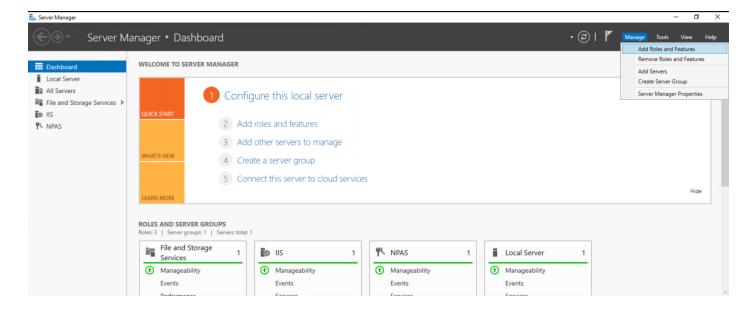
Windows Server

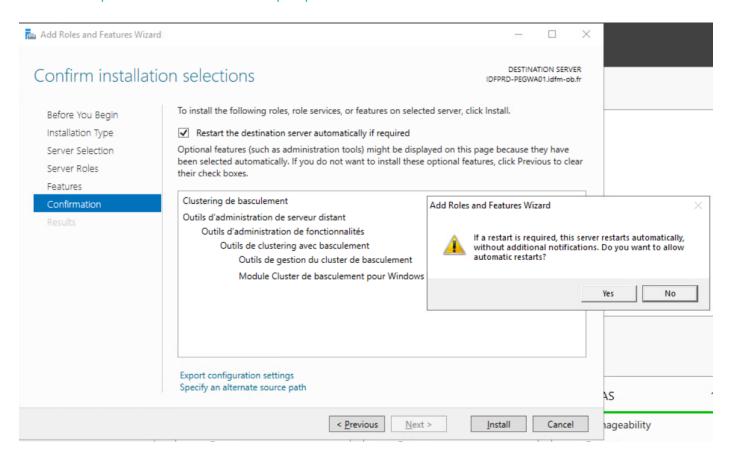
- Création Cluster FAIL OVER
- Event Arrêt Redémarrage système
- SYSVOL non synchronisé
- Réparation BCD (BOOT CONFIGURATION DATA)
- Reset complet de WSUS
- Retention logs Task-Scheduler (planificateur de tâches)
- Serveur ne remonte pas dans WSUS
- WSUS Reset Windows Update Tool
- Limitation Shadowcopy
- Erreur Création Cluster

Création Cluster FAIL OVER

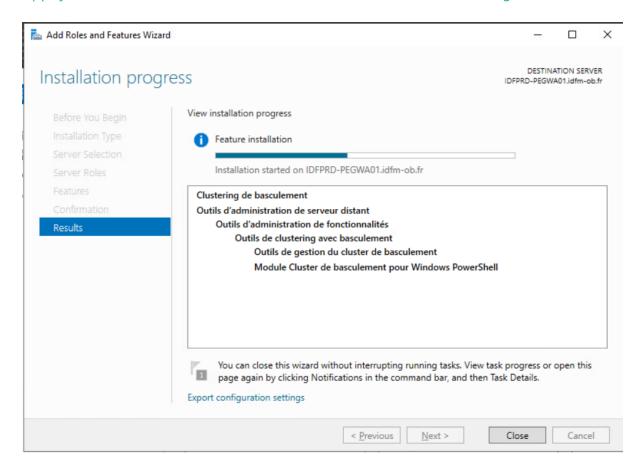
Nous devons d'abord installé les features sur les serveurs sur lesquels aura lieu le cluster Pour ça lancer le Server Manager allez dans Manage > Add Roles and Features



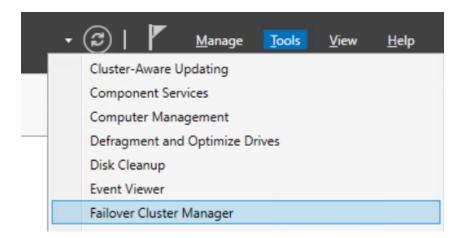
Faire NEXT jusque Features, sélectionner clustering de basculement et Add Features Faire NEXT puis cocher Restart si requis puis faire YES



