Windows Serveur 2012.

Présentation :

Windows Serveur 2012 est une nouvelle version de Windows Server qui apporte de nombreuses nouveautés qui permettent de rendre les serveurs plus évolutifs, virtualisables (Hyper-V) et favorise les évolutions vers les cloud.

L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes,

Objectif :

Installer et configurer un autre Windows Serveur 2012 pour faire de la réplication Active Directory.

Pré requis :

- ➔ Avoir une connexion internet
- → Avoir deux IP fixe pour les Windows Serveurs.
- ➔ Ma machine s'appelle WinServQuantin et son @IP est 192.168.1.134/24
- ➔ Mon second AD s'appelle ADQuantin2 et son @IP est 192.168.1.135/24
- → Le troisième (RODC) s'appelle ADQuantin3 et son @IP est 192.168.1.136/24
- → Le nom de domaine est quantin.local

Sommaire :

- I) Configuration des Sites
- II) Test de la réplication
- III) Configuration de la stratégie RODC

I) Configuration des sites

On va dans l'outil « Site et services Active Directory » afin de créer trois sites depuis le principal, Caen pour le principal, Boston pour le second et Marseille pour le RODC :



On crée un lien du site entre Caen et Boston :

	Nouvel objet - Li	ien du site	x	
Créer dan	s : quantin.local/Conf	iguration/Sites/Inter-Site		
Nom :	Lien 1			
Sites absents de ce de sites :	elien	Sites présents dans ce lien de sites :		
Cefault-First-Site-N Marseille	Ajouter >> << Supprimer	Boston Caen		
Un lien de sites doit contenir au moins deux sites.				
		ОК	Annuler	

On peut modifier le temps de réplication, ici 240 minutes :

			Propriétés	de : Lien 1		? X
Général	Objet	Sécurité	Éditeur d'attributs			
	Lie	en 1				
Descrip	tion :					
Sites ab sites :	sents de	ce lien de		Sites présents dans ce lien de sites :		
Default Marseil	:-First-Site le	-Name	Ajouter >>	Boston Caen		
<	III	>				
Coût :			100 🔹			
Réplica	tion toute	s les :	240 nmin	utes		
Modifie	er la plani	fication				
			ОК	Annuler Appliqu	ier	Aide



Et on peut aussi modifier la planification horaire des réplications :

II) Test sur la réplication

Via le CMd :

repadmin /showrepl NomduServeur afficher les partenaires



repadmin /showconn NomduServeur afficher les connexions



repadmin /syncall NomduServeur /A /e forcer la réplication

C:\Users\Administrateur>repadmin /syncall WinServQuantin /A /e Synchronisation de tous les contextes de nom détenus sur WinServQuantin. Synchronisation de la partition : DC=ForestDnsZones,DC=quantin,DC=local MESSAGE DE RAPPEL : La réplication suivante est en cours : dcdiag /test :topology vérifier la topologie de réplication

```
C:\Users\Administrateur>dcdiag /test:topology
Diagnostic du serveur d'annuaire
Exécution de l'installation initiale :
Tentative de recherche de serveur associé...
Serveur associé : WinServQuantin
* Forêt AD identifiée.
Collecte des informations initiales terminée.
Exécution des tests initiaux nécessaires
Test du serveur : Caen\WINSERVQUANTIN
Démarrage du test : Connectivity
de WINSERVQUANTIN a réussi
Exécution des tests principaux
Test du serveur : Caen\WINSERVQUANTIN
Démarrage du test : Topology
de WINSERVQUANTIN a réussi
Exécution de tests de partitions sur ForestDnsZones
Exécution de tests de partitions sur DomainDnsZones
Exécution de tests de partitions sur Schema
Exécution de tests de partitions sur Configuration
Exécution de tests de partitions sur Quantin
Exécution de tests de partitions sur Quantin
Exécution de tests de partitions sur Quantin
```

