# Etapes générales de la mise en place de l'infrastructure

## I. Mise en place du routeur

### 1. Création des interfaces

Au premier démarrage, seules 2 interfaces réseaux de pfSense sont actives, et ont chacune une adresses IP attribuée automatiquement ; en effet, pfSense intègre un serveur DHCP, mais nous ne l'utiliserons pas. On peut remarquer que chaque interface a un nom qui lui est propre : **em0**, **em1**…. La connexion **em0**, correspondante au réseau interne, sera donc la passerelle du réseau serveur (**10.1.10.0/29**) ; la **em1**, en bridge, sera la passerelle du réseau des postes (**192.168.1.0/24).**

Dans le menu principal, entrez le chiffre **1** pour lancer la configuration des interfaces. Faites **Non** à la demande de configuration des VLANs. Affectez l'interface **em0** au **WAN**, et la **em1** au **LAN**. Validez en saisissant **yes**.

```
em1     08:00:27:2d:61:96   (up) Intel(R) PRO/1000 Legacy Network Connection 1.

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y|n]? y
```

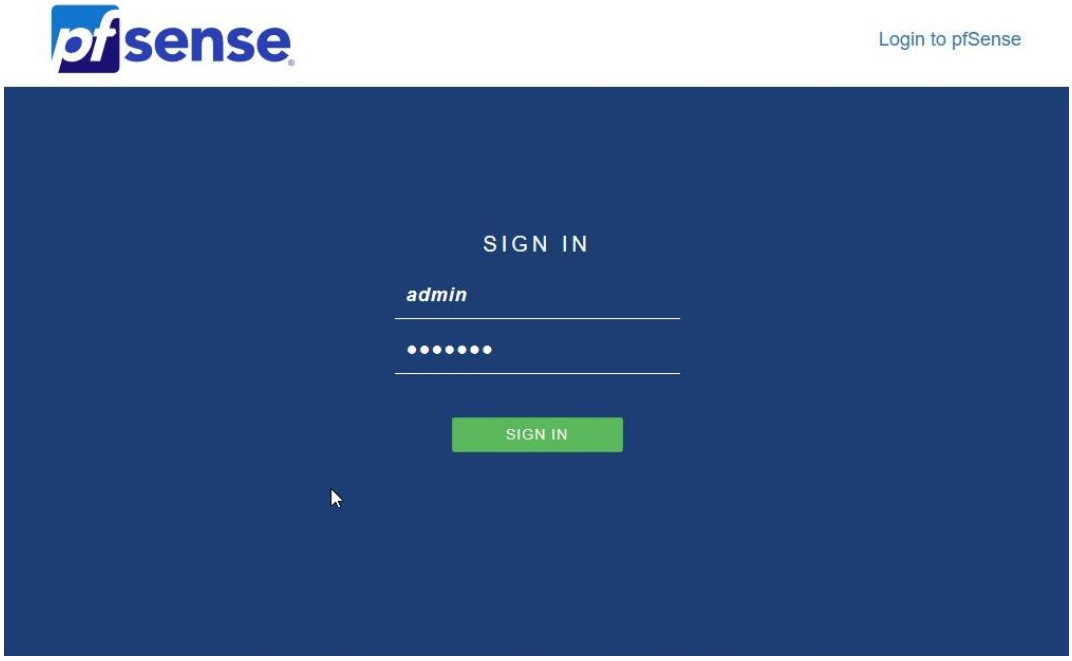
### 2. Attribution des adresses IP

De retour au menu, saisissez **2** pour configurer les adresses IP. Puis pour chaque interface, configurez l'adresse IP et le CIDR. N'activez pas le DHCP et l'IPv6. La configuration finale doit être la suivante :

```
The IPv4 LAN address has been set to 192.168.1.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.1.254/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 71c9ea4a10848952302f

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 10.1.10.6/29
 LAN (lan)       -> em1        -> v4: 192.168.1.254/24

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

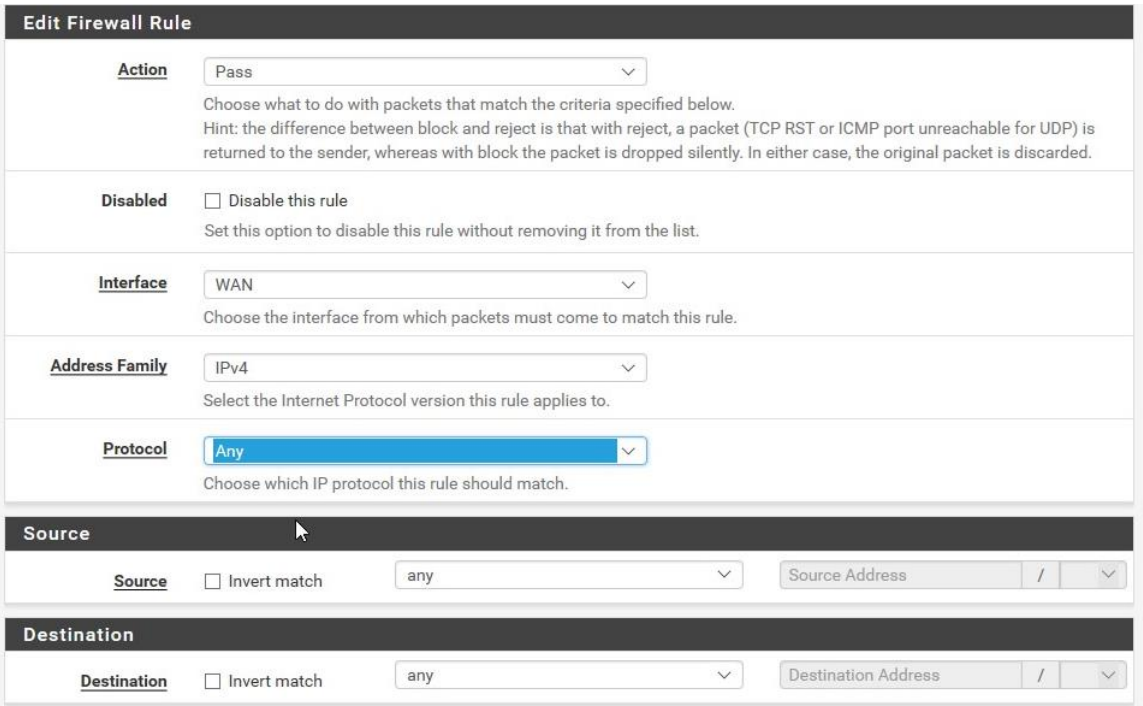
## 3. Configuration du Pare-Feu en Allow-All

Une fois la configuration IP de pfSense terminée, l'interface WEB du routeur devrait être accessible. Pour cela, branchez une machine à l'interface **LAN** de pfSense (il faut donc qu'elle soit sur le même réseau et qu'elle ait **192.168.1.254** en passerelle par défaut), lancez un navigateur WEB et dans la barre de recherche, saisissez l'adresse de la passerelle : **https://192.168.1.254/.** Le login est **admin**, le mot de passe **pfsense**.



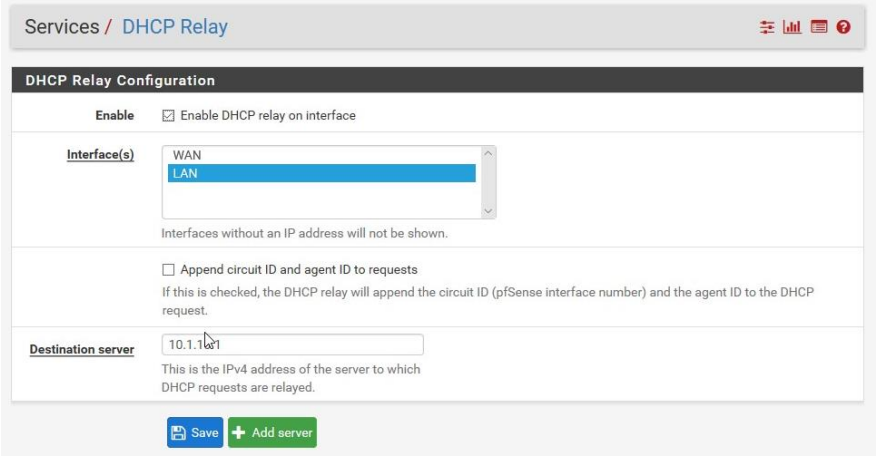

Faites suivant à toutes les pages ; une fois arrivé sur la page d'accueil, allez dans **Firewall > Rules**.

Chaque onglet correspond à une interface (**WAN**, ou **LAN**). Pour chaque interface, ajoutez une nouvelle règle en haut de liste, autorisant les flux de tous les protocoles, venants de n'importe quelle source, vers n'importe quelle destination. Sauvegardez et appliquez.



### 4. Mise en place du relai DHCP

Une fois les règles de pare-feu configurées, nous allons maintenant avoir besoin d'un relai DHCP afin de transférer toutes les requêtes DHCP des clients vers notre futur serveur DHCP. Pour cela, rendez-vous dans **Services > DHCP Relay**.



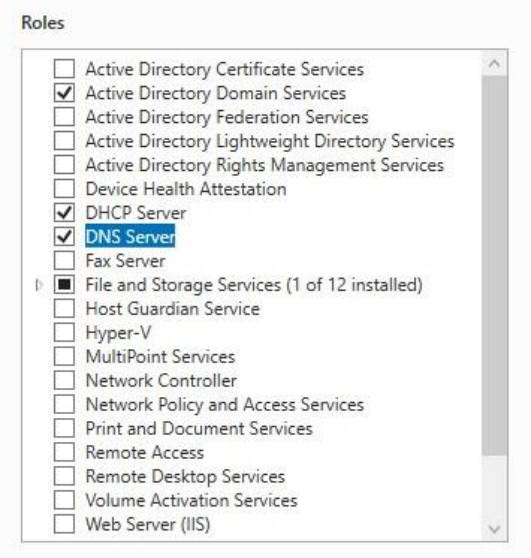

Cochez **Enable DHCP relay on interface** puis sélectionnez l'interface à laquelle appliquer le relai (le **LAN**). Dans **Destination Server**, renseignez l'IP du futur serveur DHCP (ici, **10.1.10.1**). Cliquez ensuite sur **Add server** et sauvegardez.

La configuration de notre routeur étant terminée, nous pouvons nous occuper du contrôleur de domaine.

## II. Installation du contrôleur de domaine

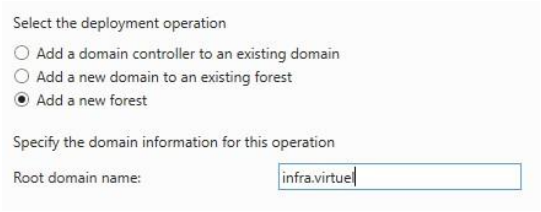
### 1. Installation des rôles de départ

Commençons par installer les rôles nécessaires à la naissance de notre infrastructure :




La première étape à réaliser pour la mise en place de DC1 est l'installation des rôles et fonctionnalités nécessaires à la mise en place de l'infrastructure. Il donc installer les rôles suivants : **Active Directory Domain Service** (ADDS), **serveur DNS** et **serveur DHCP**.

Ensuite, il faut promouvoir le serveur en contrôleur de domaine. Pour cela, cliquez sur l'icône en forme de drapeau en haut à droite, puis sur **Promouvoir ce poste en contrôleur de domaine**.

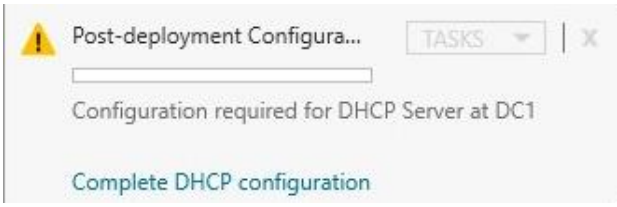



Ensuite, **créez une nouvelle forêt** et saisissez le nom de domaine racine : **infra.virtuel.**

Puis faites **suivant** jusqu'à l'installation finale.

## 2. Configuration du rôle DHCP

Les options BootDHCP et BootFileName nous seront utile afin de pouvoir démarrer sur PXE lors des tests de master. Pour cela, nous avons besoin d'un DHCP fonctionnel.




Une fois le rôle DHCP installé, cliquez sur le drapeau, puis sur **Terminer la configuration DHCP**.

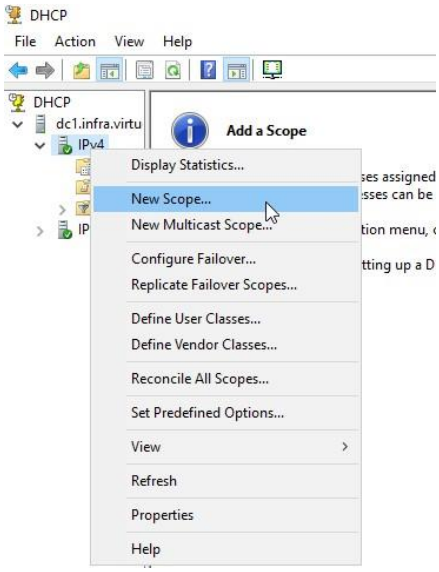
Suivez les indications à l'écran et validez.

### *a. Création de l'étendue unique*

Voici les caractéristiques de la seule étendue que nous devrons créer :

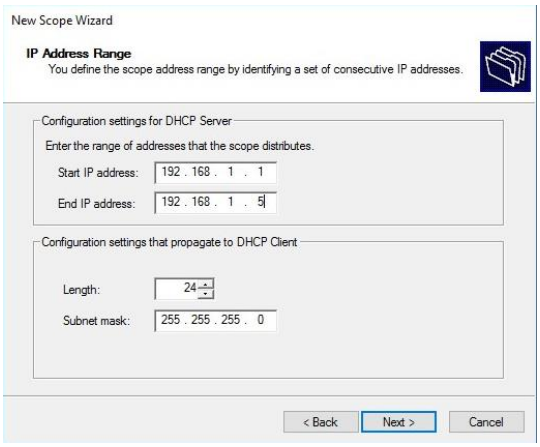
| | |
|---|---|
| **RANGE D'ADRESSES IPV4** | 192.168.1.1 – 192.168.1.5 |
| **MASQUE** | 255.255.255.0 |
| **PASSERELLE PAR DEFAUT** | 192.168.1.254 |
| **SERVEUR DNS** | 10.1.10.1 |
| **BOOT SERVER HOST NAME** | SCCMPS.infra.virtuel |
| **BOOT FILE NAME** | SMSBoot\x64\pxeboot.n12 |

Accédez à la configuration de l'outil DHCP.

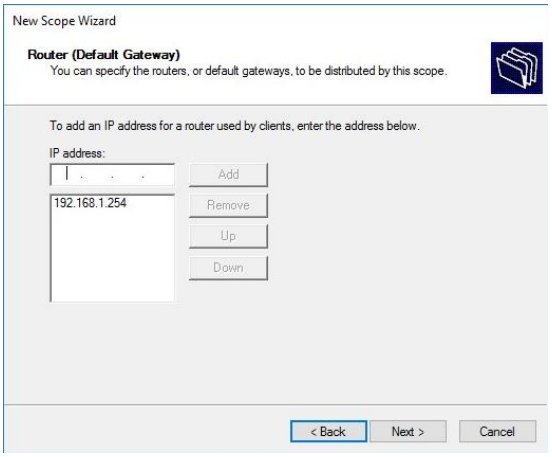



Développez **dc1.infra.virtuel,** faites clic droit sur **IPv4**, et cliquez sur **Nouvelle étendue.**

Entrez un nom permettant d'identifier rapidement l'étendue, si vous souhaitez en créer plusieurs.




Dans le champ **Adresse IP de début**, saisissez **192.168.1.1** ; dans le champ **Adresse IP de fin**, saisissez **192.168.1.5**. Validez les paramètres en vérifiant que la longueur du masque est de **24**. Faites **suivant** jusqu'à arriver à la configuration de la passerelle par défaut.




Dans le champ **adresse IP**, saisissez l'adresse de la passerelle par défaut des postes de test : **192.168.1.254**.

Dans la fenêtre suivante, vérifiez que le domaine parent est bien infra.virtuel, et que l'adresse de DNS déployée est celle de votre serveur DNS (soit ici : 10.1.10.1).
Faites suivant jusqu'à terminer la configuration.

Toujours dans **l'outil DHCP**, section **Options d'étendues**, faites clic droit > **Configurer les options** pour chaque élément ci-dessous :

| Option | Name | Value |
|---|---|---|
| **003** | Router | 192.168.1.254 |
| **066** | Boot Server Host Name | SCCMPS.infra.virtuel |
| **067** | Bootfile Name | SMSBoot\x64\pxeboot.n12 |

On obtient finalement cette configuration :

| Option Name | Vendor | Value |
|---|---|---|
| 003 Router | Standard | 192.168.1.254 |
| 006 DNS Servers | Standard | 10.1.10.1 |
| 015 DNS Domain Name | Standard | infra.virtuel |
| 066 Boot Server Host Name | Standard | SCCMPS.infra.virtuel |
| 067 Bootfile Name | Standard | SMSBoot\x64\pxeboot.n12 |

### b. *Vérification du bon fonctionnement du DHCP*

Afin de vérifier qu'un client récupère bien la configuration mis en place précédemment, nous pouvons utiliser l'hôte virtuel ou une autre machine virtuelle (sur Windows 7 ou 10). **Attention : il faut que le poste utilisé soit intégré au domaine infra.virtuel, qu'il soit sur le réseau 192.168.1.0/24 et que sa configuration IPv4 soit réglée sur la récupération automatique d'adresses IP.**

## 3. Extension du schéma Active Directory

Nous allons désormais voire comment étendre le schéma Active Directory ; c'est notamment ce qui permettra aux clients de localiser serveurs & ressources lors de déploiements. Pour cela, nous devrons exécuter l'utilitaire **extadsch.exe**, qui se trouve dans le disque d'installation d'SCCM. **Attention : il faut être membre du groupe « Administrateurs du schéma » pour pouvoir utiliser cet outil.**

Insérez le disque d'installation d'SCCM (sur VirtualBox, nous pouvons aller dans **Périphériques > Disques Optiques > Choose/Create a disk image…,** puis sélectionner le .iso d'SCCM.) Ouvrez un invité de commande en Administrateur, placez-vous sur le disque d'SCCM inséré, et entrez **\SMSSETUP\BIN\X64\extadsch.exe** :

