Cours Migration 2003-2008R2

Le but de cette migration est de basculer un vieux serveur 2003 qui est DC, DNS, WINS et DHCP vers un nouveau serveur en 2008R2 qui reprendra tous ces rôles.

Différentes étapes sont nécessaires pour cette migration :

1) Préparation de la forêt :

On suppose que vous voulez installer la dernière version de Windows 2008R2. Pour préparer le réseau, on va devoir utiliser un outil appelé ADPREP.Mettre me DVD de 2008R2 dans SRV01 et tapez en ligne de commande :

a. H:\support\adprep\adprep32.exe /forestprep Pour faire cela, il faut que tous les DC soit Windows 2000 SP4 pour éviter des corruptions. Bien entendu, il faut que votre Windows 2000 soit à jour et donc, idéalement, en SP4.

```
H:\support\adprep>adprep32 /forestprep
ADPREP WARNING:
Before running adprep, all Windows 2000 Active Directory Domain Controllers in t
he forest should be upgraded to Windows 2000 Service Pack 4 (SP4) or later.
[User Action]
If ALL your existing Windows 2000 Active Directory Domain Controllers meet this
requirement, type C and then press ENTER to continue. Otherwise, type any other
key and press ENTER to quit.
```

Attention à bien appuyer sur C puis sur ENTER. Pour faire cette opération, il faut être Schema Admins car on va modifier le Schema de la forêt.

b. H:\support\adprep\adprep32.exe /domainprep

Ici, il prépare le domaine et il ne faut être que Domain Admins car on ne va modifier que l'architecture du domaine.

Vous risquez d'avoir un message d'avertissement vous disant que votre domaine n'est pas en mode natif. Si ce n'est pas le cas, vous devez passer le domaine en 2000 natif minimum (Dans l'ADUC, raise Domain functionnal Level).

H:\support\adprep>h:\support\adprep\adprep32.exe /domainprep Running domainprep
Adprep successfully updated the domain-wide information.
The new cross domain planning functionality for Group Policy, RSOP Planning Mode, requires file system and Active Directory Domain Services permissions to be updated for existing Group Policy Objects (GPOs). You can enable this functionality at any time by running "adprep.exe /domainprep /gpprep" on the Active Directory Domain Controller that holds the infrastructure operations
master role. This operation will cause all GPOs located in the policies folder of the SYSUOL to be replicated once between the AD DCs in this domain. Microsoft recommends reading KB Q324392, particularly if you have a large number of Group policy Objects.

c. H:\support\adprep\adprep32.exe /domainprep /gpprep

Cette commande va préparer les GPO existantes pour qu'elles puissent utiliser les nouvelles fonctionnalités de notre domaine. Elle va aussi forcer la réplication des GPO vers les autres DC si vous en avez.

- d. H:\support\adprep\adprep32.exe /domainprep /rodcprep : nécessaire uniquement si vous voulez faire un RODC plus tard.
- 2) Configuration du 2008R2 pour qu'il puisse devenir DC
 - a. Mise en IP fixe

Attention de bien le mettre en tant que client DNS sur serveur 2000 dans un premier temps.

LAN Properties	Internet Protocol Version 4 (TCP/IPv4) Properties
Networking	General
Connect using:	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Configure	Obtain an IP address automatically Obtain an IP address:
 Client for Microsoft Networks QoS Packet Scheduler 	IP address: 192.168.17.2
File and Printer Sharing for Microsoft Networks	Subnet mask: 255 . 255 . 255 . 0
Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4)	Default gateway:
Link-Layer Topology Discovery Mapper I/O Driver Link-Layer Topology Discovery Responder	C Obtain DNS server address automatically
	• Use the following DNS server addresses:
Install Uninstall Properties	Preferred DNS server: 192 . 168 . 17 . 1
Description	Alternate DNS server:
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	Validate settings upon exit Advanced

b. Promotion de notre serveur 2008R2 SP1 en DC :

Taper « dcpromo » sur votre serveur 2008R2. On va faire un DC secondaire

Choose a Deployment Configuration You can create a domain controller for an existing forest or for a new forest.	
Existing forest	
Add a domain controller to an existing domain	
C Create a new domain in an existing forest	
This server will become the first domain controller in the new domain.	
\square Create a new domain tree root instead of a new child domain	
C Create a new domain in a new forest	

Ensuite, vous devez mettre le domaine que vous voulez joindre et les crédits d'une personne autorisée à transformer ce serveur en DC (un Domain Admins).

