

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 MATIERES

MONTAGE MAQUETTE DC + 3 SRV + 5 CLT	3
OBJECTIF DE LA MAQUETTE 1 DC + 3 SRV + 5 CLIENTS	3
SERVEUR PHYSIQUE « HOTE » HYPER-V	4
<i>Stockage</i>	4
<i>Cartes Réseau</i>	4
<i>Commutateurs Réseau virtuels</i>	4
UTILISATION D'UN SCRIPT POWERSHELL.....	5
CREATION DES DISQUES DE DIFFERENTIATION + CREATION VM	6
PHASE OOBE DES VM.....	7
CONFIGURATION DES OS-WINDOWS ET OS-SERVEUR DANS LES VM	8
TEST RESEAU LAN	10
SNAPSHOT BASE	11
MONTAGE DOMAINE FORM.EDU	12
OBJECTIF DE LA MAQUETTE FORM.EDU	12
UTILISATION D'UN SCRIPT POWERSHELL.....	13
CREATION DOMAINE – SUR VM-S1	13
LOGIN ADMINISTRATEUR DOMAINE – SUR VM-S1	14
BUG SERVEUR WINDOWS DC SUR SSD	15
GESTION DOMAINE FORM.EDU – DC = S1 DANS VM-S1	15
<i>Création zone DNS inversée principale 10.0.0.1</i>	16
<i>GPO mot de passe et pare feu</i>	16
INTEGRATION DES 3 VM SERVEUR ET 5 VM CLIENT AU DOMAINE.....	19
<i>Adhésion détaillée pour s2</i>	19
<i>Adhésion des autres Vm</i>	20
TEST IP DEPUIS LE DC SUR VM-S1	21
SNAPSHOT DOMAINE-OK.....	21

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

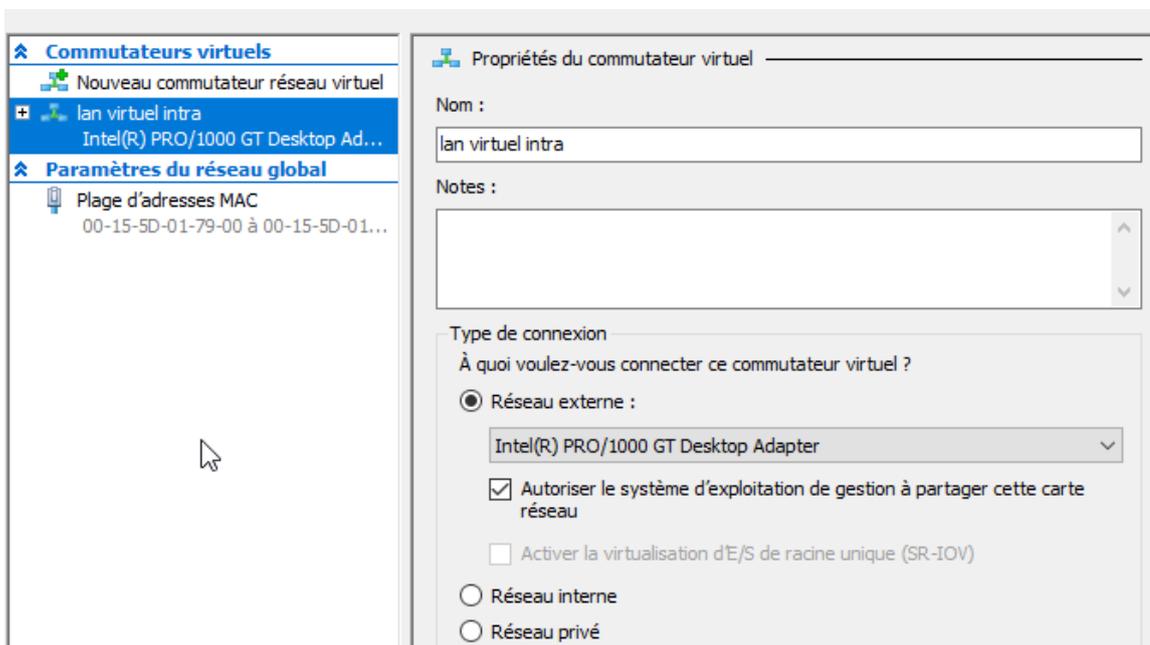
Possède un stockage en X:\vm avec de la place (disques de différenciation)

Cartes Réseau

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

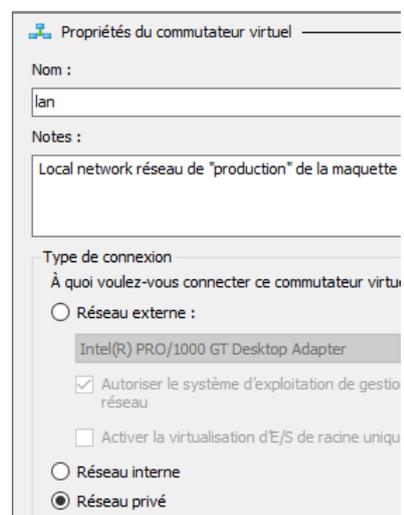


Commutateurs Réseau virtuels



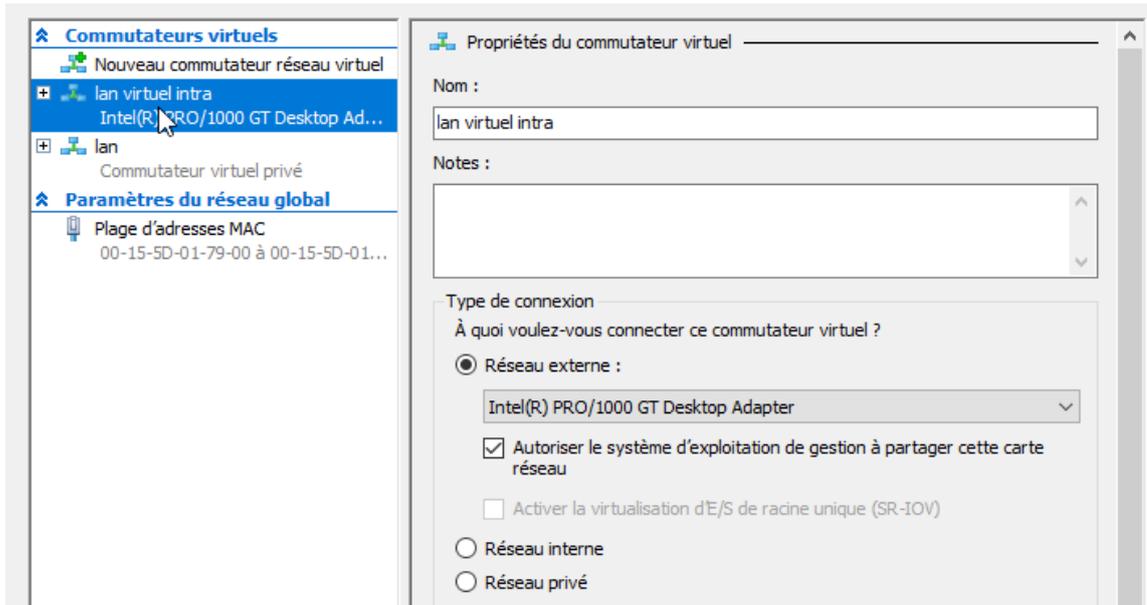
On devrait avoir 1 **commutateur Virtuel Externe** nommé **lan virtuel intra** permettant un accès à internet. C'est le seul accès réseau physique disponible. Il est indispensable à la maquette pour la récupération des mises à jour sur le Site de Microsoft.