```
C:\Users\Administrator>D:

D:\>\SMSSETUP\BIN\X64\extadsch.exe

Microsoft System Center Configuration Manager v5.00 (Build 8634)
Copyright (C) 2011 Microsoft Corp.


Successfully extended the Active Directory schema.

Please refer to the ConfigMgr documentation for instructions on the manual configuration of access rights in active directory
 which may still need to be performed.  (Although the AD schema has now be extended, AD must be configured to allow each Conf
igMgr Site security rights to publish in each of their domains.)

D:\>_
```

Si vous souhaitez vérifier que le schéma est bien étendu et avoir des informations sur les opérations effectuées, vous pouvez consulter le fichier de log **C:\ExtADSch.log.**

## 4. Création des comptes utilisateurs et groupes

Dans cette partie, nous verrons comment créer des utilisateurs finaux (cad ceux qui nécessitent l'installation d'un logiciel sur leurs postes, et qui ne possèdent aucun droits), des utilisateurs administrateurs du parc (ayant les droits administrateurs sur l'ensemble des postes, et des droits restreints sur SCCM), ainsi que des utilisateurs administrateurs SCCM (ayant les droits complets sur SCCM). Ces comptes serviront à simuler un environnement de production.

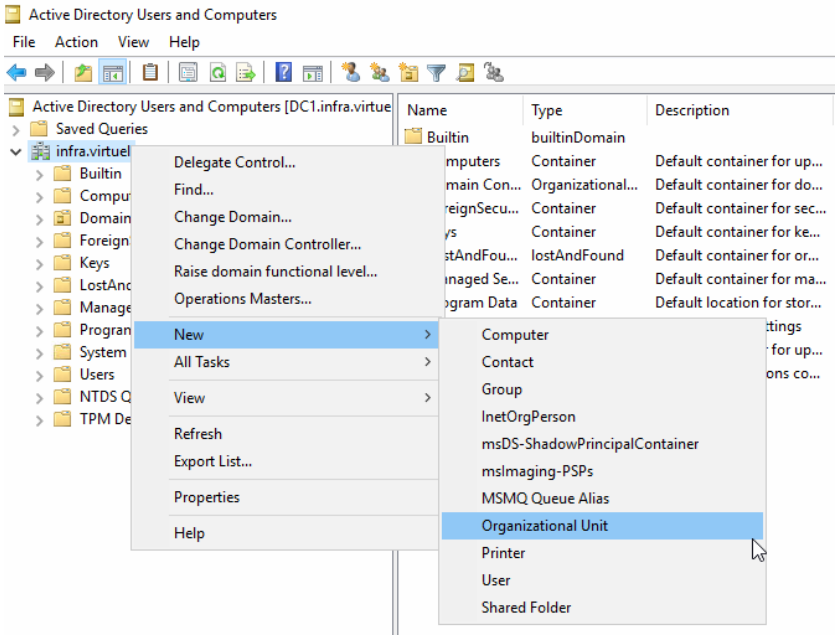
Le tableau suivant résume les comptes et groupes créés pour notre maquette virtuelle :

| Nom du groupe | Description du groupe | Utilisateurs |
|---|---|---|
| **Infra_admins_parc** | Administrateur du parc | John Doe (j.doe@infra.local)<br>Eric Untel (e.untel@infra.local)<br>SCCM2020 (sccm2020@infra.local) |
| **Infra_admins_SCCM** | Administrateur d'SCCM, compte de service | SCCM2020 (sccm2020@infra.local) |
| **Infra_users_SCCM** | Utilisateur SCCM aux droits restreints | Eric Untel (e.untel@infra.local) |
| **-** | Utilisateur final | Pierre Dupont (p.dupont@infra.local) |

Les comptes précédents, sauf SCCM2020, seront placés dans une Unité d'Organisation (UO) à part nommée par exemple **Siège**.

### *a. Création des UOs*

Ici, nous verrons comment créer une UO appelée **Siège**. Elle sera créée à la racine de l'AD. Vous pouvez également consulter les annexes pour découvrir quelles commandes PowerShell permettent de créer des UO.



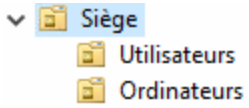

Pour cela, sur DC1, dans **Utilisateurs et groupes Active Directory**, faites clic droit sur **infra.virtuel > Nouveau > Unité d'organisation.**

Dans la fenêtre qui s'ouvre, saisissez comme nom **Siège** et faites **OK**.

Ensuite placez-vous sur Siège, et créez la sous-UO **Ordinateurs** de la même manière que vous avez créé **Siège**. Nous y mettrons les postes de travail, afin de leur attribuer des stratégies de groupe.

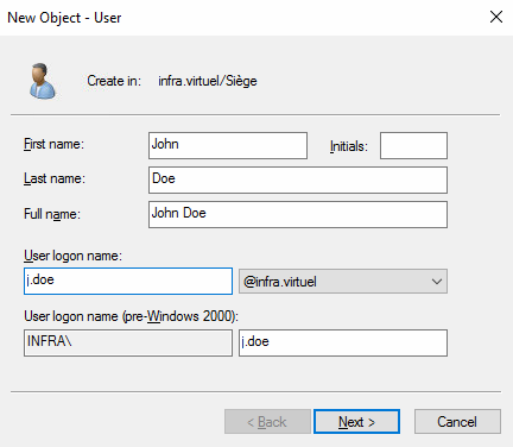
Puis toujours dans **Siège**, créez une nouvelle sous-UO appelée **Utilisateurs**. Nous y mettrons donc nos utilisateurs, afin de leur attribuer des groupes de sécurité.

Vous devriez obtenir l'architecture suivante :




### *b. Création des utilisateurs*

Nous verrons ici comment créer les utilisateurs John Doe, Éric Untel et Pierre Dupont. Vous trouverez en annexes les commandes PowerShell permettant de créer des utilisateurs. Toujours dans **Utilisateurs et groupes Active Directory**, faîtes un clic droit sur **Siège > Utilisateurs > Nouveau > Utilisateur.**




Dans **Prénom** mettez John, dans **Nom** mettez Doe. Dans **Nom d'ouverture de session de l'utilisateur**, mettez j.doe ; faites **Suivant**.

Dans la fenêtre suivante, définissez-lui un mot de passe. **Attention : dans le cadre de notre maquette, nous cocherons la case Le mot de passe n'expire jamais, mais ce n'est pas à reproduire en environnement réel.**

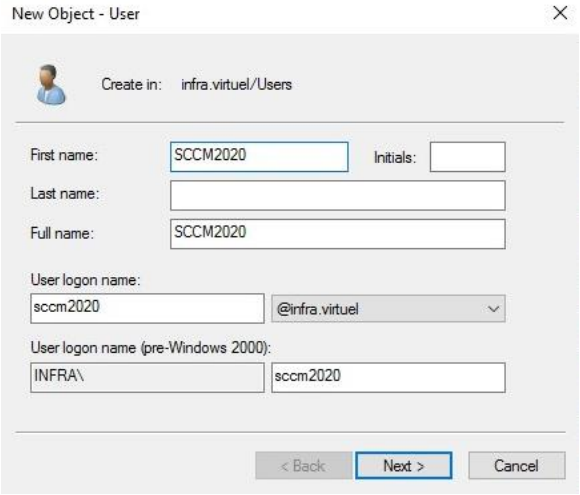
Faîtes **Suivant** puis **Terminer.**

Les opérations précédentes sont à réitérer pour chaque utilisateur (sauf SCCM2020).

### *c. Création d'un utilisateur système : SQL et SCCM*

Nous allons créer un utilisateur dédié au lancement du service SQL Server, ou plutôt un utilisateur identique pour SQL Server et SCCM. Libre à vous de faire un ou deux utilisateurs. Ainsi, cet utilisateur fera partie du groupe **Infra_admins_SCCM** et sera créé dans l'UO préexistante « **Utilisateurs**» (à ne pas confondre avec l'UO **Utilisateurs** que nous venons de créer).

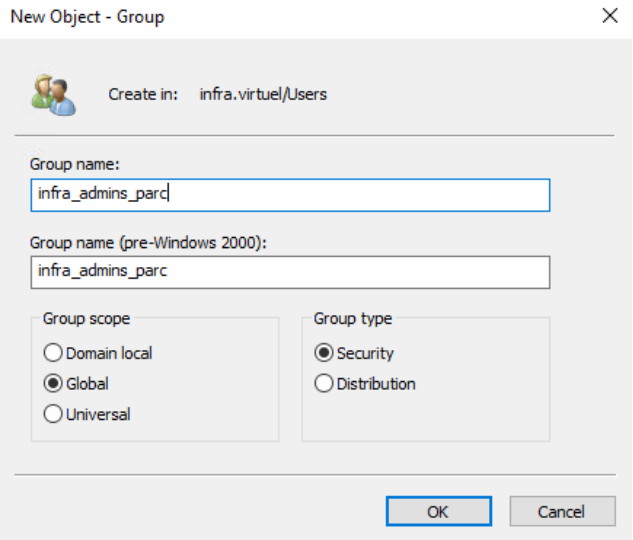
**Note : Microsoft recommande de ne pas utiliser de comptes locaux pour les comptes de service, mais plutôt de s'orienter vers un compte dans l'annuaire.**




Dans **Utilisateurs et groupes Active Directory > infra.virtuel > Users**, faites clic droit **> Nouveau… > Utilisateur**. Saisissez par exemple SCCM2020, faites **Suivant**, définissez un mot de passe et terminez.

### *d. Création des groupes de sécurité et affectations*

Ici, nous allons créer des groupes de sécurité permettant la délégation de certains droits à nos utilisateurs. Vous trouverez en annexe les commandes PowerShell permettant ces opérations.




Faites clic droit sur l'UO Préexistante **Utilisateurs > Nouveau > Groupe.** Dans le champ **Nom du groupe,** saisissez **Infra_admins_parc.** Vérifiez bien que le type de groupe est sur **Sécurité.** Faites **Suivant.**

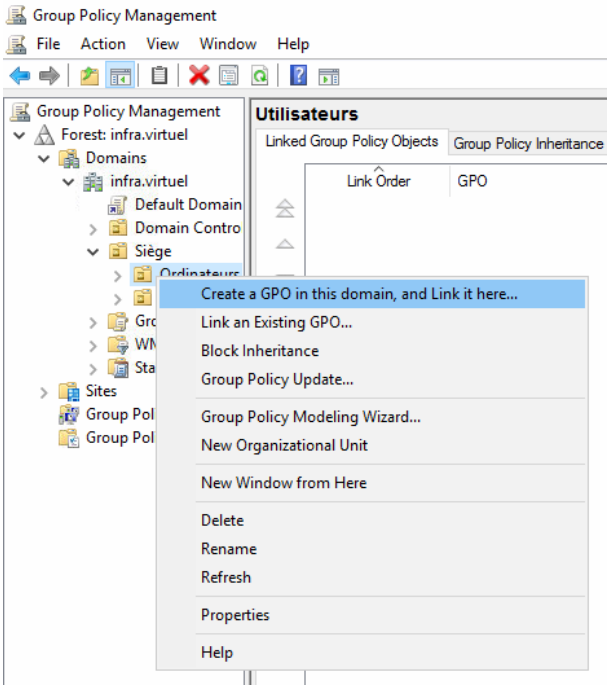
Réitérez les opérations pour les groupes **Infra_admins_SCCM** et **Infra_users_SCCM.**

Ensuite rendez-vous dans Siège > Utilisateurs, puis chaque utilisateur faites clic-droit > Ajouter à un groupe… et saisissez les noms des groupes respectifs.

## 5. Délégation des droits

Dans cette dernière sous-partie nous verrons comment créer des stratégies de groupe permettant la délégation de droits d'administration, aux groupes que nous avons créés précédemment. Pour rappel : une stratégie de groupe Ordinateur est une collection de paramètres à définir, s'appliquant au démarrage d'un poste.

### *a. Administration du parc via stratégies de groupe*

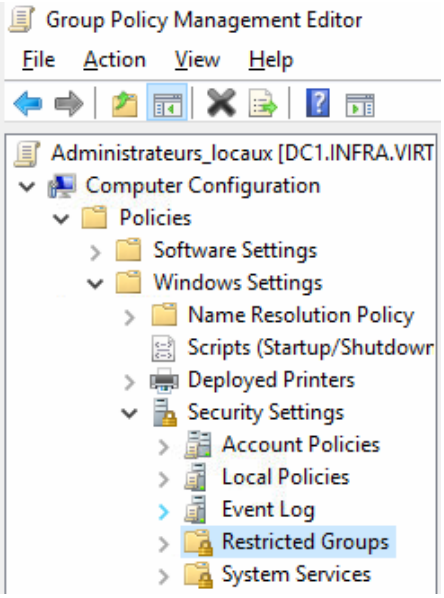



Nous verrons ici quelle stratégie de groupe mettre en place pour déléguer l'administration du parc à, par exemple, un technicien faisant partie du groupe **Infra_admins_parc**.

Rendez-vous dans le **Gestionnaire de stratégies de groupe** et développez **forêt : infra.virtuel > Domains > infra.virtuel > Siège, puis faites clic-droit sur Ordinateurs > Créer un objet GPO dans ce domaine, et le lier ici...**.

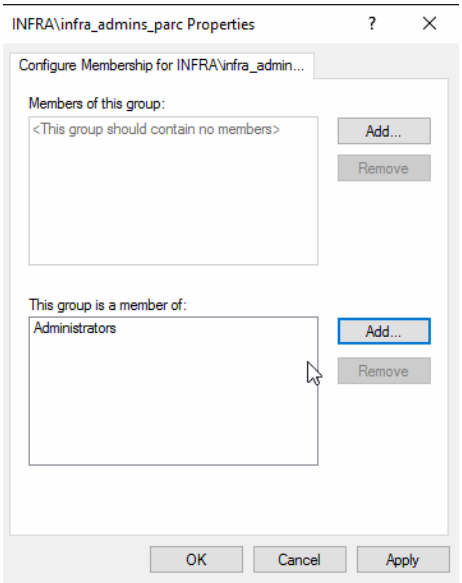
Une fenêtre s'ouvre vous demander de nommer la stratégie de groupe. On peut la nommer par exemple **Administrateurs_locaux**.

Une fois la GPO créée, faites clic droit dessus **> Modifier**.




Accédez à **Configuration Ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Accès restreints.**

Faites-y clic droit **> Ajouter un groupe…** et saisissez **INFRA\Infra_admins_parc.**




Dans le champ **Ce groupe est membre de**, cliquez sur **Ajouter**, puis entrez **Administrateurs**. Laissez le premier champ vide.

Faites **OK**.

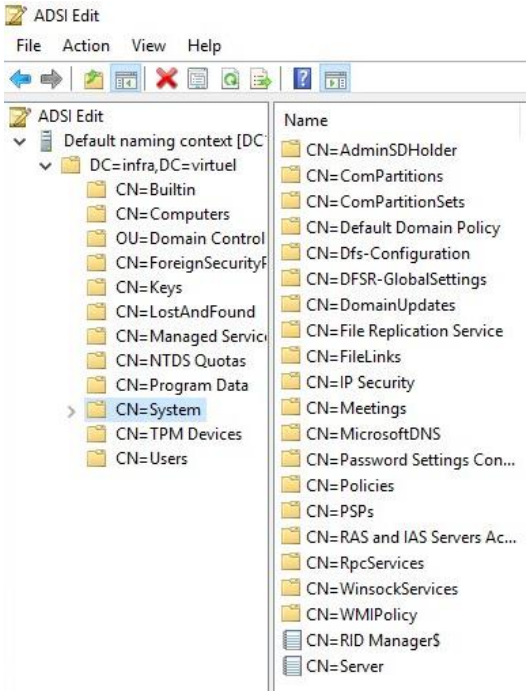
Nous venons de donner les droits Administrateurs à tous les membres du groupe **Infra_admins_parc** (soit John Doe et Eric Untel) sur tous les postes de l'UO **Siège\Ordinateurs**.

### *b. Administration d'SCCM*

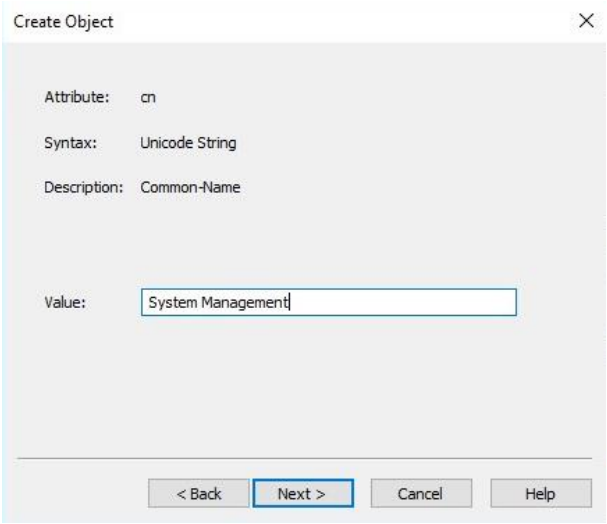
