**Formation GPO  
 - sys 26 – T.p. maquette**

Michel Cabaré / www.cabare.net / michel@cabare.net

GPO Montage maquette (1DC 3 SRV 5 CLT)  
 - sys 26 – T.p. V1-00 - Déc 2021

|  |  |  |
| --- | --- | --- |
| https://WWW.CABARE.NET © |  |  |

|  |  |
| --- | --- |
|  |  |

Table des matières

[Montage MAQUETTE DC + 3 SRV + 5 Clt 2](#_Toc90746454)

[Objectif de la maquette 1 DC + 3 SRV + 5 CLIENTS 2](#_Toc90746455)

[Serveur Physique « Hôte » Hyper-V 2](#_Toc90746456)

[Stockage 2](#_Toc90746457)

[Cartes Réseau 2](#_Toc90746458)

[Commutateurs Réseau virtuels 2](#_Toc90746459)

[Utilisation d’un script Powershell 2](#_Toc90746460)

[Création des disques de différentiation + Création vm 2](#_Toc90746461)

[Phase OOBE des Vm 2](#_Toc90746462)

[Configuration des OS-Windows et OS-Serveur dans les VM 2](#_Toc90746463)

[Test Réseau lan 2](#_Toc90746464)

[Snapshoot base 2](#_Toc90746465)

[Montage Domaine Form.edu 2](#_Toc90746466)

[Objectif de la maquette form.edu 2](#_Toc90746467)

[Utilisation d’un script Powershell 2](#_Toc90746468)

[Création Domaine – sur Vm-s1 2](#_Toc90746469)

[Login Administrateur Domaine – sur Vm-s1 2](#_Toc90746470)

[BUG Serveur Windows DC sur SSD 2](#_Toc90746471)

[Gestion domaine form.edu – Dc = S1 dans Vm-s1 2](#_Toc90746472)

[**Création zone DNS invérsée principale 10.0.0.1** 2](#_Toc90746473)

[**GPO mot de passe et pare feu** 2](#_Toc90746474)

[Intégration des 3 Vm serveur et 5 Vm client au domaine 2](#_Toc90746475)

[Adhésion détaillée pour s2 2](#_Toc90746476)

[Adhésion des autres Vm 2](#_Toc90746477)

[Test IP depuis le DC sur Vm-S1 2](#_Toc90746478)

[Snapshoot Domaine-ok 2](#_Toc90746479)

# Montage MAQUETTE DC + 3 SRV + 5 Clt

## Objectif de la maquette 1 DC + 3 SRV + 5 CLIENTS

Dans un Serveur Hyper-V 2016-2019 configuré correctement, on va monter 9 Vm correspondant à un réseau en domaine :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nom VM** | **Nom Système Hôte** | **OS** | **Rôle (futur)** | **Remarque** | **@ IP** |
| Vm-S1 | S1 | Serveur | DC | Pour l’instant Workgroup | 10.0.0.1/255.0.0.0 |
| Vm-S2 | S2 | Serveur | - | Pour l’instant Workgroup | 10.0.0.2/255.0.0.0 |
| Vm-S3 | S3 | Serveur | - | Pour l’instant Workgroup | 10.0.0.3/255.0.0.0 |
| Vm-S4 | S4 | Serveur | - | Pour l’instant Workgroup | 10.0.0.4/255.0.0.0 |
| Vm-S5 | S5 | Client10 | - | Pour l’instant Workgroup | 10.0.0.5/255.0.0.0 |
| Vm-S6 | S6 | Client10 | - | Pour l’instant Workgroup | 10.0.0.6/255.0.0.0 |
| Vm-S7 | S7 | Client10 | - | Pour l’instant Workgroup | 10.0.0.7/255.0.0.0 |
| Vm-S8 | S8 | Client10 | - | Pour l’instant Workgroup | 10.0.0.8/255.0.0.0 |
| Vm-S9 | S9 | Client10 | - | Pour l’instant Workgroup | 10.0.0.9/255.0.0.0 |

Le réseau est en Adresse Ip de classe **A** en **10.0.0.x/255.0.0.0**

Les comptes **Administrateur Local** Hôtes Srv : **Administrateur / Local2019**

Les comptes **Administrateur Local** Hôtes Windows10 : **Admin / Local**

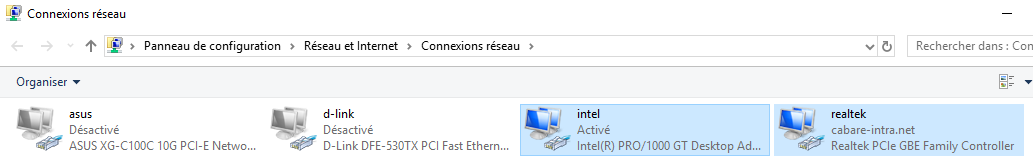
## Serveur Physique « Hôte » Hyper-V

### Stockage

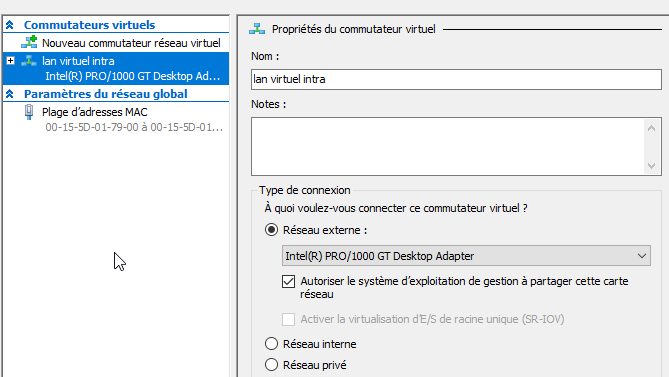
Possède un stockage en X:\vm avec de la place (disques de différentiation)

