Administration Active Directory Guillaume MATHIEU Directeur Technique Flexsi

Sommaire (1/2)

- 1. Présentation de Windows Server
- Les nouveautés
- Les Best Practice

2. Présentation Active Directory

- Qu'est ce qu'un annuaire.
- Les notions de forêt / domaine / OU / schéma Active Directory.

3. Les comptes utilisateurs

- Propriétés d'un compte utilisateur.
- Les modèles de compte utilisateur.

4. Les comptes ordinateurs

- Présentation compte ordinateur.
- Joindre un domaine

5. Les groupes

- Les étendues et les types de groupe.
- Les Best Practice.

6. Les Unités d'organisation

- Présentation générale
- Délégation d'administration.

Sommaire 2/2

7. Les stratégies de groupe

- Les grands principes
- Présentation de GPMC
- Les outils de diagnostics

8. Les mécanismes de réplication

- Présentation de la console Sites et Services Active Directory
- La topologie de réplication

9. Sauvegarde et restauration Active Directory

- Sauvegarde Active Directory
- Restauration autoritaire / la corbeille Active Directory

10. Notions avancées Active Directory

Les outils de supervision / dépannage (DCDIAG, ASIEDIT, REPMON, REPADMIN).

11. Les services réseaux

- Le service DHCP
- Le service WINS

12. Sécuriser son annuaire Active Directory

Les bonnes pratiques pour sécuriser un annuaire Active Directory

1. Présentation de Windows Server

Ouverture session 1/2

Le champ « Se connecter A » n'existe plus depuis Windows Server 2008. Pour se connecter à la base SAM local sur Windows Server 2008, taper : nom_machine\utilisateur ou .\utilisateur

Si la machine est membre d'un domaine, se connecter au domaine en tapant : Nom_NETBIOS\SamAccountName (msreportform\administrateur) UserPrincipalName (administrateur@formation10.lan)



Ouverture session 2/2

Il est possible de définir des noms de domaine DNS supplémentaires appelés suffixes UPN.

Intérêt : le login de l'utilisateur = l'adresse de messagerie (plus simple à retenir). Toujours vérifier que le suffixe UPN n'est pas déjà utilisé au niveau d'une autre forêt que l'on approuve.

3	Active Directory Domains and Trusts	
File Action View Help 	Active Directory Domains and Trusts [MILDC1.oi ? × UPN Suffixes The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names. If you want alternative domain names. If you want alternative domain names. Active Directory User.	s and Computers
	Image: Active Directory Users and Concerning	Image: Second
	▷ I GRP Image: Comparing the second sec	Profile Telephones Organization @msreport.fr ✓ 000): @oimmil.intra Qmsreport.fr AMELIE.MATHIEU

Gestionnaire de Server

La console Server Manager permet :

- De paramétrer le serveur (adresse IP, pare feu, bureau à distance, Windows Update).
- > D'ajouter les composants Windows répartis entre rôles et fonctionnalités.
- D'activer ou de désactiver la configuration renforcée de la sécurité d'Internet Explorer (IE ESC).
- De configurer les paramètres de mises à jour.
- De se connecter à un autre serveur à distance.
- D'accéder depuis un point unique aux principales consoles pour gérer chaque rôle / fonctionnalité.

		Serv	er Manager		
Server Ma	nager • Local Se	erver		© 🚩 🗕	Manage Tools View Help
T Dashboard	PROPERTIES For MILDC1				Add Roles and Features Remove Roles and Features
Local Server	Computer name	MILDC1	Last installed updates	24/01/2019 10:46	Create Server Group
All Servers	Domain	oimmil.intra	Windows Update	Install updates aut	Server Manager Properties
AD CS			Last checked for updates	04/03/2019 14:53	=
AD DS					
DNS DNS	Windows Firewall	Private: Off	Windows Error Reporting	Off	
File and Storage Services	Remote management	Enabled	Customer Experience Improvement Program	Not participating	
	Remote Desktop	Enabled	IE Enhanced Security Configuration	Off	
IS 115	NIC Teaming	Disabled	Time zone	(UTC+01:00) Brussels	s, Copenhagen, Madrid, Paris
	Ethernet	192.168.140.91, IPv6 enabled	Product ID	00252-80025-06751-	-AA978 (activated)

Le bureau à distance

	Sy	ystem Pro	perties		X
Computer Name	Hardware	Advanced	Remote		
- Remote Assista	nce				
Allow Remo	te Assistanc	e connectior	ns to this co	mputer	
				Advanced	
- Remote Deskto	p				
Choose an opti	on, and ther	n specify who	can conne	ct.	
O Don't allow	remote conr	nections to th	is computer		
Allow remote	e connectior	ns to this con	nputer		
Allow co Desktop	nnections or with Netwo	nly from com rk Level Auth	outers runnir nentication (ng Remote recommended)	
Help me choos	<u>e</u>			Select Users	
		ОК	C	ancel	pply

A ne pas confondre avec le rôle Bureau à distance (anciennement appelé Terminal Server / Terminal Server mode serveur d'applications).

La connexion entre un client RDP et le serveur RDP est chiffrée maintenant. Windows Server génère un certificat auto-signé d'où le message d'erreur lorsque que l'on se connecte à distance. Pour ne plus avoir de message d'erreur, installer un certificat reconnu qui n'a pas expiré et se connecter au serveur avec le nom indiqué au niveau du certificat.

Activer l'authentification NLA (plus sécurisé).

PowerShell

Présentation PowerShell :

Nouvelle interface ligne de commande / s'appuie sur le .Net Framework. Active Directory Center exécute en fait des commandes PowerShell. Extensible (ajout de CMDLETs via l'ajout de modules / snapins)

Les commandes PowerShell indispensables :

Get-Help nom_cmdlet : Get-Help Get-Aduser –full Get-Help Get-Aduser -examples Get-Modules -ListAvailable : liste des modules installés Select-object : permet de sélectionner que certains attributs de l'objet de sortie Install-Module XXX : permet d'installer le module XX (nécessite MPowerShell V5).

