TP Core et Wsus

Architecture de départ pour le TP :

- 1 Windows 2016 Full controleur de domaine Nom : SRV-WSUS.lpasr.loc IP : 192.168.<binome>.10
- 1 Windows 2012R2 Core Nom : CLI-WSUS.lpasr.loc IP : 192.168.<binome>.11

Pour toutes les VM :

Login : lpasr Mdp : Lpasr1990!

I Monter un serveur Core 2016 R2

Prérequis : Un Windows 2016 full (ex : SRV-WSUS) avec un domaine déjà existant (ex : lpasr.loc) avec des pare-feu désactivés

- Administrator: C\Windows\system32\cmd.exe
- Se connecter au serveur en RDP

- 1) Désactiver les pare-feu
 - a. Utiliser l'utilitaire powershell
 - b. Set-NetFirewallProfile -Profile * -Enabled False
 - c. Verifier avec Get-NetFirewallProfile | ft Name,Enabled
- 2) Vérifier la bonne connectivité avec le serveur SRV-WSUS (ping)
- 3) Rejoindre le domaine lpasr.loc de SRV-WSUS
 - a. Utiliser l'utilitaire sconfig
 - b. Renommer le serveur en CLI-WSUS

Connexion au portail azure :

URL : portal.azure.com Login : b<n° de binome>@formation.mysimonet.fr (ex : b1@formation.mysimonet.fr) Mdp : Lpassr1990 !

II Monter le service WSUS

Maintenant tous les prérequis sont remplis nous pouvons donc commencer à monter notre serveur WSUS :

• Suivant,

Before You Begin	Select one or more roles to install on the selected server.		
Installation Type	Roles		
Server Selection		^	
Server Roles	Application Server		
Features	DHCP Server		
- Colores	DNS Server (Installed)		
Confirmation	Fax Server		
Results	File and Storage Services (2 of 12 installed)		
	Hyper-V		
	Network Policy and Access Services		
	Print and Document Services		
	Remote Access		
	Remote Desktop Services	=	
	Volume Activation Services		
	Web Server (IIS)		
	Windows Deployment Services		
	Windows Server Essentials Experience		
	Windows Server Update Services	$\overline{}$	

• Tout laisser par defaut

You cannot install Windows Server Update Services unless the following role services or features are also installed.

 .NET Framework 4.5 Features 		
ASP.NET 4.5	_	
▲ Remote Server Administration Tools		
▲ Role Administration Tools		
 Windows Server Update Services Tools 		
API and PowerShell cmdlets		
Web Server (IIS)		
▲ Management Tools		
 IIS 6 Management Compatibility 	\sim	
Include management tools (if applicable)		
	.NET Framework 4.5 Features ASP.NET 4.5 Remote Server Administration Tools A Role Administration Tools Windows Server Update Services Tools API and PowerShell cmdlets Web Server (IIS) A Management Tools IIS 6 Management Compatibility Include management tools (if applicable)	



• Créer le dossier C:\WSUS

If you have a drive formatted with NTFS and at least 6 GB of free disk space, you can use it to store updates for client computers to download quickly.

If you need to save disk space, clear the check box to store updates on Microsoft Update; downloads will be slower.

If you choose to store updates locally, updates are not downloaded to your WSUS server until you approve them. By default, when updates are approved, they are downloaded for all languages.

Store updates in the following location (choose a valid local path on WIN-SRV-002.agire.src, or a remote path):
C:WSUS

Puis dans les

options de WSUS indiquer le dossier nouvellement créé

• Installer

•

• Vous devez donc maintenant avoir une notification de ce type indiquant que WSUS necessite des tâches de post-installation

_		- 🗷 I 🍢
		Post-deployment Configuration
		Configuration required for Windows Server Update Services at SRV-WSUS
		Launch Post-Installation tasks
	0	Feature installation TASKS V
1		Configuration required. Installation succeeded on SRV-WSUS.lpasr.loc.
		Add Roles and Features
		Task Details

- Lancer donc la tâche de post-install (cela peut prendre un certain temps)
- Une fois la tâche terminée lancer WSUS

Windows	Server Update Services Configuration Wizard:WIN-SRV-002.AGIRE.SRC
Before You Beg Things you sho	gin ould do before starting this wizard
Before You Begin Microsoft Update Improvement Program Choose Upstream Server Specify Proxy Server Choose Languages Choose Products Choose Classifications Configure Sync Schedule Finished What's Next	 Before you begin: 1. Is the server firewall configured to allow clients to access the server? 2. Can this computer connect to the upstream server (such as Microsoft Update)? 3. Do you have user credentials for the proxy server, if needed? To run this wizard again, launch the WSUS Administration Snap-in and go to Options
	< Back Next > Finish Cancel