Ici, nous verrons comment créer un container dédié à SCCM et lui déléguer des tâches précises.
**Attention : le serveur SCCMPS doit être sous-tension, avoir son IP configurée et intégré au domaine. Cependant, inutile de lui attribuer de rôles pour le moment.**

- Création du container

Cela se fait dans l'outils **ADSI Edit**, sur **DC1.**



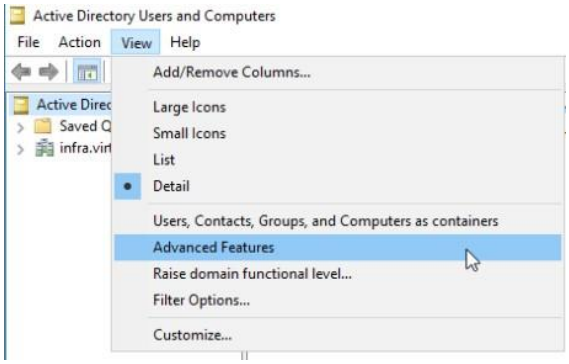

Une fois dans l'outil, faites clic droit > **Se connecter à …** > **OK**. Développez **Default naming context** et sélectionnez le container **Système.**



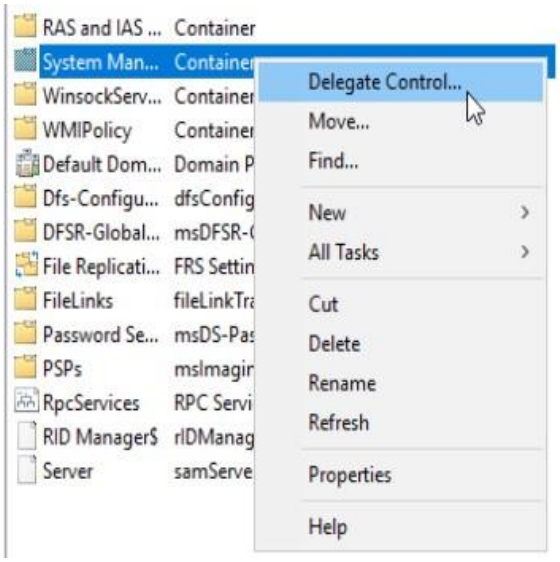

Faites donc clic droit dans ce dossier, **Créer**, **container** ; dans le champ **Value**, entrez **System Management**, faites **Suivant** et **Terminer**.

- Délégation de contrôle

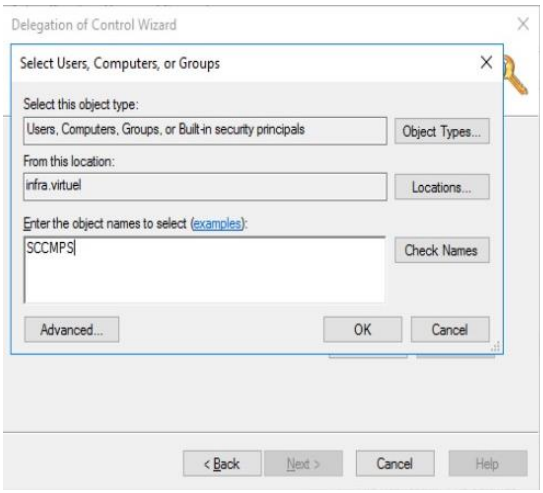
Nous pouvons maintenant déléguer la gestion du container à notre serveur SCCM et ses Administrateurs. Pour cela, rendez-vous dans **Utilisateurs et groupes Active Directory**.




Dans l'onglet **Affichage**, cliquez sur **Fonctionnalités avancées** ; cela nous permettra d'afficher les containers cachés par défaut, dont celui que l'on vient de créer.



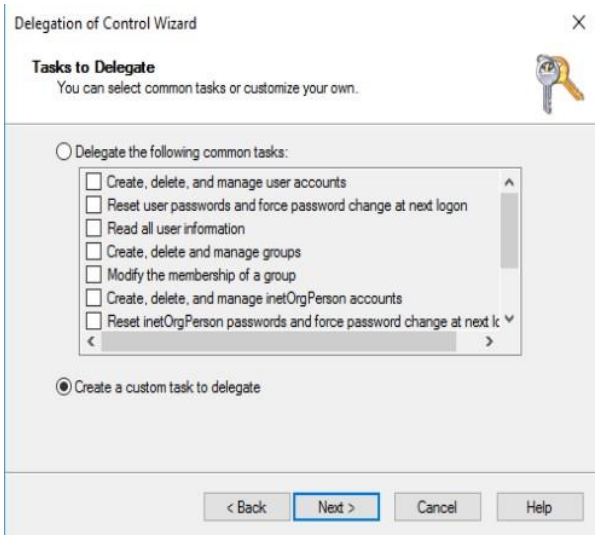

Vous devriez donc retrouver notre container **System Management** sous **infra.virtuel > System**. Faites un clic droit dessus **> Délégation de contrôle**…




Cliquez ensuite sur **Suivant** puis **Ajouter** ; dans **Types d'objets**, cochez la case **Ordinateurs** ; entrez le nom de votre serveur SCCM (ici, **SCCMPS**) et faites **OK**.

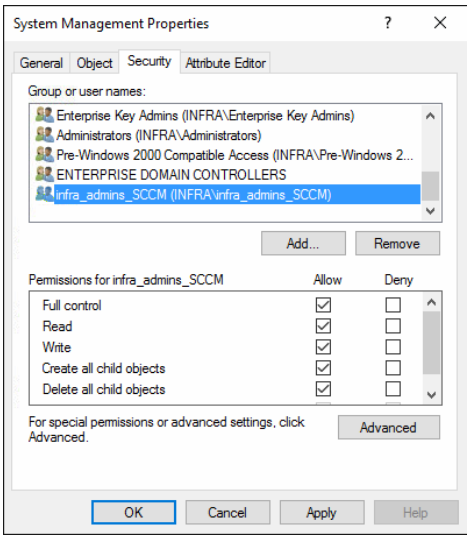
Réitérez avec le groupe **Infra_admins_SCCM**.

Votre serveur apparaît dans la liste des utilisateurs et groupes sélectionnés ; faites **Suivant**.




Maintenant nous allons pouvoir définir quelles tâches déléguer à **SCCMPS** et ses administrateurs ; cochez **Créer une tâche personnalisée** et faites **Suivant**, **Suivant**, cochez toutes les cases, puis **Suivant** jusqu'à **Terminer**.

Enfin, faites clic droit **> Propriétés** sur le container **System Management**.




Dans l'onglet **Sécurité**, vérifiez bien que SCCMPS a le contrôle total du container. Ajoutez également le groupe **Infra_admins_SCCM** en contrôle total, puis faites **OK**.

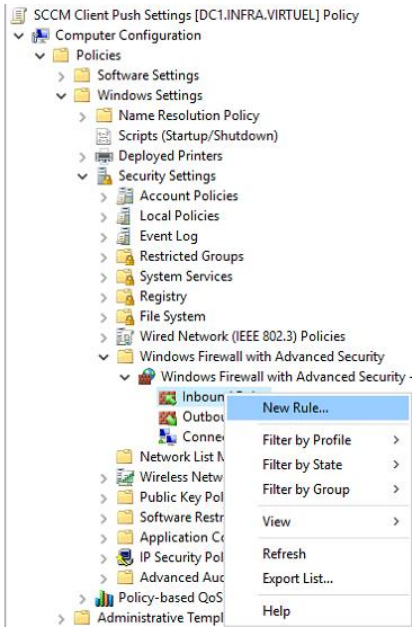
Vous venez de déléguer le contrôle total du container System Management à votre serveur SCCMPS et ses administrateurs.

## 6. Configuration du Pare-Feu par GPO

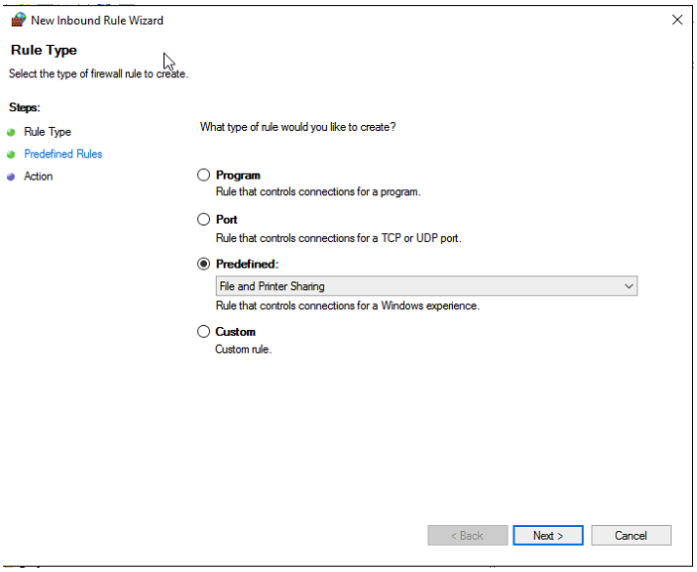
SCCM étant un système client/serveur, il est indispensable de mettre en place des règles de Pare-feu autorisant les communications entre le serveur et ses clients. Consultez l'article Docs.Microsoft "**Windows Firewall and Port Settings for Client Computers in Configuration Manager**" pour en savoir plus sur les ports utilisés par SCCM.

### *a. Autorisation du partage de fichier et d'imprimante*

Nous allons voir comment créer une **GPO** qui nous permettra d'ouvrir automatiquement certains ports entrants et sortants. Ainsi nous ajouterons **le partage de fichiers et d'imprimante** en tant qu'exception. Rendez-vous dans le **Gestionnaire de stratégies de groupe** sur **DC1**. Faites un clic droit sur **intra.virtuel > Créer un objet de GPO dans ce domaine, et le lier ici…** Nommez-le par exemple **SCCM Client Push Settings.** Faites ensuite clic droit sur la GPO que vous venez de créer **> Modifier**.




Rendez-vous dans **Configuration de l'ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec fonctions avancées de sécurité** ; faites un clic droit sur **Règles de trafic entrant > Nouvelle règle…**

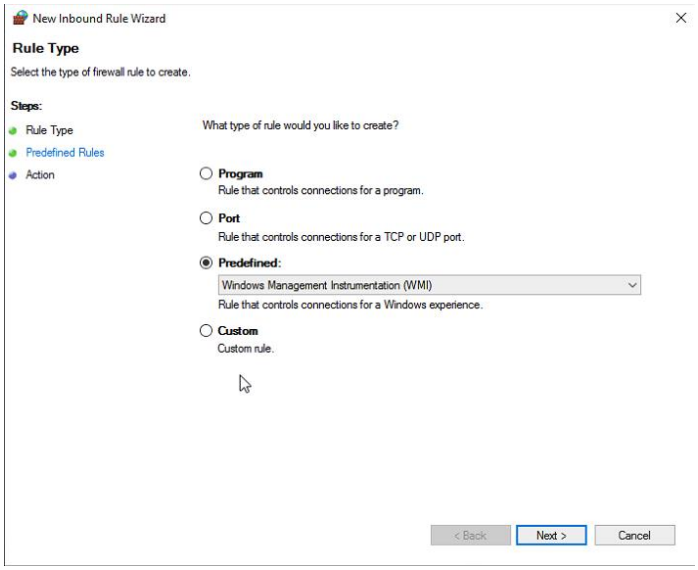



Cochez **Prédéfinies** et sélectionnez **Partage de fichiers et d'imprimantes**. Faites **Suivant**, **Suivant**, **Autoriser la connexion**, puis **Terminer**.

Réitérez les opérations précédentes avec une **Règle de trafic sortant**.

### *b. Autorisation de l'infrastructure de gestion Windows*

Nous allons maintenant créer une **Règle de trafic entrant** pour permettre aux services WMI de fonctionner correctement avec SCCM. Effectuez un clic droit sur **Règles de trafic entrant** et cliquez sur **Nouvelle règle…**



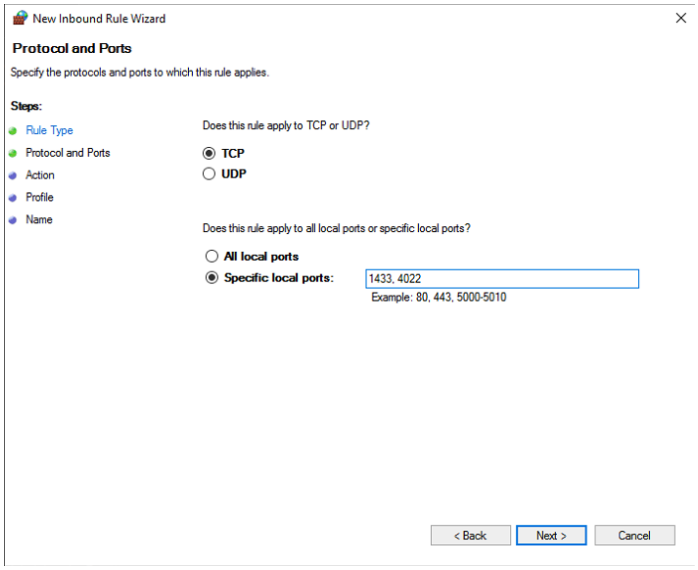

Cochez **Prédéfinies** et sélectionnez **Infrastructure de gestion Windows (WMI).** Faites **Suivant**, **Suivant**, **Autoriser la connexion**, puis **Terminer**.

Réitérez ces opérations avec une **Règle de trafic sortant**.

### *c. Ouverture de ports pour la réplication SQL*

Nous allons maintenant voir les étapes pour ouvrir les ports nécessaires pour la réplication SQL. Attention, SCCM ne prend pas en charge les ports dynamiques. Si vous ne souhaitez pas utiliser une instance SQL par défaut, mais une nouvelle, alors elle sera configurée pour utiliser des ports dynamiques pour la connexion au moteur de base de données. Vous devrez alors configurer manuellement le port en tant que port statique. Par défaut, sur Windows, le port **1433** est fermé pour empêcher les ordinateurs d'Internet de se connecter à une instance par défaut de SQL Server sur votre ordinateur. Nous allons donc maintenant créer une stratégie de groupe pour ouvrir les ports **TCP 1433** et **4022**

Ouvrez le **Gestionnaire de stratégie de groupe** et créez un nouvel objet GPO sur le domaine **infra.virtuel**. Nommez-le par exemple **Ports SQL SCCM**. Modifiez ensuite la stratégie, et créez une **Règle de trafic entrant**, cochez **Port** puis faites **Suivant**.




Cochez **TCP** puis **Ports locaux spécifiques**. Saisissez-y : **1433, 4022.** Faites **Suivant**, **Autoriser la connexion, Suivant,** et saisissez un nom de règle (par exemple, ALLOW PORTS 1433 + 4022). Faites **Terminer**.

Vous pouvez dès à présent lancer la commande **gpupdate /force** sur l'ensemble des machines de l'infrastructure, même les serveurs.

Nous en avons désormais fini avec la configuration du contrôleur de domaine.

# III. Préparation du serveur SCCM

## 1. Installation des rôles et fonctionnalités

Dans un premier temps, nous allons devoir installer via PowerShell le rôle **Serveur IIS**, ainsi que les fonctionnalités suivantes :

- **Transfert intelligent en arrière-plan (BITS)**
- **Compression différentielle à distance (RDC)**
- **.NET Framework 3.5 (obligatoire avec n'importe quelle version complémentaire)**
- **.NET Framework xx (la version est à vérifier selon votre OS. Ici, nous utiliserons la 4.6)**

Ouvrez donc un PowerShell en Administrateur sur le **SCCMPS** et saisissez les commandes suivantes :

➔ **Install-WindowsFeature -Name BITS , RDC**

➔ **Install-WindowsFeature -Name NET-Framework-Core , NET-Framework-46-Features**

➔ **Install-WindowsFeature -Name Web-Server , Web-Common-Http , Web-Static-Content , Web-Http-Errors , Web-Security , Web-Windows-Auth , Web-App-Dev , Web-Asp-Net, Web-Asp-Net46, Web-Net-Ext, Web-Net-Ext46, Web-ISAPI-Ext, Web-Mgmt-Compat, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Wmi, Web-Scripting-Tools -IncludeManagementTools**

Si elles échouent, essayez de faire l'installation manuellement (via le gestionnaire de serveur ou via le disque d'installation, dans *\sources\sxs*). Vous trouverez en annexe des commandes PowerShell avancées pour l'installation de rôles et de fonctionnalités.