Les opérateurs (< > | where –ne), les variables \$_.attributs et les filtres

La sortie de la première réponse devient un paramètre en entrée de la seconde commande. Exemple (lister les utilisateurs et afficher certains attributs) Get-ADUser -Filter * -SearchBase "DC=MSREPORT,DC=INTRA" -Properties * |Select-Object CN,LastLogonDate,MemberOf,Manager,Name,SamAccountname, UserPrincipalName,HomePhone | Export-Csv -UseCulture -Encoding UTF8 -Path c:\export.csv

IPV6

Les adresses IPV6 sont en DHCP. Cela génère donc des messages d'erreurs lorsque l'on fait un DCPROMO (Windows 2008 R2)

Pour désactiver IPV6, il <u>ne faut pas</u> décocher la case IPV6 au niveau des propriétés TCP/IP de chaque carte réseau. <u>Créer la valeur DWORD 32 Bits</u> <u>DisabledComponents avec la valeur FF.</u>

En fixant *DisabledComponents* à 0x20, on configure IPV4 comme protocole prioritaire sur IPV6 (configuration recommandée)

http://support.microsoft.com/kb/929852/en-us

📸 Éditeur du Registre			
Fichier Edition Affichage Favoris ?			
🚊 🕛 ТСРІР6 📃	Nom	Туре	Données
Linkage	(par défaut)	REG_SZ	(valeur non définie)
🖻 🤚 Parameters	B Dhcpv6DUID	REG_BINARY	00 01 00 01 13 0a a6 dc 00 24 e8 fa 77 d9
🕀 📄 📄 Interfaces	30 DisabledComponents	REG_DWORD	0xffffffff (4294967295)
Winsock	Modifier la valeur DWORD	32 bits	X
tcpipreg TCPIPTUNNEL tcsd_win32.exe TdmNetworkProvider TdmService TDPIPE TDPIPE TDPIPE	Nom de la valeur : DisabledComponents Données de la valeur :	Base • Hexadécimale • Décimale	
TermDD		OK Ann	nuler
Ordinateur \HKEY_LOCAL_MACHINE \SYSTEM \	CurrentControlSet\services\TCPI	P6\Parameters	

Le pare feu Windows

Par défaut depuis Windows Server 2008 / 2008 R2 le pare feu est activé. Il est recommandé de conserver le pare feu actif.

Si vous souhaitez désactiver le pare-feu Windows :

Toujours passer par la console « *Pare feu avec Fonctionnalités avancées* ». En effet, le pare feu de Windows Server 2008 / 2008 R2 dispose de 3 profils (public, privé, domaine).

Il faut bien penser à désactiver la pare-feu pour les 3 profils.

			Propriétés de : Pare-feu Windows avec fonctions avancées de se
💣 Pare-feu Windows avec fonctio	ns avancées de sécurité	_ D ×	Profil de domaine Profil privé Profil public Paramètres IPsec
Fichier Action Affichage ?			Spécifiez le comportement lorsqu'un ordinateur est connecté à son domaine d'entreprise.
Pare-feu Windows avec fonctions	Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local	Actions	État du pare-feu :
Règles de trafic entrant	-	Pare-feu Windows avec fonctions avanc 🔺	
Règles de sécurité de connexix	Le Pare-feu Windows avec sécurité avancée offre une sécurité réseau pour les	Importer la stratégie	Propriétés de : Pare-feu Windows avec fonctions avancées de sé
🗈 🍢 Analyse		😥 Exporter la stratégie	Profil de domaine Profil privé Profil public Paramètres IPsec
	Yue d'ensemble	Restaurer la stratégie par défaut	Spécifiez le comportement lorsqu'un ordinateur est connecté à un
	Le profil du domaine est actif	Diagnostiquer / Réparer	emplacement réseau privé.
	Le Pare-feu Windows est désactivé.	Affichage 🕨	État du pare-feu : Inactif
	Profil privé	G Actualiser	
	Le Pare-leu Windows est désactivé.	Propriétés	Proprietes de : Pare-feu Windows avec fonctions avancees de se
	Profil public	Aide	Profil de domaine Profil privé Profil public Paramètres IPsec
	Le Pare-leu Windows est désactivé.		Spécifiez le comportement lorsqu'un ordinateur est connecté à un emplacement réseau public
			État

L'UAC (1/2)

Quand on se logue sur une machine, un TGT est créé. Ce dernier liste le ou les SID du compte utilisateur et de tous les groupes auxquels le compte utilisateur appartient.

L'UAC permet de générer un second ticket. Tous les SID des groupes avec des privilèges importants comme « *Administrateurs* » sont supprimés. L'utilisateur utilise par défaut ce second ticket.

Pour pouvoir bénéficier de toutes les fonctionnalités, il faut cliquer sur OK ou exécuter le programme en tant qu'administrateur. L'UAC est paramétrable par stratégie de groupe.





Epingler au menu Démarrer

Supprimer de cette liste

Propriétés

ĽUAC (2/2)

Par défaut depuis Windows Server 2008 / 2008 R2 l'UAC est activé. Il est recommandé de laisser actif l'UAC. Cependant ce dernier peut générer des problèmes avec certains scripts ou des applications qui lancent des scripts. On peut avoir des accès refusés par exemple lors de l'exécution de certains scripts.

Comment désactiver l'UAC

Sous Windows 2008 R2, aller dans le *Panneau de configuration* | *Comptes utilisateurs*. Il faut redémarrer obligatoirement.

A partir de Windows 2012, lancer la console GPEDIT et définir l'option de sécurité *User Account Control: Run all administrators in Admin Approval Mode.*



Renommer / activer Windows

Renommer la machine :

A l'installation, Windows génère un nom aléatoire. Penser à renommer. Ne pas renommer un serveur déjà promu en tant que contrôleur de domaine.

Pour activer Windows, il faut aller dans *Panneau de configuration* | Système et sécurité puis cliquer sur « Système ». Cliquer ensuite sur « Modifier la clé produit ». Cela va lancer automatiquement l'activation par Internet. Penser à configurer un proxy auparavant si besoin. Pour plus d'informations, voir : http://msreport.free.fr/?p=153

Propriétés de Explorateur d'ordinateurs (Ordinateur local)	Modification du nom ou du domaine de l'ordinateur 🔀
Général Connexion Récupération Dépendances	Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ceci peut influer sur l'accès aux ressources en réseau. <u>Informations complémentaires</u>
Nom complet : Explorateur d'ordinateurs Description : Tient à jour une liste des ordinateurs présents sur le réseau et fournit cette liste aux ordinateurs désignés	Nom de l'ordinateur : WIN-GB14VCE9GP9 Nom complet de l'ordinateur :
Chemin d'accès des fichiers exécutables : C:\Windows\System32\svchost.exe -k netsvcs	WIN-GB14VCE9GP9
Type de démarrage : Automatique Obtenir de l'aide pour configurer les options de démarrage des services.	O Domaine :
État du service : Démarré	Groupe de travail : WORKGROUP
Vous pouvez spécifier les paramètres qui s'appliquent au démarrage du service.	OK Annuler

TP: Windows Server

Installer Windows Server 2008 R2 ou versions ultérieures.

Renommer la machine.

Configurer la machine en IP fixe. A quoi sert un masque de sous réseau, une passerelle, un serveur DNS, un serveur Wins ?

Qu'est ce que l'APIPA, la configuration alternative (visible si station en DHCP).