- Dans la catégorie **Microsoft Update Improvment Program** décocher la case qui accepte de rejondre ce programme
- Dans la catégorie **Chosir le serveur en amont** laisser par défaut, ce serveur étant notre serveur primaire aucune raison de selectionner un serveur en amont, il téléchargera donc ses mises à jour depuis internet
- Dans la catégorie **Définir le serveur proxy** laisser par defaut car nous n'avons pas de serveur proxy
- Ensuite on **démarre la synchronisation** depuis le serveur (cela peut prendre **beaucoup** de temps)
- Il nous faut ensuite **Choisir les langues** des mises à jour, pour un soucis de légéreté et de temps nous n'allons prendre uniquement que les mises à jour en **anglais**.
- Dans la catégorie Choisir les produits on va de nouveau selectionner que quelques mises à jour car sinon cela riquerait de prendre trop de temps/place. Selectionner la mise à jour correspondant à Windows Serveur 2016 et Windows 2012R2 et seulement celles là (dans la catégorie Windows).



A savoir que dans un contexte d'entreprise il peut être intéressant de selectionner également le pack office pour les postes clients

- Dans la catégorie Choisir les classifications selectionner « Mise à jour critique, Mise à jour de la sécurité»
- Dans la catégorie **Configurer la planification de la synchronisation s**electionner synchroniser automatiquement à 23h tout les jours
- Enfin dans **Terminé** laisser cocher Commencer la synchronisation initiale pour que WSUS télécharge les mises à jour correspondantes.

Une fois terminé ceci s'affiche:

Next Steps: To fully configure your system, you should explore the following topics:
 1. Using SSL with WSUS
 2. Create computer groups
 3. Assign computers to groups using Group Policy
 4. Configure auto-approval rules

Il est important de respecter ces étapes dans l'ordre mais tout d'abord vérifions quelques prérequis :

Lancez la console WSUS, vous devez tomber sur quelque chose de ce type là :
 Update Services



• Allez dans l'onglet **Synchronisations** et attendre que la synchronisation se termine. Vous pouvez continuer le TP en attendant ce n'est pas **bloquant**.

Synchroniza	tions (2 synchroniz	ations)			
③ Started	Ŧ	Finished		Туре	Result
2	N/A		N/A	N/A	Running
v	12/4/2016 5:24 PM		12/4/2016 5:40 PM	Manual	Succeeded



Synchronization Status Status: Synchronizing... Progress: 28% Une fois terminé reprendre les étapes :

1) Using SSL with WSUS

• Nous allons sauter cette étape là dédié uniquement à la sécurité (bien qu'elle soit très importante) pour nous concentrer sur veritablement l'exploitation de WSUS

2) Create computer groups



• Créer deux groupes d'ordinateurs **w2016** et **w2012**, sans configuration de notre part les ordinateurs vont directement dans le groupe « Ordinateurs non attribués », ces groupes sont donc destinés à acceuillir les ordinateurs correspondants.

4) Assign computers to groups using Group Policy



- Pour l'instant comme vu plus haut pour l'instant les ordinateurs vont directement dans le group « Unassigned computers », nous allons donc créer un GPO pour que les ordianteurs aillent directement dans le groupe correspondant. Créer une GPO **wsus_2016.**
- Editer la GPO, puis aller dans Editeur de gestion de stratégies de groupe >> Configuration Ordinateur >> Modèle d'administration >> Composants Windows >> Windows Update. Voici ce que vous devez obtenir