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

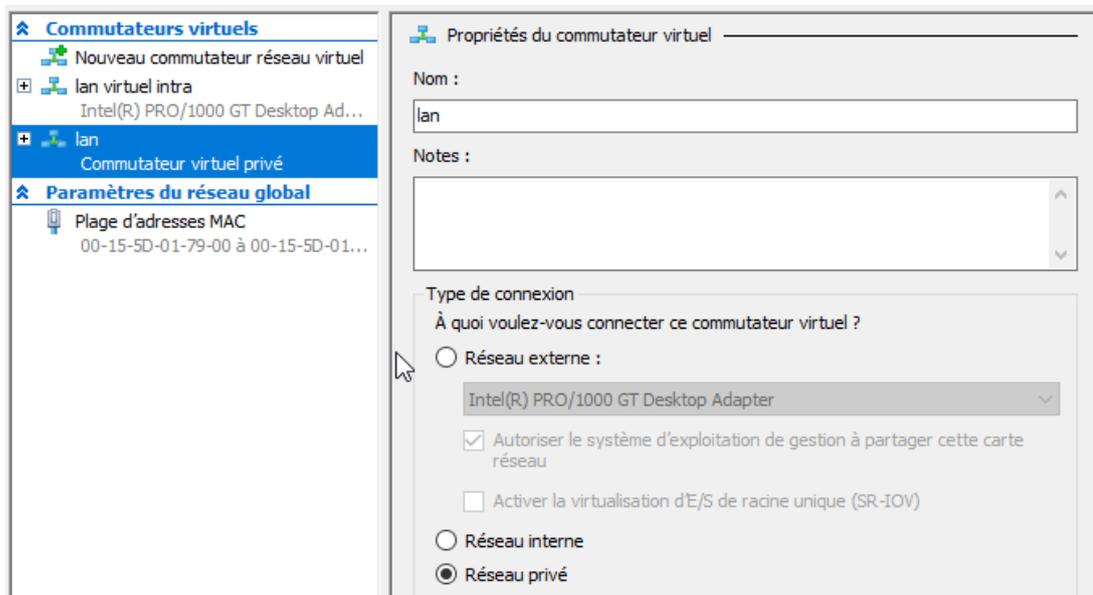


De manière à avoir au final 2 commutateurs réseaux

Ian virtuel intra – Externe -



Ian – privé

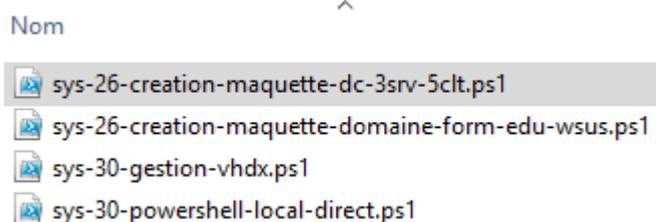


Utilisation d'un script Powershell

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

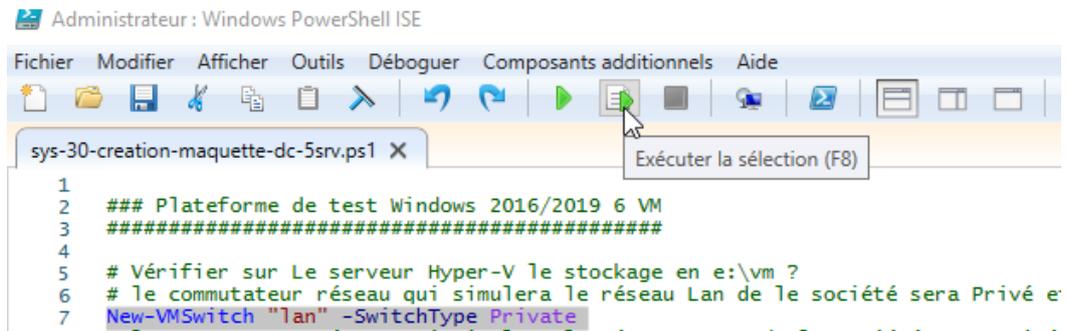
Le script à ouvrir via **Modifier** dans **PowershellISE** se nomme

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 créé les commutateurs réseau manuellement précédemment, dans notre machine physique, on peut les créer via le **script powershell**



```
Administrateur : Windows PowerShell ISE
Fichier Modifier Afficher Outils Débuguer Composants additionnels Aide
sys-30-creation-maquette-dc-5srv.ps1 X
1
2 ### Plateforme de test Windows 2016/2019 6 VM
3 #####
4
5 # Vérifier sur Le serveur Hyper-V le stockage en e:\vm ?
6 # le commutateur réseau qui simulera le réseau Lan de la société sera Privé e
7 New-VMSwitch "lan" -SwitchType Private
```

Création des disques de différenciation + Création vm

A la main :

Il faut copier le fichier vhdx « disque de base », nommé par exemple pour nous **serveur-2019-1tsc-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)

Nom	État
Vm-S1	Désactivé
Vm-S2	Désactivé
Vm-S3	Désactivé
Vm-S4	Désactivé

En powershell :

```
10 # le vhdx de depart en lecture seule est e:\vm\serveur-2019-1tsc-1809-datacenter-sysprep.vhdx
11 # Créer les disques de différenciation, et les vm dessus
12 for ($i = 1; $i -lt 5; $i++)
13 {
14     New-VHD -Differencing -Path e:\vm\vm-s$i.vhdx -ParentPath e:\vm\serveur-2019-1tsc-1809-datacenter-sysprep.vhdx
15     New-VM -Name Vm-S$i -MemoryStartupBytes 2048MB -SwitchName Lan -VHDPATH e:\vm\vm-s$i.vhdx -Generation 2
16 }
18 # Mémoire dynamique + 2 processeurs
19 Get-VM | Stop-VM
20 Get-VM | Set-VMemory -DynamicMemoryEnabled $True -MaximumBytes 4096MB -MinimumBytes 1024MB -StartupBytes 2048MB
21 Get-VM | Set-VMProcessor -Count 2
22 Get-VM | Start-VM
```

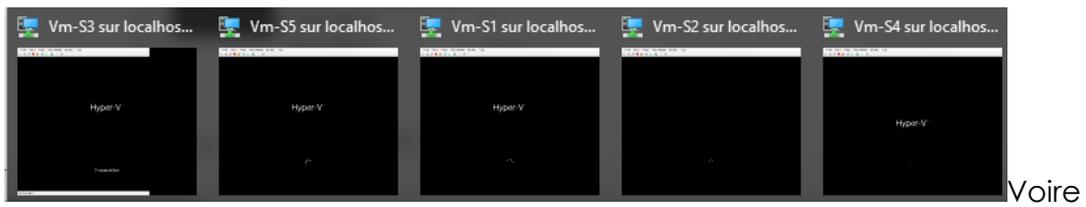
On refait la même chose pour les 5 clients avec fichier vhdx « disque de base », nommé par exemple pour nous **windows-10-20H2-sysprep.vhdx**.

Et au final on devrait avoir

Ordinateurs virtuels		
Nom	État	Utilisation d...
Vm-S1	Désactivé	
Vm-S2	Désactivé	
Vm-S3	Désactivé	
Vm-S4	Désactivé	
Vm-S5	Désactivé	
Vm-S6	Désactivé	
Vm-S7	Désactivé	
Vm-S8	Désactivé	
Vm-S9	Désactivé	

Phase OOBÉ des Vm

Il faut lancer les consoles



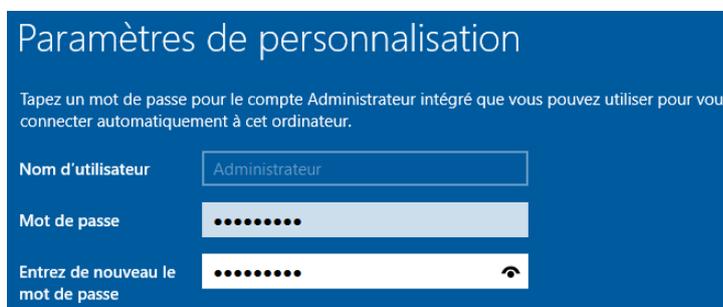
```
36 # ouverture Console de connection sur les VM
37 for ($i = 1; $i -lt 10; $i++)
38 {
39     $VmName = "VM-s"+$i
40     VmConnect localhost $VmName
41 }
```

A la main :

Les consoles étants lancés ; comme les machines sont syspréps, il faut les démarrer, et dérouler la phase OOBÉ (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

