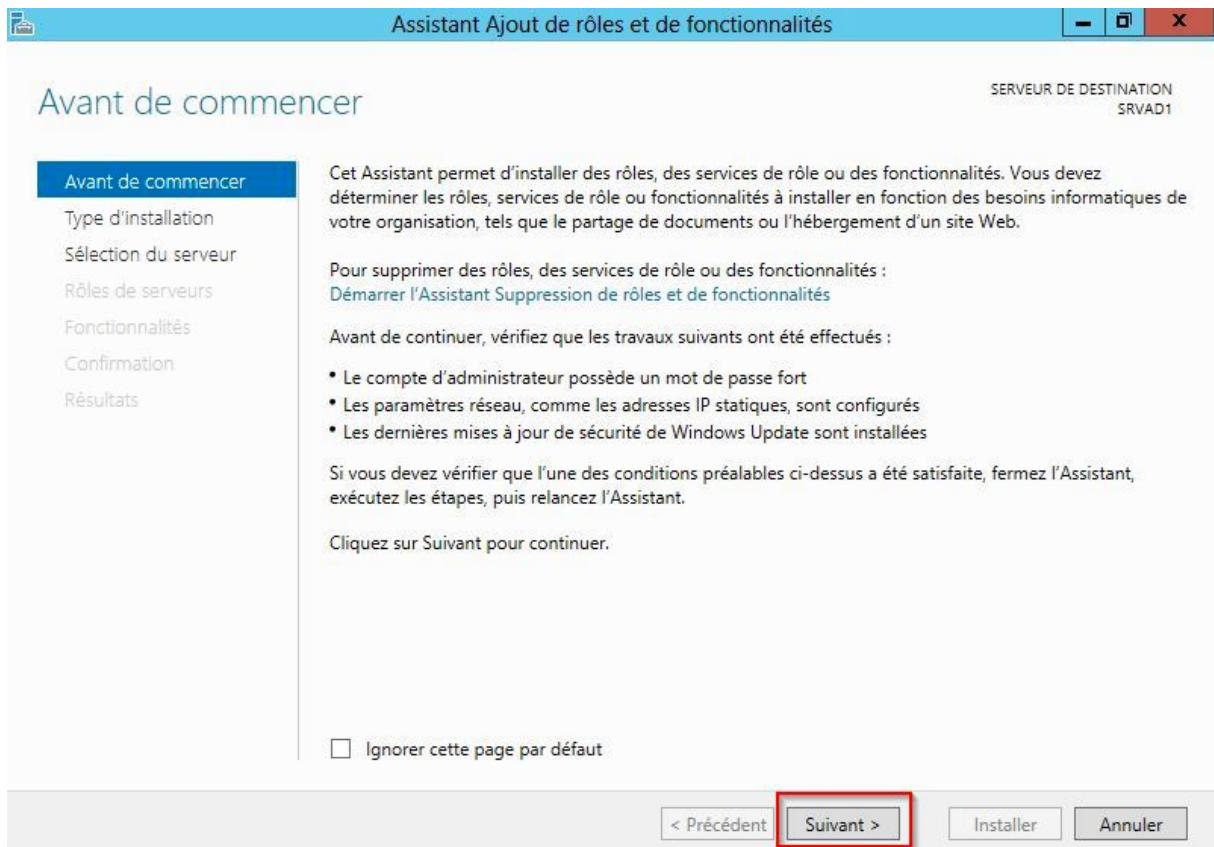
L'étape suivante consiste à installer le rôle IIS sur notre machine qui correspond au rôle de serveur Web.

d) Installation du rôle IIS

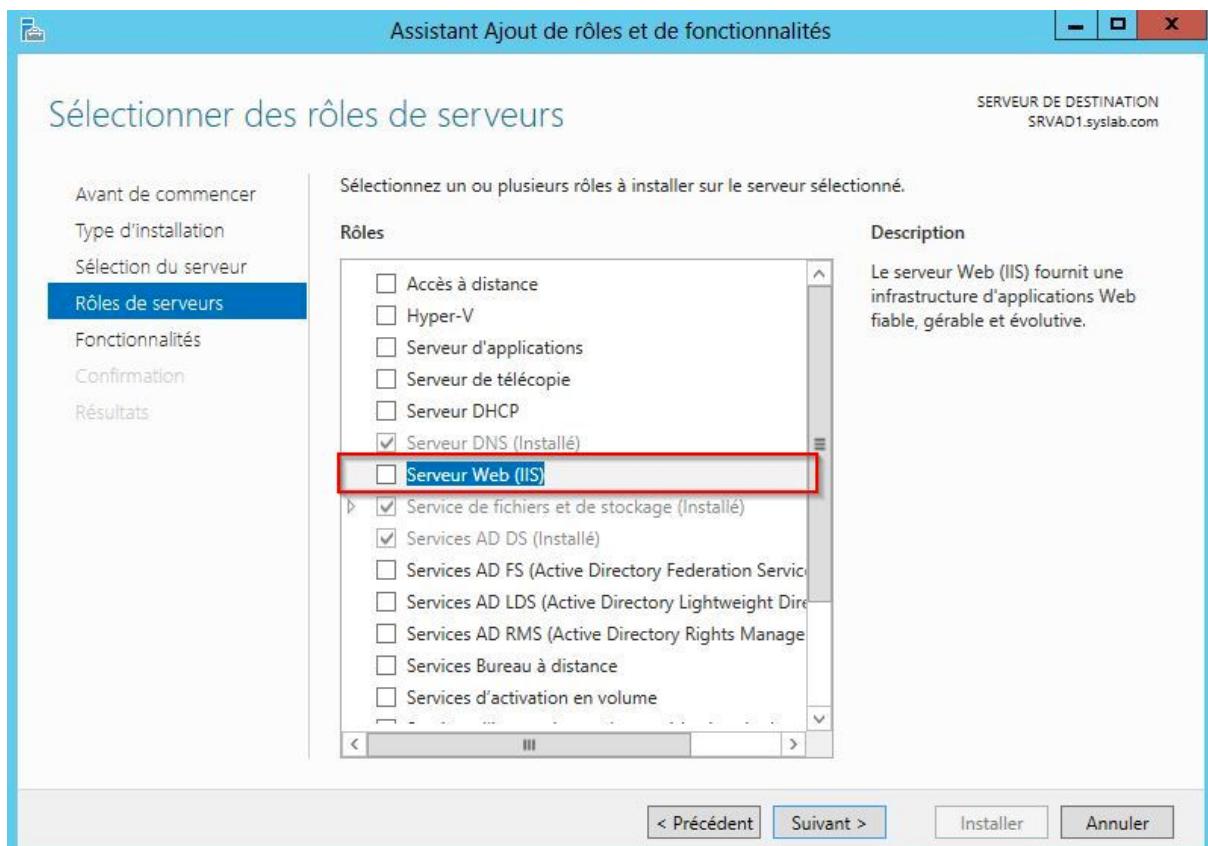
Depuis le Gestionnaire de serveur, cliquez sur **Gérer** puis sur **Ajouter des rôles ou des fonctionnalités** :



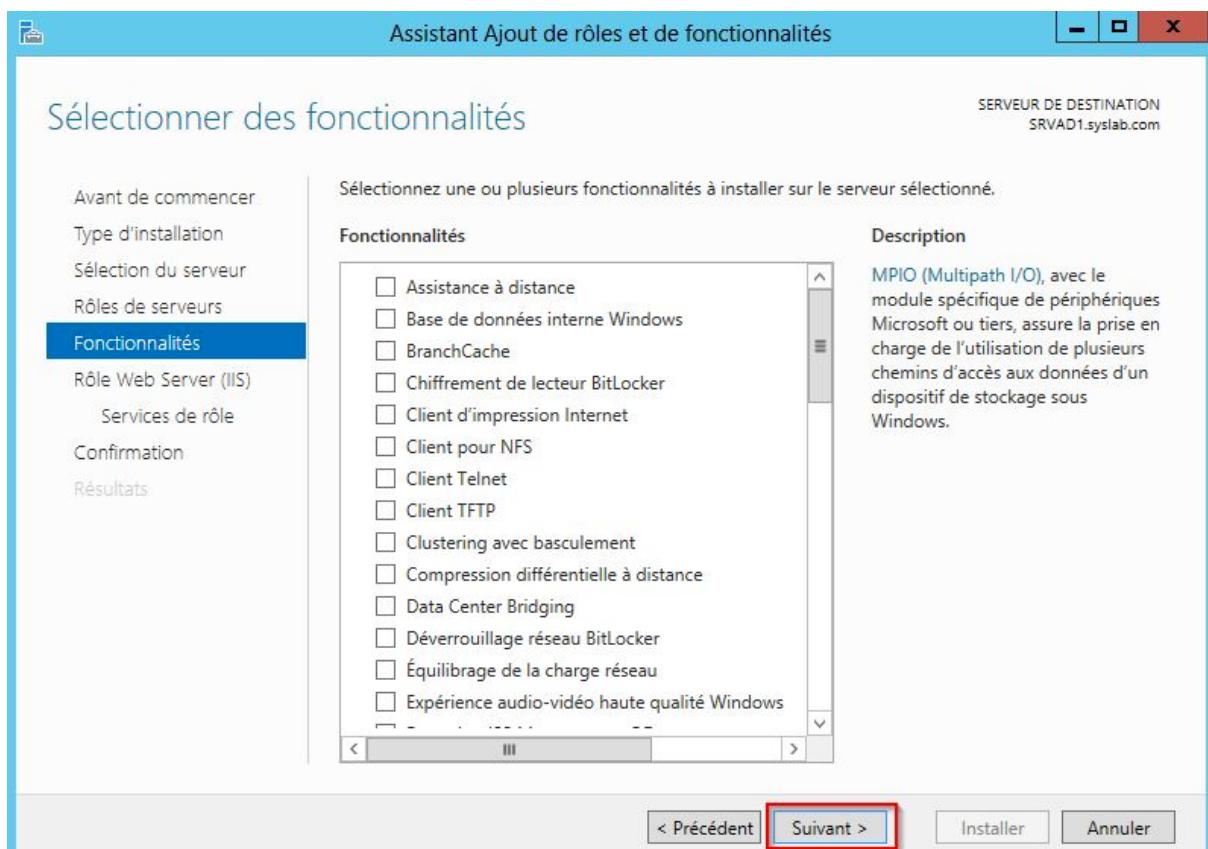
Une fenêtre apparaît avec diverses informations, cliquer sur **Suivant** :



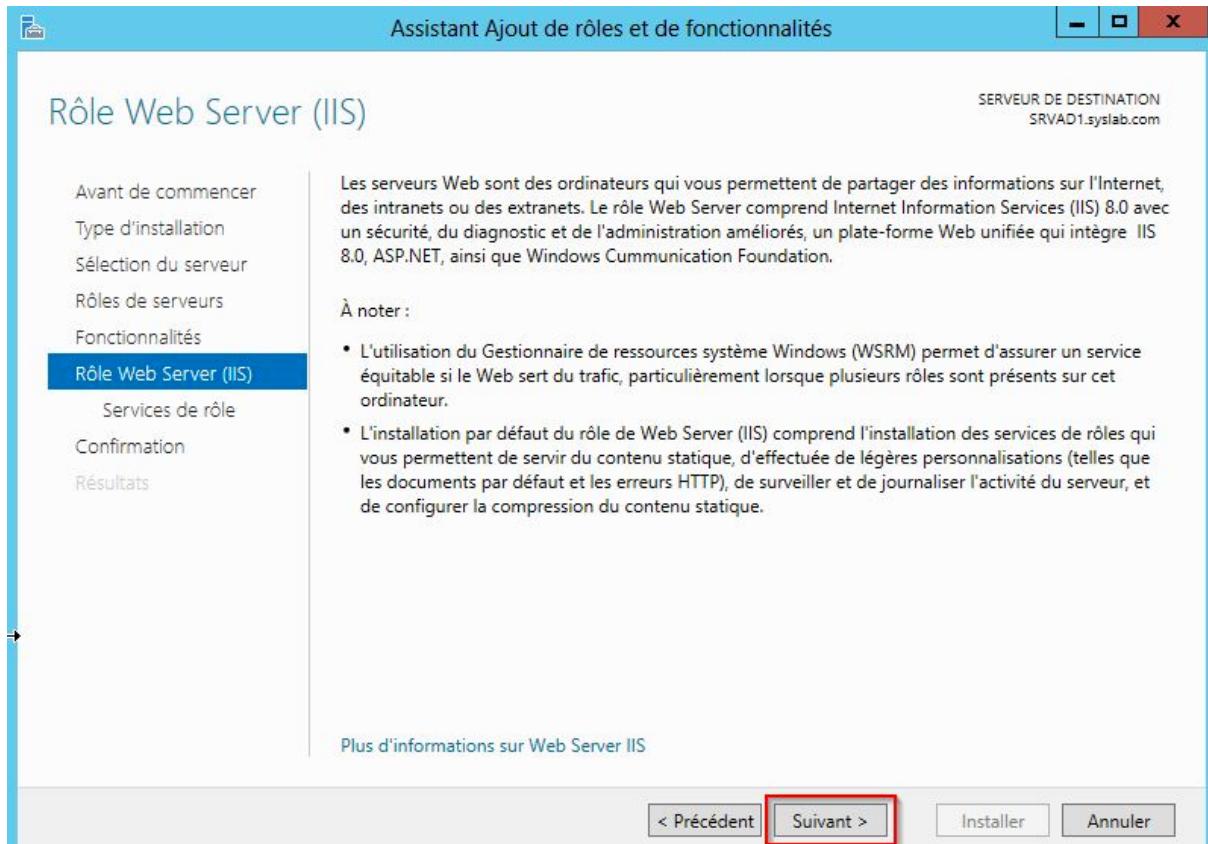
On laisse le type d'installation par défaut, on clique sur **suivant**, on vérifie qu'il s'agit bien de notre serveur et on clique sur **suivant**. Dans les rôles du serveur, on va aller chercher le rôle IIS et valider en cliquant sur **Ajouter des fonctionnalités**, cliquer alors sur **suivant** :



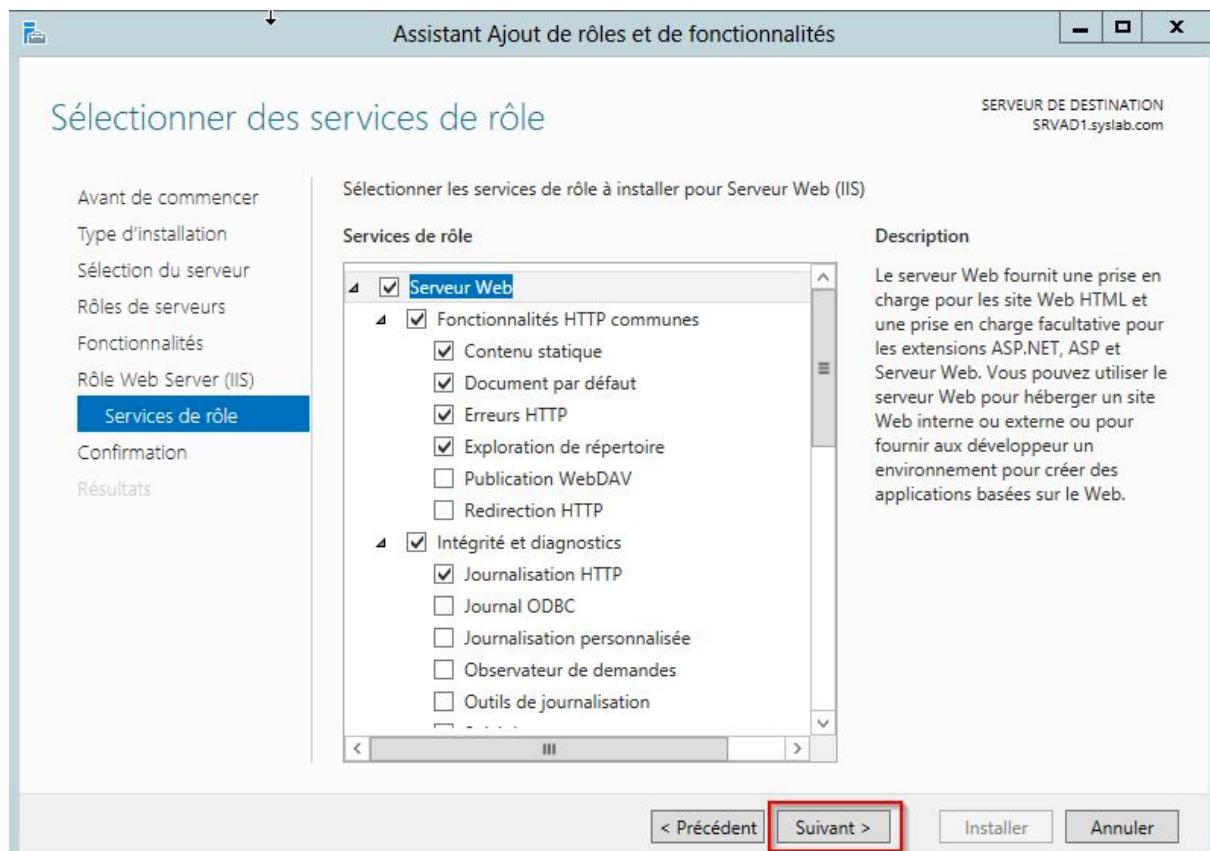
Pas de fonctionnalité supplémentaire à ajouter, on peut cliquer sur suivant :



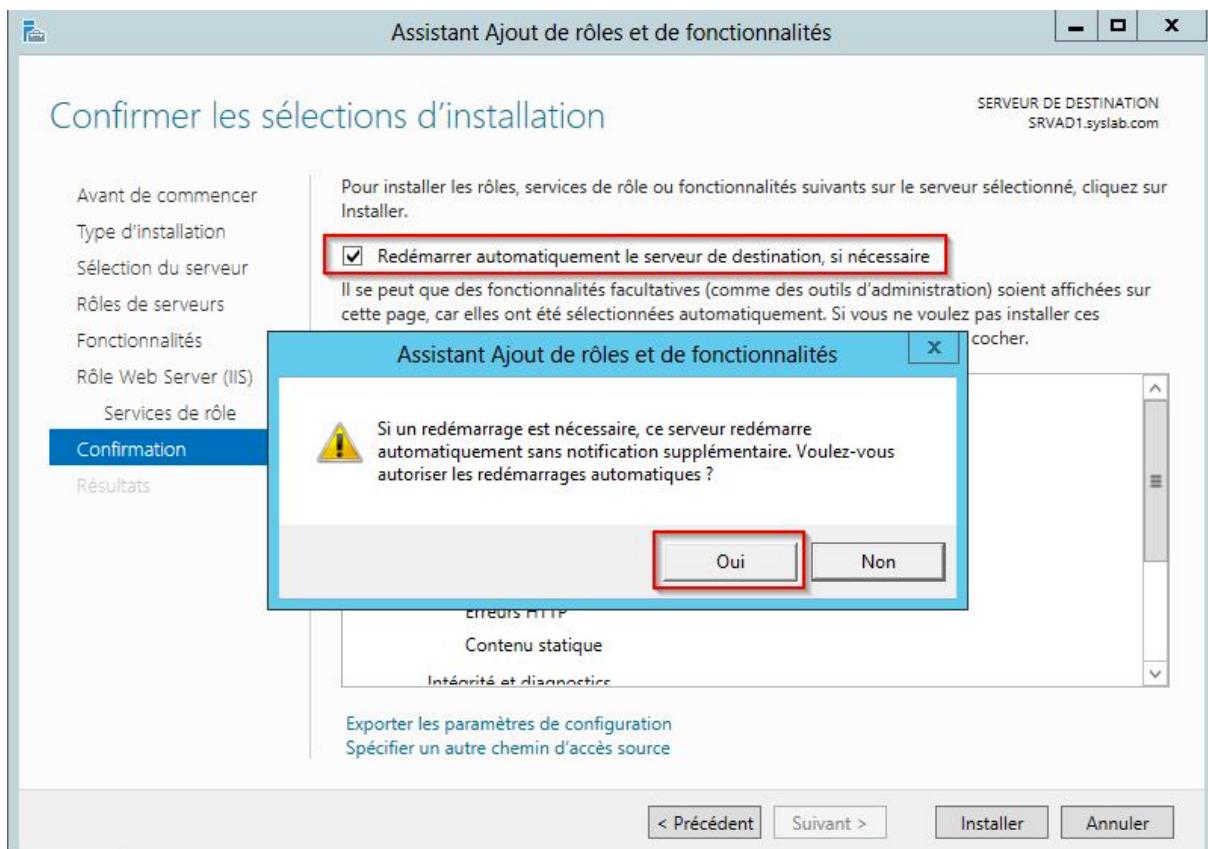
Une description du serveur Web IIS nous est donné dans la fenêtre suivante, cliquer sur **Suivant** :



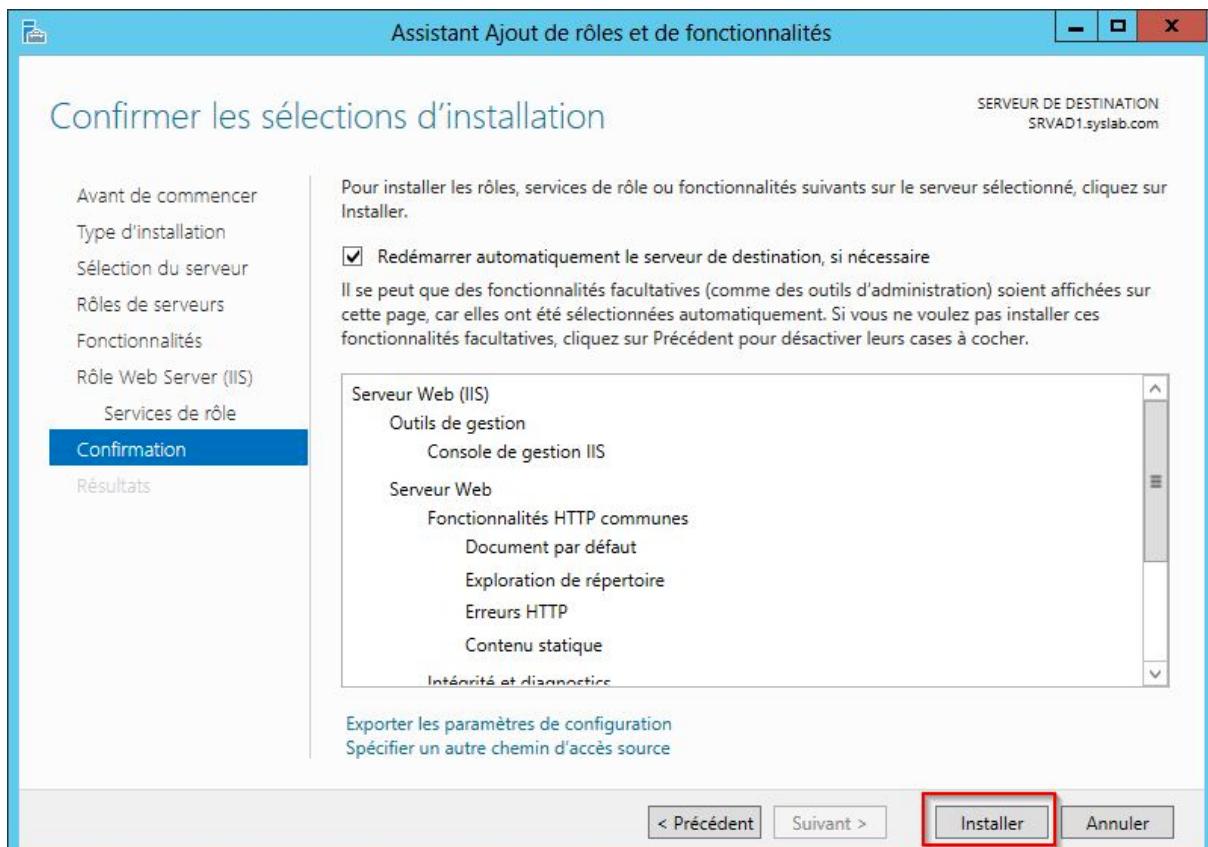
L'assistant liste alors les rôles qui vont être installés, cliquer sur **Suivant** :



Sur la fenêtre suivante, cocher la case **Redémarrer automatiquement le serveur de destination si nécessaire** puis cliquer sur **Oui** :



Enfin, cliquer sur **Installer** :



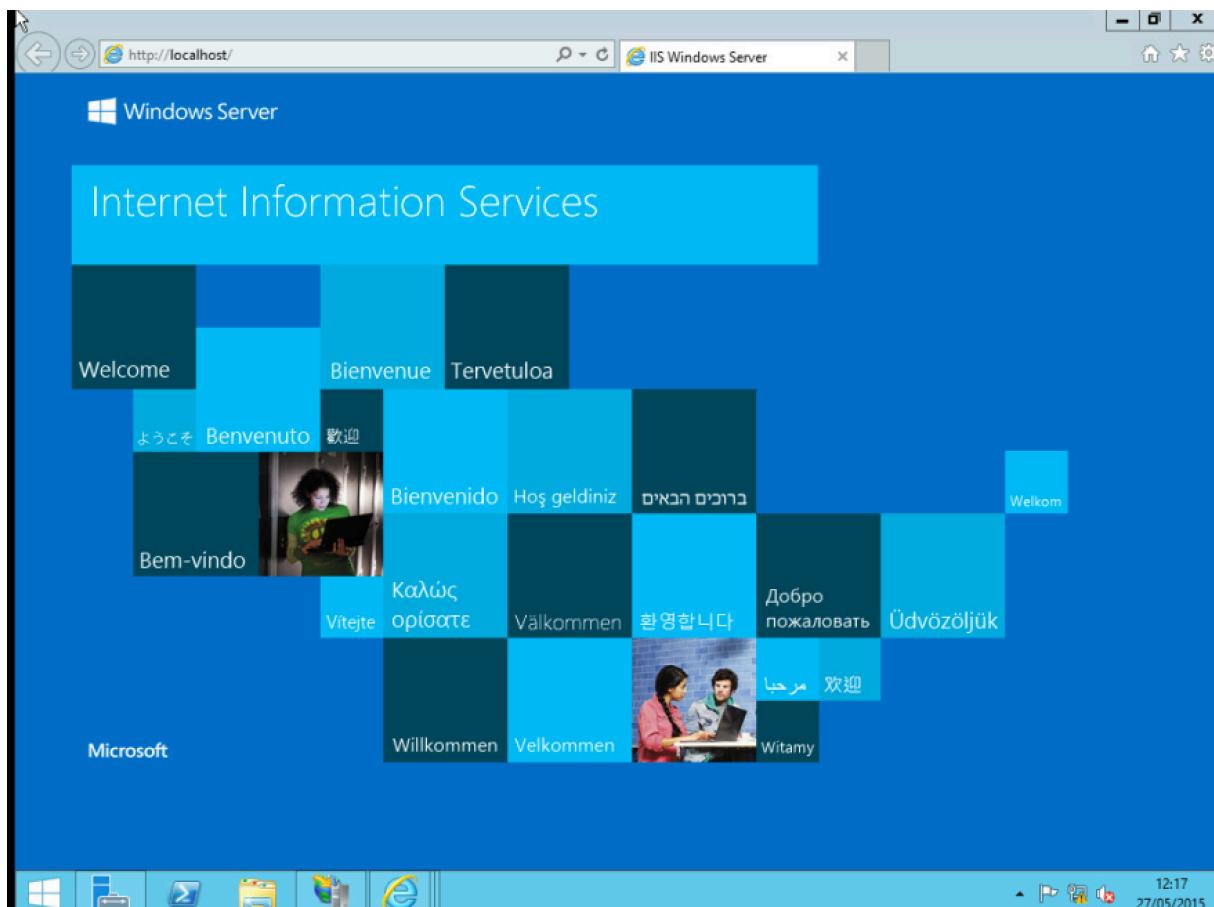
Une fois l'installation terminée et le serveur redémarré, on se rend dans l'onglet **IIS** du panneau de gauche puis en descendant dans la rubrique **Services**, on peut constater que de nouveaux services ont démarré :

Nom du serveur	Nom complet	Nom du service	Statut	Type de démarrage
NYFE1	Service de publication World Wide Web	W3SVC	En cours d'exécution	Automatique
NYFE1	Application Host Helper Service	AppHostSvc	En cours d'exécution	Automatique
NYFE1	Service d'activation des processus Windows	WAS	En cours d'exécution	Manuel

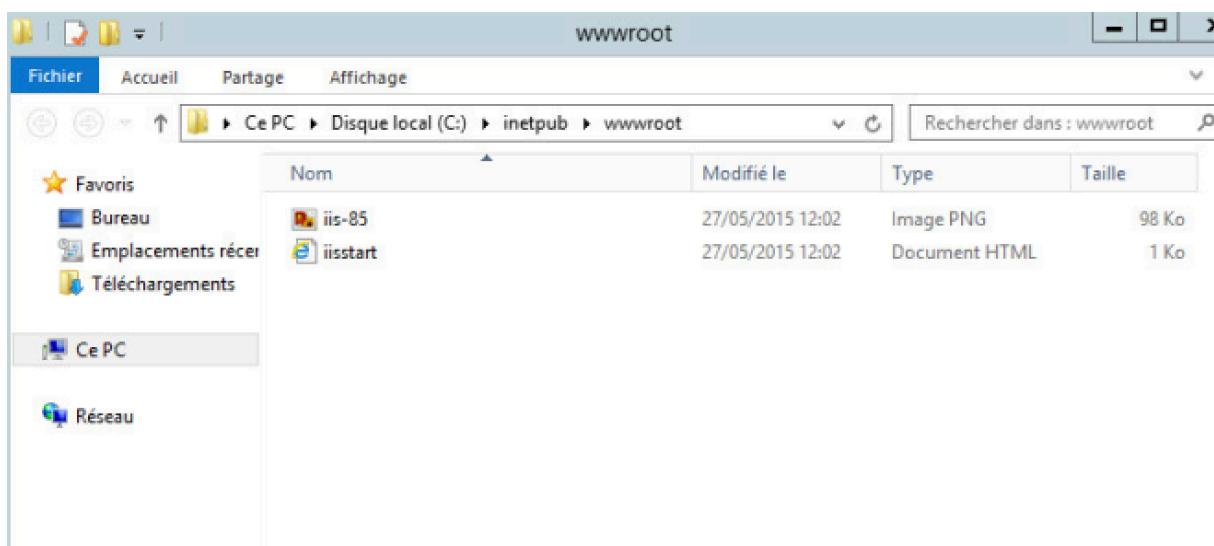
e) Accès à la console d'administration du IIS et test du site web par défaut

Pour cela rendons-nous dans le **Gestionnaire de serveur** puis dans l'onglet **Outils** cliquons sur **Gestionnaire des services Internet (IIS)**. Une nouvelle console s'affiche alors :

Pour tester le bon fonctionnement du site web par défaut, déployons l'arborescence de gauche et sélectionnons **Default Web Site**. Cliquons ensuite sur **Parcourir * :80 (http)** dans le volet de droite pour ouvrir la page du site par défaut :



Pour localiser l'emplacement des fichiers du site par défaut, effectuons un clic-droit sur **Default Web Site** et cliquons sur **Explorer**. L'explorateur Windows s'ouvre alors directement à l'emplacement des fichiers situés dans **C:/inetpub/wwwroot/** :



H. Installation et configuration d'un serveur WEB Back-End (NYBE1)

L'installation et la configuration de cette machine virtuelle est identique à celle vue dans la partie **1.F.a).b).c)** de ce document. Réitérer alors ces étapes en appliquant le bon hostname et la bonne adresse IP.

Dans la partie Back-end de notre infrastructure va tourner notre API qui requiert un serveur Node JS. Ce dernier sera installé après avoir créer le cluster des serveurs back-end.

I. Installation et configuration d'un serveur de Base de données (NYBDD1)

Enfin, pour compléter notre architecture trois-tiers, il nous manque notre serveur de base de données. On va pour cela créer une troisième machine virtuelle et installer un Windows Server 2012 Datacenter en guise de système d'exploitation comme précédemment fait dans les points **1.F.a).b).c).**

Pour terminer notre architecture trois-tiers, un serveur MongoDB va être installé plus tard, une fois que notre serveur NYBDD1 formera un cluster avec le serveur NYBDD2.

J. Création des machines NYFE2, NYBE2 et NYBDD2 attachées à NYESX2

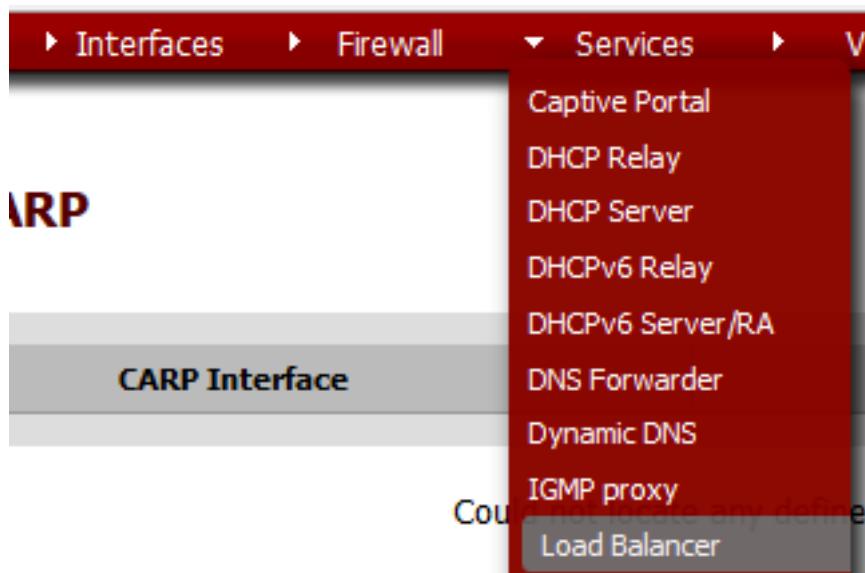
Reprendre les points **F, G et I** pour installer les machines NYFE2, NYBE2 et NYBDD2. La configuration des clusters pour chaque partie de l'architecture trois-tiers s'effectuera plus tard.

K. Load-balancing et Fail-Over des serveurs WEB (Front-end)

Afin d'assurer une répartition de charge et une haute disponibilité de notre service Web, nous allons configurer un pool de load-balancing pour nos serveurs web sur nos routeurs pfSense.

a) Création du pool de load-balancing

On va commencer par créer un pool, c'est à dire un groupe, dans lequel nous mettrons ensuite nos serveurs. On se rend donc dans **Services** puis dans **Load Balancer** :



On se retrouve ensuite face à un tableau qui est le tableau de gestion des Pools. On cliquera sur le + à droite de ce tableau pour en créer un nouveau :

Services: Load Balancer: Pool

Name	Mode	Servers	Port	Monitor	Description
------	------	---------	------	---------	-------------

On arrivera sur un formulaire sur lequel on pourra créer notre pool de serveur :

Name	Pool_serveur_web
Mode	Load Balance
Description	Pool des serveurs web.
Port	80 This is the port your servers are listening on. You may also specify a port alias listed in Firewall -> Aliases here.
Retry	3 Optionally specify how many times to retry checking a server before declaring it down.

Dans ce nouveau formulaire nous allons remplir le premier cadre dans lequel nous saisirons le nom de notre Pool, le mode (ici **Load-Balance**), éventuellement une description et le port sur lequel il agira. On saisi ensuite la valeur **Retry** qui permet d'indiquer combien de fois un serveur va être vérifié avant d'être déclaré hors service. Ici "3" signifie qu'au bout de 3 réponses de suite invalides de la part d'un serveur, celui-ci sera considéré comme hors service et s'appliquera alors le Fail-over, le seul serveur restant prendra toute la charge :

Monitor	HTTP	
Server IP Address	172.16.4.30	Add to pool

Current Pool Members							
Members	<table border="1"> <tr> <td>Pool Disabled</td> <td>></td> <td>Enabled (default)</td> </tr> <tr> <td><input type="button" value="Remove"/></td> <td><</td> <td><input type="button" value="Remove"/></td> </tr> </table>	Pool Disabled	>	Enabled (default)	<input type="button" value="Remove"/>	<	<input type="button" value="Remove"/>
Pool Disabled	>	Enabled (default)					
<input type="button" value="Remove"/>	<	<input type="button" value="Remove"/>					
<input type="button" value="Save"/> <input type="button" value="Cancel"/>							

Puis on ajoutera les différentes IP de nos serveurs web. Ici j'en ai deux, je les saisis puis cliquer sur **Add to pool**. On cliquera ensuite sur **Save** puis sur **Apply Change** sur la page suivante. On pourra alors voir un récapitulatif de notre pool dans le tableau des Pools :

Pools Virtual Servers Monitors Settings

Name	Mode	Servers	Port	Monitor	Description
Pool_serveur_web	loadbalance	172.16.4.20 172.16.4.30	80	HTTP	Pool des serveurs web

b) Instanciation du serveur virtuel

Maintenant que notre pool est créé, nous allons faire ce que l'on appelle un serveur virtuel. C'est un serveur qui va représenter notre pool sur l'interface WAN sur lequel les requêtes web client arrivons. On va se rendre dans le tableau **Virtual Server** puis cliquer sur le + à droite du tableau pour arriver sur ce formulaire :

Edit Load Balancer - Virtual Server entry

Name	VS_WEB
Description	
IP Address	10.0.0.254
This is normally the WAN IP address that you would like to be forwarded to the pool cluster. You may also specify a host alias listed in Firewall -> Alias.	
Port	80
This is the port that the clients will connect to. All connections will be forwarded to the pool cluster. If left blank, listening ports from the pool will be used. You may also specify a port alias listed in Firewall -> Alias.	
Virtual Server Pool	Pool_serveur_web
Fall Back Pool	none
The server pool to which clients will be redirected if *ALL* ports are busy. This option is NOT compatible with the DNS relay protocol.	
Relay Protocol	tcp
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

On renseigne un nom, l'adresse IP sur laquelle les requêtes clients arriveront. Ici, il s'agit de l'adresse IP WAN du cluster Pfsense. On va ensuite lier notre pool web à ce serveur virtuel et indiquer le protocole de transport qui est ici TCP. Une fois de plus nous cliquerons sur **Submit** puis sur **Apply Change** :

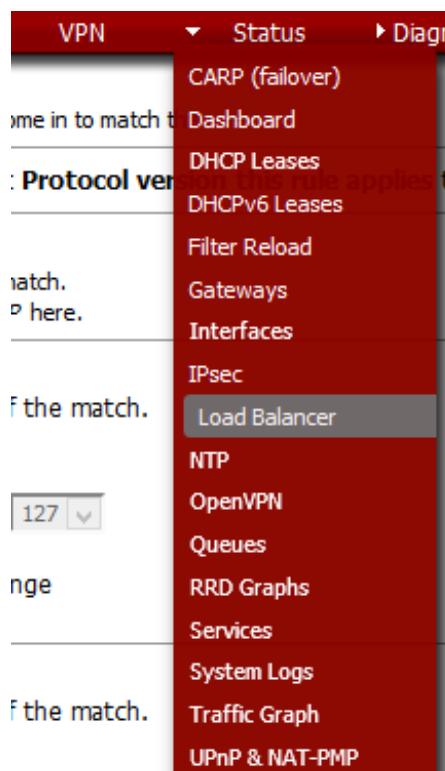
Pools	Virtual Servers	Monitors	Settings			
Name	Protocol	IP Address	Port	Pool	Fall Back Pool	Description
VS_WEB	tcp	10.0.0.254	80	Pool_serveur_web	none	

Dans notre cas, les requêtes arrivent de l'extérieur, il faut donc créer une règle qui permettra aux requêtes d'arriver et d'être acceptées. Nous allons donc dans **Firewall** puis **Rules** on cliquera sur le + à droite du tableau pour ajouter une règle :

The screenshot shows the 'Destination port range' configuration section. It includes fields for 'from:' (set to 'HTTP') and 'to:' (also set to 'HTTP'), both with dropdown menus. Below these fields is a descriptive note: 'Specify the port or port range for the destination of the packet for Hint: you can leave the 'to' field empty if you only want to filter a single port'.

c) Vérification

Pfsense met en place différents outils permettant de voir l'état du Pool de serveur. On peut aller dans **Status** puis dans **Load Balancer** :



Ici on verra l'état des serveurs du pools ainsi que leur disponibilité actuelle et cumulée. Le pourcentage présent représente le temps global de disponibilité de chacun des serveurs par rapport au protocole de vérification indiqué :

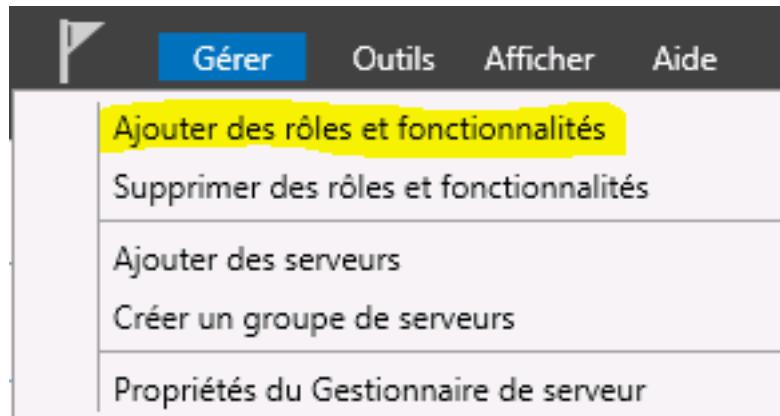
Pools	Virtual Servers			
Name	Mode	Servers	Monitor	Description
Pool_serveur_web	Load balancing	<input checked="" type="checkbox"/> 172.16.4.20:80 (100.00%) <input checked="" type="checkbox"/> 172.16.4.30:80 (96.30%)	HTTP	Pool des serveurs web
Save	Reset			

Nous verrons plus globalement dans l'onglet **Virtual Servers** l'état actuelle du ou des serveurs virtuels :

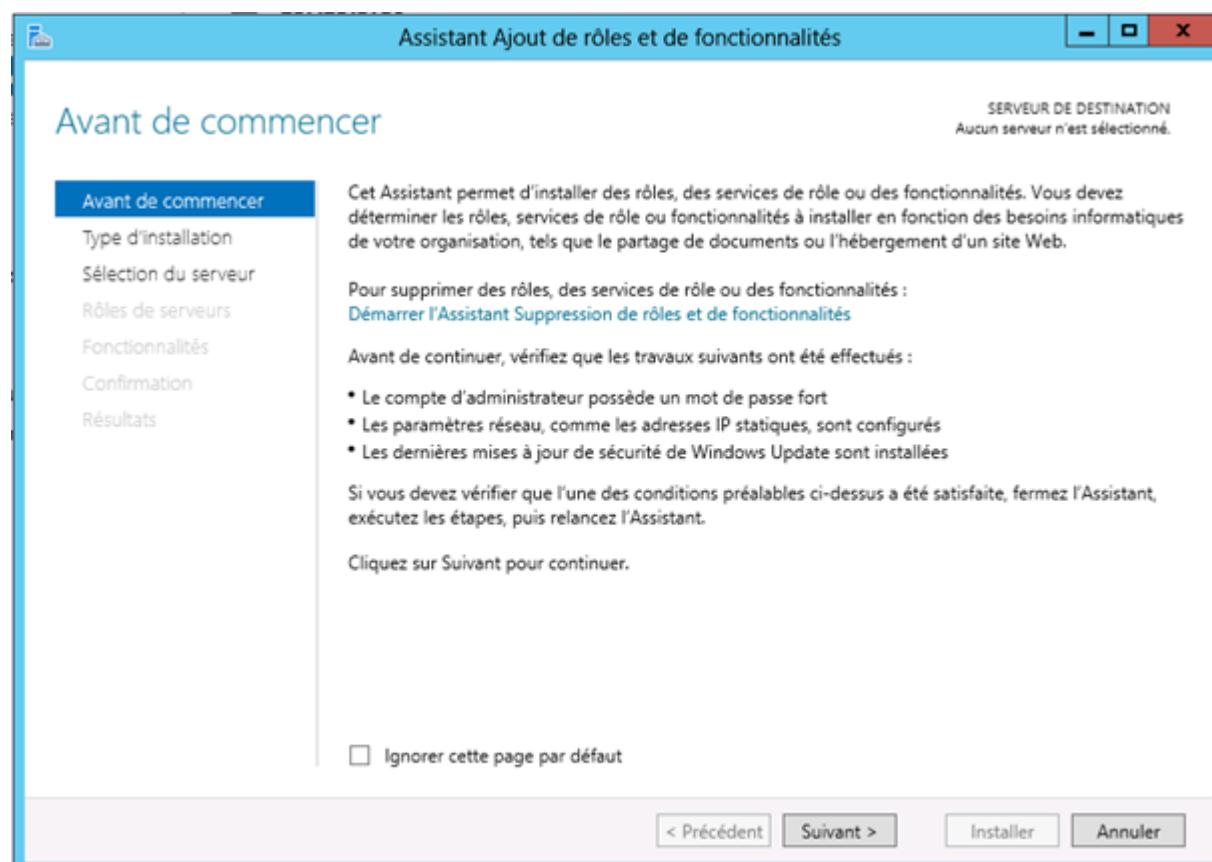
Pools	Virtual Servers		
Name	Address	Servers	Status
VS_WEB	10.0.0.254 : 80	172.16.4.20 172.16.4.30	Active

L. Clustering des serveurs de l'architecture trois-tiers

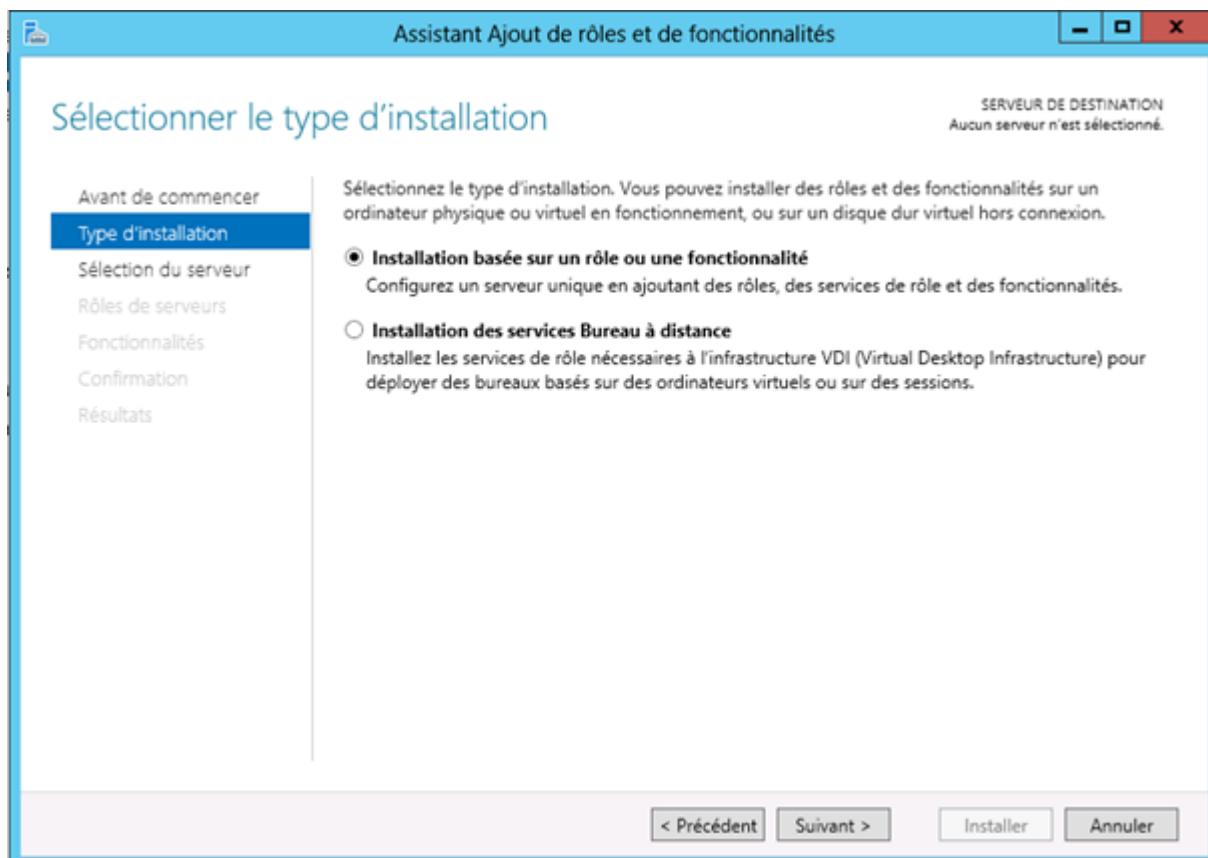
Afin de déployer les clusters des trois niveaux de notre architecture trois-tiers, nous allons commencer par ouvrir le **Gestionnaire de serveur**. Cliquons sur **Gérer** puis sur **Ajouter des rôles et fonctionnalités** :



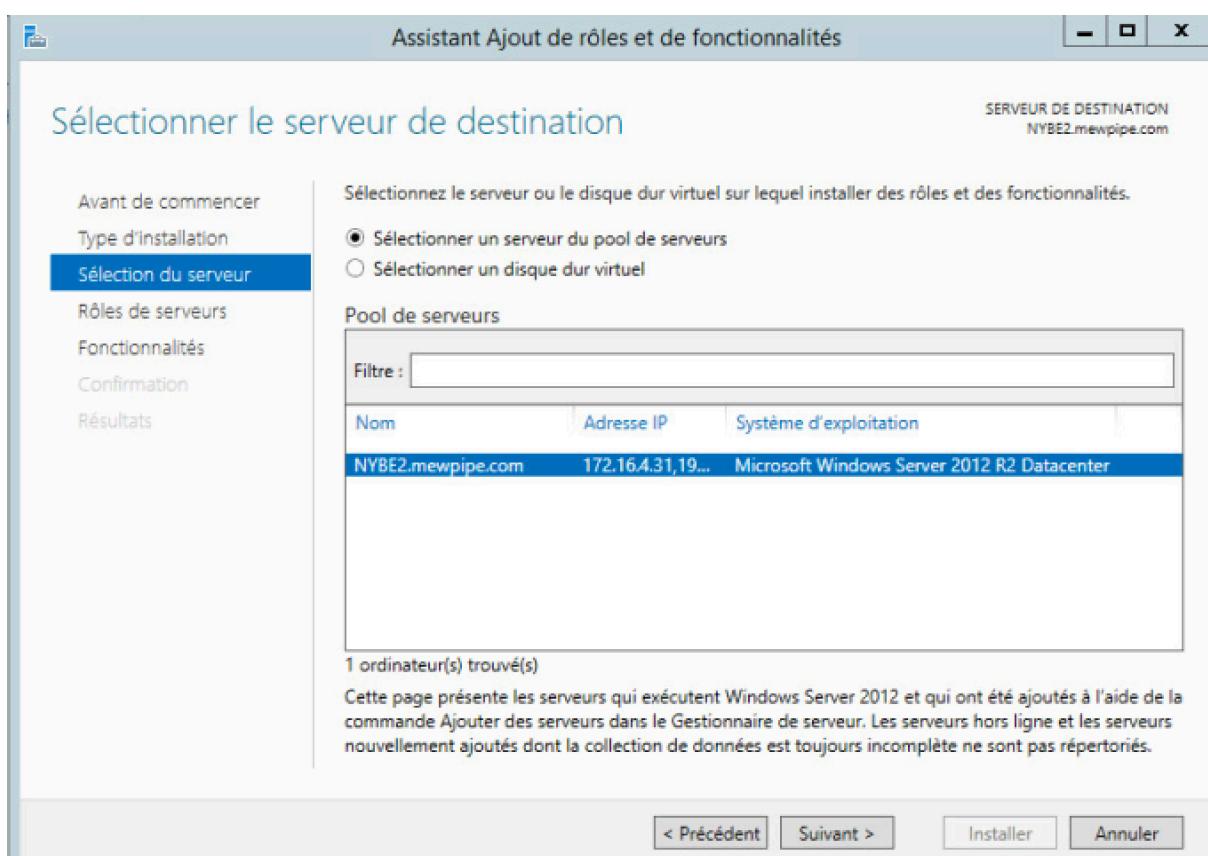
Dans le fenêtre qui vient de s'ouvrir, cliquons sur **Suivant** :