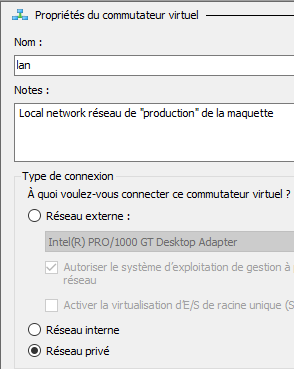
### Cartes Réseau

Possède une carte réseau ***intel Pro 1000*** branchée sur le réseau physique



### Commutateurs Réseau virtuels



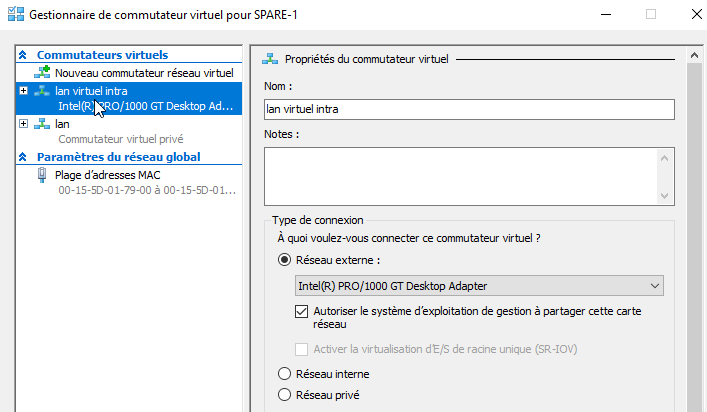
On devrait avoir 1 **commutateur Virtuel Externe** nommé ***lan virtuel intra*** permettant un accès à internet. C’est le seul accès réseau physique disponible. Il est indispensable à la maquette pour la récupération des mises à jour sur le Site de Microsoft.

On créera au minimum 1 **Commutateur réseaux virtuel privé** nommé ***lan***

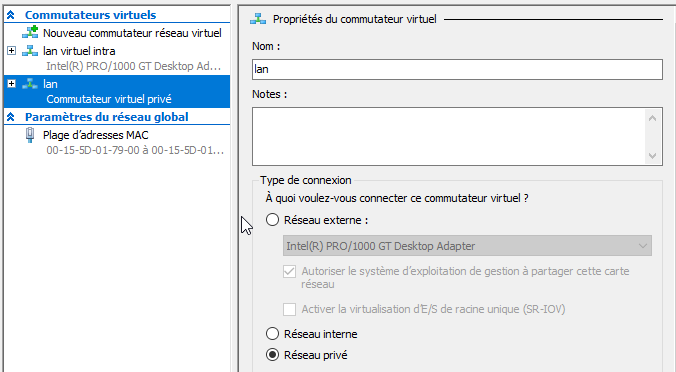


De manière à avoir au final 2 commutateurs réseaux

***lan virtuel intra – Externe -***



***lan – privé***

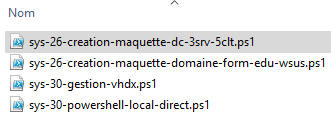


## Utilisation d’un script Powershell

On va utiliser des morceaux de script **powershell** pour monter la maquette

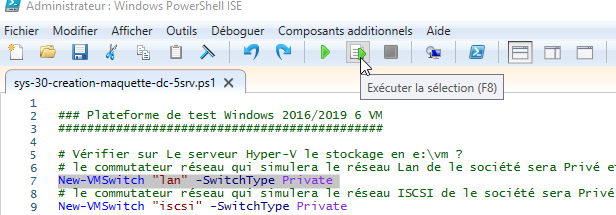
Le script à ouvrir via **Modifier** dans **PowershellISE** se nomme

***sys-26-creation-maquette-dc-3srv-5clt.ps1***



On se placera sur les lignes voulues, et on demandera de les exécuter

Si on n’a pas créer les commutateurs réseau manuellement précédemment, dans notre machine physique, on peut les créer via le **script powershell**

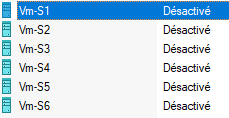


## Création des disques de différentiation + Création vm

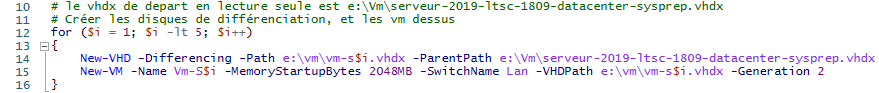
*A la main* :

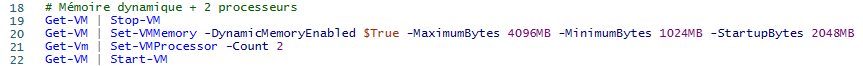
Il faut copier le fichier vhdx « disque de base », nommé par exemple pour nous ***serveur-2019-ltsc-1809-datacenter-sysprep.vhdx*** et le mettre en lecture seule. Puis créer les 4 disques de différenciation pour nos futures 4 vm.

Il faut ensuite créer les 4 Vm, de **génération 2**, leur donner chacune **4 Giga de Ram**, et leur donner une **carte réseau** sur le réseau « entreprise » **lan.**

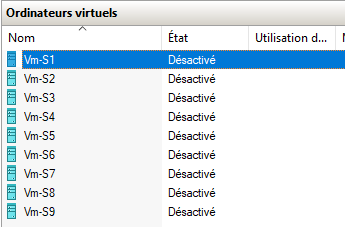
Ensuite leur affecter 2 processeurs, et leur allouer de la mémoire dynamique (max 4096, Min 1024 initial 2048)

En powershell :