Installer le rôle serveur de fichiers (installer tous les services de rôles).

Installer le rôle IIS. N'installer que les services de rôles proposées par défaut.

Quels sont les modules IIS installés par défaut ?

Activer le bureau à distance sur son serveur et accéder au serveur d'un collègue de son choix. Pourquoi y a-t-il un message d'avertissement ?

Désactiver la configuration renforcée de la sécurité d'Internet Explorer pour les administrateurs. Quels risques en terme de sécurité ?

Lancer PowerShell.

Exécuter la commande PowerShell Get-Modules -ListAvailable

Exécuter la commande Powershell Get-Alias dir et Get-Alias Is

Comparer PowerShell avec l'invite de commande CMD.

2. Présentation Active Directory

Qu'est ce qu'un service d'annuaire ?

Un service d'annuaire permet :

D'identifier des ressources.

Offre une méthode cohérente pour nommer, décrire, rechercher, accéder, gérer et sécuriser l'accès aux ressources de l'entreprise.

Les limites Active Directory (taille, nombre d'objets...) :

http://technet2.microsoft.com/windowsserver/en/library/d2fc40d8-50ba-450c-959b-28fd7e31b9961033.mspx?mfr=true

Fonctionnement avancé :

http://technet.microsoft.com/en-us/library/cc772829(WS.10).aspx

Différence base SAM avec AD : AD est annuaire centralisé (accessible depuis plusieurs machines). Une base SAM est un annuaire local.



Les consoles d'administration 1/2

Utilisateurs et Ordinateurs Active Directory : permet de créer les comptes utilisateurs, groupe, compte ordinateur, OU.

Active Directory Centre d'administration : permet de créer les comptes utilisateurs / ordinateurs, groupes, unités d'organisation (OU). Console très orientée tâches d'administration quotidiennes (créations de comptes...).

Sites et Services Active Directory : permet de forcer la réplication Active Directory et de gérer les services qui se basent sur Active Directory.

Domaine et Approbation Active Directory : permet de gérer les suffixes UPN et les relations d'approbation.

Active Directory Module for Windows PowerShell : permet de créer les comptes utilisateurs / ordinateurs, groupes, unités d'organisation (OU) en ligne de commande ou à l'aide de script.

📔 Utilisateurs et ordinateurs Activ	e Directory		📜 Centre d'a	administration Active D	irectory			
Fichier Action Affichage ?				Services de domain	e Active Directory + format	tion10 (local) 🔸 Forma	ation	
♦ ♦ 2 🖬 4 🗎 🗙 🗄	1 🖬 🔒 🛛 🖬 🔧	& 🛅 🝸 🖻 &	👬 Ajouter o	des nœuds de navigation				
Utilisateurs et ordinateurs Active Di	Nom Type	Description	📑 💦 Servi	ices de dom	Formation (1)			Tâches
	👗 guillaume.ma Utilisate	ur Consultant Pôle Architect	12 12	=	Filtrer		P Requêtes 👻 📘 👻 🐼	
🕀 🧰 Builtin	Proprietes de : guillaum	e.mathieu	👬 Vue d'ens	semble	💠 Ajouter des critères 🔻			guillaume.mathieu
Computers Domain Controllers	Environnement Profil des services Pur	Sessions Contrôle à distance	in formation	n10 (local) 🔹 🕨	Nom	Туре	Description	Réinitialiser le mot de passe.
	Général Adresse Com	pte Profil Téléphones Organisation Membre de Appel entrant	Formati	ion	S guillaume.matnieu	Utilisateur	Consultant Pole Architecture & Integration	Ajouter au groupe
Hormation Managed Service Accounts		· · · · · · · · · · · · · · · · · · ·	P Recherche	e globale				Désactiver
🕀 🧰 Users	👗 guillaume.ma	athieu	튏 guillaum	e.mathieu				Supprimer
			🧏 а	uillaume mathieu				Propriétés
	Prénom :	Guillaume Initiales :	9°				Täches Ajouter des sections 🗸	1 1 nation
	Nom :	Mathieu	Compte	Compte			?⊗⊙	Nouveau
	Nom complet :	guillaume.mathieu	Organisat	tion Prénom :	Guillaume		Date d'expiration du com 💿 Jamais	Déplacer
			Membre o	de Initiales des autres	prén		O Fin	Supprimer
	Description :	Lonsuitant Pole Architecture & Integration	Profil	Nom : Nom complet :	Mathieu		Options de mot de passe : ^	Propriétés
	Bureau :	172 Bureaux de la colline	Extension	ns	1. Januaria		Changer le mot de passe a la prochaine session Autros artigns de mot de passe	

Les consoles d'administration 2/2



Domaines et approbations Active Directory		🛒 Sites et services Active Directory	_
Picher Action Arrichage ?	Type Actions domainDN5 Domaines et a	Fichier Action Affichage ?	2 📰 🖸
Général Approbations Géré par Domaines approuvés par ce domaine	Assistant Nouvelle approbation	Sites et services Active Directory [: No	om C
Nom du domaine j Type c	Cet Assistant vous aide à créer une approbation entre ce domaine et l'un des domaines suivants : • Un domaine Windows de cette forêt ou d'une autre forêt. • Un domaine Windows NT 4.0.	 □ Sites □ Subnets □ Inter-Site Transports 	≤9 Déplacer Répliquer maintenant
Domaines qui approuvent ce domain Nom du domaine Type c	 Une approbation de domaine Kerberos V5. Une approbation est une relation qui permet à des utilisateurs 	 Default-First-Site-Name Servers 	Toutes les tâches
	d'un domaine, d'une forêt ou d'un domaine Kerberos d'être authentifiés dans un domaine, une forêt ou un domaine Kerberos spécifié. Cliquez sur Suivant pour continuer.	SFR1 SFR2 SFR2	Renommer
Nouvelle approbation	< Précédent Suivant > Annuler	NTDS Settings	Propriétés

TP : Zoom sur ADUC 1/2

Si l'on active le mode d'affichage « Fonctionnalités avancées », les conteneurs suivants apparaissent :

- Lost and Found : contient tous les objets en conflits.
- Program Data : conteneur vide, permet à des applications de stocker des données spécifiques à une application.
- NTDS Quota : contient les objets quotas qui permettent de limiter le nombre d'objets que peut créer un compte utilisateur. Le but est de se protéger des attaques par déni de service.
- System : contient tous les dossiers systèmes nécessaires aux bons fonctionnement d'Active Directory (les objets pour les stratégies de groupe...).





TP : Zoom sur ADUC 2/2

MSA / gMSA : comptes de services gérés (nouveautés 2008 R2 / 2012). Cela permet de changer le mot de passe d'un compte de service sans avoir à changer le mot de passe dans la configuration du service.

