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
Stockage	4
Cartes Réseau	4
Commutateurs Réseau virtuels	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	
SNAPSHOOT BASE	11
MONTAGE DOMAINE FORM.EDU	12
OBJECTIF DE LA MAQUETTE FORM.EDU	12
UTILISATION D'UN SCRIPT POWERSHELL	
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
Création zone DNS invérsée principale 10.0.0.1	
GPO mot de passe et pare feu	
INTEGRATION DES 3 VM SERVEUR ET 5 VM CLIENT AU DOMAINE	19
Adhésion détaillée pour s2	
Adhésion des autres Vm	
TEST IP DEPUIS LE DC SUR VM-S1	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 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. <u>C'est le seul accès réseau physique</u> <u>disponible</u>. Il est indispensable à la maquette pour la récupération des mises à jour sur le Site de Microsoft.

		Nom : an Notes :
On créera au minimum 1 (réseaux virtuel privé nommé lan	Commutateur	Local network réseau de "production" de la maquette
Ian Commutateur virtuel privé		Type de connexion À quoi voulez-vous connecter ce commutateur virtue O Réseau externe :
		Intel(R) PRO/1000 GT Desktop Adapter Autoriser le système d'exploitation de gestio réseau
		Activer la virtualisation d'E/S de racine uniqu Réseau interne Réseau privé



🚜 Propriétés du commutateur virtuel -

De manière à avoir au final 2 commutateurs réseaux

lan virtuel intra – Externe -



lan – privé

Commutateurs virtuels	🛃 Propriétés du commutateur virtuel —	-
 Nouveau commutateur réseau virtuel Intel(R) PRO/1000 GT Desktop Ad 	Nom :	٦
 Jan Commutateur virtuel privé 	Notes :	
Paramètres du réseau global Plage d'adresses MAC 00-15-5D-01-79-00 à 00-15-5D-01	Type de connexion À quoi voulez-vous connecter ce commutateur virtuel ?	
	Intel(R) PRO/1000 GT Desktop Adapter Autoriser le système d'exploitation de gestion à partager cette carte réseau Activer la virtualisation d'E/S de racine unique (SR-IOV) Réseau interne Réseau 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

Nom

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

- sys-26-creation-maquette-domaine-form-edu-wsus.ps1
- sys-30-gestion-vhdx.ps1
- sys-30-powershell-local-direct.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)

👘 vm-s i	Desactive
Vm-S2	Désactivé
🗧 Vm-S3	Désactivé
Vm-S4	Désactivé

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

0	Ordinateurs virtuels				
Nom		État	Utilisation d 1		
-	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			



https://www.cabare.net Pr - Michel Cabaré -

Phase OOBE des Vm

Il faut lancer les consoles

🔄 Vm-S3 sur localhos	🔄 Vm-S5 sur localhos	🖳 Vm-S1 sur localhos	🜉 Vm-S2 sur localhos	🔄 Vm-S4 sur local	hos
Hyper-V	Hyper-V*	Hypar V*		Hyper-V"	
	~	<u>.</u>			
					Voire
🕎 Vm-S9 sur localhost 👳 Vm-S6 su	ur localhost 🕎 Vm-S4 sur localhost	🕎 Vm-S3 sur localhost 🕎 Vm-S5	sur localhost 🛛 🕎 Vm-S8 sur localhost	🕎 Vm-S2 sur localhost 🚦	👳 Vm-S1 sur localhost 📜 Vm-S7 sur localhost
	100 (00) 100 (000 (0) -●*** + ●**			The late two page in the second seco	The case was and a set of the case of the
	en en et al anna de la construcción de la construcción de la construcción de la construcción de la construcción en el construcción de la construcción en el construcción de la construcción en el construcción de la construcc		e and The Signature and Signature Sector and Antonionis Sector Signature Sector	Augustanting of a finite set for a set	
■				la hanan an	
36 # ouvertur	re Console de cor	nection sur les	VM		
38 ⊡ { 39 \$VmNar	me = "VM-s"+\$i				
40 VmCon 41 }	nect localhost \$\	/mName			