Active Direct	ory Domain Services Installation Wizard	×
Network Cre Specify the credentials	dentials e name of the forest where the installation will occur and accur that have sufficient privileges to perform the installation.	ount
Type the n controller:	ame of any domain in the forest where you plan to install this	domain
startrek.tn	g	
Specify the	e account credentials to use to perform the installation:	
C My cur	rent logged on credentials (SRV02\Administrator)	
▲ The cor	e current user credentials cannot be selected because they a mputer. A set of domain credentials is needed.	are local to this
Alterna	te credentials:	
startrek.tn	g\administrator	Set



Si vous n'avez pas fait le RODCPrep, il vous met un message d'avertissement comme quoi le serveur ne peut pas être RODC (de toute façon, vu qu'il est le seul 2008R2, il ne saurait pas l'être).

Â	You will not be able to install a read-only domain controller in this domain because "adprep /rodcprep" was not yet run.
	Do you want to continue?

Dans l'écran suivant, si vous avez configuré plusieurs sites (dans Active Directory Site and Services), vous pouvez choisir à quel site appartiendra le DC

Si vous n'avez pas encore installé le service DNS, il vous propose de l'installer. Il vous propose aussi automatiquement de mettre le SRV02 comme Global Catalog

additional Domain Controller Options	
Select additional options for this domain controller.	
DNS server	
Global catalog	
<u>B</u> ead-only domain controller (RODC)	
Additional information:	
There is currently 1 DNS server that is registered as an authoritative name server for this domain.	-
A domain controller running Windows Server 2008 or Windows Server 2008 could not be located in this domain. To install a read-only domain controller t	R2
domain must have a domain controller running Windows Server 2008 or Windows Server 2008 R2.	

Il va ensuite vous mettre un message pour un problème de délégation DNS (parce qu'il ne trouve pas de serveur « Parent », ce qui est normal

Active	Directory Domain Services Installation	n Wizard	×
<u>.</u>	A delegation for this DNS server cannot be of authoritative parent zone cannot be found of Windows DNS server. If you are integrating infrastructure, you should manually create a DNS server in the parent zone to ensure reli from outside the domain "startrek.tng". Other required. Do you want to continue?	created because the or it does not run with an existing DNS a delegation to this able name resolution erwise, no action is	
	Ŷ	/es No	

Il vous propose ensuite de synchroniser avec un DC via réseau ou de restaurer une sauvegarde (ce qui peut être pratique si vous avez une ligne lente entre les 2).

Active Directory Domain Services Installation Wizard	×
Install from Media	
Select one of the following options, depending on whether you want to replicate domain data over the network from an existing domain controller or you want to replicate domain data from media created from an existing domain controller (install from media). In either case, the existing domain controller must be in the same domain as the new domain controller.	
 Replicate data over the network from an existing domain controller Replicate data from media at the following location Consult the help to make sure that the media you are using is compatible with the of domain controller you are installing. Even if you select this option, some data is copied over the network. Location: 	type
C:\NTDSRestore Browse C:\NTDSRestore Browse Browse Browse	
More about install from media	

Enfin, comme pour une autre DC, lui mettre les dossiers dans lesquels il doit mettre les DB, les logs et le SYSVOL (pour rappel, il faut mettre les DB et les logs sur des HDD différents).

logs sur des HDD différents). Il vous demande le mot de passe à mettre pour quand on sera en mode Active Directory Restore. Comme la sécurité est déjà mise en place, on est obligé de rentrer un mot de passe complexe