Passer en mode « Fonctionnalités avancées » permet d'afficher des onglets supplémentaires au niveau des propriétés des objets :

- Editeur d'attributs: sorte d'ADSIEDIT intégré au niveau des propriétés d'un compte utilisateur.
- Objet : permet de déterminer où se trouve l'objet (pratique pour les recherches) et de désactiver la protection contre la suppression accidentelle.
- Réplication des mots de passe : permet de déterminer si l'on peut mettre en cache le mot de passe sur les RODC.

		rioprieces de l'gamaanne		
		Membre de Réplic	ation de mot de passe Appe	el entrant Objet Sécurité
Proprietes de : guillaume.matnieu	ropriétés de : guillaume.mathieu	Enviormement	Jessions	Controle a distance
		Général Adresse C	compte Profil Téléphones	Organisation Certificats publiés
Environnement Sessions Contrôle à dista	Environnement Sessions Contrôle à dist	Profil des services Bureau	i à distance Bureau virtuel per	sonnel COM+ Editeur d'attributs
Profil des services Bureau à distance Bureau virtuel personnel COM+ Édite		Attribute		
Général Adresse Compte Profil Téléphones Organisation Certifi	Profil des services Bureau à distance Bureau virtuel personnel CUM+ Edite	Attributs :	r	
Membro do D. Réplication do not do passo D. Appel ontrant Objet	Général Adresse Compte Profil Téléphones Organisation Certif	Attribut	Valeur	<u> </u>
Membre de l'inéplication de mot de passe l'Apperentiant de la	Manharda I. Dásfastian de met de name I. Annet antente . Objet	accountExpires	(jamais)	
Nien envenieur de Pakisk.	Membre de Replication de mot de passe Appel entrant Object	adminCount	1	
Nom canonique de l'object		badPasswordTime	(jamais)	
formation10.lan/Formation/guillaume.mathieu	E Derker Kalistate einer die seiter die	badPwdCount	0	
	Proteger i objet des suppressions accidentelles	cn	guillaume.mathieu	
		-		

TP : Zoom sur la console Sites et Services

La console Sites et Services n'affichent pas par défaut le nœud « services » :

Ce nœud permet d'avoir une vue simplifiée du conteneur « *Services* » dans la partition de configuration de l'annuaire Active Directory.

Pour afficher le nœud services :

Ouvrir la console Sites et Services Active Directory. Sélectionner la racine de la console et cliquer sur Affichage | Afficher le nœud des services.



Modification ADSI			
Modification AD51 Fichier Action Affichage ? Modification AD51 Configuration [SFR1.formation10.lan] Configuration [SFR1.formation10.JC=lar CN=Configuration,DC=formation10,DC=lar CN=Extended-Rights CN=ForestUpdates CN=ForestUpdates CN=LostAndFoundConfig CN=NotAndFoundConfig	Nom CN=MsmqServices CN=NetServices CN=Public Key Services CN=RRAS CN=RRAS CN=Windows NT	Classe mSMQEnterpr container container container container	Nom unique CN=MsmqServices, CN=Services, CN=Config CN=Public Key Services, CN=Services, CN=Configuration, CN=Public Key Services, CN=Configuration, CN=RRAS, CN=Services, CN=Configuration, CN=Windows NT, CN=Services, CN=Configu
CIN=Partitions CIN=Physical Locations CIN=Physical Locations CIN=MsmqServices CIN=NetServices CIN=RedS CIN=RAS CIN=RAS CIN=Windows NT			

Le service DNS 1/3

Protocole permettant de résoudre un nom DNS (<u>www.google.fr</u>) en une adresse IP et inversement.

Deux systèmes de résolution de noms :

- Zone de recherche directe : résout un nom en IP.
- Zone de recherche inversée : résout une IP en nom.

L'espace de noms DNS est découpé en zones DNS. Ces zones sont répartis sur des milliers de serveurs DNS.

L'interconnexion entre serveurs DNS se fait via le mécanisme de délégation et de redirection.

Afin de fournir une tolérance de panne et de répartir la charge, un serveur DNS peut disposer d'une copie en lecture seule (zone secondaire) de la zone d'un autre serveur en lecteur / écriture (zone principale).



Le service DNS 2/3

La redirection : un serveur DNS peut rediriger les requêtes non résolues vers un autre serveur DNS.

La délégation : un serveur DNS peut déléguer une partie de l'espace de noms qu'il gère à un autre serveur (payant).

Interface : serveur DNS ne répond aux requêtes que sur certaines interfaces / IP. Un serveur DNS génère toujours une entrée de type A (Nom -> IP) pour ses interfaces en écoute même si on désactive la mise à jour dynamique DNS au niveau de la carte réseau. Problématique si des stations de travail ne peuvent pas accéder aux serveurs via certaines IP / cartes.

Le round Robin : quand on dispose de plusieurs entrées A, le serveur répond aléatoirement sur les différentes entrées.

Le TRI DNS : si plusieurs réponses possibles, le serveur DNS répond toujours avec une IP qui est dans le même réseau IP que la machine qui a fait la requête (prioritaire sur le Round Robin).

Mise à jour dynamique DNS : activable au niveau des zones DNS. Commande *ipconfig /registerdns* permet de forcer création enregistrement A et PTR d'une machine Windows (mise à jour dynamique DNS).