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



de VM-S1 à VM-S4



sur les client 10 : Admin / Local





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

🚰 Paramètres pour Vm-S1 sur localhost	
Matériel Ajouter un matériel Microprogramme Démarrer à partir de Fichier Sécurité Démarrage sécurisé activé Mémoire 2048 Mo	Carte réseau Spécifiez la configuration de la carte réseau Commutateur virtuel : lan ID du réseau local virtuel Activer l'identification LAN virtuelle
 Processeur 2 processeurs virtuels Contrôleur SCSI Disque dur vm-s1.vhdx Carte réseau lan 	L'identificateur VLAN spécifie le réseau loc pour toutes les communications réseau pa 2 Gestion de bande passante Activer la gestion de bande passante

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)

Fichier	Modifier Afficher Outils Déboguer Composants additionnels Aide
1	▶ 🖬 🐇 🛍 ≻ ┛ ┍▫ ▶ 📭 🔳 👁 🛛 🗆 🖻 🖬
sys-27	/-creation-maquette-dc-3srv-5clt.ps1 X
50	# paramétrage de l'OS Windows des 9 VM
51	# donc Configuration possible via Powershell Direct
52	
53	# 1° technique
54	# Session Powershell Direct (avec session interactive sur 1 machine : Enter-PSSession)
55	# N.B: a entrer en inter-actif depuis l'hote physique, pas en executant le script
56	# Sur chaque ligne, ligne par ligne "pour comprendre"
57	
58	Enter-PSSession -VMName Vm-s1
59	
60	Get-NetAdapter
61	New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.0.1 -PrefixLength 8





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

1	🛎 🖬 🐇 🗈 🔉 🔍 🔍 🕨 💽 🖬 🖓 🕲 🔚 🗂 🗂 🛍
sys-	7-creation-maquette-dc-3srv-5clt.ps1 X Exécuter la sélection (F8)
55	# N.B: a entrer en inter-actif depuis l'hote physique, pas en executant le script
5(# Sur chaque ligne, ligne par ligne "pour comprendre"
57	
58	Enter-PSSession -VMName Vm-s1
59	
60	Get-NetAdapter
61	New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.0.1 -PrefixLength 8
62	Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.1
63	Get-NetFirewallRule *fps* Format-Table Name,Enabled
64	Get-NetFirewallRule *fps* Enable-NetFirewallRule
65	Get-NetFirewallRule *fps* Format-Table Name,Enabled
6	Powercfg -change -monitor-timeout-ac 0
67	Rename-Computer s1
68	Restart-Computer -Force

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 Déboguer Composants additionnels Aide
1 🖆) 🔒 🐇 🕒 🔈 🔍 🕨 💽 🔳 🐼 🖉 🗐 🗖 🗖 🖉 📮
sys-27-	creation-maquette-dc-3srv-5clt.ps1 X
72	# 2° technique
73	# Session Powershell Direct (avec bloc de commande directe : Invoke-Command)
74	# Mémorisation des crédentials à utiliser ensuite avec le paramètre -Credential
75	spassword = ConvertTo-SecureString "Local2019" -ASPlainText -Force
76	<pre>\$cred= New-Object System.Management.Automation.PSCredential ("administrateur", \$password)</pre>
77	
78	<pre>\$password10 = ConvertTo-SecureString "Local" -AsPlainText -Force</pre>
79	<pre>\$cred10= New-Object System.Management.Automation.PSCredential ("admin", \$password10)</pre>
-	

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

81 82 83 84 85 86 87	# 	<pre>Serie de Invoke-Command "personnalisé" par VM Invoke-Command -VMName Vm-s2 -Credential \$cred -ScriptBloc{ New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 10.0.0.2 -PrefixLength 8 Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses 10.0.0.1 Get-NetFirewallRule *fps* Enable-NetFirewallRule Powercfg -change -monitor-timeout-ac 0 Rename-Computer s2 -Restart}</pre>
88	-	
89	-	Invoke-Command -VMName Vm-s3 -Credential <mark>\$cred</mark> -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 *fns* Enable-NetFirewallRule