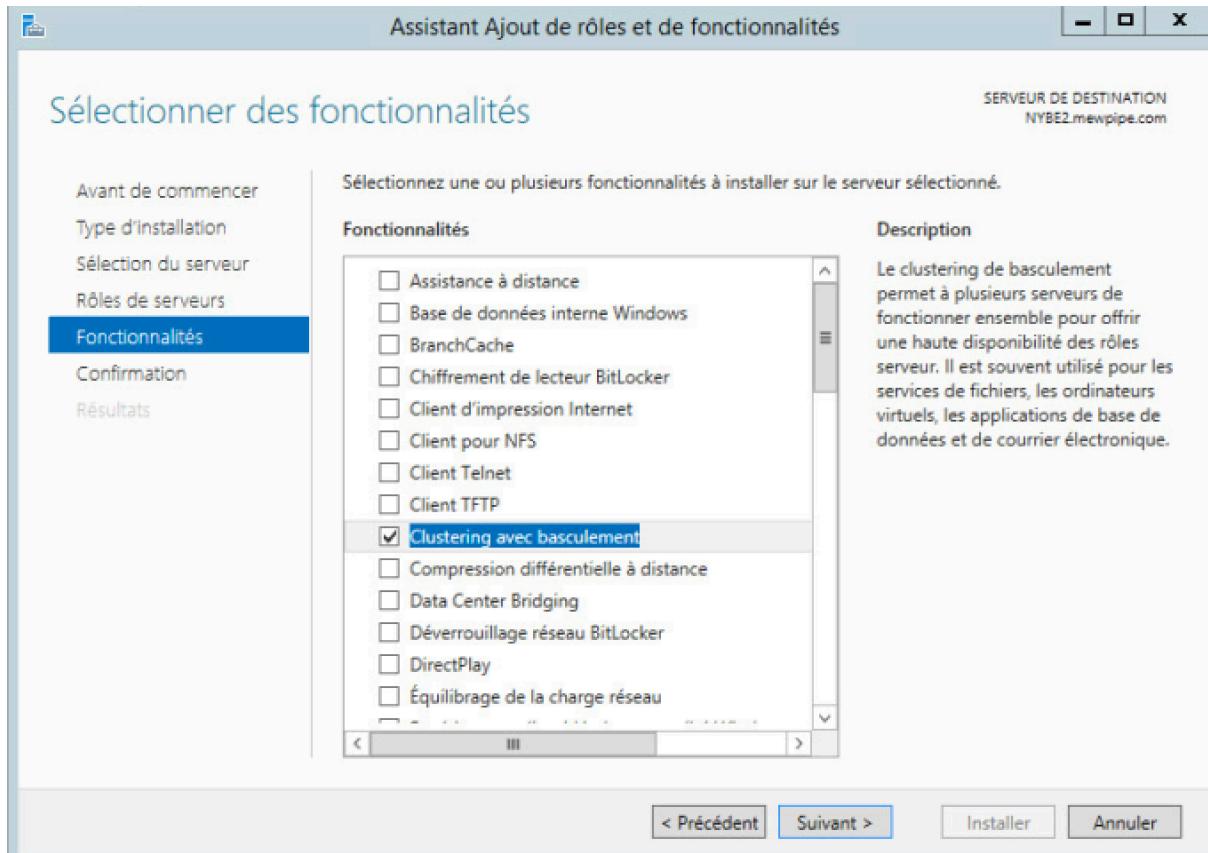
Nous choisissons ensuite l'option **Installation basée sur un rôle ou une fonctionnalité**. On clique sur **Suivant** :



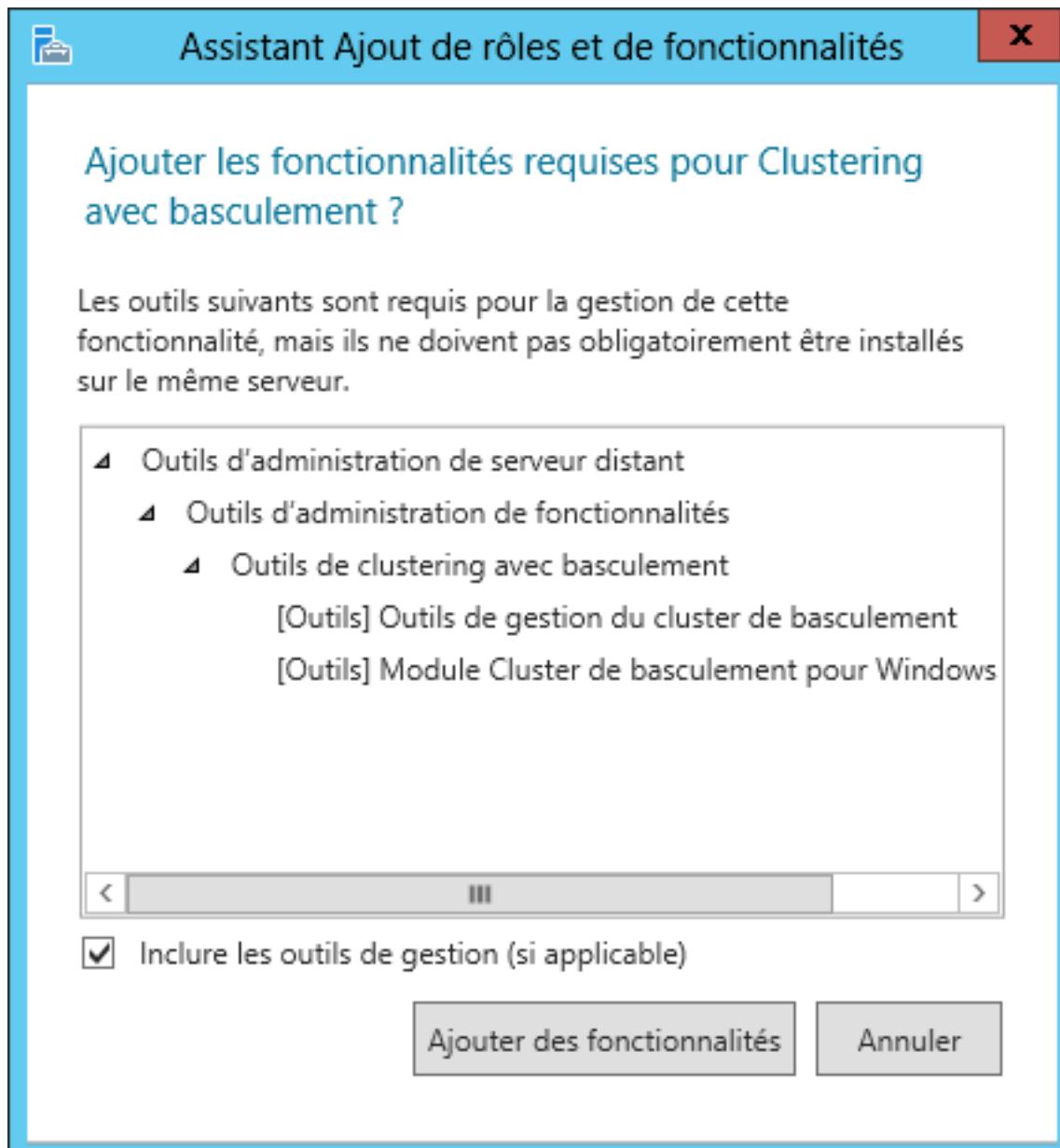
On vérifie que l'assistant a bien sélectionnée notre serveur et on clique sur **Suivant** :



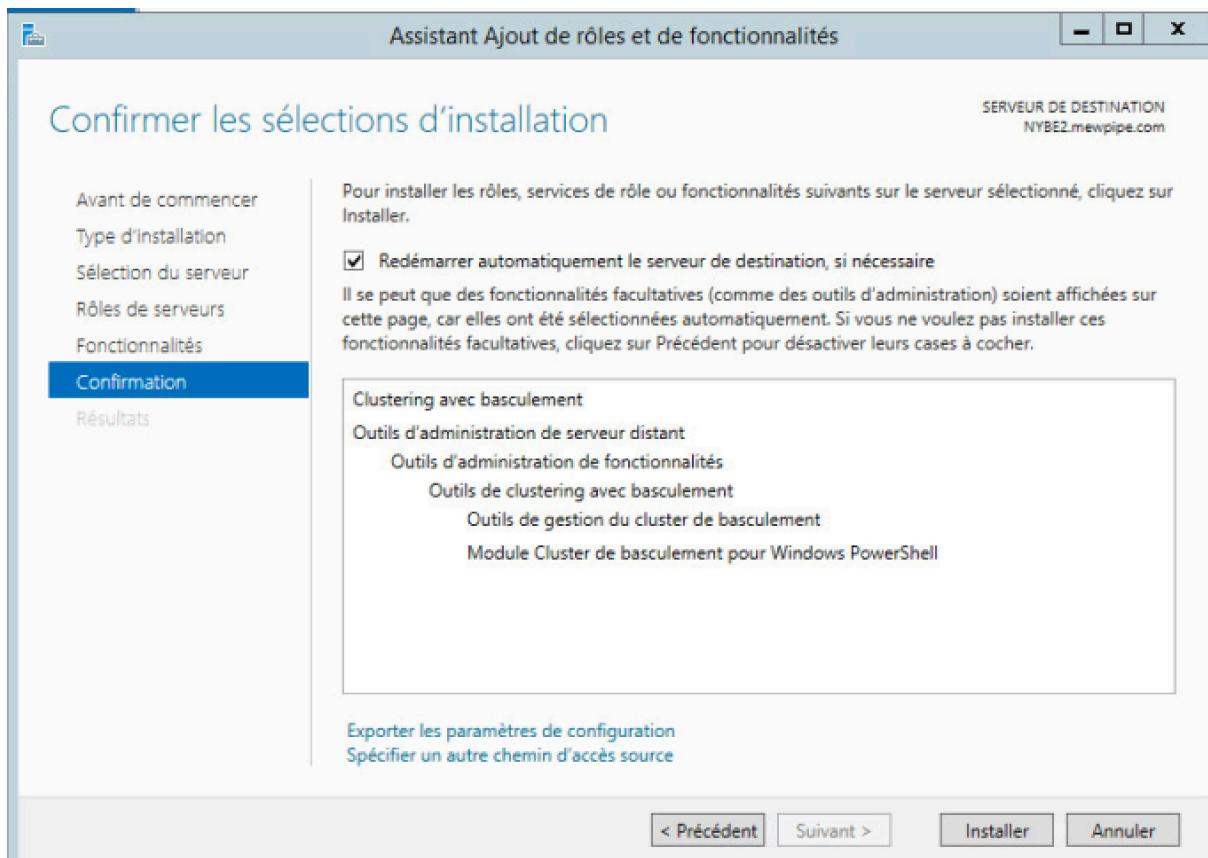
On clique sur **Suivant** et on sélectionne la fonctionnalité **Clustering avec basculement** :



On confirme en cliquant sur **Ajouter des fonctionnalités** :

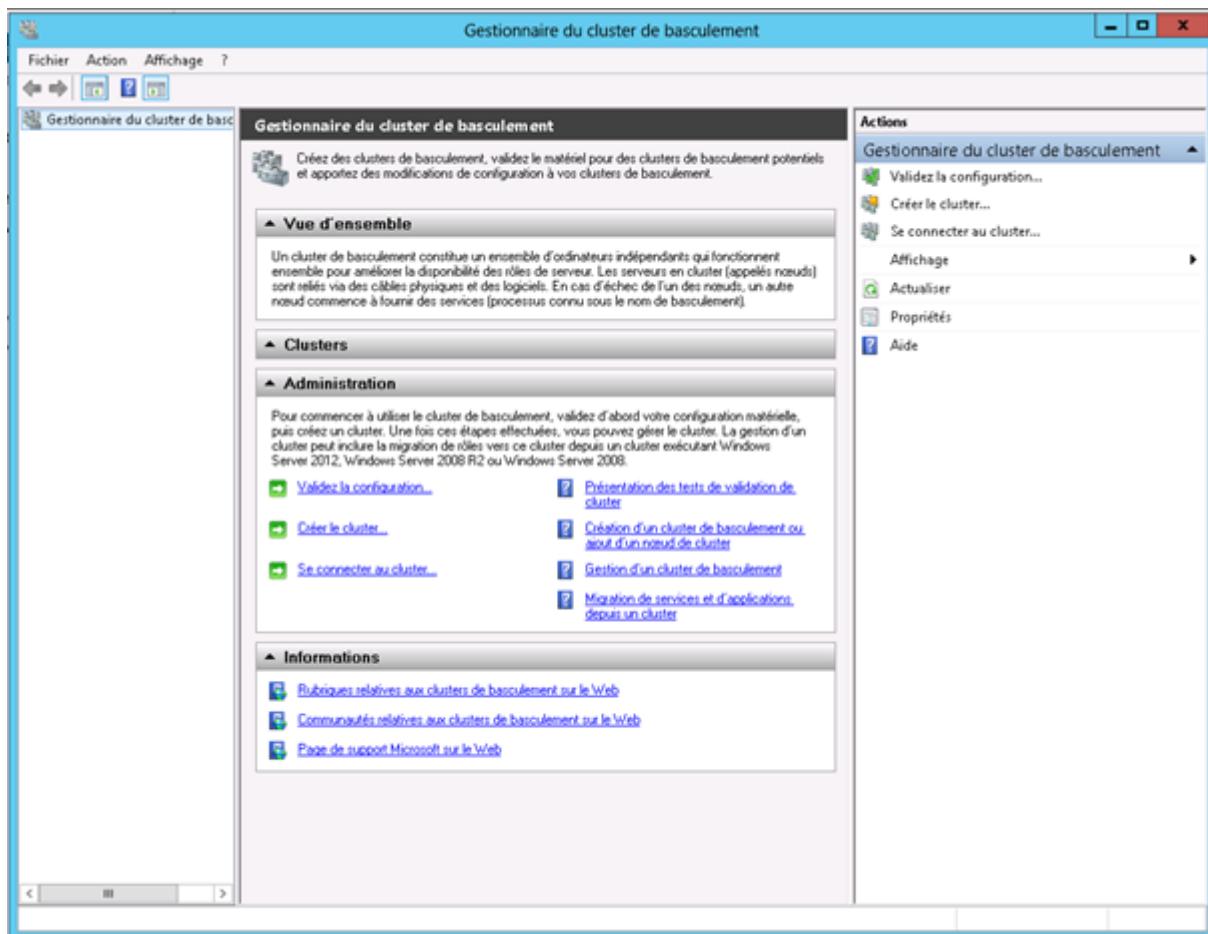


On coche la case **Redémarrer automatiquement le serveur de destination si nécessaire**. Cliquons sur **Installer** :



On procède à la même installation sur le second serveur back-end.

Une fois l'installation terminée, on ouvre le **Gestionnaire du cluster de basculement** :



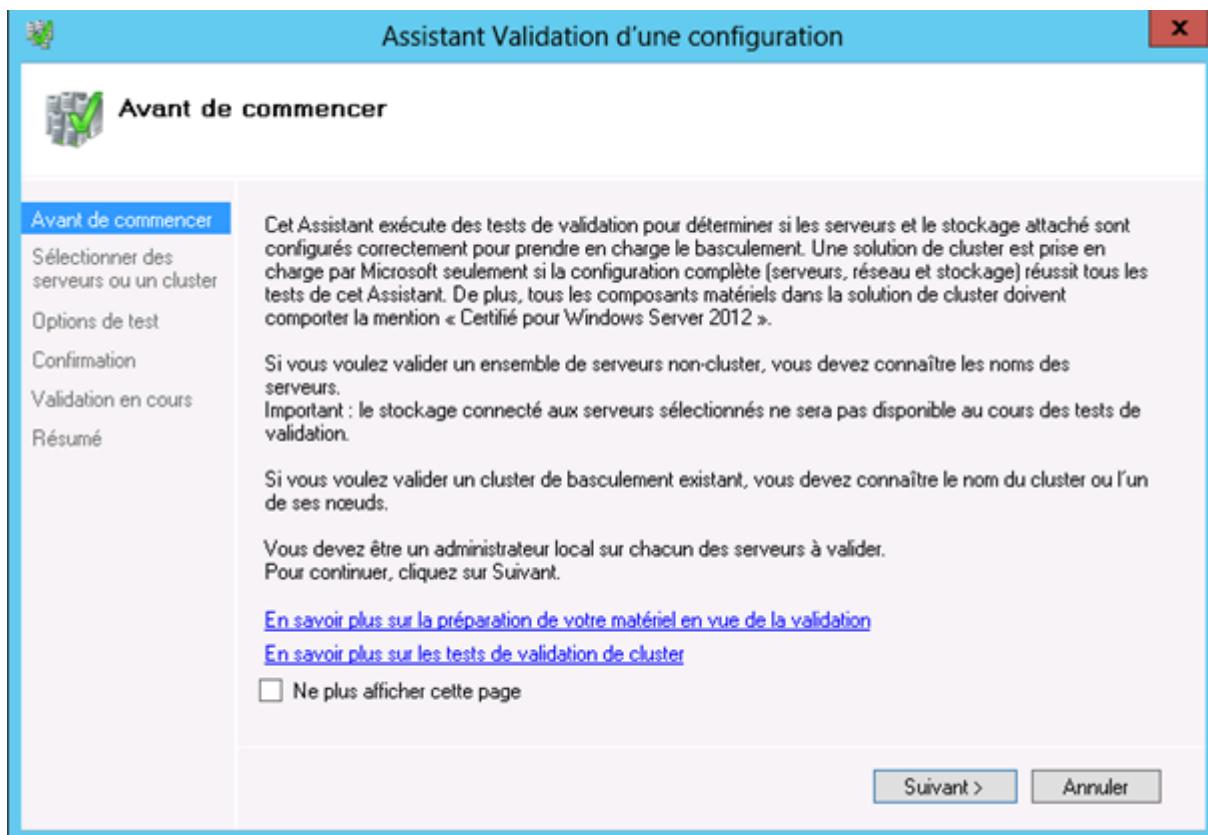
On clique sur **Valider la configuration** :

Administration

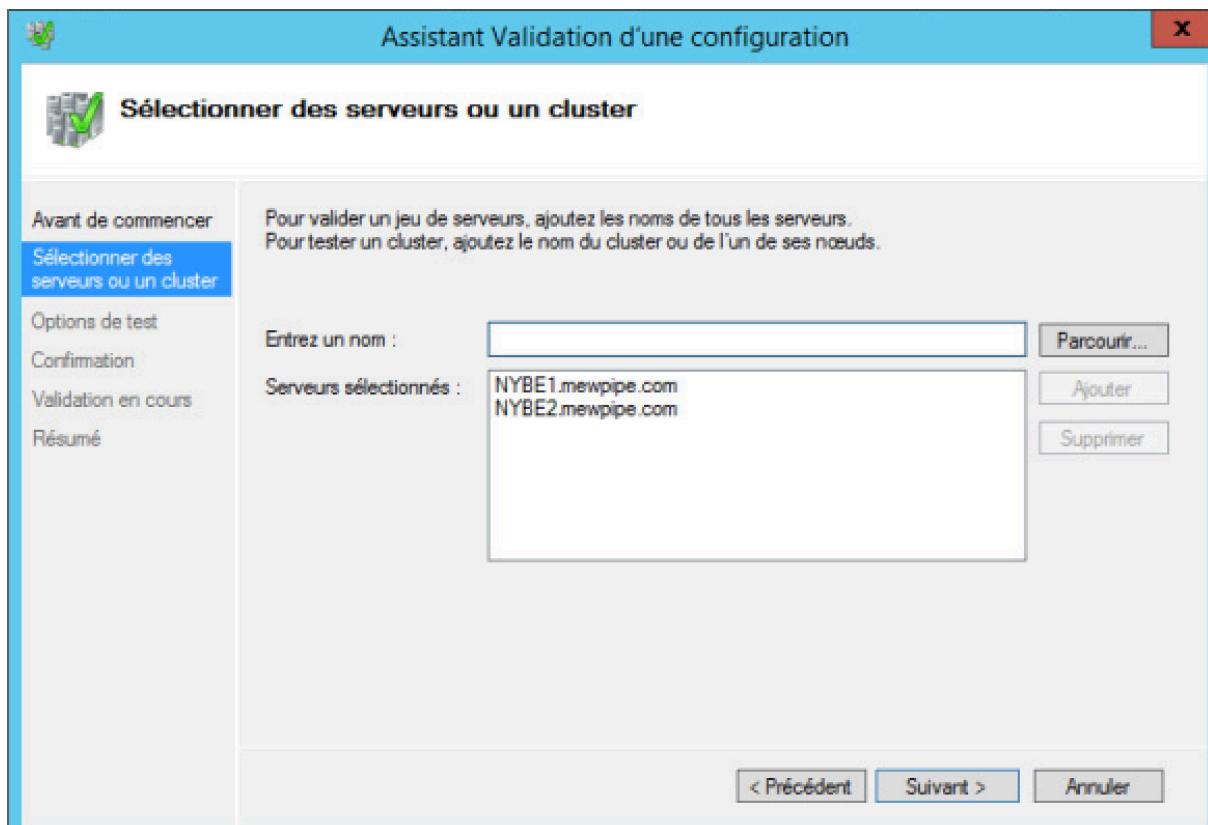
Pour commencer à utiliser le cluster de basculement, validez d'abord votre configuration matérielle, puis créez un cluster. Une fois ces étapes effectuées, vous pouvez gérer le cluster. La gestion d'un cluster peut inclure la migration de rôles vers ce cluster depuis un cluster exécutant Windows Server 2012, Windows Server 2008 R2 ou Windows Server 2008.

➡ Validez la configuration... ➡ Créer le cluster... ➡ Se connecter au cluster...	? Présentation des tests de validation de cluster ? Création d'un cluster de basculement ou ajout d'un nœud de cluster ? Gestion d'un cluster de basculement ? Migration de services et d'applications depuis un cluster
---	---

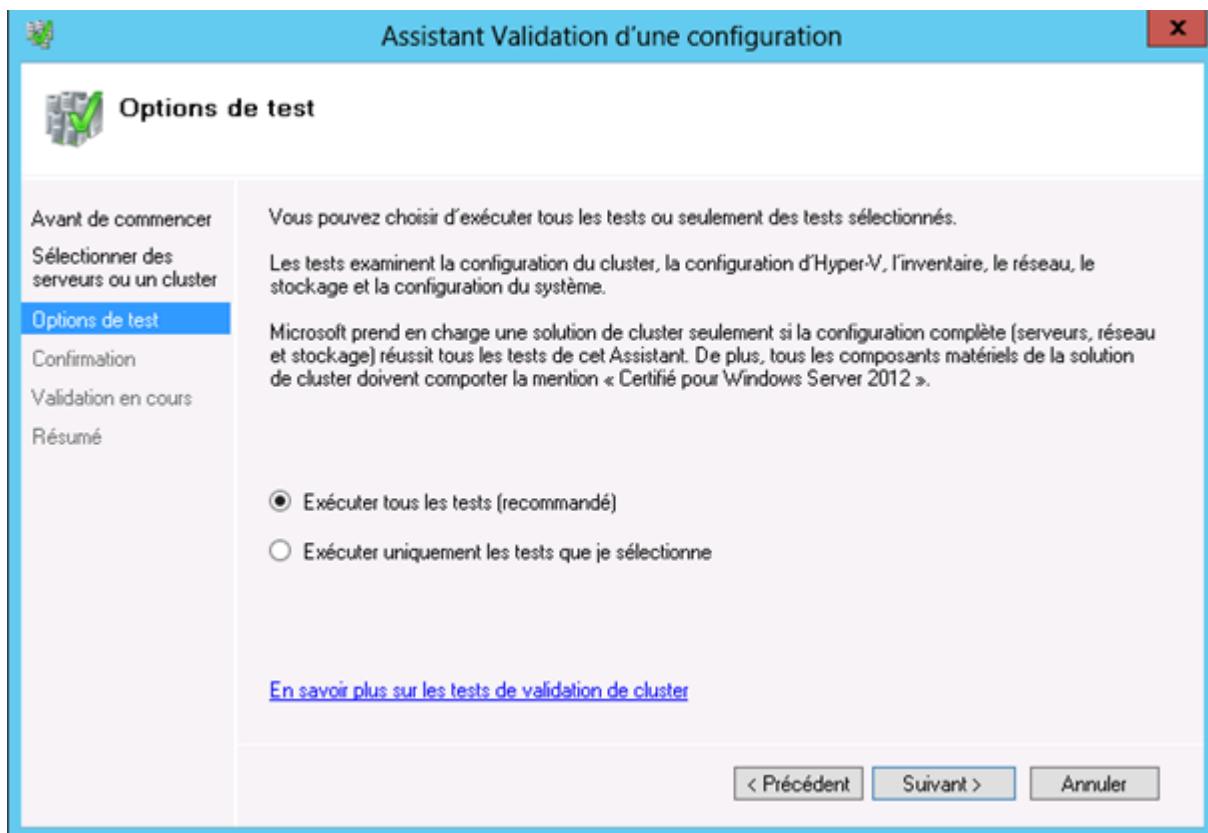
On clique sur **Suivant** :



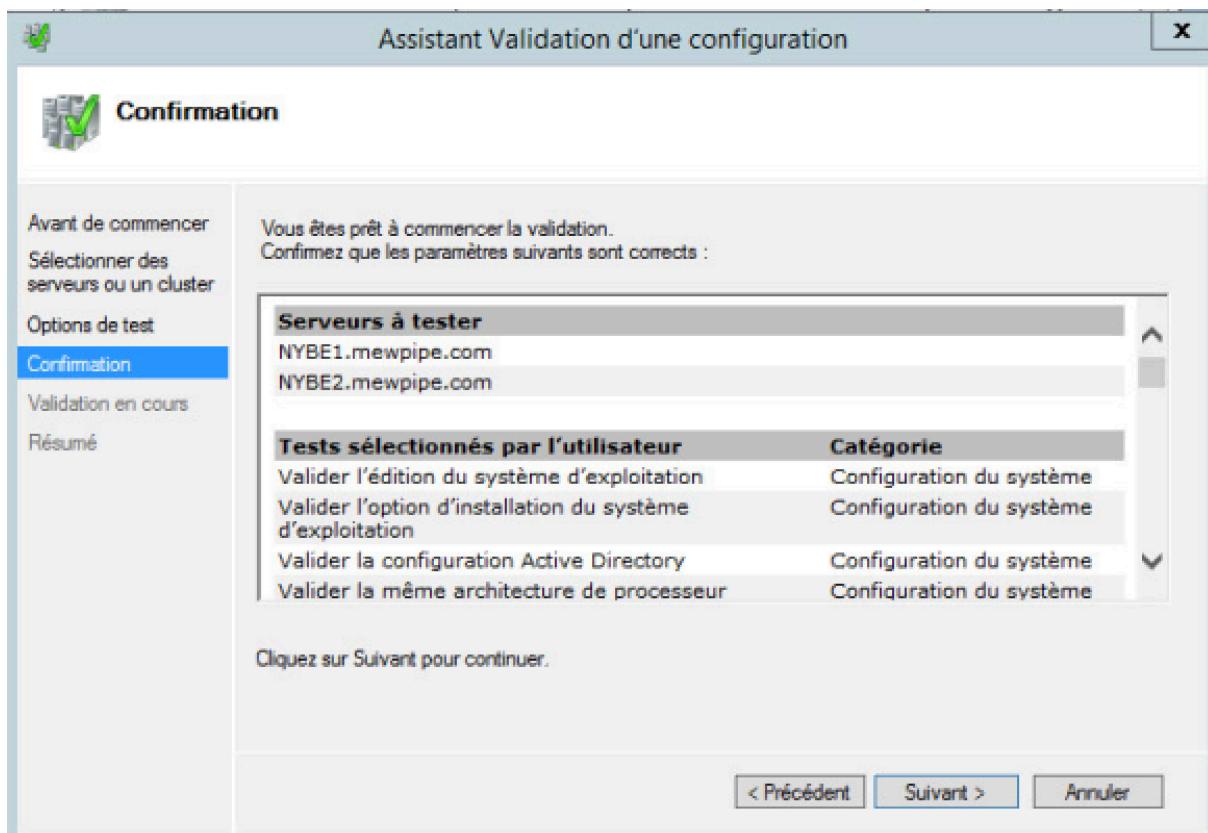
On renseigne le nom des nœuds et on clique sur **Suivant** :



On sélectionne **Exécuter tous les tests (recommandé)** puis on clique sur **Suivant** :

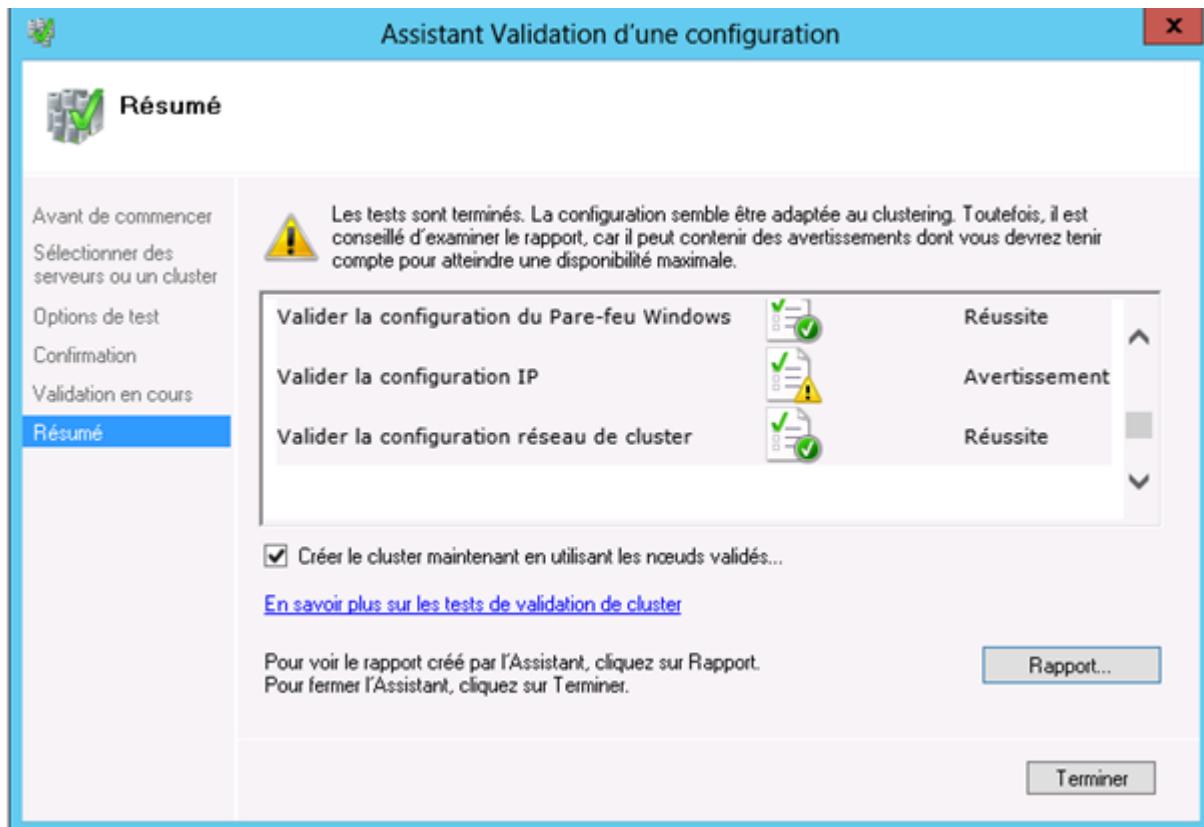


On clique de nouveau sur **Suivant** :

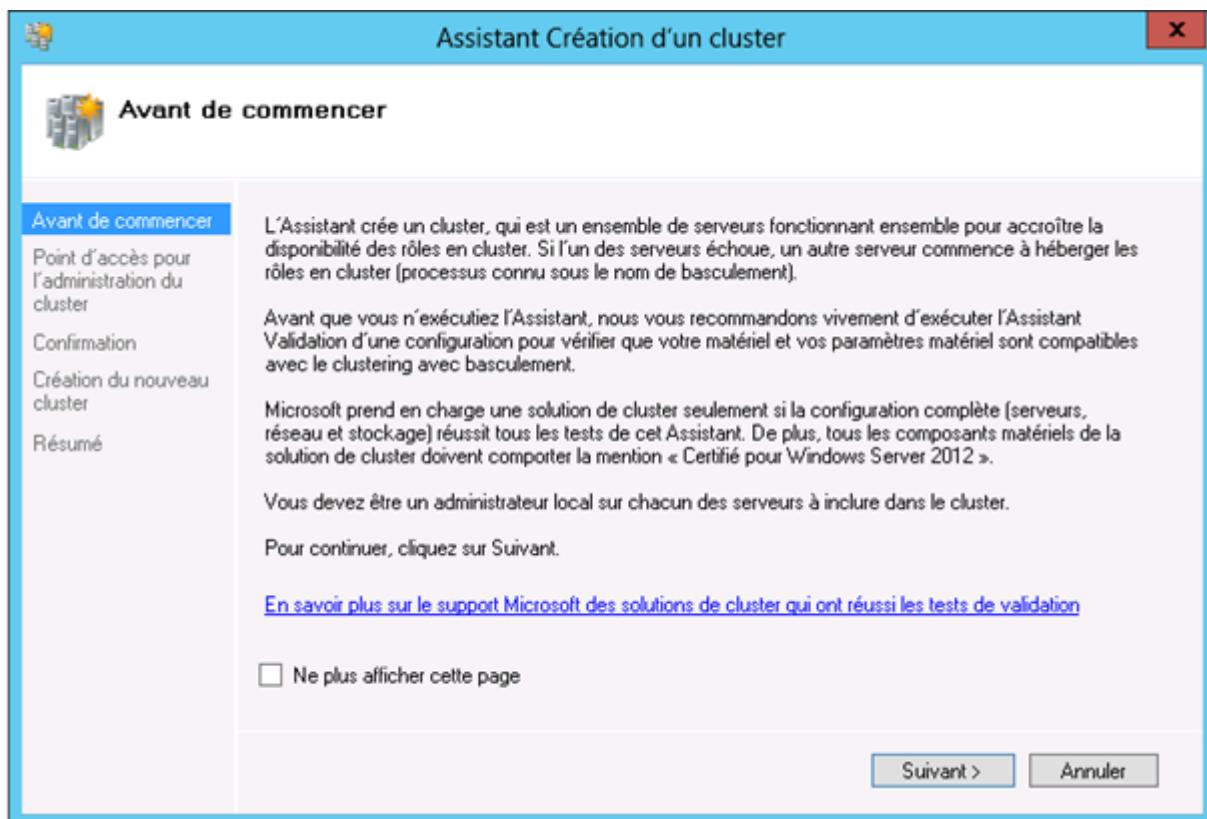


Une fois les tests terminés, des avertissements peuvent être affichés.

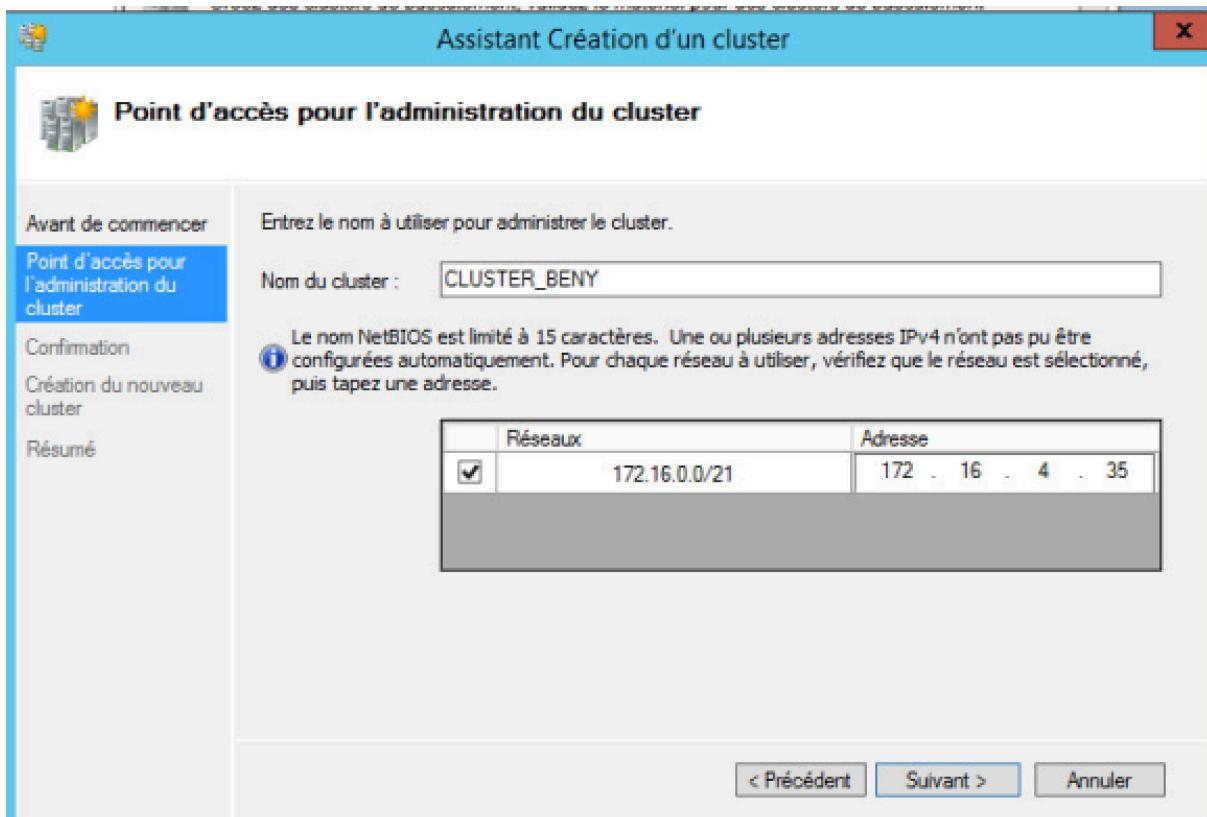
Cochons la case **Créer le cluster maintenant en utilisant les nœuds validés** puis cliquer sur **Terminer** :



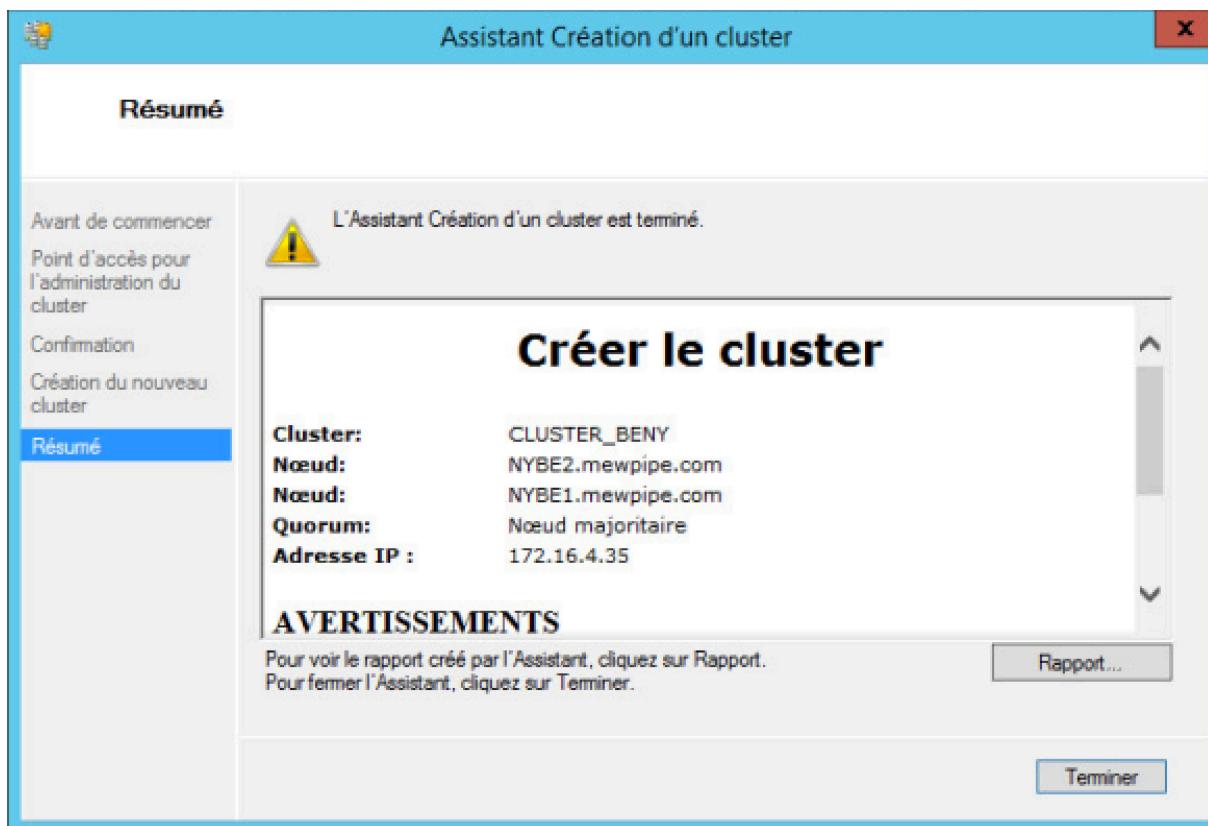
On clique sur **Suivant** :



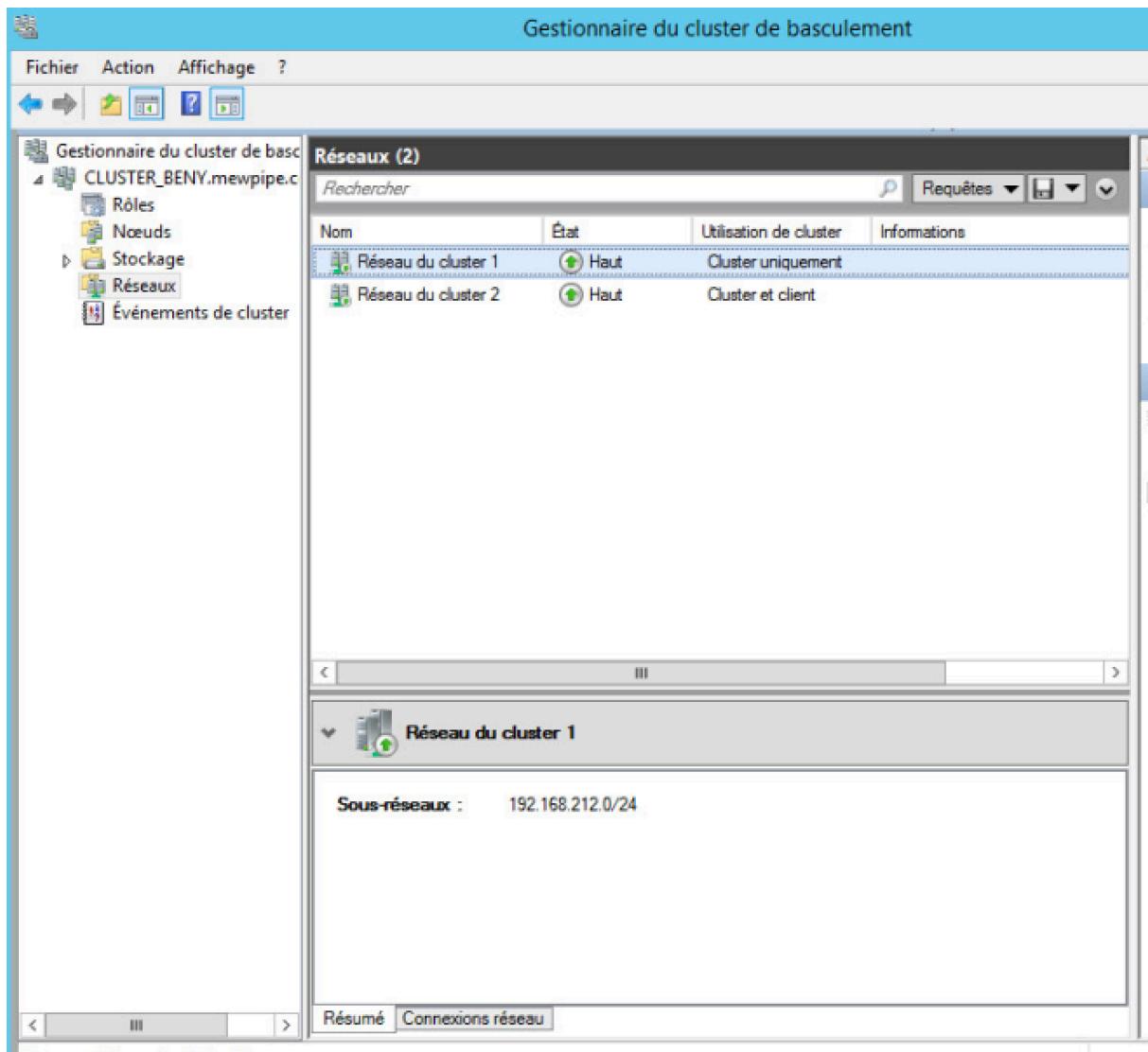
On renseigne le **nom NetBios** et l'adresse **IP** du cluster et on clique sur **Suivant** :



Après avoir de nouveau cliquer sur **Suivant**, le cluster s'est créé :



Notre nouveau cluster apparaît désormais dans notre inventaire du **Gestionnaire du cluster de basculement** et on peut voir que notre réseau en 192.168.211.0/24 est dédié au cluster :



Nos deux machines répondent désormais à une adresse IP commune.

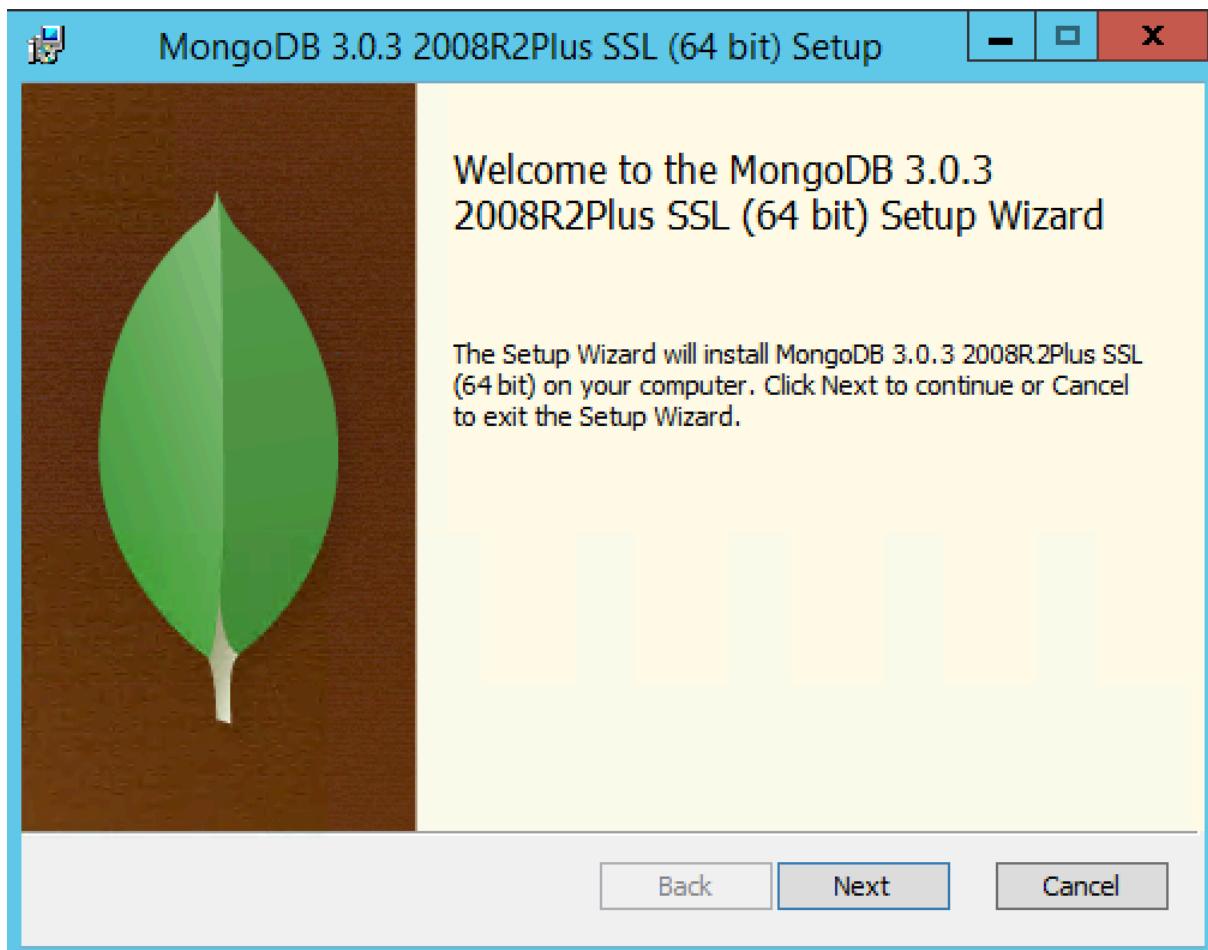
Toutes ces étapes sont maintenant à répéter pour les deux niveaux restants de l'architecture trois-tiers, à savoir front-end et base de données.