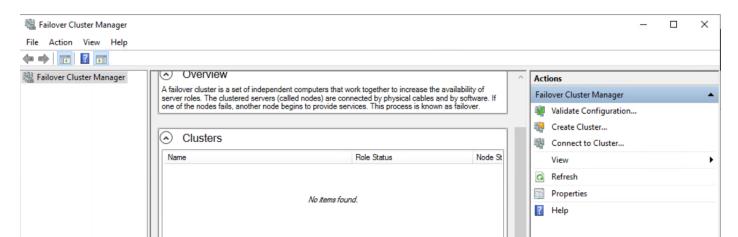
Appuyer sur Install et attendre la fin de l'installation et le redémarrage



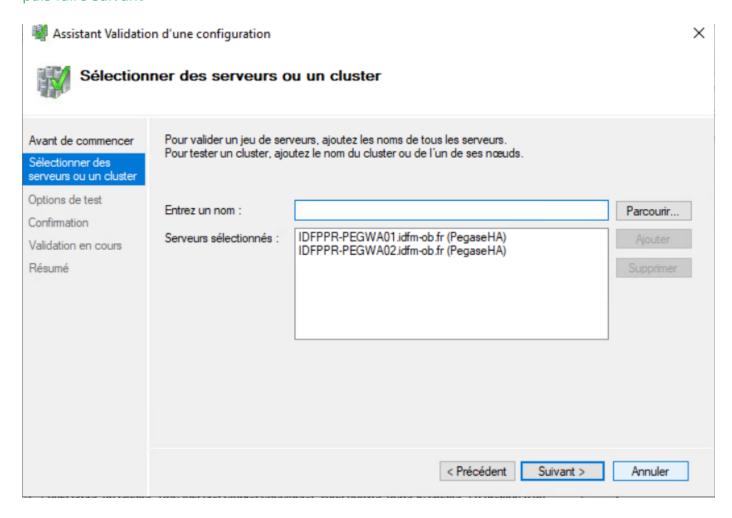
Une fois le redémarrage effectué, nous allons le configurer. pour accéder à la gestion, nous allons dans server manager > outils > Failover Cluster Manager



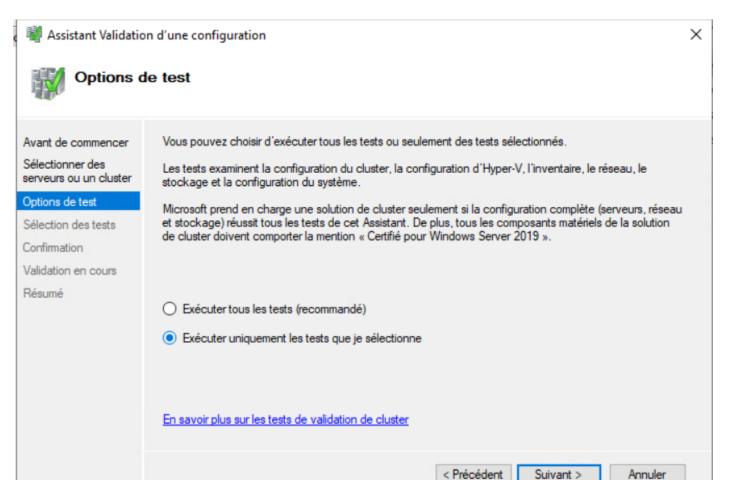
Sélectionner Validate Configuration pour tester la connexion entre les serveurs