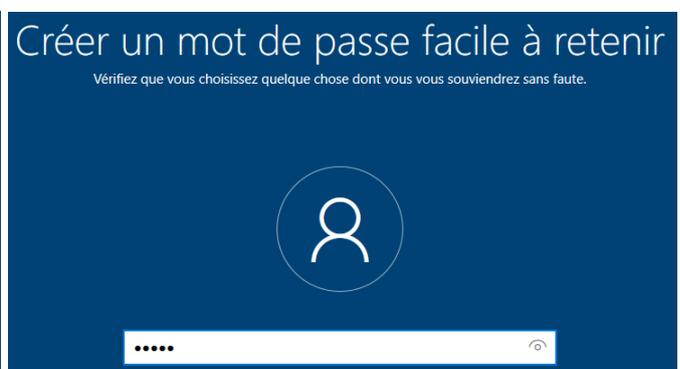
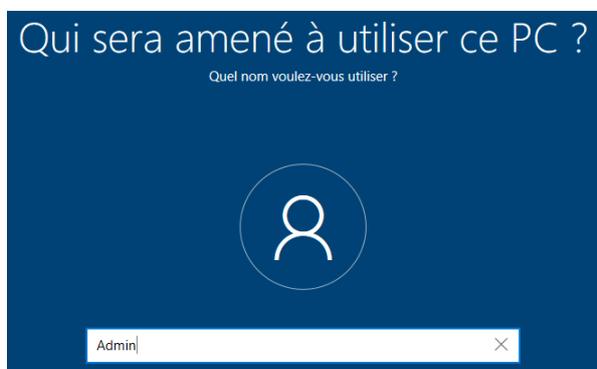
sur les Serveurs : **Administrateur / Local2019**

de VM-S1 à VM-S4



sur les client 10 : **Admin / Local**

de VM-S5 à VM-S9

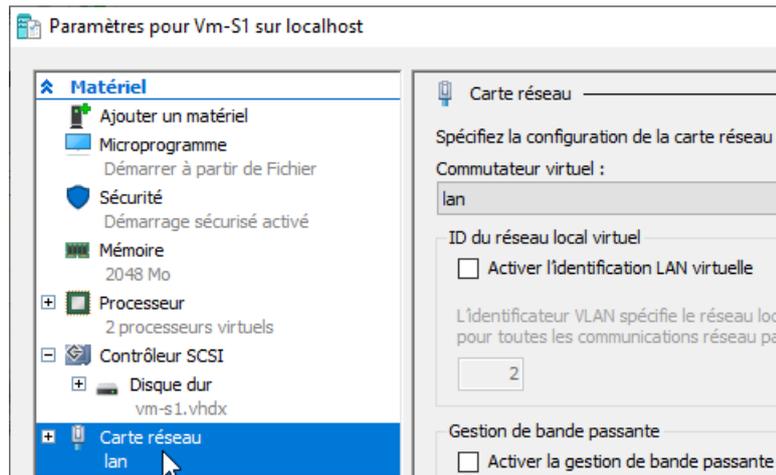


Sur les clients windows 10, on ignore le 2° clavier- pas d'internet- installation limitée, on répons 1-2-3 au questions de sécurité du mot de passe, et on répons de manière générale non partout, pas de cortana...

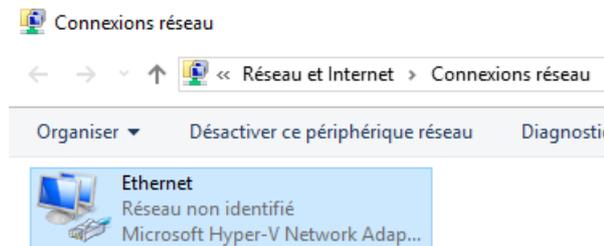


On peut ouvrir une session sur une Vm via **CTRL + ALT + FIN**

Chaque Vm devait avoir ses caractéristiques



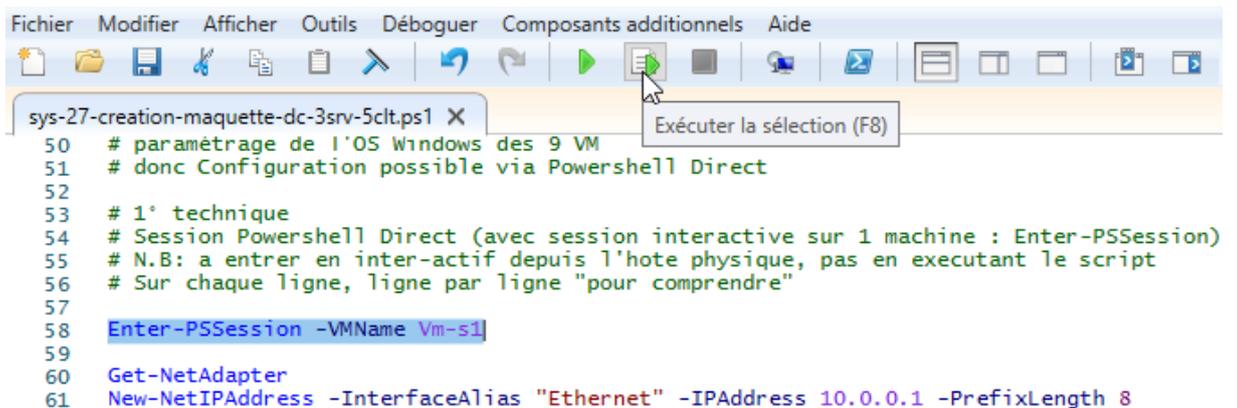
Et une carte réseau nommée **Ethernet** branchée sur le commutateur **lan**

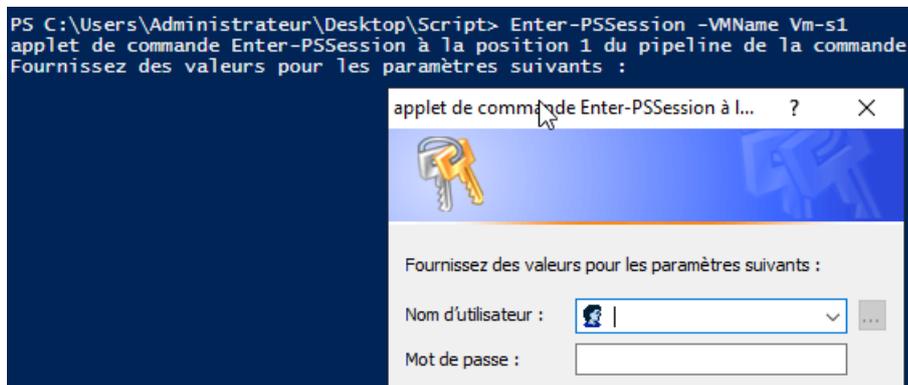


Configuration des OS-Windows et OS-Serveur dans les VM

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

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





Et ensuite les commandes powershell, en session interactive...

```

sys-27-creation-maquette-dc-3srv-5clt.ps1 X
55 # N.B: a entrer en inter-actif depuis l'ho...
56 # Sur chaque ligne, ligne par ligne "pour...
57
58 Enter-PSSession -VMName Vm-s1
59
60 Get-NetAdapter
61 New-NetIPAddress -InterfaceAlias "Ethernet" -IP...
62 Set-DnsClientServerAddress -InterfaceAlias "...
63 Get-NetFirewallRule *fps* | Format-Table Na...
64 Get-NetFirewallRule *fps* | Enable-NetFire...
65 Get-NetFirewallRule *fps* | Format-Table Na...
66 Powercfg -change -monitor-timeout-ac 0
67 Rename-Computer s1
68 Restart-Computer -Force
69
70

```

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

```

Fichier Modifier Afficher Outils Débugger Composants additionnels Aide
72 # 2° technique
73 # Session Powershell Direct (avec bloc de...
74 # Mémorisation des credentials à utiliser...
75 $password = ConvertTo-SecureString "Local2019" -AsPlainText -Force
76 $cred= New-Object System.Management.Automation.PSCredential ("administrateur", $password )
77
78 $password10 = ConvertTo-SecureString "Local" -AsPlainText -Force
79 $cred10= New-Object System.Management.Automation.PSCredential ("admin", $password10 )
80
81