dcdiag /test :replications vérifier ponctualité du contrôleur

```
C:\Users\Administrateur>dcdiag /test:replications

Diagnostic du serveur d'annuaire

Exécution de l'installation initiale :

Tentative de recherche de serveur associé...

Serveur associé : WinServQuantin

* Forêt AD identifiée.

Collecte des informations initiales terminée.

Exécution des tests initiaux nécessaires

Test du serveur : Caen\WINSERVQUANTIN

Démarrage du test : Connectivity

..... Le test Connectivity

de WINSERVQUANTIN a réussi

Exécution des tests principaux

Test du serveur : Caen\WINSERVQUANTIN

Démarrage du test : Replications

..... Le test Replications

de WINSERVQUANTIN a réussi

Exécution de tests de partitions sur ForestDnsZones

Exécution de tests de partitions sur Schema

Exécution de tests de partitions sur Configuration

Exécution de tests de partitions sur Configuration

Exécution de tests de partitions sur quantin

Exécution de tests de partitions sur quantin
```

III) Configuration de la stratégie RODCOn installe le service ADDS sur ADQuantin3 :

📥 Assis	tant Configuration des services de domaine Active Directory	_ 🗆 X
Assist Configuration de déploie Options du contrôleur de Options supplémentaires Chemins d'accès Examiner les options Vérification de la configur Installation Résultats	stant Configuration des services de domaine Active Directory déploiement Sélectionner l'opération de déploiement Ajouter un contrôleur de domaine à un domaine existant Ajouter un nouveau domaine à une forêt existante Ajouter une nouvelle forêt Spécifiez les informations de domaine pour cette opération Domaine : quantin.local Fournir les informations d'identification pour effectuer cette opération quantin\administrateur	Sélectionner
	En savoir plus configurations de déploiement < Précédent	nstaller Annuler

Puis on choisit RODC :

🚡 Assis	🚡 Assistant Configuration des services de domaine Active Directory 📃 🗖 🗙							
Configuration de déploie Options du contrôleur de Options du contrôleur de Options RODC Options supplémentaires Chemins d'accès Examiner les options	SERVEUR CIBLE ADQuantin3							
Vérification de la configur	Taper le mot de passe du mode de resta Mot de passe :	per le mot de passe du mode de restauration des services d'annuaire (DSRM) ot de passe :						
Installation Résultats	Confirmer le mot de passe :	nfirmer le mot de passe :						
	En savoir plus options du contrôleur de	domaine						
	< Pré	cédent Suivant > Installer	Annuler					

Dans utilisateurs et ordinateurs de l'AD, on voit bien l'ADQuantin3 qui est en lecture seule (RODC).



Dans Sites, on voit la présence du Serveur RODC :



Vu que c'est en RODC, on a bien ce type de message d'erreur :



Enfin, on remarque que les enregistrements DNS se sont fait correctement :

Directe :

🚊 DNS	Nom	Туре	Données	Horodateur
⊿	🗊 _msdcs			
⊿ Zones de recherche directes	🚞 _sites			
[] _msdcs.quantin.local	🚞 _tcp			
quantin.local	🚞 _udp			
Zones de recherche inversée	📔 DomainDnsZones			
Points d'approbation	ForestDnsZones			
Redirecteurs conditionnels	(identique au dossier parent)	Source de nom (SOA)	[119], winservquantin.qua	statique
Dournaux globaux	(identique au dossier parent)	Serveur de noms (NS)	winservquantin.quantin.lo	statique
	(identique au dossier parent)	Serveur de noms (NS)	adquantin2.quantin.local.	statique
	(identique au dossier parent)	Hôte (A)	192.168.1.134	03/12/2015 09:00:00
	(identique au dossier parent)	Hôte (A)	192.168.1.135	03/12/2015 09:00:00
	ADQUANTIN2	Hôte (A)	192.168.1.135	statique
	ADQUANTIN3	Hôte (A)	192.168.1.136	03/12/2015 10:00:00
	Pc-PC	Hôte (A)	192.168.1.2	19/11/2015 08:00:00
	winservquantin	Hôte (A)	192.168.1.134	statique

Inversé :