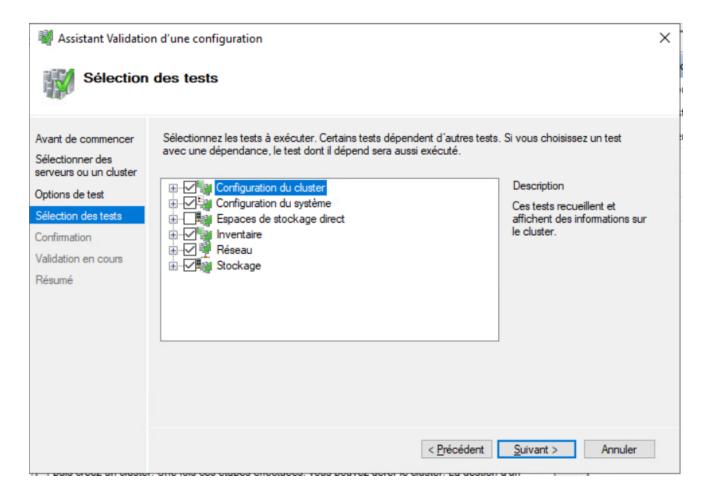
Rajouter les noms des serveurs (ne pas prendre en compte le nom PegaseHA serveur déjà configure) puis faire suivant



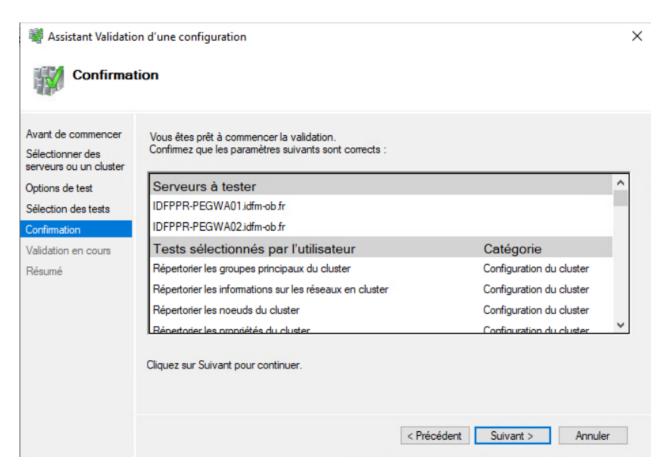
Selectionner l'option Exécuter uniquement