```

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

```

81 # Serie de Invoke-Command "personnalisé" par VM
82 Invoke-Command -VMName Vm-s2 -Credential $cred -ScriptBloc{
83     New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.0.2 -PrefixLength 8
84     Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.1
85     Get-NetFirewallRule *fps* | Enable-NetFirewallRule
86     Powercfg -change -monitor-timeout-ac 0
87     Rename-Computer s2 -Restart}
88
89 Invoke-Command -VMName Vm-s3 -Credential $cred -ScriptBloc{
90     New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.0.3 -PrefixLength 8
91     Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.1
92     Get-NetFirewallRule *fps* | Enable-NetFirewallRule
93 }
94

```

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

```

# Option boucle pour gérer les 5 VM de 2 à 4 plutot que 5 block scriptblock
# avec passage de variable en paramètre dans le -scriptbloc via $Using:
for ($i = 2; $i -lt 5; $i++)
{
    Invoke-Command -VMName Vm-s$i -Credential $cred -ScriptBloc{
        New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.0.$Using:i -PrefixLength 8
        Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.1
        Get-NetFirewallRule *fps* | Enable-NetFirewallRule
        Powercfg -change -monitor-timeout-ac 0
        Rename-Computer s$Using:i -Restart}
}

```

Ou a la main :

- Il faut pour chaque OS Serveur, executer les opérations suivantes : par exemple pour S1
- 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) S1
- 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**

```
sys-27-creation-maquette-dc-3srv-5clt.ps1 X
160
161 # test du fonctionnement du réseau sur commutateur prive lan depuis S1
162 Invoke-Command -VMName Vm-s1 -Credential $cred -ScriptBlock {
163     Ping 10.0.0.2
164     Ping 10.0.0.3
165     Ping 10.0.0.4
166     Ping 10.0.0.5
167     Ping 10.0.0.6
168     Ping 10.0.0.7
169     Ping 10.0.0.8
170     Ping 10.0.0.9
171 }
```

A la main :

Ping...

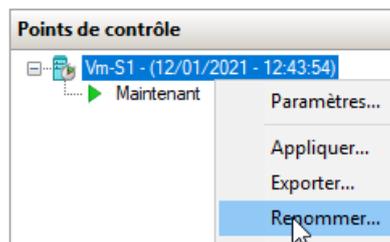
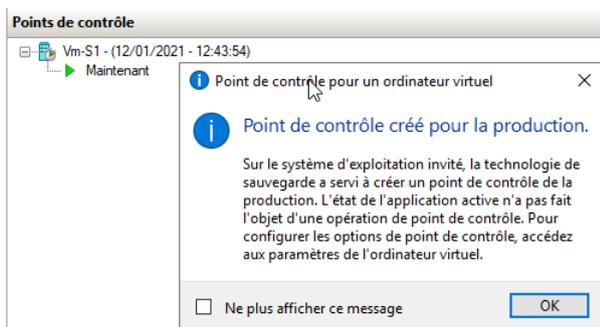
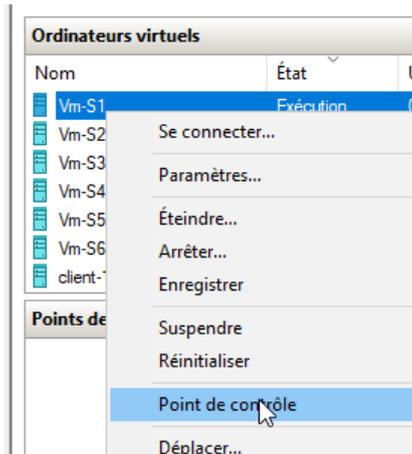
Snapshot base

Via Powershell

```

Administrateur : Windows PowerShell ISE
Fichier Modifier Afficher Outils Débugger Composants additionnels Aide
sys-30-creation-maquette-dc-5srv.ps1 X
126
127 # Crée un point de contrôle "Base"
128 #####
129 Get-VM | ? State -EQ Running | Checkpoint-VM -SnapshotName Base
130 Get-VM | ? Name -Like *Vm-S*
131 Get-VM | ? Name -Like *Vm-S* | Checkpoint-VM -SnapshotName Base
    
```

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



maquette de 70 Giga !

Nom	Modifié le	Type	Taille
serveur-2019-ltsc-1809-datacenter-sysprep.vhdx	06/01/2021 13:55	Fichier image de d...	15 994 880 ...
vm-s1.vhdx	22/05/2021 09:35	Fichier image de d...	2 494 464 Ko
vm-s1_EBD19D66-5EC2-4220-96D9-774D290D0CA8.avhdx	22/05/2021 09:38	Fichier AVHDX	233 472 Ko
vm-s2.vhdx	22/05/2021 09:35	Fichier image de d...	2 437 120 Ko
vm-s2_B008FB81-507B-4E9F-849D-63AA11F54DE5.avhdx	22/05/2021 09:38	Fichier AVHDX	200 704 Ko
vm-s3.vhdx	22/05/2021 09:35	Fichier image de d...	2 422 784 Ko
vm-s3_7ED88CB7-2BF4-4826-AC08-D2302169F833.avhdx	22/05/2021 09:38	Fichier AVHDX	200 704 Ko
vm-s4.vhdx	22/05/2021 09:35	Fichier image de d...	2 134 016 Ko
vm-s4_2FF94AF2-C99D-41AB-81A3-64342EDD0F1E.avhdx	22/05/2021 09:38	Fichier AVHDX	167 936 Ko
vm-s5.vhdx	22/05/2021 09:35	Fichier image de d...	4 688 896 Ko
vm-s5_C9491DFE-76CD-4D45-AEC4-1059A2423B31.avhdx	22/05/2021 09:38	Fichier AVHDX	430 080 Ko
vm-s6.vhdx	22/05/2021 09:35	Fichier image de d...	4 656 128 Ko
vm-s6_82F710D3-6CB1-45AC-8DB0-38F550EF7509.avhdx	22/05/2021 09:38	Fichier AVHDX	331 776 Ko
vm-s7.vhdx	22/05/2021 09:36	Fichier image de d...	4 721 664 Ko
vm-s7_DABBDf63-36A1-43FB-BC19-C7B0267211E9.avhdx	22/05/2021 09:38	Fichier AVHDX	266 240 Ko
vm-s8.vhdx	22/05/2021 09:36	Fichier image de d...	4 754 432 Ko
vm-s8_B8958817-2E52-46EF-8A4F-B45BA76419A2.avhdx	22/05/2021 09:38	Fichier AVHDX	331 776 Ko
vm-s9.vhdx	22/05/2021 09:36	Fichier image de d...	4 688 896 Ko
vm-s9_7BA00EF8-1EC7-42E9-B528-F64759AB080E.avhdx	22/05/2021 09:38	Fichier AVHDX	331 776 Ko
windows-10-20H2-sysprep.vhdx	08/01/2021 18:32	Fichier image de d...	25 530 368 ...