La dernière commande installe le serveur web IIS, ainsi que sa console de gestion et tout un lot de fonctionnalités étant des prérequis de SCCM : Fonctionnalités HTTP communes (Contenu statique, document par défaut, erreurs HTTP), Sécurité (Authentification Windows), Développement d'applications (ASP.NET 3.5, ASP.NET 4.6, extensibilité .NET 3.5, extensibilité .NET 4.6, extensions ISAPI), Compatibilité avec la gestion IIS 6 (Console de Gestion IIS, compatibilité de métadonnées IIS 6, compatibilité avec le service WMI de IIS 6, scripts et outils de gestion IIS).

Si les installations se sont correctement déroulées, vous pouvez passer à la suite.

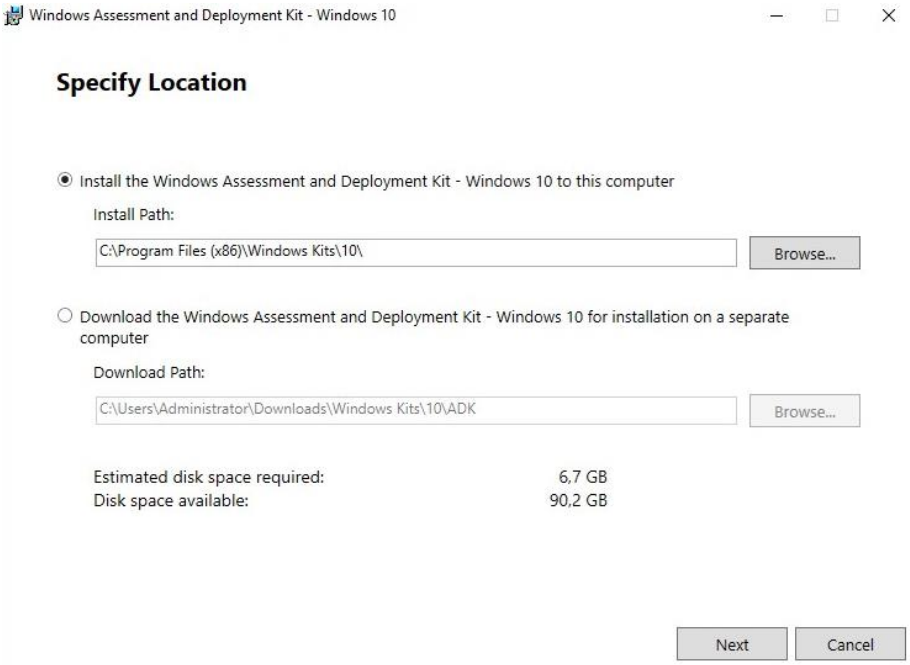
## 2. Installation du kit ADK Windows 10

Assessment and Deployement Kit est une suite d'outils et de technologies conçue par Microsoft pour faciliter le déploiement des images des systèmes d'exploitation sur des ordinateurs ou un disque virtuel de type VHD. **Ainsi, si vous souhaitez déployer une image de Windows 10 version 1809, vous devrez installer l'ADK de cette même version**. Pour notre infra virtuelle, nous utiliserons donc l'ADK de Windows 10 v.1809. Vous pourrez le trouver sur Internet.

Nous n'installerons pas toutes les fonctionnalités du kit mais seulement :

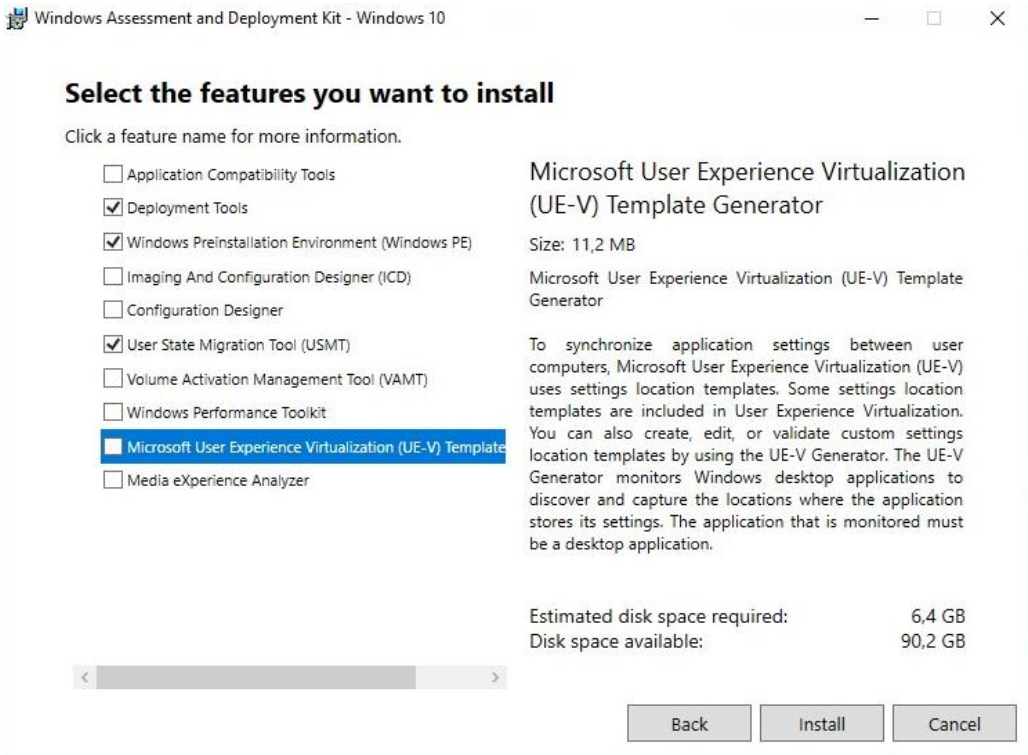
- **Outils de déploiement**
- **Environnement de pré-installation de Windows (Windows PE)**
- **Outil de migration utilisateur (USMT)**

Exécutez donc **adksetup.exe** en tant qu'Administrateur. Vous devriez vous retrouver sur cette page :




Vous avez donc le choix d'installer directement les fonctionnalités si elles sont présentes dans le package ou de télécharger l'intégralité du kit sur votre PC, afin de le réutiliser ultérieurement. Le choix est vôtre.

Acceptez le contrat de licence et cochez uniquement les cases des fonctionnalités qui nous intéresse :




La configuration de base de SCCMPS est terminée, nous pouvons maintenant attaquer SQL Server.

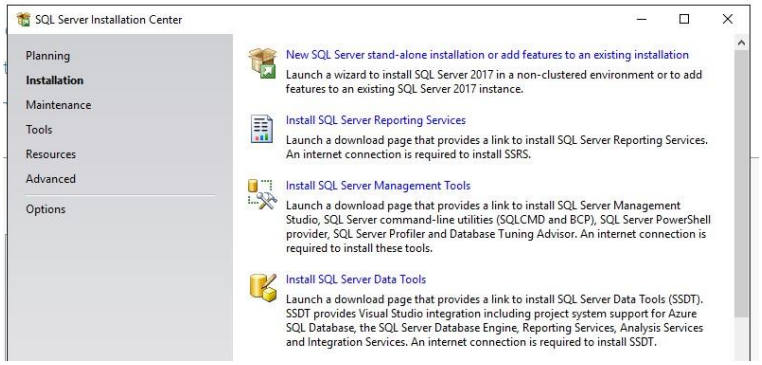
# IV. Mise en place de SQL Server

Pour stocker ses données, **System Center Configuration Manager** utilise une base de données via **SQL Server**, qui peut être installée sur le même serveur que le Site Primaire. Seulement en environnement réel, il vaut mieux isoler la base de données sur un serveur (physique ou VM) dédié à cela, notamment pour passer sur un cluster de serveurs SQL si le besoin s'en fait sentir par la suite ; tout dépend de vos besoins. De notre côté, l'installation de SQL Server 2014 sera effectuée sur SCCMPS.

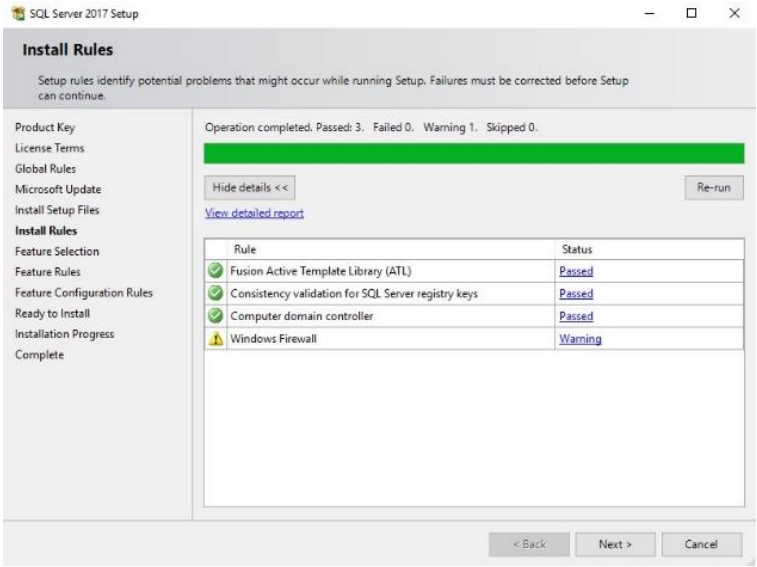
Téléchargez SQL Server 2017(version d'évaluation pour 180 jours). **Attention : vérifiez bien que le .NET Framework 3.5 est installé sur votre serveur avant d'installer SQL Server. Vérifiez également que la partition SQL est créée et fait au moins 70 Go.**

## 1. Installation de SQL Server

Insérez le disque d'installation (ou le .ISO) sur **SCCMPS** et lancez le **setup.exe**.




Sur le volet de gauche, allez dans **Installation** et cliquez sur **Nouvelle installation autonome SQL Server ou ajout de fonctionnalités à une installation existante.** Spécifiez ensuite si vous souhaitez utiliser une clef d'activation du produit, ou la version d'évaluation. Acceptez les termes de la licence.



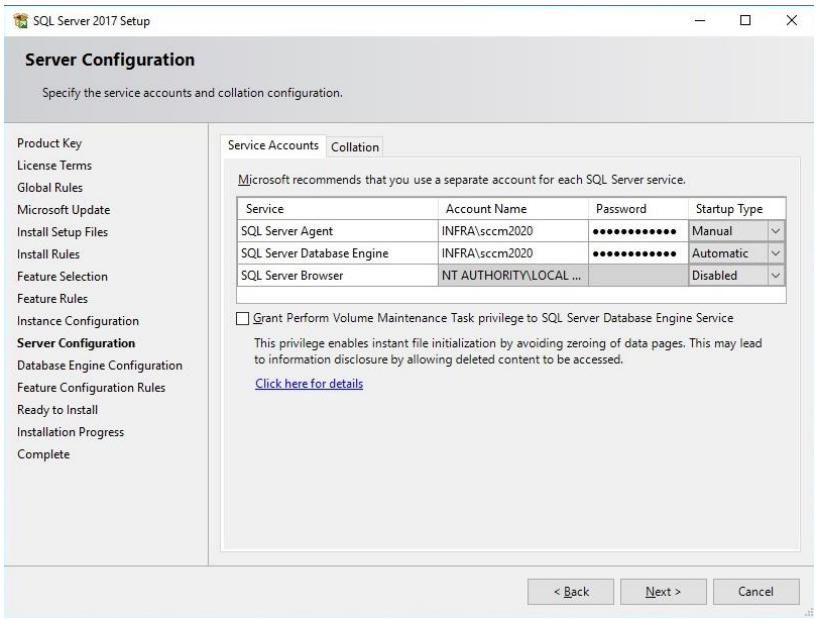

Cette fenêtre vous indique que le paramétrage est terminé ; Faites **Suivant**.

Dans la liste des fonctionnalités, cochez les suivantes (Si certaines fonctionnalités n'apparaissent pas dans la liste, vous pouvez les télécharger et les installer directement). :

- **Services Moteur de base de données**
- **Reporting Services – Natif**
- **Outils de gestion – Complet (SSMS)**

Cette sélection n'est pas définitive, vous pourrez y revenir plus tard si vous nécessaire, notamment si vous désirez utiliser le serveur SQL pour stocker la Database d'une autre application. Dans le **Répertoire racine de l'instance**, choisissez le répertoire de votre partition SQL. Faites **Suivant**.

Ensuite, vous pourrez définir un nom d'instance à SQL Server. Pour SCCM il est recommandé d'utiliser l'instance par défaut telle que la propose l'assistant, sinon des erreurs seront rencontrés pendant l'utilisation de System Center, à cause des ports dynamiques. Si vous souhaitez à tout prix utiliser une instance nommée, il vous faudra modifier la configuration des ports pour cette instance.




Ici, il faut spécifier le compte AD (et son mot de passe) qui va gérer les trois services affichés. Précédemment, nous en avons défini un spécialement pour cette occasion : **SCCM2020**. Dans **Nom de compte**, développez le menu et sélectionnez **Parcourir**. Dans la nouvelle fenêtre, entrez le compte **SCCM2020** et validez. Il faut que les **services Moteur de base de données SQL** et **SQL Server Reporting Services** soit en démarrage automatique. Dans l'onglet collation, mettez **SQL_Latin1_General_CP1_CI_AI.**

Dans la fenêtre suivante, laissez cochée **Mode d'Authentification Windows** et dans la rubrique **Administrateurs SQL Server**, cliquez sur **Ajouter.** Rentrez ensuite **Infra_admins_SCCM**, puis faites **Suivant** puis **Installer.** Consultez bien le résumé à la fin de l'installation pour vous assurer que tout s'est bien installé. Vous trouverez en annexes comment effectuer une sauvegarde d'une base SQL.

## 2. Installer SQL Server Management Studio (optionnel)

Selon les versions de SQL Server que vous installez, il se peut qu'SQL Server Management Studio (SSMS) ne soit pas inclut dans le package d'installation d'SQL Server. Pour résoudre ce problème, vous pouvez toujours télécharger SSMS depuis Internet, et faire l'installation manuellement. Une fois SSMS téléchargé, lancez le setup. Vous pouvez également saisir la commande suivante dans un invité en administrateur, en vous étant placé dans le répertoire où il se situe :

**ssms-setup-Enu.exe /quiet /log c:\logs\ssms2017_Install.log**

Cette commande permet de lancer le setup en mode silencieux et de générer un fichier log, afin de consulter les éventuelles erreurs lors de l'installation.

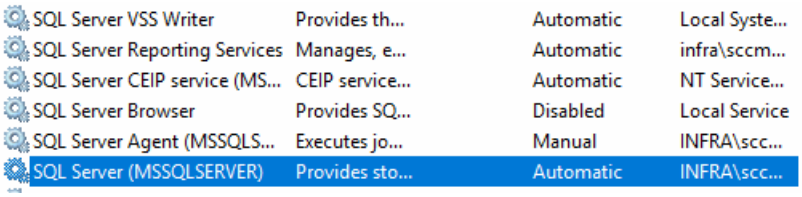
Ces indications fonctionnent également avec **SQL Server Reporting Service**, la commande étant adapter.

## 3. Paramétrages approfondis

Les étapes qui suivent consistent essentiellement à confirmer le bon paramétrage d'SQL Server, mais ne sont pas facultative pour autant.

### *a. Modifier la collation*

Il se peut que lors de son installation, SCCM vous alerte sur la collation utilisée par votre serveur SQL. En effet, SCCM nécessite la collation « **SQL_Latin1_General_CP1_CI_AS** ». Vous pouvez définir celle-ci lors de l'installation de SQL server, partie Configuration du Serveur, onglet Collation. Si vous ne l'avez pas fait, vous pouvez toujours changer cette collation. Rendez-vous dans les **Services**.




Stoppez tous les services **SQL Server** en cours d'exécution.

Ensuite, ouvrez un invité de commande en Administrateur, et placez-vous sur le dossier **Binn** de votre répertoire d'installation d'SQL Server (dans notre cas sur le disque E: ) :