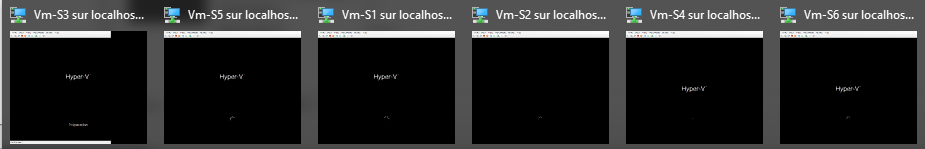


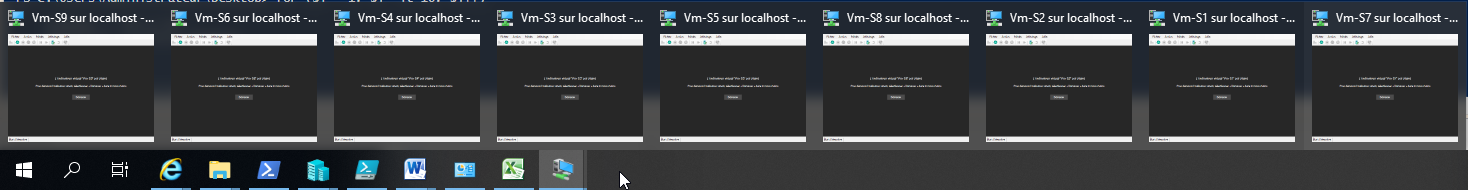
On refait la même chose pour les 5 clients avec fichier vhdx « disque de base », nommé par exemple pour nous ***windows-10-20H2-sysprep.vhdx.***

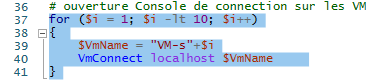
Et au final on devrait avoir

## Phase OOBE des Vm

Il faut lancer les consoles

Voire

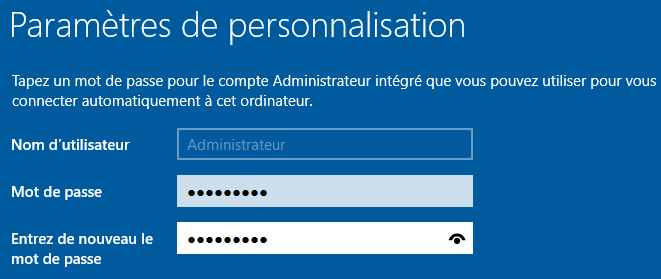




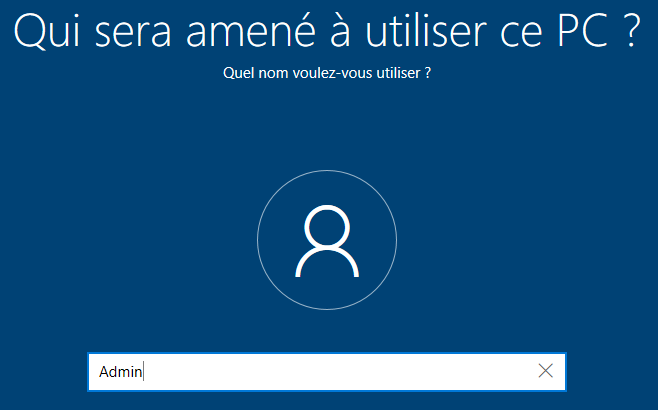
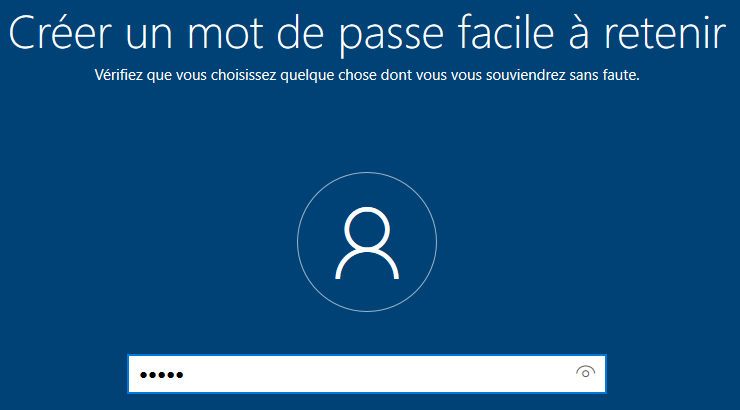
*A la main* :

Les consoles étants lancés ; comme les machines sont sysprépés, il faut les démarrer, et dérouler la phase OOBE (cela prendra 10 mn, avec les saisies de mot de passe), De manière à obtenir les VM opérationnelle. La seule chose importante c’est indiquer le mot de passe des administrateur

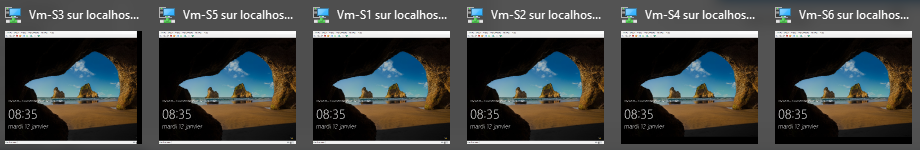
sur les Serveurs : ***Administrateur / Local2019 de VM-S1 à VM-S4***



sur les client 10 : ***Admin / Local de VM-S5 à VM-S9***

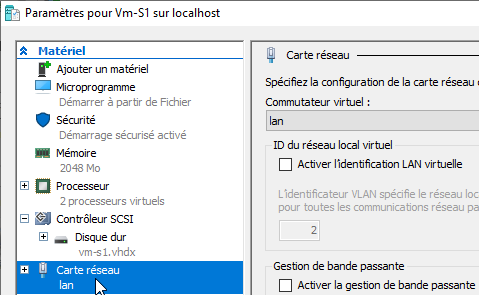
 

Sur les clients windows 10, on ignore le 2° clavier- pas d’internet- installation limitée, on réponds 1-2-3 au questions de sécurité du mot de passe, et on réponds de manière générale non partout, pas de cortana…