M. Déploiement du site Web MEWPIPE

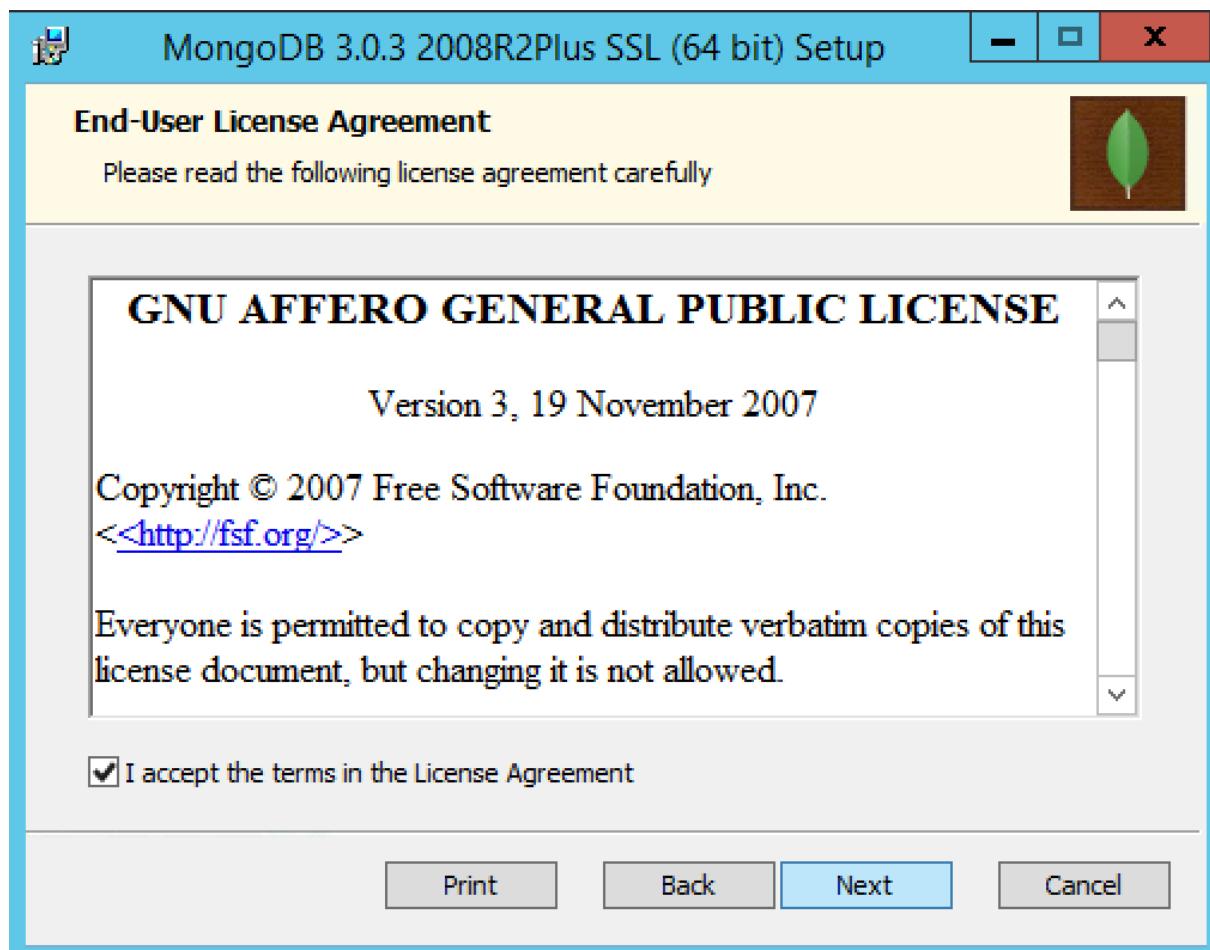
- a) Installation de MongoDB avec réPLICATION de BDD

Tout d'abord, il faut télécharger le fichier exécutable sur le site de MongodB : <https://mongodb.org>

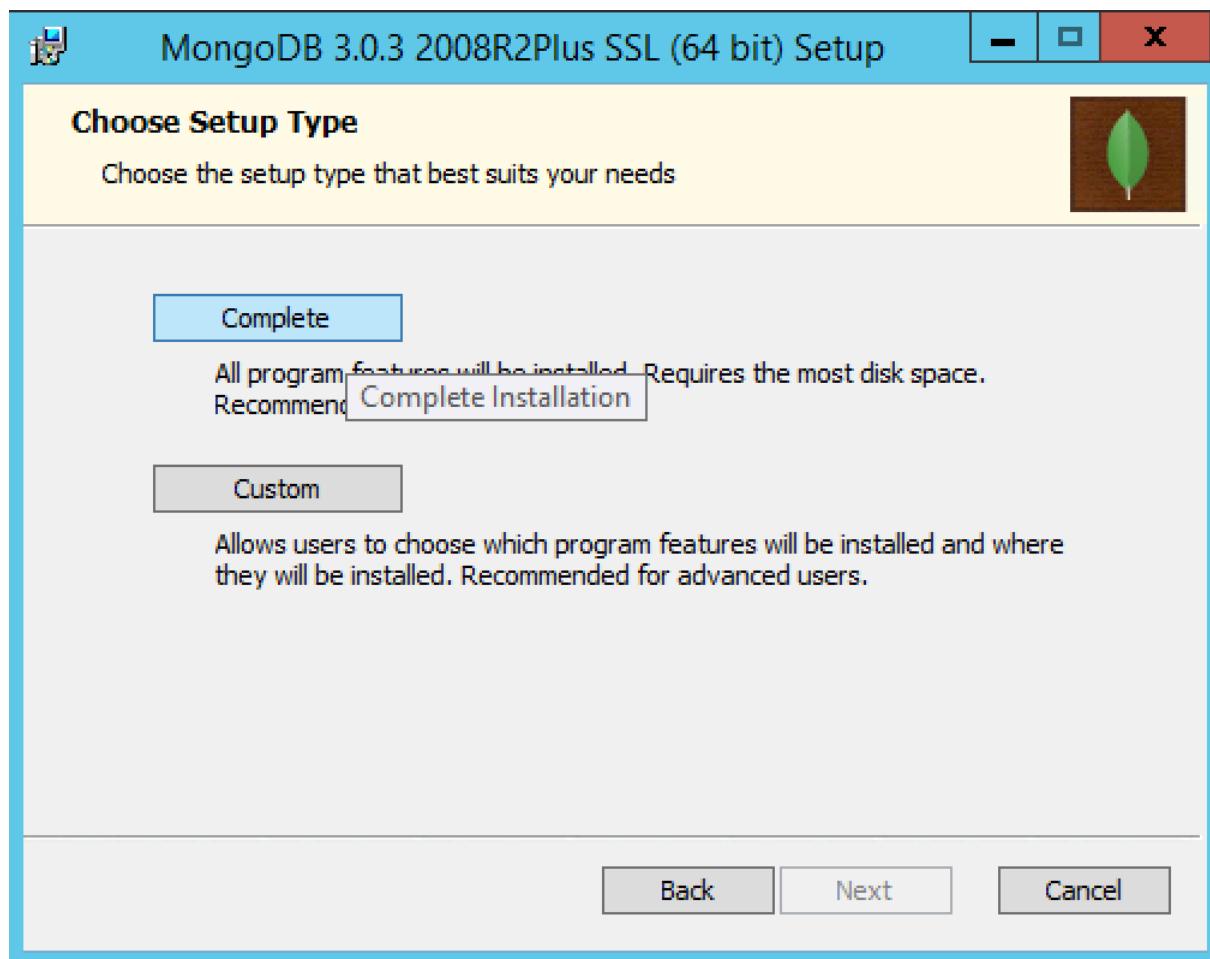
Une fois le fichier téléchargé, exécutons-le. On clique alors sur **Next** pour poursuivre l'installation :



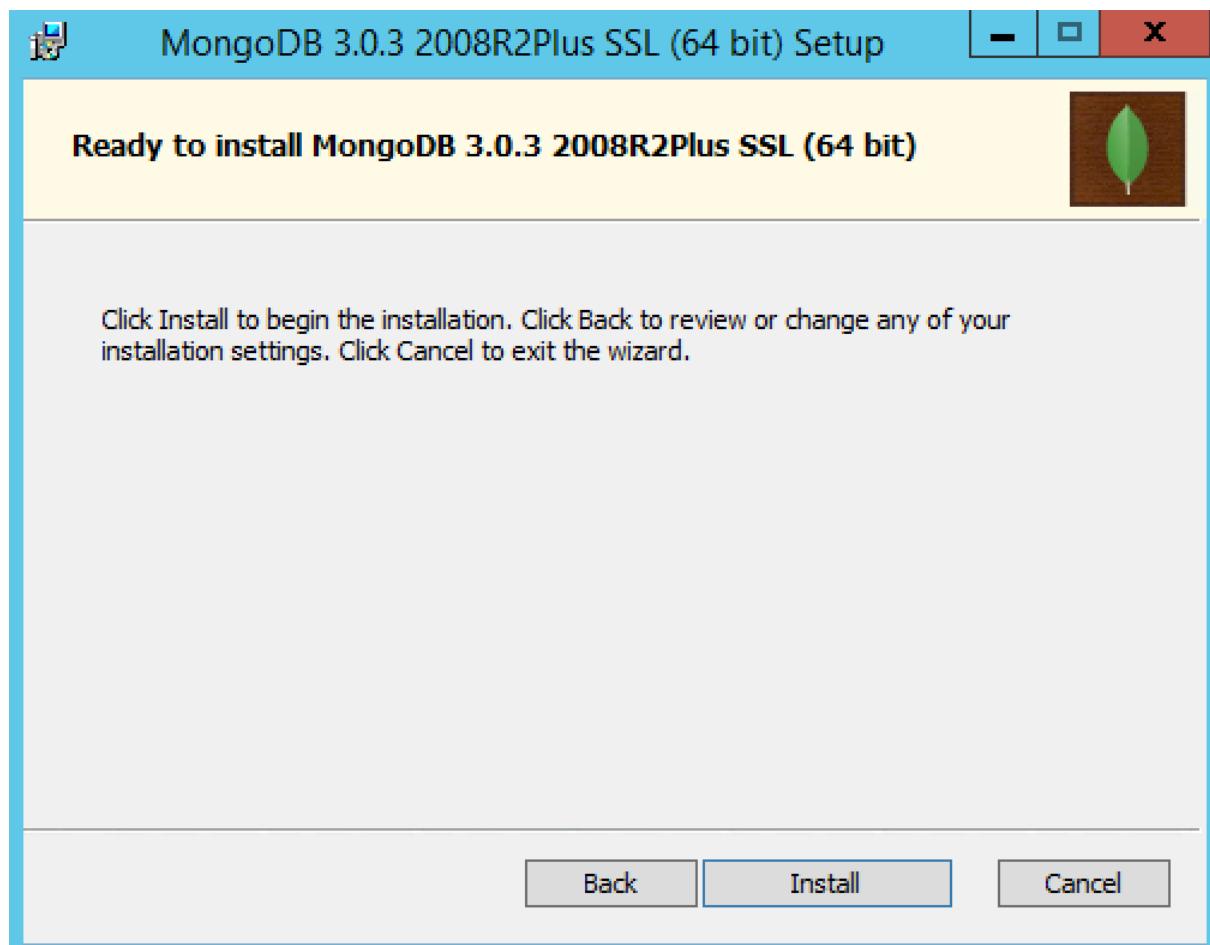
On coche la case pour accepter les conditions d'utilisations et on continue en cliquant sur **Next** :



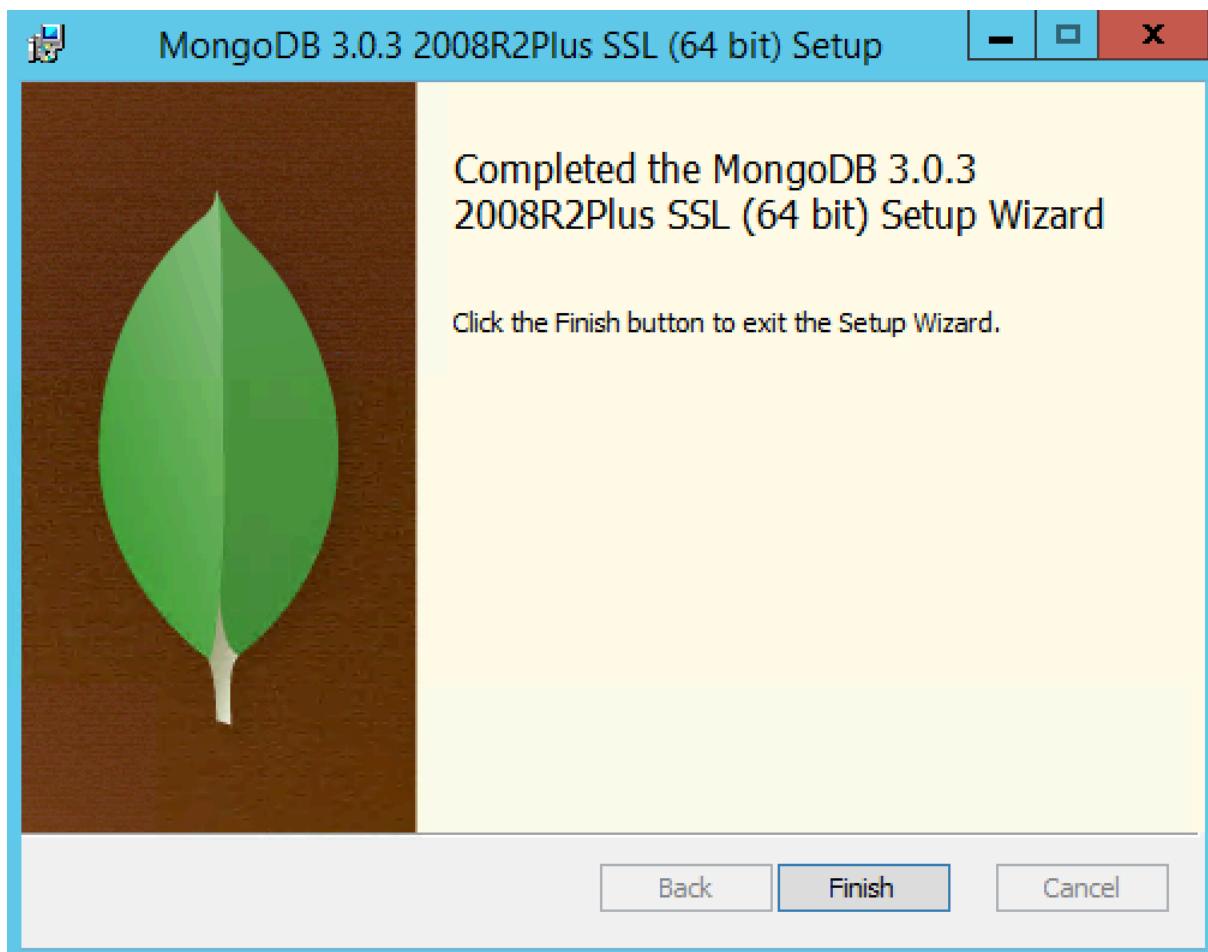
Nous choisissons maintenant l'option **Complete** pour effectuer une installation complète de MongoDB :



L'installateur est prêt à être lancé, nous cliquons alors sur **Install** :



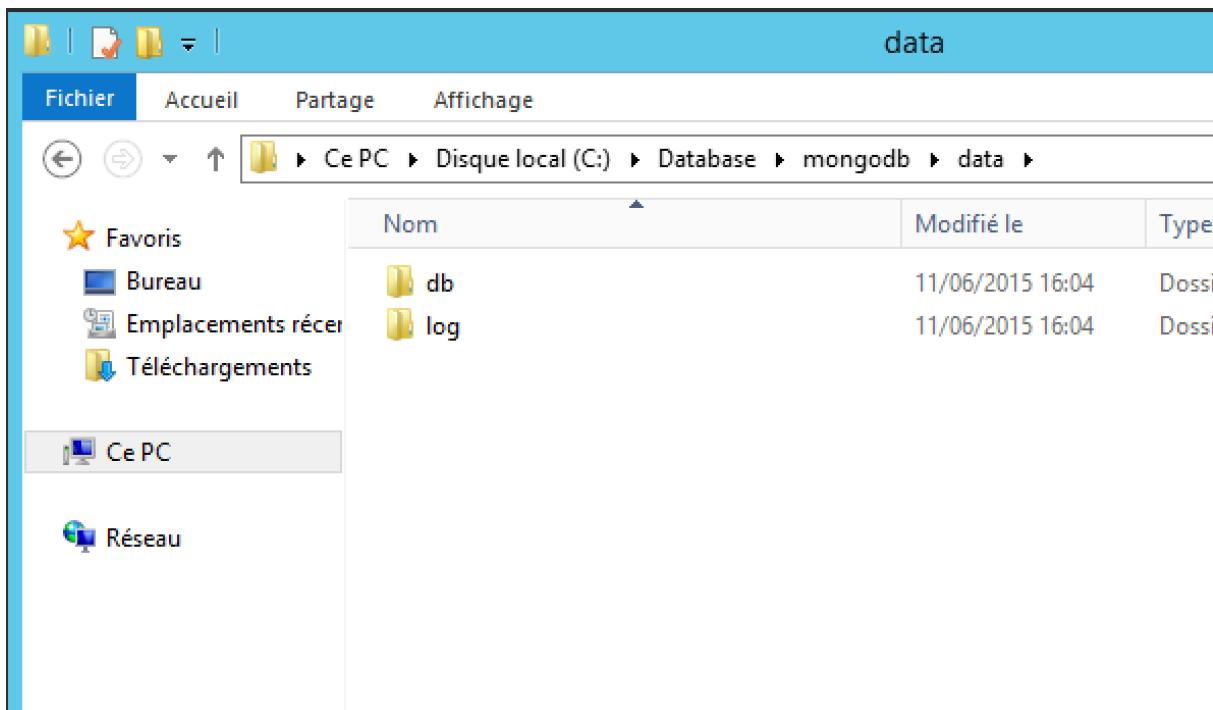
Une fois l'installation terminée, nous pouvons cliquer sur **Finish** :



Cette opération est à répéter sur notre deuxième serveur BDD (NYBDD2).

Il nous faut maintenant créer plusieurs répertoires qui seront utilisés par MongoDB par la suite :

- C:\mewpipe\mongodb\data\db
- C:\mewpipe\mongodb\data\log
- C:\mewpipe\mongodb\config

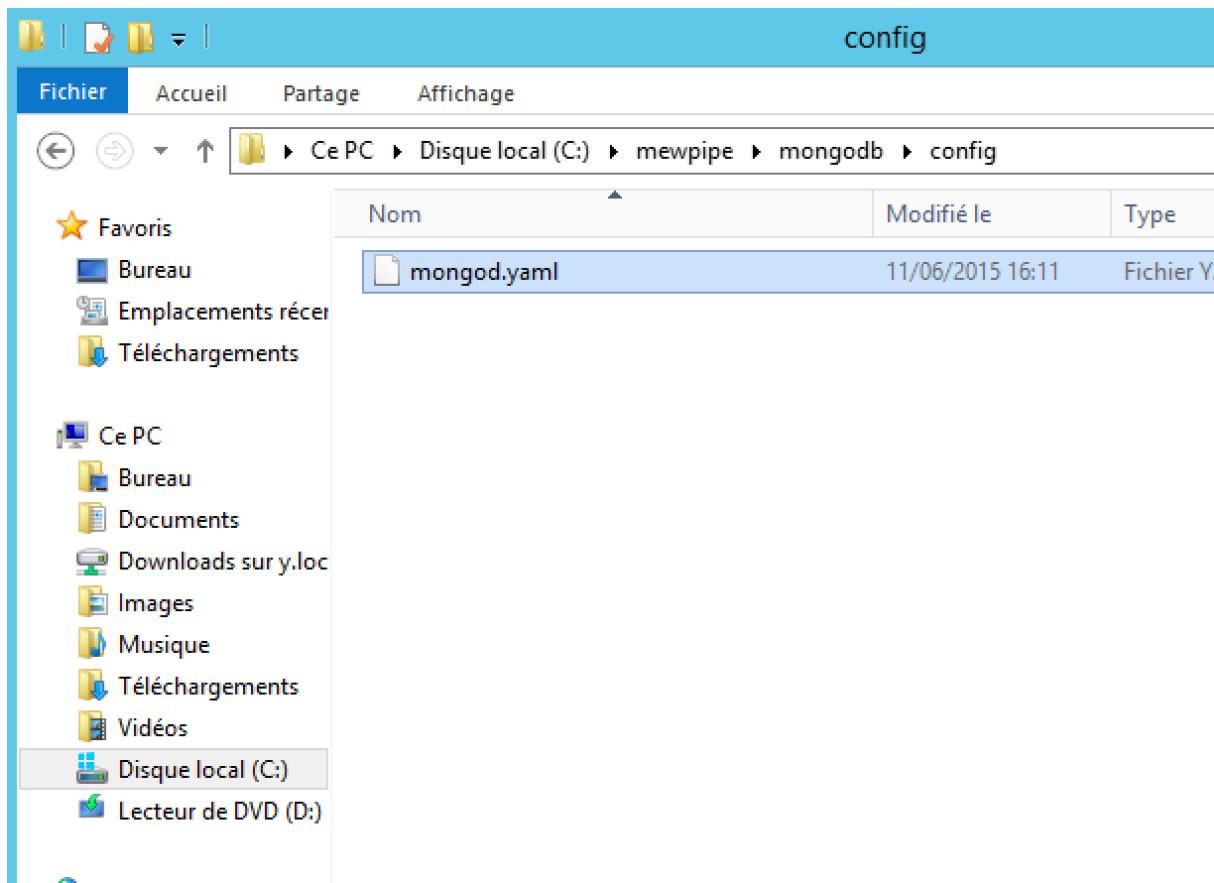


Cette opération est également à répéter sur notre deuxième serveur BDD (NYBDD2).

Nous allons ensuite créer un fichier de configuration pour mongoDB que l'on va placer dans **C:\mewpipe\mongodb\config\mongod.yaml**. Voici son contenu :

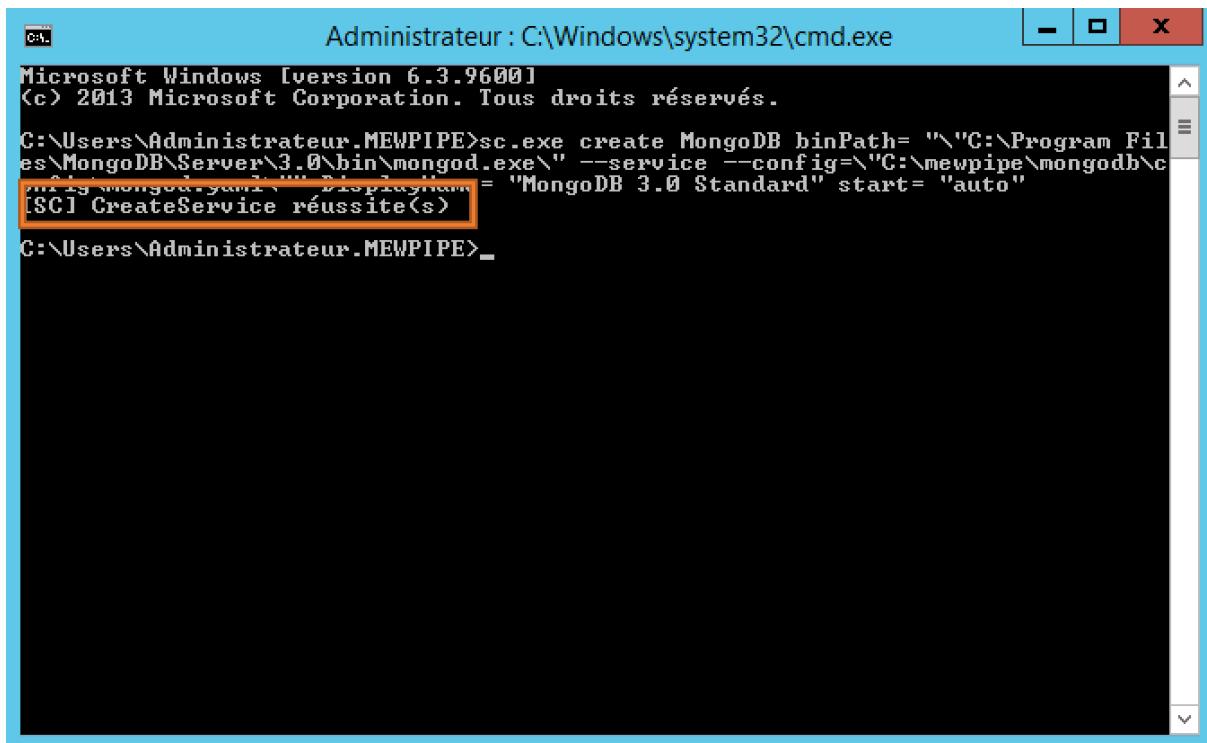
```
systemLog:
  destination: file
  path: "C:/mewpipe/mongodb/data/log/mongod.log"
  logAppend: true
storage:
  dbPath: "C:/mewpipe/mongodb/data/db"
  journal:
    enabled: true
net:
  bindIp: 0.0.0.0
  port: 27017
replication:
  replSetName: mewpipe
```

Cette opération est également à répéter sur notre deuxième serveur BDD (NYBDD2).



On va maintenant lancer une commande qui va permettre de lancer le service mongoDB à chaque démarrage du serveur :

```
sc.exe create MongoDB binPath= "\"C:\Program
Files\MongoDB\Server\3.0\bin\mongod.exe\" --service --
config=\"C:\mewpipe\mongodb\config\mongod.yaml\"" DisplayName= "MongoDB 3.0
Standard" start= "auto"
```



```
Administrator : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

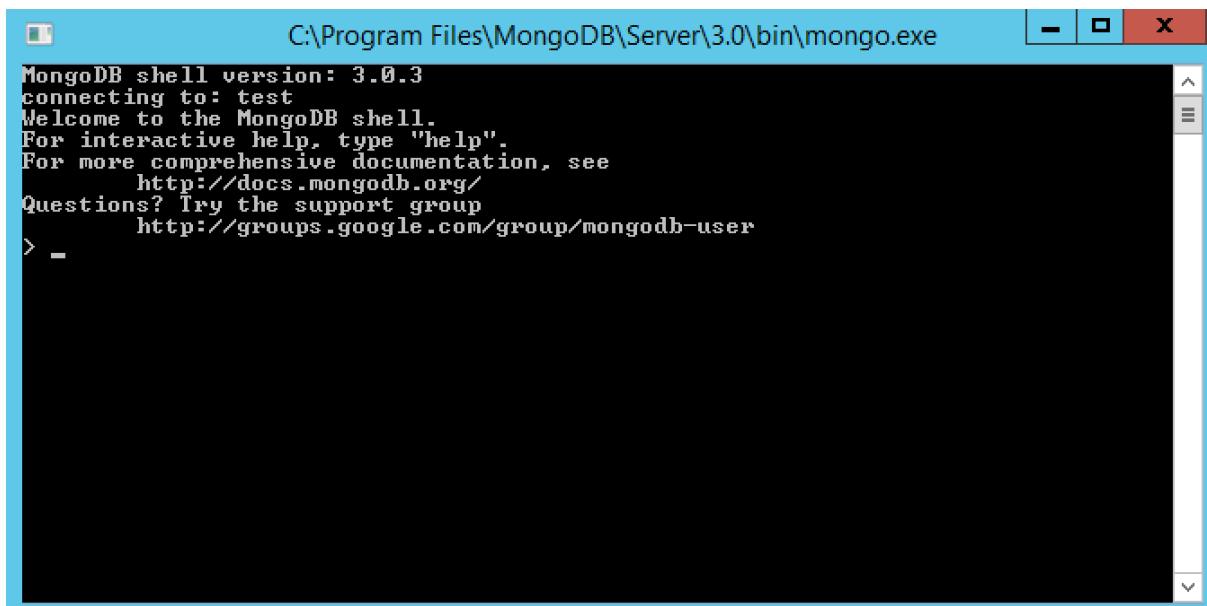
C:\Users\Administrateur.MEWPIPE>sc.exe create MongoDB binPath= "\"C:\Program Files\MongoDB\Server\3.0\bin\mongod.exe\" --service --config=\"C:\mewpipe\mongodb\config\mongod.conf" DisplayName = "MongoDB 3.0 Standard" start= "auto"
[SC] CreateService réussite(s)

C:\Users\Administrateur.MEWPIPE>
```

Cette opération est également à répéter sur notre deuxième serveur BDD (NYBDD2).

Dans un prompt, nous pouvons maintenant lancer le shell mongo avec la commande suivante :

```
c:\Program Files\MongoDB\Server\3.0\bin\mongo
```



```
C:\Program Files\MongoDB\Server\3.0\bin\mongo.exe
MongoDB shell version: 3.0.3
connecting to: test
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
    http://docs.mongodb.org/
Questions? Try the support group
    http://groups.google.com/group/mongodb-user
> -
```

Nous allons maintenant mettre en place la réPLICATION de la base de données. Pour cela, on va se placer sur notre premier serveur dans un shell mongo comme vu précédemment et nous allons taper les commandes suivantes :

```
rs.initiate()
rs.add("nybdd2:27017")
```

```

cfg = rs.conf()
cfg.members[0].priority = 100
cfg.members[1].priority = 50
rs.reconfig(cfg)
C:\Program Files\MongoDB\Server\3.0\bin\mongo.exe
MongoDB shell version: 3.0.3
connecting to: test
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
      http://docs.mongodb.org/
Questions? Try the support group
      http://groups.google.com/group/mongodb-user
> rs.initiate()
{
    "info2" : "no configuration explicitly specified -- making one",
    "me" : "nybdd1:27017",
    "ok" : 1
}
newpipe:PRIMARY> rs.add("nybdd2:27017")
{
    "ok" : 1
}
newpipe:PRIMARY> cfg=rs.conf()
{
    "_id" : "newpipe",
    "version" : 2,
    "members" : [
        {
            "_id" : 0,
            "host" : "nybdd1:27017",
            "arbiterOnly" : false,
            "buildIndexes" : true,
            "hidden" : false,
            "priority" : 1,
            "tags" : {
                "slaveDelay" : 0,
                "votes" : 1
            }
        },
        {
            "_id" : 1,
            "host" : "nybdd2:27017",
            "arbiterOnly" : false,
            "buildIndexes" : true,
            "hidden" : false,
            "priority" : 1,
            "tags" : {
                "slaveDelay" : 0,
                "votes" : 1
            }
        }
    ],
    "settings" : {
        "chainingAllowed" : true,
        "heartbeatTimeoutSecs" : 10,
        "getLastErrorModes" : {
            "getLastErrorDefaults" : {
                "w" : 1,
                "wtimeout" : 0
            }
        }
    }
}
newpipe:PRIMARY> cfg.members[0].priority = 100
100
newpipe:PRIMARY> cfg.members[1].priority = 50
50
newpipe:PRIMARY> rs.reconfig(cfg)
{
    "ok" : 1
}
newpipe:PRIMARY>

```

Nous pouvons alors tester notre configuration avec la commande suivante :

```
rs.status()
```

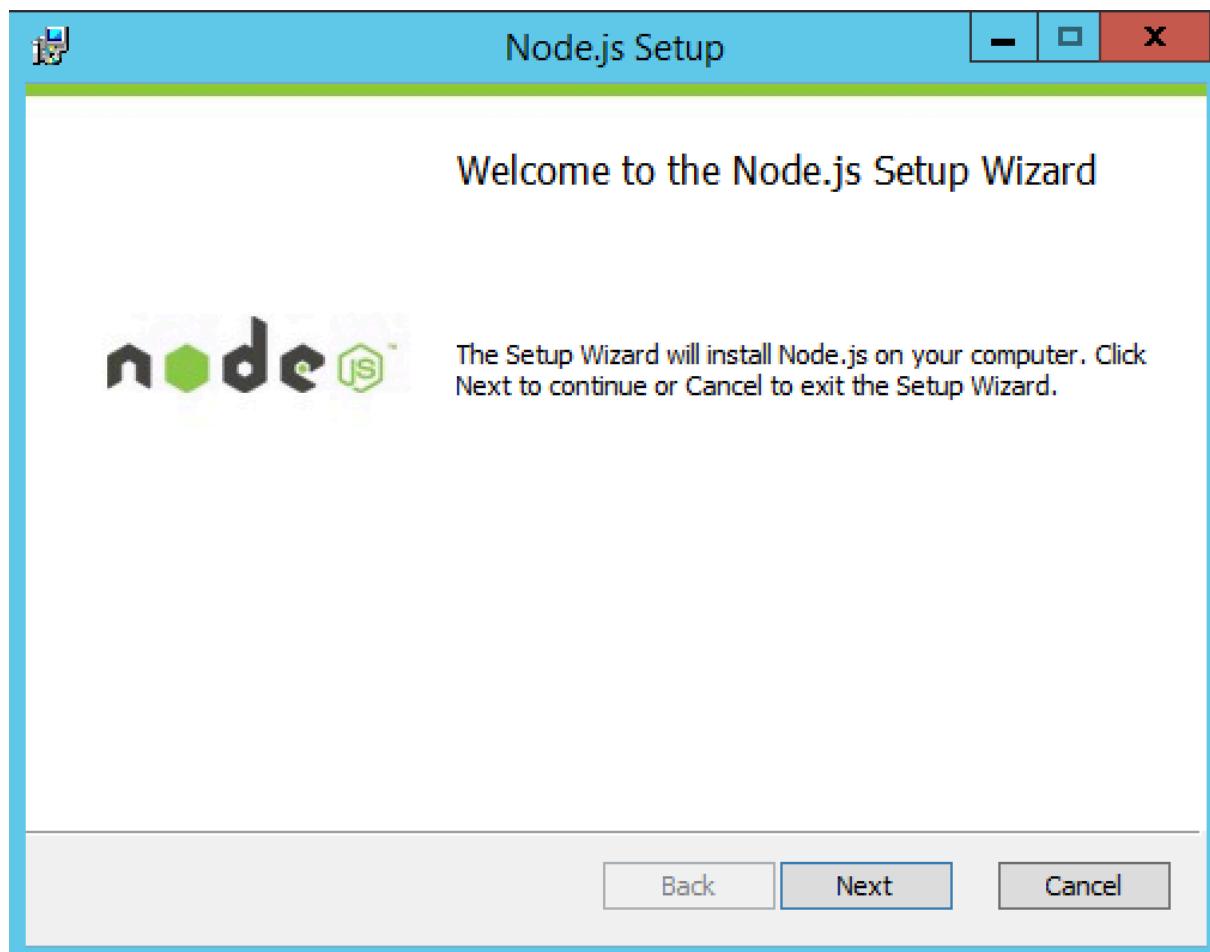
```
mewpipe:PRIMARY> rs.status()
{
  "set" : "mewpipe",
  "date" : ISODate("2015-06-11T14:30:34.477Z"),
  "myState" : 1,
  "members" : [
    {
      "_id" : 0,
      "name" : "NYBDD1:27017",
      "health" : 1,
      "state" : 1,
      "stateStr" : "PRIMARY",
      "uptime" : 501,
      "optime" : Timestamp(1434033009, 1),
      "optimeDate" : ISODate("2015-06-11T14:30:09Z"),
      "electionTime" : Timestamp(1434032868, 2),
      "electionDate" : ISODate("2015-06-11T14:27:48Z"),
      "configVersion" : 3,
      "self" : true
    },
    {
      "_id" : 1,
      "name" : "nybdd2:27017",
      "health" : 1,
      "state" : 2,
      "stateStr" : "SECONDARY",
      "uptime" : 122,
      "optime" : Timestamp(1434033009, 1),
      "optimeDate" : ISODate("2015-06-11T14:30:09Z"),
      "lastHeartbeat" : ISODate("2015-06-11T14:30:33.590Z"),
      "lastHeartbeatRecv" : ISODate("2015-06-11T14:30:33.613Z")
    }
  ],
  "ok" : 1
}
mewpipe:PRIMARY>
```

Nous avons alors notre serveur NYBDD1 en **PRIMARY** et notre serveur NYBDD2 en **SECONDARY** avec notre future base de données répliquée.

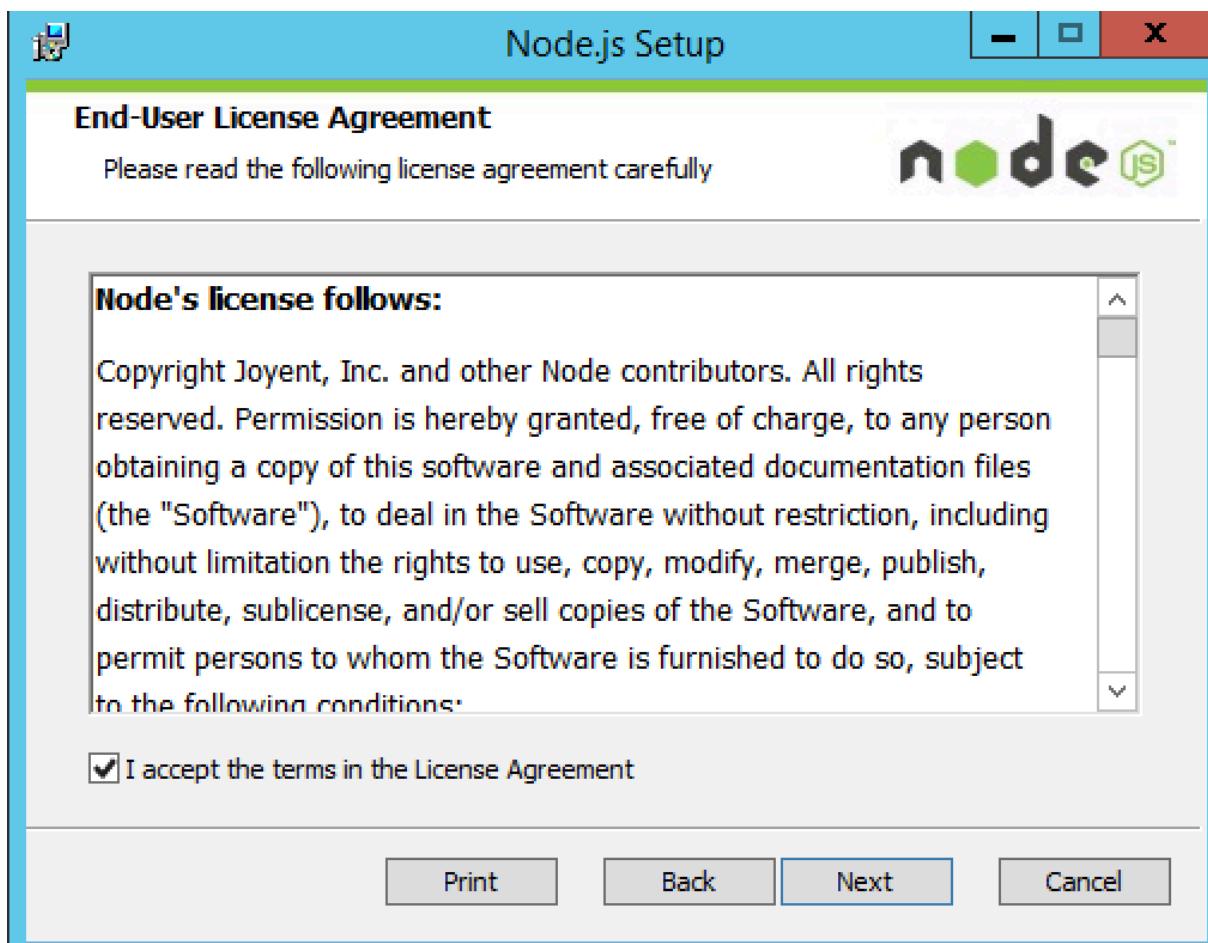
b) Installation du serveur node

Toutes les opérations à suivre pour l'installation du serveur node sont à effectuées sur les deux serveurs Back-end.

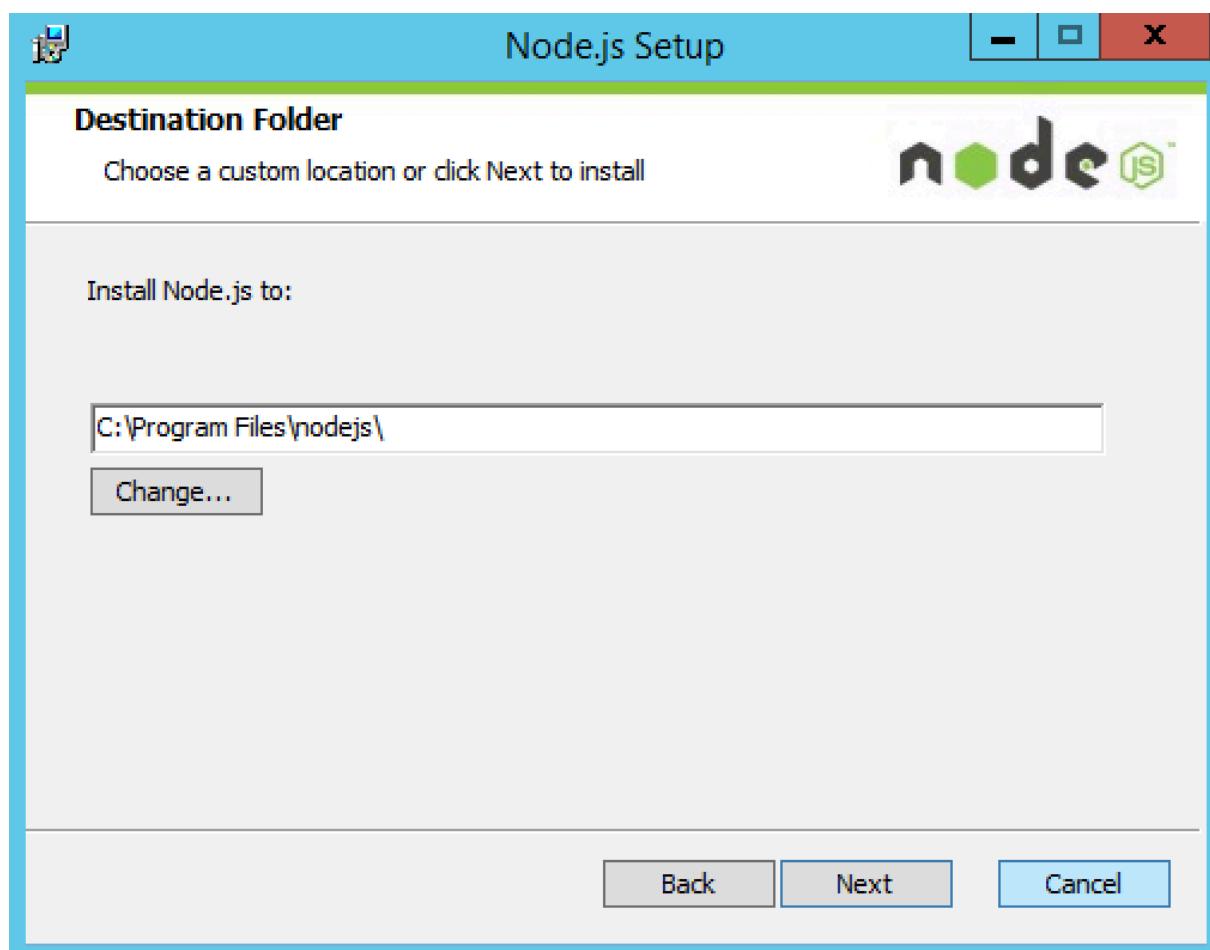
Nous allons commencer par installer Node.js sur nos serveurs pour cela, on le télécharger sur le site suivant : <https://nodejs.org/> puis on lance l'exécutable. Un message d'accueil apparaît, nous pouvons cliquer sur **Next** :



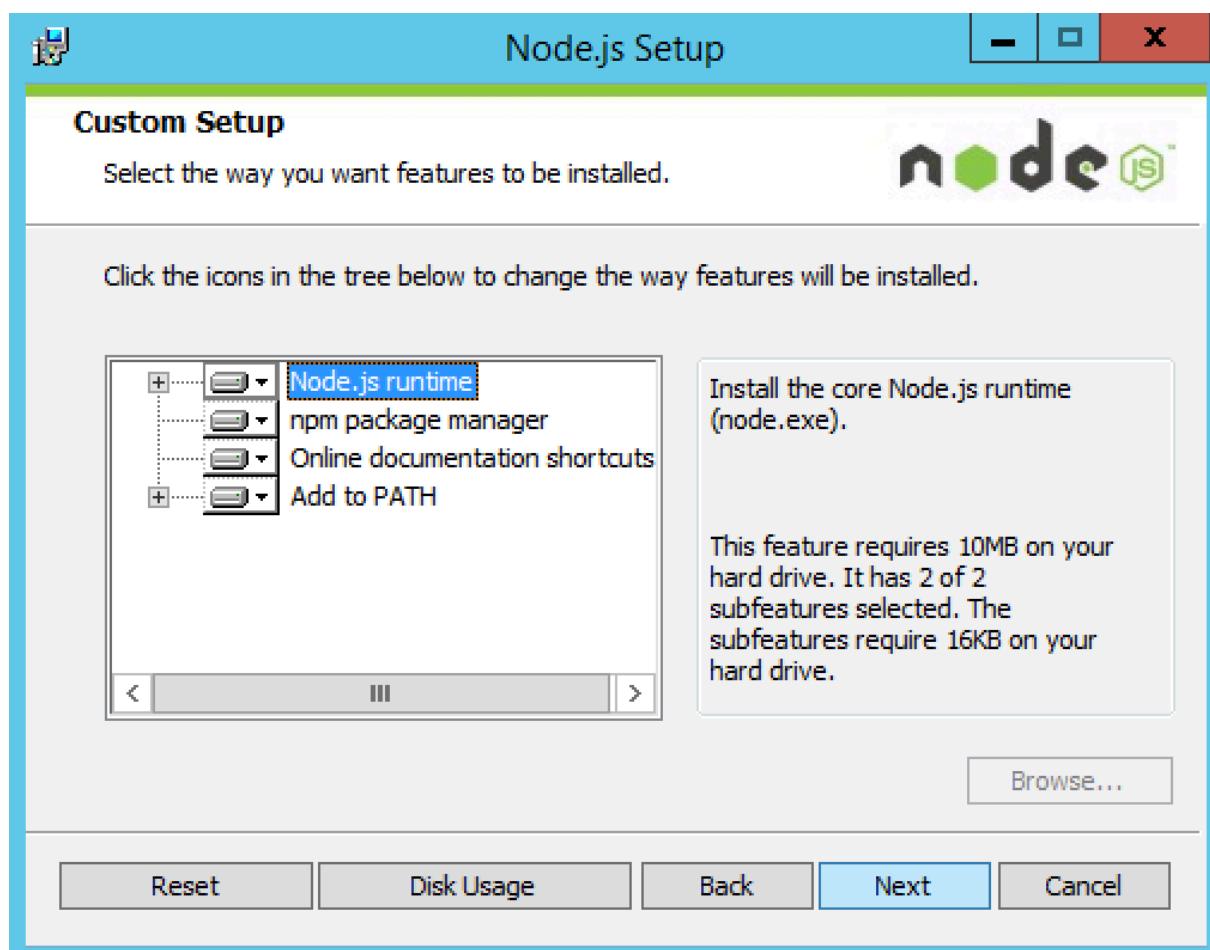
Ensuite, on coche la case pour accepter les termes de la licence et on poursuit en cliquant sur **Next** :



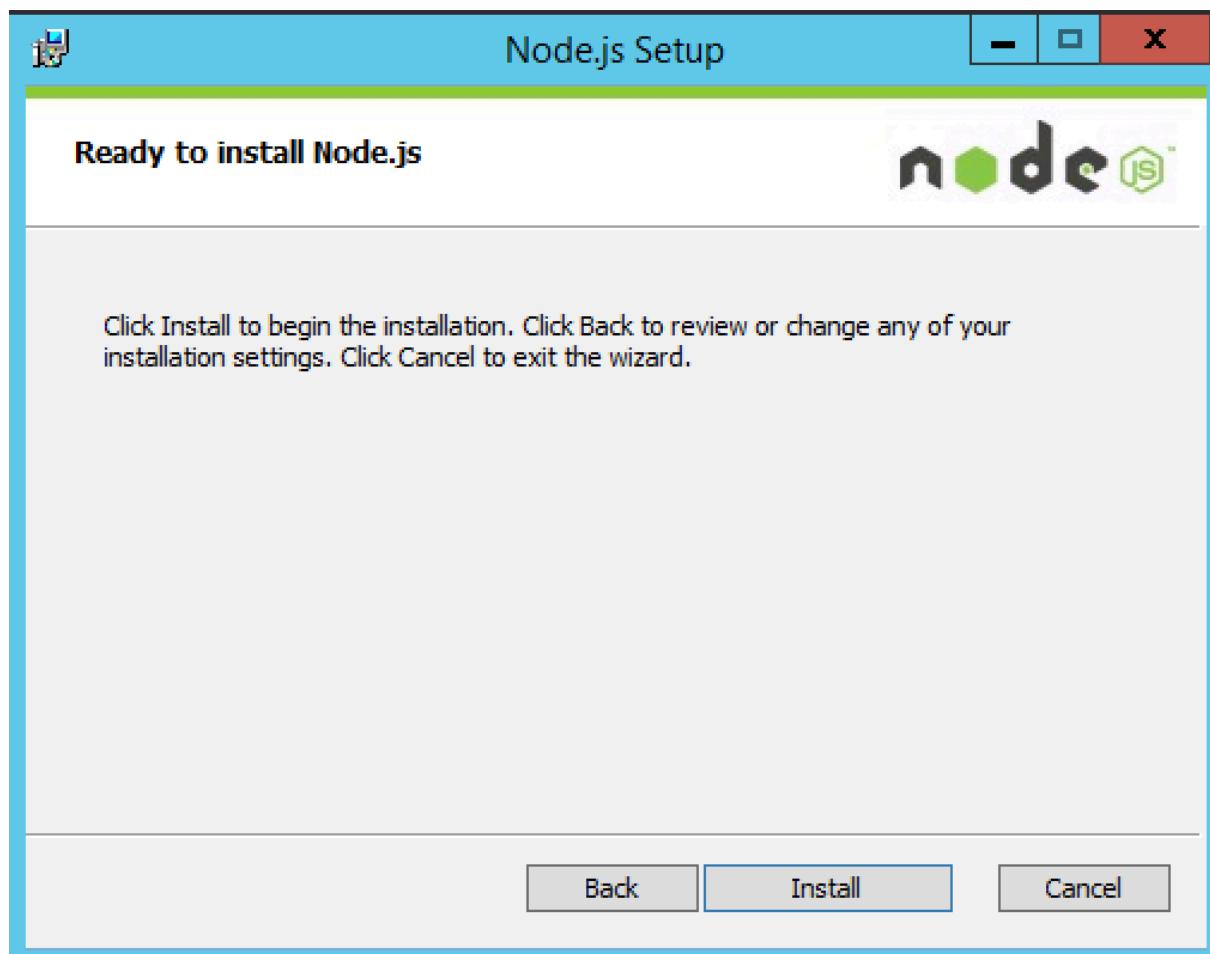
On laisse le répertoire d'installation définit par défaut et on clique de nouveau sur **Next** :



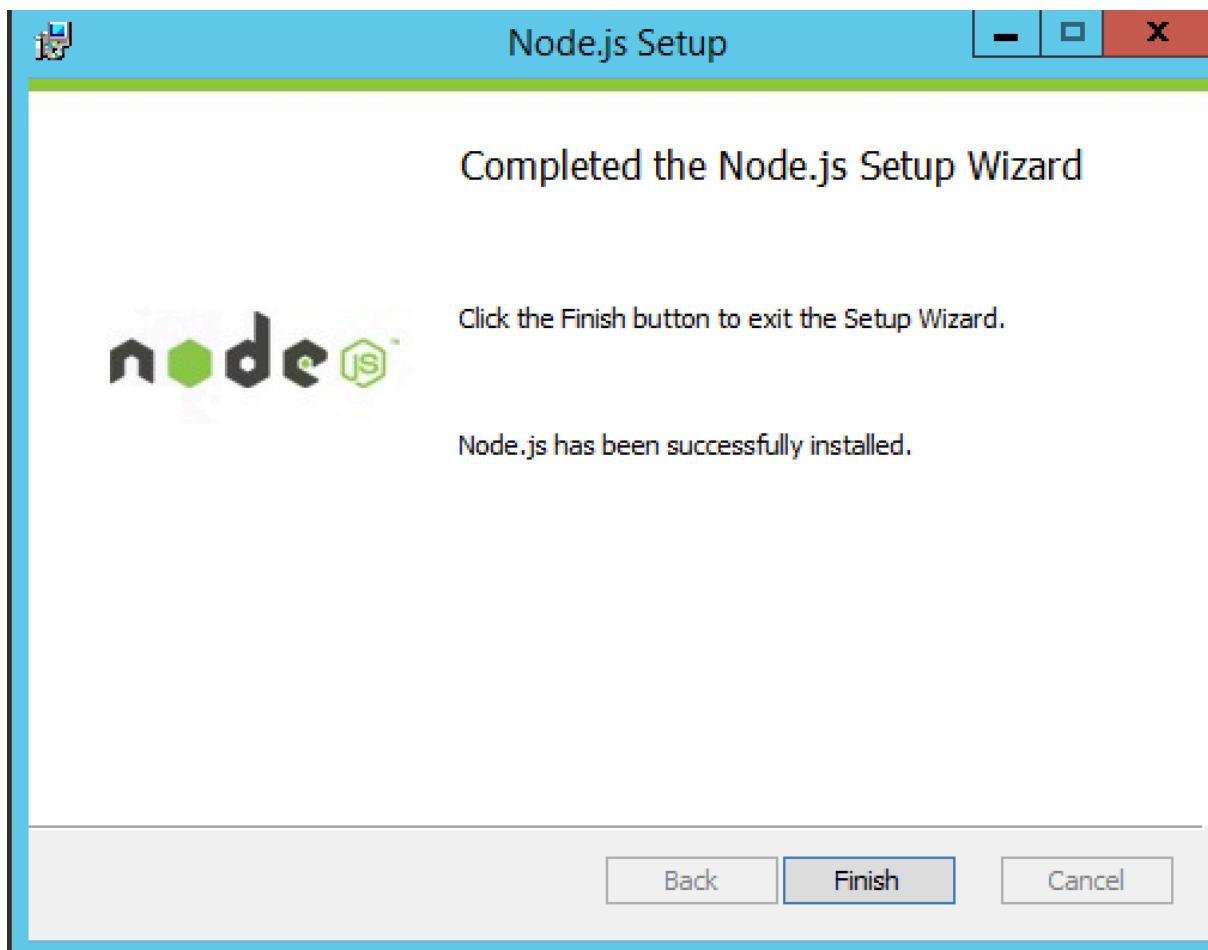
Vient alors le choix des fonctionnalités à installer, on laisse par défaut et on clique sur **Next** :



L'installation est enfin prête, on clique sur **Install** :



Une fois l'installation terminée, nous pouvons cliquer sur **Finish** :



Après avoir rapatrier les sources de notre API, dans le dossier **C:\www** (via Github sur un repository privé). Nous allons maintenant lancer une série de commande permettant d'instancier notre serveur node.js :

- On commence par se placer dans le dossier API :

```
cd c:\www\MewPipe\API
```

- On installe les dépendances via le gestionnaire de paquets **npm** :

```
npm install
```

```

Administrator : Invité de commandes
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.MEWPIPE>cd C:\www\MewPipe\API
C:\www\MewPipe\API>npm install
/

> handbrake-js@2.0.4 postinstall C:\www\MewPipe\API\node_modules\handbrake-js
> node scripts/install.js

fetching: https://handbrake.fr/rotation.php?file=HandBrake-0.10.2-x86_64-Win_CLI
.zip
extracting: unzipped\HandBrakeCLI.exe
HandBrakeCLI installation complete

> kerberos@0.0.9 install C:\www\MewPipe\API\node_modules\mongoose\node_modules\mongod
on\mongodb\node_modules\kerberos
> <node-gyp rebuild 2> builderror.log> || <exit 0>

C:\www\MewPipe\API\node_modules\mongoose\node_modules\mongodb\node_modules\kerber
os>if not defined npm_config_node_gyp (node "C:\Program Files\nodejs\node_modul
es\npm\bin\node-gyp-bin\\..\..\node_modules\node-gyp\bin\node-gyp.js" rebuild ) e
lse <rebuild>
> bson@0.2.21 install C:\www\MewPipe\API\node_modules\mongoose\node_modules\mong
odb\node_modules\bson
> <node-gyp rebuild 2> builderror.log> || <exit 0>

C:\www\MewPipe\API\node_modules\mongoose\node_modules\mongodb\node_modules\bson>
if not defined npm_config_node_gyp (node "C:\Program Files\nodejs\node_modul
es\npm\bin\node-gyp-bin\\..\..\node_modules\node-gyp\bin\node-gyp.js" rebuild ) e
lse <rebuild>
node-fs@0.1.7 node_modules\node-fs

crypto@0.0.3 node_modules\crypto

bcrypt-nodejs@0.0.3 node_modules\bcrypt-nodejs

passport-local@1.0.0 node_modules\passport-local
└── passport-strategy@1.0.0

passport@0.2.2 node_modules\passport
└── passport-strategy@1.0.0
    └── pause@0.0.1

morgan@1.3.2 node_modules\morgan
└── basic-auth@1.0.0
└── depd@0.4.5
└── on-finished@2.1.0 <ee-first@1.0.5>

passport-google@0.3.0 node_modules\passport-google
└── pkginfo@0.2.3
└── passport-openid@0.3.1 <passport@0.1.18, openid@0.5.13>

passport-facebook@2.0.0 node_modules\passport-facebook
└── passport-oauth2@1.1.2 <uid2@0.0.3, passport-strategy@1.0.0, oauth@0.9.13>

errorhandler@1.2.4 node_modules\errorhandler
└── escape-html@1.0.1
└── accepts@1.1.4 <negotiator@0.4.9, mime-types@2.0.14>

connect-multiparty@1.2.5 node_modules\connect-multiparty
└── qs@2.2.5
└── on-finished@2.1.1 <ee-first@1.1.0>

```

Afin de passer une d'une étape de développement à une étape de production, il nous faut changer l'adresse IP sur laquelle repose le serveur de base de données dans le fichier **C:\www\MewPipe\API\models\bdd.js**. Dans notre cas, il s'agit de l'adresse IP commune du cluster de base de données (172.16.4.45) :

```
bdd - Bloc-notes
Fichier Edition Format Affichage ?
var mongoose = require('mongoose');mongoose.connect('mongodb://172.16.4.45:27017/MewPipe', {
```

- On va maintenant lancer une commande qui va permettre de lancer le serveur node.js à chaque démarrage du serveur :

```
sc.exe create NodeJs binPath= "\"C:\Program Files\nodejs\node.exe\" --service --config=\"C:\www\MewPipe\API\server.js\" DisplayName= "NodeJS Standard" start= "auto"
```

- Nous pouvons alors lancer notre API via la commande suivante :

```
node server.js
```

```
C:\www\MewPipe\API>node server.js
< [Error: Cannot find module '../build/Release/bson'] code: 'MODULE_NOT_FOUND' >
js-bson: Failed to load c++ bson extension, using pure JS version
#####
Started since: 2015-06-12T09:02:13.802Z
Environement: DEU
Debug ON
MewPipe API listening on localhost:8080
#####
```