```
cd "E:\SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn"
```

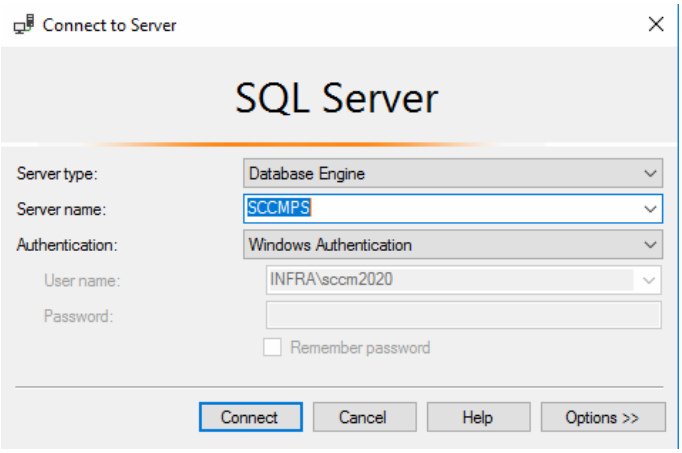
Puis lancez la commande suivante :

```
sqlservr -m -T4022 -T1433 -q"SQL_Latin1_General_CP1_CI_AI"
```

Vous pouvez ensuite relancer les services SQL Server et vérifier que dans SSMS, serveur **virtuel.infra > Général**, la collation soit **SQL_Latin1_General_CP1_CI_AI.**

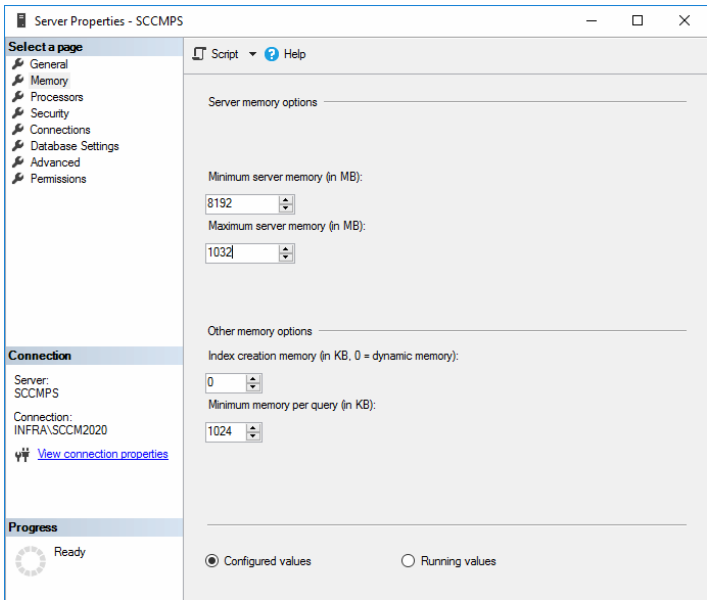
### *b. Modifier la mémoire RAM consommée par SQL Server*

Toujours sur SCCMPS, connectez-vous à la session SCCM2020 puis ouvrez **SQL Server Management Studio**. Si vous ne le trouvez pas, recherchez « ssms » via Cortana, et sélectionnez « Exécuter la commande ».




Ce pop-up s'affiche ; entrez le nom du serveur exécutant SQL server (ici SCCMPS), puis connectez-vous.

Une fois que la liste des serveurs de base de données s'affiche dans l'explorateur d'objets, faites un clic droit sur le nom du serveur **> Propriétés.**

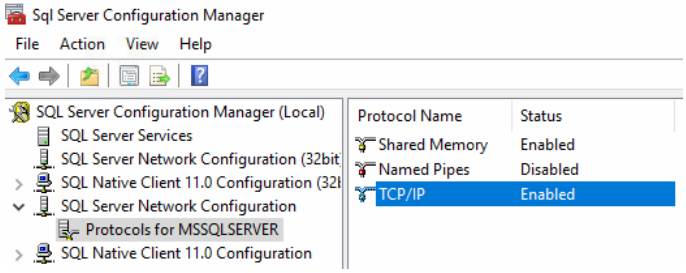



Dans l'onglet **Mémoire**, mettez par exemple *8192* dans la box **Mémoire minimale du serveur (en MB)** ; et *1032* à la mémoire maximale. Ainsi, SQL Server consommera uniquement de la mémoire RAM dans cet intervalle. SCCM nécessite qu'SQL puisse utiliser au moins 8 Go de RAM.

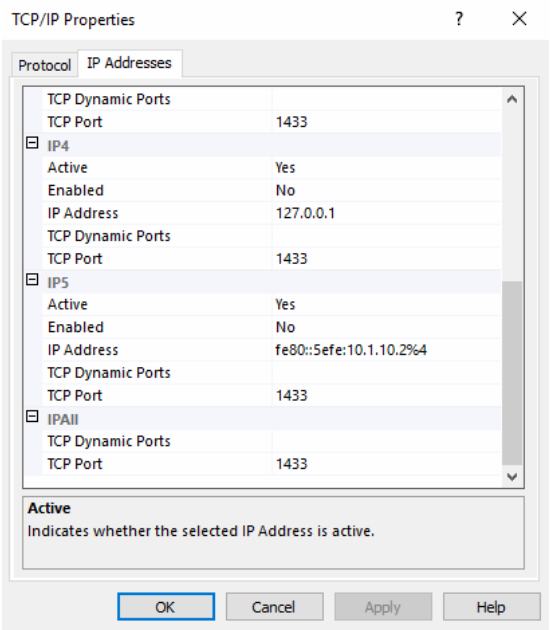
Bien-sûr, ce dernier est à adapter selon les capacités de votre machine exécutant SQL Server.

### *c. Configuration du port fixe 1433*

Toujours sur la session SCCM2020 sur SCCMMPS, ouvrez **SQL Server Configuration Manager (SSCM).**




Allez dans **SQL Server Network Configuration > Protocoles pour MSSQLSERVER > TCP/IP.**




Dans l'onglet **Adresses IP**, descendez complètement en bas de la fenêtre. Vérifiez bien que le champ **Ports dynamiques TCP** est vide, et que le champ **Port TCP** ait la valeur **1433**. Faites **OK**.

Si c'est bien le cas, laissez-les comme tel. Sinon modifiez-les de la sorte.

Ainsi, SQL Server n'utilisera pas de ports dynamiques lors de ses communications avec notre site primaire, mais le port fixe **1433**.

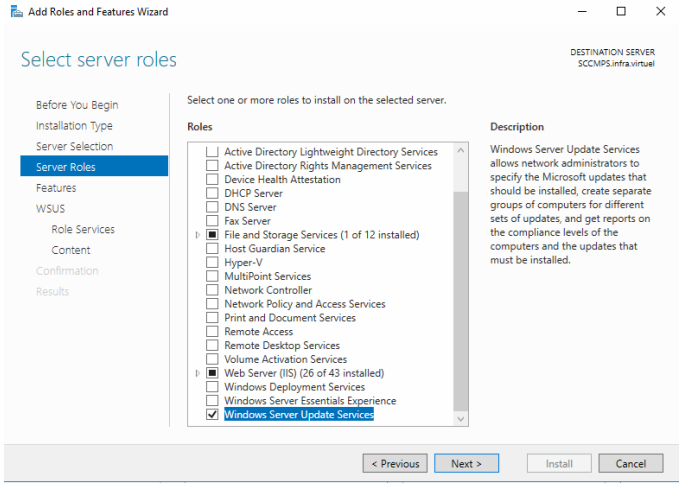
Nous pouvons attaquer la configuration du rôle WSUS.

## V. Installation du service de mise à jour

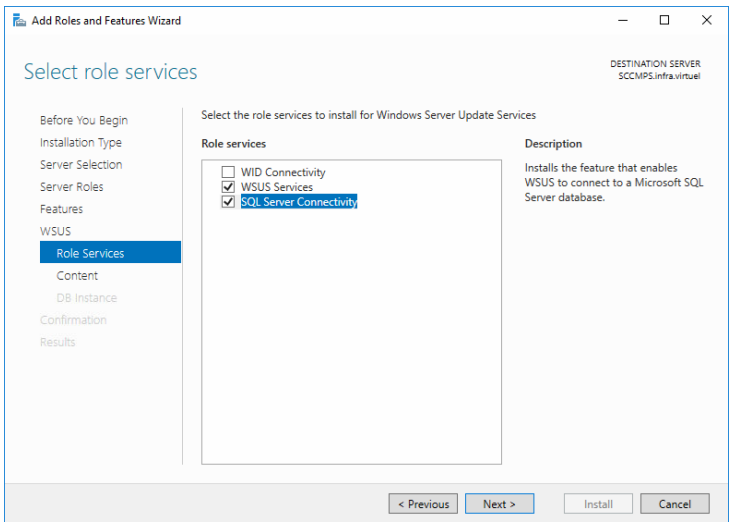
**Windows Server Update Services (WSUS)** est un service permettant de distribuer les mises à jour pour Windows et d'autres applications Microsoft sur les différents ordinateurs fonctionnant sous Windows au sein d'un parc informatique. WSUS est un rôle pour serveur Windows lui permettant ainsi de devenir un serveur de mises à jour local, en téléchargeant et stockant ponctuellement l'ensemble des mises à jour disponibles auprès des serveurs Windows Update de Microsoft, afin de rendre possible le contrôle de la diffusion de celles-ci dans le parc via, par exemple, SCCM.

Pour SCCM 2012 R2 il nécessaire d'installer au minimum **WSUS 3.0** Service Pack 2 car il ne supporte pas le 32 bits pour les sites SCCM. Il faut donc utiliser la version 64bits de WSUS.

Sur SCCMPS, rendez-vous dans l'Assistant de rôles et de fonctionnalités.




Dans l'onglet **Rôle**, sélectionnez **Services WSUS (Windows Server Updates Services).** Aucune fonctionnalité supplémentaire n'est nécessaire.

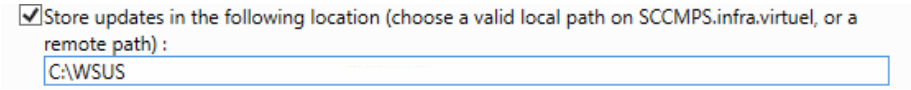



Faites **Suivant** jusqu'à arriver à l'onglet **Services de rôles**, et cochez **WSUS Services** et **Base de données.** Décochez **WID Connectivity** s'il est coché par défaut.

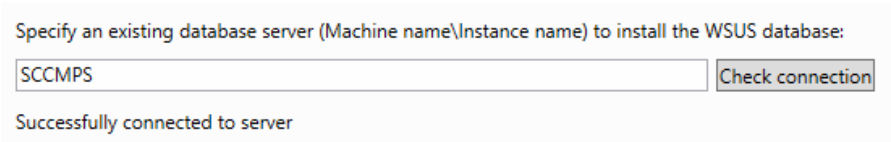
Faites **Suivant**.

La prochaine fenêtre vous demande le répertoire où vous souhaitez stocker les packages de mises à jour reçues. Vous avez même la possibilité de mettre un emplacement réseau.

Dans notre cas, nous indiquerons le chemin vers un dossier nommé *WSUS* créé préalablement à la racine du *C:* .



Ensuite, vous pourrez indiquer le nom de votre serveur de base de données (ici, **SCCMPS**) et cliquer sur **Vérifier la connexion** :




Vous pouvez ensuite faire **Suivant** jusqu'à lancer l'installation ; redémarrez le serveur.

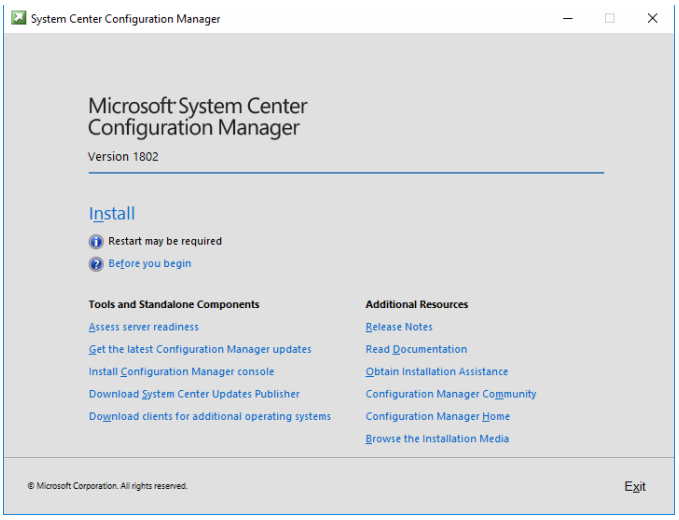
Lors de la première ouverture de la console WSUS, vous verrez **l'Assistant de configuration de Windows Server Update Services**. Cliquez sur **Annuler**. Il est maintenant préférable de tout gérer via SCCM, même si vous pouvez tout de même lancer la console WSUS pour vérifier l'état des mises à jour.

# VI. Mise en place du serveur SCCM

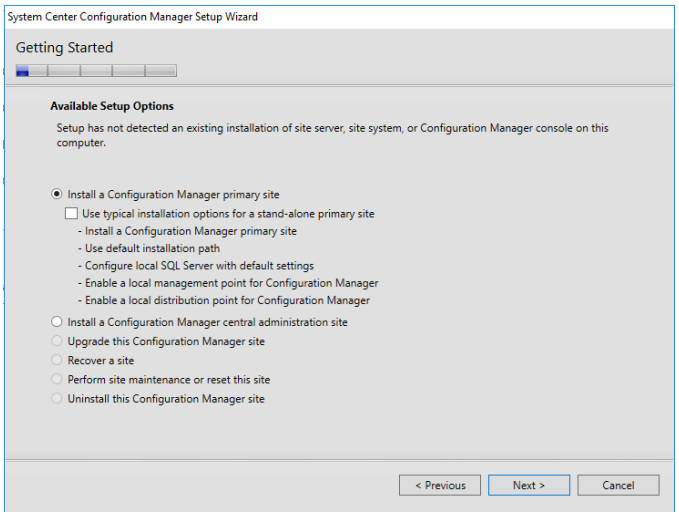