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

PROPRIÉTÉS Pour WIN-75FIHT87293		devient	
Nom de l'ordinateur	WIN-7SFIHT87293	PROPRIÉTÉS Pour s1	
Groupe de travail	WORKSROOP	Nom de l'ordinateur Groupe de travail	s1 WORKGROUP
Pare-feu Windows Defender	Public : Actif		
Gestion à distance	Activé	Pare-feu Windows Defende	er Public : Actif
Bureau à distance	Désactivé	Gestion à distance	Activé
Association de cartes réseau	Désactivé	Bureau à distance	Désactivé
Ethernet	Adresse IPv4 attribuée par DHCP, Compatible IPv¶r	Association de cartes résea	u Désactivé
Devient		Ethernet	10.0.0.1, Compatible IPv6

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**



Ping...



Snapshoot base

Via Powershell

🛃 Admi	nistrateur : Wind	ows PowerShell ISE			
Fichier	Modifier Affic	her Outils Débe	oguer Comp	osants additionnels	Aide
1 🗖	1 🔒 🖌	ĥ İ 入	2	Image:	🐅 🔼 E
sys-30-	-creation-maque	tte-dc-5srv.ps1 🗙		Exécuter la	a sélection (F8)
126	# Crée un n	oint de contrá	ile "Base"		
128	#############	#######################################	*##########		
129	Get-VM ?	State -EQ Runn	ning Chec	kpoint-VM -Snap	oshotName Base
130	Get-Vm ?	Name -Like *Vr	n−S*		
131	Get-VM ?	Name -Like *Vn	∥-S* Chec	kpoint-VM -Snap	oshotName Base

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

Ordinateurs	virtuels					
Nom		État L				
Vm-S1		Exécution 0				
Vm-S2	Se connec	cter	Points de contrôle			
Vm-S3	Paramètre	25	⊡	1/2021 - 12:43:54)		
Vm-S4	Étaindra		Maintenan	t Doint de contrêle pou	ır un ordinateur virtuel	×
- vm-55	Arrâtar				nêle enéé nevrole nonedriet	
client-1	Arreter				role cree pour la producti	on.
Delate de	Enregistre			Sur le système d' sauvegarde a sen	exploitation invité, la technologie /i à créer un point de contrôle de	de la
onts de	Suspendre	e		production. L'éta l'objet d'une opé	t de l'application active n'a pas fa ration de point de contrôle. Pour	it
	Réinitialis	er		configurer les op aux paramètres d	tions de point de contrôle, accéd e l'ordinateur virtuel.	ez
	Point de c	:on vôle				
	Déplacer.	ν <u>γ</u>		Ne plus afficher ce r	nessage OK	
	- cprocern		I			
ints de con	trôle					
🖳 📷 Vm-S1	- (12/01/202	21 - 12:43:54)				
🕨 Ma	intenant	Paramètres				
		Appliquer	Points do con	trâlo		
		Appriquer	romts de con	luole		
		Exporter	⊟… 📷 Base			
		Kenommer	: > Ma	aintenant MC	quette de 70 C	Giaa !
Nom				Madifiéla	Turne	Taille
NOTT				Modifie le	туре	Tallie
🕳 servei	ur-2019-ltsc	-1809-datacenter-sysprep	o.vhdx	06/01/2021 13:55	Fichier image de d	15 994 880
🕳 vm-s1	1.vhdx	15		22/05/2021 09:35	Fichier image de d	2 494 464 k
📄 vm-s1	1_EBD19D66	5-5EC2-4220-96D9-774D29	00D0CA8.avhdx	22/05/2021 09:38	Fichier AVHDX	233 472 1
🕳 vm-s2	2.vhdx			22/05/2021 09:35	Fichier image de d	2 437 120 k
📄 vm-s2	2_B008FB81-	-507B-4E9F-849D-63AA11	F54DE5.avhdx	22/05/2021 09:38	Fichier AVHDX	200 704 k
🕳 vm-s	3.vhdx			22/05/2021 09:35	Fichier image de d	2 422 784 K
🗋 vm-s	3_7ED88CB7	-2BF4-4826-AC08-D2302	169F833.avhdx	22/05/2021 09:38	Fichier AVHDX	200 704 k
🕳 vm-s4	4.vhdx			22/05/2021 09:35	Fichier image de d	2 134 016 K
📄 vm-s4	4_2FF94AF2-	-C99D-41AB-81A3-64342E	DD0F1E.avhdx	22/05/2021 09:38	Fichier AVHDX	167 936 K
🕳 vm-s	5.vhdx			22/05/2021 09:35	Fichier image de d	4 688 896 k
📄 vm-s	5_C9491DFE	-76CD-4D45-AEC4-1059A	2423B31.avhdx	22/05/2021 09:38	Fichier AVHDX	430 080 k
🕳 vm-st	5.vhdx			22/05/2021 09:35	Fichier image de d	4 656 128 k
📄 vm-st	5_82F710D3-	-6CB1-45AC-8DB0-38F55(0EF7509.avhdx	22/05/2021 09:38	Fichier AVHDX	331 776 K
🕳 vm-sī	7.vhdx			22/05/2021 09:36	Fichier image de d	4 721 664 k
📄 vm-s	7_DABBDF63	3-36A1-43FB-BC19-C7B02	267211E9.avhdx	22/05/2021 09:38	Fichier AVHDX	266 240 k
🕳 vm-s8	3.vhdx			22/05/2021 09:36	Fichier image de d	4 754 432 k
🗋 vm-s8	8_B8958817-	2E52-46EF-8A4F-B45BA7	6419A2.avhdx	22/05/2021 09:38	Fichier AVHDX	331 776 k
🕳 vm-s	9.vhdx			22/05/2021 09:36	Fichier image de d	4 688 896 k
vm-ss	9_7BA00EF8	-1EC7-42E9-B528-F64759/	AB080E.avhdx	22/05/2021 09:38	Fichier AVHDX	331 776 k