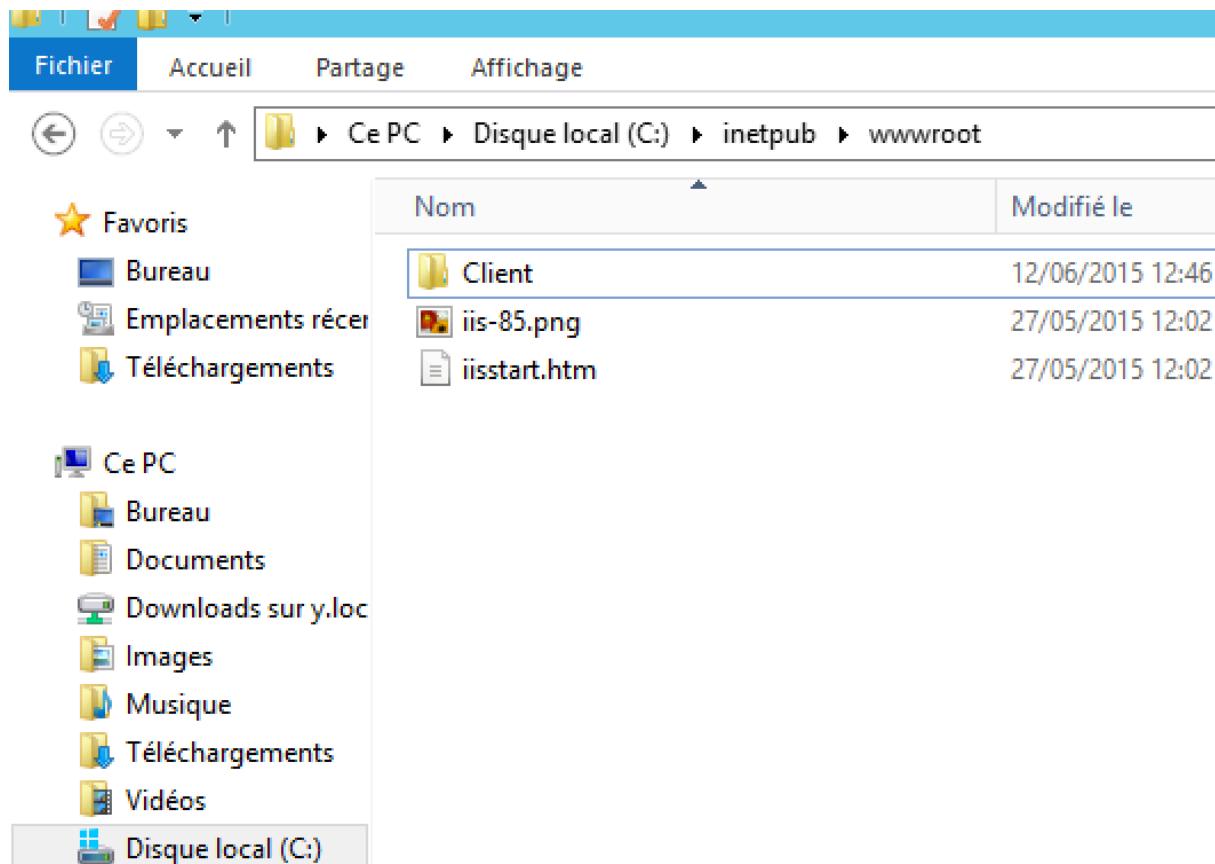
Nous vérifions son fonctionnement via le navigateur :



c) Mise en place du front-end sur nos serveurs NYFE1 et NYFE2

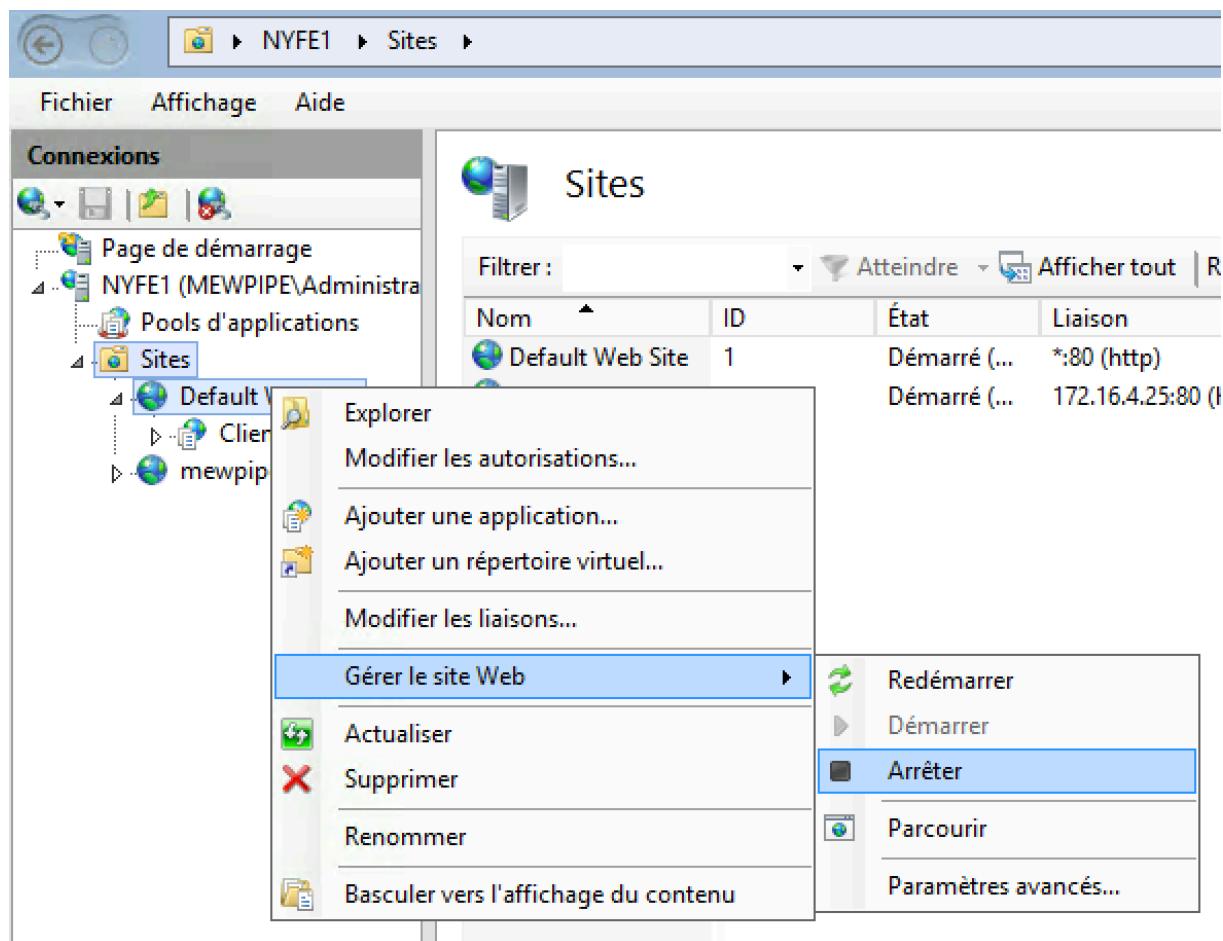
i. *Rapatriement des sources*

Afin de mettre en place notre front-end sur nos serveurs correspondants, nous devons rapatrier les sources sur ces derniers. Nous allons donc copier le dossier **Client** contenu dans **MewPipe**, dans le dossier **C:\inetpub\wwwroot** :

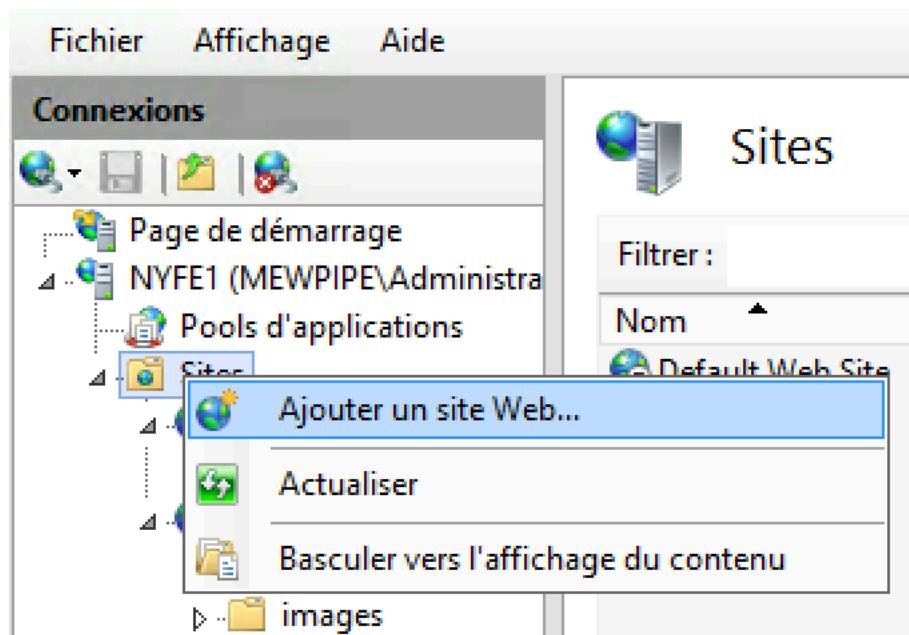


ii. Création du site Mewpipe

Nous allons créer notre site Mewpipe dans notre **Gestionnaire des services IIS**, pour cela dans notre **Gestionnaire de serveurs**, nous cliquons sur **Outils** puis sur **Gestionnaire des services IIS**. Une fois ouvert on déploie l'arborescence de nos sites. Nous allons commencer par arrêter le **Default Web Site**, pour cela nous effectuons un clic-droit dessus, puis sous **Gérer le site Web**, nous cliquons sur **Arrêter** :



Nous allons maintenant ajouter notre site web, pour cela nous effectuons un clic-droit sur **Sites**, puis nous cliquons sur **Ajouter un site Web...** :



Nous renseignons alors le nom du site, le chemin d'accès physique (notre répertoire **Client**) et enfin l'adresse IP (l'IP de notre cluster front-end : 172.16.4.25) :

Ajouter un site Web

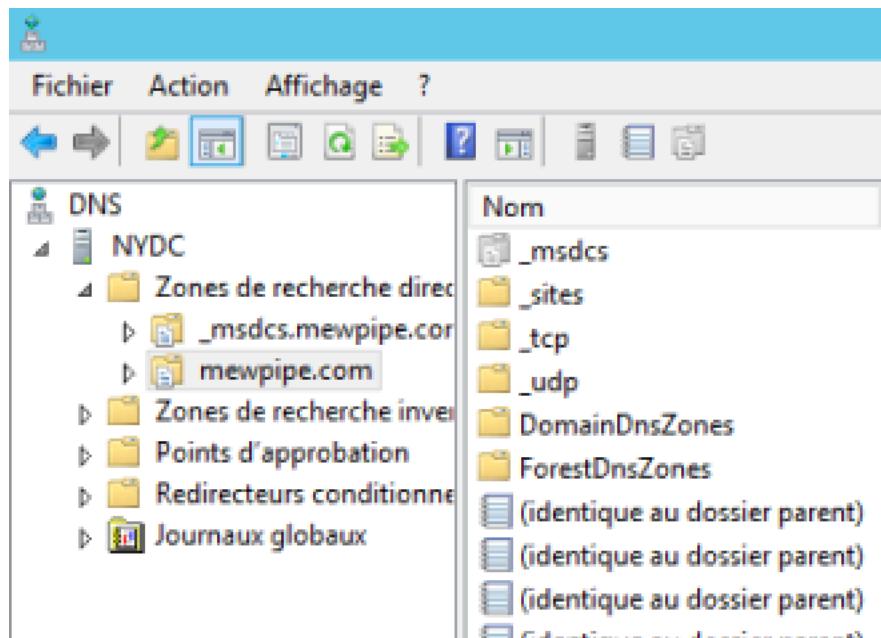
Nom du site :	Pool d'applications :	<input type="button" value="Sélectionner..."/>
<input type="text" value="mewpipe"/>	<input type="text" value="mewpipe"/>	
Répertoire de contenu		
Chemin d'accès physique :	<input type="text" value="C:\inetpub\wwwroot\Client"/>	<input type="button" value="..."/>
Authentification directe		
<input type="button" value="Se connecter en tant que..."/>	<input type="button" value="Tester les paramètres..."/>	
Liaison		
Type :	Adresse IP :	Port :
<input checked="" type="radio" value="http"/>	<input type="text" value="172.16.4.25"/>	<input type="text" value="80"/>
Nom de l'hôte :		
<input type="text"/>		
Exemple : www.contoso.com ou marketing.contoso.com		
<input checked="" type="checkbox"/> Démarrez le site Web immédiatement		
<input type="button" value="OK"/>		<input type="button" value="Annuler"/>

Nous pouvons alors constater que notre site est créé et qu'il tourne :

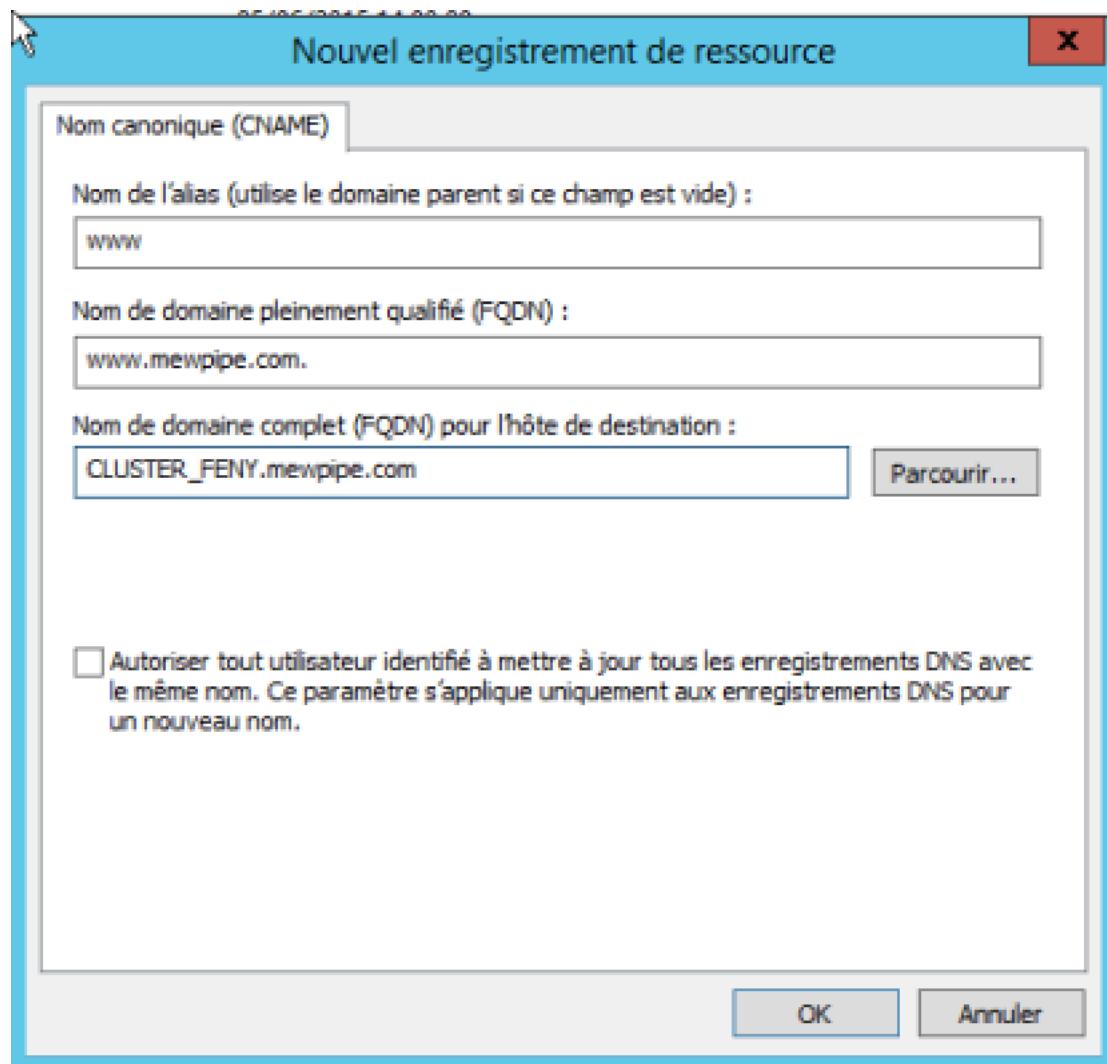
Filtrer :	Atteindre	Afficher tout	Regrouper par :	Aucun regroupement
Nom	ID	État	Liaison	Chemin d'accès
Default Web Site	1	Arrêté (http)	*:80 (http)	%SystemDrive%\inetpub\wwwroot
mewpipe	2	Démarré (...)	172.16.4.25:80 (http)	C:\inetpub\wwwroot\Client

iii. Création de l'alias du site web

Nous allons maintenant créer un alias sur le nom FQDN de notre cluster front-end afin d'y accéder via l'adresse www.mewpipe.com. Pour cela, on se rend sur le contrôleur de domaine (NYDC), on ouvre le **Gestionnaire DNS**, via l'onglet **Outils** du **Gestionnaire de serveurs**. On déploie l'arborescence et on double-clique sur notre domaine **mewpipe.com** :



On effectue alors un clic-droit, et on va cliquer sur **Nouveau alias (CNAME)**. On va alors renseigner le nom de l'alias (**www**), ainsi que le nom FQDN de l'hôte de destination (**CLUSTER_FENY.mewpipe.com**) :



Nous pouvons alors voir notre alias dans la liste des enregistrements de notre domaine :

	Nom	Type	Données	Horodateur
irec	_msdcs			
cor	_sites			
iver	_tcp			
nne	_udp			
	DomainDnsZones			
	ForestDnsZones			
	(identique au dossier parent)	Source de nom (SOA)	[305], nydc.mewpipe.com...	statique
	(identique au dossier parent)	Serveur de noms (NS)	txdc.mewpipe.com.	statique
	(identique au dossier parent)	Serveur de noms (NS)	nydc.mewpipe.com.	statique
	(identique au dossier parent)	Hôte (A)	172.16.4.1	05/06/2015 14:00:00
	(identique au dossier parent)	Hôte (A)	172.16.6.1	29/05/2015 12:00:00
	(identique au dossier parent)	Hôte (A)	192.168.212.183	12/06/2015 10:00:00
	Cluster-ISCSI	Hôte (A)	172.16.4.42	27/05/2015 16:00:00
	CLUSTER_BDDNY	Hôte (A)	172.16.4.45	11/06/2015 16:00:00
	CLUSTER_BENY	Hôte (A)	172.16.4.35	09/06/2015 14:00:00
	CLUSTER_FENY	Hôte (A)	172.16.4.25	12/06/2015 11:00:00
	NYBDD1	Hôte (A)	172.16.4.22	10/06/2015 17:00:00
	NYBDD2	Hôte (A)	172.16.4.32	11/06/2015 15:00:00
	NYBE1	Hôte (A)	172.16.4.21	08/06/2015 15:00:00
	NYBE2	Hôte (A)	172.16.4.31	08/06/2015 15:00:00
	nydc	Hôte (A)	172.16.4.1	statique
	nydc	Hôte (A)	192.168.212.183	statique
	NYFE1	Hôte (A)	172.16.4.20	12/06/2015 10:00:00
	NYFE2	Hôte (A)	172.16.4.30	12/06/2015 11:00:00
	NYFIL1	Hôte (A)	172.16.4.40	27/05/2015 15:00:00
	NYFIL2	Hôte (A)	172.16.4.41	27/05/2015 15:00:00
	NYVCE	Hôte (A)	172.16.4.10	08/06/2015 14:00:00
	TXDC	Hôte (A)	172.16.10.1	statique
	www	Alias (CNAME)	CLUSTER_FENY.mewpipe...	

Enfin, nous pouvons lancer notre site web dans notre navigateur préféré via l'adresse www.mewpipe.com :

The screenshot shows a web browser window for 'Mew Pipe - Video' at www.mewpipe.com/#/user/profile. The page has a dark blue header with the 'MewPipe' logo and a slogan 'We must do what nobody doing for you'. It features a navigation bar with 'HOME', 'MY VIDEO', 'UPLOAD', and 'PROFILE' links. A search bar is present. On the left, there's a sidebar with an 'Edit account' button and a list of profile details:

Joined	June 12th 2015, 1:22
Email:	tt@tt.fr
Real name	tt
Birthdate	June 12th 2015
Role:	Client
Last seen	Yesterday

The main content area is titled 'Profile' and contains a message 'Hello tt tt !' with 'You' and 'Stats' buttons below it. At the bottom, there's an 'Activity' section.

N. Mise en place d'un stockage iSCSI sur un réseau dédié pour les VMs

a) Contexte

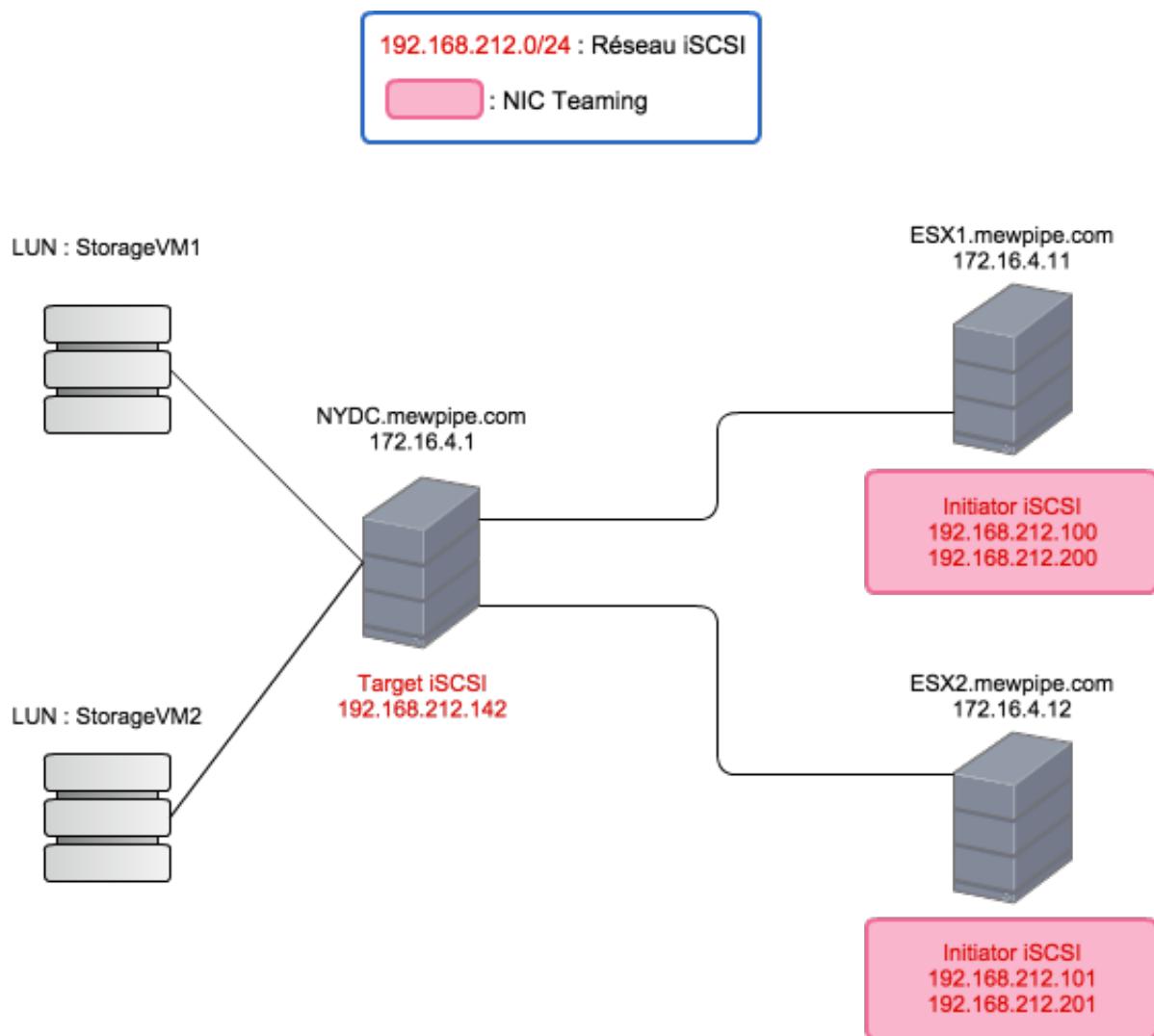
Comme indiqué dans le cahier des charges, le stockage des machines virtuelles doit s'effectuer sur un réseau iSCSI dédié. Ce point sera consacré à la mise en place du stockage et du réseau iSCSI dédié.

b) Principe et application

La mise en place d'un stockage iSCSI comprend l'implémentation d'une Target iSCSI et dans le cas présent, deux initiateurs iSCSI sont demandés.

Dans cette présentation, la target iSCSI a été implémenté sur le serveur contrôleur de domaine, le réseau utilisé pour le stockage iSCSI est 192.168.212.0/24.

Le schéma suivant récapitule le fonctionnement :



Ainsi, le stockage des machines virtuelles s'effectuent exclusivement sur le réseau iSCSI dédié en 192.168.212.0/24. Les initiateurs possèdent deux cartes réseaux en NIC Teaming afin de prévoir la panne de l'une d'entre elles.

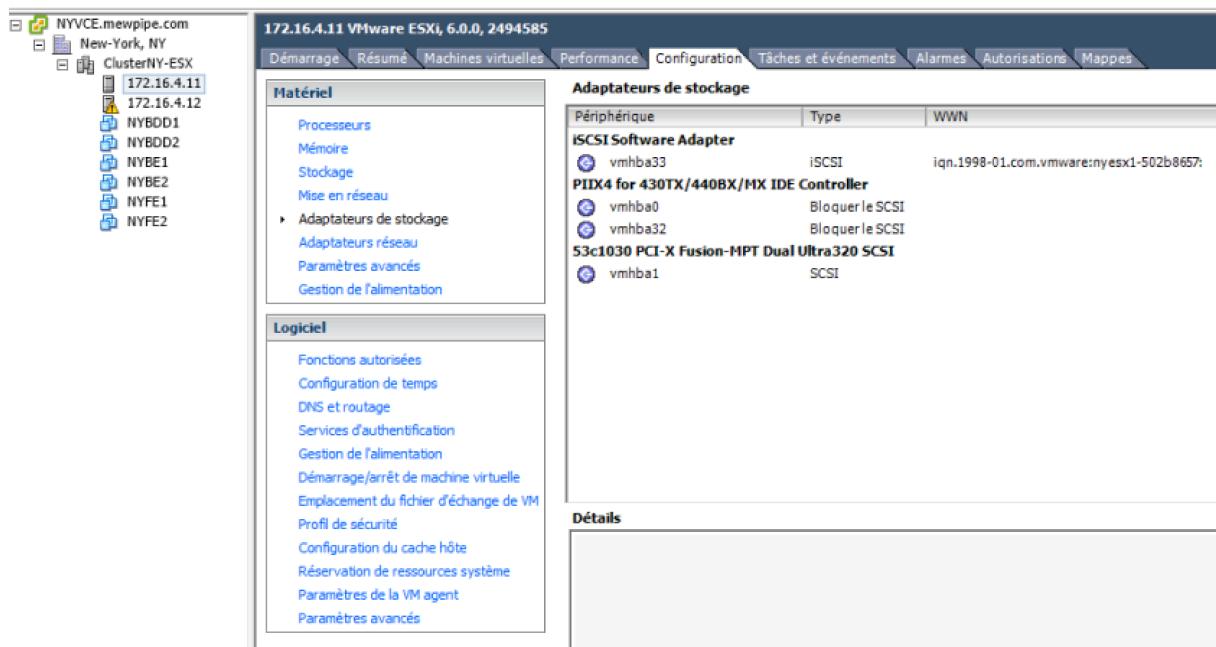
c) Configuration

i. Ajout des adaptateurs réseaux pour le réseau iSCSI dédié

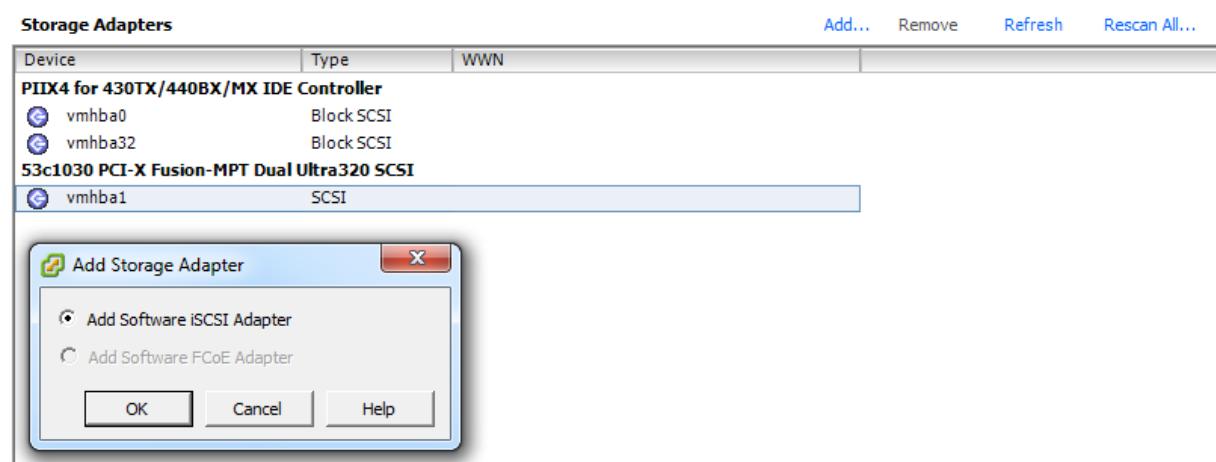
Afin de pouvoir faire transiter tous les flux de stockage iSCSI via le réseau approprié il faut ajouter un adaptateur réseau sur notre contrôleur de domaine (NYDC.mewpipe.com) qui fera office de Target iSCSI et deux adaptateurs réseaux sur chacun de nos ESXi. Tout ces adaptateurs sont à ajouter dans le réseau 192.168.212.0/24.

ii. Ajout des adaptateurs de stockage iSCSI sur les initiateurs

Pour ajouter nos adaptateurs de stockage iSCSI sur nos initiateurs (ESXi), on se rend sur l'**interface client vSphere**. Après avoir sélectionné notre premier ESXi dans la liste de gauche, on se rend dans l'onglet **Configuration** et on va cliquer sur **Adaptateurs de stockage** dans la liste de gauche, on obtient alors l'interface suivante (Après ajout de l'adaptateur iSCSI) :



Ainsi, pour ajouter notre adaptateur, il faut cliquer sur **Ajouter...** et confirmer le choix d'un adaptateur iSCSI, une fenêtre s'ouvre alors pour nous demander d'aller dans les propriétés de l'adaptateur pour en compléter sa configuration, cliquer sur **OK** :



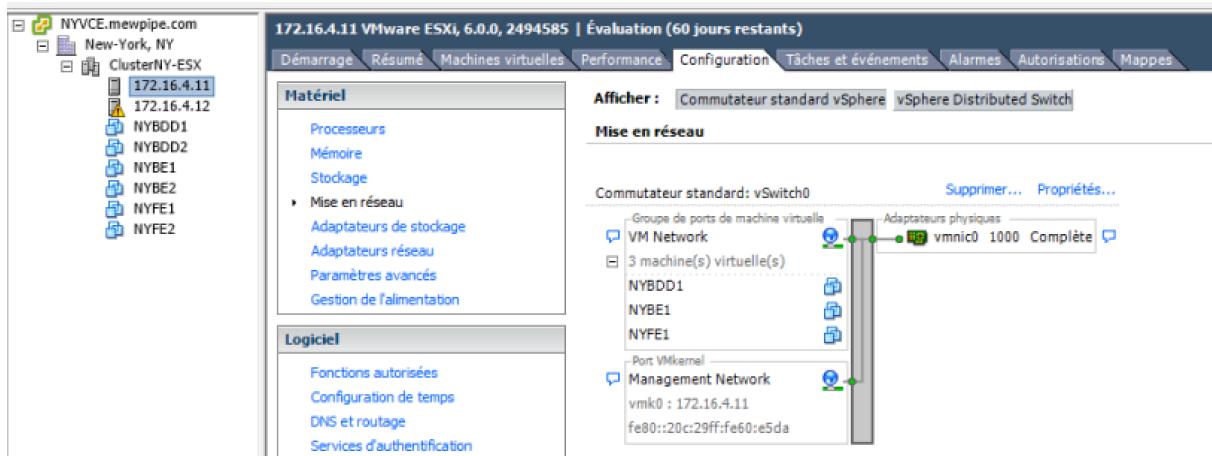
Ensuite, nous faisons de même pour notre deuxième initiateur, on remarque alors qu'un nom IQN unique a été généré par adaptateur, dans notre cas :

Périphérique	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:nyesx1-502b8657:
Périphérique	Type	WWN
iSCSI Software Adapter		
vmhba33	iSCSI	iqn.1998-01.com.vmware:nyesx2-0e9644ee:

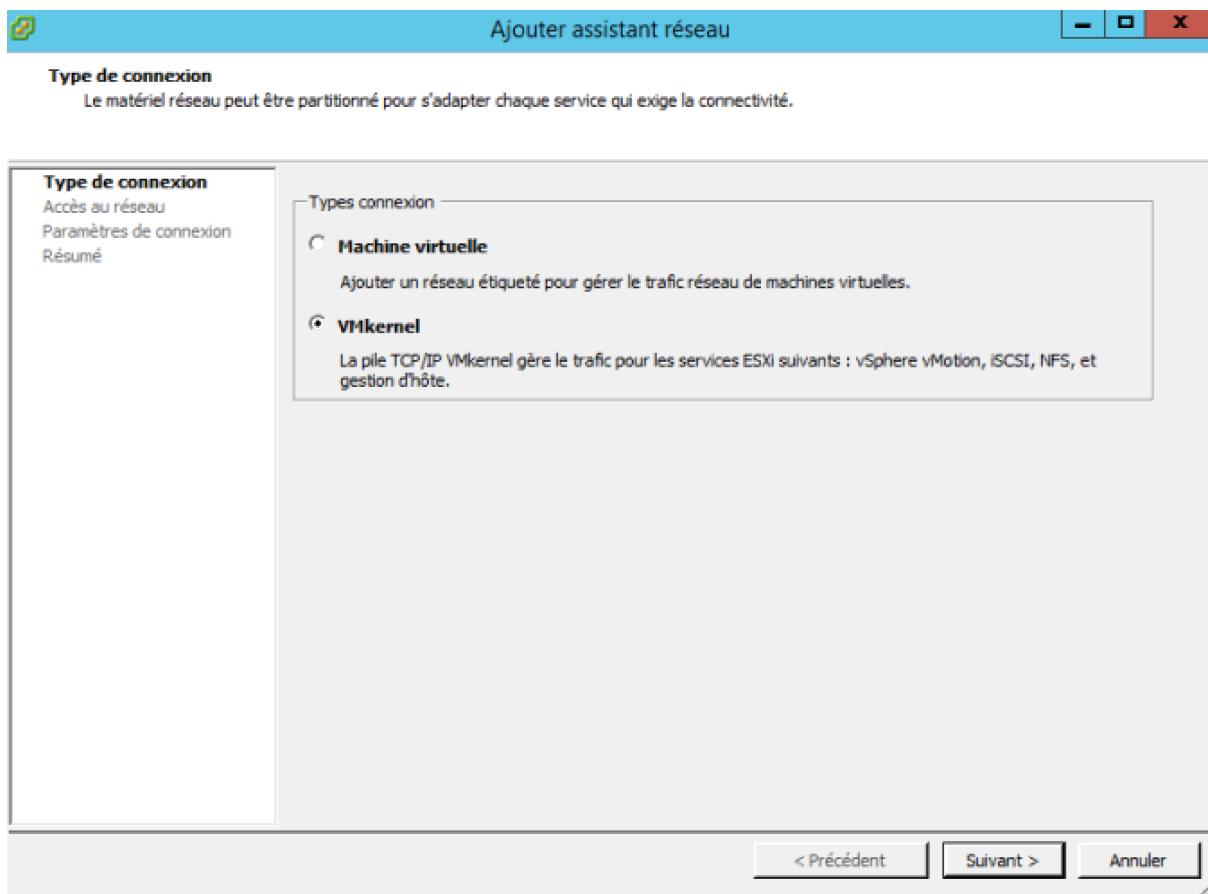
Nous allons maintenant configurer notre réseau iSCSI.

iii. Configuration du réseau iSCSI

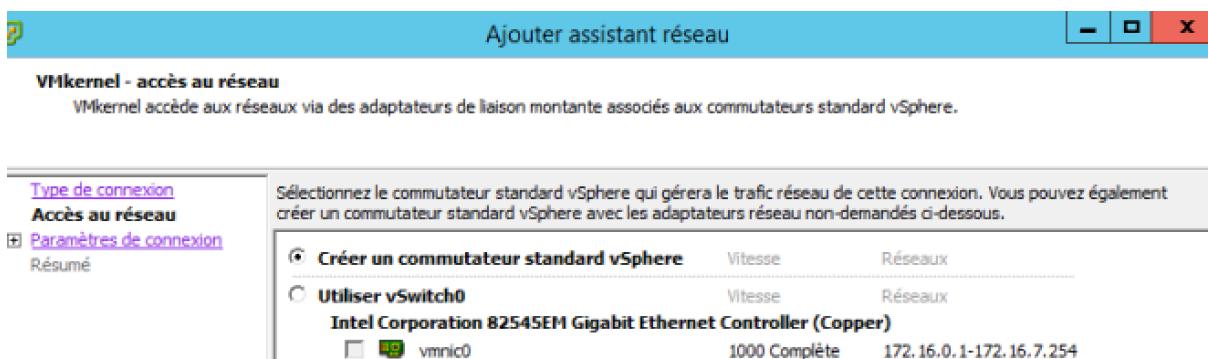
Pour cela, après avoir sélectionné notre premier ESXi dans la liste de gauche de vSphere client, nous nous rendons dans l'onglet **Configuration** puis nous cliquons sur **Mise en réseau** afin d'obtenir l'interface suivante :



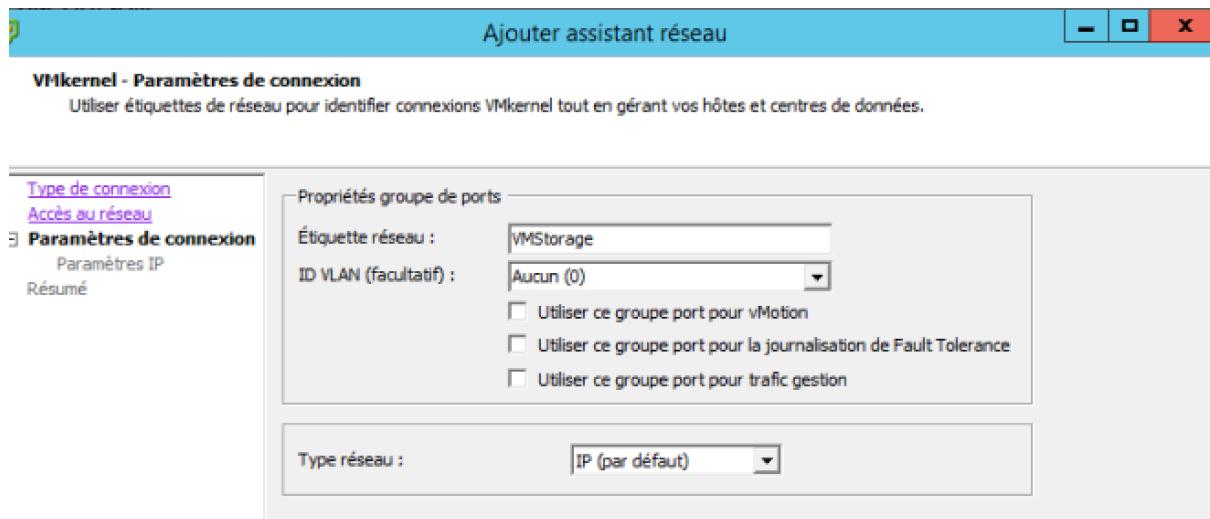
Cliquons alors sur **Ajouter une mise en réseau**, une nouvelle fenêtre s'ouvre, on choisit alors l'option VMkernel car c'est ce type de connexion qui gère les flux iSCSI :



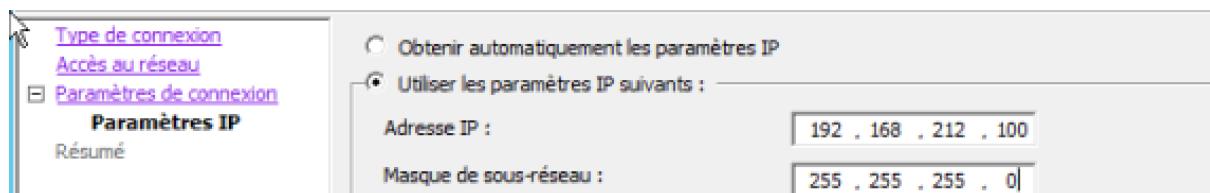
Après avoir cliquer sur **Suivant**, nous choisissons de créer un Commutateur standard vSphere avec **vmnic1** comme adaptateur :



Cliquons sur **Suivant**, il faut maintenant donner un nom à notre nouveau réseau, dans notre cas ce sera **VMStorage** :



Enfin, nous lui adressons une adresse IP :



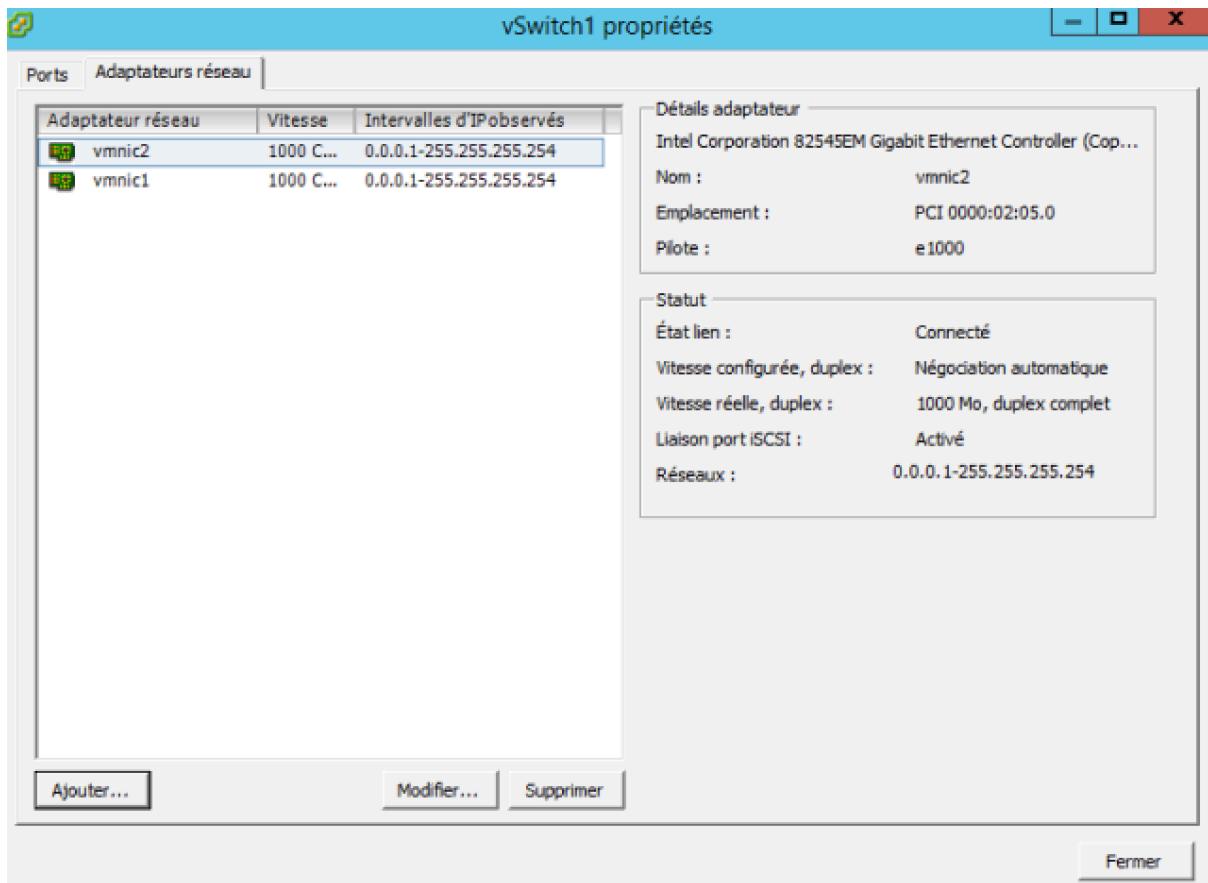
Cliquer alors **Suivant** puis sur **Terminer**.

Notre nouveau réseau est alors créé. On va maintenant ajouter notre deuxième adaptateur réseau et configurer un NIC Teaming de nos deux cartes afin de tolérer la panne de l'une d'entre elles.

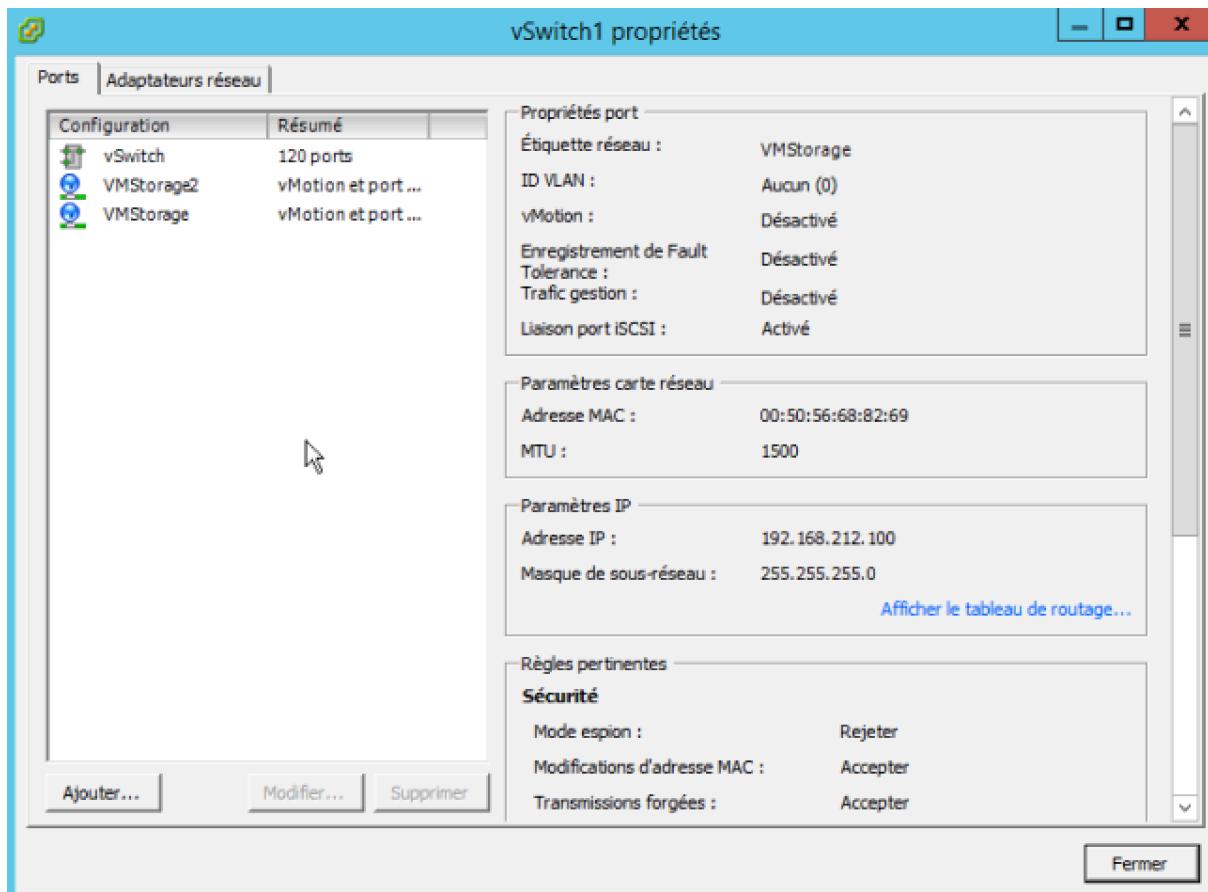
Pour cela, on va se rendre dans les **Propriétés** de notre nouveau commutateur virtuel :



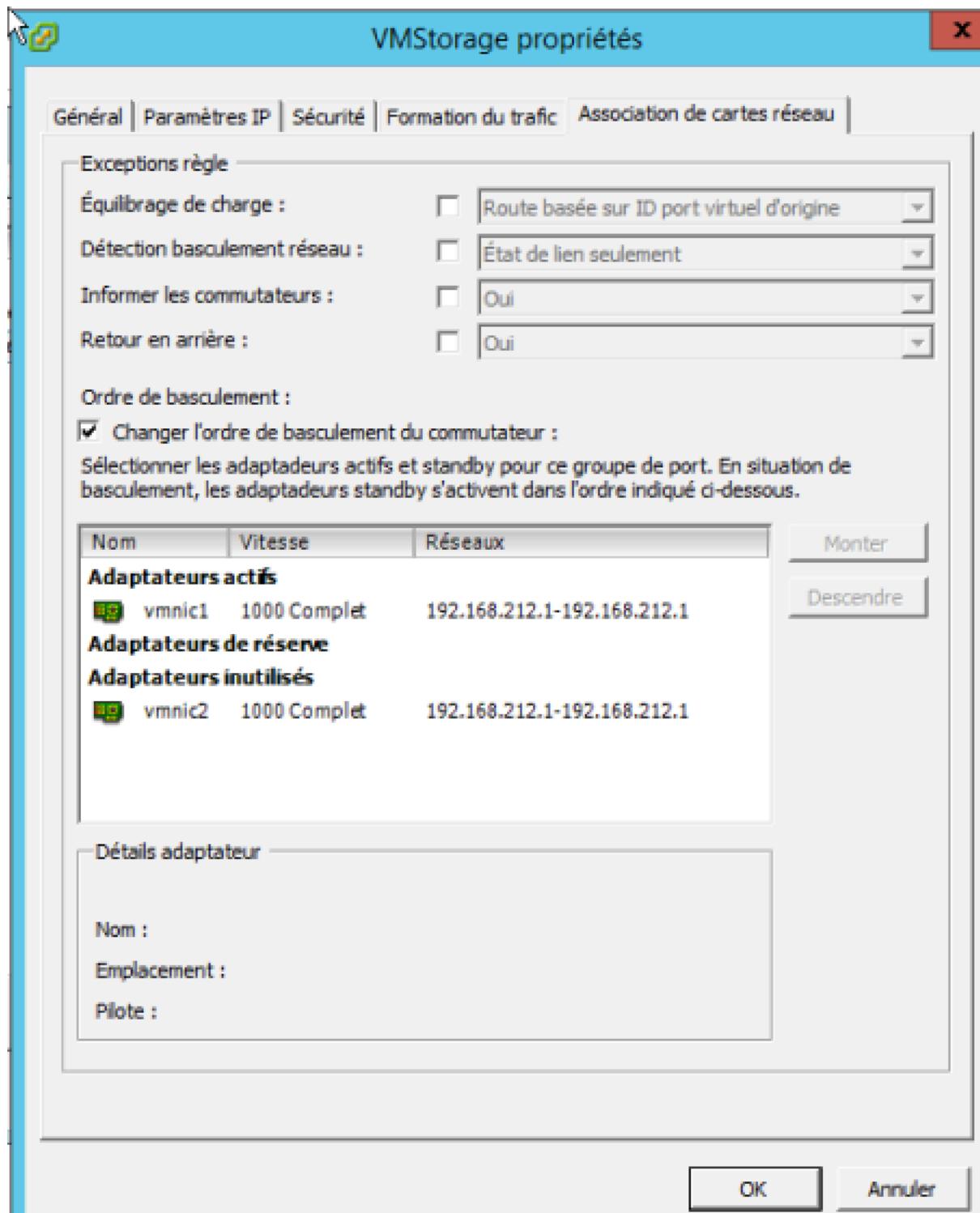
Dans l'onglet **Adaptateurs réseau**, cliquons sur **Ajouter** en bas de la fenêtre. Une nouvelle fenêtre vient alors s'ouvrir, nous sélectionnons notre adaptateur **vmnic2**, on clique sur **Suivant** et on laisse tout par défaut pour le moment. Validons, nous obtenons alors ceci dans l'onglet **Adaptateurs réseau** de notre **vSwitch1** :



Rendons-nous dans l'onglet **Ports**, puis cliquons sur **Ajouter...** afin d'ajouter une seconde mise en réseau. Comme tout à l'heure, on choisit **VMkernel**, on lui indique notre **vmnic2**, on le nomme **VMStorage2**, on lui indique une nouvelle adresse IP et on valide. On obtient alors l'interface suivante dans l'onglet **Ports** des propriétés de notre **vSwitch1** :



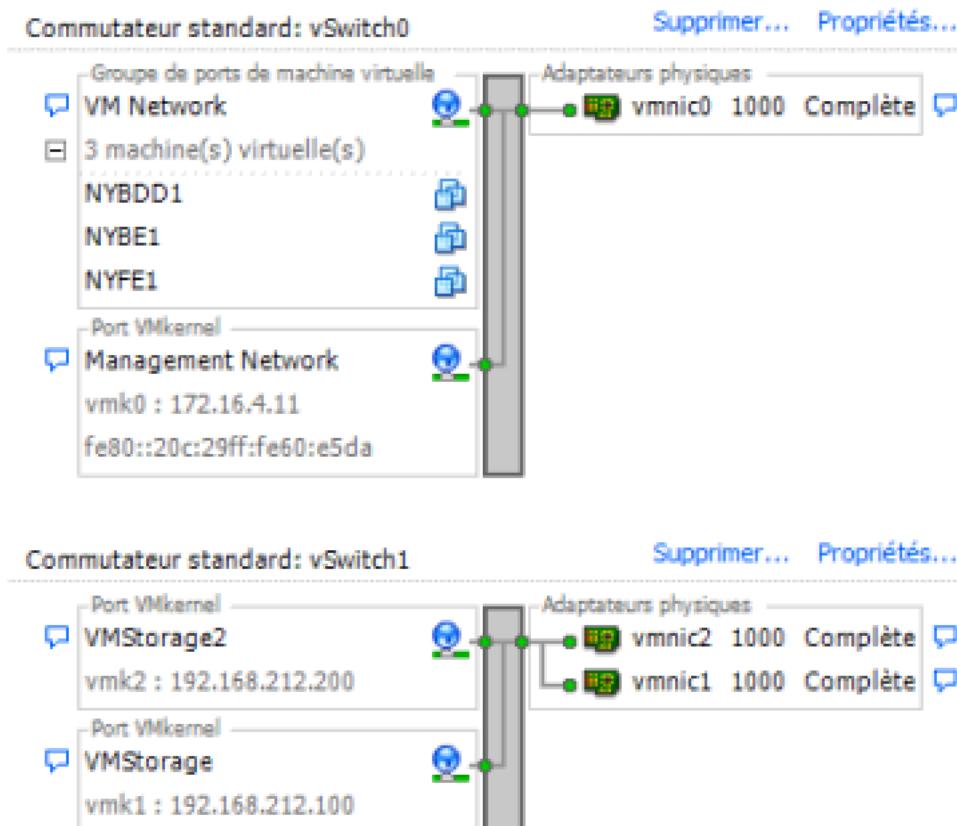
Sélectionnons **VMStorage**, puis cliquons sur **Modifier...** une nouvelle fenêtre s'ouvre, rendons-nous dans l'onglet **Association de cartes réseau**. Enfin, cocher la case **changer l'ordre de basculement du commutateur** puis mettre un adaptateur réseau dans les adaptateurs actifs et le second dans les adaptateurs inutilisés :



Réitérer cette opération pour **VMStorage2** en inversant les adaptateurs réseau (mettre l'actif du VMStorage en inutilisé dans VMStorage2 et inversement)

On obtient alors la mise en réseau suivante :

Mise en réseau



Il faut maintenant effectuer les mêmes opérations sur notre deuxième ESXi, en donnant exactement les mêmes noms, seules les adresses IP doivent changer.