Notre infrastructure étant prête, nous pouvons nous atteler à l'installation d'SCCM. **Attention : Nous installerons ici la version 1802, qui n'est pas la plus récente.**

## 1. Installation du site primaire

Sur SCCMPS, insérez le disque d'SCCM et exécutez le setup. .

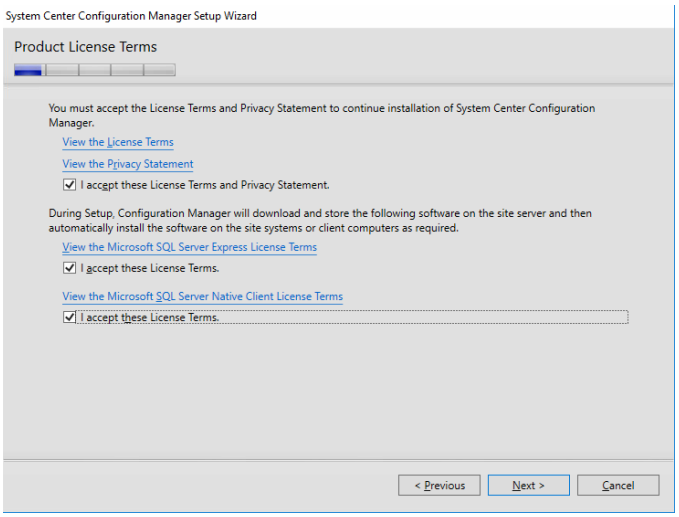



Cliquez sur **Obtenir les dernières mises à jour de Configuration manager** et définissez un chemin où seront disposés les fichiers. Vous aurez besoin d'une connexion à Internet. Ensuite, cliquez sur **Installer**. Sur la prochaine page, faites **Suivant**.



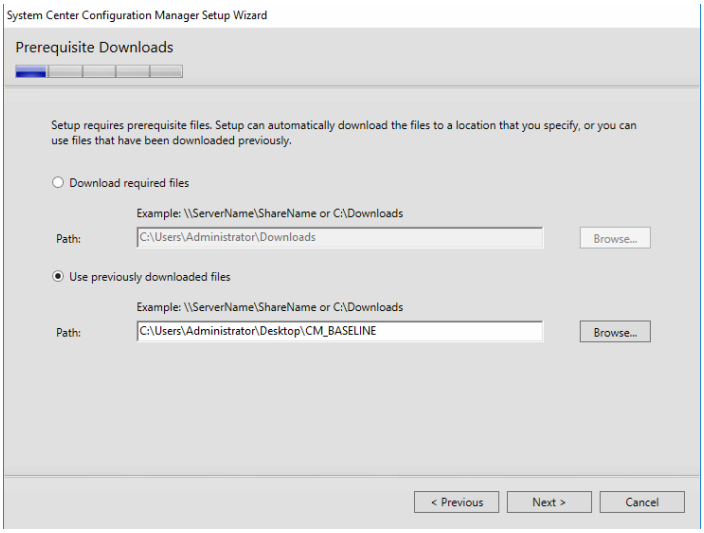

Vérifiez bien qu'Installer **un site principal Configuration Manager** est coché. Faites **Suivant**.

Entrez ensuite la clé de produit si vous avez acheté SCCM. Si vous souhaitez le tester, cliquez sur **Installer l'édition d'évaluation de ce produit.** Faites **Suivant**.



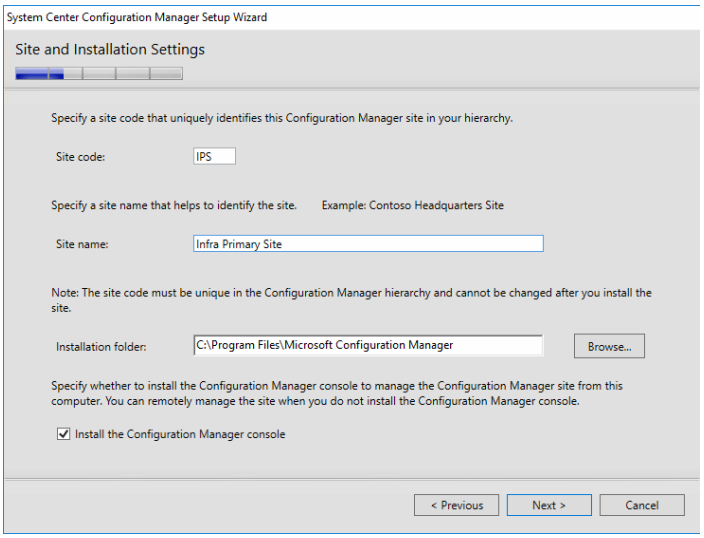

Cochez toutes les cases et faites **Suivant**.

Sur la prochaine page, le setup vous demande d'indiquer le répertoire où se situent les fichiers prérequis à l'installation. Il s'agit en fait de la Baseline de Configuration Manager (MECM), que vous avez télécharger lors de la première étape.




Cochez donc **Utiliser des fichiers précédemment téléchargés** et renseignez le chemin d'accès à ces derniers. Faites **Suivant**.

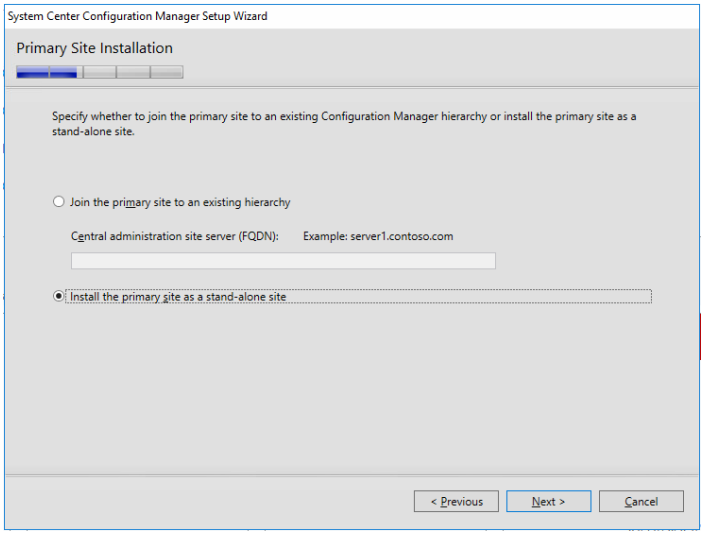
Sur les pages suivantes, sélectionnez les langues utilisées au sein de votre organisation pour le serveur, et pour les clients (ici nous n'utiliserons que le Français).



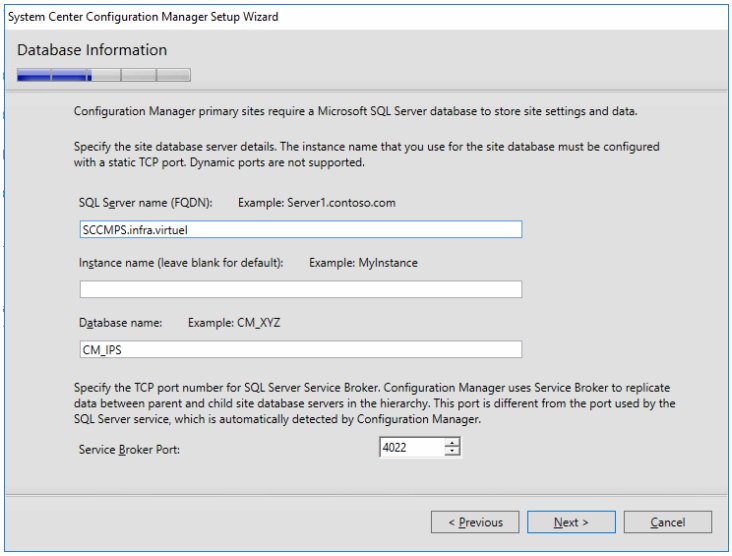

Spécifiez un code de site (ici : **IPS**), et un nom de site (ici : **Infra Primary Site**).

Cochez la case **Installer la console Configuration Management**.

Faites **Suivant**.




Si vous souhaitez rejoindre CAS déjà existant, choisissez **Joindre le site principal à une hiérarchie existante** ; vous devrez alors fournir le nom du serveur CAS complet pour pouvoir rejoindre la hiérarchie. **Attention : si vous envisagez de construire votre hiérarchie avec plus d'un site principal, vous devez installer un CAS en premier**. Sinon, si vous installez le site principal comme un site autonome alors choisissez la deuxième option. Faites **Suivant** .

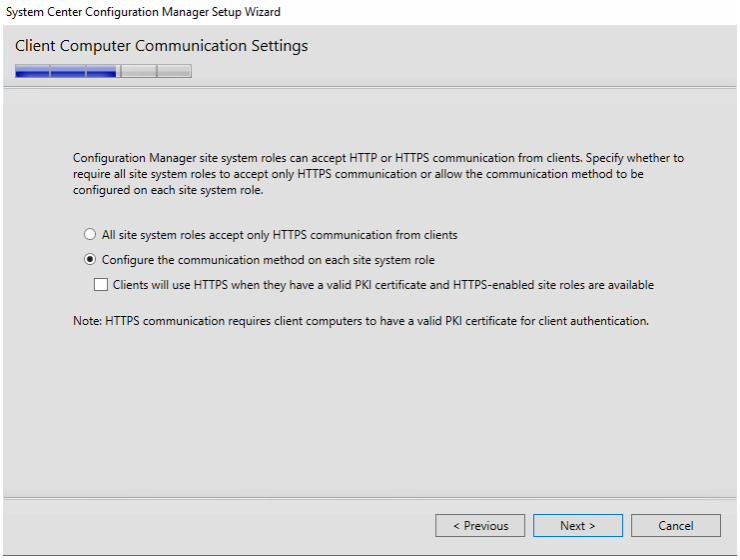



Dans le premier champ, saisissez le FQDN du serveur SQL (soit **SCCMPS.infra.virtuel**).

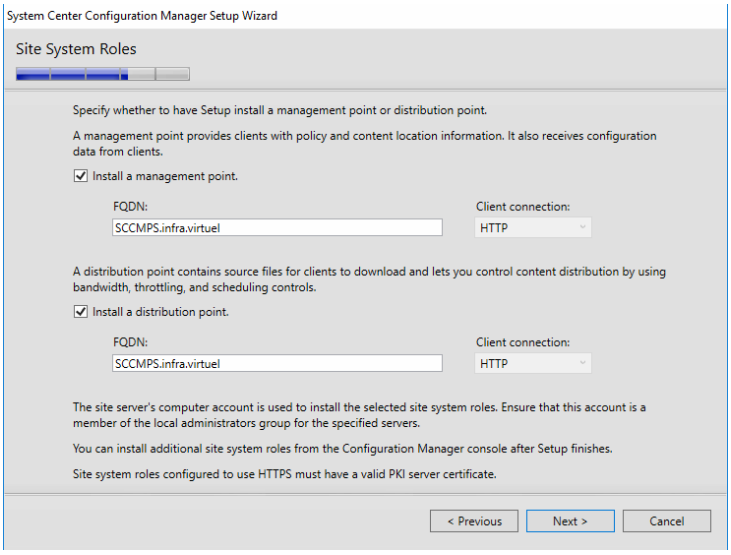
Vous pouvez laisser le champ **Nom d'instance** vide si vous avez fait le choix de laisser le nom d'instance d'SQL Server par défaut.

Pour terminer, donner un nom à votre base de données, vérifier que le port pour le **Service Broker** est le **4022** et cliquez sur **Suivant**.

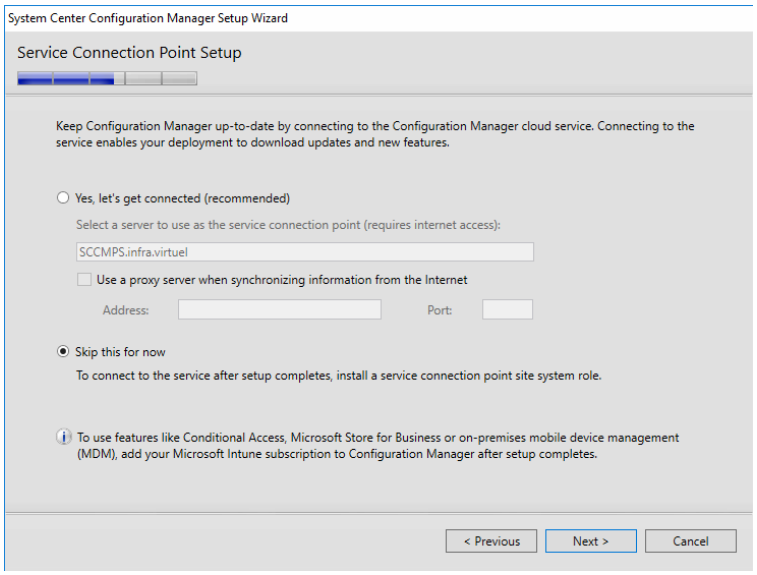
Sur la page suivante, gardez les répertoires par défaut (sauf si vous avez nommé votre instance d'SQL Server) et faites **Suivant**. Ensuite, spécifiez le serveur sur lequel sera installé le fournisseur SMS (dans notre cas, on laisse **SCCMPS.infra.virtuel** par défaut).




Cochez **Configurer la méthode de communication sur chaque rôle de système de site.** Ainsi, ce sera à vous de préciser si le protocole HTTPS sera utilisé pour les communications clients/serveurs. Faites **Suivant**.

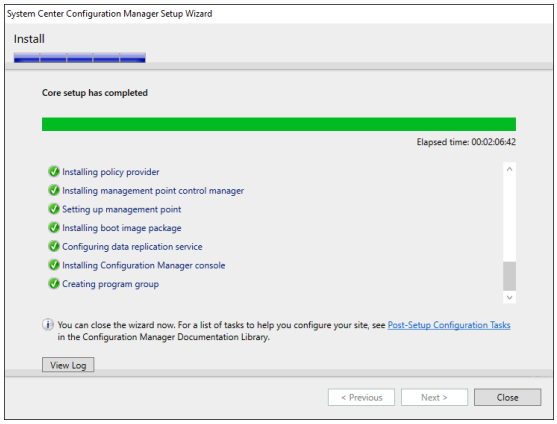



Cochez **Installer un point de gestion** et **Installer un point de distribution**. Vérifiez que le protocole de connexion utilisé est bien **http**, et que les FQDN renseignés correspondent à celui du serveur SCCMPS. Faites **Suivant**.

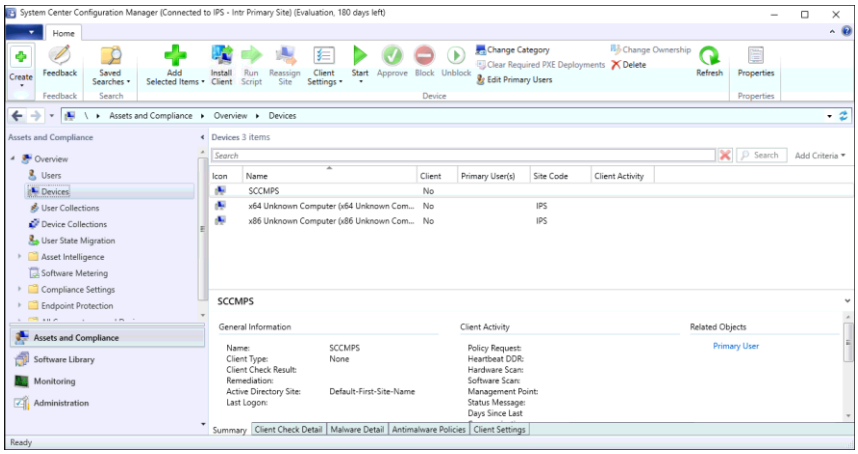



Cette page vous propose de permettre à votre serveur SCCM de télécharger automatiquement les mises à jour et fonctionnalités à partir d'Internet. Nous n'utiliserons donc pas cette fonctionnalité. Cochez **Passer pour le moment**, et faites **Suivant**.

Vous arrivez ensuite à un résumé des paramètres que vous avez renseigné précédemment. Vérifiez vos entrées et faites **Suivant**. L'installation d'SCCM commence ; le setup va d'abord vérifier si les prérequis sont bien en place, et vous indiquera si un problème a été détecté, en vous communiquant ses détails. Une fois ce checkup effectué, et que tout est ok, vous pouvez lancer l'installation.




L'installation est terminée ; vérifiez que tout est dans le vert et fermez la fenêtre.



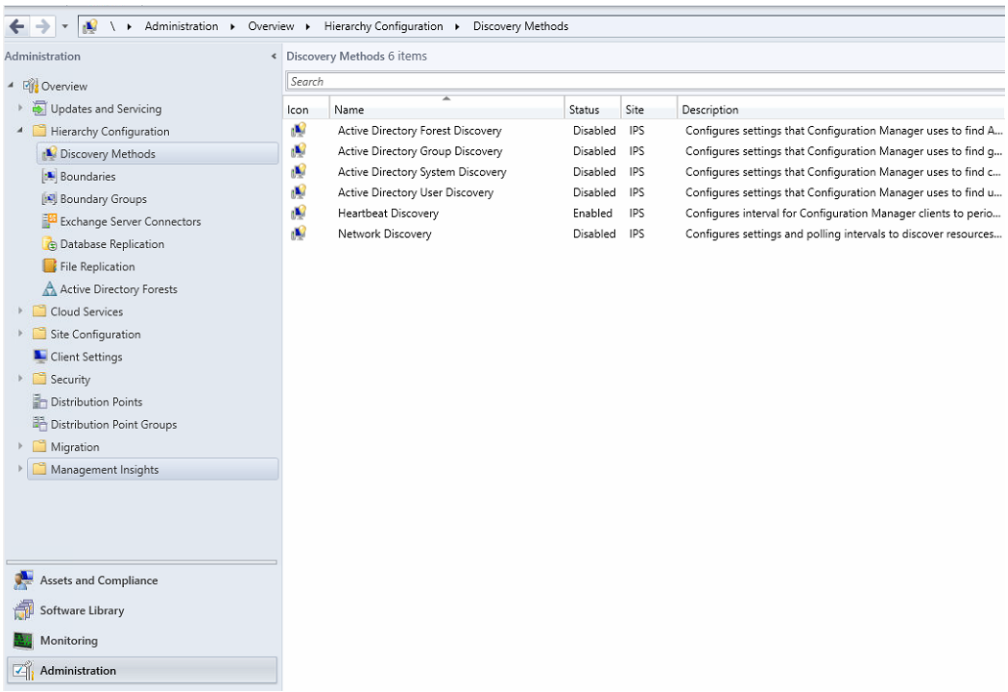

Vous pouvez ensuite lancer la console Configuration Manager et vérifier que vous retrouvez votre serveur SCCMPS dans les **Appareils**.

## 2. Intégration de clients

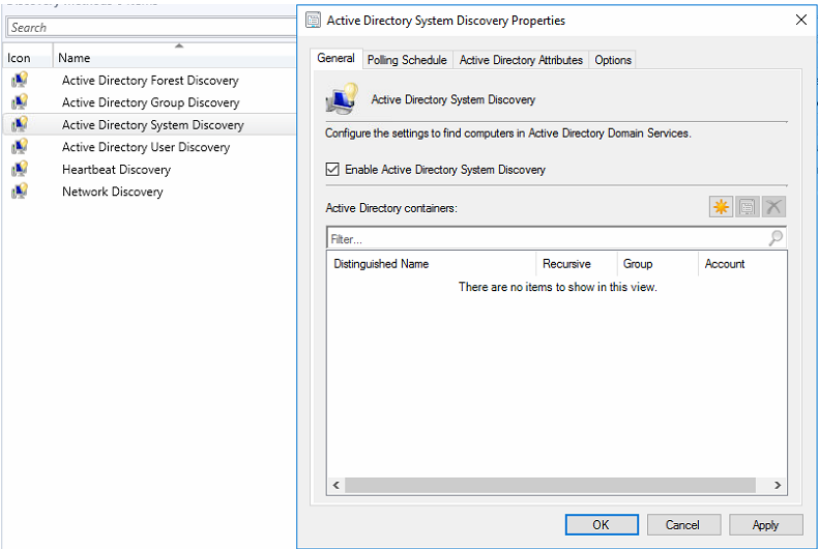