Le service DNS 3/3

Propriétés de : SFR1	Propriétés de : SFR1	Propriétés de : formation10.lan
Propriétés de : SFR1 Enregistrement des événements Ancres d'approbation Analyse Interfaces Redirecteurs Avancé Indications de racine Enregistrem Les indications de racine résolvent les requêtes concernant des zones qui r sur le serveur DNS local. Elles sont uniquement utilisées si les redirecteurs n configurés ou s'ils ne répondent pas. Serveurs de noms : Nom de domaine pleinement qualifié du serveur (FQDN) Adresse IP a.root-servers.net. [192.33.4] d.root-servers.net. [192.33.4] d.root-servers.net. [192.33.4]	Propriétés de : SFR1 Enregistrement des événements Ancres d'approbation Analyse Sé ent de déboga i vexistent pas le sont pas Options de serveur : Désactiver la récursivité (désactive également les redirecteurs) Désactiver la récursivité (désactive également les redirecteurs) Désactiver la fonction Round Robin Vérification de nom : Sur plusieurs octets (UTF8)	Propriétés de : formation10.lan cuité bogage WINS Général Source de noms (SDA) État : En cours d'exécution Type : Intégré à Active Directory Modifier Ponnées enregistrées dans Active Directory.
e.root-servers.net. [192.203.2] f.root-servers.net. [192.112.3] h.root-servers.net. [192.112.3] h.root-servers.net. [128.63.2.5] irpnt-servers.net. [129.36.14] Propriétés de : formation10.lan WINS Transferts de zone Sécurité Général Source de noms (SOA) Serveurs de noms	Charger les domées de zone au démarrage : Apartir de Active Directory et du Registre au démarrage : Activer le nettoyage automatique des enregistrements obsolètes Activer le nettoyage : Délai de nettoyage : Propriétés de : formation 10.lan Général Source de noms (SOA)	 Mises à jour dynamiques : Sécurisé uniquement Autoriser les mises à jour dynam Aucun données en danger car les mise Non sécurisé et sécurisé denuis une source non approur Sécurisé uniquement Propriétés de : SFR1
Numéro de série : Incrémenter Serveur principal : sír1.formation10.lan. Seriormation10.lan. Parcourit Personne responsable : Parcourit Intervalle d'actualisation 10.lan. Parcourit Intervalle d'actualisation : 15 Minutes Intervalle avant nouvelle tentative : 10 Minutes Expire après : 1 Jours V Durée de vie minimale (par défaut) : 1 Heures V	WINS Transferts de zone Un transfert de zone envoie une copie de la zone aux serve font la demande. Image: Comparison of the serve	Enregistrement des événements Ancres d'approba surs q Interfaces Redirecteurs Avancé Indications de rac Les redirecteurs sont des serveurs DNS qui permettent à résoudre les requêtes DNS liées aux enregistrements n'ay résolus.
Durée de vie pour cet enregistrement: 0 :1 :0 (JUJU:HH.MM.SS) Modifier les redirecteurs Adresses IP des serveurs de redirection : Adresse IP Nom de domaine complet du Validé Ccliquez ici pour ajouter une adresse IP ou un nom DNS> Ccliquez 1ci pour ajouter une adresse IP ou un nom DNS> Col 212.27.40.240 dns1.proxad.net OK	I 132. 156. U. 161 SFR2 I 132. 157. 157. 157. 157. 157. 157. 157. 157	212.27.40.240 dns I. proxad.net riétés de : formation10.lan Enregistrement des événements Général Source de WINS Trai /ous pouvez utiliser WINS pour résouc Sélectionnez les adresses IP qui serviront le requêtes DNS sur toutes les adresses IP déf limiter aux adresses IP sélectionnées. LUtiliser la recherche directe WINS © Toutes les adresses IP suivantes : Ne pas répliquer cet enregistrer O Uniquement les adresses IP suivantes :

192.168.0.160

Le service DNS 3/4

Transfert de zones : permet à un serveur hébergeant une zone secondaire (en lecture seule) de télécharger la zone depuis un autre serveur.

Wins-R : le serveur DNS s'appuie les enregistrements d'un serveur WINS.

Phénomène d'Ilot DNS : <u>http://support.microsoft.com/kb/291382/fr</u>

Cache Wins sur le serveur DNS :

http://technet2.microsoft.com/windowsserver/en/library/92654b58-b10f-4c35ab22-389b70d94a521033.mspx?mfr=true

Zones DNS en double : <u>http://support.microsoft.com/kb/867464</u>

Bug au niveau des zones secondaires sous Windows 2008 : <u>http://msreport.free.fr/?p=145</u>

Interaction DNS / Active Directory

Les stations de travail localisent les contrôleurs de domaine en effectuant des requêtes sur les enregistrements DNS suivants :

- _ldap._tcp.orga2.lan
- _Idap._tcp.le_nom_du_site_de_rattachement.Lan

Les contrôleurs de domaine se servent du DNS comme d'un fichier de configuration en mettant à jour leurs enregistrements. C'est le service « *CLIENT DHCP* » qui gère cela (ne jamais désactiver ce service).

Serveur de noms (NS)

Alias (CNAME)

Alias (CNAME)

🛔 Gestionnaire DNS					
Fichier Action Affichage ?					
🗢 🄿 🔰 📅 🖬 🖬 🖉					
DNS SFR1 Zones de recherche directe Cones de recherche	Nom gc gc kerberos kerberos kpasswd kpasswd jdap jdap	Données [0][100][3268] s [0][100][88] sfr: [0][100][88] sfr: [0][100][88] sfr: [0][100][464] sf [0][100][464] sf [0][100][389] sf [0][100][389] sf	fr2.formation10.lan. fr1.formation10.lan. 2.formation10.lan. 1.formation10.lan. r2.formation10.lan. r1.formation10.lan. r2.formation10.lan. r1.formation10.lan.	Type Emplaceme Emplaceme Emplaceme Emplaceme Emplaceme Emplaceme Emplaceme	ent du service (SRV) ent du service (SRV)
Gestionnaire DNS Fichier Action Affichane 2					
DNS SFR1 DISS Cones de recherche directe Cones de recherche directe DISS	: omains : dc		Données		Туре
t to the second	dentique au dossier p dentique au dossier p	arent) arent)	[21], sfr1.formation10.k sfr1.formation10.lan.	an., hostm	Source de nom (SOA) Serveur de noms (NS)

63103527-5715-4271-915a-5e26eb1ac1a8 sfr1.formation10.lan.

b2b45a67-64b0-457e-b7b6-248ade88aaa2 sfr2.formation10.lan

sfr2.formation10.lan.

(identique au dossier parent)

🧻 pdc

formation10.lan

Pour localiser qui est Emulateur PDC (lors changement mot de passe...) :

_ldap._tcp.pdc._msdcs.orga2.lan

Pour forcer l'actualisation des enregistrements de services des contrôleurs de domaine (par défaut toutes les 5 minutes), taper les commandes suivantes :

Net stop netlogon & net start netlogon

Le fichier Netlogon.dns

Les entrées du fichier *C:\Windows\System32\Config\Netlogon.dns* sont chargées au démarrage du service NETLOGON (Isass.exe) du contrôleur de domaine.