Une fois cette opération effectuée, nous allons installer le rôle Target iSCSI sur notre contrôleur de domaine.

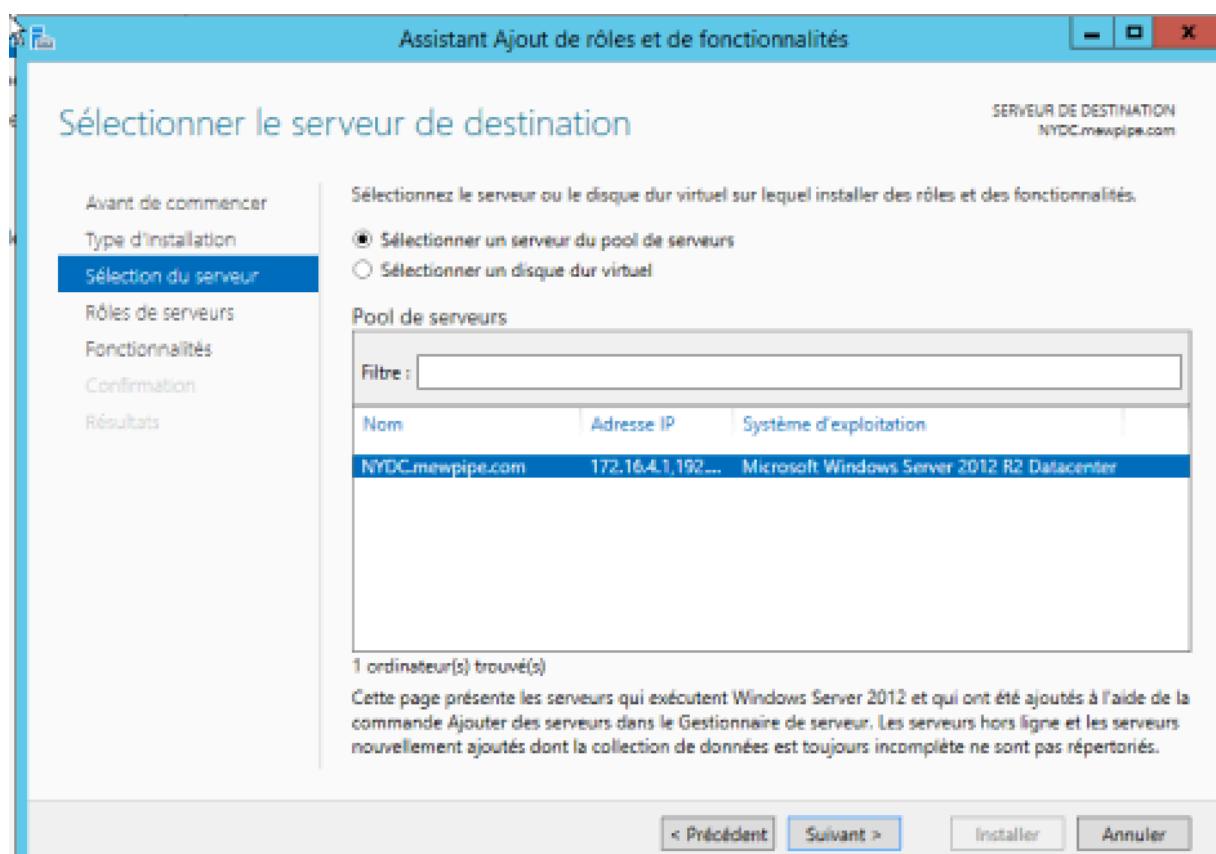
iv. Installation et configuration de la Target iSCSI

Avant d'entrer dans la configuration de la target iSCSI on va ajouter un disque à notre contrôleur de domaine. Ce dernier servira à monter des volumes logiques qui seront ensuite utilisés pour le stockage de nos machines virtuelles.

Dans le **Gestionnaire de serveur**, cliquons sur **Ajouter des rôles et des fonctionnalités** :

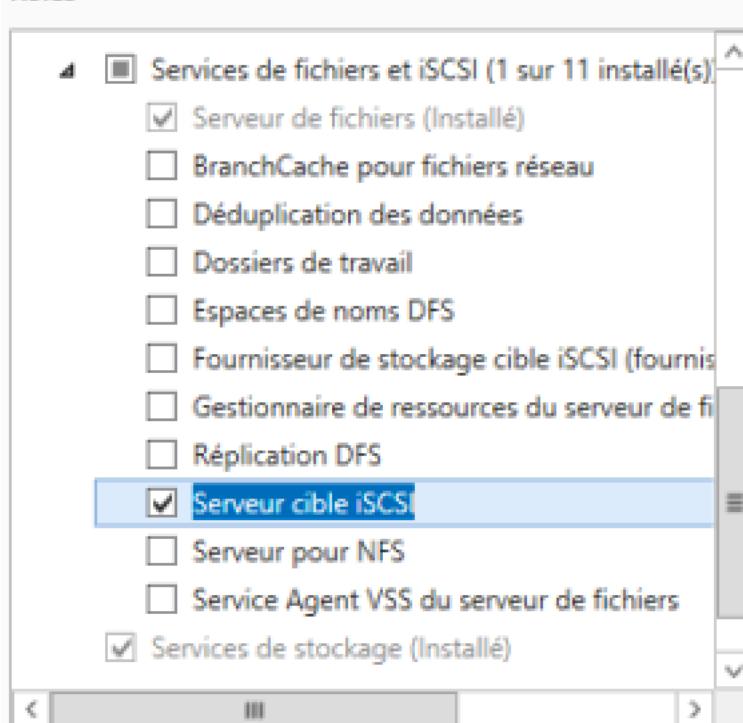


Cliquons alors sur **Suivant**, laissons une installation basée sur un rôle ou une fonctionnalité, on clique sur **Suivant**, on vérifie qu'il a bien choisi notre serveur et de nouveau on clique sur **Suivant** :



On va ensuite chercher la fonctionnalité **Serveur cible iSCSI** :

Rôles



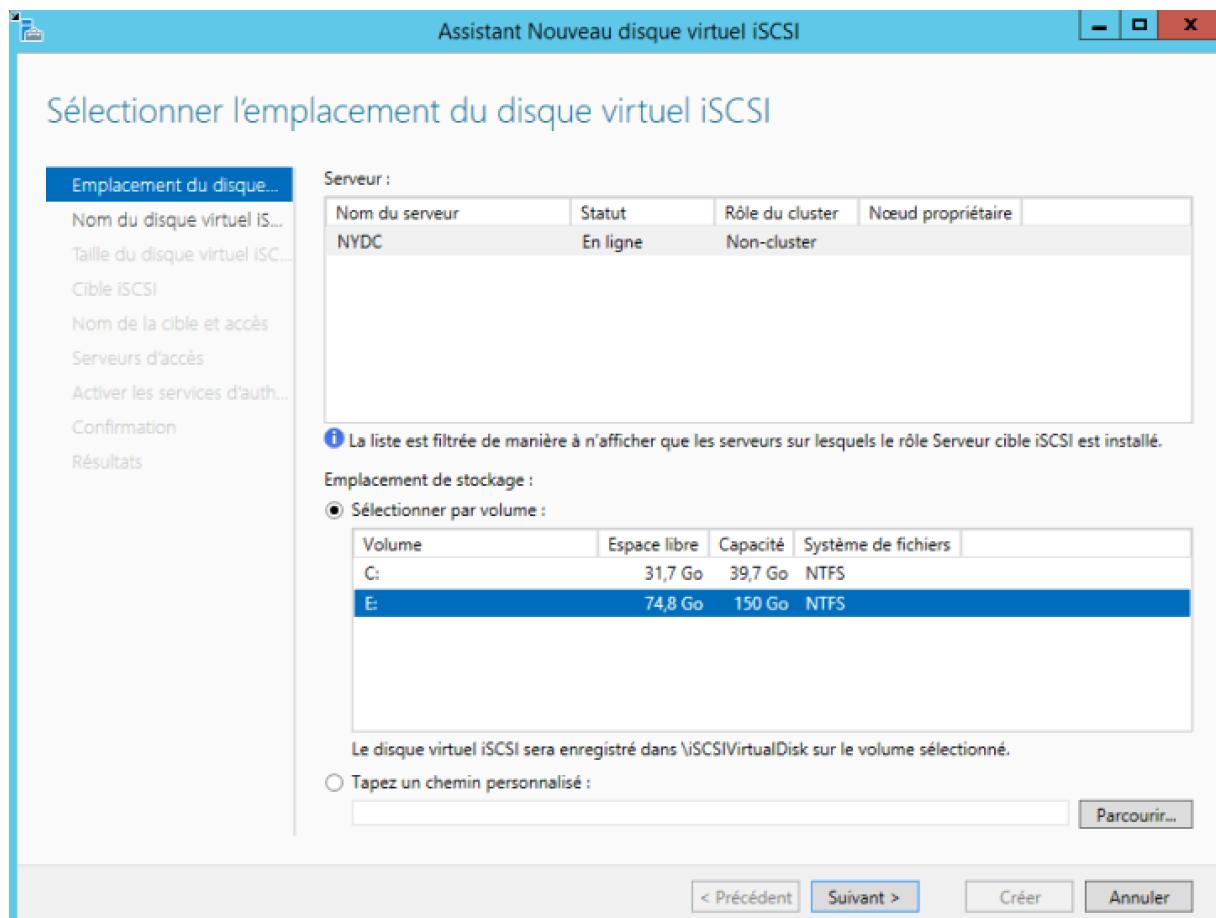
Cliquons sur **Suivant** puis sur **Installer**, on redémarre notre serveur.

Dans le **Gestionnaire de serveur**, cliquons sur **Service de fichiers et de stockage** dans la liste de gauche puis sur **iSCSI**, nous obtenons alors l'interface suivante :

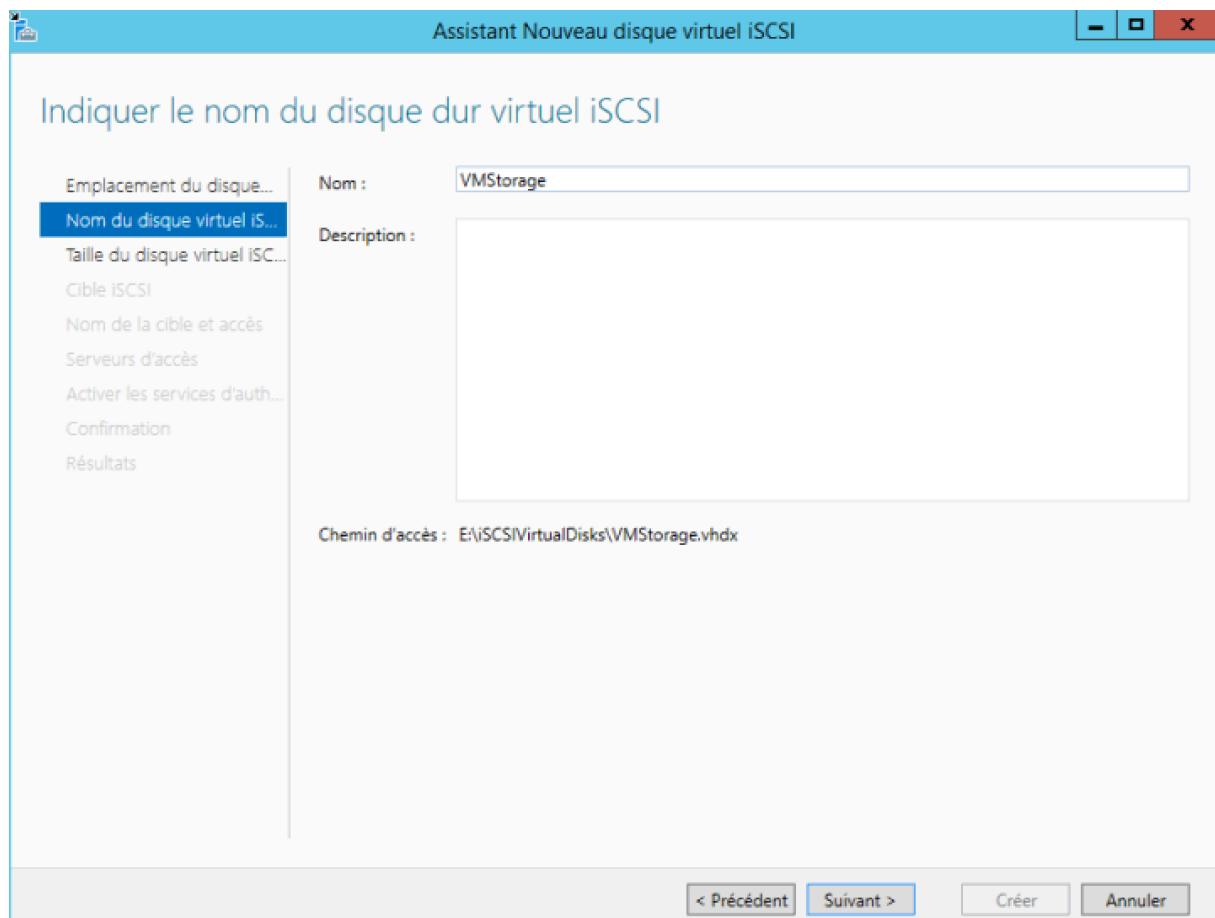
The screenshot shows the 'DISQUES VIRTUELS iSCSI' interface. On the left, a navigation pane lists 'Serveurs', 'Volumes', 'Disques', 'Pools de stockage', 'Partages', 'iSCSI' (which is selected and highlighted in blue), and 'Dossier de travail'. The main pane displays a table titled 'Tous les disques virtuels iSCSI | 1 au total'. It includes a 'Filtrer' search bar and a 'Chemin d'accès' column showing 'NYDC (1)' and the path 'E:\iSCSIVirtualDisks\StorageVM1.vhdx'.

Chemin d'accès	État
NYDC (1) E:\iSCSIVirtualDisks\StorageVM1.vhdx	

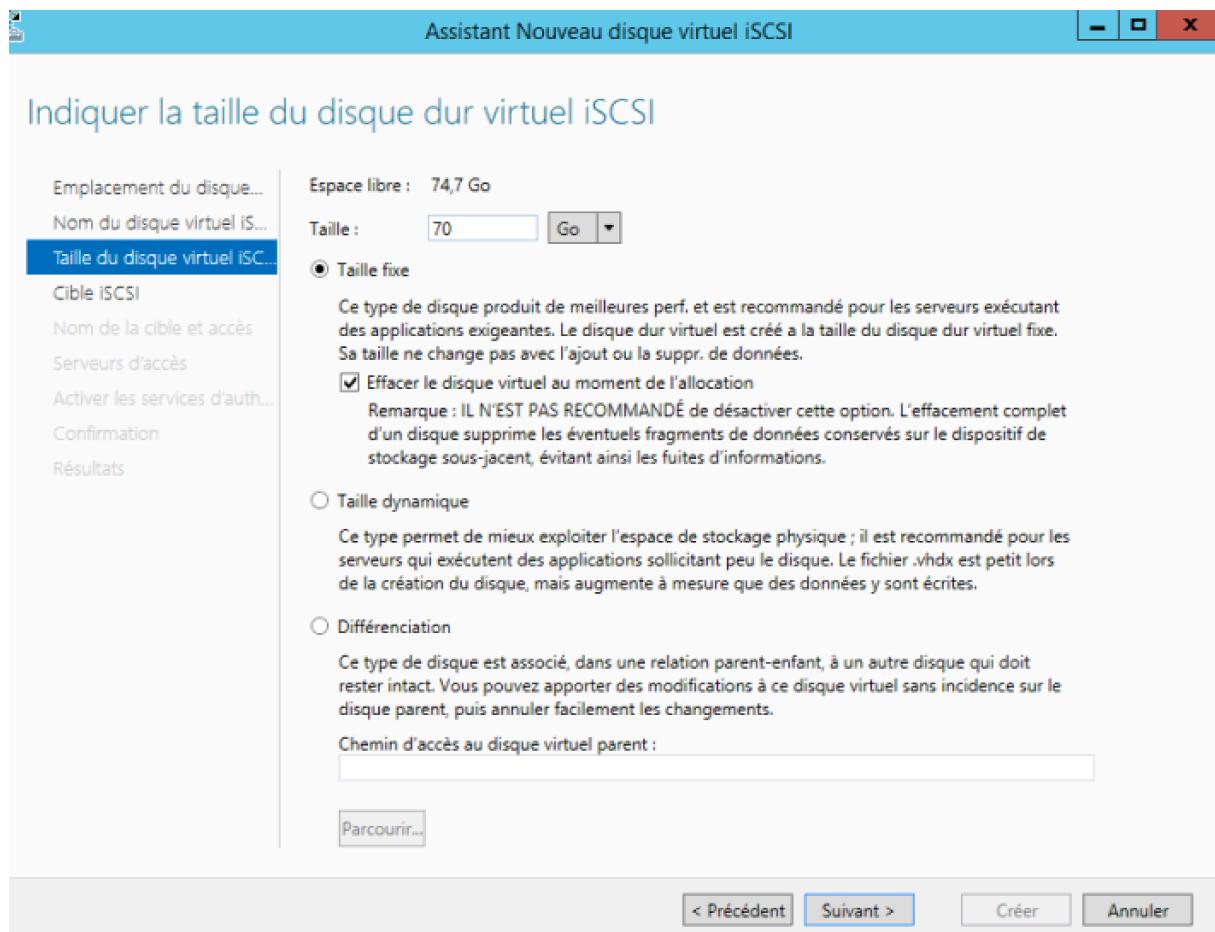
Cliquons alors sur **Tâches** en haut à droite de la fenêtre, puis sur **Nouveau disque virtuel iSCSI...** Une nouvelle fenêtre apparaît. On choisit notre disque récemment ajouté. (S'il n'apparaît pas, il faut mettre en ligne le disque et le monter pour cela aller **Outils>Gestion de l'ordinateur>Gestion des disques** clic-droit **Mettre en ligne** puis **Nouveau volume**) :



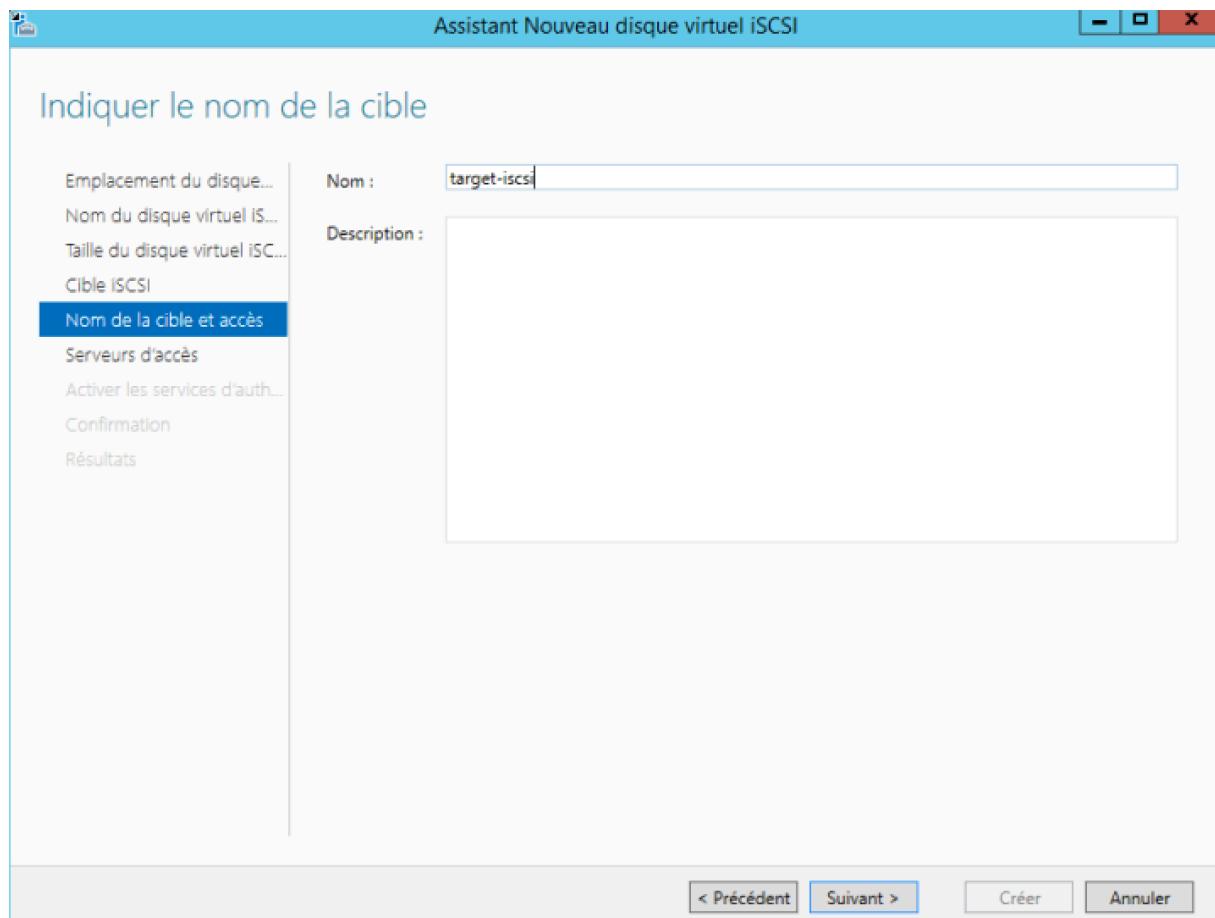
Après sélection de notre volume, nous donnons un nom à notre nouveau disque virtuel iSCSI :



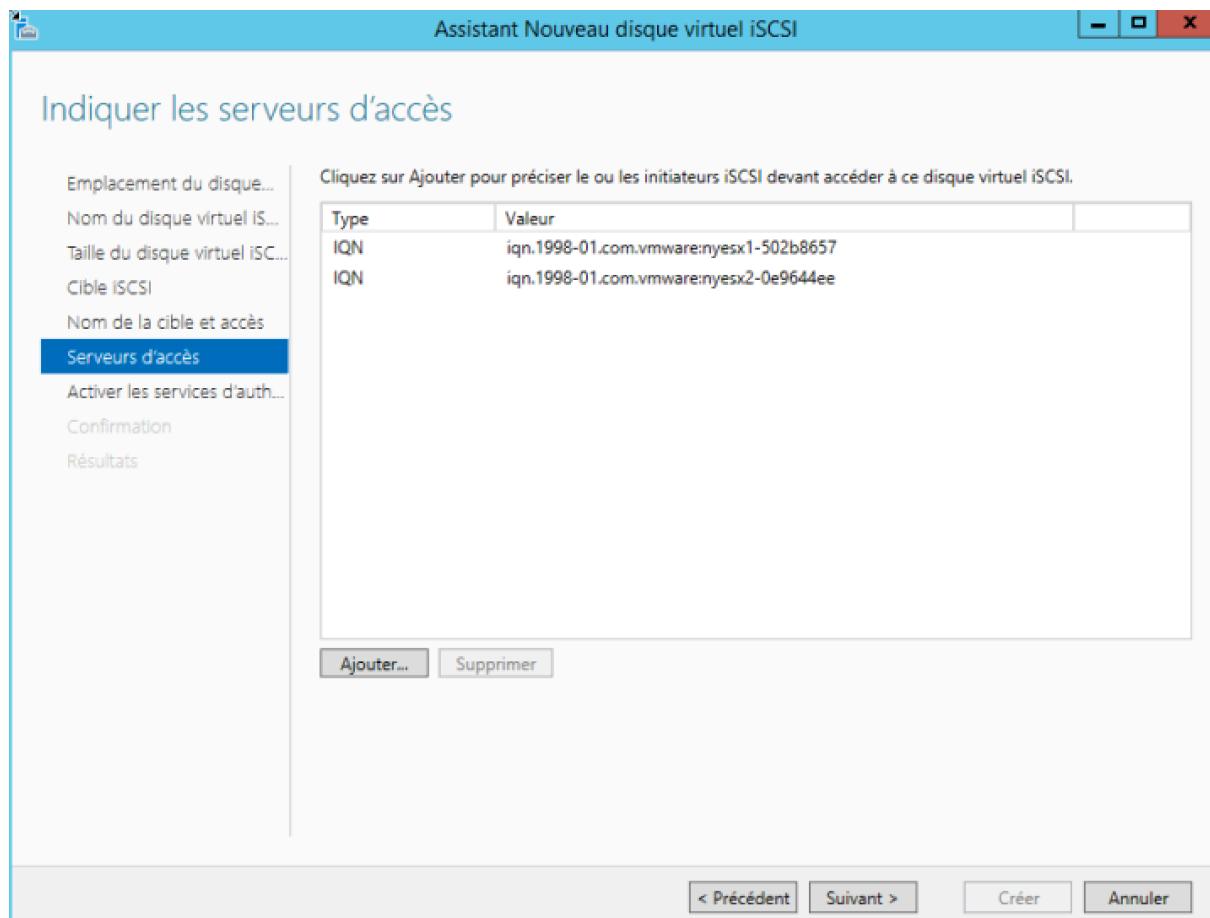
Cliquons sur **Suivant**, il faut alors choisir la taille de notre disque :



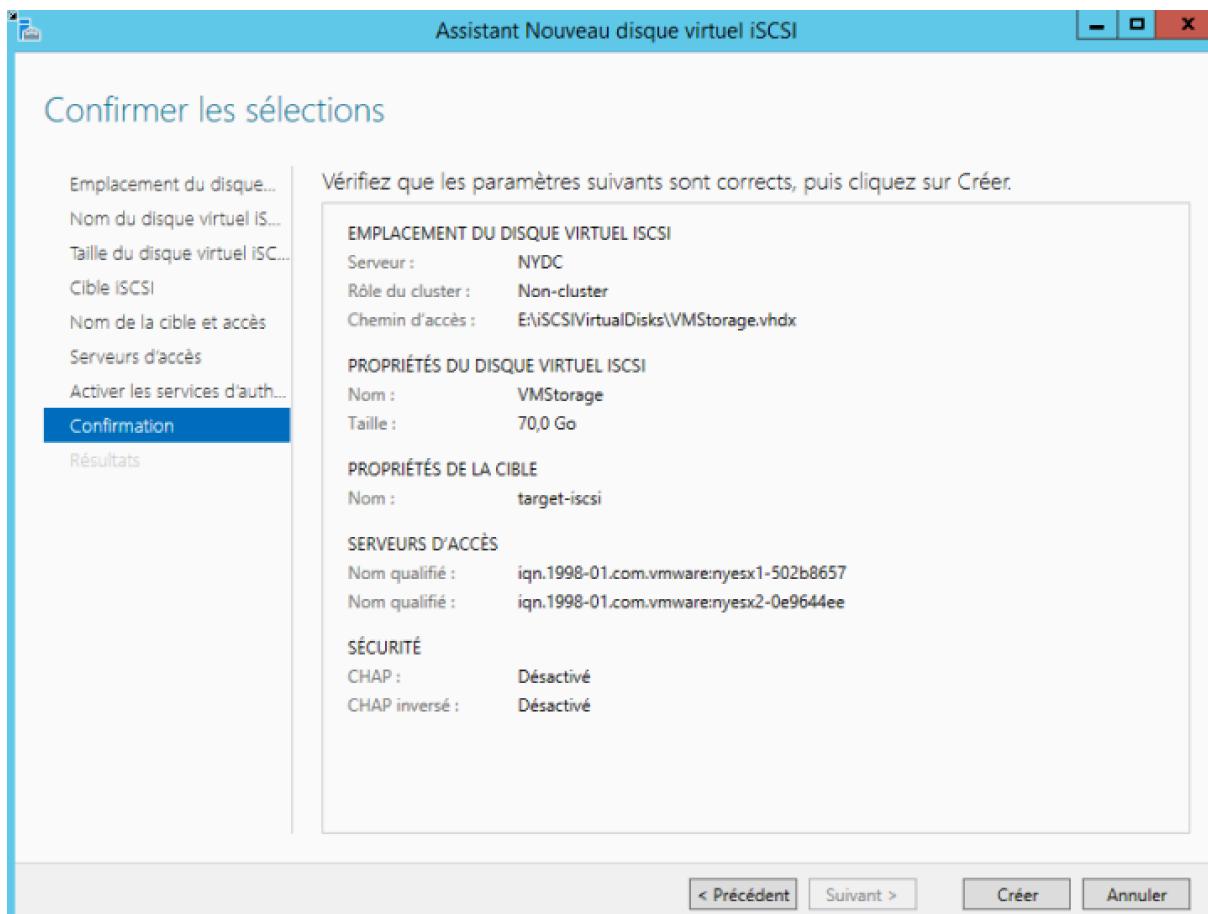
Ensuite, nous choisissons de créer une nouvelle target iSCSI, nous la nommons :



Nous ajoutons nos deux initiateurs dans la liste des serveurs d'accès :



Vient alors un résumé :



Nous pouvons maintenant cliquer sur **Créer**, notre disque virtuel iSCSI et notre nouvelle target iSCSI sont maintenant créés.

v. *Création de la nouvelle banque de données*

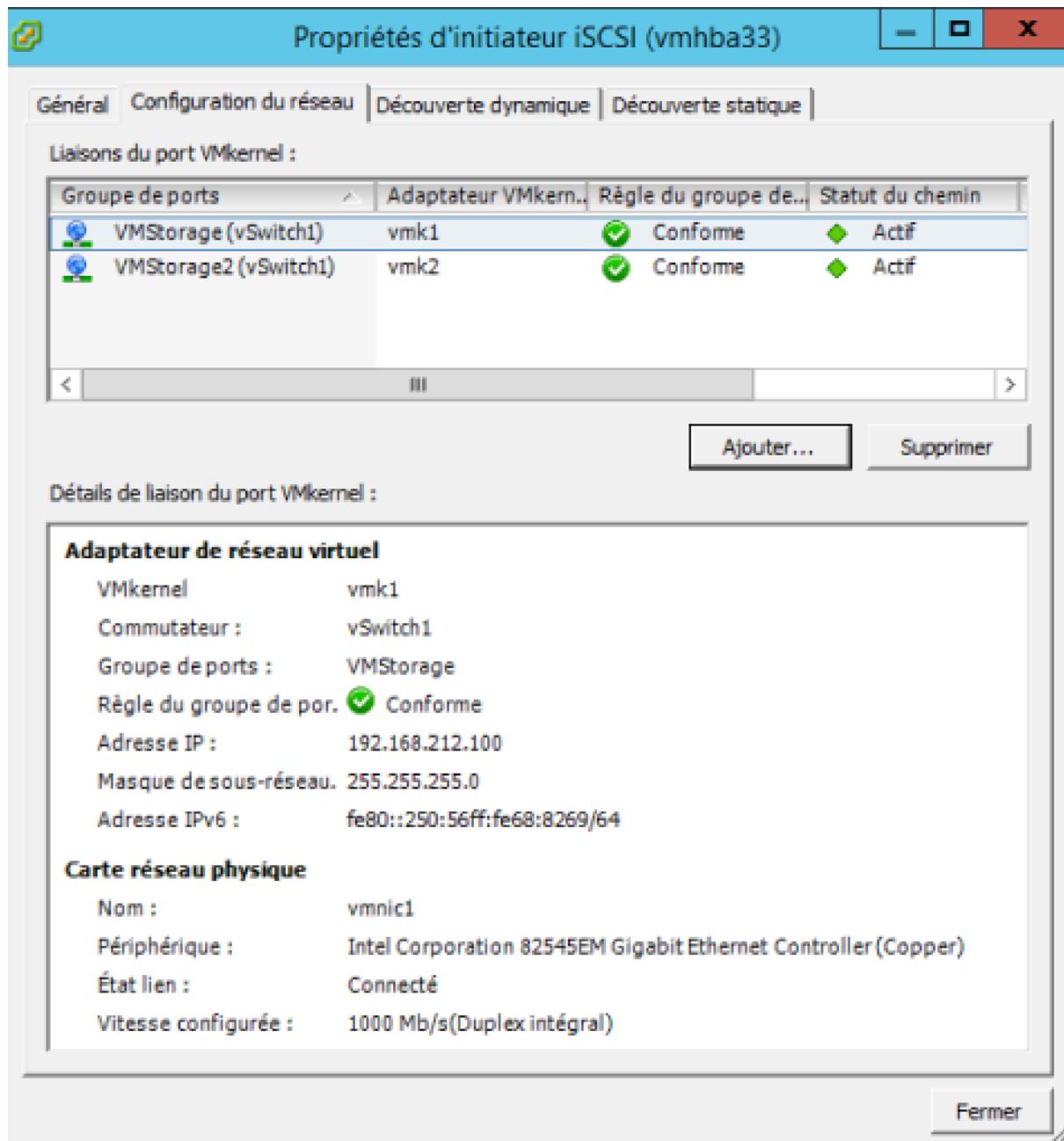
On va désormais créer notre nouvelle banque de données qui nous permettra de stocker les machines virtuelles.

Pour cela, rendons-nous sur notre Client vSphere, après avoir sélectionné notre premier ESXi, on se rend dans l'onglet **Configuration** puis nous cliquons sur **Adaptateurs de stockage**, on sélectionne notre adaptateur iSCSI et on clique sur **Propriétés...** :

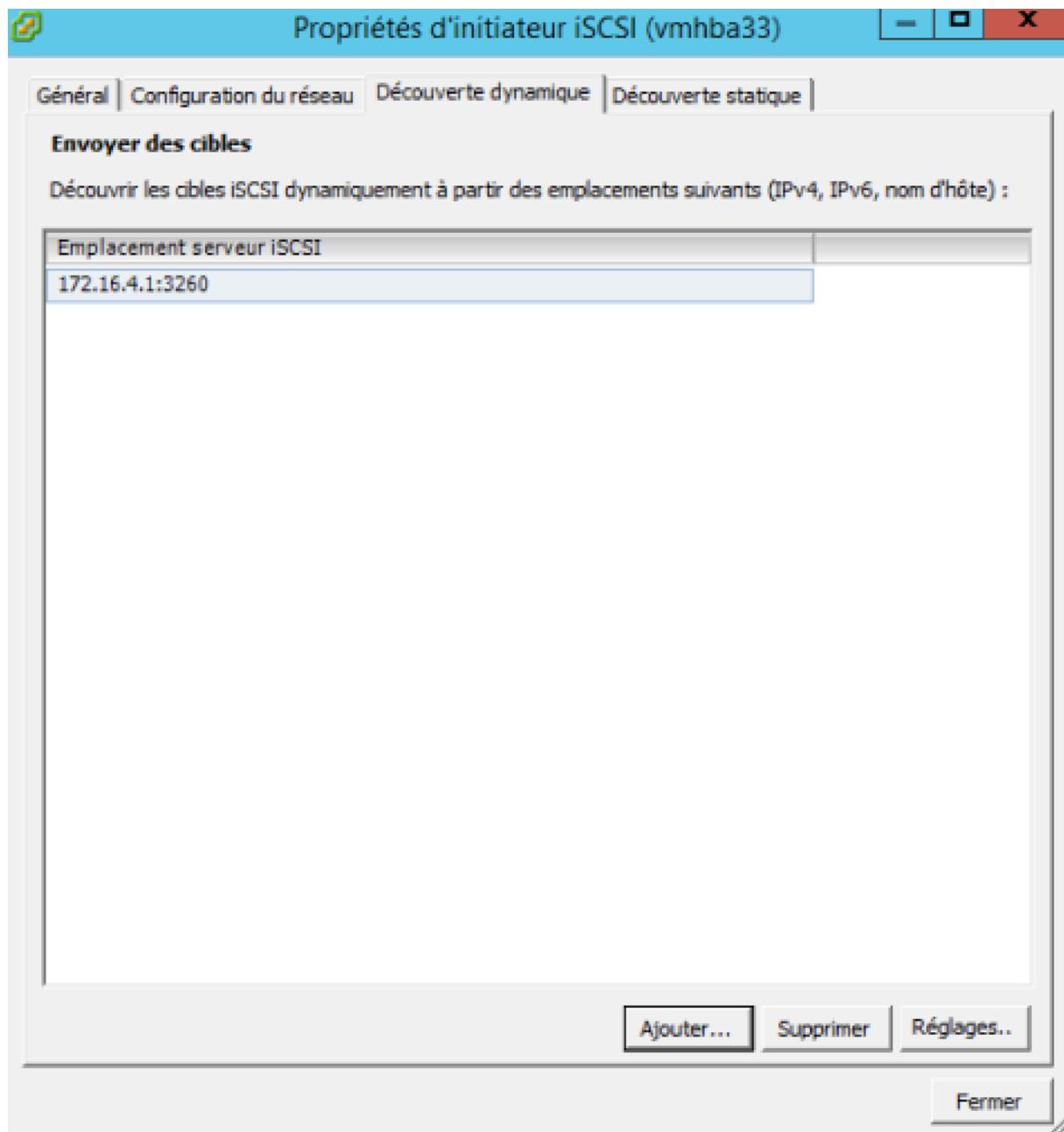
Adaptateurs de stockage		
Périphérique	Type	WWN
vmhba33	ISCSI	iqn.1998-01.com.vmware:yesx1-502b8657
PIIX4 for 430TX/440BX/MX IDE Controller	Bloquer le SCSI	
vmhba0	Bloquer le SCSI	
vmhba32	Bloquer le SCSI	
53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI	SCSI	
vmhba1	SCSI	

Détails	
vmhba33	Propriétés...
Modèle : ISCSI Software Adapter	
Nom iSCSI : iqn.1998-01.com.vmware:yesx1-502b8657	
Alias iSCSI :	
Cibles connectées : 2	Périphériques : 1 Chemins : 2

Nous allons alors dans l'onglet **Configuration du réseau** puis nous ajoutons nos deux **VMStorage** afin d'obtenir ceci :



Enfin, dans l'onglet **Découverte dynamique**, on va ajouter l'adresse IP du serveur où l'on a installé notre Target iSCSI (notre contrôleur de domaine dans notre cas) :



En cliquant sur **Fermer**, le vCenter va effectuer un balayage pour chercher les disques disponibles.

Notre disque apparaît alors :

Adaptateurs de stockage

Péphérique	Type	WWN
ISCSI Software Adapter	ISCSI	iqn.1998-01.com.vmware:nysesx1-502b8657
vmhba33	ISCSI	
vmhba0	Bloquer le SCSI	
vmhba32	Bloquer le SCSI	
PIIX4 pour 430BX/440BX/MX IDE Controller		
vmhba1	SCSI	
53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI		

Ajouter... Supprimer Actualiser Réanalyser tout...

Détails

vmhba33

Modèle :	ISCSI Software Adapter	Propriétés																				
Nom iSCSI :	iqn.1998-01.com.vmware:nysesx1-502b8657																					
Alias iSCSI :																						
Câbles connectées :	2	Péphériques : 1 Chemins : 2																				
Afficher : Banques de données Péphériques																						
<table border="1"> <thead> <tr> <th>Nom</th> <th>Nom exécution</th> <th>État opérationnel</th> <th>LUN</th> <th>Type</th> <th>Type de lecteur</th> <th>Transport</th> <th>Capacité</th> <th>Propriétaire</th> <th>Accélération matérielle</th> </tr> </thead> <tbody> <tr> <td>MSFTiSCSI Disk (naa.60003ff44dc...</td> <td>vmhba33:C4:T0:L0</td> <td>Monté</td> <td>0</td> <td>disk</td> <td>Non-SSD</td> <td>ISCSI</td> <td>75,00 Go</td> <td>NMP</td> <td>Non pris en charge</td> </tr> </tbody> </table>			Nom	Nom exécution	État opérationnel	LUN	Type	Type de lecteur	Transport	Capacité	Propriétaire	Accélération matérielle	MSFTiSCSI Disk (naa.60003ff44dc...	vmhba33:C4:T0:L0	Monté	0	disk	Non-SSD	ISCSI	75,00 Go	NMP	Non pris en charge
Nom	Nom exécution	État opérationnel	LUN	Type	Type de lecteur	Transport	Capacité	Propriétaire	Accélération matérielle													
MSFTiSCSI Disk (naa.60003ff44dc...	vmhba33:C4:T0:L0	Monté	0	disk	Non-SSD	ISCSI	75,00 Go	NMP	Non pris en charge													

Nous pouvons alors maintenant nous rendre dans la partie **Stockage** de l'onglet **Configuration** :

172.16.4.11 VMware ESXi, 6.0.0, 2494585 | Évaluation (60 jours restants)

Démarrage Résumé Machines virtuelles Performances Configuration Tâches et événements Alarmes Autorisations Mappages

Materiel

- Processeurs
- Mémoire
- Stockage**
- Mise en réseau
- Adaptateurs de stockage
- Adaptateurs réseau
- paramètres avancés
- Gestion de l'alimentation

Logiciel

- Fonctions autorisées
- Configuration de temp
- DNS et routage
- Services d'authentification
- Gestion de l'alimentation
- Démarrage/arrêt de machine virtuelle
- Emplacement du fichier d'échange de VM

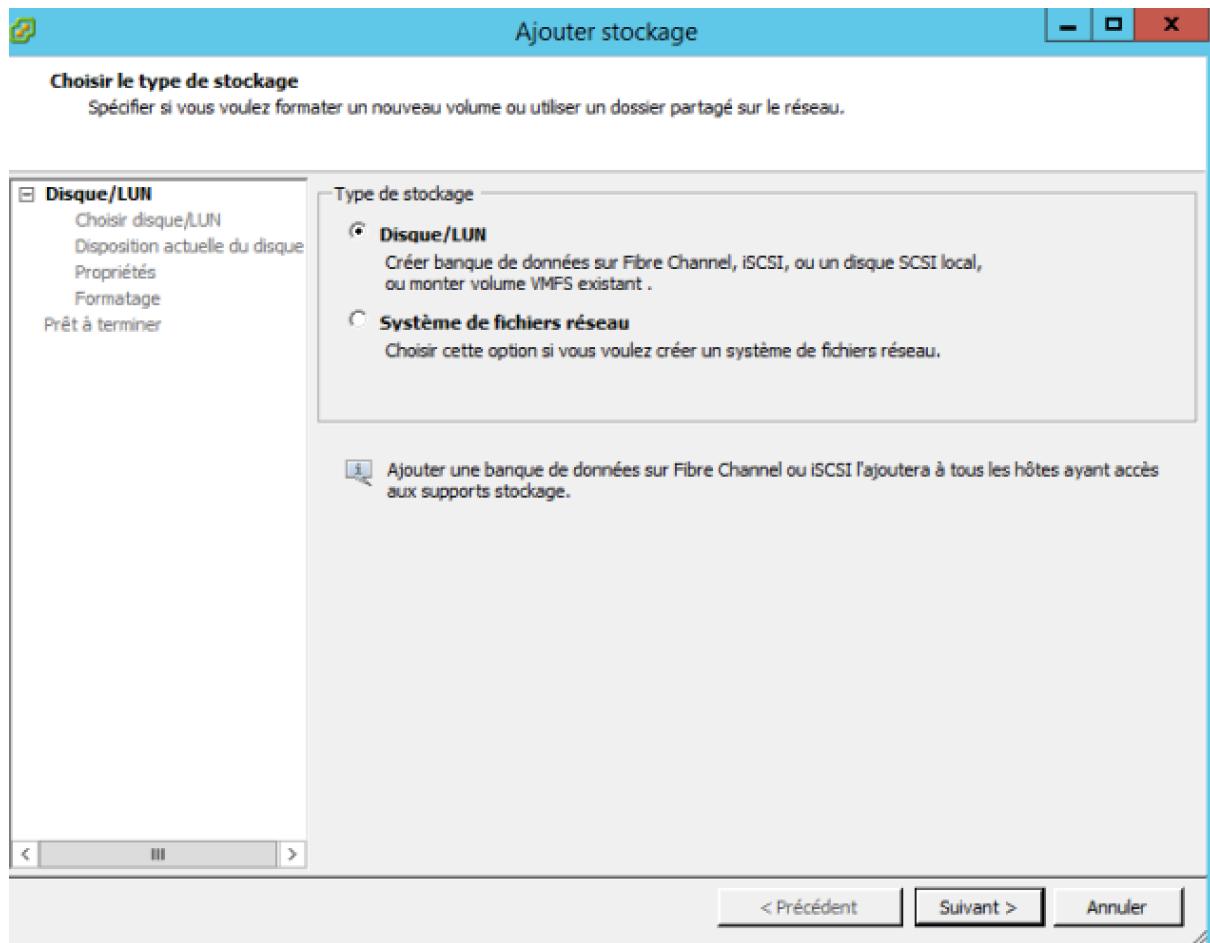
Afficher : [Banques de données](#) [Péphériques](#)

Banques de données

Identification	Statut	Péphérique	Type de lecteur	Capacité	Libre	Type	Dernière mise à jour	Actions d'alarme	Storage I/O Control	Accélération matérielle
datastore1	Normale	Local VMware, Di...	SSD	72,50 Go	39,90 Go	VMFS5	28/05/2015 12:35:29	Activé	Désactivé	Non pris en charge

Actualiser Supprimer Ajouter stockage... Réanalyser tout...

Cliquons alors sur **Ajouter stockage...** en haut à droite de notre fenêtre. A l'ouverture de la nouvelle fenêtre, nous choisissons **Disque/LUN** en type de stockage :



On choisit ensuite notre disque et on clique sur **Suivant**.

Pour le reste de la configuration on laisse par défaut hormis le nom de ce nouveau stockage qu'on essaie de rendre parlant. On obtient alors notre nouvelle banque de données :

Afficher : Banques de données Périphériques							
Banques de données							
Identification	Statut	Périphérique	Type de lecteur	Capacité	Libre	Type	
datastore1 (1)	Normale	Local VMware, Di...	SSD	62,50 Go	7,53 Go	VMFS5	
DatastoreVM	Normale	MSFT iSCSI Disk ...	Non-SSD	74,75 Go	66,13 Go	VMFS5	

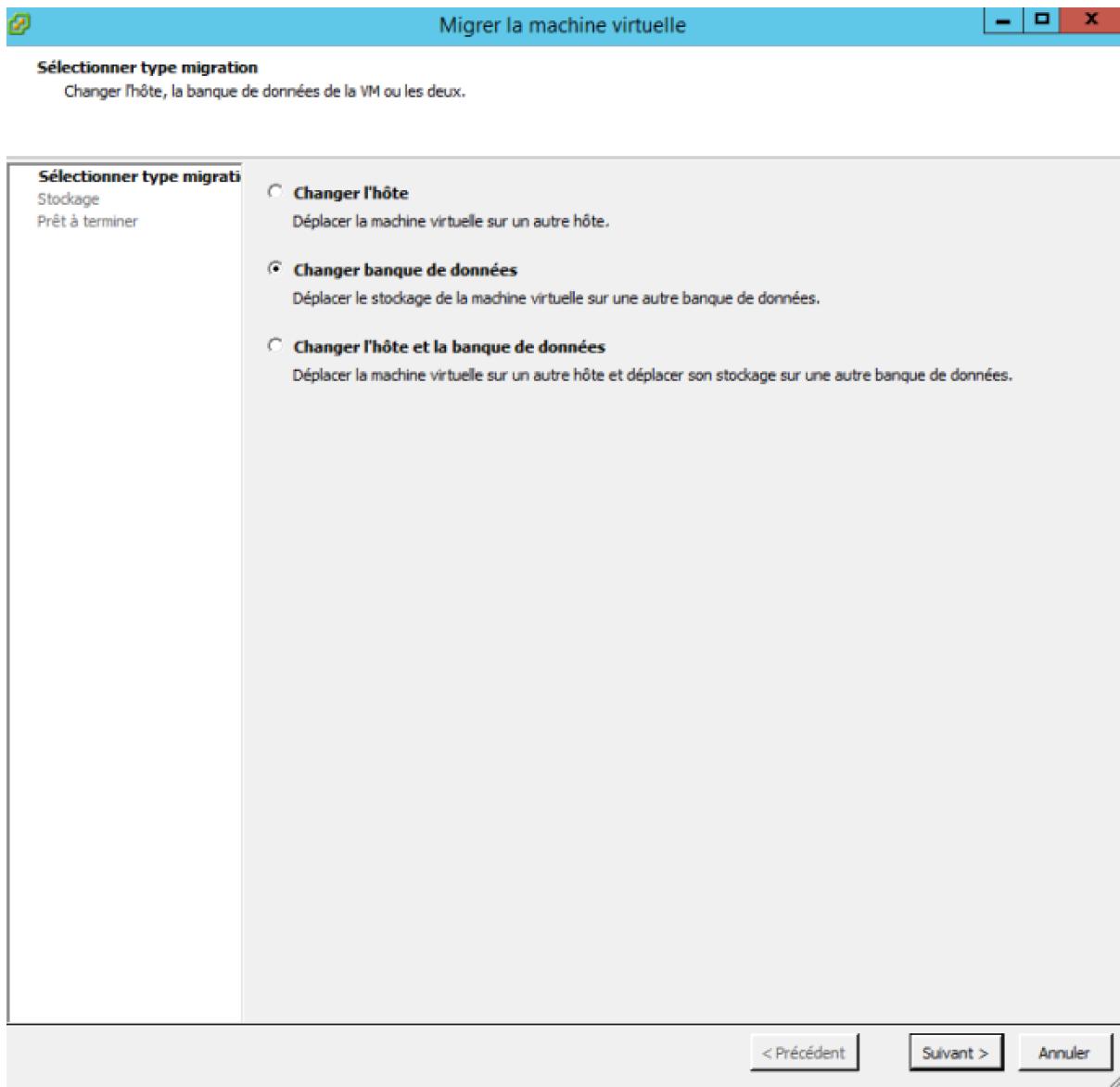
vi. Migration du stockage d'une machine virtuelle

Nous allons maintenant procéder à la migration du stockage des machines virtuelles.