Une fois notre serveur SCCM en place, il convient désormais d'intégrer les clients déjà dans le parc dans notre base de clients SCCM.

### *a. Découverte d'objets Ordinateurs, Utilisateur et Groupes*

Pour ce qui est de l'intégration de clients lors de la masterisation d'un poste, on peut passer par des scripts PowerShell pour automatiser le déploiement des clients SCCM. Alors que pour les postes déjà actifs dans le parc, il existe trois méthodes pour intégrer des postes (voir même des utilisateurs) dans la base SCCM : l'ajout manuel, la découverte réseau et la découverte Active Directory. Vous trouverez ces méthodes dans la **console SCCM > Administration > Configuration de la hiérarchie > Méthodes de découvertes.**

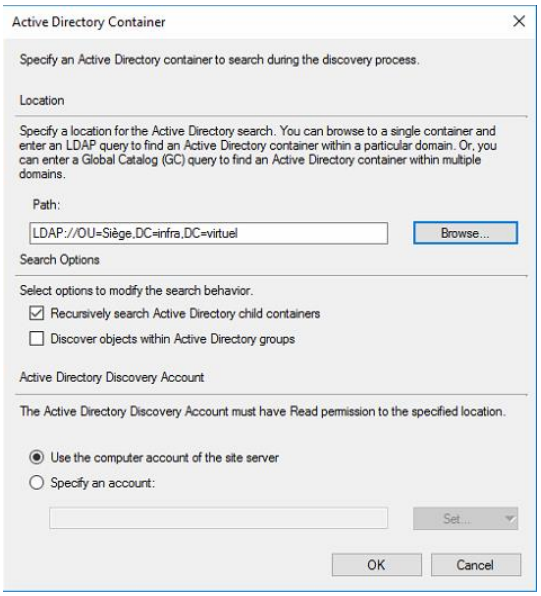



Le choix est vôtre ; dans notre cas, nous activerons la découverte Active Directory, qui permettra à SCCM de scanner l'AD pour détecter tout appareil/utilisateur/groupe d'utilisateur qui n'est pas dans sa database, afin de l'ajouter.




Faites clic droit sur **Découverte de Systèmes Active Directory > Propriétés.** Dans la fenêtre qui s'ouvre, cochez la case **Activer la Découverte de Systèmes Active Directory**.

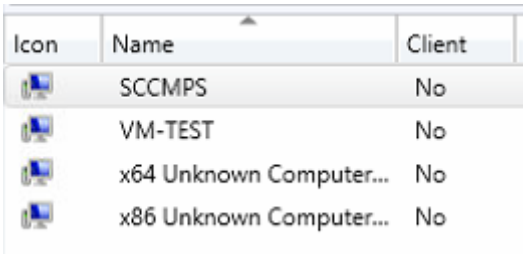
Il faut maintenant préciser où rechercher les objets Ordinateurs dans l'AD. Cliquez sur l'icône en forme de soleil.




Dans cette fenêtre, faites Parcourir pour sélectionner l'UO racine de votre domaine (où se situent vos UO Ordinateurs et Utilisateurs). Cochez bien la case **Faire une recherche récursive dans les containers enfants Active Directory** si vous sélectionnez l'UO racine ; sinon SCCM ne cherchera que dans celle-ci.

Ne changez pas le compte utilisé pour la recherche, sauf si votre compte **SCCM2020** n'a pas les droits de lecture sur l'AD. Faites **OK**.

Refaites un clic droit sur **Découverte de Systèmes Active Directory > Lancer une découverte.** Vous pouvez réitérer ces opérations pour la découverte d'utilisateurs.

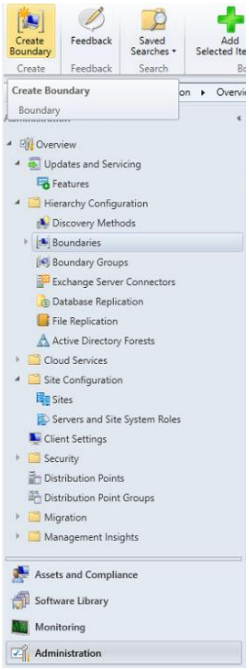


| Icon | Name | Client |
|---|---|---|
| | SCCMPS | No |
| | VM-TEST | No |
| | x64 Unknown Computer... | No |
| | x86 Unknown Computer... | No |

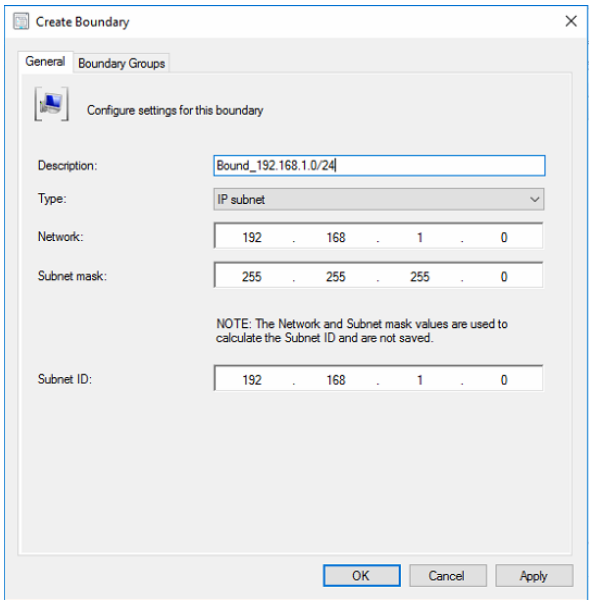
Notre VM-TEST apparaît dans la collection d'appareils. Seulement, on remarque que le client n'y est pas encore installé.

### *b. Création des limitation et affectation de site*

Chaque client découvert est affecté à un site SCCM particulier selon des règles définissables, appelées « **groupe de limitation** » (ou **boundary group**). Il est donc primordial de d'abord créer une limite, de l'affecter à un groupe, et de désigner un site vers lequel rediriger l'affectation de clients.

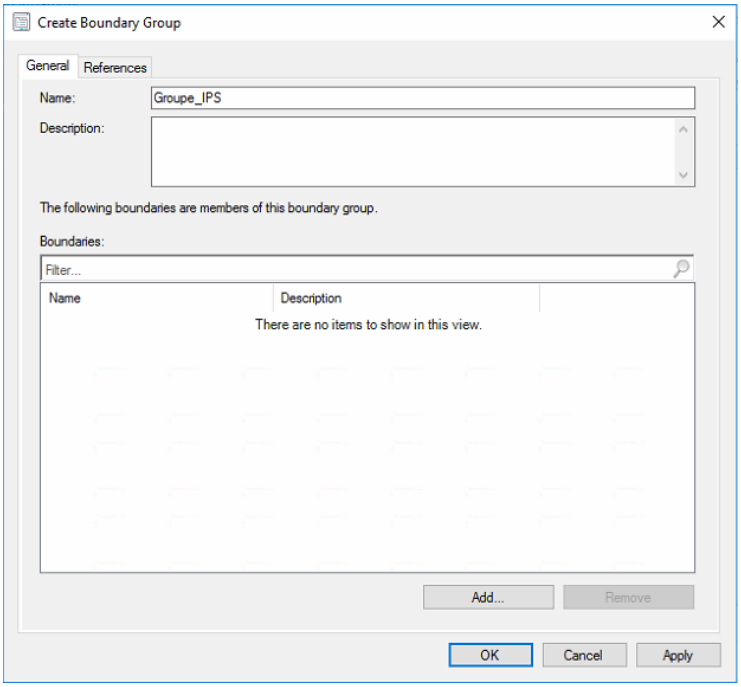



Dans **Administration > Configuration de la hiérarchie > Limitation,** faites **Créer une limite**.




Donnez-lui une description (vous ne pouvez pas changer son nom), et définissez le type de limite (ici, nous utiliserons les limites par sous-réseau). Indiquez le réseau où se situent vos postes (ici, **192.168.1.0**) et son masque.

Faites **OK**.




Rendez-vous ensuite dans **Administration > Configuration de la hiérarchie > Groupes de limites.** Faites **Créer un groupe de limites**.

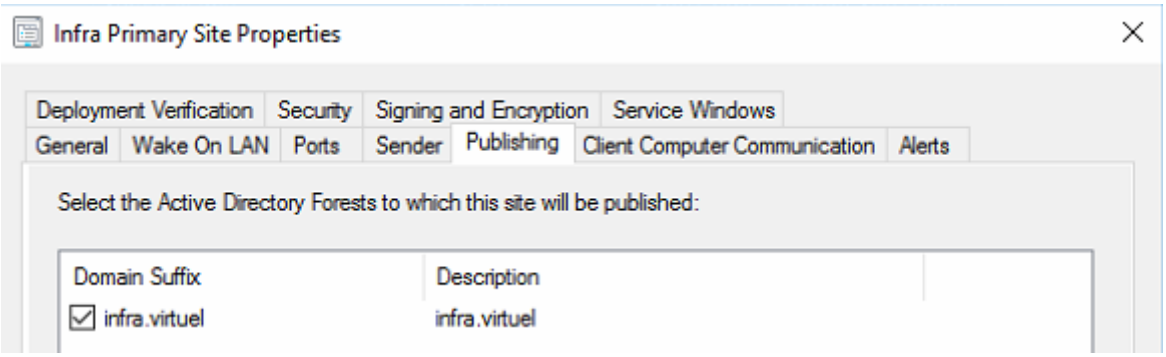
Donnez-lui un nom, et cliquez sur **Ajouter**. Sélectionnez la limite que vous venez de créer, à savoir **192.168.1.0**.

Dans l'onglet **Référence, cochez la case Utiliser ce groupe de limites pour l'affectation de sites** et assignez le site **IPS-Infra Primary Site.**

Dans **Serveurs de système de sites**, faites ajouter et entrez **SCCMPS**.

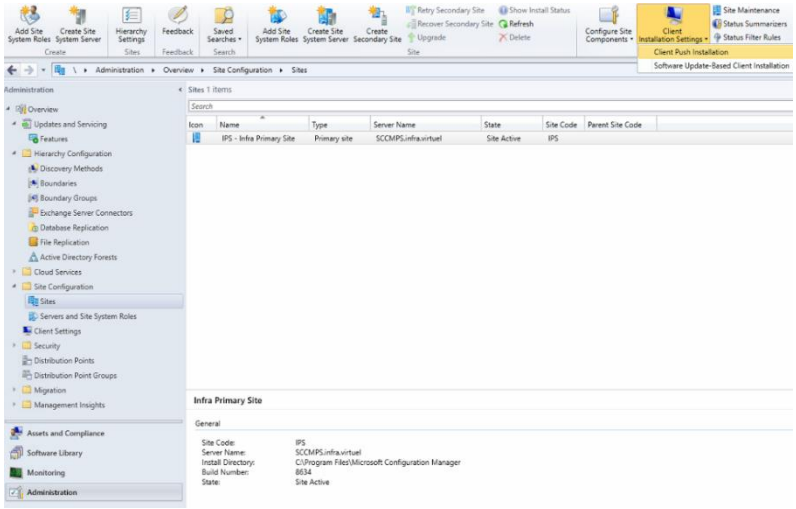
Faites **OK**.

Dans **Administration > Configuration de sites > Sites,** faites clic droit **> Propriétés** sur **IPS-Infra Primary Site.** Dans l'onglet **Publication**, vérifiez bien que votre domaine **infra.virtuel** est coché. Cela permettra à notre site primaire de publier dans les containers AD qui lui sont autorisés.

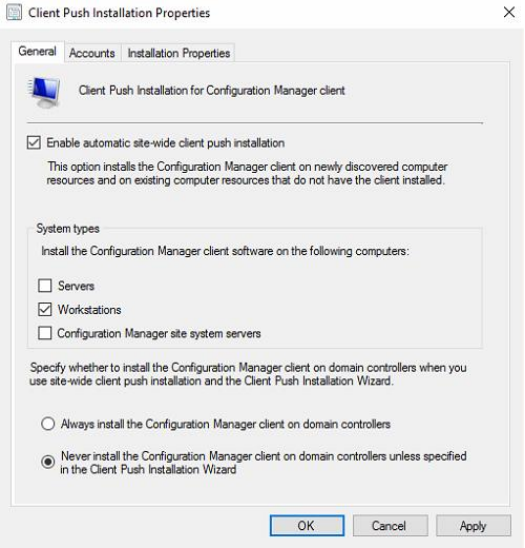


### c. *Déploiement du client SCCM*

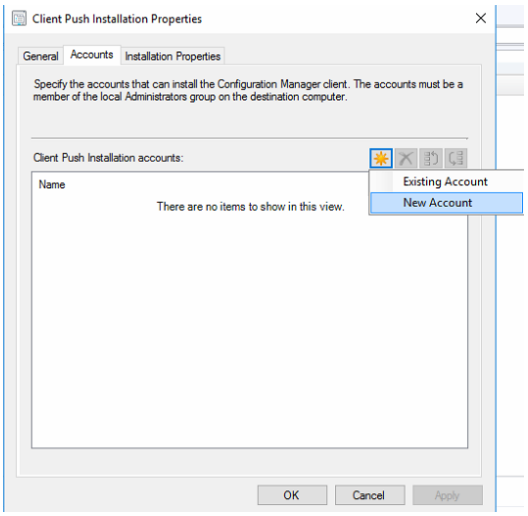
Ici, nous verrons comment déployer le client SCCM sur un appareil client, comme par exemple VM-TEST. Le client SCCM est un agent permettant le contact du serveur SCCM et ainsi la remontée de scans hardware, la prise de main à distance ou même le déploiement d'applications sur le poste. Pour déployer ce client, vous pouvez très bien l'installer manuellement sur le poste ; mais si votre parc est très vaste, il convient de le faire via la console SCCM.