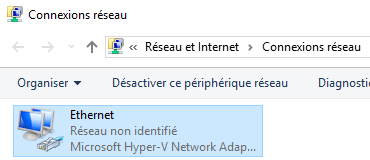


On peut ouvrir une session sur une Vm via **CTRL + ALT + FIN**

Chaque Vm devait avoir ses caractéristiques



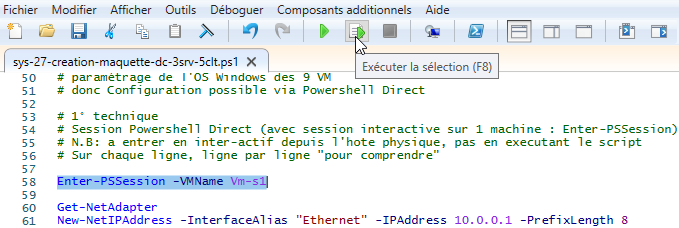
Et une carte réseau nommée ***Ethernet*** branchée sur le commutateur ***lan***

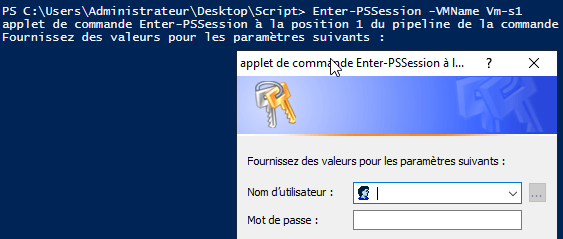


## Configuration des OS-Windows et OS-Serveur dans les VM

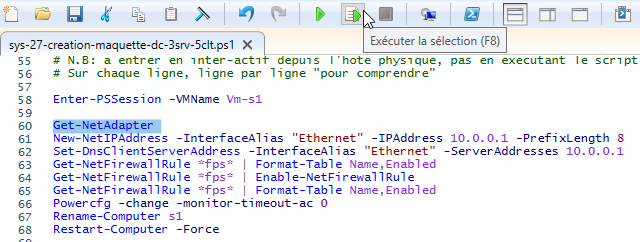
Via Powershell c’est possible, En **powershell Direct**

**1° technique** Ligne par ligne, en **Session inter-active** (de manière a ce que l’on on voit ce que l’on fait, par exemple pour la Vm-1)

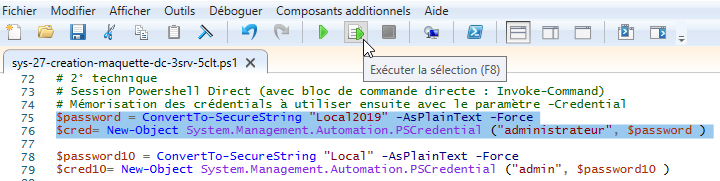




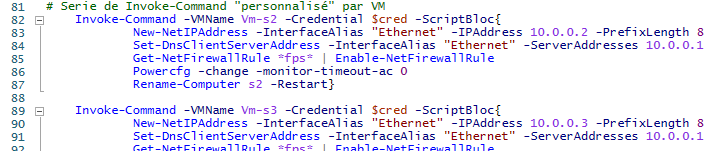
*Et ensuite les commandes powershell, en session interactive…*



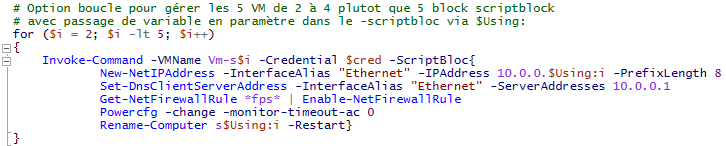
Soit on Ajoute la notion de **-Credential**, (un jeu stocké dans $cred et un jeu stocké dans $cred10) et on execute les Block personnalisés pour chaque VM



*Et les blocs personnalisés (pour les serveurs, et pour les clients)*



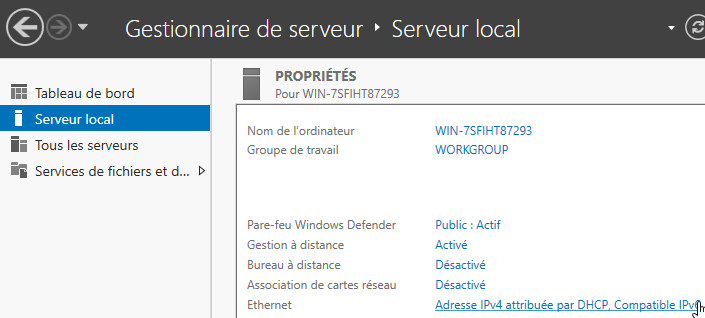
*Voir avec une boucle (une pour les serveurs, et une pour les clients )*



*Ou a la main* :

* Il faut pour chaque OS Serveur, executer les opérations suivantes : par exemple pour S***1***
* Donner une adresse IP cohérente 10.0.0.***1*** / 255.0.0.0 avec une adresse de DNS 10.0.0.1
* Ouvrir le pare-feu pour toutes les règles de partage de fichier et d’imprimantes
* Nommer l’ordinateur (nom d’hôte) S***1***
* Désactiver l’économiseur d’écran (veille)
* Redémarrer l’ordinateur .