MONTAGE DOMAINE FORM.EDU

Objectif de la maquette form.edu

Dans un Serveur **Hyper-V** 2016-2019, sur lequel on a monté la maquette **1DC + 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

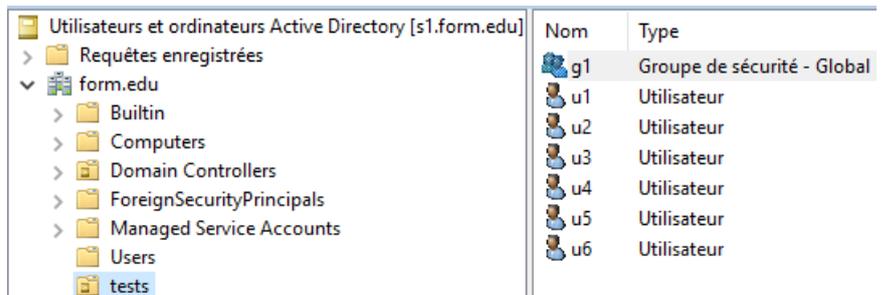
Le domaine se nomme **form.edu** Les adresse Ip de classe **A 10.0.0.x/255.0.0.0**

L' **Administrateur** du Domaine **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**

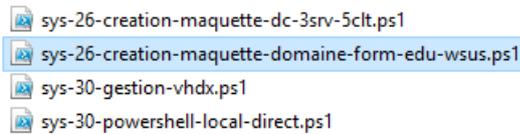


Nom	Type
g1	Groupe de sécurité - Global
u1	Utilisateur
u2	Utilisateur
u3	Utilisateur
u4	Utilisateur
u5	Utilisateur
u6	Utilisateur

Utilisation d'un script Powershell

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

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

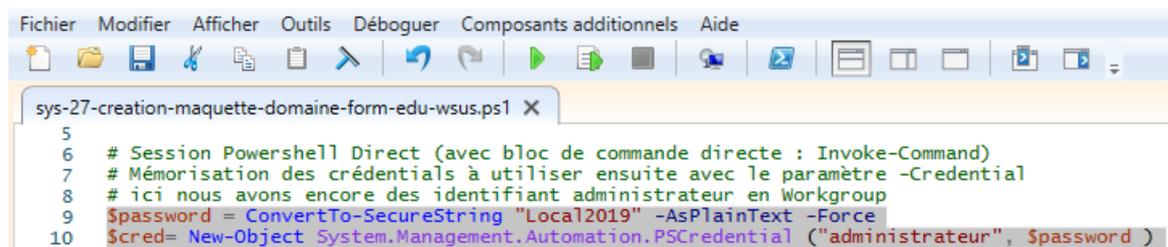


On se placera sur les lignes voulues, et on demandera de les exécuter

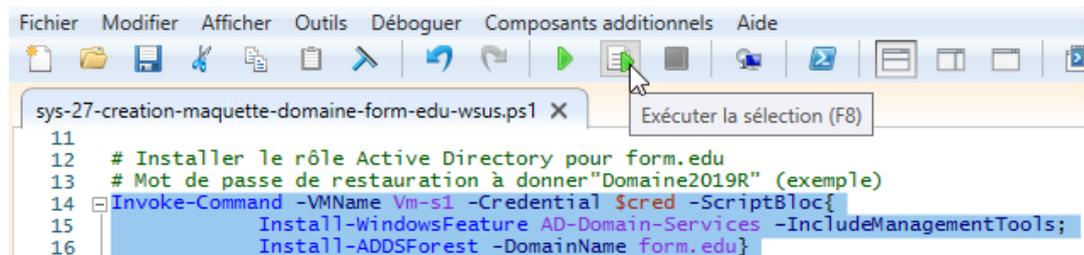
Création Domaine – sur Vm-s1

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

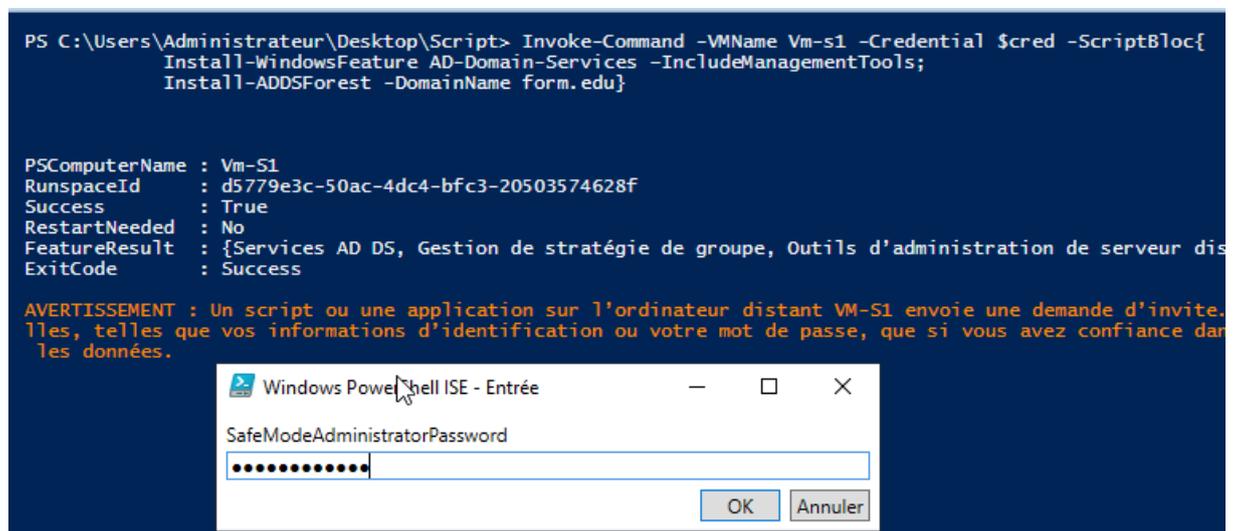
Via Powershell ISE, depuis le serveur Hyper-V (machine physique) on peut, s'authentifier avec le login local (puisque l'on est en workgroup)

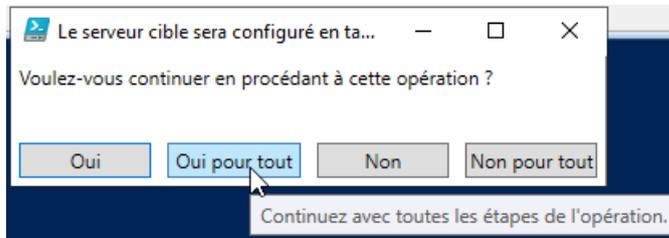


Et demander de monter un domaine **form.edu** sur **Vm-S1**



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





Confirmer

```

PSComputerName : Vm-S1
RunspaceId      : ae0fce40-976c-4699-890c-6bdad75cf40d
Message         : L'opération s'est déroulée avec succès.
Context         : DCPromo.General.3
RebootRequired  : False
Status          : Success
  
```

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 ...

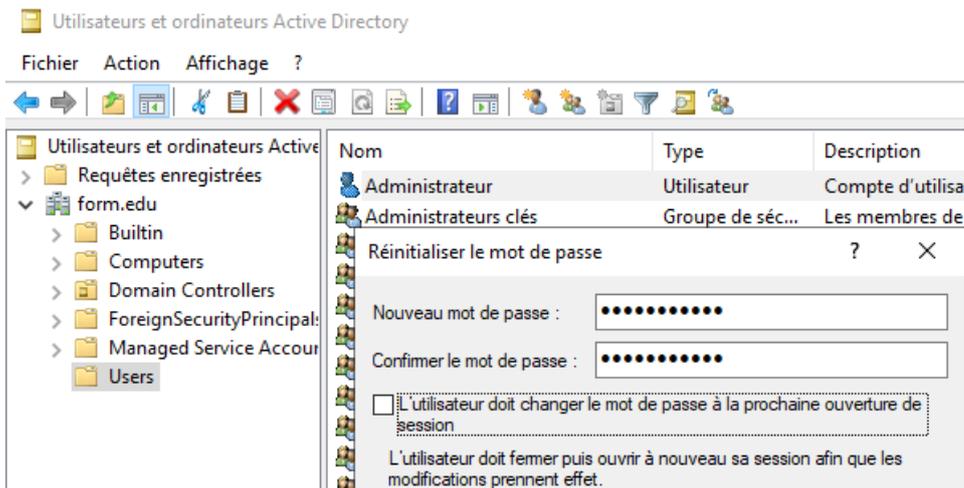
Le compte **Administrateur local** : **Administrateur / Local2019**

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 snapshot 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 snapshot si on y est arrivé

BUG Serveur Windows DC sur SSD

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

Nom de l'ordinateur	s1	Nom de l'ordinateur	s1
Domaine	form.edu	Domaine	form.edu
Pare-feu Windows Defender	Public : Actif	Pare-feu Windows Defender	Domaine : Actif