Hyper-V maquette 1dc 3 srv 5 clt - SYS 26 - GPO - ver 1.00 -

- Michel Cabaré -

https://www.cabare.net

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 lp 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

Utilisateurs et ordinateurs Active Directory [s1.form.edu]	Nom	Туре
✓ ∰ form.edu	8 g1	Groupe de sécurité - Global
> 📋 Builtin	💑 u1 <u>Å</u> u2	Utilisateur Utilisateur
Computers Demain Controllers	📥 u3	Utilisateur
ForeignSecurityPrincipals	📥 u4	Utilisateur
> Managed Service Accounts	💑 u5	Utilisateur
Users	💍 uo	Utilisateur
a tests		



https://www.cabare.net - Michel Cabaré -

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)

Fichier	Modifier	Afficher	Outils	Déboguer	Composant	ts additi	ionnels	Aide					
1	<u>ا</u>	🖌 🗳	Ū	> 7	6			9				2	Ŧ
sys-27	-creation-	maquette-c	domaine	e-form-edu-w	/sus.ps1 🗙								
5													
6	# Sess	ion Powe	rshel	l Direct (avec bloc	de co	mmande	direct	e : Invok	e-Con	nmand)		
7	# Mémo	risation	des (crédential	s à utilis	er en	suite	avec le	paramètr	e -Cr	edential		
8	# ici	nous avo	ns end	core des i	dentifiant	admi	nistra	teur en	Workgrou	p			
9	\$passw	ord = Co	nvert]	Fo-SecureS ¹	tring "Loc	al201	9" -As	PlainTe:	xt -Force	Í.			
10	\$cred=	New-Obi	ect S	stem.Mana	gement.Aut	omati	on.PSC	redentia	al ("admi	nistr	ateur". Si	oasswo	rd)

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

Fichier M	odifier Aff	icher Outil	s Déboguer	Composan	ts additionnels	Aide			
1 🖻	. 4		> 7	6		9			
sys-27-cr	eation-maqu	uette-domain	ne-form-edu-v	vsus.ps1 🗙	Exécuter	la sélecti	ion (F8)		
11 12 #	f Installe	er le rôle	Active Di	rectory p	our form.edu	I			
13 #	≠ Mot de p	oasse de r	restauratio	n à donne	r"Domaine201	.9R" (e	xemple)		
14 🖂	Invoke-Con	nmand -VMN	Name Vm-s1	-Credenti	al \$cred -Sc	riptB1	oc{		
15		Install	-WindowsFe	ature AD-	Domain-Servi	ces -I	includeMana	gement	tTools;
16		Install	-ADDSFores	t -Domain	Name form.ed	lu}			