Décocher les Espaces de stockage direct puis faire Suivant



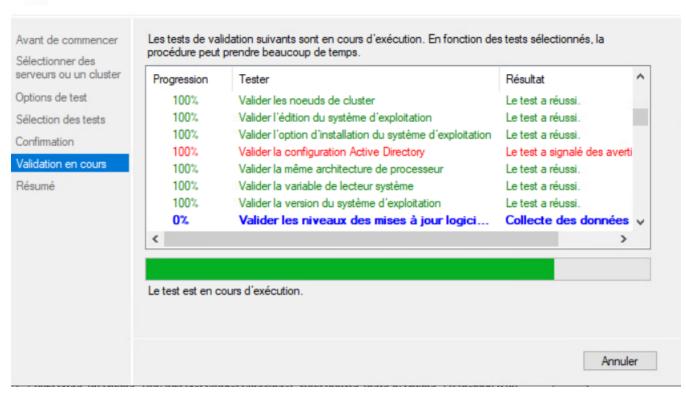
Faire Suivant





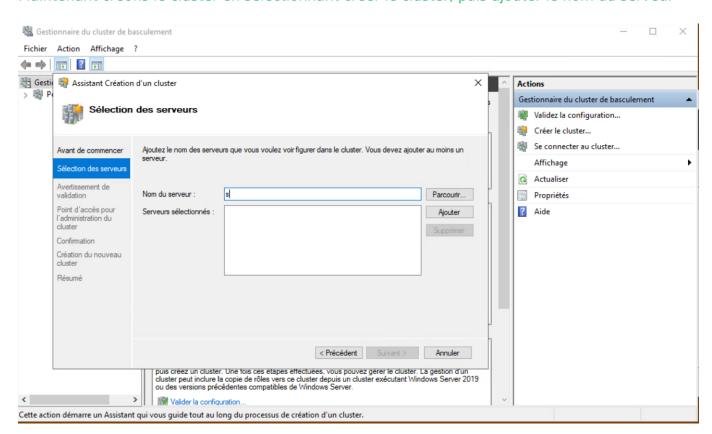


Validation en cours

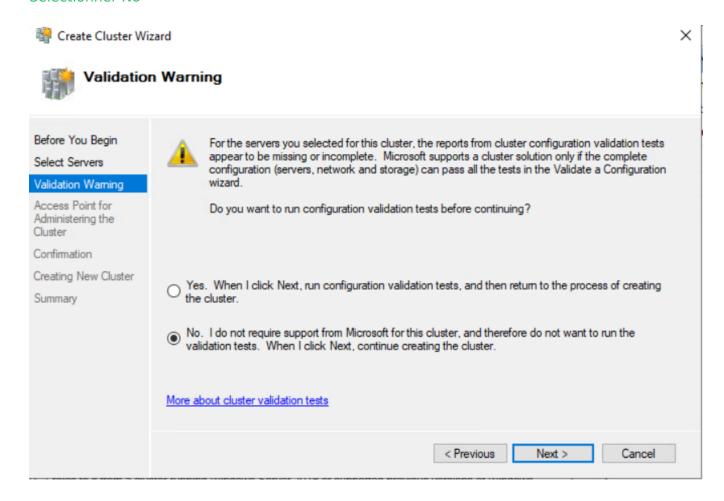


×

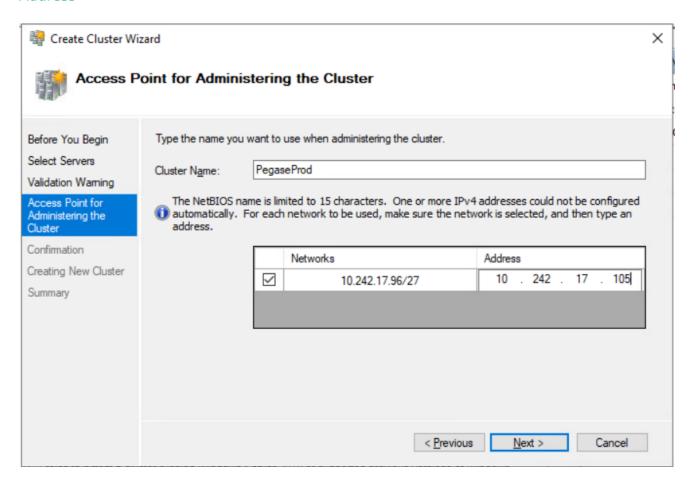
Maintenant créons le cluster en sélectionnant créer le cluster, puis ajouter le nom du serveur



Sélectionner No

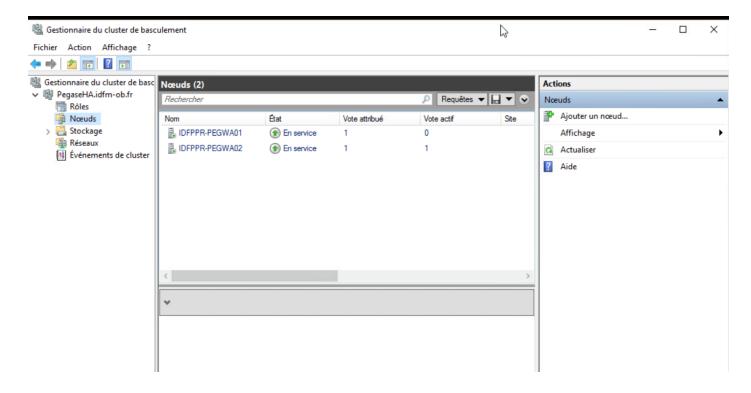


Définissez le nom de Votre cluster, puis ajouter l'adresse VIP qui vous servira pour le cluster dans Address

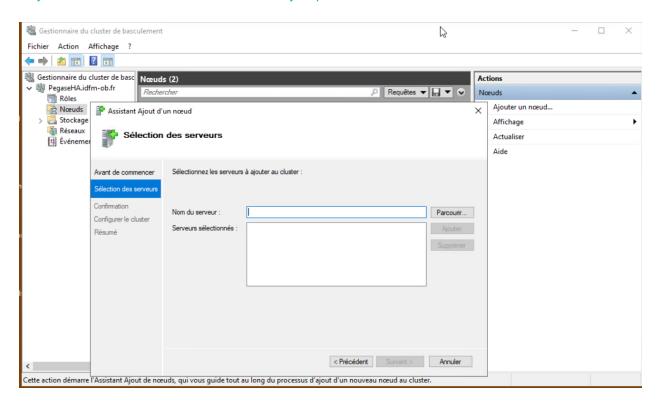


Faire Suivant jusqu'à la création du cluster.