	B DNS	Nom	Туре	Données	Horodateur
	⊿ WINSERVQUANTIN	(identique au dossier parent)	Source de nom (SOA)	[8], winservquantin.quanti	statique
	⊿ Zones de recherche directes	(identique au dossier parent)	Serveur de noms (NS)	adquantin2.quantin.local.	statique
	Image: Second	(identique au dossier parent)	Serveur de noms (NS)	winservquantin.quantin.lo	statique
	Quantin.local	192.168.1.134	Pointeur (PTR)	winservquantin.quantin.lo	statique
	Zones de recherche inversée	192.168.1.135	Pointeur (PTR)	adquantin2.quantin.local.	03/12/2015 09:00:00
	1.168.192.in-addr.arpa	192.168.1.136	Pointeur (PTR)	adquantin3.quantin.local.	03/12/2015 10:00:00
	Points d'approbation				
	Redirecteurs conditionnels				
	Journaux globaux				
_					

IV) Mise en cache des mots de passe

On va créer des groupes de sécurité :

	Utilisateurs et ord	inateurs Active Direc	ctory	_ 0 ×
Fichier Action Affichage ?				
* + 2 🖬 📋 🖾 🔒 🛛 🖬 🖏	¥ 🛅 🍸 🖻 ¥			
Utilisateurs et ordinateurs Active Directory [WinServ	Nom		Туре	Description
Requêtes enregistrées	🍇 Compliance Management		Groupe de sécurité - Universel	Ce groupe de rôles permet à
⊿ 🙀 quantin.local	💐 Delegated Setup		Groupe de sécurité - Universel	Les membres de ce groupe d
▷ Builtin	🚨 Discovery Management		Groupe de sécurité - Universel	Les membres de ce groupe d
Computers	Servers Exchange Servers		Groupe de sécurité - Universel	Ce groupe contient tous les s
Domain Controllers	🍇 Exchange Trusted Subsystem		Groupe de sécurité - Universel	Ce groupe contient des serve
FL-Corporation	& Exchange Windows Permissions	5	Groupe de sécurité - Universel	Ce groupe contient des serve
Profession Accounts	A ExchangeLegacyInterop		Groupe de sécurité - Universel	Ce groupe a une fonction d'i
Microsoft Exchange Security Groups	👫 Help Desk		Groupe de sécurité - Universel	Les membres de ce groupe d
Users	👫 Hygiene Management		Groupe de sécurité - Universel	Les membres de ce groupe d
	🍇 Managed Availability Server:		Nouvel objet - Groupe	contient tous les s
	Section Management			res de ce groupe d
	Section 2018 Public Folder Management	Ga		res de ce groupe d
	🔏 Recipient Management	Créer dans :	quantin.local/Microsoft Exchange Security Gro	oups res de ce groupe d
	& Records Management			res de ce groupe d
	Server Management	Nom du groupe :		res de ce groupe d
	🚨 UM Management	Utilisateur-Marseille		res de ce groupe d
	💐 View-Only Organization Mai			res de ce groupe d
		Nom de groupe (antérieu	r à Windows 2000) :	
		Utilisateur-Marseille		
				-
		Etendue du groupe	Type de groupe	
		O Domaine local	 Sécurité 	
		 Globale 	 Distribution 	
		O Universelle		
			OK A	nnuler
	<			>

Puis, on va créer des utilisateurs (1 et 2) :