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

PS C:\Users\Admir Insta Insta	nistrateur\Desktop\Script> Invoke-Command -VMName Vm-s1 -Credential \$cred -ScriptBloc{ lll-WindowsFeature AD-Domain-Services -IncludeManagementTools; lll-ADDSForest -DomainName form.edu}
PSComputerName : RunspaceId : Success : RestartNeeded : FeatureResult : ExitCode :	Vm-51 d5779e3c-50ac-4dc4-bfc3-20503574628f True No {Services AD DS, Gestion de stratégie de groupe, Outils d'administration de serveur dis Success
AVERTISSEMENT : l lles, telles que les données.	In script ou une application sur l'ordinateur distant VM-S1 envoie une demande d'invite. vos informations d'identification ou votre mot de passe, que si vous avez confiance dar
	🛃 Windows Powe 🖓 HI ISE - Entrée — 🗆 🗙
	SafeModeAdministratorPassword
	••••••
	OK Annuler



https://www.cabare.net Pag - Michel Cabaré -

	🔮 Le serveur cible sera configuré en ta — 🗆 🗙
	Voulez-vous continuer en procédant à cette opération ?
	Oui Oui pour tout Non Non pour tout
Confirmer	Continuez avec toutes les étapes de l'opération.
Et c'est fini	PSComputerName : Vm-S1 RunspaceId : aeOfce40-976c-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

Gestionnai	ire de serveur 🕨 Se	rveur local
Tableau de bord	PROPRIÉTÉS Pour s1	
Serveur local	Nom de l'ardinateur	
Tous les serveurs	Domaine	form.edu
📔 AD DS		/
🛱 DNS		
Services de fichiers et d >	Pare-feu Windows Defender Gestion à distance	Public : Actif Activé
	Association de cartes réseau Ethernet	Désactivé 10.0.0.1 Compatible IPv6
	Letter tee	relevent, compatible if vo

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





📔 Utilisateurs et ordinateurs Active	Directory		
Fichier Action Affichage ?			
🗢 🔿 🗖 📰 🔏 📋 🗙 🛙] @ 📑 🛛 🖬 🐍 🔌 🛅 🎙	' 🗾 🍇	
Utilisateurs et ordinateurs Active	Nom	Туре	Description
Requêtes enregistrées	Administrateur	Utilisateur	Compte d'utilisa
V m form.edu	Administrateurs clés	Groupe de séc	Les membres de
Builtin Computers	Réinitialiser le mot de passe		? ×
 Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	Nouveau mot de passe : Confirmer le mot de passe : L'utilisateur doit changer le mot de session L'utilisateur doit fermer puis ouvrir à modifications prennent effet.	e passe à la prochain nouveau sa session	e ouverture de afin que les

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

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 Invoke-Command -VMName Vm-S1 -Credential \$cred -ScriptBloc{Restart-NetAdapter Ethernet}_ 27

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





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

Éditeur de gestion des stratégies de groupe			– 🗆 X	
Fichier Action Affichage ?				
 Configuration ordinateur Stratégies Paramètres du logiciel Paramètres Windows Stratégie de résolution de noms Scripts (démarrage/arrêt) Imprimantes déployées Paramètres de sécurité Stratégies de comptes Stratégie de mot de passe Stratégie de verrouillage du c Stratégie Kerberos 	^	Stratégie Audit de la longueur minimale du mot de passe Conserver l'historique des mots de passe Durée de vie maximale du mot de passe Durée de vie minimale du mot de passe Enregistrer les mots de passe en utilisant un chi Le mot de passe doit respecter des exigences d Longueur minimale du mot de passe	Paramètres de stratégie Non défini 0 mots de passe mémorisés 0 0 jours Non défini Désactivé 0 caractère(s)	

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,

🔣 Gestion de stratégie de groupe

🛒 Default Domain Policy 🛒 reglages-maquette

A Forêt : form.edu
 Domaines
 form.edu



bjets de stratégie de gro	upe liés	Héritage de stratégie de g
Ordre des liens		de stratégie de groupe
1	🛒 re	glages-maquette
2	🗐 🗐	efault Domain Policy
	Ordre des liens 1 2	Ordre des liens Objet 1 2 Drdre des liens Objet



https://www.cabare.net

Page 16 / 21

- Michel Cabaré -

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	Quel type de règle voulez-vous créer ?	
Règles prédéfinies		
 Action 	 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. O 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.