📔 Différer les mises à jour Windows		
🖹 Ne pas afficher l'option « Installer les mises à jour et éteindr	Non configuré	Non
🖹 Ne pas modifier l'option par défaut « Installer les mises à jou	Non configuré	Non
E Activation de la fonctionnalité de gestion de l'alimentation	Non configuré	Non
🖹 Désactiver le redémarrage automatique pour les mises à jou	Non configuré	Non
🖹 Toujours redémarrer automatiquement à l'heure planifiée	Non configuré	Non
🖹 Spécifier l'échéance avant le redémarrage automatique pour	Non configuré	Non
🖹 Configuration du service Mises à jour automatiques	Activé	Non
🖹 Spécifier l'emplacement intranet du service de mise à jour	Activé	Non
🖹 Fréquence de détection des mises à jour automatiques	Non configuré	Non
🖹 Supprimer l'accès à l'utilisation de toutes les fonctionnalités	Non configuré	Non
🖹 Ne pas se connecter à des emplacements Internet Windows	Non configuré	Non
🖹 Autoriser les non-administrateurs à recevoir les notifications	Non configuré	Non
🖹 Ne pas inclure les pilotes avec les mises à jour Windows	Non configuré	Non
Activer les notifications d'applications	Non configuré	Non
🖹 Autoriser l'installation immédiate des mises à jour automati	Non configuré	Non
🖹 Activer les mises à jour automatiques recommandées via le	Non configuré	Non
🗱 Pas de redémarrage automatique avec des utilisateurs conn	Activé	Non
🖹 Redemander un redémarrage avec les installations planifiées	Non configuré	Non
🖹 Délai de redémarrage pour les installations planifiées	Non configuré	Non
🖹 Replanifier les installations planifiées des mises à jour autom	Non configuré	Non
🖹 Autoriser le ciblage côté client	Activé	Non
🖹 Autoriser les mises à jour signées provenant d'un emplacem	Non configuré	Non

• Configurez « **Configuration du service Mises à jour automatiques** », cette option permet à l'ordinateur client de savoir comment se mettre à jour et à quelle heure. Activer l'option et la configurer comme ci-dessous :

Configuration de la mise à jour automatique :				
4 - Téléchargement automatique et planification des installations \sim				
Les paramètres suivants ne sont n l'option 4 est sélectionnée.	écessaires et ne s'appliquent que si			
Installer durant la maintenance	automatique			
Jour de l'installation planifiée :	0 - Tous les jours 🛛 🗸 🗸			
Heure de l'installation planifiée :	20:00 ~			
Installer les mises à jour d'autre	s produits Microsoft			

• Configurez « Spécifier l'emplacement intranet du service de mise à jour Microsoft », cette option permet de specifier sur quel site local le client va se rendre pour récupérer les mises à jour. Activer l'option et la configurer comme ci-dessous :

Configurer le service de Mise à jour pour la détection des mises à jour :

http://SRV-WSUS:8530

Configurer le serveur intranet de statistiques :

http://SRV-WSUS:8530

Set the alternate download server:

(par exemple : http://IntranetUpd01)

Nom du groupe cible de cet ordinateur	
w2016	

- Configurez « **Autoriser le ciblage côté client** », cette option permet de savoir à quel groupe sera attribué le client. Activer l'option et la configurer comme ci-dessous :
- Configurez « Pas de redémarrage automatique avec des utilisateurs connectés pour les installations planifiées », cette option permet d'éviter que l'ordinateur redémarre tout seul lorsqu'un utilisateur est loggé sur le poste. Activer l'option.

4) Configure auto-approval rule

- Lorsqu'une nouvelle mise à jour est proposée l'administrateur doit « l'approuver » manuellement. Cette tâche peut être redondante et faire perdre du temps. Nous pouvons donc configurer une règle d'approbation automatique.
- Depuis la console WSUS allez dans **Options** puis **Approbations Automatiques.**

Update Rules Advanced
You can specify rules for automatically approving new updates when they are synchronized.
New Rule Edit 🗙 Delete Run Rule
Default Automatic Approval Rule
Rule properties (click an underlined value to edit)
When an update is in Critical Updates, Security Updates
Approve the update for <u>all computers</u>
OK Cancel Arch
OK Cancel Apply

- Cocher la règle par défaut, verifier en dessous que seul les mises à jour Critiques et de Sécurité sont selectionné. Ce qui permet de les approuver automatiquement mais de laisser la main à l'administrateur sur les mises à jours classique
- Puis cliquez sur **Run Rule**

• Allez ensuite dans **Options** puis **Ordinateurs.** Configurez comme ci-dessous afin que les postes hérites de la GPO



Maintenant que WSUS est bien configuré lancer une console PowerShell et faire un **gpupdate** /**force** ainsi qu'un **wuauclt.exe** /**detectnow** sur le SRV-WSUS et CLI-WSUS

• Verifier que les postes remontent dans l'onglet Ordinateur et dans le bon groupe



Bonus

Pour l'instant la GPO que nous avons configurée s'applique sur tout les postes mais dans un contexte d'entreprises souvent les postes sur laquelle la GPO s'applique ont des OS hétérogènes. Et dans notre cas tous les postes vont dans le groupe w2016 !

Il faudrait donc faire une GPO par OS (ex : wsus_2012, wsus_w2016...) et faire en sorte que ces GPO ne s'appliquent uniquement que sur les postes dont l'OS correspond *Astuce : Rechercher du côté des filtres WMI*...

BON COURAGE