	Utilisateurs et ordina	teurs Active Directo	ry	_ 0 ×
Fichier Action Affichage ?				
	2. 11 🝸 🗾 2.			
1 Utilisateurs et ordinateurs Active Directory [WinSen	Nom		Туре	Description
Requêtes enregistrées	🙎 Administrateur		Utilisateur	Compte d'utilisateur d'ad
⊿ 🚔 quantin.local	🍇 Administrateurs de l'entreprise		Groupe de sécurité - Universel	Administrateurs désignés
▷ Builtin	Administrateurs DHCP		Groupe de sécurité - Domaine local	Les membres qui ont un a
Computers	🍇 Administrateurs du schéma		Groupe de sécurité - Universel	Administrateurs désignés
Domain Controllers	🍇 Admins du domaine		Groupe de sécurité - Global	Administrateurs désignés
FL-Corporation	🍇 Contrôleurs de domaine		Groupe de sécurité - Global	Tous les contrôleurs de d
PoreignsecurityPrincipals Managed Service Accounts	& Contrôleurs de domaine clonables		Groupe de sécurité - Global	Les membres de ce group
Microsoft Exchange Security Groups	& Contrôleurs de domaine d'entrepris	e en lecture seule	Groupe de sécurité - Universel	Les membres de ce group
Users	& Contrôleurs de domaine en lecture	seule	Groupe de sécurité - Global	Les membres de ce group
	🕹 DiscoverySearchMailbox {D919BA05	-46A6-415f-80AD-7E093	Utilisateur	
	& DnsAdmins		Nouvel objet - Utilisateur	x inistrateu
	& DnsUpdateProxy			ui sont a
	& Editeurs de certificats			ce group
	Exchange Online-ApplicationAcco	Créer dans	: quantin.local/Users	
	FederatedEmail.4c1f4d8b-8179-414			
	Soupe de réplication dont le mot	D./		e des me
	Scoupe de réplication dont le mot	Prenom :	utilisateur i Initiales :	e des me
	🚡 Invité	Nom :		teur invit
	Minvites du domaine	N 1.		lu domai
	Migration.8f3e//16-2011-43e4-96b 4a O L	Nom complet :	utilisateuri	
	Ordinateurs du domaine	Nom d'ouverture de s	aesion de l'utilisateur	ns de trav
	Proprietaires createurs de la strateg	utiliesteur1	Orwantia la sal	ce group
	Serveurs KAS et IAS	utiliaateur I	@quantin.local	e groupe
	System Vallbox (1034927-4010-420	Nom d'ouverture de s	ession de l'utilisateur (antérieur à Windows 20	JOO) :
	System Mailbox (00dc1c20, 90c2, 402	QUANTIN\	utilisateur1	
	System viail box eouc rc25-65C3-403			i ont un
	& Utilisateurs du domaine			urs du de
	& WinBMRemoteWMIUsers			
			< Precedent Suivant >	Annuler
	L			
<	<			

On a bien nos 2 utilisateurs :

& utilisateur1	Utilisateur
گ utilisateur2	Utilisateur

On l'ajoute au groupe Utilisateur-marseille :

📙 🚠 Exchange 🔿 🖃	- A	
🐁 Federated	Copier	
🎎 Groupe d	Ajouter à un groupe	utorisé
& Groupe d	Désactiver le compte	fusé
🐁 Invité	Réinitialiser le mot de passe	
🍇 Invités du	Déplacer	
🐁 Migration	Ouvrir la page de démarrage	
Solution at a constant of the second	Envoyer un mersage	
Service a Propriéta	Envoyer un message	
Serveurs 8	Toutes les tâches	
🛃 System M	Couper	3}
🐁 System M	Supprimer	:}
🐁 System M	Deserver	19}
🖧 Utilisateu	Renommer	
🍇 Utilisateu	Propriétés	
& WinRMR	Aide	
👗 utilisateu		

On créer deux ordinateurs :

Fichier Action Affichage Image: Chief of the service of the servic		Utilisateurs et ordi	nateurs Active Directory
Image: Second	Fichier Action Affichage ?		
Image: Control of the subscription of the subscriptic of the subscription of the subscription o	🗢 🔶 🙇 🗊 📋 🖾 🍳 📄 🔧	🤽 🛅 🍸 🚨 🖧	
	 Utilisateurs et ordinateurs Active Directory [WinSer Requétes enregistrées Builtin Computers Domain Controllers El-Corporation ForeignSecurityPrincipals Managed Service Accounts Microsoft Exchange Security Groups Users 	Nom PC-PC SERVEXCHANGEQ	Type Description Ordinateur Ordinateur Ordinateur X Image: Créer dans :: quantin.local/Computers Image: Créer dans :: Quantin.local/Computer dans du domaine Image: Créer dans :: Quantin.local/Computer dans du domaine Image: Créer dans :: Quantin.local/Computer dans du domaine
	<	<	