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

```
26 # Corriger le bug du pare-feu CD sur SSD
27 Invoke-Command -VMName Vm-S1 -Credential $cred -ScriptBlock{Restart-NetAdapter Ethernet}..
```

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

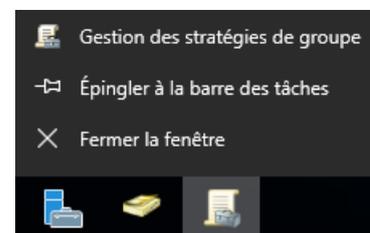
Il serait bon d'épingler sur la Barre des Taches quelques consoles :

Gestion de Serveur

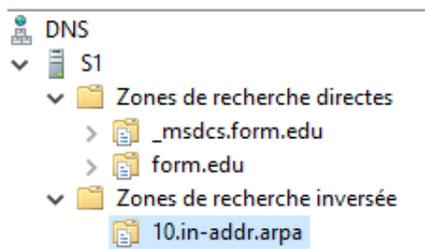
Utilisateurs et ordinateurs Active Directory

Gestion des Stratégies de groupe

Dns



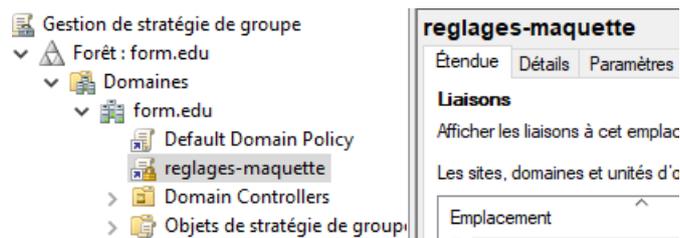
Création zone DNS inversée principale 10.0.0.1



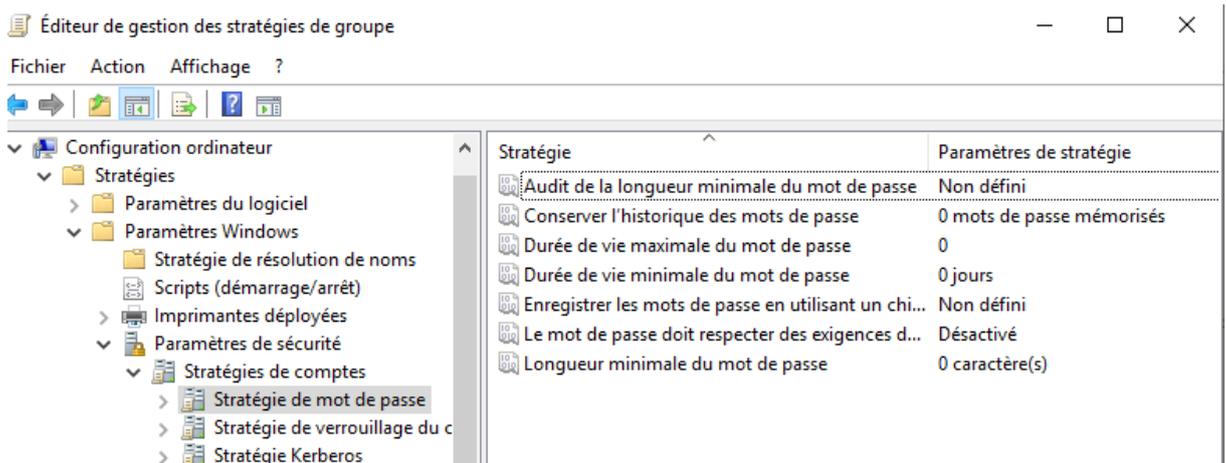
Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[1], s1.form.edu
(identique au dossier parent)	Serveur de noms (NS)	s1.form.edu.
10.0.0.1	Pointeur (PTR)	s1.form.edu

GPO mot de passe et pare feu

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

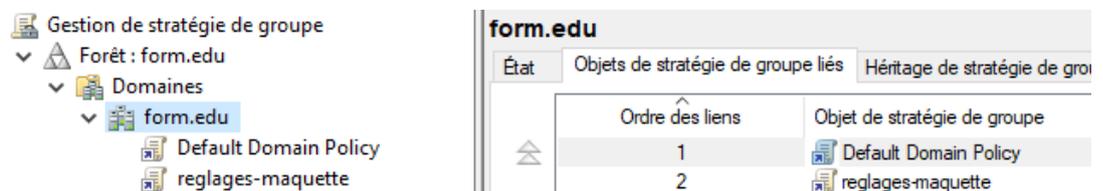


Mots de Passe Complexe

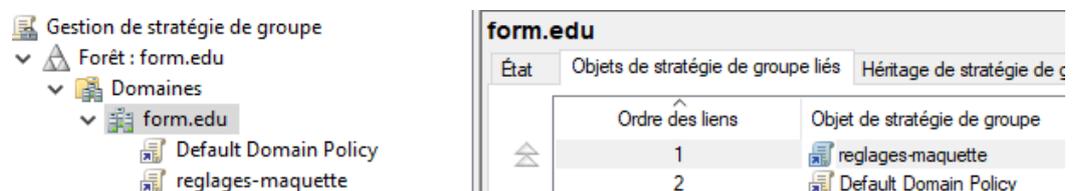


Mais l'ordre du coup ne convient pas, car dans la stratégie Default domain Policy un réglage est demandé, concernant ces mots de passe

Donc de cette situation,

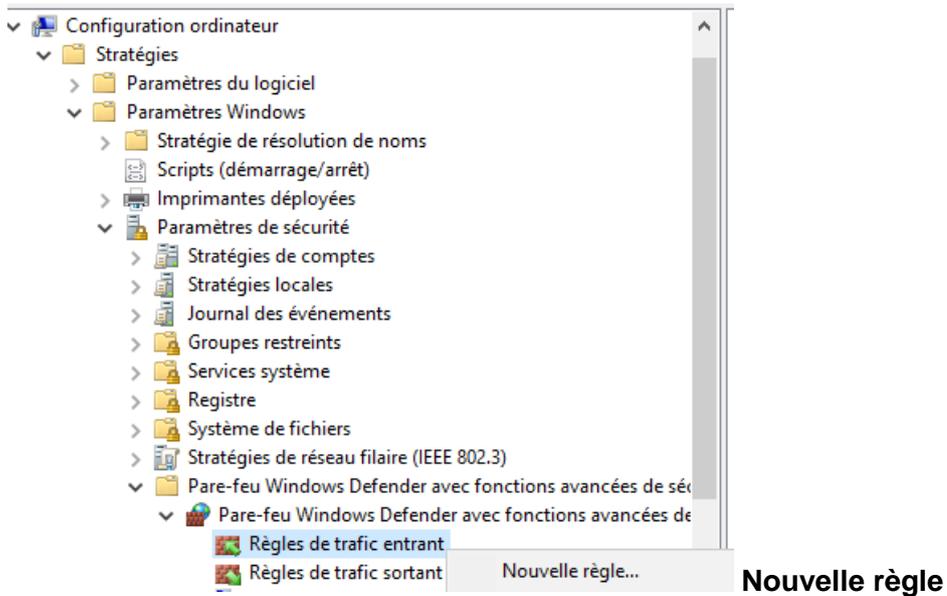


Il faut passer à



Règle du pare-feu

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



Assistant Nouvelle règle de trafic entrant

Type de règle

Sélectionnez le type de règle de pare-feu à créer.

Étapes :

- Type de règle
- Règles prédéfinies
- Action

Quel type de règle voulez-vous créer ?

Programme
Règle qui contrôle les connexions d'un programme.

Port
Règle qui contrôle les connexions d'un port TCP ou UDP.

Prédéfinie :
Partage de fichiers et d'imprimantes
Règle qui contrôle les connexions liées à l'utilisation de Windows.

Personnalisée
Règle personnalisée.

Assistant Nouvelle règle de trafic entrant

Règles prédéfinies

Sélectionner les règles à créer pour cette utilisation.