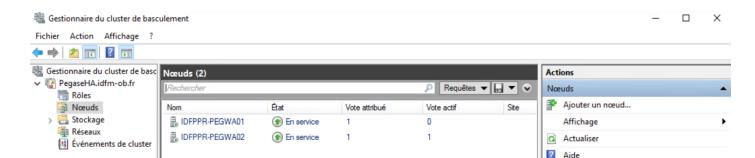
Nous allons maintenant ajouter le 2e serveur, ouvrir votre cluster puis allez dans Nœuds et faire ajouter un nœud



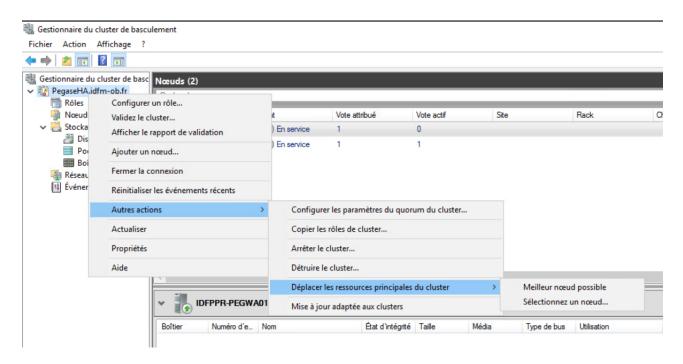
Rajouter le 2e serveur et faire suivant jusqu'au bout



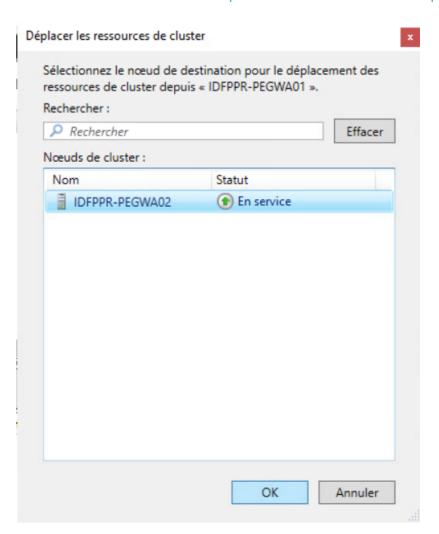
Le cluster est fonctionnel.



Si vous souhaitez changer votre Master, faites un clic droit sur le nom de votre cluster > autres actions > déplacer les ressources principales... > sélectionnez un nœud...



Sélectionnez le serveur sur lequel vous souhaiter basculer puis faites ok



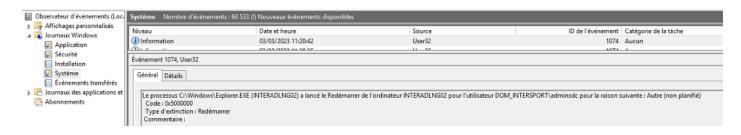
Event Arrêt Redémarrage système

L'event ID Système 12 Kernel-General définit l'heure du démarrage du système :



L'event ID Système 1074 User32 définit le processus à l'origine de l'arrêt ou redémarrage du système :

En cas de crash, cet évènement n'est pas présent



SYSVOL non synchronisé

KB de référence : https://docs.microsoft.com/fr-fr/troubleshoot/windows-server/networking/use-burflags-to-reinitialize-frs

Beaucoup plus simple: https://it-central.fr/probleme-de-replication-sysvol-et-netlogon/

Le KCC (Knowledge Consistency Checker) est un service qui s'exécute à intervalles réguliers sur les contrôleurs de domaine et qui a pour rôle de déterminer si les liens de réplications sont suffisants. Le KCC peut créer automatiquement des liens entre des contrôleurs de domaine de plusieurs sites.