On ajoute les deux ordinateurs au groupe utilisateur-Marseille :



Maintenant, on édite les propriétés du RODC :



Puis, dans l'onglet Stratégie de réplication de mot de passe, on double clic sur l'encadré en rouge :

	Propriétés d	e : AD	QUANTI	N3		?	x	
Général	Système d'exploitatio	n	Memb	re de	Dél	égatio	n	
Stratégie de réplicatio	n de mot de passe	Empla	cement	Géré par	Ap	pel en	itrant	
Ceci est un contrôleur de domaine en lecture ordinateurs selon la st figurant dans les grou peuvent être répliqués Groupes, utilisateurs e	de domaine en lecture e seule stocke les mots ratégie suivante : seuls pes d'autorisation, et n s sur le contrôleur de do et ordinateurs :	e seule (de pass les mot on dans omaine (RODC). Un se des utilisa s de passe (les groupes en lecture se	contrôleur ateurs et des des comptes a de refus, aule.				
Nom	Dossier Service	s de d	Paramètr	e				
Administrateurs	quantin local/Bu	iiltin	Refuser	1				
Groupe de réplicatio	n quantin.local/Us	sers	Autoriser					
Groupe de réplicatio	n quantin.local/U	sers	Refuser					
Opérateurs de comp	ote quantin.local/Bu	uiltin	Refuser					
Opérateurs de sauv	eg quantin.local/Bu	uiltin	Refuser					
Uperateurs de serve	ur quantin.local/Bu	ultin	Hefuser					
Avancé	ОК	Ajoute	Annuler	Applique	er	Ai	ide	

Onglet Membres puis Ajouter :

Propriétés de : ADQUANTIN3 ? X pston	
Général Membres Membre de Géré par Membres :	com ? ×
Sélectionnez le type de cet objet : des utilisateurs, des comptes de service, des groupes ou Autres objets À partir de cet emplacement :	Types d'objets
quantin.local Entrez les noms des objets à sélectionner (exemples) :	Emplacements
	Vérifier les noms
Ajouter Supprimer	
OK Annuler Appliquer	
OK Annuler Appliquer Aide	

Puis, on met le groupe Utilisateur-Marseille (deux ok pour valider):

Sélectionnez des utilisateurs, des contacts, des ordinateurs, de	es com ? ×
Sélectionnez le type de cet objet :	
des utilisateurs, des comptes de service, des groupes ou Autres objets	Types d'objets
À partir de cet emplacement :	
quantin.local	Emplacements
E <u>n</u> trez les noms des objets à sélectionner (<u>exemples</u>) :	
<u>Utilisateur-Marseille</u>	Vérifier les noms
Avancé Oł	K Annuler
	.11

	Propriétés o	le : AD(QUANTI	N3	? X
Général Stratégie de réplic Ceci est un contrô de domaine en lec ordinateurs selon I figurant dans les g peuvent être réplic Groupes, utilisateu	Système d'exploitati ation de mot de passe ileur de domaine en lectur sture seule stocke les mot a stratégie suivante : seu proupes d'autorisation, et r qués sur le contrôleur de o urs et ordinateurs :	e seule (F s de passe s les mots ton dans l domaine et	Memb cement RODC). Un e des utilisa de passe (es groupes n lecture se Paramètr	re de Géré par Contrôleur ateurs et des des comptes s de refus, eule.	Délégation Appel entrant
Administrateurs Groupe de réplic Groupe de réplic Opérateurs de sa Opérateurs de sa	quantin.local/E ation quantin.local/E ation quantin.local/C ompte quantin.local/E auveg quantin.local/E erveur quantin.local/E	Julitin Jsers Jsers Julitin Julitin Bulitin	Refuser Autoriser Refuser Refuser Refuser		
Avancé	ОК	Ajouter.	S	Supprimer	er Aide

Puis dans l'onglet Stratégie résultante, ajouter :