Rendez-vous dans **Administration > Site configuration > Sites**, puis dans **Paramètres d'installation du client > Pousser l'installation du client**.



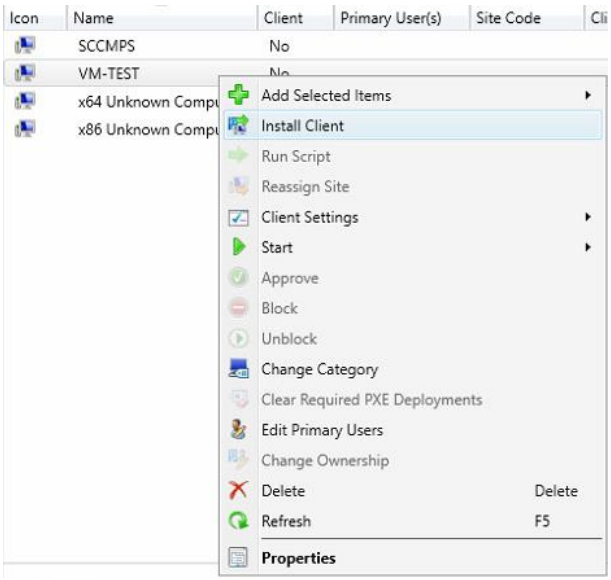

Cochez **Activez l'installation automatique du client par site**, puis décochez la case **Serveurs** ; en environnement réel il vaut mieux ne pas installer de client SCCM sur serveur, sauf si c'est prévu à l'avance. Faites **Appliquer**, puis rendez-vous dans l'onglet **Comptes**.




Cliquez sur le soleil puis sur **Nouveau Compte.** Dans la fenêtre qui s'ouvre, faites **Parcourir**, puis entrez **SCCM2020**.

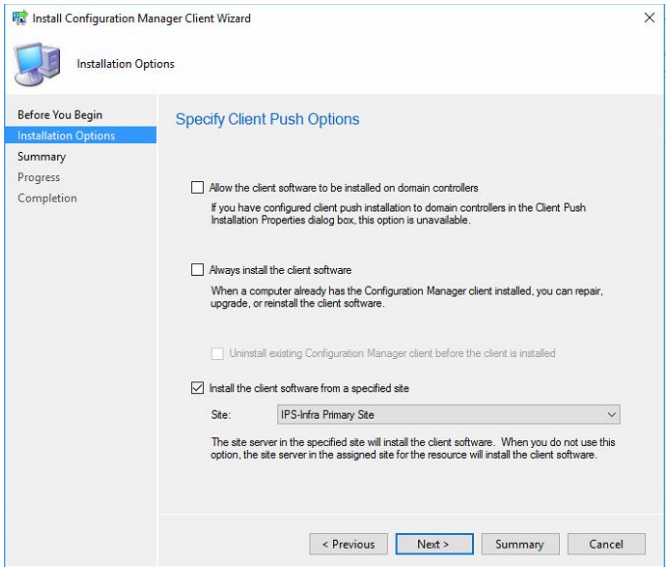
Spécifiez ensuite le mot de passe du compte **SCCM2020**.

Faites **OK**.

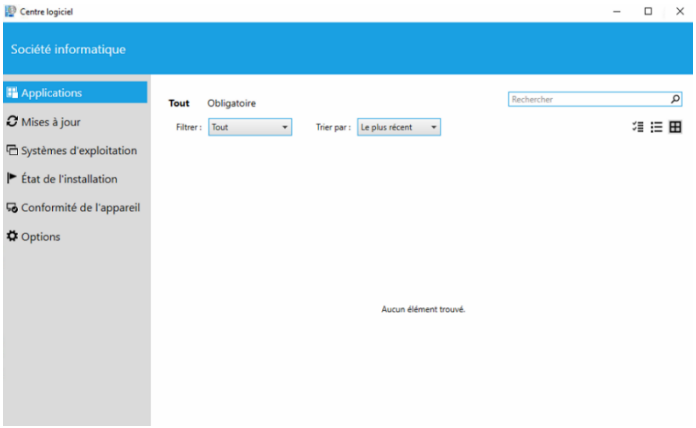



Retournez dans la liste d'appareils.

Faites un clic droit **> Installer le client** sur le poste. Un assistant s'ouvre.




Cochez la case **Installer le client depuis un site spécifique**. Sélectionnez le site depuis lequel vous souhaitez l'installer. Faites **Suivant** jusqu'à terminer le déploiement.

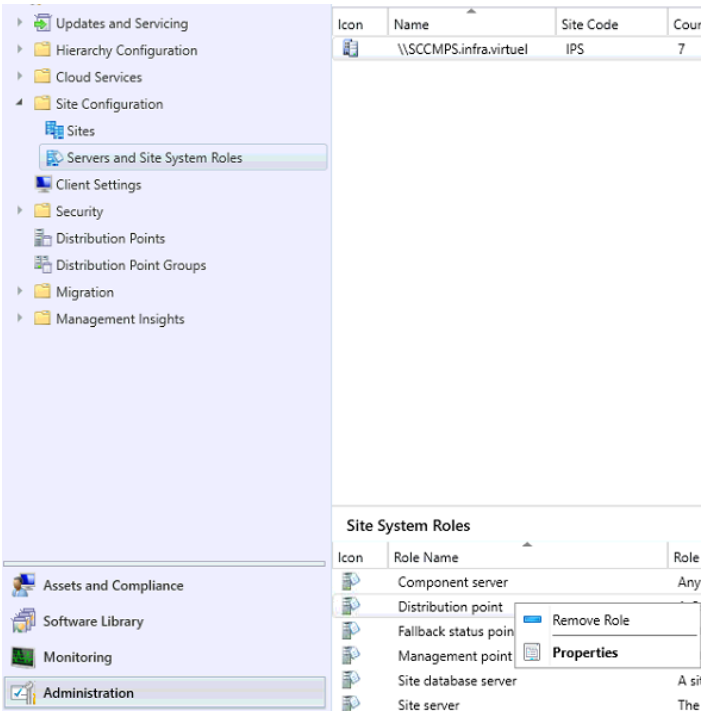



Assurez-vous que votre VM-TEST est bien allumée, et attendez environ 10 minutes. Vérifiez ensuite dans le panneau de configuration si le client **Configuration Manager** est bien présent, et qu'il s'ouvre correctement. Vous pouvez également vérifier l'ouverture du **Centre Logiciel**.

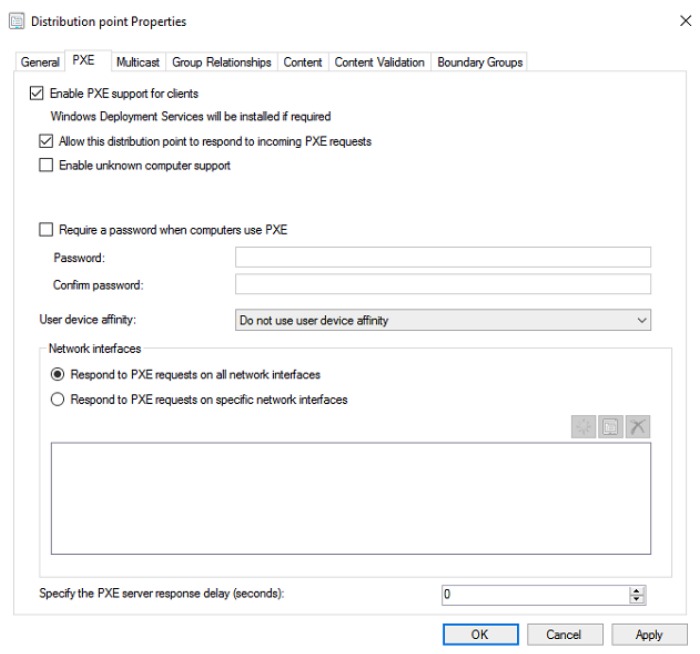
Si votre déploiement du client échoue, vérifiez que le compte utilisé pour le déployer est administrateur du poste VM-TEST. Vérifiez également que les ports 1433 et 4022 sont ouverts (nous avons configuré cela par GPO). Il faut également que le poste ait été ajouté dans SCCM via la découverte AD. Les logs peuvent être consultable sur le poste client dans *C:\windows\ccmsetup\logs*.

## 3. Activation du support PXE

Afin de permettre aux clients de booter sur le réseau lors de la masterisation, nous devons activer le support PXE sur le serveur SCCMPS.




Pour cela rendez-vous dans **Administration > Configuration des sites > Serveurs et rôles de systèmes de site**, cliquez sur **\\SCCMPS.infra.virtuel** puis plus bas sur **Point de Distribution > Propriétés**.

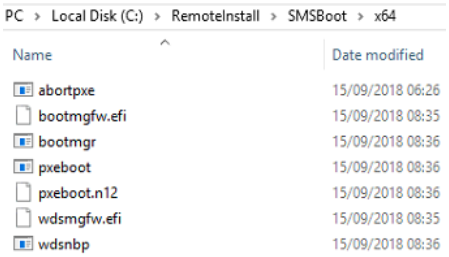



Cochez **Activer le support PXE pour clients**, puis **Autoriser ce point de distribution à répondre aux requêtes PXE entrantes**.

Vous pouvez également choisir si vous voulez définir un mot de passe au boot PXE ou non.

Faites **OK**.

Vous pouvez ensuite vérifier la présence des fichiers de boot dans ***C:\RemoteInstall\SMSBoot\x64***.



## 1. Déploiement de console

Dans cette dernière partie, nous allons voir comment déployer la console SCCM sur, par exemple, un poste de technicien. Nous effectuerons ce déploiement via la console elle-même, mais vous pouvez toujours utiliser le disque d'installation d'SCCM. Chaque console Configuration Manager peut se connecter à un site d'administration centrale ou à un site principal ; vous ne pouvez pas la connecter à un site secondaire.

Premièrement, récupérez les sources d'installation de la console sur le site primaire dans ***Program Files\Microsoft Configuration Manager\Tools\ConsoleSetup*** (si vous avez gardé le répertoire d'installation par défaut). Si vous avez téléchargé des mises à jour de la console, récupérez également le dernier patch dans ***Program Files\Microsoft Configuration Manager\EasySetupPayload\<GUID Hotfix>\smssetup\BIN\I386\ConsoleUpdate***. Réunissez donc ces différentes sources dans un dossier **Console SCCM version xxx\Sources** par exemple, que vous partagerez.

Ensuite, créez-y deux fichiers **.bat** ; un pour l'installation, l'autre pour la désinstallation.

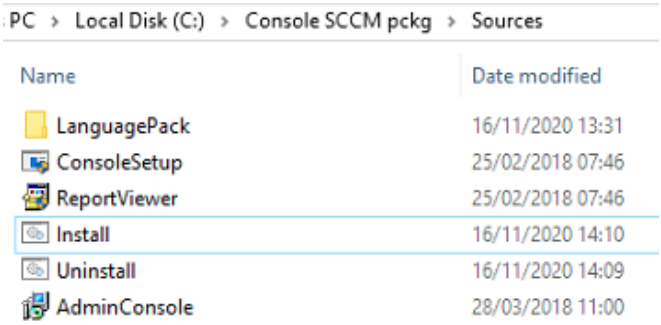
Script d'installation (remplacez avec le FQDN de votre site primaire, et le nom du patch) :

```
mkdir "C:\Program Files\ConfigMgr Console"

ConsoleSetup.exe /q TargetDir="C:\Program Files\ConfigMgr Console" DefaultSiteServerName=SCCMPS.infra.virtuel


ReportViewer.exe /q /norestart
```

Script de désinstallation :

```
ConsoleSetup.exe /q /uninstall

ReportViewer.exe /q /uninstall
```

Le contenu de notre dossier ressemble à cela :




Sur le poste devant recevoir la console, déposez-y le dossier **Console SCCM pckg** et lancez le fichier **Install.bat** en administrateur.

Vous devriez désormais pouvoir utiliser pleinement SCCM et les fonctions de démarrage sur réseau (PXE), afin de déployer des images disques ou des logiciels.