D2, également appelée restauration en mode nonhoritatif ou sans référence - > reconstruction de la partie FRS du contrôleur de domaine réplica à partir du contrôleur de domaine faisant autorité comme si le contrôleur de domaine était nouveau.

D4, également appelée restauration en mode faisant autorité. -> reconstruction de la partie FRS du premier contrôleur de domaine (depuis sa copie local de l'arborescence SYSVOL) dans un nouveau domaine.

MACHINE (DC faisant autorité ou de référence) SERVEUR (DC secondaire ou non autoritaire)

Sauvegarde de l'état système des deux contrôleurs de domaine Snapshot ?

Arrêt et désactivation du service FRS sur tous les DC

Get-Service -ComputerName \$MachineName -Name "NtFrs" | Stop-Service ?

Set-Service -Computer \$MachineName -Name "NtFrs" -StartupType "Disabled" ?

Copier en tant que backup/sauvegarde les dossiers C:\Windows\Sysvol ; \\NOMCLIENT.local\sysvol et \\NOMSERV\sysvol

Renommer le dossier sysvol en sysvol.old sur SERVEUR

Stopper les réplications pour préserver l'intégrité du SYSVOL pour ne pas générer de More Folder supplémentaires (précaution)

Arrêter le service FRS:

net stop ntfrs

Supprimer la gestion de la réplication par le KCC Désactivation du KCC sur le site principal depuis le contrôleur de domaine MACHINE :

repadmin /siteoptions /Site:Premier-Site-par-defaut +IS_AUTO_TOPOLOGY_DISABLED

Supprimer l'ensemble des ponts de réplications générés automatiquement depuis le site et services Active Directory

Modification des connexions de réplication pour spécifier uniquement un contrôleur de domaine MACHINE (SYSVOL complet)

Réplication de cette information de topologie

Vérifier la bonne réplication de ces changements

Restauration autoritaire du sysvol à partir de MACHINE (BurFlags à D4) vers les autres DCs Depuis MACHINE (référence), Positionner la clé de registre BurFlags à D4 dans

 $\label{local_Machine} \label{local_Machine} HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup$

Même étape pour

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\Cumulative Replica Sets

Vérifier le partenaire de réplication : clé « Registre Replica Set Parent » dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters\SysVol\NOMCLIENT.I ocal

Redémarrer le service FRS sur MACHINE :

net start ntfrs

Vérifier le partenaire de réplication : clé « Registre Replica Set Parent » à nouveau

Recréer un pont MACHINE et SERVEUR depuis le site et services Active Directory

Relancer la réplication et restauration du SYSVOL sur SERVEUR

Depuis SERVEUR (non autoritaire), Positionner la clé de registre BurFlags à D2 dans

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup/Restore\Process at Startup

Même étape pour

 $\label{local_MACHINE} HKEY_LOCAL_MACHINE \ System \ Current Control Set \ Services \ NtFrs \ Parameters \ Cumulative \ Replica Sets$

Redémarrer le service FRS sur SERVEUR :

net start ntfrs

La réplication se relance depuis le partenaire de réplication MACHINE. Evènement 16515 + repositionnement à la valeur 0 de la clé BurFlags.

durée estimé à moins de 5 minutes / 44 Mo env. à répliquer. Pendant ce laps de temps les GPO/login scripts ne sont plus présentes sur le contrôleur du site.

Vérifier le partenaire de réplication : clé « Registre Replica Set Parent » dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters\SysVol\NOMCLIENT.I ocal

Vérification que la réplication est terminée par l'évènement 16516.