📔 C:\Windows\System3	2\config			_ 8
Compo	uter 🔹 Local Disk (C:) 🔹 Windows 🔹 System32 🔹 config 🔹 🛛 🔹 💽 Search config	<u> 2</u>		
File Edit View Tools	Help		vindow 📃 🗖	<u>× </u>
Organize 🔻 🤎 Open	📗 netlogon.dns - Notepad			<u>- 🗆 ×</u>
	File Edit Format View Help			
Name ^	c8a0bd5f-841f-4fab-ae85-bb848e88e7a8msdcs.newlife.lan. 600 IN CNAME FR	925V0001.r	newlife.lan.	*
퉬 Journal		newlife.la	an.	
📗 RegBack	_ldap.tcp.pdcmsdcs.newlife.lan. 600 IN SRV 1280 100 389 FR925V0001.ne	wlife.lan.	1.	
svstemprofile	_ldaptcp.Parissites.gcmsdcs.newlife.lan. 600 IN SRV 1280 IN SRV 1280 100 3268	FR925V000	1. newlife.lan.	
TVR	_ldaptcp.4ee9f1d4-866e-446a-a8bc-4d58b5d6747f.domainsmsdcs.newlife.l	an. 600 IN	N SRV 1280 100 389 F	-R92:
BCD Tomplate	_kerberostcp.Parissites.dcmsdcs.newlife.lan. 600 IN SRV 1280 100 8	8 FR925V0	001.newlife.lan.	
	_ldaptcp.dcmsdcs.newlife.lan. 600 IN SRV 1280 100 389 FR92SV0001.new ldap_tcp_paris_sites_dc_msdcs_newlife_lan_600 IN SRV 1280 100 389 F	life.lan. 8925v0001	newlife lan	
BCD-Template.LOG	_kerberostcp.new]ife.]an. 600 IN SRV 1280 100 88 FR92SV0001.new]ife.]a	n.		
	_kerberostcp.Parissites.newlife.lan. 600 IN SRV 1280 100 88 FR925V00	01.newlife	e.lan.	
COMPONENTS.LOG	_gctcp.Parissites.newlife.lan. 600 IN SRV 1280 IO S208 FR92SV0001.newlife.lan.	ewlife.la	in.	
COMPONENTS.LOG1	_kerberosudp.newlife.lan. 600 IN SRV 1280 100 88 FR92SV0001.newlife.la	n.		
COMPONENTS.LOG2	_kpasswdudp.newlife.lan. 600 IN SRV 1280 100 464 FR92SV0001.newlife.la	n.		
COMPONENTS (016888b)	[_]daptcp.ForestDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR925V000 Idap_tcp_Paris_sites_ForestDnsZones_newlife_lan_600 IN SRV 1280 100	1.newlife.	an. 20001 newlife lan	
COMPONENTS (016888b)	_]daptcp.DomainDnsZones.newlife.lan. 600 IN SRV 1280 100 389 FR92SV000	1.newlife	alan.	
	Idaptcp.Parissites.DomainDnsZones.newlife.lan. 600 IN SRV 1280 100 newlife.lan. 600 IN A 10.1.1.2	389 FR925\	W0001.newlife.lan.	
	gcmsdcs.newlife.lan. 600 IN A 10.1.1.2			
	ForestDnsZones.newlife.lan. 600 IN A 10.1.1.2			
DEFAULT.LOG	_]daptcp.Lyonsites.new]ife.lan. 600 IN SRV 1280 100 389 FR925V0001.n	ewlife.la	in.	
DEFAULT.LOG1	_ldaptcp.Lyonsites.gcmsdcs.newlife.lan. 600 IN SRV 1280 100 3268 F	R925V0001	.newlife.lan.	
DEFAULT.LOG2	_ldaptcp.Lyonsites.dcmsdcs.newlife.lan. 600 IN SRV 1280 100 389 FR	925V0001.1	newlife.lan.	
a netlogon.dnb	_kerberostcp.Lyonsites.newlife.lan. 600 IN SRV 1280 100 88 FR925V000	1.newlife	.lan.	
netlogon.dns	daptcp.Lyonsites.ForestDnsZones.newlife.lan. 600 IN SRV 1280 100 SZ08 FR92SV0001.Ne	89 FR925V	0001.newlife.lan.	
netlogon ftl	_ldaptcp.Lyonsites.DomainDnsZones.newlife.lan. 600 IN SRV 1280 100 3	89 FR925V	0001.newlife.lan.	

TP : le service DNS

Avec le bloc Note, ouvrir le fichier C:\WINDOWS\system32\drivers\etc\hosts. A quoi sert ce fichier ?

Installer le service DNS (Gestionnaire de Server | Ajout de rôles).

Créer la zone formationXX.fr où XX est correspond à vos initiales. Autoriser les mises à jour dynamiques non sécurisées et sécurisées.

Créer un enregistrement www avec comme IP 192.168.140.2. Faire un ping de www.formationXX.fr puis un ipconfig /displaydns puis ipconfig /flushdns puis de nouveau ipconfig /displaydns. A quoi sert le cache DNS ?

Au niveau du serveur DNS, purger le cache DNS. Expliquer la différence avec la commande ipconfig /flushdns.

Définir un suffixe DNS sur une machine en groupe de travail (*Panneau de configuration* | *Propriétés Systèmes* | *Nom de l'ordinateur* | *Avancé*).

Faire un ipconfig /registerdns. Que fait cette commande ?

Aller dans les paramètres avancés TCP/IP, onglet DNS et désactiver la case « *Enregistrer les adresses de cette connexion dans le système DNS* ».

Créer une entrée dans le fichier HOST et faire un ipconfig /displaydns.

Se mettre par deux. Créer la zone « . » sur le serveur 1. Créer une nouvelle délégation pour la zone « *fr* » en indiquant l'IP du serveur 2.

Sur le serveur 2, créer la zone « *fr* » et le sous domaine *google*. Créer un entrée www dans « *google.fr* ». Faire un ping <u>www.google.fr</u> depuis le serveur 1 et 2.

Les notions fondamentales 1/2

Forêt (symbole : rectangle) : limite de réplication et de sécurité. Ensemble d'arborescences de domaine. Créer deux forêts pour séparer deux entités pour des raisons de sécurités (créer ensuite une relation d'approbation avec authentification sélective).

Arborescence de domaine (symbole plusieurs triangles reliés ensemble) : Ensemble de domaine avec une même racine de noms (noms contigus).

Domaine (symbole : triangle) : contient les objets (comptes utilisateur / ordinateur, groupes, unités d'organisation...).

Unité d'organisation (OU, symbole : le rond) : C'est un conteneur. Permet d'organiser l'annuaire, déléguer l'administration et créer des objets de stratégie de groupe.

DCPROMO : permet de convertir un serveur en groupe de travail / membre du domaine en un contrôleur de domaine et inversement (exécuter DCPROMO sur un contrôleur de domaine).

Serveur de Catalogue global : contient un réplique partielle de tous les objets de la forêt (que certains attributs). Permet de résoudre les membres des groupes universels et de faire de recherche dans l'annuaire.

SYSVOL : répertoire spécial contenant les scripts et les GPO qui répliquent sur tous les contrôleurs de domaine.

Les notions fondamentales 2/2

NTDS.DIT : il s'agit de la base de données Active Directory (NTDS : New Technology Directory Service). Cette base est un dérivé des bases JET (moyennement fiable mais très rapide en lecture).