On peut vérifier une partie de la configuration dans le **gestionnaire de serveur** / **Serveur local,** par exemple

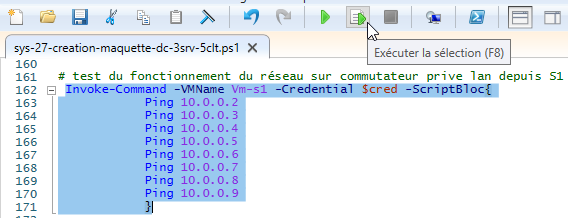
devient

Devient

## Test Réseau lan

Il faudrait tester par un Ping, depuis le Serveur S1 (c’est-à-dire la Vm-S1) qu’il puisse Effectuer un Ping sur les 5 autres Serveurs

Via Powershell c’est aussi possible, En **powershell Direct**

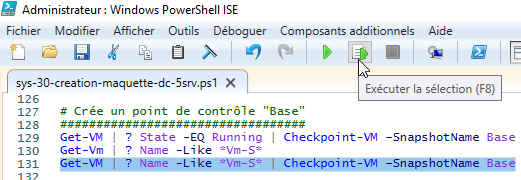


*A la main* :

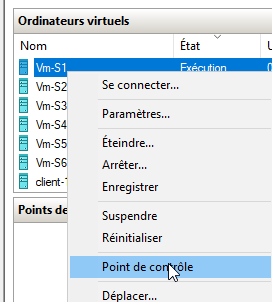
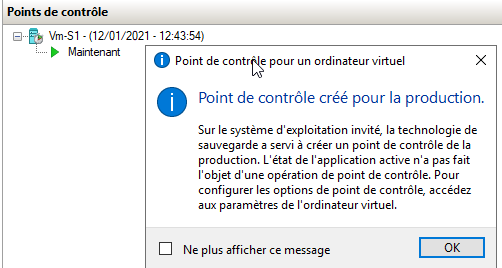
Ping…

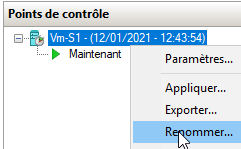
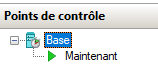
## Snapshoot base

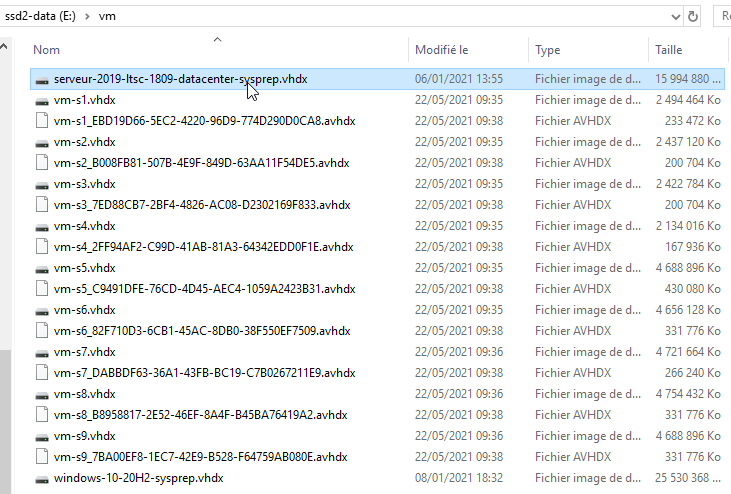
Via Powershell



A la main : pour chaque VM on crée le snapshot, et on le nomme ***base***

  maquette de 70 Giga !



# Montage Domaine Form.edu

## Objectif de la maquette form.edu

Dans un Serveur **Hyper-V** 2016-2019, sur lequel on a monté la maquette 1***DC + 3 SRV + 5 CLT***, on va monter le DC du domaine ***form.edu*** sur la ***VM-S1***

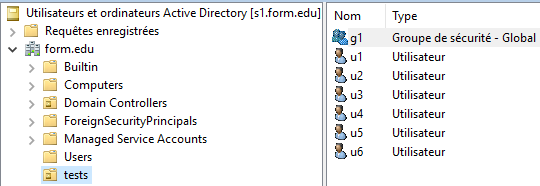
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nom VM** | **Nom Hôte** | **OS** | **Rôle** | **Remarque** | **@ IP** |
| Vm-S1 | S1 | Serveur | DC | Form.edu | 10.0.0.1/255.0.0.0 |
| Vm-S2 | S2 | Serveur | Membre | - | 10.0.0.2/255.0.0.0 |
| Vm-S3 | S3 | Serveur | Membre | - | 10.0.0.3/255.0.0.0 |
| Vm-S4 | S4 | Serveur | Membre | - | 10.0.0.4/255.0.0.0 |
| Vm-S5 | S5 | Client 10 | Membre | - | 10.0.0.5/255.0.0.0 |
| Vm-Sx | Sx | Client 10 | Membre | - | 10.0.0.X/255.0.0.0 |
| Vm-S9 | S9 | Client 10 | Membre | - | 10.0.0.9/255.0.0.0 |

Le domaine se nomme **form.edu** Les adresse Ip de classe **A 10.0.0.x/255.0.0.0**

L’ **Administrateur** duDomaine **Form.edu** : **Administrateur / Domaine2019**

Les comptes **Administrateur Local** des SRV  : **Administrateur / Local2019**

Les comptes **Administrateur Local** Hôtes Windows10 : **Admin / Local**

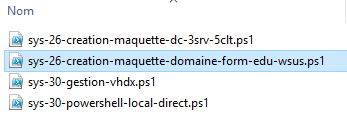


Une **UO** ***tests*** existe, avec 4 **utilisateur** ***U1*** à ***U6*** ayant le même mot de passe ***pw***, dans un **groupe global** ***g1***