Rèales :

Regles :			
Nom	La règle existe	Profil	Desc
Partage de fichiers et d'imprimantes (LLMNR	Non	Tout	Règle
Partage de fichiers et d'imprimantes (Demand	Non	Tout	Les n
Partage de fichiers et d'imprimantes (Demand	Non	Tout	Les n
Partage de fichiers et d'imprimantes (Service	Non	Tout	Règle
Partage de fichiers et d'imprimantes (service S	Non	Tout	Rèale



https://www.cabare.net

- Michel Cabaré -

💣 Assistant Nouvelle règle de trafic entrant

Action

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

Étapes :	
Type de règle	Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?
Règles prédéfinies	A Adminute according
Action	
	Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.
	O 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.
	Personnaliser
	O Bloquer la connexion

Pour obtenir

🖌 👰 Configuration ordinateur	^	Nom	Groupe
 Stratégies Paramètres du logiciel Paramètres Windows Stratégie de résolution de noms Scripts (démarrage/arrêt) Imprimantes déployées Paramètres de sécurité Stratégies de comptes Stratégies locales Stratégies locales Journal des événements Groupes restreints Services système Registre Système de fichiers Stratégies de réseau filaire (IEEE 802.3) Pare-feu Windows Defender avec fonctions avancées de séc Règles de trafic entrant Règles de trafic sortant 		 Partage de fichiers et d'imprimantes (LL Partage de fichiers et d'imprimantes (De Partage de fichiers et d'imprimantes (De Partage de fichiers et d'imprimantes (Ser Partage de fichiers et d'imprimantes (ser Partage de fichiers et d'imprimantes (NB Partage de fichiers et d'imprimantes (NB Partage de fichiers et d'imprimantes (SM Partage de fichiers et d'imprimantes (NB Partage de fichiers et d'imprimantes (NB 	Partage de fic Partage de fic

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

grobal gr	Utilisateurs et ordinateurs Active Directory [s1.form.edu]	Nom	Туре
	> Construction de la construcción de la construc	🧟 g1	Groupe de sécurité - Global
	V in form.edu	<u>u</u> 1	Utilisateur
	> Computers	🖁 u2	Utilisateur
	> 🖬 Domain Controllers	💑 u3	Utilisateur
	> 🧮 ForeignSecurityPrincipals	👗 u4	Utilisateur
	> Managed Service Accounts	00 US	Utilisateur
	Users	00	otilisateur



Hyper-V maquette 1dc 3 srv 5 clt https://www.cabare.net - SYS 26 - GPO - ver 1.00 -

- Michel Cabaré -

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-maguette-domaine-form-edu-wsus.ps1 X 42 # Intégrer les serveurs au domaine # integret les serveurs au domaine # il faut depuis chaque serveur à intégrer, en tant que administrateur local faire une demande avec u # c'est donc un paramétrage de l'OS Windows des 5 VM 43 44 # donc un parametrage de i os windows des 5 MM
donc Configuration possible via Powershell Direct
Session Powershell Direct (avec session interactive sur 1 machine : Enter-PSSession)
N.B: a entrer en inter-actif ligne par ligne, depuis l'hote physique, pas en executant le script
Sur chaque ligne, ligne par ligne "pour comprendre"
Rappel \$cred =authentification locale \$credom =authentification de domaine 45 46 47 48 49 50 Enter-PSSession -VMName Vm-s2 -Credential \$cred 52 hostname Add-Computer -DomainName form.edu -Credential \$Using:credom -Restart 53 54 # normallement 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-52] : P5 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