Vérification de la réplication par création d'une nouvelle GPO Réactivation de la topologie KCC Réactivation du KCC sur le site principal :

repadmin /siteoptions /Site:Premier-Site-par-defaut -IS_AUTO_TOPOLOGY_DISABLED

Suppression des liens de sites manuellement créés Génération automatique des liens

Réparation BCD (BOOT CONFIGURATION DATA)

UEFI boot: /EFI/Microsoft/Boot/BCD

BIOS boot: /boot/BCD sur la partition active

Avant de démarrer sur l'iso d'installation de Windows Server 2012:

réaliser un backup du BCD (Backup Boot Configuration Data)

bcdedit /export "emplacement à renseigner.bcd"

Lancer le boot de l'iso en mode réparation avec les lignes de commandes. Lancer les commandes :

diskpart
list disk
select disk [numero_disk]
list partition
list volume
detail disk pour vérifier les disques actifs

identifier la lettre où est installé la partition windows (dans le cas de srvtech, il s'agissait du disque D)

sfc /SCANNOW /OFFBOOTDIR=D:\ /OFFWINDIR=D:\windows

bootrec /rebuildbcd

BOOTREC /FIXMBR

bootrec /fixboot

Commande la plus importante et la plus délicate : (/v : verbose) Add a boot entry for your Windows partition

bcdboot D:\windows /v

bootsect.exe /nt60 all /force

sfc /SCANNOW /OFFBOOTDIR=D:\/OFFWINDIR=D:\/windows

Reset complet de WSUS

- 1- Lancer une invite Powershell en tant qu'admin
- 2- Arrêter le service Microsoft Update : net stop wuauserv
- 3- Supprimer le dossier de téléchargement de Windows Update : C:\Windows\SoftwareDistribution
- 4- Taper les lignes suivantes dans l'invite powershell :

REG DELETE "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v SusClientId /f
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate" /v SusClientIdValidation /f
regsvr32 /s atl.dll

regsvr32 /s wucltui.dll

regsvr32 /s wups.dll

regsvr32 /s wuaueng.dll

regsvr32 /s wuapi.dll

regsvr32 /s msxml3.dll

regsvr32 /s mssip32.dll

regsvr32 /s initpki.dll

regsvr32 /s softpub.dll

net start wuauserv

wuauclt /resetauthorization /detectnow

Relancer une recherche de MAJ Windows.

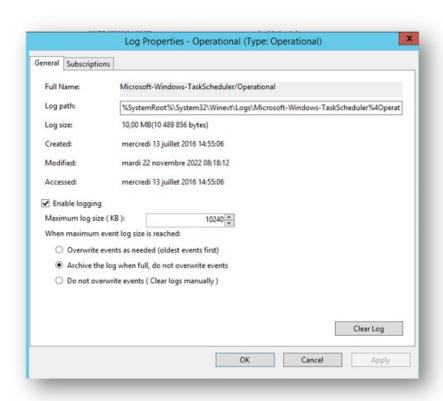
Suite à ce reset, il peut être nécessaire de lancer 4 à 5 recherches avant de ne plus avoir d'erreur.

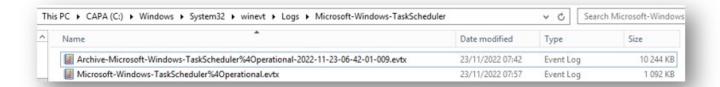
Stop-Service -Name BITS, wuauserv -Force Remove-ItemProperty -Name AccountDomainSid, PingID, SusClientId, SusClientIDValidation -Path HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\ -ErrorAction SilentlyContinue Remove-Item "\$env:SystemRoot\SoftwareDistribution\" -Recurse -Force -ErrorAction SilentlyContinue Start-Service -Name BITS, wuauserv wuauclt /resetauthorization /detectnow (New-Object -ComObject Microsoft.Update.AutoUpdate).DetectNow()

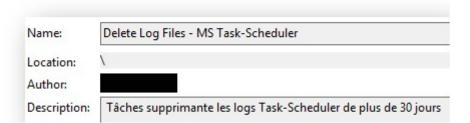
Retention logs Task-Scheduler (planificateur de tâches)

Les actions suivantes ont été effectuées :

- Augmentation de la taille des journaux des opérations des tâches planifiées de 10 Mo à 20 Mo
- Archivage de ces journaux quand le fichier est plein avec conservation des anciens journaux
- Modification de l'emplacement de ces journaux C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler\Microsoft-Windows-TaskScheduler\% 4 Operational. evtx
- Création d'une tâche Delete Log Files MS Task-Scheduler pour supprimer les logs de plus de 30 jours uniquement dans le répertoire C:\Windows\System32\winevt\Logs\Microsoft-Windows-TaskScheduler.