Étapes :

- Type de règle
- Règles prédéfinies
- Action

Quelles règles voulez-vous créer ?

Les règles suivantes définissent les besoins en connectivité réseau pour le groupe prédéfini sélectionné. Les règles qui sont cochées seront créées. Si une règle cochée existe déjà, son contenu sera remplacé.

Règles :

Nom	La règle existe...	Profil	Desc
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (LLMNR-...	Non	Tout	Règle
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Demand...	Non	Tout	Les n
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Demand...	Non	Tout	Les n
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (Service ...	Non	Tout	Règle
<input checked="" type="checkbox"/> Partage de fichiers et d'imprimantes (service S	Non	Tout	Règle

Action

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

Étapes :

- Type de règle
- Règles prédéfinies
- Action

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

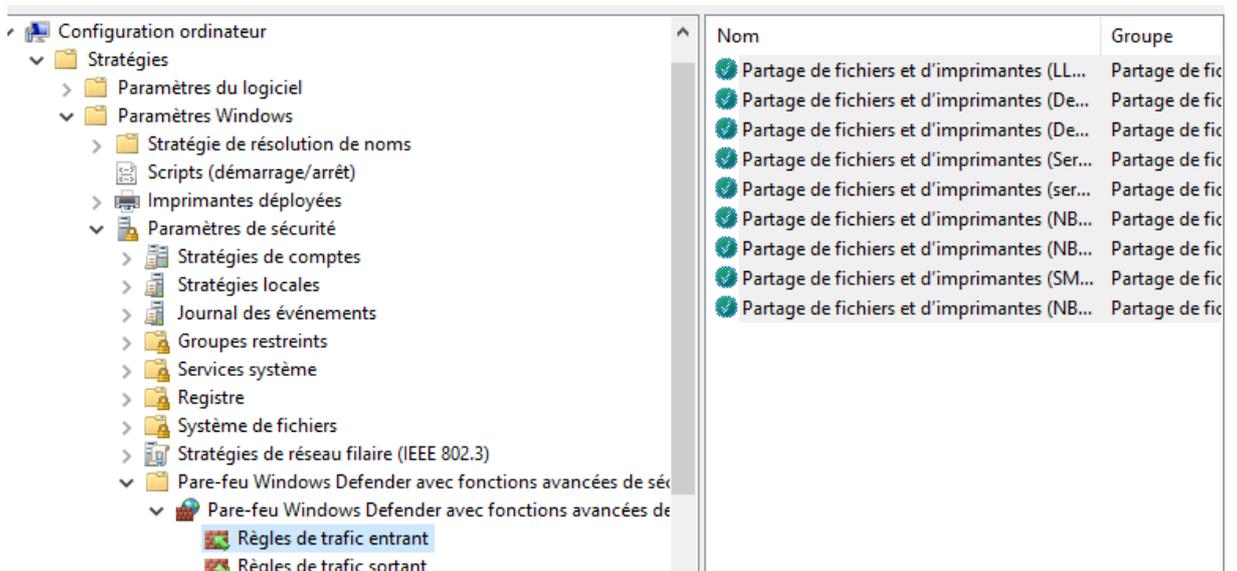
Autoriser la connexion
Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

Autoriser la connexion si elle est sécurisée
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

Bloquer la connexion

Personnaliser...

Pour obtenir



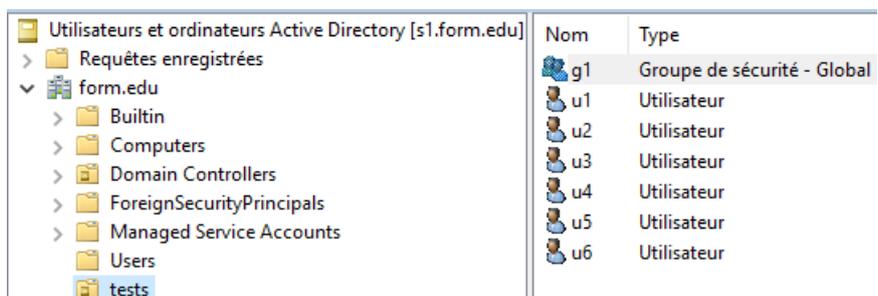
On referme la **Console des GPO** et on applique au serveur **Gpupdate / force**

```
C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
```

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

```
sys-27-creation-maquette-domaine-form-edu-wsus.ps1 X
42 # Intégrer les serveurs au domaine
43 # il faut depuis chaque serveur à intégrer, en tant que administrateur local faire une demande avec u
44 # c'est donc un paramétrage de l'OS Windows des 5 VM
45 # donc Configuration possible via Powershell Direct
46 # Session Powershell Direct (avec session interactive sur 1 machine : Enter-PSSession)
47 # N.B: a entrer en inter-actif ligne par ligne, depuis l'hote physique, pas en executant le script
48 # Sur chaque ligne, ligne par ligne "pour comprendre"
49 # Rappel $cred =authentification locale $credom =authentification de domaine
50
51 Enter-PSSession -VMName Vm-s2 -Credential $cred
52 hostname
53 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
54 # normalement il faudrait faire un exit, mais comme le serveur a redémarré, notre session est finie
55 #Exit
```

On ouvre la session avec une authentification locale

```
PS C:\Users\Administrateur\Desktop> Script> Enter-PSSession -VMName Vm-s2 -Credential $cred
[Vm-S2] : PS C:\Users\administrateur\Documents>
```

On est bien loggué en tant qu'administrateur local

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

```
[Vm-S2] : PS C:\Users\administrateur\Documents> hostname
s2
```

On lance l'adhésion au domaine

```
Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
```

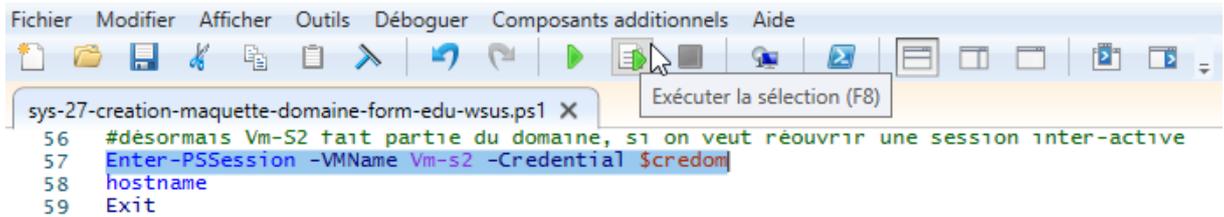
Le poste S2 redémarre, on peut vérifier dans le **gestionnaire de serveur** de S2 qu'il appartient bien au domaine form.edu



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

```
PS C:\Users\Administrateur\Desktop\Script> Enter-PSSession -VMName Vm-s2 -Credential $cred
Enter-PSSession : Les informations d'identification ne sont pas valides.
```

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

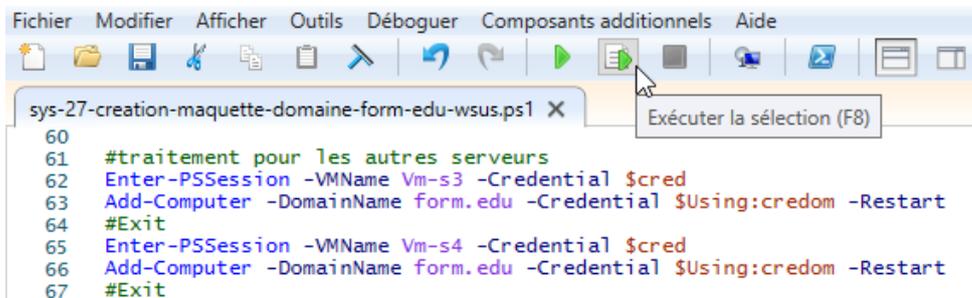


```
Fichier Modifier Afficher Outils Débugger Composants additionnels Aide
sys-27-creation-maquette-domaine-form-edu-wsus.ps1 X Exécuter la sélection (F8)
56 #désormais Vm-S2 fait partie du domaine, si on veut réouvrir une session inter-active
57 Enter-PSSession -VMName Vm-s2 -Credential $credom
58 hostname
59 Exit
```

```
PS C:\Users\Administrateur\Desktop\Script> Enter-PSSession -VMName Vm-s2 -Credential $credom
[VM-S2] : PS C:\Users\administrateur.FORM\Documents> |
```