📑 Act	ive Directory Domain Services Installation Wizard	>
Dir	ectory Services Restore Mode Administrator Password	
	The Directory Services Restore Mode Administrator account is different from the domain Administrator account.	I
	Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.	
	Password:	
	Confirm password:	
	More about Directory Services Restore Mode password	
	Active Directory Domain Services Installation Wizard X The password does not meet the minimum password length requirement of the password policy. Enter a longer password.	
	ОК	

3) Installation des différents services

Une fois que votre serveur est devenu DC, vous devez encore installer les différents services que l'autre serveur gère pour pouvoir basculer sur votre nouveau DC.

a. DNS : sous Windows 2008R2, c'est un rôle

Vu qu'on ne l'a pas installé avant le DCPromo, le DNS a été installé automatiquement par Windows. L'avantage du DNS, c'est que quand on l'installe sur un DC, il n'y a rien à configurer (aucune zone ni rien) car il va aller chercher ses données dans l'Active Directory (si, bien entendu, vos zones étaient intégrées à l'AD).

ATTENTION : en DNS 2008, certaines URL sont bloquées par défaut (voir <u>http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=8219</u>)

🚊 DNS Manager				
File Action View Help				
🗢 🔿 🖄 📅 🔀 🖾 😣	2 🖬 🗄 🗐 🖬			
 DNS SRV02 Global Logs Forward Lookup Zones Startrek.tng msdcs startrek.toe mstartrekent.be 	Name msdcs itcp udp DomainDnsZones ForestDnsZones (same as parent folder) (same as parent	Type Start of Authority (SOA) Name Server (NS) Name Server (NS) Host (A) Host (A) Host (A) Host (A) Host (A)	Data [63], srv02.startrek.tng., h srv01.startrek.tng. srv02.startrek.tng. 192.168.17.2 192.168.17.1 192.168.17.69 192.168.17.70 192.168.17.1	
	srv02	Host (A) Host (A)	192.168.17.2 192.168.17.3	

b. WINS : sous Windows 2008R2, c'est une Feature

Pour le WINS, il faut juste momentanément configurer une synchro avec celui du serveur 1. Vous allez devoir créer un partenaire de réplication



Attention qu'il faut créer les partenaires sur les deux serveurs WINS

c. DHCP : sous Windows 2008R2, c'est un rôle

Pour le DHCP, c'est un peu plus compliqué, car il n'y a pas de communication ni de réplication entre plusieurs DHCP.

On devra exporter la configuration du serveur 1 et l'importer dans le serveur 2. Sur SRV01 :

• clic droit sur le serveur, backup.



Il faut faire la sauvegarde dans un dossier accessible depuis les 2 serveurs car il va falloir recopier le résultat sur l'autre serveur.

G [[[\srv01.startrek.tng\c\$\Uti]			
Organize 👻 🏹 Open New folder			
🔆 Favorites	Name *		
🔙 Desktop	📕 BackupDHCP		

Sur SRV02 :

• clic droit sur le serveur, Restore. Attention qu'il n'accepte pas de chemin réseau, la sauvegarde doit être locale.

DHCP	
E 🖡 IPv4	Add/Remove Bindings Authorize
 	Backup Restore

Quand il met un message de problème de permissions, il suffit de lui dire de le corriger.



Petit problème de cette méthode graphique : il n'importe pas les réservations. Il existe des outils de migration mais il y a une méthode plus simple : la ligne de commande.

Sur SRV01 :

- netsh dhcp server dump >C:\Util\BackupDHCP\dhcpdump.txt Il va exporter la configuration existante. Il faut ensuite modifier le fichier pour remplacer l'ancienne IP du serveur (192.168.17.1) par la nouvelle (192.168.17.2). Pour réimporter la configuration, depuis SRV02 ou SRV01 :
- netsh exec C:\Util\BackupDHCP\dhcpdump.txt

Dans ce cas, il va importer tout (réservations comprises) sauf les crédits DNS.