## Utilisation d’un script Powershell

Le script à ouvrir via **Modifier** dans **PowershellISE** se nomme

***sys-26-creation-maquette-domaine-form-edu-wsus***

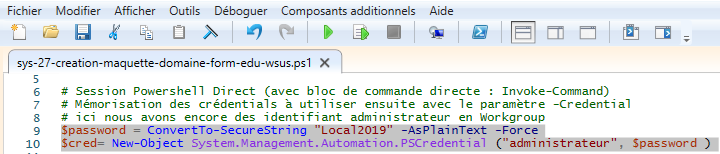


On se placera sur les lignes voulues, et on demandera de les exécuter

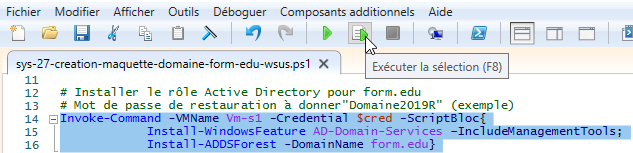
## Création Domaine – sur Vm-s1

On va transformer **S1** en **CD**, du domaine ***form.edu***

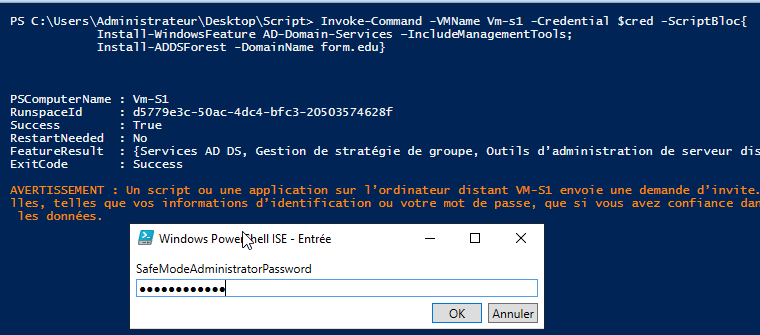
Via Powershell ISE, depuis le serveur Hyper-V (machine physique) on peut, s’authentifier avec le login local (puisque l’on est en workgroup)

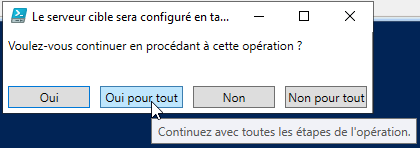


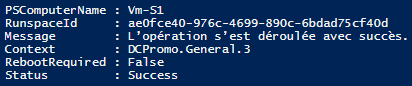
Et demander de monter un domaine ***form.edu*** sur ***Vm-S1***



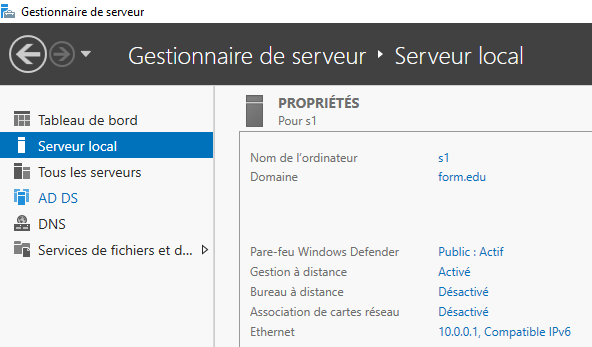
Il faudra rentrer le mot de passe de restauration des service d’annuaires, par exemple ***Domaine2019R (à confirmer 1 fois)***



Confirmer 

Et c’est fini 

On ouvre la session **login** sur form\administrateur **pswd** Local2019 et on peut vérifier que l’on a un Domaine ***form.edu*** sur la bonne adresse ***IP***



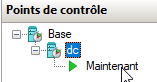
## Login Administrateur Domaine – sur Vm-s1

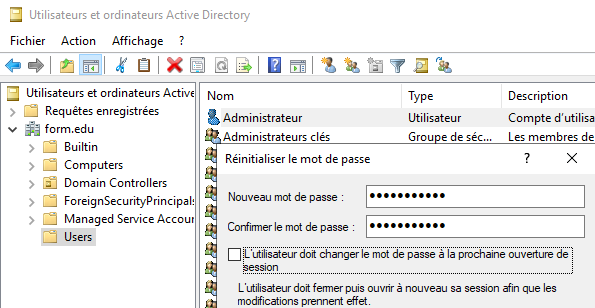
Pour ne pas se mélanger entre compte de domaine, et comptes locaux, on va changer le compte d’administrateur de domaine, qui pour l’instant est le même que le compte administrateur local …

Le compte **Administrateur local** : **Administrateur / Local2019**

Le compte **Admin du Domaine (Form.edu)** : **Administrateur / Domaine2019**

On fait cela sur le CD en inter-actif, dans **Utilisateur et Ordinateurs AD**

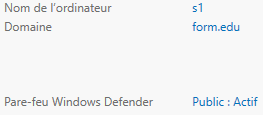
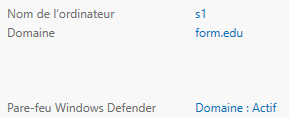
**N.B** : si on est pas sur de la manipulation, on peut faire un snapshoot de VM-S1 avant que l’on nommera Dc



On teste la re-ouverture de session avec les nouveaux identifiants de domaine, et on supprime le snapshoot si on y est arrivé

## BUG Serveur Windows DC sur SSD

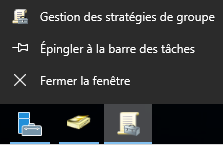
Le programme de diagnostique profil réseau BUG, car on démarre trop vite, il met le **pare-feu de Domaine** en **Public** ! alors qu’il devrait être en **Domaine**

Une solution, **Désactiver / Activer** la carte réseau (en attendant un correctif)



## Gestion domaine form.edu – Dc = S1 dans Vm-s1

Il serait bon d’epingler sur la Barre des Taches quelques consoles :