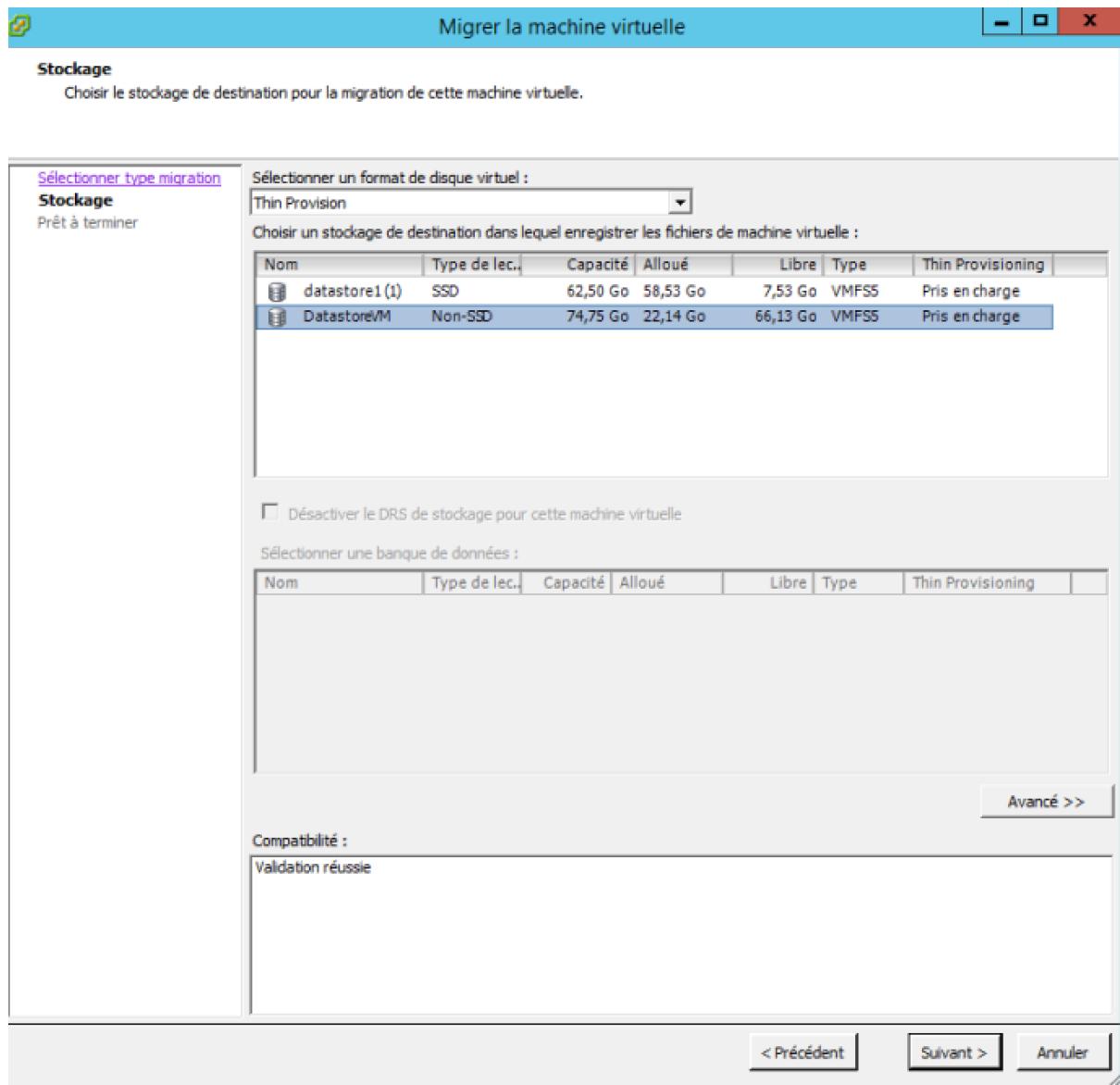
Pour cela, rendons-nous dans l'onglet **Résumé** et cliquons sur **Migrer** :

The screenshot shows the vSphere Web Client interface. On the left, a tree view lists hosts and clusters under 'NYVCE.mewpipe.com'. The 'ClusterNY-ESX' node has several virtual machines (VMs) listed: 172.16.4.11, 172.16.4.12, NYBDD1, NYBDD2 (which is selected), NYBE1, NYBE2, NYFE1, and NYFE2. The main pane displays the 'Résumé' tab for the selected VM, 'NYBDD2'. The 'Général' section provides basic information: SE client (Microsoft Windows Server 2012 (64 bits)), Version VM (11), CPU (1 vCPU), Mémoire (1024 Mo), and Charge mémoire. It also shows VMware Tools status (Inactif (Non installé)) and IP addresses. The 'Commandes' section contains several options: Activer, Modifier les paramètres, Migrer (which is highlighted with an orange box), Cloner vers la nouvelle machine virtuelle, and Convertir au modèle.

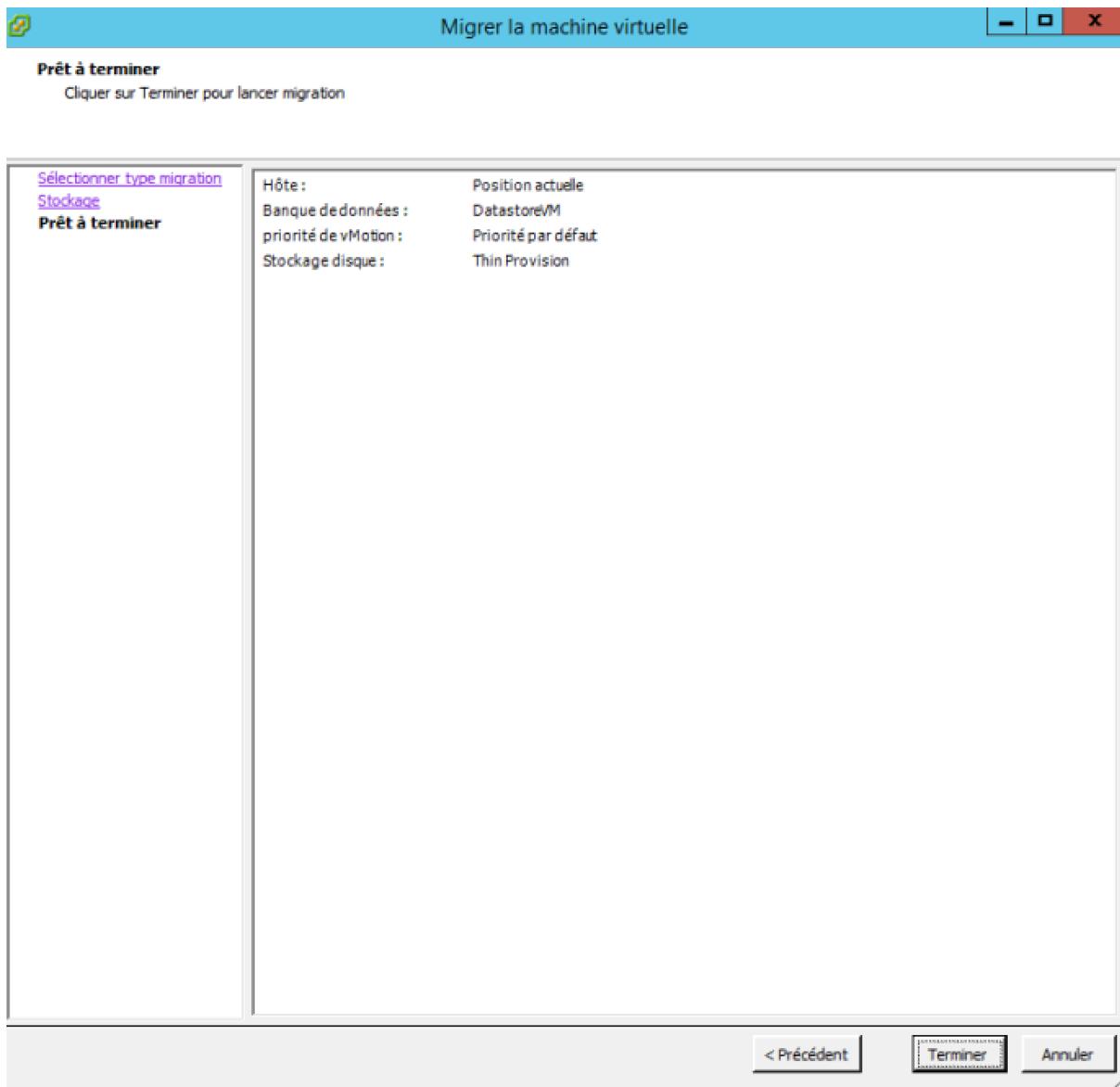
On nous demande alors qu'est-ce que nous souhaitons migrer, dans notre cas, nous souhaitons migrer uniquement la banque de données :



Nous choisissons alors notre nouvelle banque de données précédemment créée, puis nous choisissons un **Provisionnement fin** afin d'économiser notre stockage :



Nous pouvons alors cliquer sur **Terminer** :



vCenter va alors procéder à la migration :

Tâches récentes					
Nom	Cible	Statut	Détails	Lancé par	vCenter Server
Replacer la machine virtuelle	NYBDD2	99%		VSPHERE.LO...	NYVCE.mewpi...

Tâches récentes					
Nom	Cible	Statut	Détails	Lancé par	vCenter Server
Replacer la machine virtuelle	NYBDD2	Terminé		VSPHERE.LO...	NYVCE.mewpi...

Notre machine virtuelle est désormais stockée sur un volume iSCSI et tout les flux passent par notre réseau de stockage.

O. Repository Linux

a) Introduction

Afin d'assurer une tolérance de panne, une solution de sauvegardes des machines virtuelles va être implémenter. En effet, les machines virtuelles doivent être sauvegardées tous les jours à 2h du matin sur un repository Linux au niveau du Datacenter passif, Dallas. Pour se faire, la solution Veeam a été choisi par notre équipe pour assurer le backup des VMs.

b) Création du repository Linux

Nous avons choisi une distribution Debian, dans sa version 8, pour assurer le repository.

Nous mettons une adresse IP statique à notre serveur à l'aide de la commande suivante :

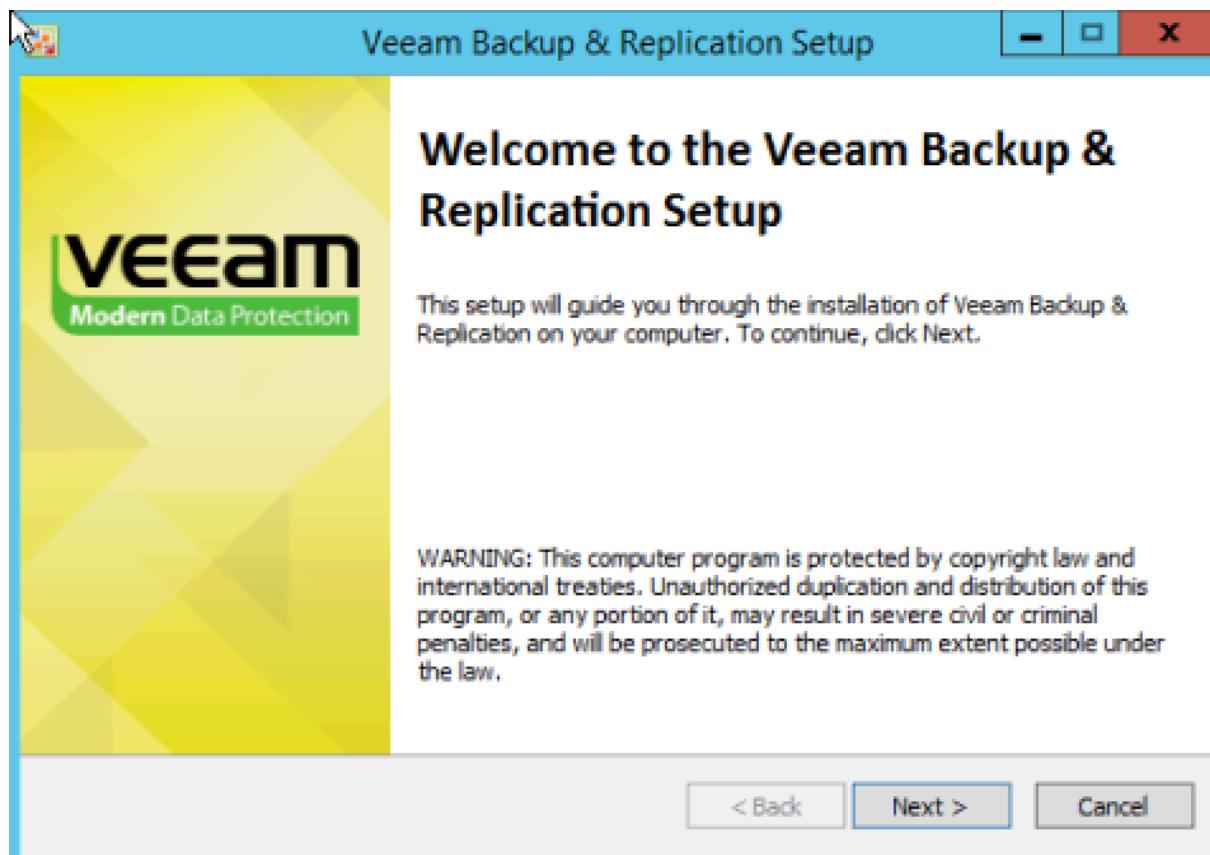
```
nano /etc/network/interfaces
```

```
# The loopback network interface
auto lo
iface lo inet loopback

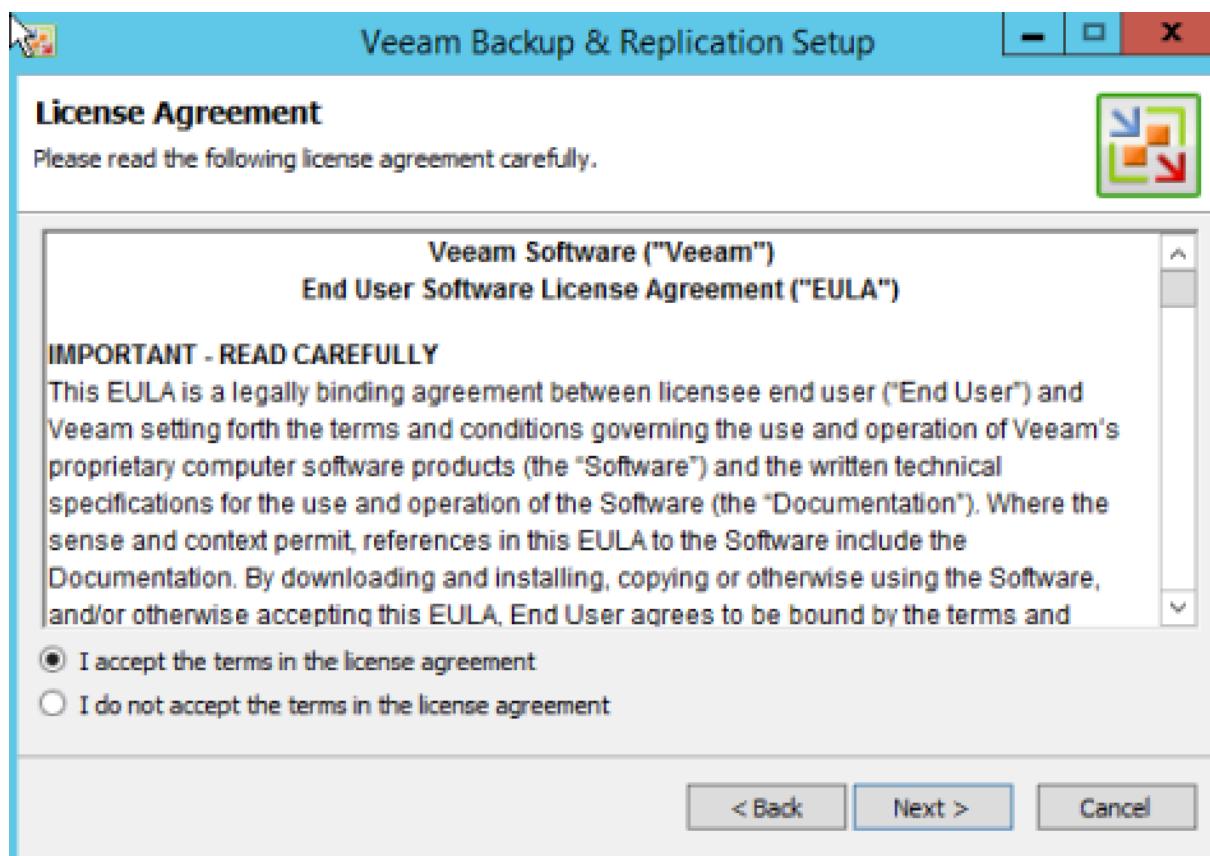
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 172.16.4.50
    netmask 255.255.248.0
    gateway 172.16.7.254
    dns-nameservers 172.16.4.1
```

c) Installation de Veeam

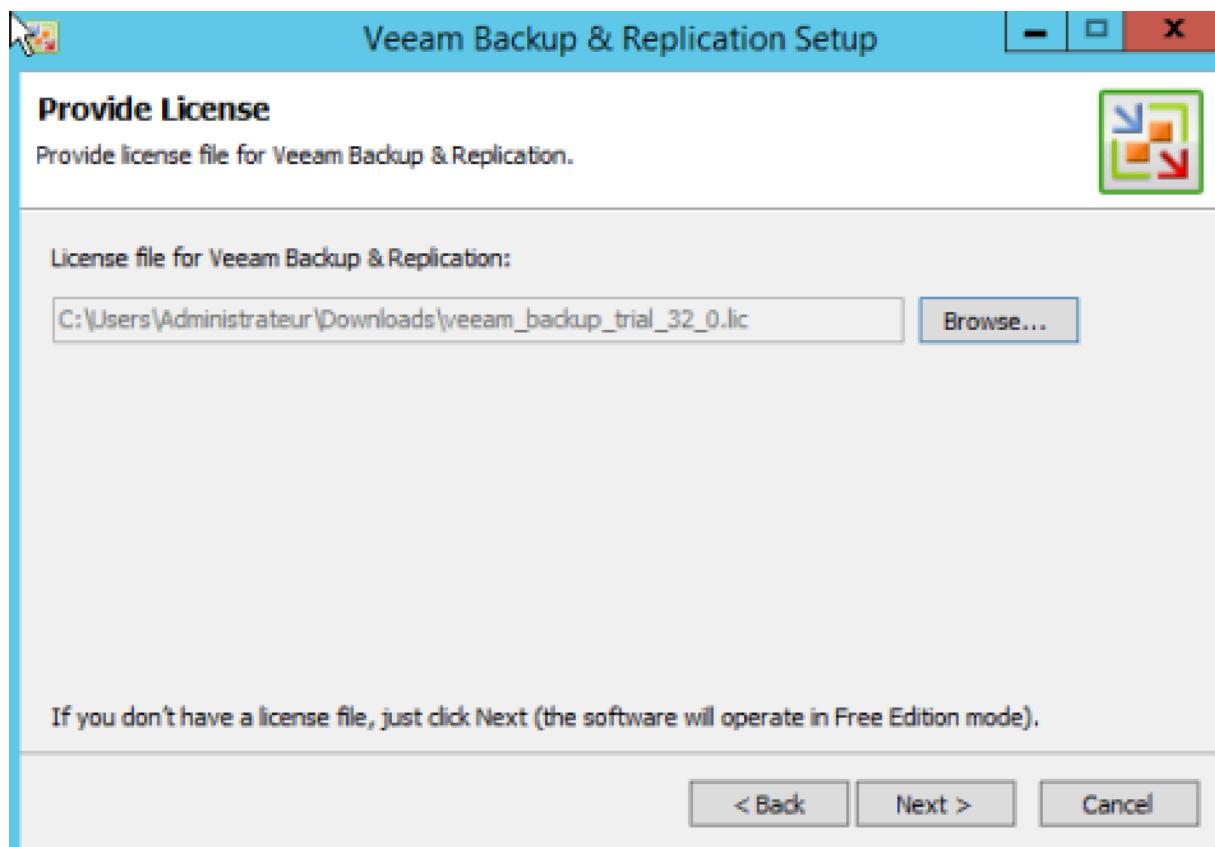
Nous allons procéder à l'installation du Veeam. Dans notre maquette, pour une question d'économie de ressources, nous avons décider de mutualiser les serveurs et d'installer Veeam sur le contrôleur de domaine. Nous commençons alors par lancer l'ISO de Veeam, un message de bienvenue, nous pouvons alors cliquer sur **Next** :



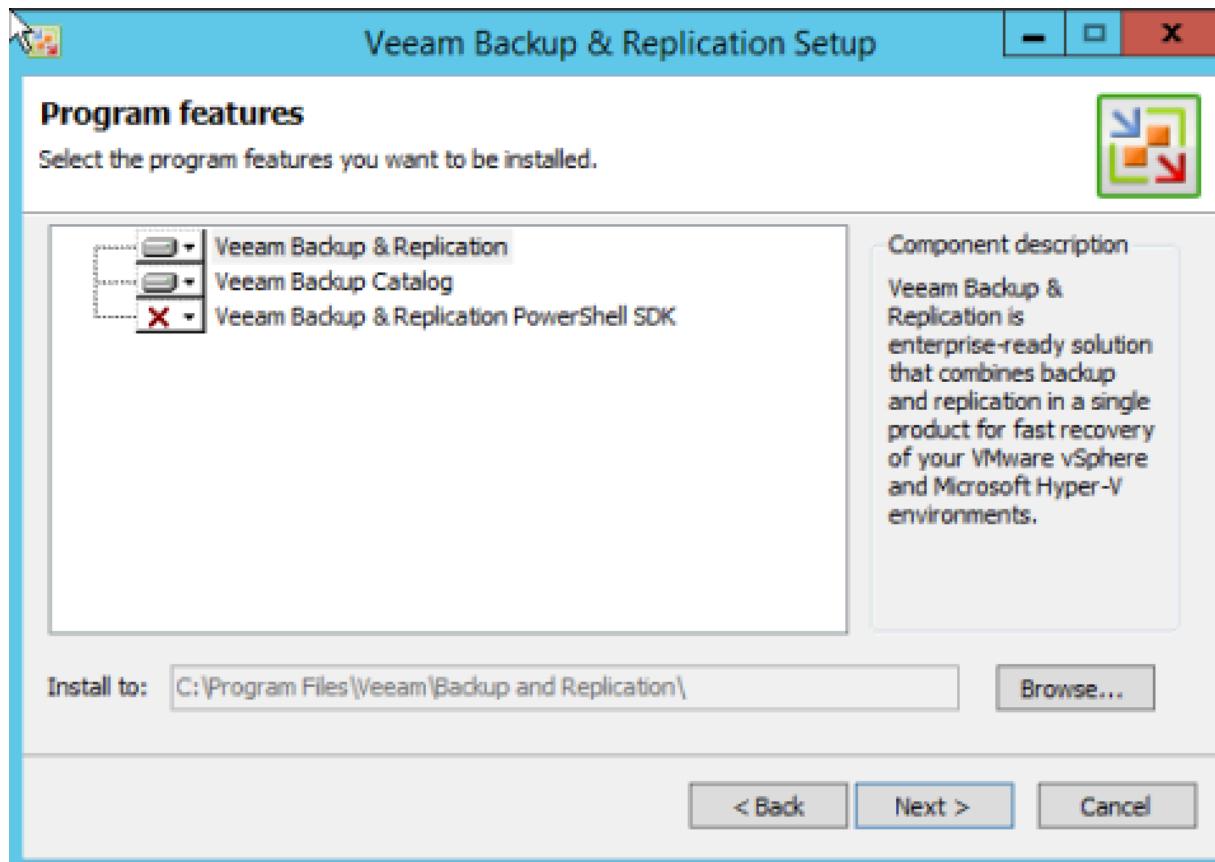
On choisit ensuite d'accepter les conditions d'utilisation, puis on clique sur **Next** :



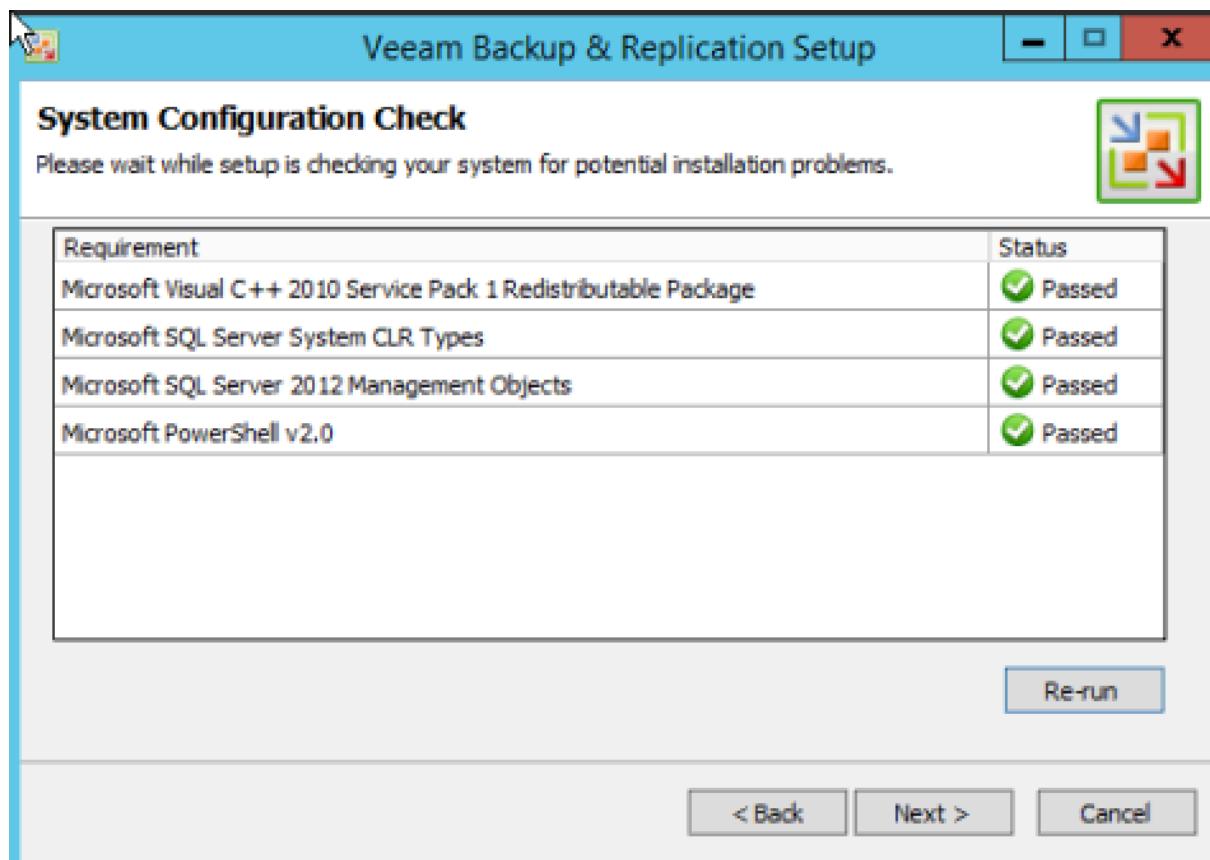
On clique sur **Browse** et on va chercher notre licence, nous pouvons alors cliquer de nouveau sur **Next** :



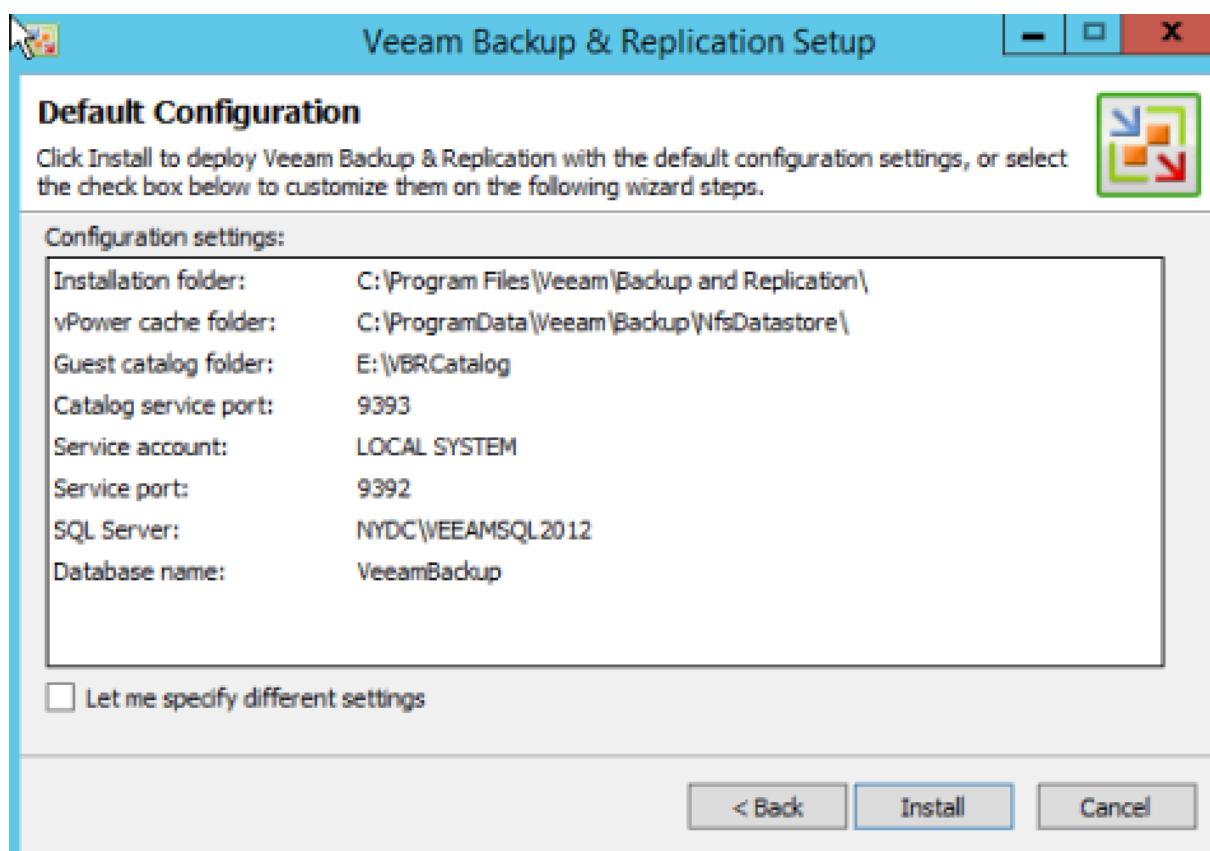
Sélection des fonctionnalités à installer, on laisse par défaut, et on clique sur **Next** :



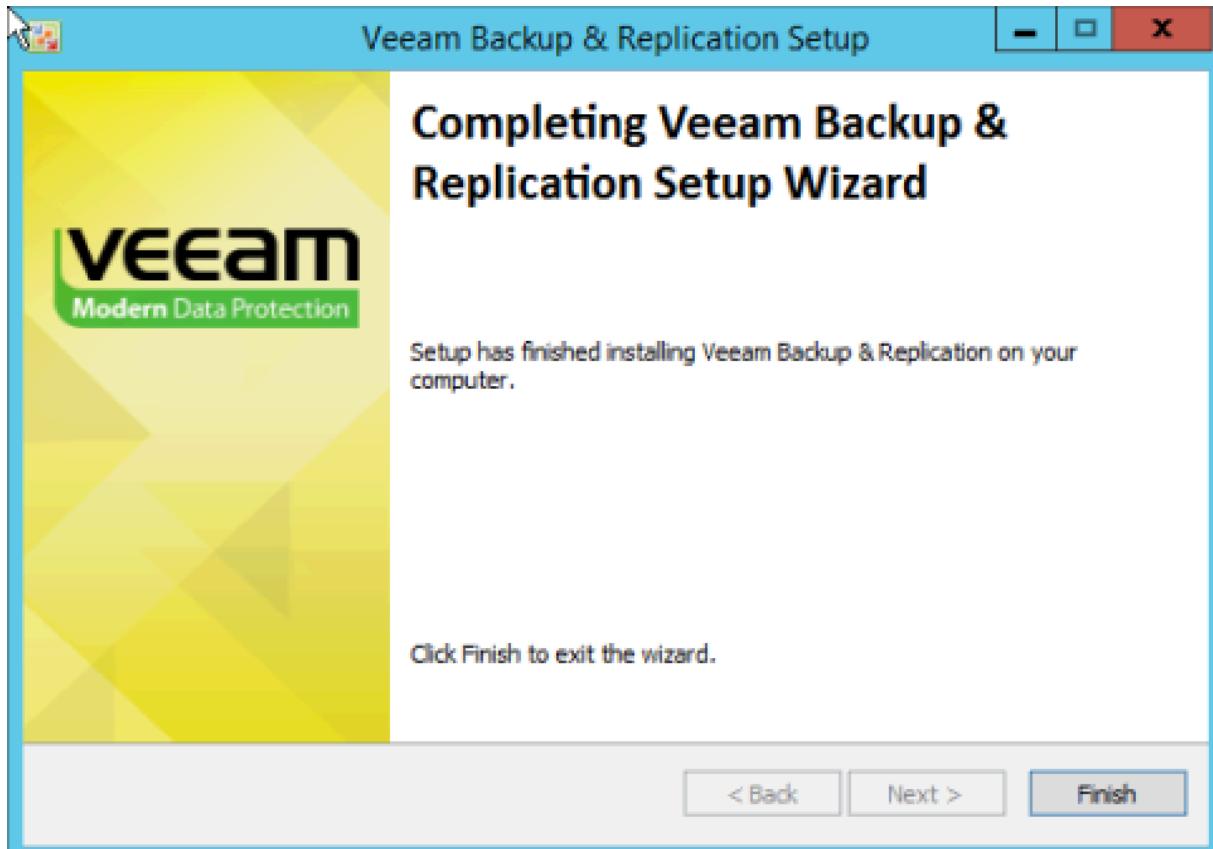
Vérification des prérequis, si tout est OK, cliquez sur **Next**, autrement cliquer sur **Install** puis **Re-run** et enfin sur **Next** :



Un résumé de l'installation à venir apparaît, on clique alors sur **Install** :



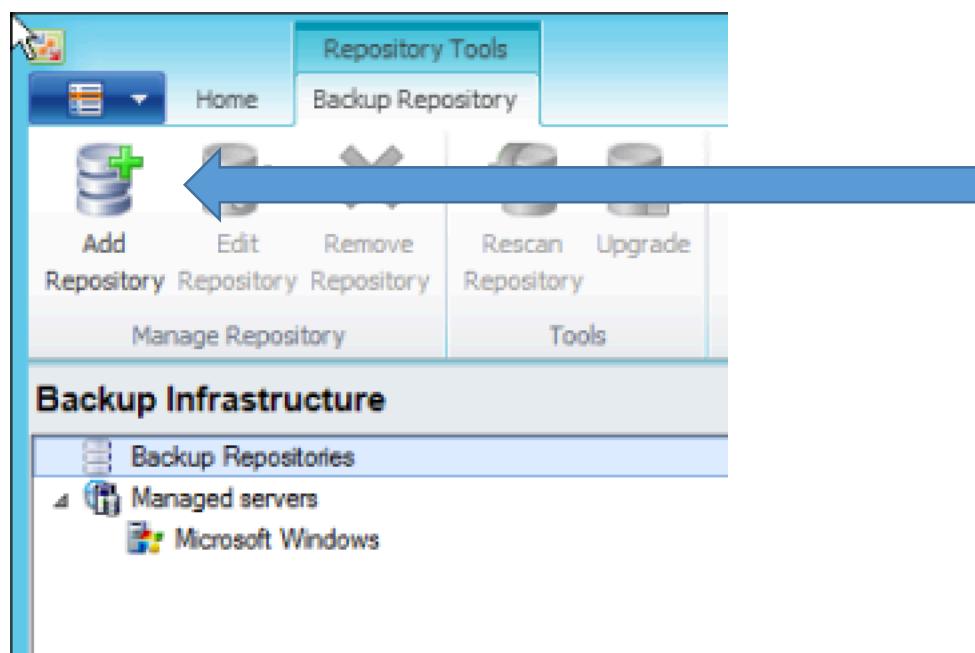
Une fois l'installation terminée, cliquer sur **Finish** :



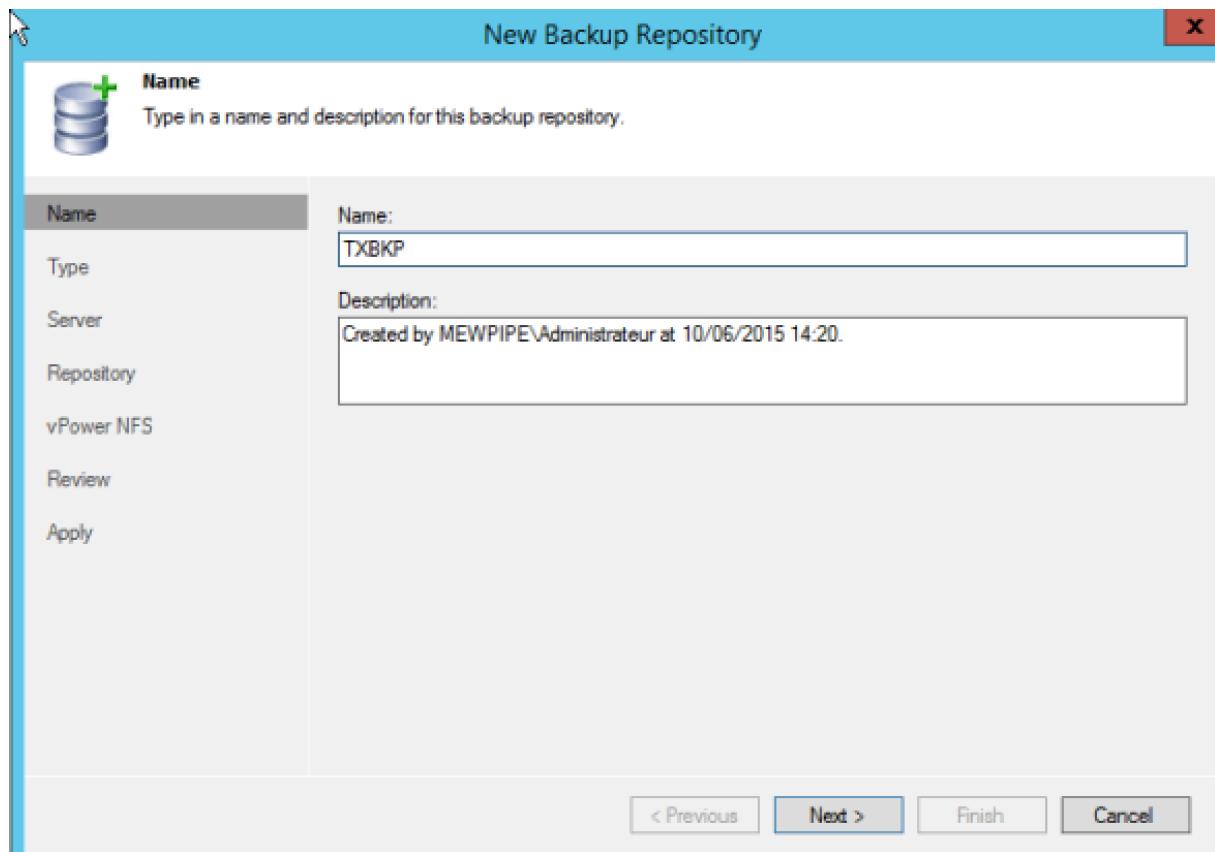
d) Ajout du repository

Nous pouvons maintenant lancer l'applicatif Veeam.

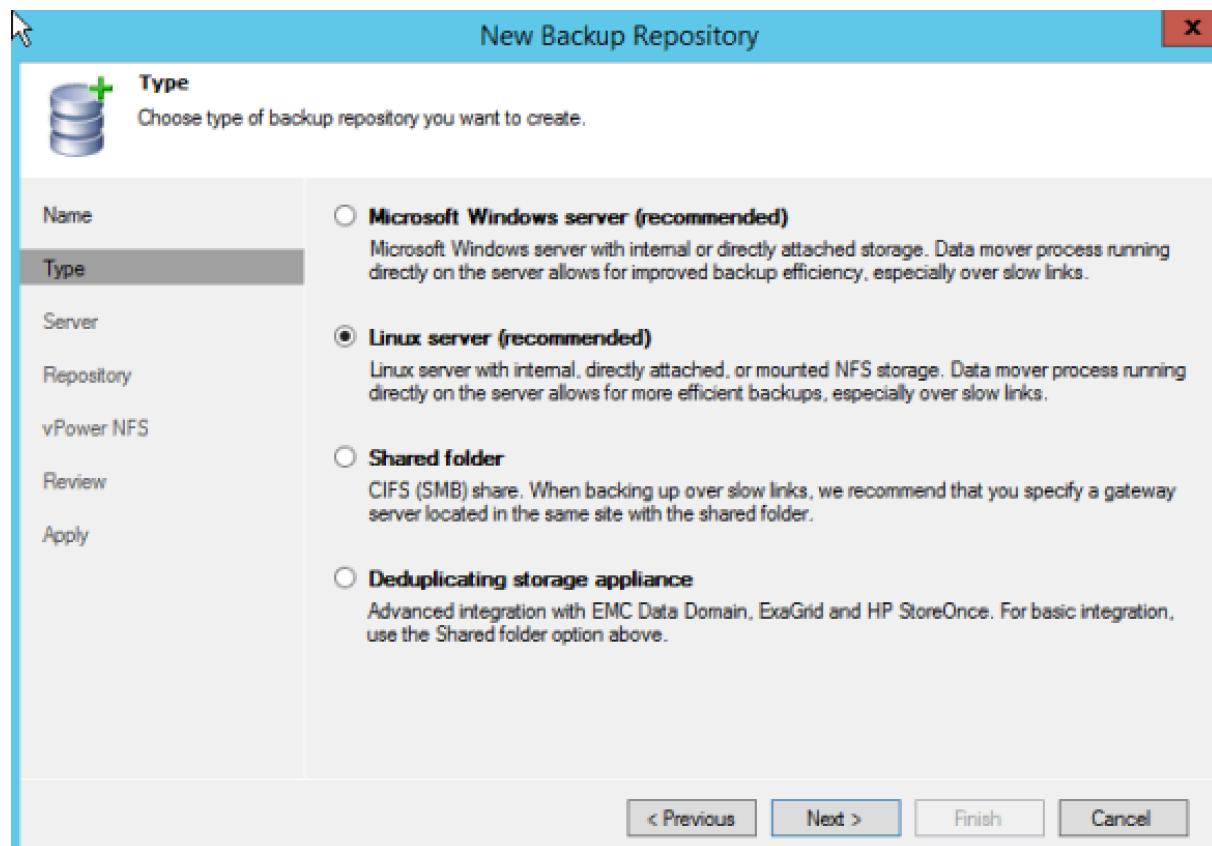
Nous allons commencer par ajouter notre repository, pour cela on va cliquer sur **Add repository** dans la partie gauche de l'interface :



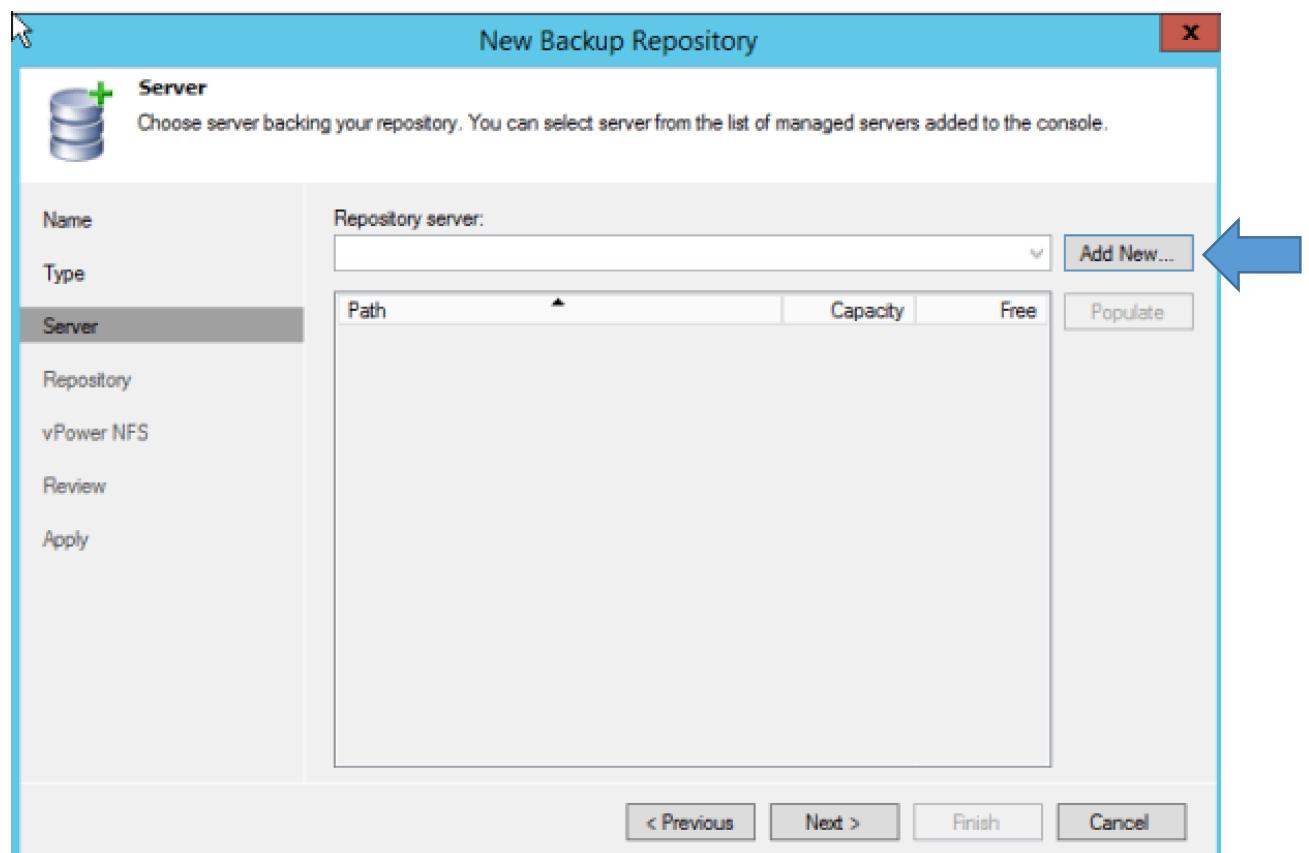
On donne un nom et une description à notre nouveau repository :



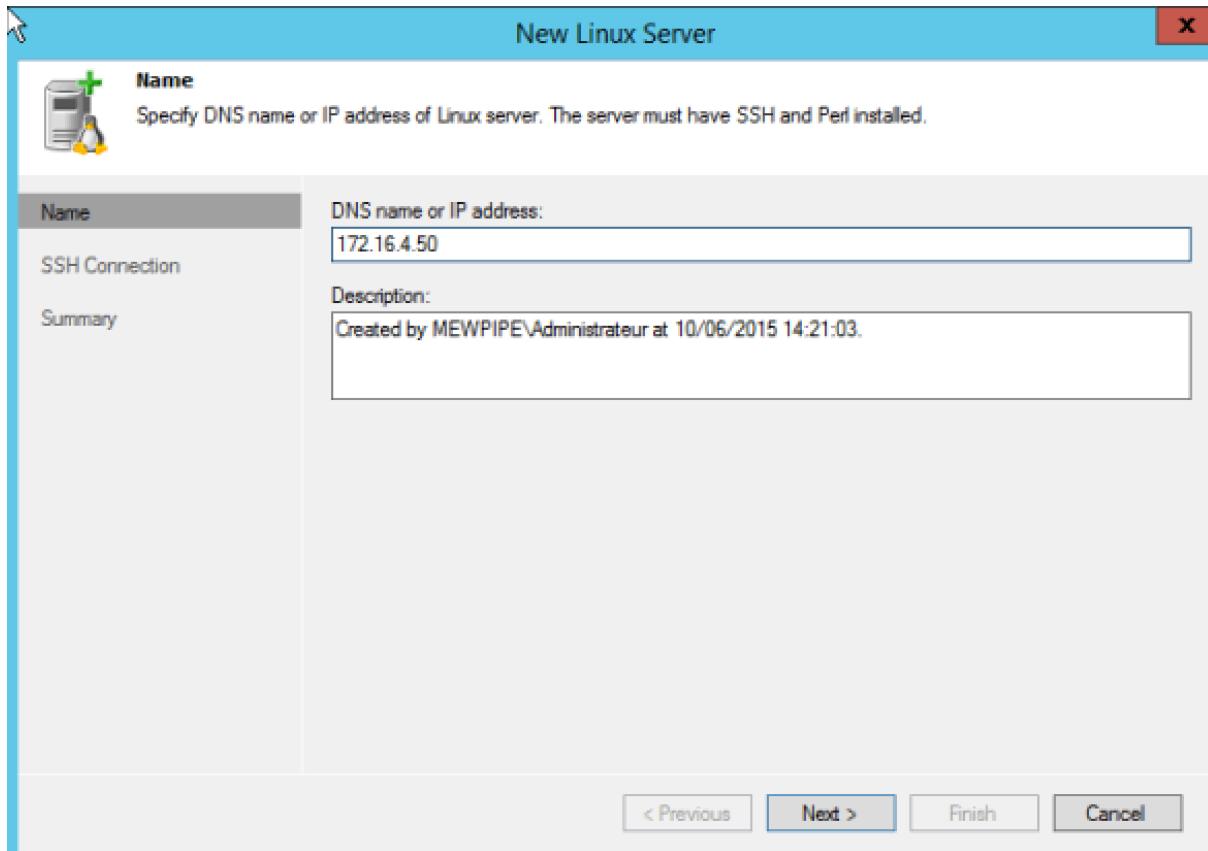
On définit ensuite le type de repository (Linux dans notre cas) :



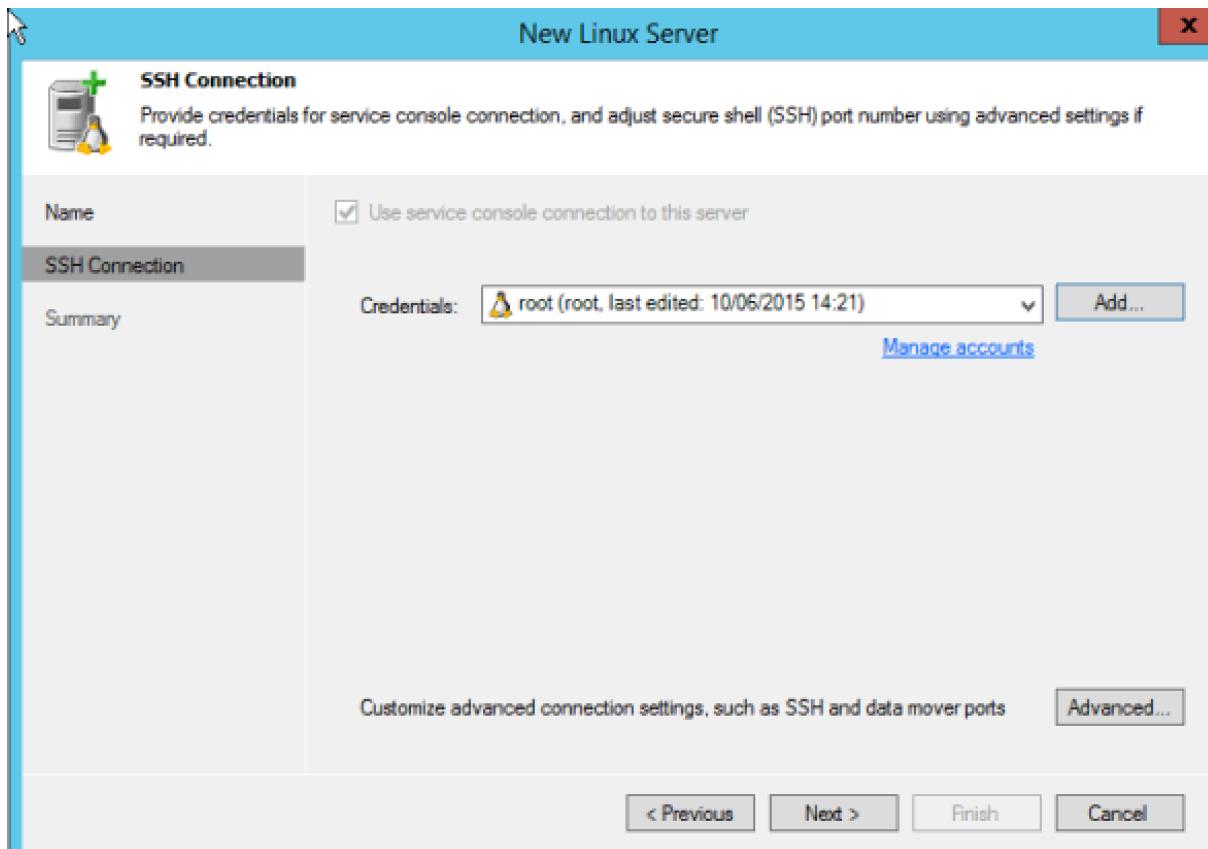
On clique sur Add new... :



On recherche ensuite notre serveur via son adresse IP :



On renseigne les credentials :



Pour autoriser la connexion de Veeam en SSH via le port 22 sur le serveur repository, il faut ajouter les informations de chiffrement dans le fichier de configuration ssh du serveur repository.