Attention qu'il faudra, dès que le serveur DHCP 02 est opérationnel, arrêter le serveur DHCP 01 pour éviter les conflits.

Il ne faudra pas oublier de modifier les options d'étendue pour qu'elles distribuent les IP du serveur 02 à la place du 01 (au niveau WINS et DNS) : si vous l'avez fait en ligne de commande, ce n'est pas nécessaire car on a fait un « remplacer ».

Une fois que tous les services ont été configurés sur SRV02, il faut vérifier l'observateur d'évènements pour voir si la réplication s'est bien passée.

Il faut encore mettre le SRV02 client de lui-même (au niveau DNS et WINS) et, par sécurité, le redémarrer. Mais, auparavant,

LAN Properties		Status of ans connection
Networking	General	ICP/IPV4) Properties
Connect using:	You can get IP settings assign this capability. Otherwise, you for the appropriate IP settings	ed automatically if your network s need to ask your network admin s.
Configure This connection uses the following items:	Obtain an IP address automatically Obtain an IP address:	
Client for Microsoft Networks	IP address:	192 . 168 . 17 . 2
Brile and Printer Sharing for Microsoft Networks	Subnet mask:	255 , 255 , 255 , 0
 ✓ ▲ Internet Protocol Version 6 (TCP/IPv6) ✓ ▲ Internet Protocol Version 4 (TCP/IPv4) 	Default gateway:	
Link-Layer Topology Discovery Manner I/O Driver Link-Layer Advanced TCP/IP Settings	<u>?</u> ×	s automatically
IP Settings DNS WINS		rver addresses:
Install		192 . 168 . 17 . 2
Description Transmission C		

Il ne faudra pas oublier non plus de passer SRV02 en **Global Catalog** si vous ne l'avez pas fait pendant le DCPromo. Pour passer un serveur en GC, il faut aller dans ADSS (Active Directory Site and Services), Sites, « le nom de votre site », le nom de votre serveur (SRV02) et dans les propriétés de NTDS Settings pour cocher la case Global Catalog

Active Directory Sites and Servic	NTDS Settings Properties
File Action View Help	General Connections Object Security Attribute Editor
Active Directory Sites and Services Active Directory Sites and Services Sites Subnets Inter-Site Transports VDS Servers SRV01 SRV02	NTDS Settings Description: Query Policy: DNS Alias: 9BDD2714-E5B3-4063-8890-77BB09A7C Iv Global Catalog

4) Transfert des rôles FSMO

Le transfert des rôles FSMO va pouvoir se faire de 2 manières :

- en ligne de commande via NTDSUTIL
- en interface graphique via plusieurs outils.

Il existe 5 rôles :

- 2 pour la forêt : Schema Master et Domain Naming Master : 1 par forêt.
- 3 pour le domaine : RID (Responsible Identifiant), IM (Infrastructure master) et PDC Emulator : 1 par *domaine*.

a. Transfert des rôles en ligne de commande

Ces opérations peuvent se lancer à partir de n'importe quel DC de votre domaine.

http://support.microsoft.com/?scid=kb%3Ben-us%3B255504&x=7&y=12

C:\>ntdsutil ntdsutil: roles fsmo maintenance: connections server connections: connect to server srv02.startrek.tng
Binding to sru02.startrek.tng Connected to sru02.startrek.tng using credentials of locally logged on user. server connections: quit fsmo maintenance: q ntdsutil: q
C:\>ntdsutil ntdsutil: r fsmo maintenance: co server connections: con t s srv02.startrek.tng Binding to srv02.startrek.tng Connected to srv02.startrek.tng using credentials of locally logged on user. server connections: q fsmo maintenance: _

La première chose à faire est de se connecter avec NTDSUtil sur le serveur vers lequel on veut transférer les différents rôles. Dans la 2^{ème} partie, vous avez la version abrégée des commandes.