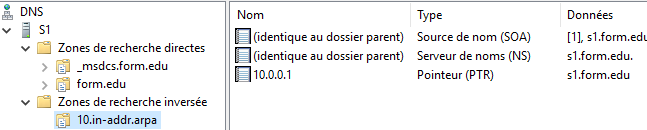
**Gestion de Serveur**

**Utilisateurs et ordinateurs Active Directory**

**Gestion des Stratégies de groupe**

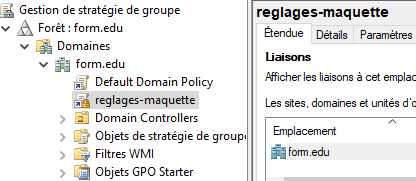
**Dns**

### **Création zone DNS invérsée principale 10.0.0.1**

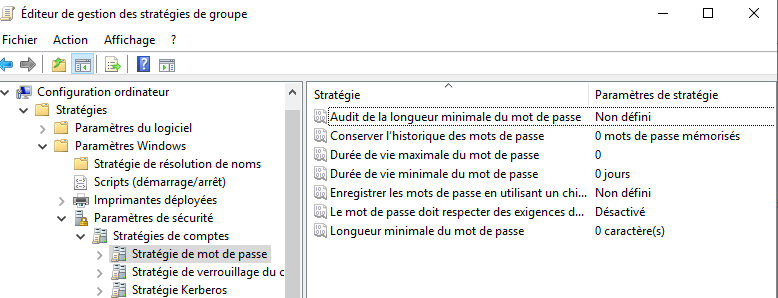


### **GPO mot de passe et pare feu**

On va se créer une **GPO de domaine**, pour désactiver les mots de passes complêxes, sur tout le domaine, et autoriser dans le pare-feu toutes les connexions liées aus partages et aux imprimantes.

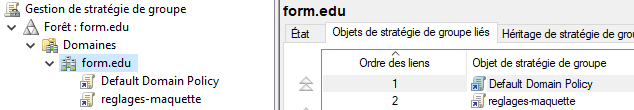


#### Mots de Passe Complêxe

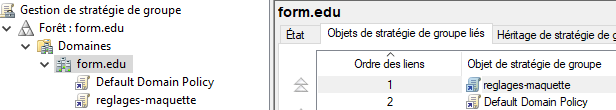


Mais l’ordre du coup ne convient pas, car dans la stratégie Default domain Policy un réglage est demandé, concernant ces mots de passe