Compte de restauration des services d'annuaires : un contrôleur de domaine n'a plus de base SAM locale. Le compte de restauration des services d'annuaire permet de démarrer en mode restauration des services d'annuaire sur un résidu de base SAM. Cela peut être utile pour effectuer certaines opérations de maintenance pour Active Directory (restauration...).

Exportation des paramètres : permet de créer un fichier de réponse au format TXT pour faire une installation en mode « *Serveur CORE* » (Windows 2008 R2 sans interface graphique).

La structure logique Active Directory 1/2



La structure logique Active Directory 2/2

Toujours faire un domaine dans une forêt sauf :

- Si les administrateurs ne doivent pas pouvoir gérer toutes les ressources.
- Si vous devez avoir un nom NETBIOS différent pour chaque entité. Il n'existe pas d'équivalent des suffixes UPN pour le nom NETBIOS. L'alternative est de faire en sorte que les utilisateurs ouvrent une session avec le nom DNS de domaine.
- En mode natif 2008, il est possible de créer plusieurs stratégies de mots de passe alors qu'en mode natif 2003 on ne peut créer qu'une stratégie de mot de passe par domaine.

Best Practice :

- > Faire un domaine dans une forêt puis créer une OU par entités / services.
- ➢ Ne pas dépasser 4 à 5 niveaux d'imbrication pour les OU si possible.
- > Déléguer l'administration au niveau des unités d'organisation.
- Faire une OU pour les comptes ordinateurs et une autre pour les comptes utilisateurs. Mapper les GPO sur ces OU.

Active Directory Users and Computers	🧧 Utilisateurs et ordinateurs Active Directory			
File Action View Help	Fichier Action Affichage ?			
🗢 🔿 📶 🤞 📋 🗙 🖻 💁 🔽 🖬 🗏 🐮 🍸	🗢 🔿 🙍 🖬 📋 🖾 🙆 📴 🖬 🧏 📚 🖆 🍸 💆 🎘			
	Utilisateurs et ordinateurs Active Directory [SFR Nom Type			
🛨 🗊 Migration 🛛 🔹 test 1 User	표 🚞 Requêtes enregistrées 🛛 🔒 guillaume.mathieu Utilisateur			
🕀 🚞 Program Data 🥼 Testgp1 🛛 Security Group	🖃 🏥 formation10.lan 🛛 🕺 Sophie Mathieu Utilisateur			
🕀 💼 Source	🖃 🖬 Administration des ventes			
🛨 🧮 System	🕀 💼 Groupes			
	🕀 🛅 Seven			
	🛅 Utilisateurs			
$ \begin{array}{c} \blacksquare \\ \blacksquare \\ \blacksquare \\ \blacksquare \\ \end{array} \xrightarrow{\begin{tabular}{c}} \begin{tabular}{c} \blacksquare \\ \blacksquare \\$	€ 🔁 XP			

Le choix des noms de domaine

Un domaine Active Directory dispose toujours de deux noms :

Le nom NETBIOS : permet aux stations antérieurs à Windows 2000 de se connecter au domaine.

Le nom DNS : peut être utilisés par les stations de travail \geq Windows 2000.

Le nom NETBIOS et le nom DNS peuvent être complètement différents.

Le nom NETBIOS apparaît au niveau du champ « Se connecter à » sur les machines Windows NT4, 2000, XP et 2003.

En mode natif 2003, on peut renommer un domaine Active Directory (utilitaire RENDOM). Cela est très déconseillé, voir impossible (avec Exchange 2007).

Les Best Practice :

Définir un nom de domaine DNS générique qui ne reprend pas le nom de la société (sauf si la probabilité que le nom de domaine change est très faible).

Utiliser les suffixes UPN pour ajouter des noms de domaine DNS.

Choisir un nom NetBIOS qui définit l'activité de la société.

Attention, pas de nom de domaine DNS de type SINGLE LABEL DNS NAME.

http://msreport.free.fr/?p=149

http://www.msexchange.org/tutorials/Domain-Rename.html

http://support.microsoft.com/kb/925822/en-us

Les modes de domaine

Définit qui peut être contrôleur au niveau d'un domaine. Débloque des fonctionnalités (groupes globaux membres d'autres groupes globaux...). Pas de retour arrière possible.

Mode de domaine	Fonctionnalités	Type de DC
2000 mixte	Fonctionnalité de base	BDC NT4, DC 2000 / 2003
2000 natif	Groupe global membre d'un autre groupe global.	2000 / 2003 / 2008 / 2008 R2
2003 natif	Nouveau algorithme de réplication / attribut LastlogonTimestamp / authentification sélective.	2003 / 2008 / 2008 R2
2008 natif	DFS-R remplace NTFRS pour la réplication de SYSVOL. AES 128 / 256. Nouveaux attributs sur les logons.Fine Grained Password Policy.	2008 / 2008 R2
2008 R2 natif	Comptes de service gérés.	2008 R2

http://msreport.free.fr/?p=128

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directoryfunctional-levels

Les modes de forêt

Définit qui peut être contrôleur dans la forêt Active Directory. Permet de débloquer des fonctionnalités (relation d'approbation inter-forêts...)

Pas de retour arrière possible sauf depuis le mode natif 2008 R2. Le retour en mode 2008 natif est possible si l'on a pas activé la corbeille Active Directory.

Mode de forêt	Fonctionnalités	Type de DC
2000 natif	Fonctionnalités de base.	BDC NT4 / 2000 / 2003 / 2008 / 2008 R2
2003 natif	Approbation de forêt / Renommage de domaine (à éviter) / support des RODC / amélioration au niveau du KCC et de l'ISTG / désactivation d'attribut.	2003 / 2008 / 2008 R2
2008 natif	Même fonctionnalités que le mode natif 2003.	2008 / 2008 R2
2008 R2 natif	Corbeille Active Directory	2008 R2

http://msreport.free.fr/?p=128

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directoryfunctional-levels
La replication NTDS (1/2)

CN=Administrator Properties	? ×
Attribute Editor Security	
Attributes:	
Attribute Value	<u> </u>
sAMAccountType 805306368 = (NORMAL_USER_	ACCOUNT
sDRightsEffective 15	
showInAddressBook CN=Mailboxes(VLV),CN=All System	n Address
Large Integer Attribute Editor	×
Authors CNChanged	
Attribute: <u>USNChanged</u>	
Value:	
499916	
Clear	Cancel
- Optimized and the second sec	
USIVCIENCE 0130	
whenChanged 15/02/2013 13:30:25 Romance S	tandard Ti
whenCreated 01/03/2011 16:16:02 Romance S	tandard li
	•
New 1	Ches 1
view	Fliter
OK Cancel Apply	Help

A chaque modification, l'attribut USNChanged est incrémenté. Les contrôleurs de domaine comparent ce numéro et détermine ainsi quel contrôleur de domaine dispose de la version la plus récente.

https://www.morgantechspace.com/2014/1 2/Active-Directory-whenChanged-vsusnChanged.html

La replication NTDS (2/2)

Comment un objet est il supprimé ?