Une fois connecté, on peut commencer le transfert des rôles.

fsmo maintenance: ?	
? Connections Help Quit Seize infrastructure master Seize naming master Seize PDC Seize RID master Seize schema master Select operation target	 Show this help information Connect to a specific AD DC/LDS instance Show this help information Return to the prior menu Overwrite infrastructure role on connected server Overwrite PDC role on connected server Overwrite RID role on connected server Overwrite schema role on connected server Select sites, servers, domains, roles and
Transfer infrastructure master Transfer naming master Transfer PDC Transfer RID master Transfer schema master	naming contexts - Make connected server the infrastructure master - Make connected server the naming master Make connected server the PDC - Make connected server the RID master - Make connected server the schema master

A chaque transfert de rôle, il demande une confirmation en interface graphique. C'est simplement par sécurité pour qu'un script (et donc un virus potentiel) ne puisse pas le faire de manière automatique.

1) PDC Emulator

• transfer pdc : transfère le PDC Emulator sur le srv02.



Résultat après la commande



2) RID Master

• transfer rid master



3) Schema Master

• transfer schema master



4) Domain Naming Master

• transfer domain naming master (en 2003) ou transfer naming master (en 2008R2)



5) Infrastructure Master

• transfer infrastructure master



A la fin des opérations, vous devez avoir un résumé où vous voyez que les 5 rôles sont bien sur SRV02.



Vous pouvez aussi vérifier cela en vous mettant dans le contexte « select operation target » et en tapant « list roles for connected server ».

Pour avoir un résumé plus clair, on peut utiliser la commande :

« netdom query fsmo »

C:∖>netdom query fsmo	
Schema master	SRV02.startrek.tng
Domain naming master	SRV02.startrek.tng
PDC	SRV02.startrek.tng
RID pool manager	SRV02.startrek.tng
Infrastructure master	SRV02.startrek.tng
The command completed	successfully.

La commande transfer permet de transférer le rôle quand le serveur qui les possède est toujours Online. Si ce n'est pas le cas, on va plutôt utiliser la commande « seize » avec les mêmes paramètres.

b. Transfert des rôles en interface graphique

Voir note de cours sur les rôles FSMO.

5) Dépromotion du SRV01

Une fois que SRV02 est GC, qu'il possède tous les rôles FSMO, qu'il contient tous les services du réseau, on peut alors dépromouvoir SRV01 via la commande DCPromo.

Lorsqu'on le fait, il nous prévient que ce DC est GC et qu'on doit s'assurer qu'il existe bien un autre GC pour authentifier les utilisateurs.



OK

Il ne faut surtout pas cocher la case à l'étape suivante

Active Directory Installation Wizard			
Remove Indic	Active Directory ate whether this is the last domain controller in the domain.		
Rem is the	oving Active Directory converts this domain controller to a member server. Or, if this a last domain controller in the domain, it will become a standalone server.		
<u>ت</u> ا	his server is the last domain controller in the domain		
⚠	After you remove Active Directory from the last domain controller in the domain, the domain no longer exists, which means that:		
	Computers that belong to this domain cannot log onto the domain or access any domain services.		
	All user accounts in this domain will be deleted.		
	All cryptographic keys will be deleted and should be exported before continuing.		
	All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.		

Il nous demande ensuite un mot de passe pour l'administrateur local car ce serveur va de nouveau avoir une SAM.



Avant le DCPromo inverse, il faut penser sur SRV01 modifier la configuration IP et le mettre client DNS de SRV02

Lorsque SRV01 sera rétrogradé en simple serveur, il faudra encore le sortir du domaine et puis, on pourra tuer la machine. Ne pas oublier avant de redémarrer le SRV02 pour être sûr que tout se passe bien.

Ne pas oublier de faire un backup quand on est sûr que tout se passe bien.

http://technet.microsoft.com/fr-fr/library/dd365353%28v=ws.10%29.aspx