Donc de cette situation,

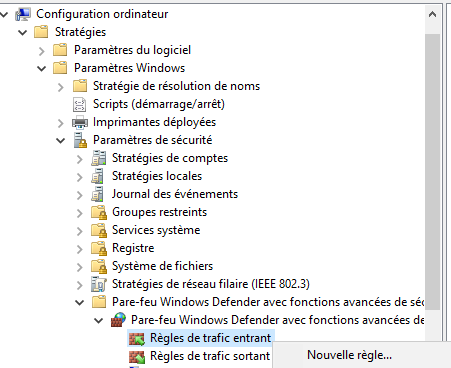


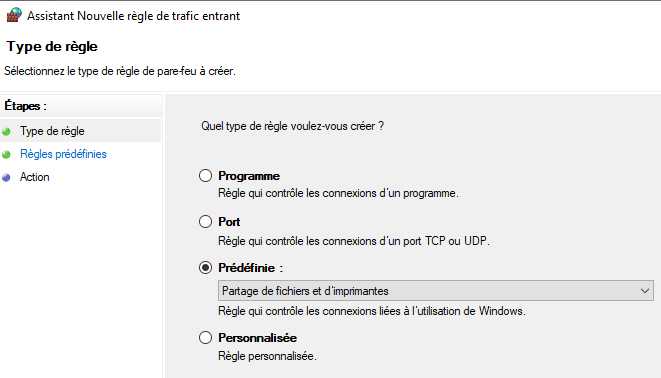
Il faut passer à

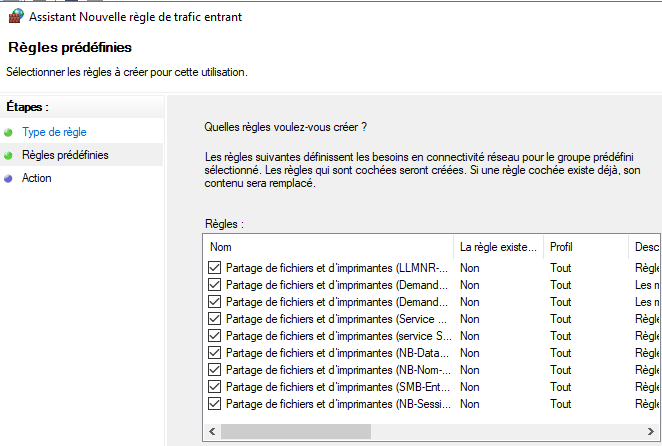


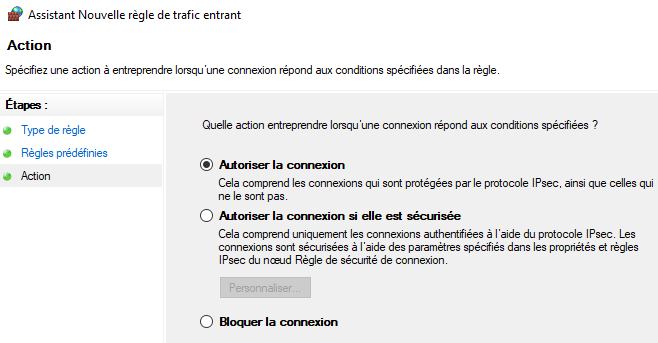
#### Règle du pare-feu

On va poser des **règles de pare-feu** pour autoriser les **partages et Ping**

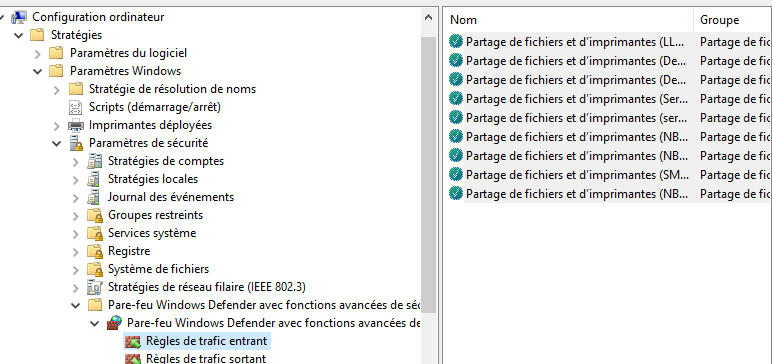
 **Nouvelle règle**



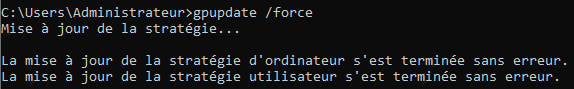




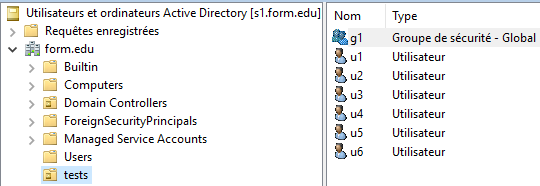
Pour obtenir



On referme la **Console des GPO** et on applique au serveur **Gpupdate / force**



Création d’une UO ***Test*** dans l’Active Directory

Création de 6 **utilisateur** ***U1*** à ***U6*** ayant le même mot de passe ***pw***, dans un **groupe global** ***g1***

## Intégration des 3 Vm serveur et 5 Vm client au domaine

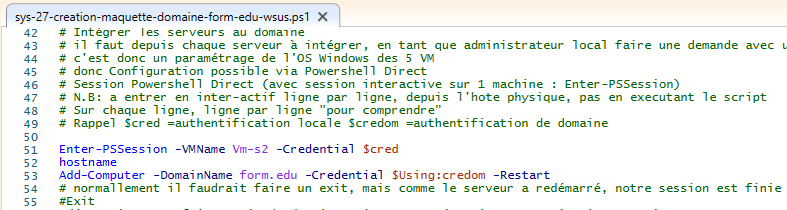
il faut depuis chaque Vm à intégrer, en tant que administrateur local faire une demande avec une authentification de domaine. C'est donc un paramétrage de l'OS Windows des 8 VM .

La configuration est possible via **Powershell Direct**

On va faire une **Session Powershell Direct** (avec session interactive sur 1 machine : Enter-PSSession)

# Rappel $cred =authentification locale $credom =authentification de domaine

### Adhésion détaillée pour s2



On ouvre la session avec une authentification locale





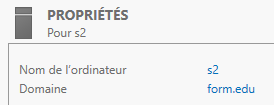
On est bien loggué en tant qu’administrateur local

On peut vérifier que l’on est bien sur la machine S2



On lance l’adhésion au domaine

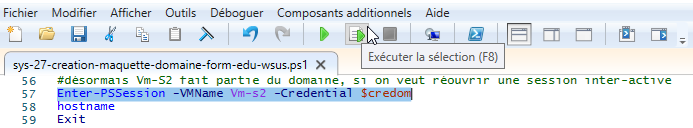


Le poste S2 redémarre, on peut vérifier dans le **gestionnaire de serveur** de S2 qu’il appartient bien au domaine form.edu

Si on veut reprendre une session Powershell, le login local ***$cred*** ne marche plus



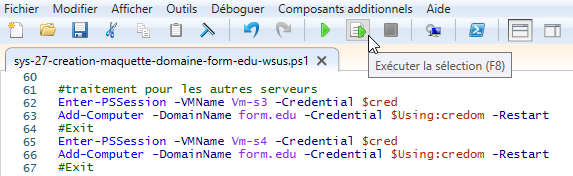
Il faut utiliser le login de domaine ***$credom***



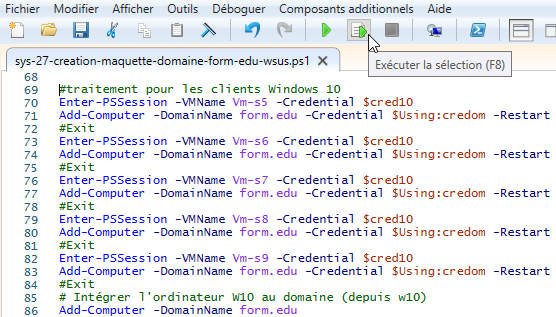


On est bien loggué en tant qu’administrateur de domaine.form

### Adhésion des autres Vm

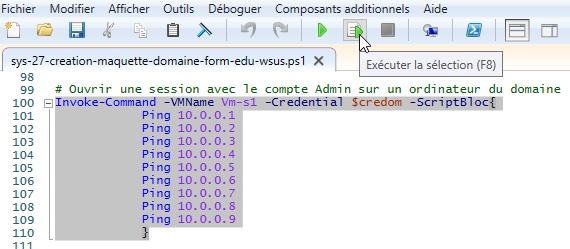


Et



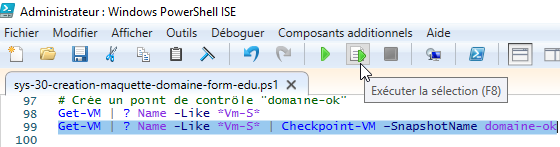
## Test IP depuis le DC sur Vm-S1

il faut depuis par exemple le serveur **DC** **S1** dans la **Vm-s1** tester un ping sur tous les serveurs membre du domaine, (vérification réseau lan et gestion des pare-feu / GPO)

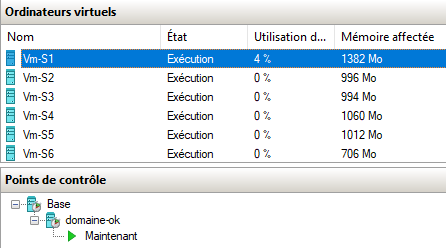
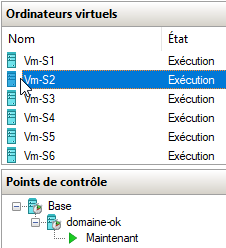


## Snapshoot Domaine-ok

Via Powershell



Désormais toutes nos Vm ont un deuxième point de contrôle



Globalement on pourra faire revenir la maquette dans un état global via