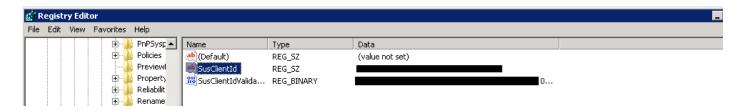


Serveur ne remonte pas dans WSUS

Certains serveurs ne remontent pas dans la console WSUS. Cependant la GPO est bien appliquée.

Cet anomalie est dû à une clef de registre qui est identique sur les différents serveurs.

La clef est SusClientId --> elle se trouve ici : HKLM\Software\Microsoft\Windows\Current Version\Windows update



Pour remédier au problème, sur le serveur à ajouter :

- Arrêter le service windows update
- Supprimer la clef SusClientId
- Exécuter

wuauclt.exe /resetauthorization /detectnow

Vérifier le lendemain que le serveur est bien remonté sur la console WSUS

Ce problème est dû au fait de cloner des VM ou d'utiliser des P2V. Pensez à lancer un sysprep à l'issue

Pensez à vérifier que les nouvelles machines que vous installez remontent bien dans WSUS.

Les machines remontent automatiquement dans la console après 24h maximum.

WSUS Reset Windows Update Tool

Outil de diagnostic (troubleshooting) pour réparer des problèmes liés à Windows Update.

Reset-Windows-Update-Tool aka wureset

https://github.com/wureset-tools

Lien de téléchargement :

https://wureset.com/downloads/

Features

The Reset Windows Update Tool provides the following features:

Resetting Windows Update components to their default settings

Deleting temporary files to free up disk space

Changing invalid values in the Windows Registry to ensure smooth operation

Scanning and repairing protected system files that may be corrupted using the "sfc /scannow" command

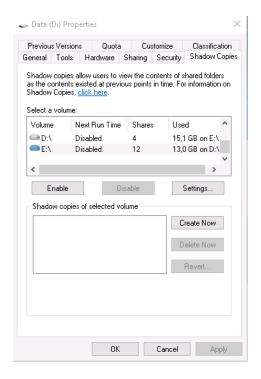
Detecting and repairing corruptions in the Windows system image

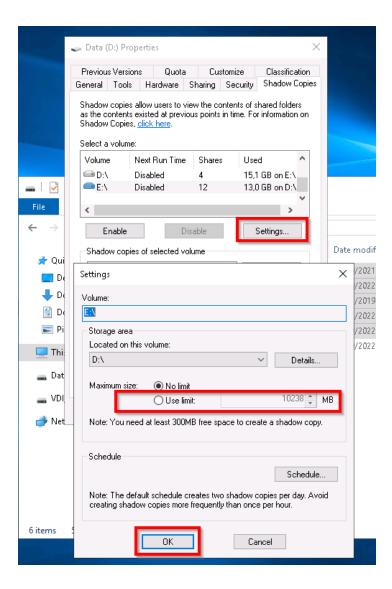
Cleaning up superseded components to optimize system performance and free up disk space

https://docs.wureset.com/diagnostic/

Limitation Shadowcopy

Clic droit sur le lecteur, propriétés, onglet shadow copies:





Temporairement mettre une limite

Powershell

vssadmin resize shadowstorage /for=C: /on=C: /maxsize=1GB

vssadmin list shadowstorage

vssadmin delete shadows /for=c: /oldest

Erreur Création Cluster

ERROR THE COMPUTER "SERVERNAME.DOMAIN" IS JOINED TO A CLUSTER

Disable Cluster Services dans services.msc Puis utiliser la Commande Clear-ClusterNode