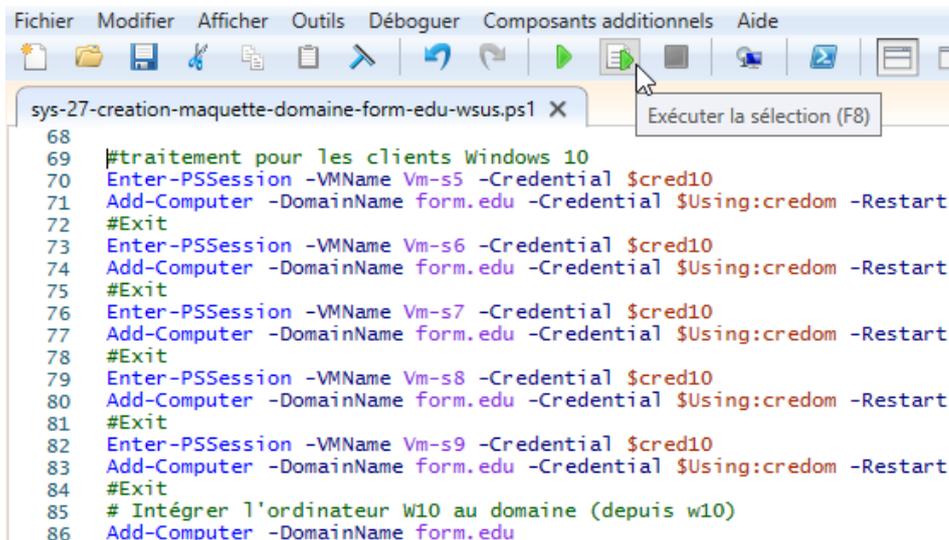
On est bien loggué en tant qu'administrateur de domaine.form

Adhésion des autres Vm



```
Fichier Modifier Afficher Outils Débugger Composants additionnels Aide
sys-27-creation-maquette-domaine-form-edu-wsus.ps1 X Exécuter la sélection (F8)
60 #traitement pour les autres serveurs
61 Enter-PSSession -VMName Vm-s3 -Credential $cred
62 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
63 #Exit
64 Enter-PSSession -VMName Vm-s4 -Credential $cred
65 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
66 #Exit
```

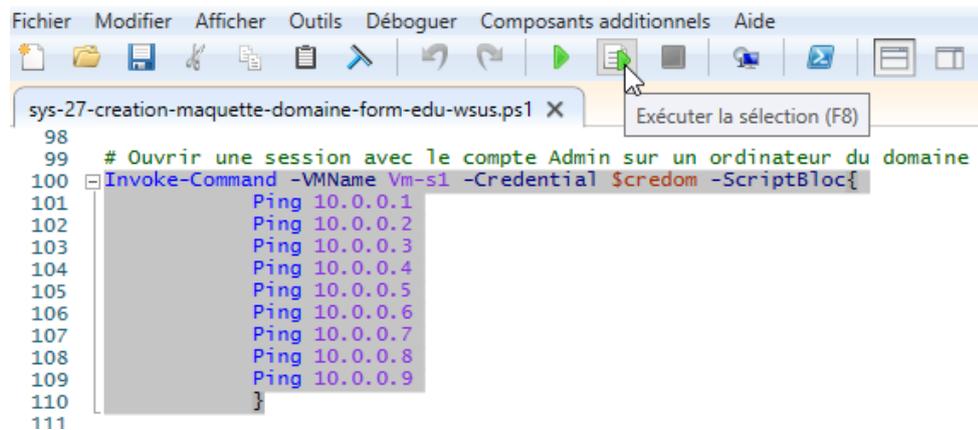
Et



```
Fichier Modifier Afficher Outils Débugger Composants additionnels Aide
sys-27-creation-maquette-domaine-form-edu-wsus.ps1 X Exécuter la sélection (F8)
68 #traitement pour les clients Windows 10
69 Enter-PSSession -VMName Vm-s5 -Credential $cred10
70 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
71 #Exit
72 Enter-PSSession -VMName Vm-s6 -Credential $cred10
73 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
74 #Exit
75 Enter-PSSession -VMName Vm-s7 -Credential $cred10
76 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
77 #Exit
78 Enter-PSSession -VMName Vm-s8 -Credential $cred10
79 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
80 #Exit
81 Enter-PSSession -VMName Vm-s9 -Credential $cred10
82 Add-Computer -DomainName form.edu -Credential $Using:credom -Restart
83 #Exit
84 # Intégrer l'ordinateur W10 au domaine (depuis w10)
85 Add-Computer -DomainName form.edu
```

Test IP depuis le DC sur Vm-S1

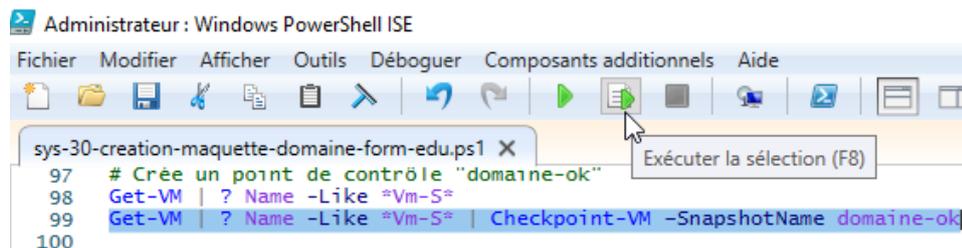
il faut depuis par exemple le serveur **DC S1** dans la **Vm-s1** tester un ping sur tous les serveurs membre du domaine, (vérification réseau lan et gestion des pare-feu / GPO)



```
sys-27-creation-maquette-domaine-form-edu-wsus.ps1 X
98
99 # Ouvrir une session avec le compte Admin sur un ordinateur du domaine
100 Invoke-Command -VMName Vm-s1 -Credential $credom -ScriptBloc{
101     Ping 10.0.0.1
102     Ping 10.0.0.2
103     Ping 10.0.0.3
104     Ping 10.0.0.4
105     Ping 10.0.0.5
106     Ping 10.0.0.6
107     Ping 10.0.0.7
108     Ping 10.0.0.8
109     Ping 10.0.0.9
110 }
111
```

Snapshot Domaine-ok

Via Powershell



```
Administrateur : Windows PowerShell ISE
Fichier Modifier Afficher Outils Débuguer Composants additionnels Aide
sys-30-creation-maquette-domaine-form-edu.ps1 X
97 # Crée un point de contrôle "domaine-ok"
98 Get-VM | ? Name -Like *Vm-S*
99 Get-VM | ? Name -Like *Vm-S* | Checkpoint-VM -SnapshotName domaine-ok
100
```

Désormais toutes nos Vm ont un deuxième point de contrôle

Ordinateurs virtuels			
Nom	État	Utilisation d...	Mémoire affectée
Vm-S1	Exécution	4 %	1382 Mo
Vm-S2	Exécution	0 %	996 Mo
Vm-S3	Exécution	0 %	994 Mo
Vm-S4	Exécution	0 %	1060 Mo
Vm-S5	Exécution	0 %	1012 Mo
Vm-S6	Exécution	0 %	706 Mo

Points de contrôle	
Base	domaine-ok
	Maintenant

Ordinateurs virtuels	
Nom	État
Vm-S1	Exécution
Vm-S2	Exécution
Vm-S3	Exécution
Vm-S4	Exécution
Vm-S5	Exécution
Vm-S6	Exécution

Points de contrôle	
Base	domaine-ok
	Maintenant

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

```
115
116 ### Restore un point de contrôle nommé « Base »
117 Get-VM | Restore-VMSnapshot -Name Base -Confirm:$false
```