Pour cela, on ouvre le fichier avec la commande :

```
nano /etc/ssh/sshd_config
```

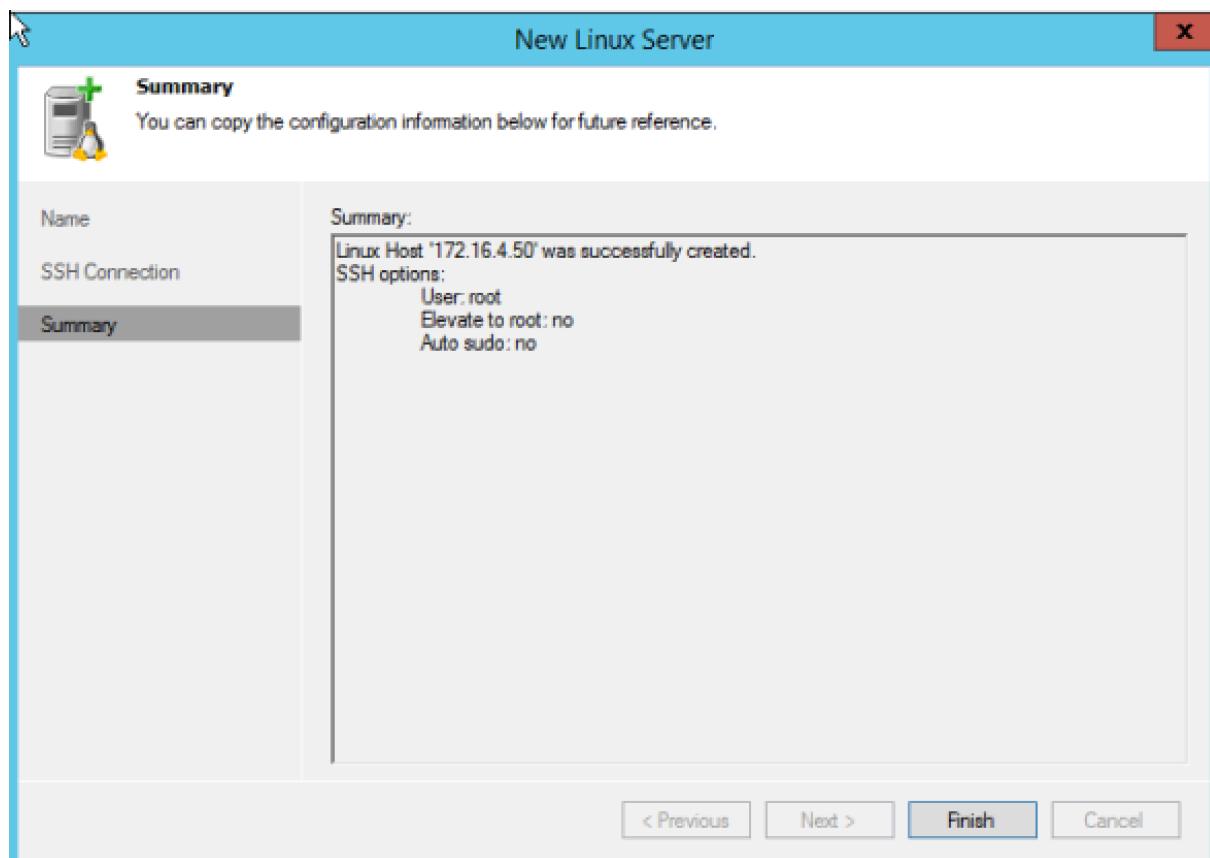
Et il faut ajouter ces deux lignes à la fin du fichier :

```
Ciphers aes128-cbc,blowfish-cbc,3des-cbc,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-poly1305@openssh.com
KexAlgorithms diffie-hellman-group1-sha1,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1
```

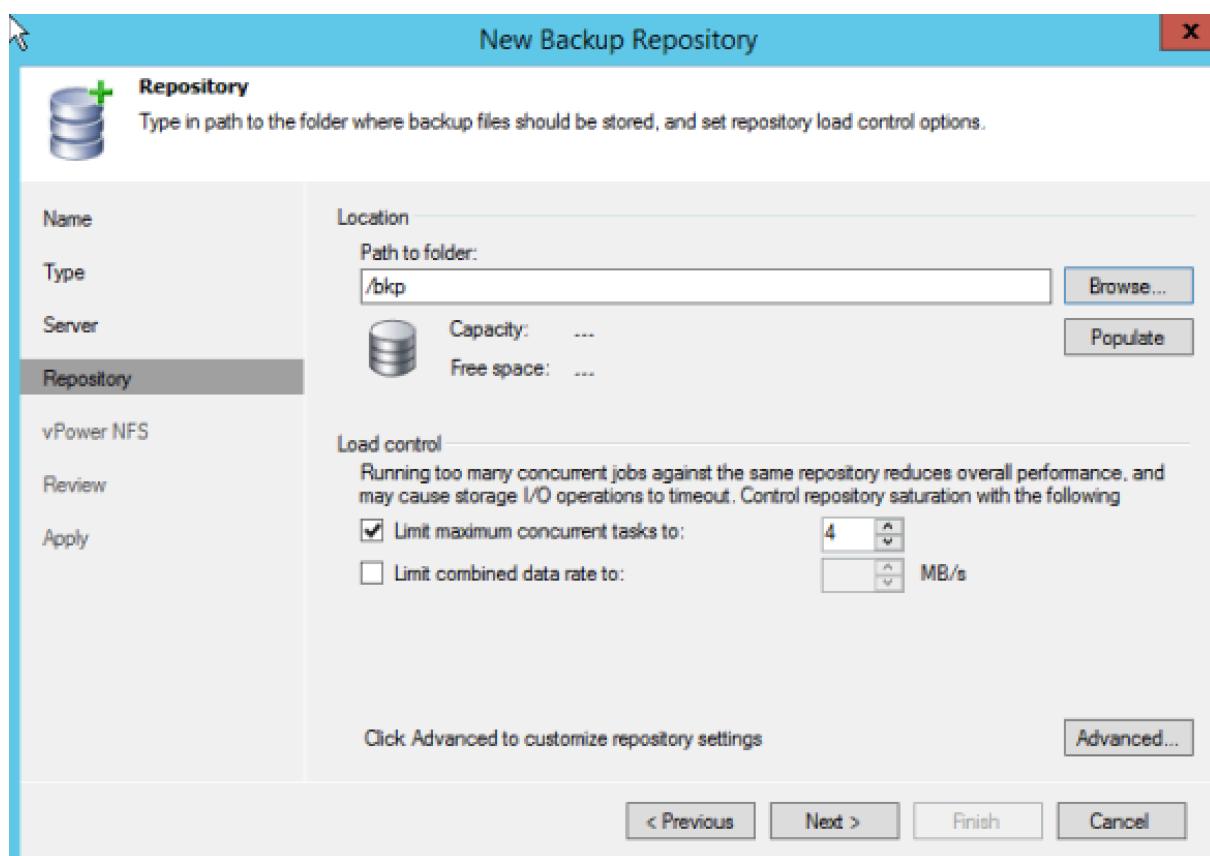
Ensuite, on redémarre le service SSH :

```
Service ssh restart
```

Notre connexion est alors établie :



On choisit alors le dossier de sauvegarde :

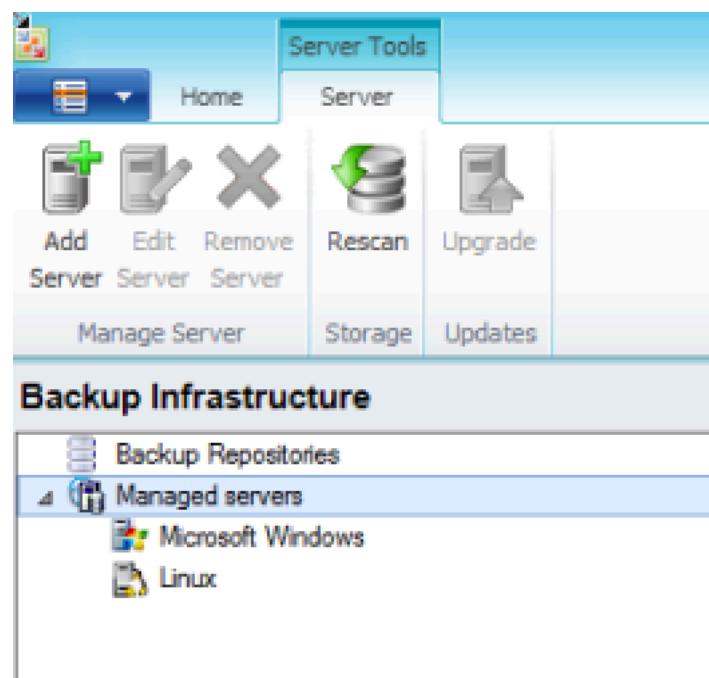


On laisse ensuite les paramètres par défaut, et on clique sur **Finish**, notre repository est alors créé :

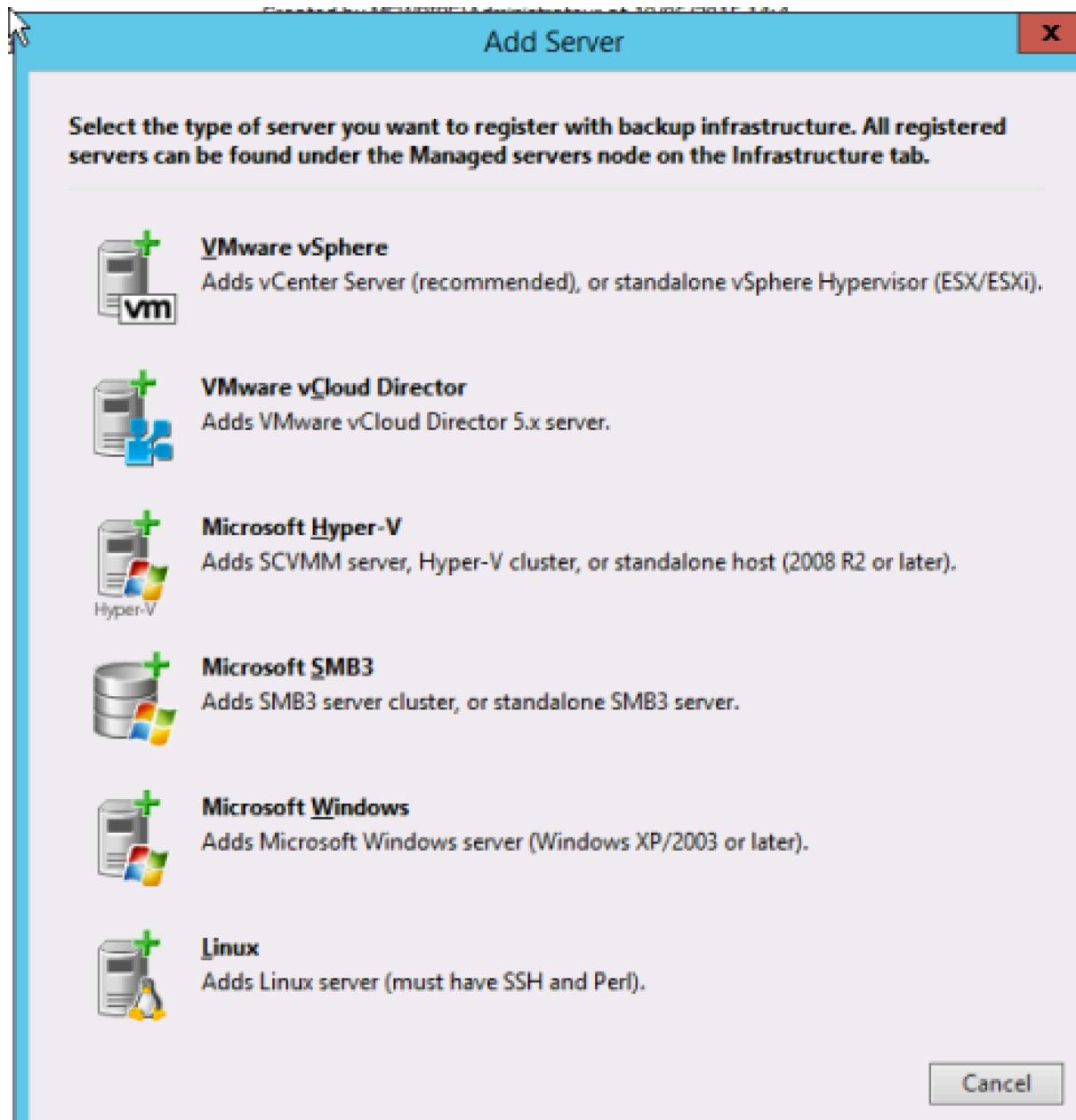
Type in an object name to search for			
Name	Type	Host	Path
Default Backup Repository	Windows	This server	E:\Backup
TXBKP	Linux	172.16.4.50	/bkp

e) Ajout du vCenter

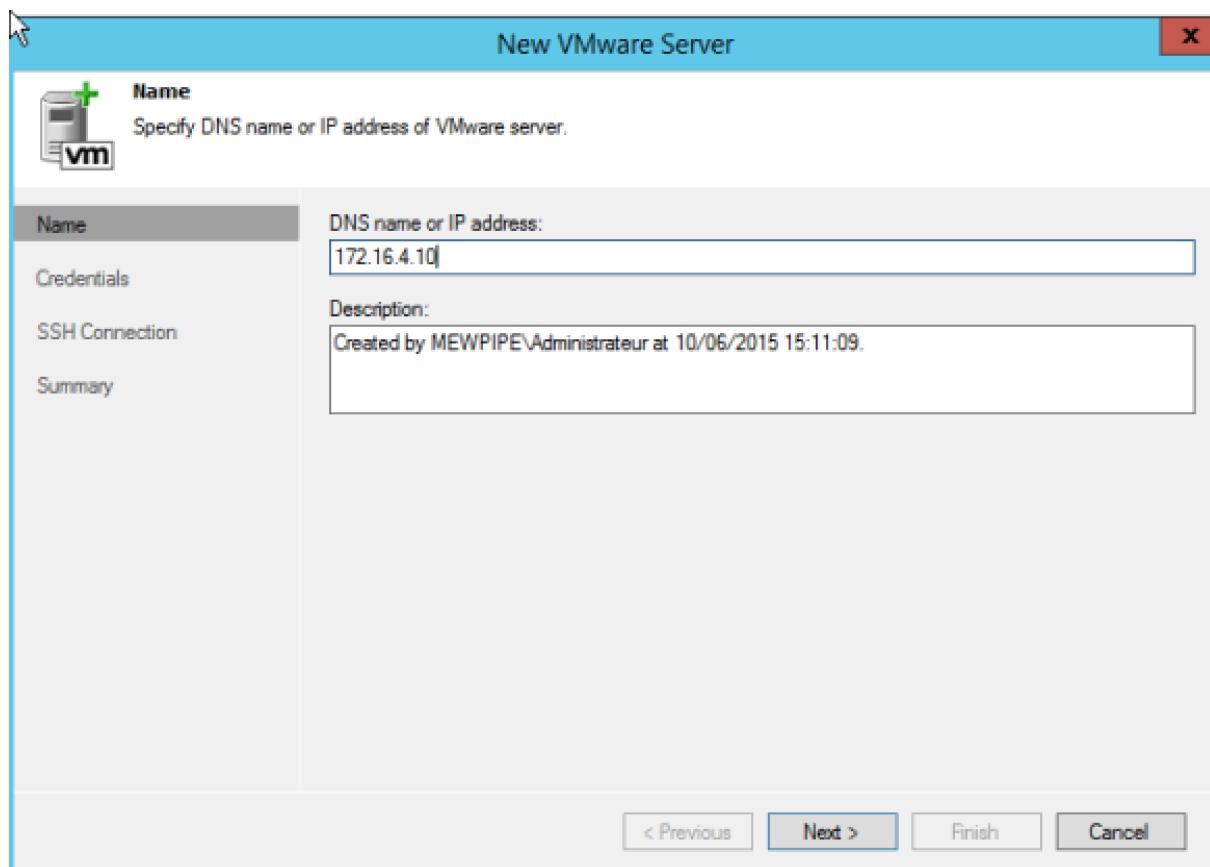
Pour cela, on va cliquer sur **Managed servers** dans l'inventaire à gauche de l'interface. Puis sur **Add server** :



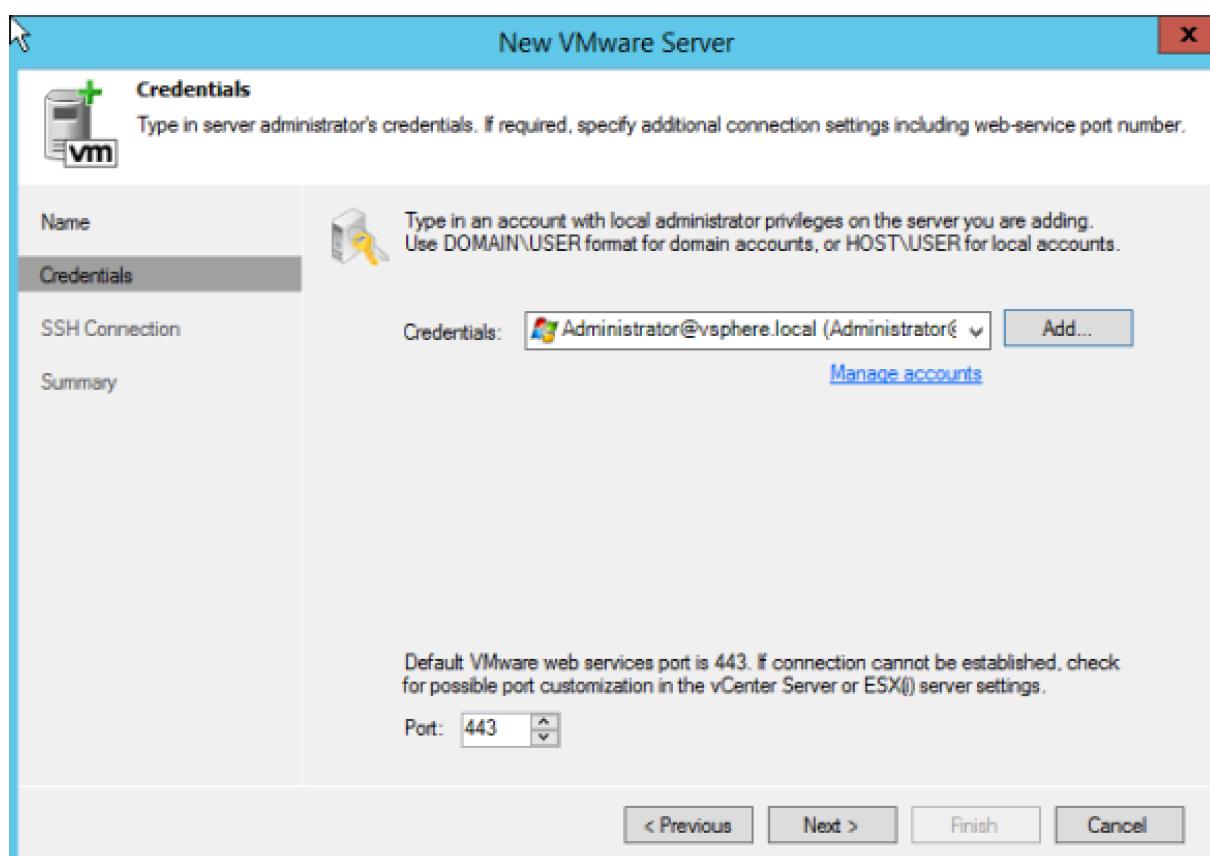
Une nouvelle fenêtre s'ouvre alors, on choisit le type (VMware vSphere dans notre cas) :



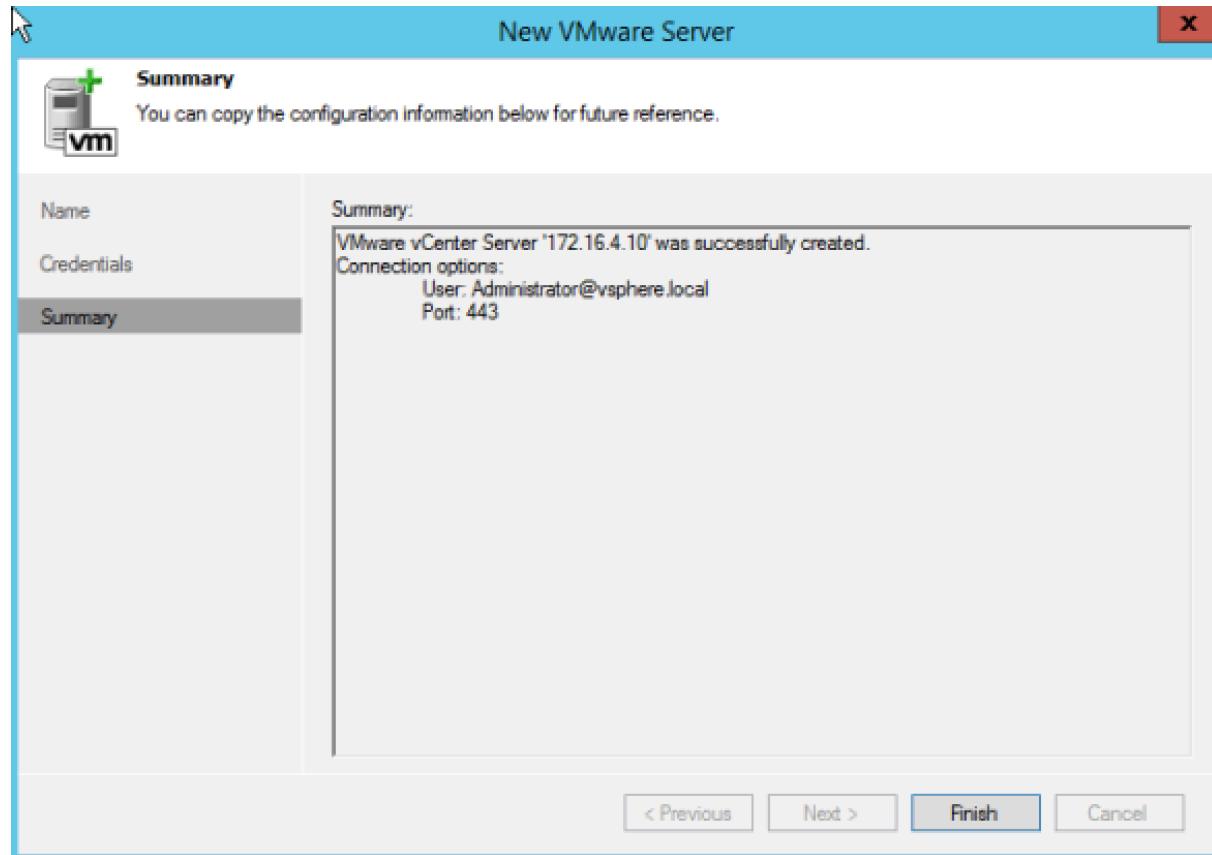
On renseigne alors l'adresse IP de notre vCenter :



On renseigne les credentials :



On clique enfin sur **Finish** :

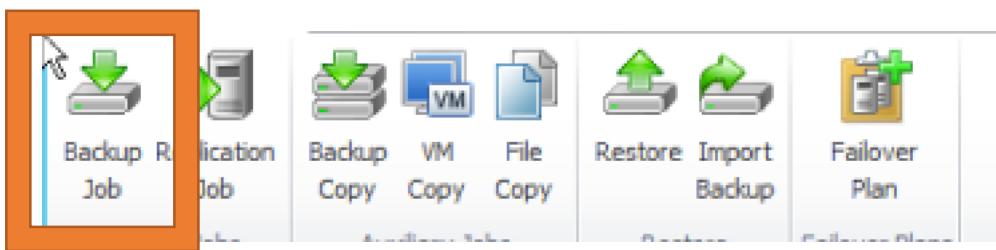


On peut alors constater que nos ESXi sont bien remontés :

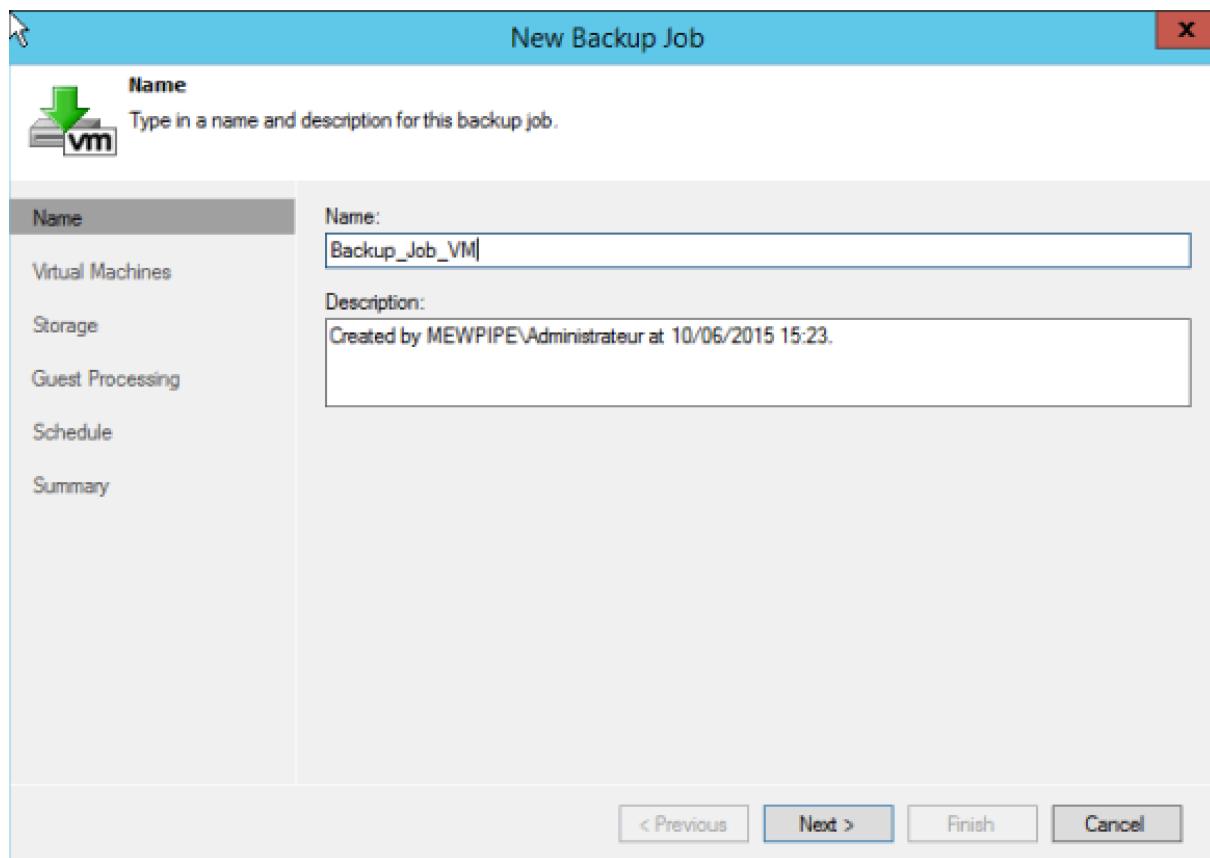
Name	Type
172.16.4.11	VMware ESXi Server
172.16.4.12	VMware ESXi Server

f) Création d'un job de sauvegarde

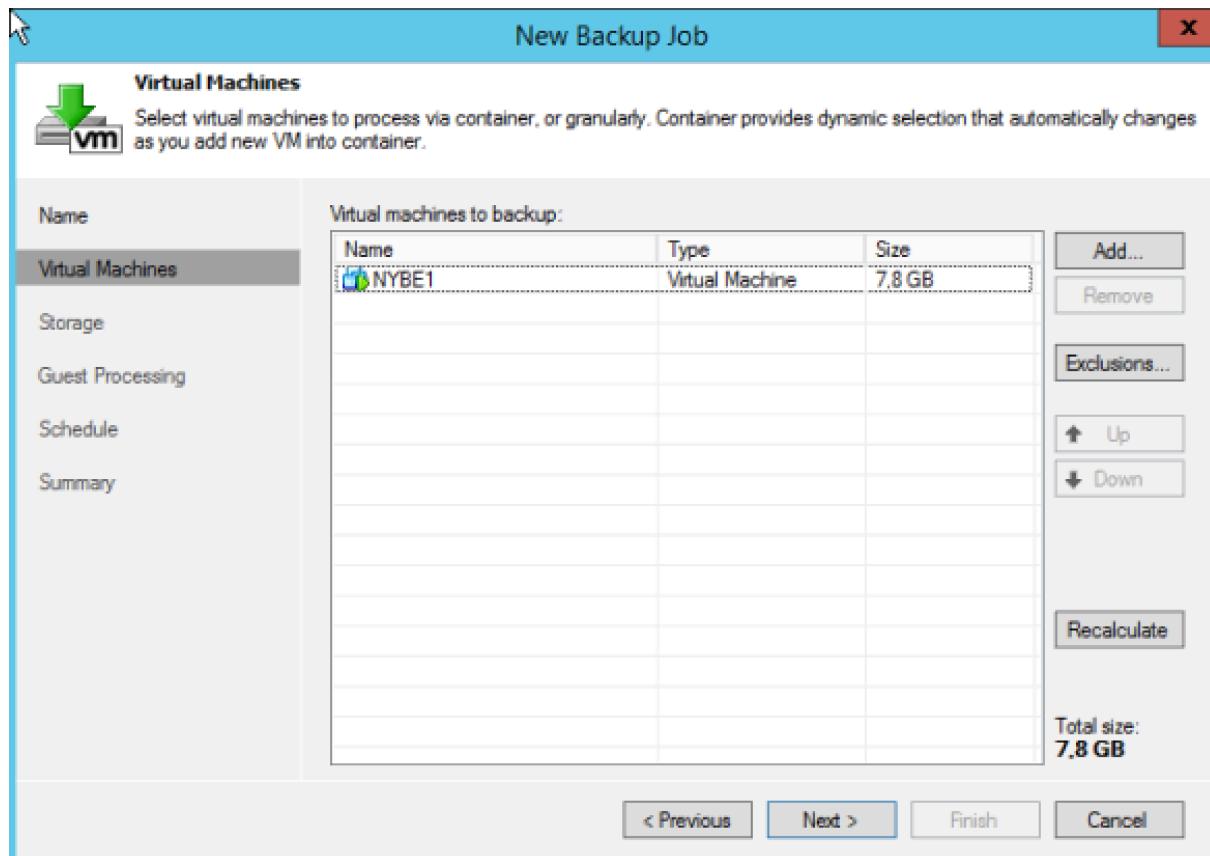
On va commencer par cliquer sur **Home** puis sur **Backup job** :



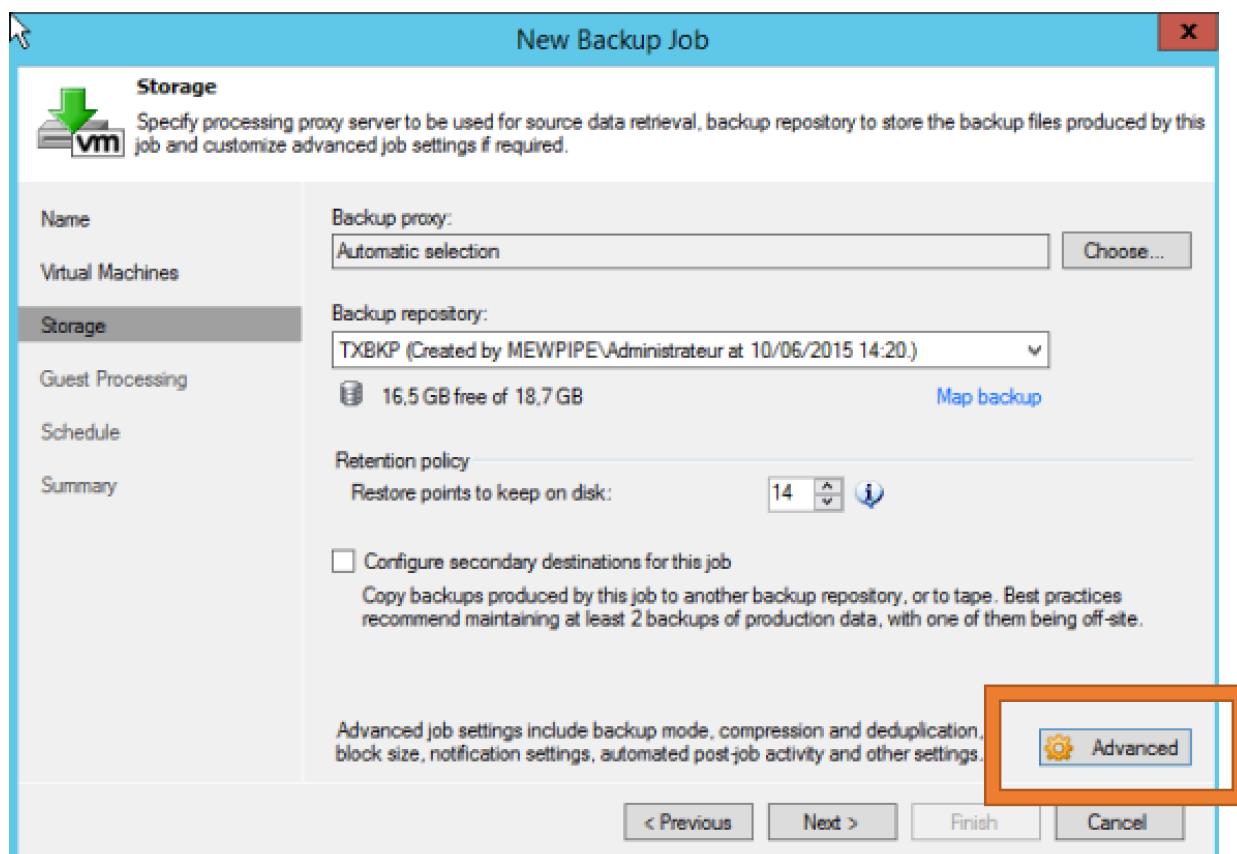
On donne un nom et une description à notre job :



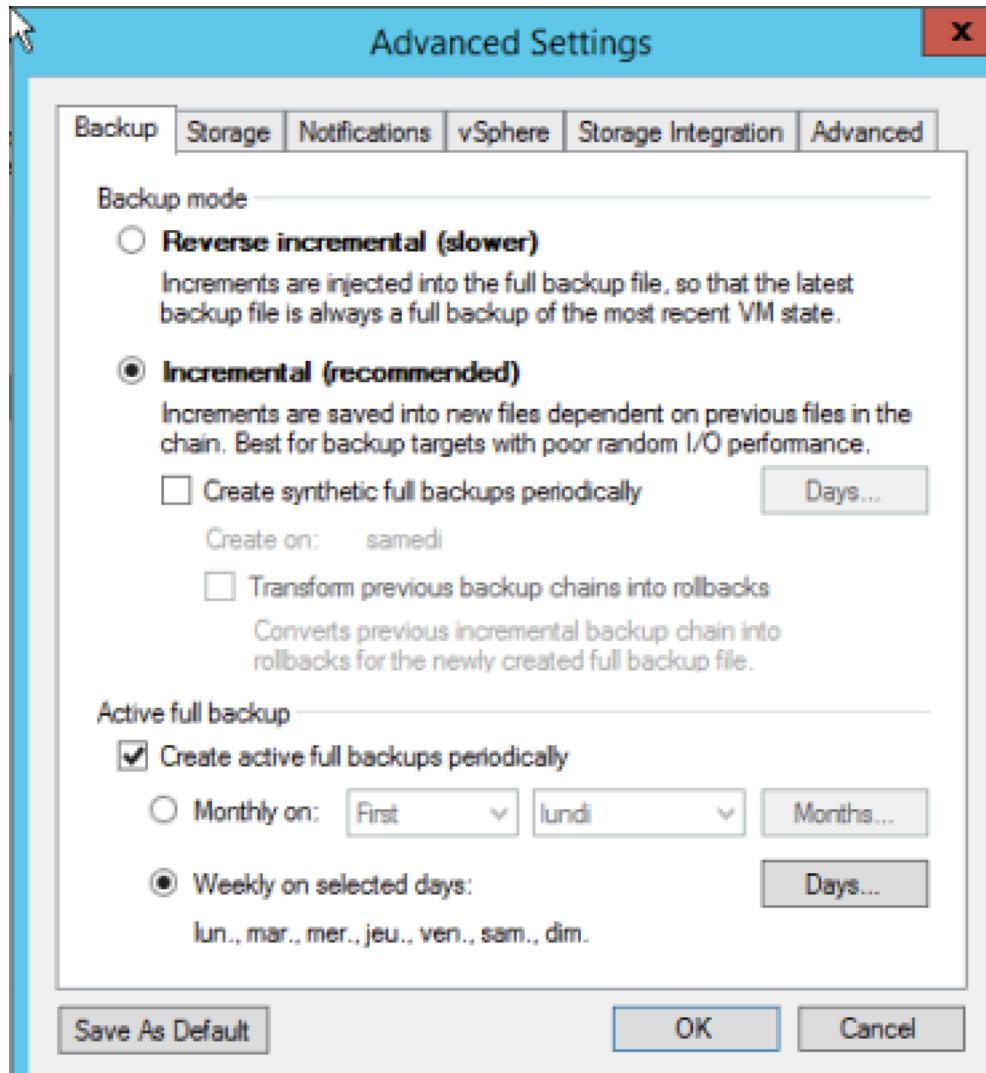
On ajoute les machines virtuelles que l'on souhaite sauvegarder :



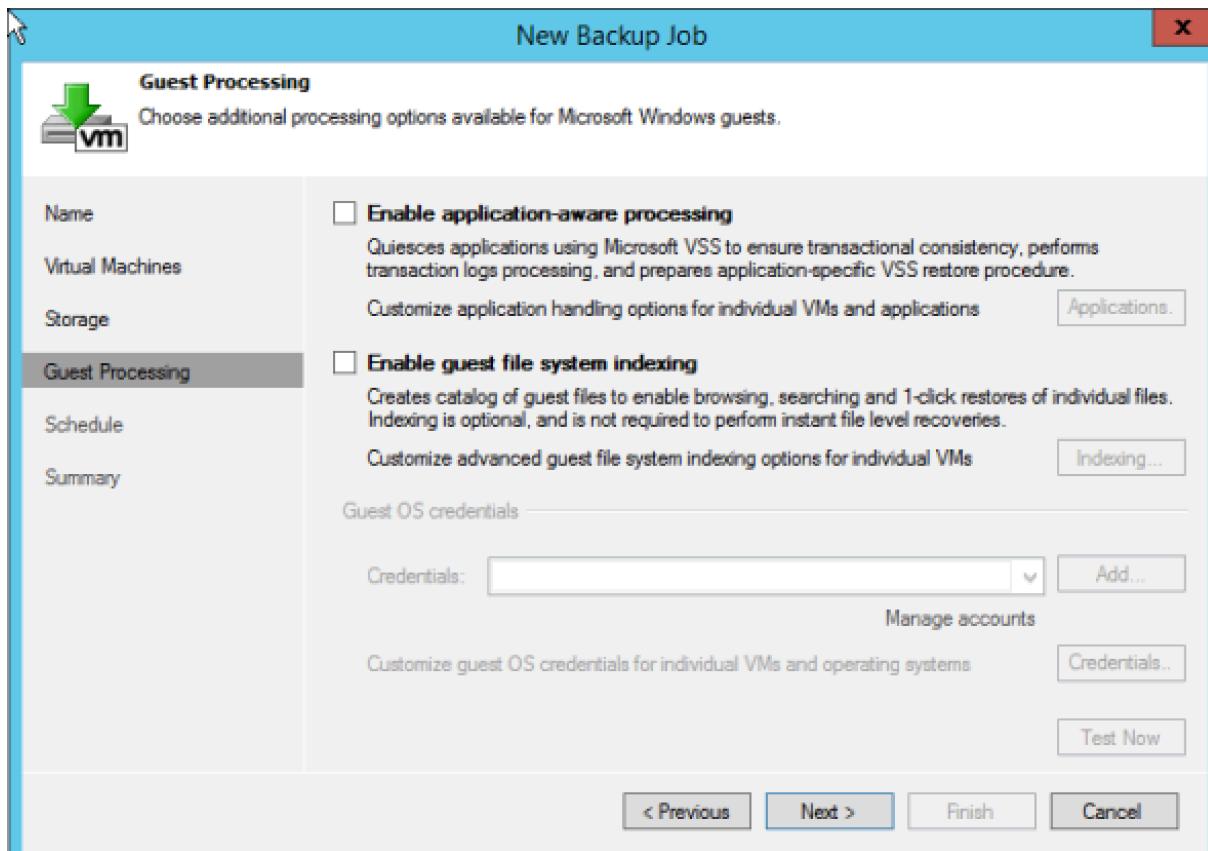
On choisit ensuite notre repository précédemment créé puis on clique sur **Advanced** :



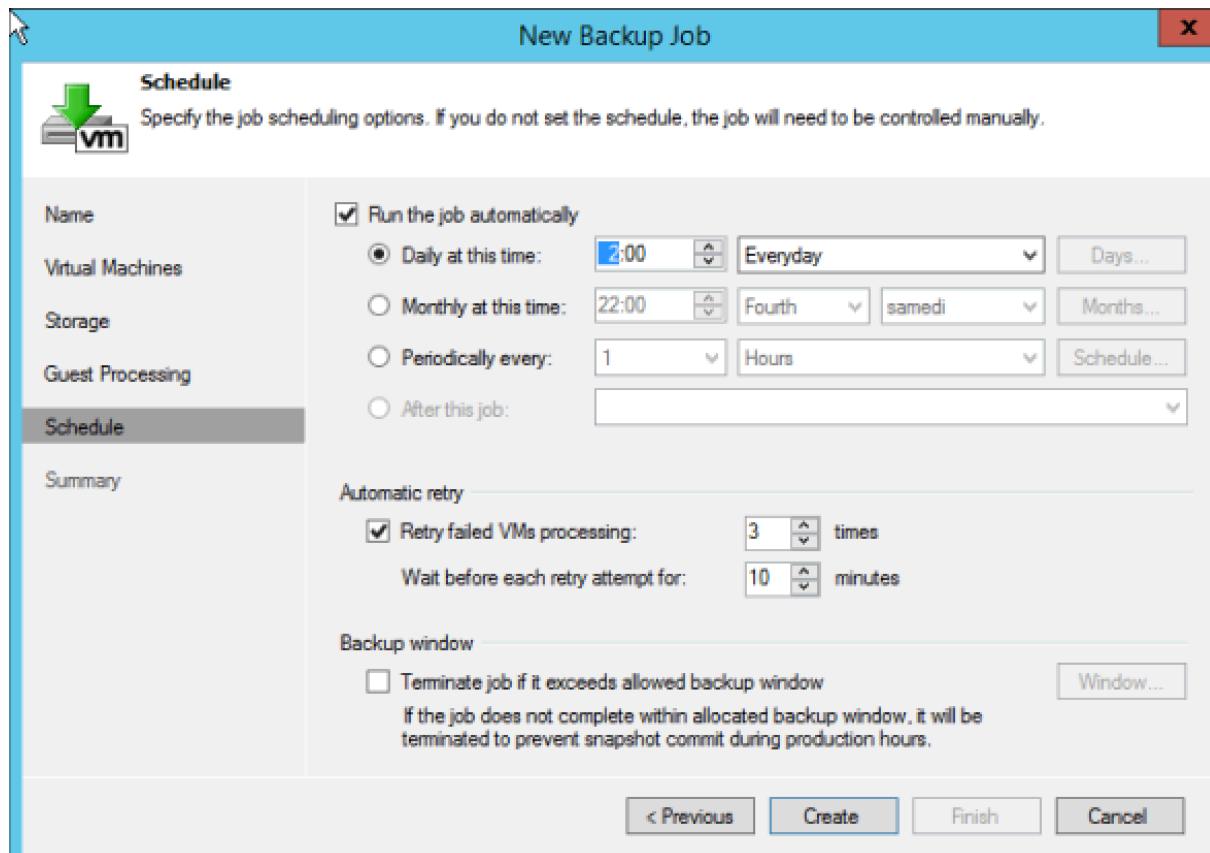
Ici, on définit que notre job tournera tous les jours :



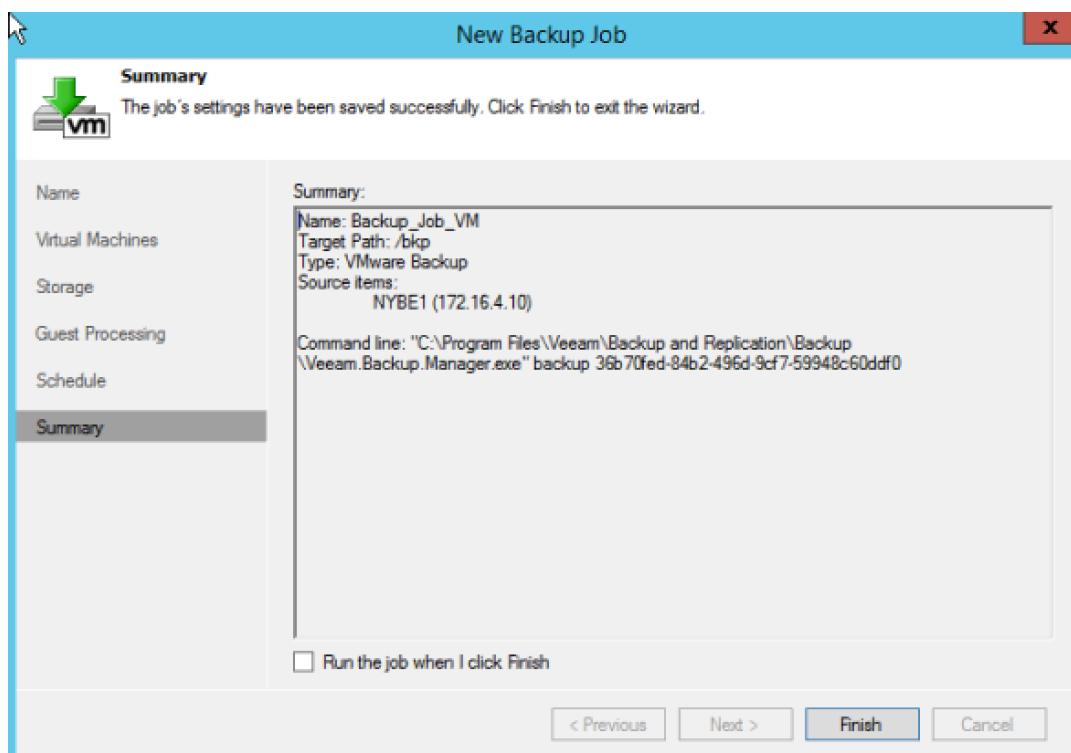
On clique sur **OK**, puis sur **Next**, sur la nouvelle fenêtre on n'active pas les options, on clique alors sur **Next** une nouvelle fois :



Ici, on coche la case **Run the job automatically** et on choisit l'option **Daily at this time**, conformément au cahier des charges on définit le lancement du job à 2h du matin tous les jours :



Enfin on clique sur **Finish** :



Notre job va alors commencé dès le lendemain à 2h du matin.

P. Mise en place du système de téléphonie IP

a) Création de la machine virtuelle et installation d'Asterisk

Nous créons une machine virtuelle sous Debian 8, dont voici la configuration :

- Disque dur : 8Go
- RAM : 512 Mo
- Configuration réseau (**nano /etc/network/interfaces**) :

```
allow-hotplug eth1
iface eth1 inet static
    address 172.16.4.50
    netmask 255.255.248.0
    gateway 172.16.7.254
    dns-nameservers 172.16.4.1
```

Nous allons maintenant procéder à l'installation d'Asterisk :

- 1) Nous commençons par mettre à jour les dépôts de paquets :

```
apt-get update && apt-get upgrade
```

- 2) Installation des dépendances :

```
apt-get install build-essential libxml2-dev libncurses5-dev linux-headers-3.2.0-4-all libsqlite3-dev uuid-dev libjansson-dev libssl-dev
```

- 3) On crée notre répertoire asterisk et on se positionne dedans :

```
mkdir /usr/src/asterisk && cd /usr/src/asterisk
```

- 4) On télécharge Dahdi et on le décomprime :

```
wget http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi-linux-complete-current.tar.gz
tar -xvzf dahdi-linux-complete-current.tar.gz && cd dahdi-linux-complete-2.6.0+2.6.0/
```

- 5) Compilation et installation de Dahdi :

```
make all && make install && make config && /etc/init.d/dahdi start
```

- 6) On se repositionne dans le dossier asterisk :

```
cd /usr/src/asterisk
```

7) Téléchargement des sources d'Asterisk :

```
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-current.tar.gz
```

8) Décompression et positionnement dans le dossier décompressé :

```
tar -xvzf asterisk-13-current.tar.gz && cd asterisk-13.4.0/
```

9) Vérification des dépendances et sélection des options de compilation :

```
./configure && make menuselect
```

10) Compilation et installation d'Asterisk :

```
make && make install
```

11) Création des fichiers de configuration et lancement des scripts :

```
make samples && make config
```

12) Démarrage d'Asterisk :

```
/etc/init.d/asterisk start
```

b) Configuration d'Asterisk

i. Configuration des utilisateurs

Nous allons commencer par configurer nos utilisateurs dans le fichier adéquate :

```
nano /etc/asterisk/users.conf
```

Voici la configuration adaptée conformément au cahier des charges (ici, seulement 3 utilisateurs par service ont été créés pour effectuer les tests) :

```
[mewpipe_user_template] (!)
```

```
type=friend
disallow=all
allow=ulaw
host=dynamic
dtmfmode=rfc2833
hassip=yes

[it_support_template] (!,mewpipe_user_template)
context=it_support_template

[accounting_template] (!,mewpipe_user_template)
context=accounting_template

[logistic_template] (!,mewpipe_user_template)
context=logistic_template

[public_relation_template] (!,mewpipe_user_template)
context=public_relation_template

[marketing_template] (!,mewpipe_user_template)
context=marketing_template

[134] (it_support_template)
fullname = Eddard STARK
username = estark
secret = *****

[135] (it_support_template)
fullname = Catelyn STARK
username = cstark
secret = *****

[136] (it_support_template)
fullname = Robb STARK
username = rstark
secret = *****

[200] (accounting_template)
fullname = Jon SNOW
username = jsnow
secret = *****

[201] (accounting_template)
fullname = Samwell TARLY
username = starly
secret = *****

[202] (accounting_template)
fullname = Jeor MORMONT
username = jmormont
secret = *****

[400] (logistic_template)
fullname = Petyr BAELISH
username = pbaelish
secret = *****

[401] (logistic_template)
fullname = Lord VARYS
```

```

username = lvarys
secret = *****

[402] (logistic_template)
fullname = Tyrion LANNISTER
username = tlannister
secret = *****

[480] (public_relation_template)
fullname = Rhaegar TARGARYEN
username = rtargaryen
secret = *****

[481] (public_relation_template)
fullname = Aegon TARGARYEN
username = atargaryen
secret = *****

[482] (public_relation_template)
fullname = Daenerys TARGARYEN
username = dtargaryen
secret = *****

[500] (marketing_template)
fullname = Jamie LANNISTER
username = jlannister
secret = *****

[501] (marketing_template)
fullname = Cersei LANNISTER
username = clannister
secret = *****

[502] (marketing_template)
fullname = Tywin LANNISTER
username = tlannister
secret = *****

```

ii. Configuration du dialplan

Nous devons maintenant configurer notre dialplan dans le fichier **extensions.conf** :

```
nano /etc/asterisk/extensions.conf
```

Voici sa configuration :

```

[it_support_template]
exten => _XXX,Dial(SIP/${EXTEN},20)
exten => _XXX,n,Hangup()

[accounting_template]
exten => _XXX,1,Dial(SIP/${EXTEN},10)
exten => _XXX,n,Hangup()

[logistic_template]

```

```

exten => _XXX,1,Dial(SIP/${EXTEN},20)
exten => _XXX,n,Hangup()

[public_relation_template]
exten => _XXX,1,Dial(SIP/${EXTEN},20)
exten => _XXX,n,Hangup()

[marketing_template]
exten => _XXX,1,Dial(SIP/${EXTEN},20)
exten => _XXX,n,Hangup()

```

Cette configuration permet à tous les utilisateurs de s'appeler entre eux. S'il n'y a pas de réponse au bout de 20 secondes, l'appel prend fin.

iii. Configuration du serveur IVR

Nous devons maintenant configurer un serveur IVR qui doit donner la possibilité aux utilisateurs de choisir entre un service et un utilisateur. Si l'utilisateur choisit un service, cela fera sonner tous les téléphones du service. Dans l'autre cas, l'utilisateur fournit l'ID de l'utilisateur qu'il veux appeler et son appel est donc redirigé vers ce dernier.