C:\Users\administrateur\Documents> hostname [Vm-52] PS

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

PROPRIÉTÉS Pour s2	
Nom de l'ordinateur	s2
Domaine	form.edu

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



Page 19 / 21 - Michel Cabaré -





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

Adhésion des autres Vm

Fichier	Modifier Afficher Outils Déboguer Composants additionnels Aide	
1 6	▶ 🖬 🐇 🛍 ≫ ┛ 🤍 ▶ 💽 🔲 👁 🗷 🚍 🗖]
sys-27	-creation-maquette-domaine-form-edu-wsus.ps1 × Exécuter la sélection (F8)	
61	#traitement pour les autres serveurs	
62	Enter-PSSession -VMName Vm-s3 -Credential \$cred	
64	#Exit	
65	Enter-PSSession -VMName Vm-s4 -Credential \$cred	
66	Add-Computer -DomainName form.edu -Credential \$Using:credom -Restart	
67	#EXIT	
L T		
ET		
Fichier	Modifier Afficher Outils Déhaguer Composants additionnels Aide	
fichiel -		
	▶ 🖬 🐇 🖞 🔪 🏹 (♥ ▶ 📑 🖬 🕸 🙋 ⊟ 🗆	
ENE-27	-creation-maguatta-domaina form-adu-uscur no1 X	
	Exécuter la sélection (F8)	
69	#traitement pour les clients Windows 10	
70	Enter-PSSession -VMName Vm-s5 -Credential \$cred10	
71	Add-Computer -DomainName form.edu -Credential \$Using:credom -Restart	
72	#Exit	
73	Enter-PSSession -VMName Vm-s6 -Credential \$cred10	
74	Add-Computer -DomainName form.edu -Credential \$Using:credom -Restart	
75	#Exter PSSession -MName /m-s7 -Credential \$cred10	
70	Add-Computer -DomainName form edu -Credential \$Using:credom -Restart	
78	#Exit	
79	Enter-PSSession -VMName Vm-s8 -Credential \$cred10	
80	Add-Computer -DomainName form.edu -Credential \$Using:credom -Restart	
81	#Exit	
82	Enter-PSSession -VMName Vm-s9 -Credential <a>\$ <a>\$ <a>Cred10	
83	Add-Computer -DomainName form.edu -Credential \$Using:credom -Restart	
84	#Exit	
85	# Intégrer l'ordinateur W10 au domaine (depuis w10)	
86	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)



Snapshoot Domaine-ok

Via Powershell

🛃 Administrateur : Windows PowerShell ISE								
Fichier	Modifier	Afficher	Outils D	éboguer	Composants add	litionnels	Aide	
1	s 🔒	🖌 🖻	Ū 入	-7	(□ ▶ □		Se 🔊	
sys-30	-creation-r	maquette-o	domaine-fo	rm-edu.ps	1 X	Exécuter	la sélection	(F8)
97	# Crée	un poin	t de con	tröle "d	lomaine-ok"	Encourter	a serection	()
98	Get-VM	? Nam	e -Like	*Vm-S*				
99	Get-VM	? Nam	e -Like	*Vm-S*	Checkpoint-\	/M –Snap	shotName	domaine-ok
100								

Désormais toutes nos Vm ont un deuxième point de contrôle

Ordinateurs virtuels				Ordinateurs virtuels	
Nom	État	Utilisation d	Mémoire affectée	Nom	État
Vm-S1	Exécution	4 %	1382 Mo	Vm-S1	Exécu
Vm-S2	Exécution	0 %	996 Mo	🗑 Vm-S2	Exécu
🗧 Vm-S3	Exécution	0 %	994 Mo	🔚 🕅 -S3	Exécu
Vm-S4	Exécution	0 %	1060 Mo	🗄 Vm-S4	Exécu
🗧 Vm-S5	Exécution	0 %	1012 Mo	🗄 Vm-S5	Exécu
Vm-S6	Exécution	0 %	706 Mo	🗧 Vm-S6	Exécu
Points de contrôle				Points de contrôle	
⊡ <mark>®</mark> Base ⊡ ® domaine-ok 				⊡ 🔂 Base ⊡ 🔂 domaine-ok	

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-VMShapshot -Name Base -Confirm:$false
```