	Propriétés de : ADOLIANTIN3 ? X pston
Stratégie d	e réplication de mot de passe avancée pourADQUANTIN3
Utilisation de la stratégie	Stratégie résultante
Ajoutez les utilisateurs e	t ordinateurs à la zone ci-dessous pour déterminer s'ils sont autorisés ou refusés par la
stratégie de réplication of	de mot de passe sur ce contrôleur de domaine en lecture seule.
-	
Compte	Paramètre résultant
	Sélectionnez des utilisateurs ou des ordinateurs
	Sélectionnez le type de cet objet :
	des utilisateurs ou des ordinateurs
	Types d objets
	A partir de cet emplacement :
	quantin.local Emplacements
	E <u>n</u> trez les noms des objets à sélectionner (<u>exemples</u>) :
	Vérifier les noms
	Avancé OK Annuler
Ajouter Ad	tualiser Effacer
2	Aida
<u> </u>	Tellilei

On ajoute l'utilisateur1 :

Sélectionnez des utilisateurs ou des ordin	nateurs ? ×
Sélectionnez le type de cet objet :	
des utilisateurs ou des ordinateurs	Types d'objets
À partir de cet emplacement :	
quantin.local	Emplacements
E <u>n</u> trez les noms des objets à sélectionner (<u>exemples</u>) :	
utilisateur1 (utilisateur1@quantin.local)	Vérifier les noms
Avancé	OK Annuler

On voit que l'utilisateur1 est autorisé. Cela veut dire que le mot de passe du compte d'utilisateur sélectionné est autorisé à être mis en cache sur le serveur RODC:

Stratégie d	e réplication de mot de pas	se avancée pourADQUANTIN3	x
Utilisation de la stratégie	Stratégie résultante		
Ajoutez les utilisateurs e stratégie de réplication o	ordinateurs à la zone ci-dessous pou le mot de passe sur ce contrôleur de o	ur déterminer s'ils sont autorisés ou refusés par domaine en lecture seule.	la
Compte		Paramètre résultant	
S utilisateur1		Autoriser	
Ajouter Ad	tualiser Effacer	Aide	mer

Cliquez sur l'onglet Utilisation de la stratégie puis sur le bouton Préremplir les mots de passe. Ensuite, on ajoute deux utilisateurs :

Sélectionnez des utilisateurs ou des ordinateu	rs ? X
Sélectionnez le type de cet objet :	
des utilisateurs ou des ordinateurs	Types d'objets
À partir de cet emplacement :	
quantin.local	Emplacements
Entrez les noms des objets à sélectionner (<u>exemples</u>) :	
utilisateur1 (utilisateur1@quantin.local); utilisateur2 (utilisateur2@quantin.local)	Vérifier les noms
Avancé OK	Annuler

Message d'information de réussite :

Réussite du préremplissage des mots de passe	x
Les mots de passe de tous les comptes ont été correctement préremplis.	
ОК	

Faire de même pour les ordianteurs 1 et 2 puis vérifier :

Stratégie de ré	éplication de mot de	passe ava	ancée pourADQUAN	TIN3
Itilisation de la stratégie Str	atégie résultante			
Afficher les utilisateurs et oro	dinateurs qui répondent aux	critères suiva	nts :	
Comptes dont les mots de p	asse sont stockés sur ce c	ontrôleur de d	omaine en lec 🗸	
Utilisateurs et ordinateurs :	Obj	ets récupérés	: 6	
Nom	Dossier Services de do	Туре	Demière modification d	Le mot de pa
ADQUANTIN3 Arbtgt_50125 CORDINATEUR1 CORDINATEUR2 CORDINATEUR2 Cutilisateur1 Cutilisateur2	quantin.local/Domain quantin.local/Users quantin.local/Computers quantin.local/Computers quantin.local/Users quantin.local/Users	Ordinateur Utilisateur Ordinateur Ordinateur Utilisateur Utilisateur	03/12/2015 11:42:12 03/12/2015 10:57:29 10/12/2015 09:02:27 10/12/2015 09:02:35 10/12/2015 08:58:53 10/12/2015 08:59:23	N'expire jama 14/01/2016 N'expire jama N'expire jama 21/01/2016 21/01/2016
<	Ш			>
Exporter Prére	mplir les mots de passe]		
			Aide	Fermer