Nous allons donc commencer par configurer des « rings group » qui permettront de faire sonner tous les téléphones d'un service. Nous avons décidé que le dernier numéro de chaque plage des différents services servira de ring group. Il nous faut donc renseigner les informations suivantes dans le dialplan :

```

[it_support_template]
exten => 146,1,Dial(SIP/134&SIP/135&SIP/136,20)
exten => 146,n,Hangup()

[accounting_template]
exten => 251,1,Dial(SIP/200&SIP/201&SIP/202,20)
exten => 251,n,Hangup()

[logistic_template]
exten => 478,1,Dial(SIP/400&SIP/401&SIP/402,20)
exten => 478,n,Hangup()

[public_relation_template]
exten => 492,1,Dial(SIP/480&SIP/481&SIP/482,20)
exten => 492,n,Hangup()

[marketing_template]
exten => 634,1,Dial(SIP/500&SIP/501&SIP/502,20)
exten => 634,n,Hangup()

```

Nous allons maintenant construire un IVR qui aura pour numéro interne 1000. Nous allons utiliser le **Text-to-speech** de GoogleTTS pour notre IVR. Pour cela, nous avons quelques dépendances à installer :

- 1) Nous commençons par installer les dépendances :

```
apt-get install perl libwww-perl sox mpg123
```

2) Téléchargement de GoogleTTS :

```
wget -O GoogleTTS.tar.gz http://github.com/zaf/asterisk-googletts/tarball/master --no-check-certificate
```

3) On le décomprime et on l'installe dans le bon dossier :

```
tar -xvf GoogleTTS.tar && cd zaf-asterisk-googletts-51c2db5 && cp googletts.agi /var/lib/asterisk/agi-bin/
```

GoogleTTS est maintenant prêt à utiliser, on va maintenant ajouter notre IVR dans le dialplan (**/etc/asterisk/extensions.conf**) :

```
[ivr_number]
exten => 1000,1,Goto(ivr,s,1)

[ivr]
exten => s,1,Answer()
exten => s,2,Set(TIMEOUT(response)=10)
exten => s,3,agi(googletts.agi,"Welcome to MEWPIPE company!",en,any)
exten => s,4,agi(googletts.agi,"Which department would you like to speak to?",en,any)
exten => s,5,agi(googletts.agi,"Press 1 to contact IT support department",en,any)
exten => s,6,agi(googletts.agi,"Press 2 to contact Accounting department",en,any)
exten => s,7,agi(googletts.agi,"Press 3 to contact Logistic department",en,any)
exten => s,8,agi(googletts.agi,"Press 4 to contact Public Relation department",en,any)
exten => s,9,agi(googletts.agi,"Press 5 to contact Marketing department",en,any)
exten => s,10,agi(googletts.agi,"Press 6 to contact directly a user",en,any)
exten => s,11,agi(googletts.agi,"Press # to listen again this message",en,any)
exten => s,12,WaitExten()

exten => 1,1,Goto(it_support_internal,146,1)
exten => 2,1,Goto(accounting_internal,251,1)
exten => 3,1,Goto(logistic_internal,478,1)
exten => 4,1,Goto(public_relation_internal,492,1)
exten => 5,1,Goto(marketing_internal,634,1)
exten => _[07-9#*],1,Goto(ivr,s,3)
exten => t,1,Goto(ivr,s,3)
```

Il faut maintenant déclarer dans chaque section des services la référence à l'IVR :

```
[it_support_template]
include => ivr_number
```

iv. Appel vers les numéros PSTN français

Nous allons commencer par configurer un trunk SIP dans notre fichier `/etc/asterisk/sip.conf` dans la section **[general]** :

```
register => mewpipe@getonsip.com:DuhQHpTk0LFtQ7Ft:mewpipe@sip.onsip.com
```

Enfin on le déclare :

```
[mewpipe_out]
type=peer
secret=DuhQHpTk0LFtQ7Ft
username=mewpipe
host=sip.onsip.com
fromuser=mewpipe
canreninvite=no
insecure=invite,port
qualify=yes
nat=yes
context=outgoing_calls
```

Nous pouvons alors déclarer nos appels sortants dans notre dialplan :

```
[mewpipe_out]
exten => _XXXXXXXXXX,1,Dial(SIP/mewpipe_out/${EXTEN})
exten => _XXXXXXXXXX,2,Goto(trunk_fail,s,1)

[trunk_fail]
exten => s,1,Answer()
exten => s,2,Playtones(congestion)
exten => s,3,Congestion()
```

Enfin, on déclare la référence dans les sections de nos services :

```
[it_support_template]
include => mewpipe_out
```

v. Configuration des clients X-Lite

Après installation du client X-Lite, on se rend dans les paramètres, et on va renseigner un **User ID** existant, le **Domain** (l'adresse IP de notre serveur Asterisk) et le mot de passe définit dans le fichier `users.conf` :

Sip Account - Ready

Account name: valentin

Use for: Call
 IM/Presence

General Voicemail Topology Presence Transport Advanced

User Details

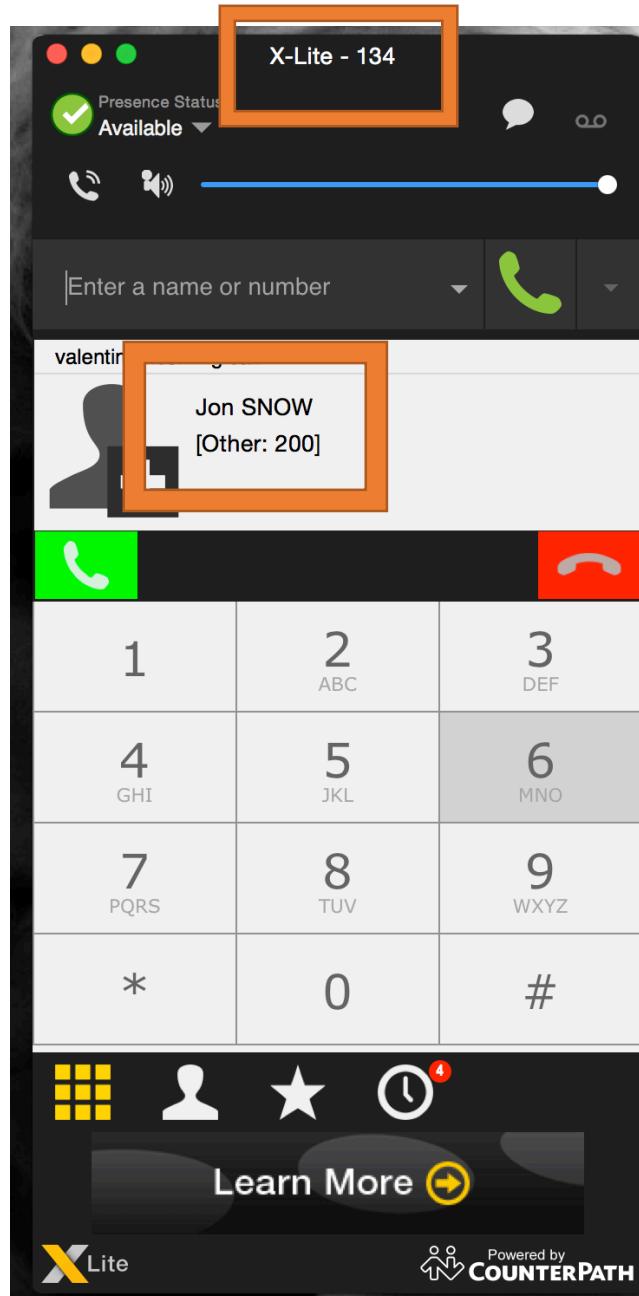
* User ID	134
* Domain	172.16.4.50
Password	•••
Display name	
Authorization name	

On peut alors voir que notre compte est activé :

The screenshot shows the X-Lite application window. At the top, there is a navigation bar with icons for Application, Accounts, Alerts, Devices, Codecs, and Call, along with a Preferences button. Below the navigation bar is a table displaying account information:

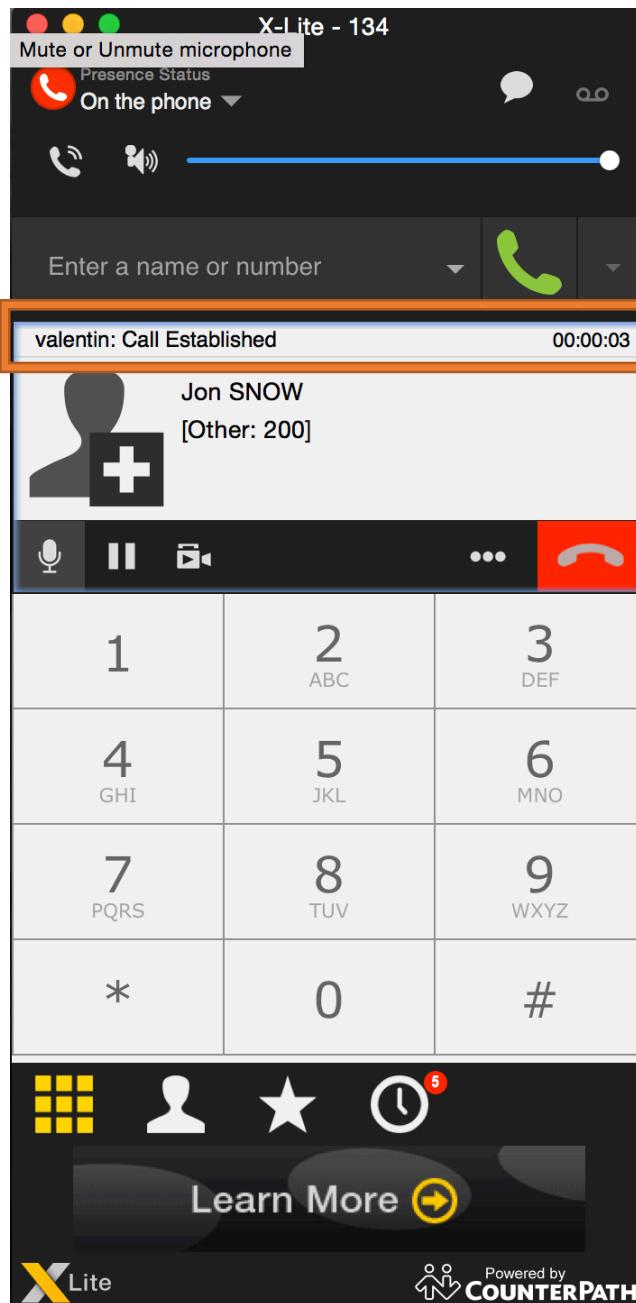
Ena...	Sta...	Account Name	Proto...	User ID	Call
<input checked="" type="checkbox"/>	●	valentin	SIP	134	✓

Enfin, d'un notre client X-Lite (ID = 200), nous appelons l'user ID 134 que nous venons de configurer.
 Voici l'appel :



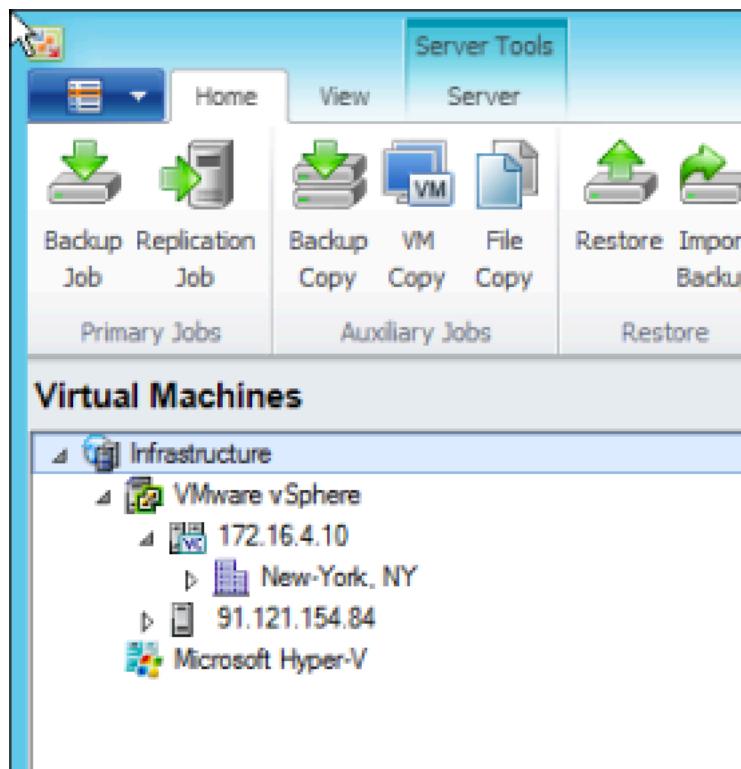
On peut alors constater dans les encadrés orange, que l'user ID 200 est bien Jon SNOW comme configuré dans notre fichier **users.conf** et qu'il appelle bien l'user ID 134.

Une fois décroché, on voit que l'appel est établi :

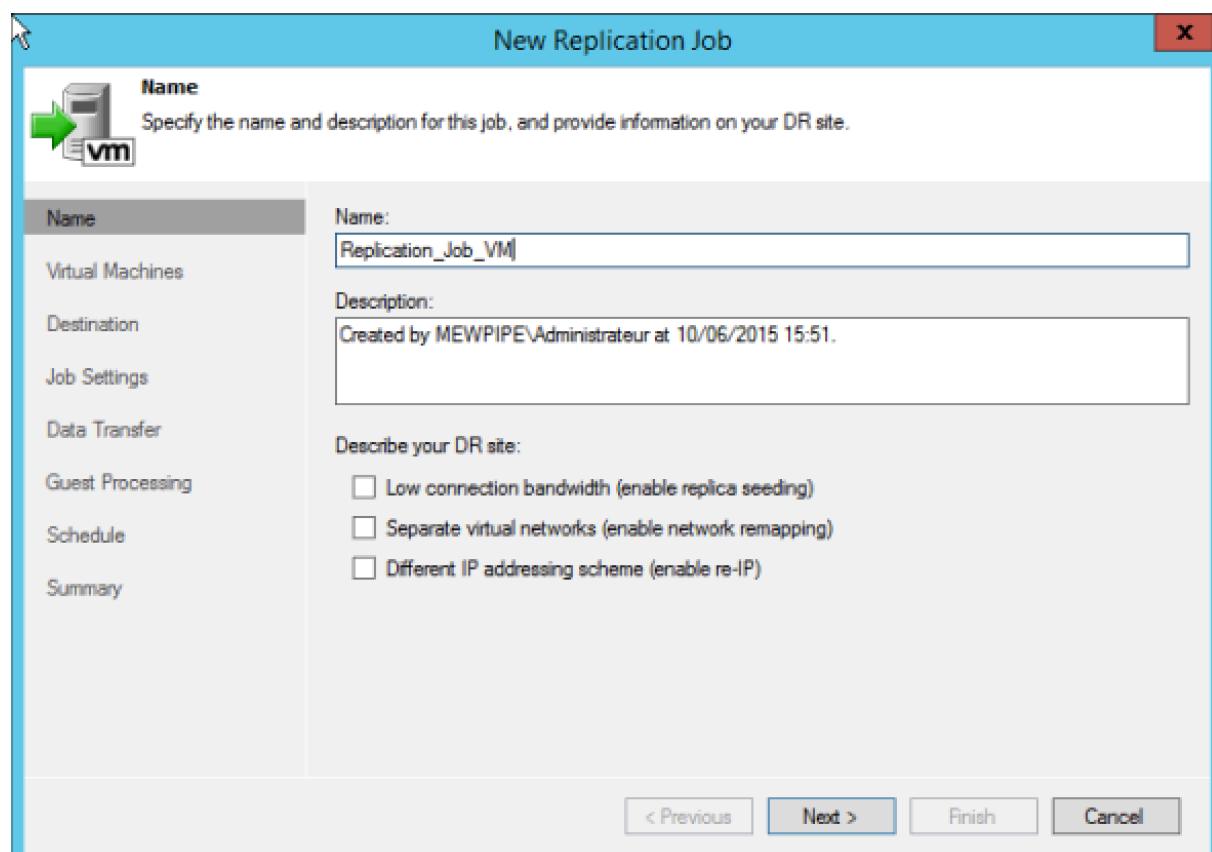


Q. Création d'un job de réPLICATION des machines virtuelles

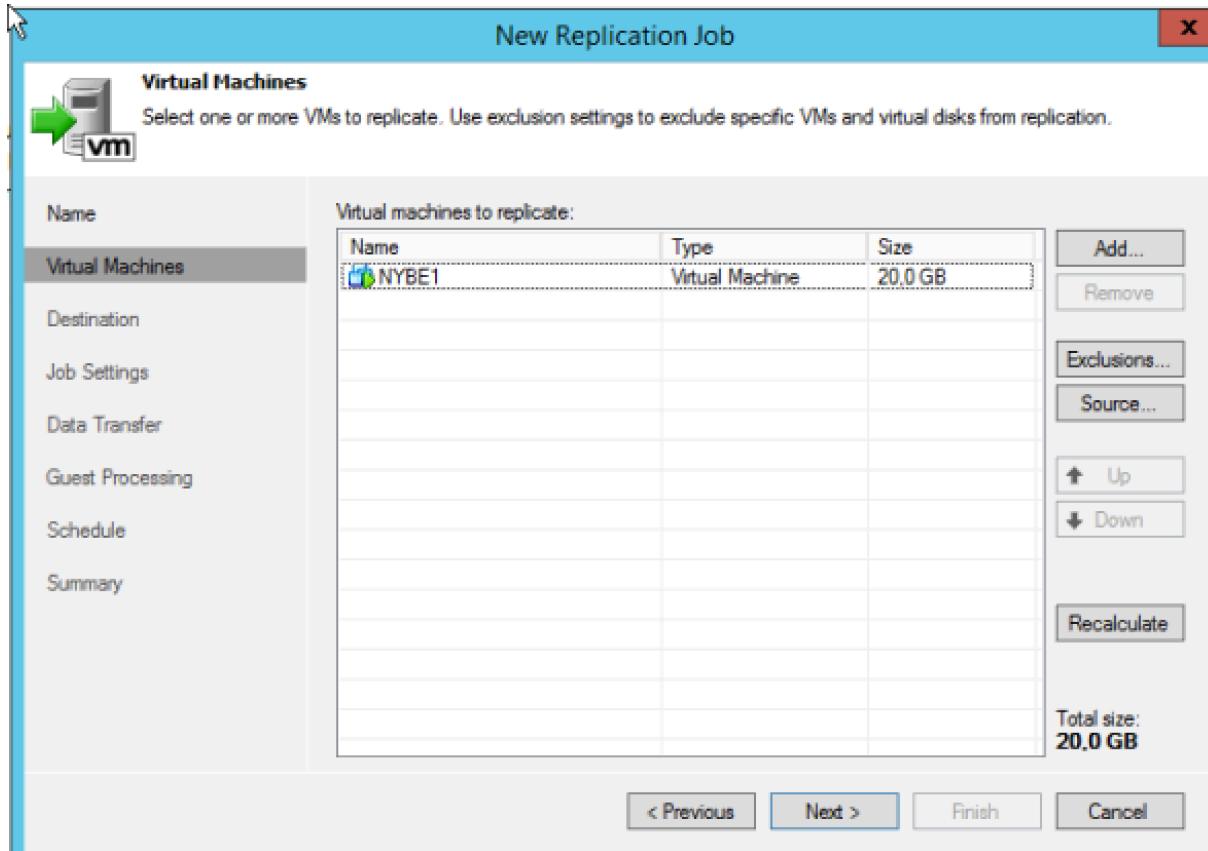
Pour cela, on clique sur **Home** puis sur **Replication job** :



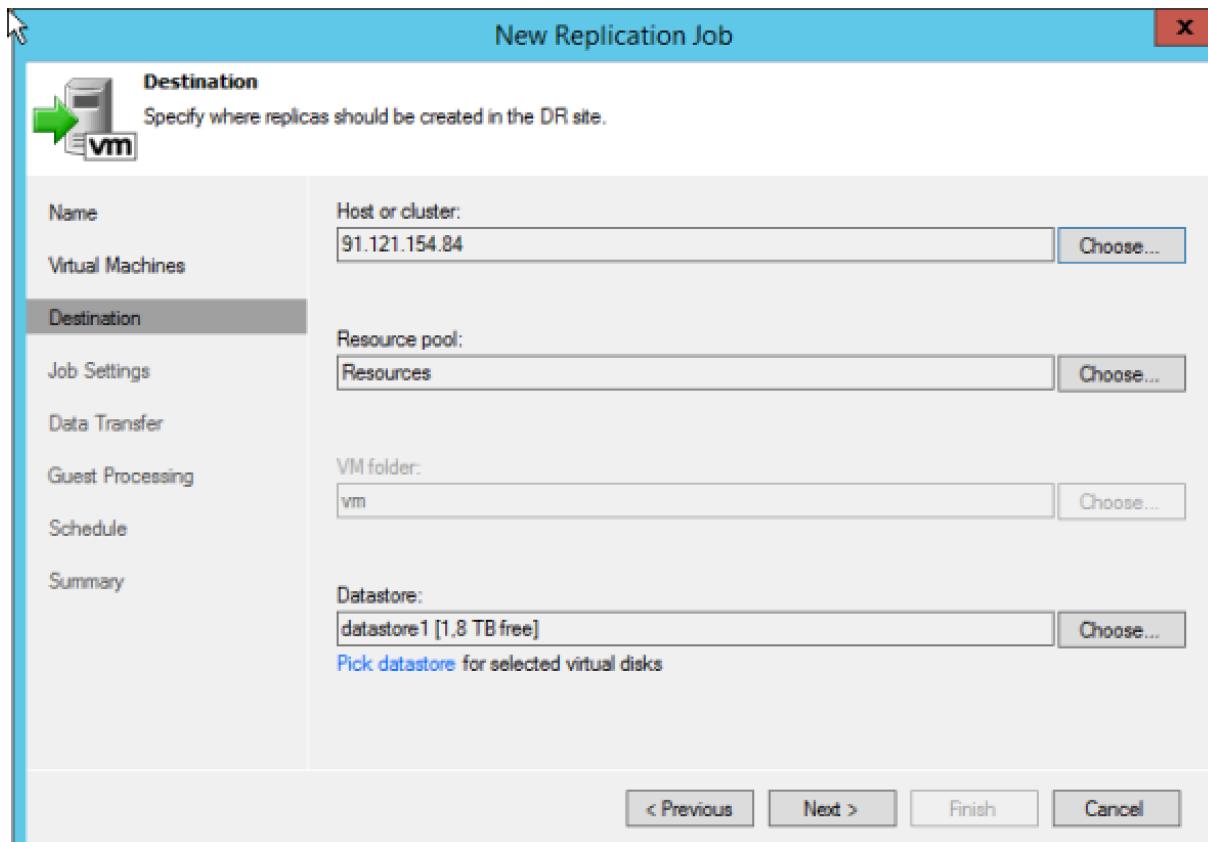
On entre le nom et la description du Job :



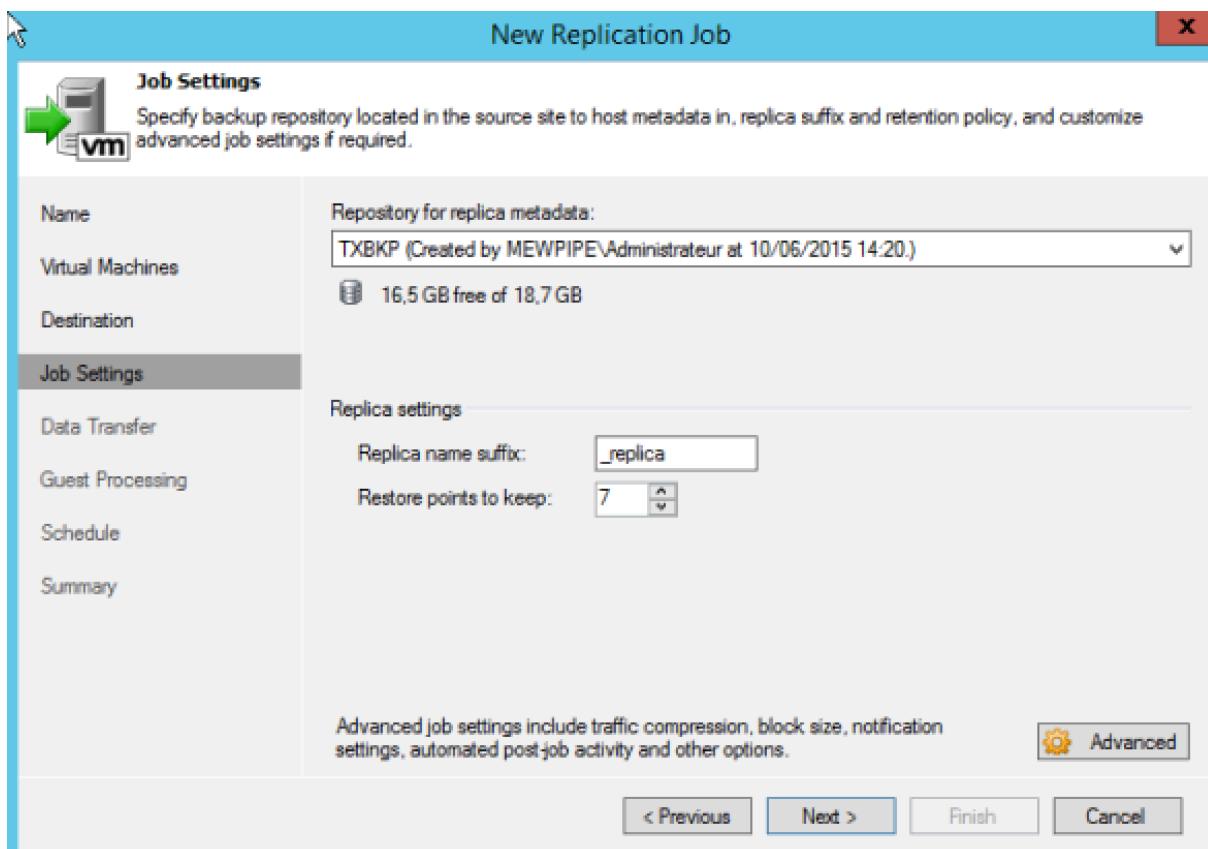
On choisit maintenant les machines virtuelles que l'on souhaite répliquer :



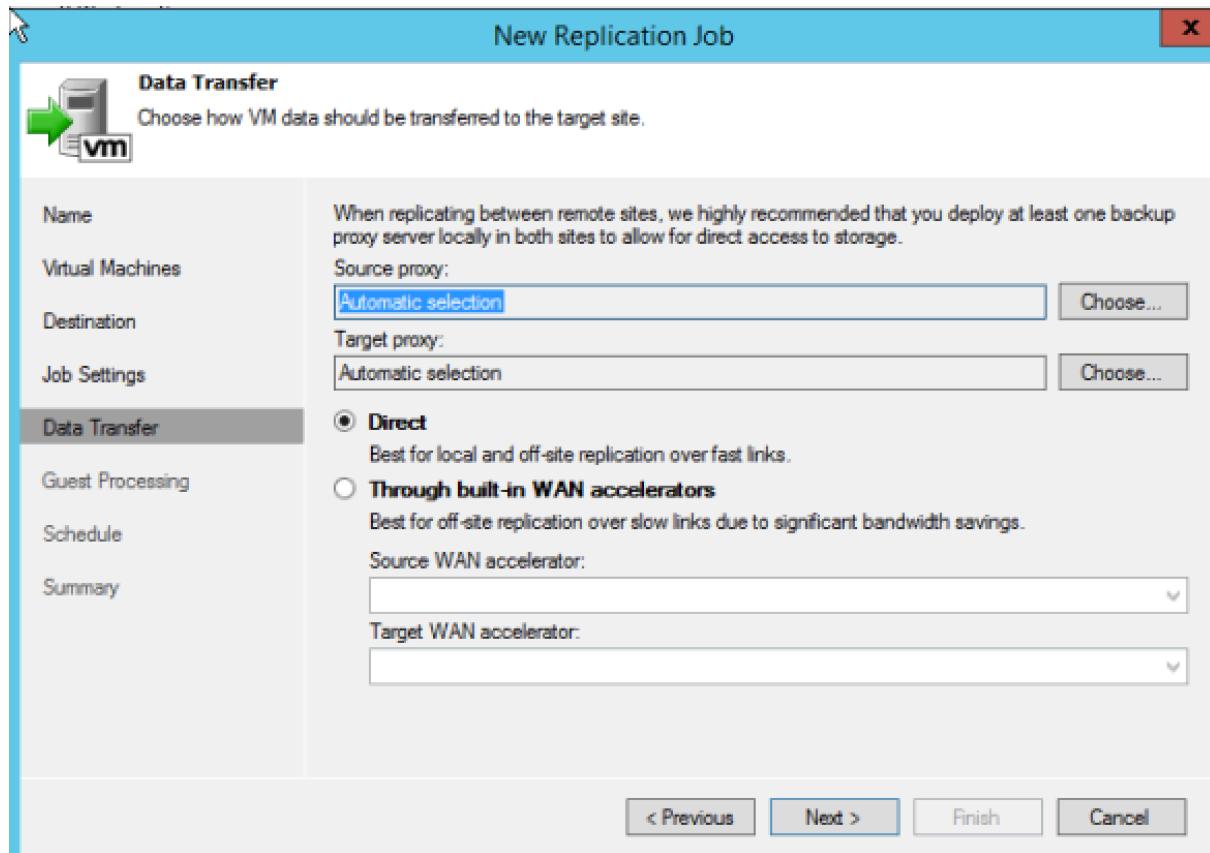
On choisit ensuite l'hôte de destination (dans le cas présent, dans un souci de ressources, le datacenter de Dallas est représenté par un ESXi, sur un serveur dédié) :



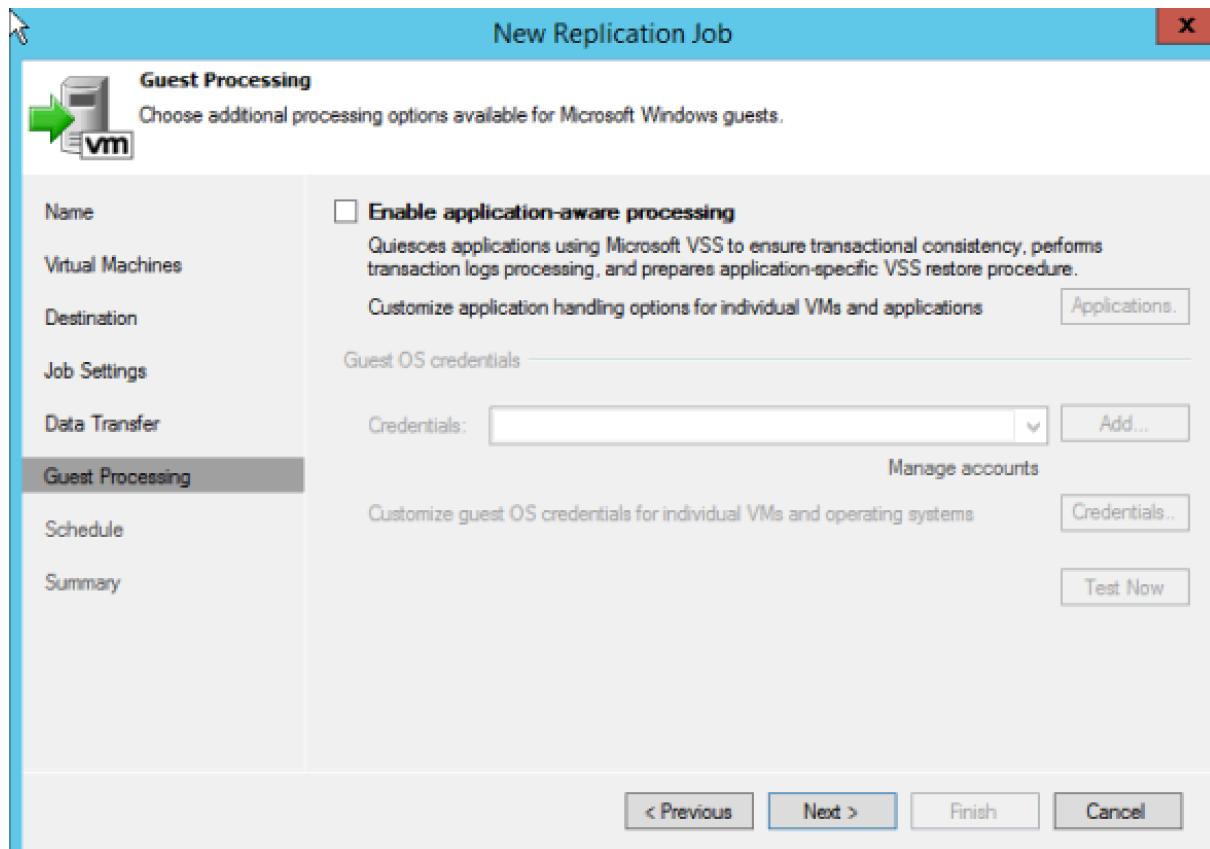
On choisit notre repository pour le réplica des metadata :



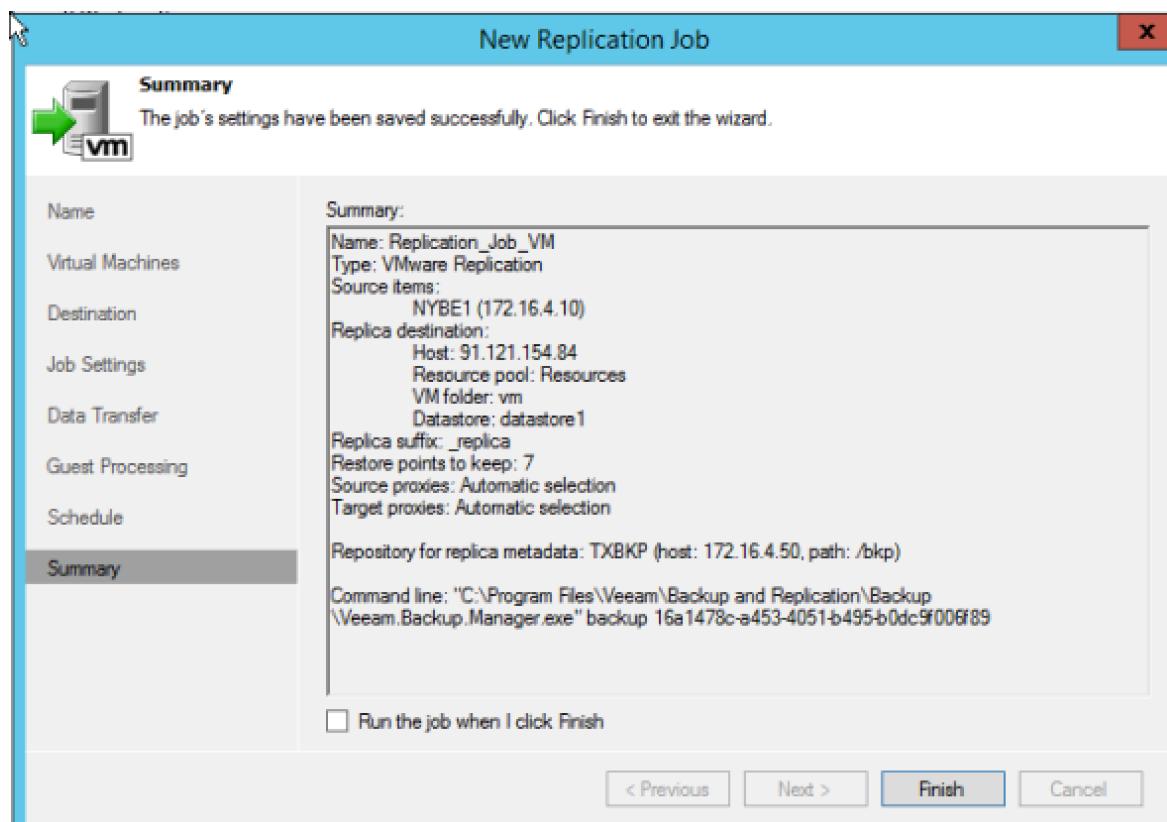
On laisse ensuite les options par défaut (**Direct**) et on clique sur **Next** :



On clique de nouveau sur **Next** :



On choisit les options de démarrage du job, puis on clique sur **Next** pour enfin cliquer sur **Create** :



Notre job est alors créé, notre machine virtuelle sera alors accessible depuis le datacenter de Dallas.

R. Gestion des cas de pannes

a) Introduction

Dans cette partie nous allons voir comment sont gérés les cas de pannes, comment la continuité de service est assurée et à quel point l'infrastructure est robuste.

b) Equipements réseaux

i. Panne d'un routeur/pare-feu

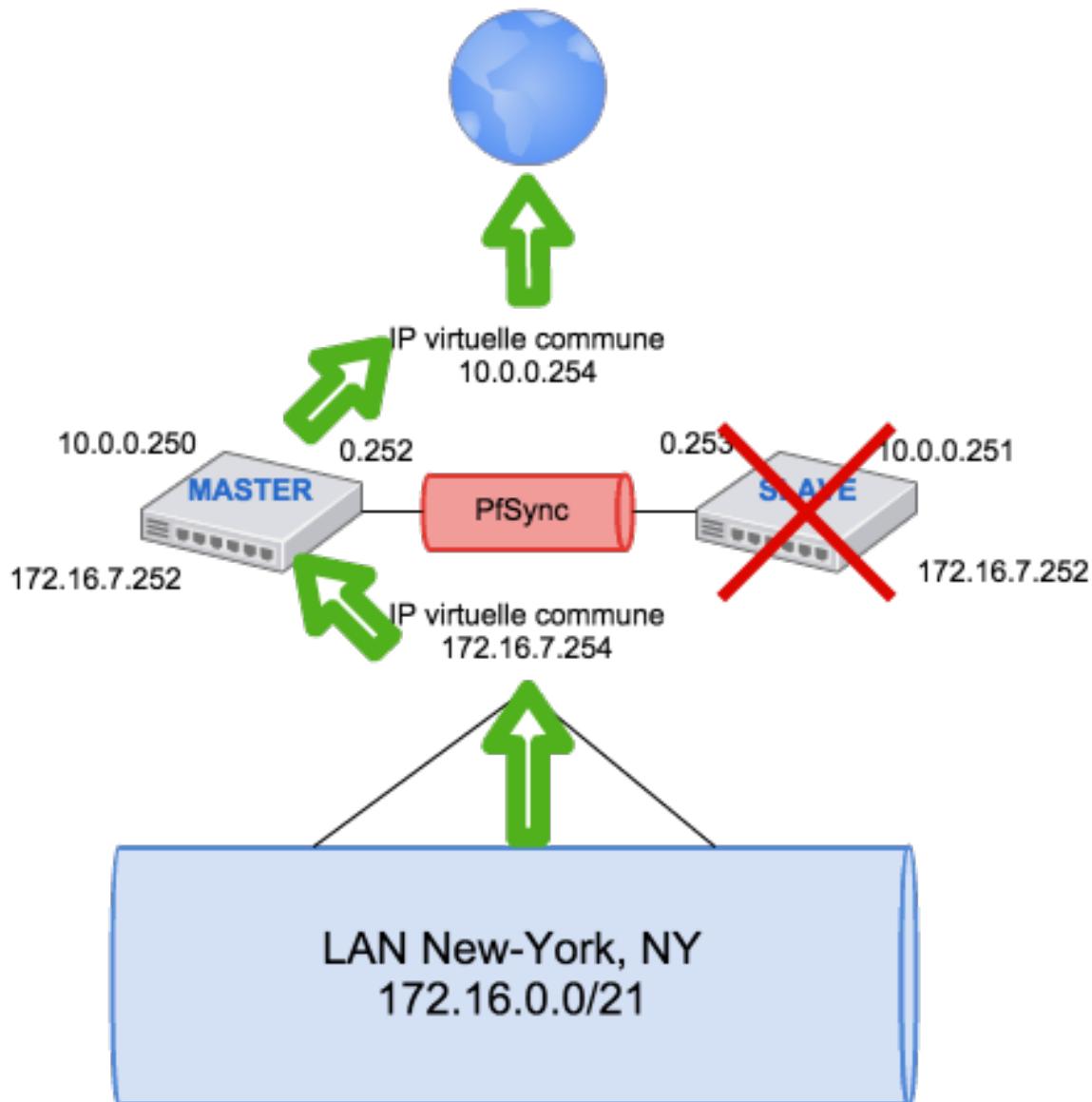
Pour chaque datacenter, si un routeur venait à tomber en panne, le service continuerait à être assurée, avec seulement la perte d'un ping, ce qui serait transparent pour l'utilisateur. Puisque chaque routeur fait partie d'un cluster qui partage une IP virtuelle LAN et une WAN.

Un routeur est désigné Master et l'autre est désigné Slave. Ainsi, lorsqu'un client effectue une requête, le routeur Master répondra en priorité via son interface virtuelle LAN.

Les deux routeurs partagent de nombreuses informations importantes (règles firewall, routes, ipsec...) via une interface dédiée appelée PfSync sur chaque routeur. Ainsi, lorsqu'une modification est effectuée sur un routeur, cette dernière est répercutée sur son acolyte.

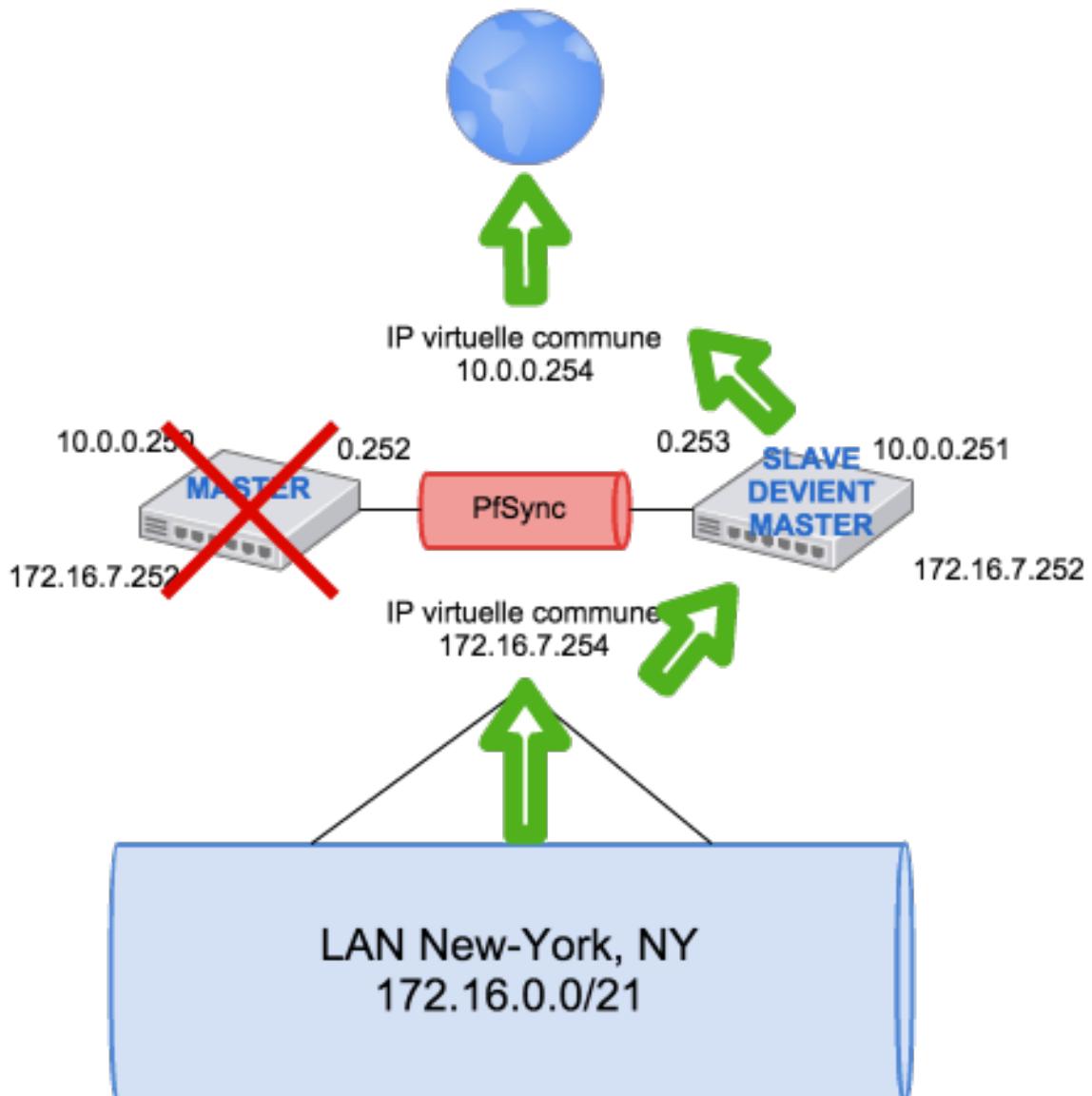
Voici les différents cas de pannes schématisés :

- Panne du routeur **slave** :



Si le routeur slave est amené à tomber, pas de changement, le routeur Master est toujours présent pour répondre aux différentes requêtes.

- Panne du routeur **Master** :

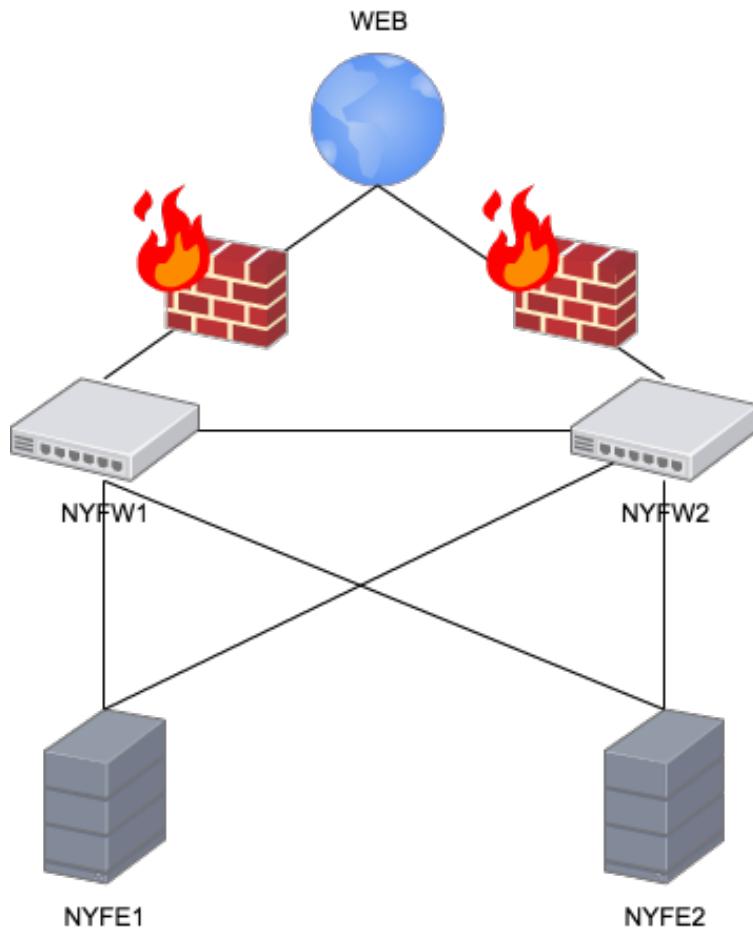


En cas de panne du routeur Master, le routeur slave (aussi appelé backup sous pfSense) devient alors le routeur Master et s'occupera de répondre aux requêtes des clients.

c) Load-balancing web des routeurs / pare-feux

Une haute disponibilité et de la répartition de charge ont été implémenté en vue de l'importance du trafic du projet Mewpipe. Ainsi, nos routeurs vont répartir la charge entre nos serveurs web (Load-balancing) voire basculer toute la charge sur l'un ou sur l'autre en cas de défaillance de l'un ou de l'autre (Fail-over).

Ceci peut se schématiser de la manière suivante :



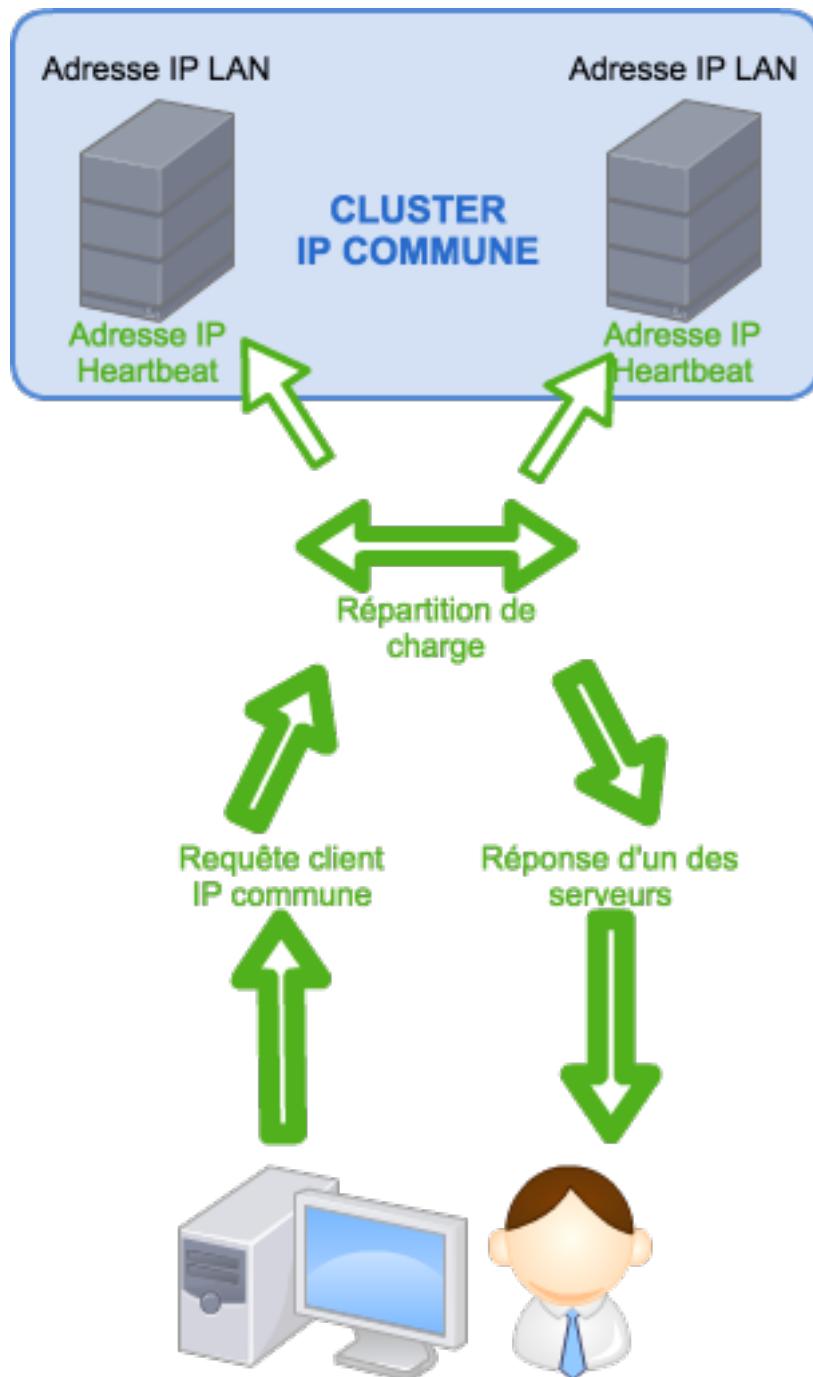
Dans la configuration actuelle, lorsqu'un serveur web ne répond pas après 3 essais consécutifs, il sera considéré comme hors service et s'appliquera alors un fail-over. Toute la charge sera alors portée sur l'autre serveur web.

Nos deux serveurs web sont en fait intégrés à un pool de load-balancing, dans lequel on crée un serveur virtuel qui représente l'interface WAN sur laquelle les requêtes clients web arrivent.

d) Panne serveur

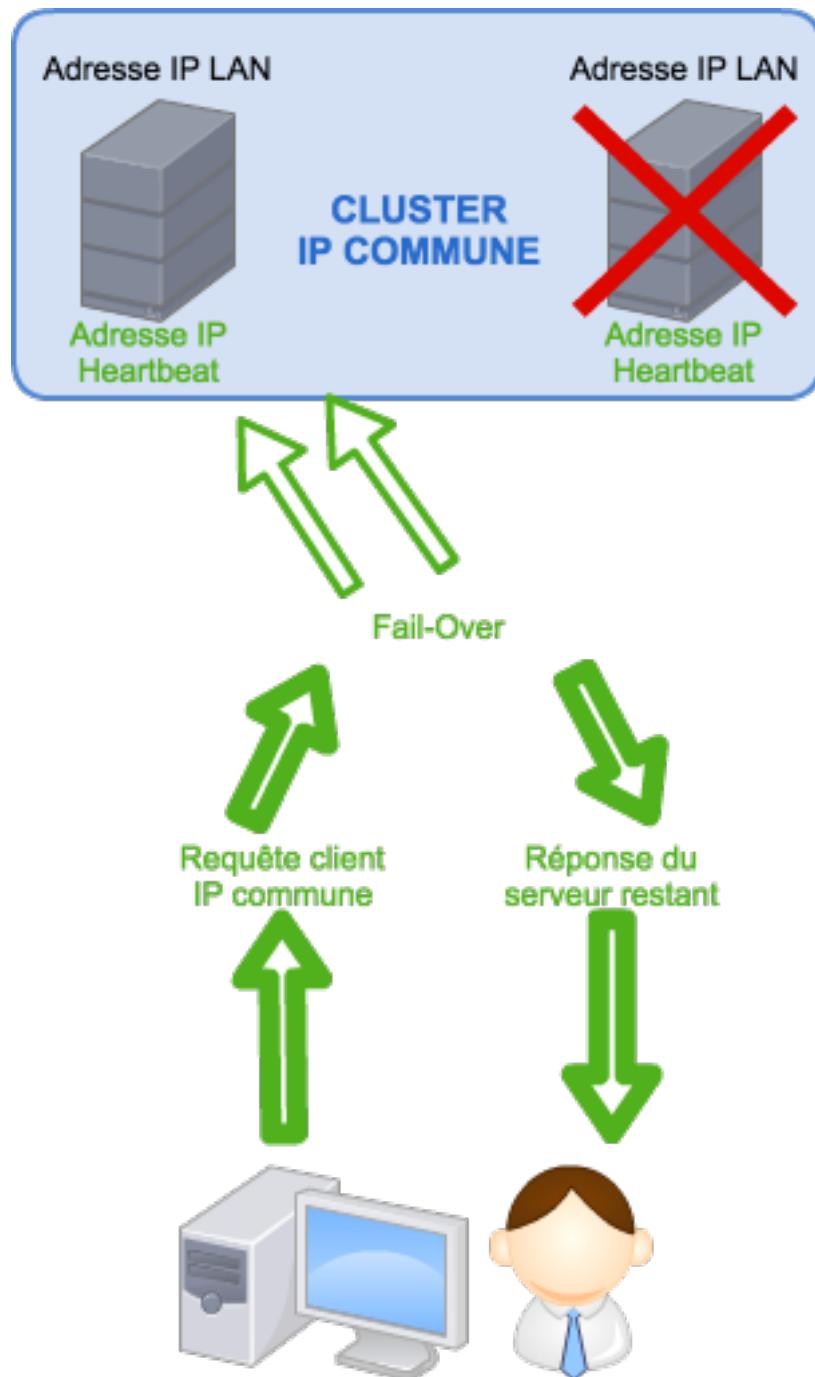
L'architecture implémentée permet une redondance à tous les niveaux et assure ainsi une continuité de service des applications tournant sur les serveurs. En effet, chaque partie de l'infrastructure trois-tiers est mise en cluster permettant ainsi un équilibrage de charge et une tolérance de panne selon le schéma suivant :

- ✓ Tolérance de panne :



Dans le cas présent, lorsqu'un client effectue une requête sur un des serveurs de notre architecture trois-tiers, il va requérir indirectement l'IP commune de ce cluster. Le cluster va ensuite effectuer une répartition de charge entre les serveurs qui composent le cluster. Toutes les informations de cluster sont échangées via un réseau dédié appelé **Heartbeat**.

- ✓ Tolérance de panne :



Ici, lorsqu'un client effectue une requête et qu'un des serveurs est tombé, le cluster va automatiquement rediriger toutes les requêtes sur le serveur qui est encore en marche. Il aura plus de charges mais les requêtes seront assurées jusqu'à ce que la panne de l'autre serveur soit réparée.

Pour résumé, nous avons au sein d'un datacenter, une tolérance de panne et une répartition de charge au niveau de notre front-end, de notre API et de notre base de données.

e) Panne datacenter

Nos deux datacenters New-York et Dallas fonctionnent comme un cluster actif/passif où New-York est le datacenter actif, conformément au cahier des charges.

Ainsi, dans le cas une catastrophe venait à survenir sur le datacenter de Dallas, les applications et différents services de seraient pas altérés. Le datacenter de New-York serait toujours présent pour répondre aux requêtes, le temps que les choses reviennent à la normal sur notre datacenter de Dallas.

En revanche, dans le cas d'une catastrophe amenant l'arrêt du datacenter de New-York, une solution a été implémenté pour assurer la continuité de services. Cette solution est schématisée ci-après :