L'attribut *USNChanged est* incrémenté et l'objet est Déplacé dans le conteneur *Deleted Users* pendant la TombstoneLifeTime.

Durée de la TombstoneLifeTime : paramétrable, 60 jours par défaut pour un domaine créé avec Windows 2000, 180 pour un domaine créé avec Windows 2003 ou versions ultérieures.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd379509(v=ws.10)

Une fois la période passée, l'objet est réellement supprimé

Pourquoi ce fonctionnement :

C'est pourvoir répliqué la suppression d'un objet

Linguering object :

C'est quand un objet apparaît comme définitivement supprimé (après la période de TombstoneLifeTime et qu'il apparaît comme présent sur un autre dc Le dc sur lequel il apparaît a comme linguering object (zombie). La réplication est bloqué automatiquement <u>https://support.microsoft.com/en-us/help/3141939/description-of-the-lingering-object-</u>

liquidator-tool

https://support.microsoft.com/en-gb/help/910205/information-about-lingering-objects-in-awindows-server-active-directo

Well-known Security Principals

Ils sont au niveau de la partition de configuration Active Directory. https://docs.microsoft.com/en-us/windows/desktop/secauthz/well-known-sids

File Action View Help Image: Second Sec
Image: Security Principal Distinguished Name Image: ADSI Edit Default naming context [FR92SV0001.newlife.lan] CN=Anonymous Logon foreignSecurityPrincipal CN=Anonymous Logon,CN=WellKnown Security Principals,CN Image: CN=Configuration,DC=newlife,DC=lan CN=Configuration,DC=newlife,DC=lan CN=Configuration,DC=newlife,DC=lan CN=Configuration,DC=newlife,DC=lan Image: CN=Configuration,DC=newlife,DC=lan CN=Configuration,DC=newlife,DC=lan CN=Console Logon foreignSecurityPrincipal CN=Batch,CN=WellKnown Security Principals,CN=Configuration Image: CN=DisplaySpecifiers CN=LostAndFoundConfig CN=Creator Group foreignSecurityPrincipal CN=Creator Group,CN=WellKnown Security Principals,CN=CC Image: CN=NerostUpdates CN=NerostUpdates CN=Creator Group foreignSecurityPrincipal CN=Creator Group,CN=WellKnown Security Principals,CN=CC Image: CN=Partitions CN=Partitions CN=Dialup foreignSecurityPrincipal CN=Dialup,CN=WellKnown Security Principals,CN=Configuration Image: CN=Physical Locations CN=Distons foreignSecurityPrincipal CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers,CN=WellKnown Security Principals,CN=Configuration Image: CN=Physical Locations CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domai
Massive Class Distinguished Name Image: Default naming context [FR92SV0001.newlife.lan] Image: CN=Anonymous Logon foreignSecurityPrincipal CN=Anonymous Logon,CN=WellKnown Security Principals,CN Image: CN=Configuration,DC=newlife,DC=lan Image: CN=Configuration,DC=newlife,DC=Configuration,DC=Newlifknown Security Principals,CN=Configuration Image: CN=Configuration,DC=newlife,DC=Configuration,DC=Newlifknown Security Principals,CN=Configuration,DC=newlife,DC=Lan Image: CN=Configuration,DC=Newlifknown Security Principals,CN=Configuration,CN=WellKnown Security Principals,CN=Configuration,CN=WellKnown Security Principals,CN=Configuration Image: CN=Configuration,CN=WellKnown Security Principals,CN=Configuration,CN=WellKnown Security Principals,CN=Configuration Image: CN=Configuratin Image: CN=Configuration,CN=W
Default naming context [FR92SV0001.newlife.lan] CN=Anonymous Logon foreignSecurityPrincipal CN=Anonymous Logon,CN=WellKnown Security Principals,CN Configuration [FR92SV0001.newlife.lan] CN=Authenticated Users foreignSecurityPrincipal CN=Authenticated Users,CN=WellKnown Security Principals,CN CN=Configuration,DC=newlife,DC=lan CN=DisplaySpecifiers CN=Batch foreignSecurityPrincipal CN=Batch,CN=WellKnown Security Principals,CN=CO CN=DisplaySpecifiers CN=Console Logon foreignSecurityPrincipal CN=Console Logon,CN=WellKnown Security Principals,CN=CO CN=Extended-Rights CN=Console Logon foreignSecurityPrincipal CN=Creator Group,CN=WellKnown Security Principals,CN=CO CN=LostAndFoundConfig CN=Creator Group foreignSecurityPrincipal CN=Creator Group,CN=WellKnown Security Principals,CN=CO CN=NTDS Quotas CN=Dialup foreignSecurityPrincipal CN=Dialup,CN=WellKnown Security Principals,CN=CO CN=Physical Locations CN=Physical Locations CN=Dialup foreignSecurityPrincipal CN=Enterprise Domain Controllers,CN=WellKnown Security Principals,CN=Configuration,CN=WellKnown Security Principals,CN=Con
Configuration [FR92SV000 1.newlife.lan] CN=Authenticated Users foreignSecurityPrincipal CN=Authenticated Users, CN=WellKnown Security Principals, CN=Configuration, DC=newlife, DC=lan CN=Configuration, DC=newlife, DC=lan CN=DisplaySpecifiers CN=DisplaySpecifiers CN=Batch, CN=WellKnown Security Principals, CN=Configurat CN=Extended-Rights CN=ForestUpdates CN=Creator Group foreignSecurityPrincipal CN=Creator Group, CN=WellKnown Security Principals, CN=Cc CN=LostAndFoundConfig CN=Authenticated Users foreignSecurityPrincipal CN=Creator Group, CN=WellKnown Security Principals, CN=Cc CN=NTDS Quotas CN=Partitions CN=Dialup, CN=WellKnown Security Principals, CN=Configurat CN=Physical Locations CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Configurat CN=Services CN=Physical Locations CN=Extervice foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Configurat
CN=Configuration,DC=newlife,DC=lan CN=Batch foreignSecurityPrincipal CN=Batch,CN=WellKnown Security Principals,CN=Configurat CN=DisplaySpecifiers CN=Console Logon foreignSecurityPrincipal CN=Console Logon,CN=WellKnown Security Principals,CN=Configurat CN=Extended-Rights CN=Creator Group foreignSecurityPrincipal CN=Creator Group,CN=WellKnown Security Principals,CN=Configurat CN=LostAndFoundConfig CN=Creator Owner foreignSecurityPrincipal CN=Creator Owner,CN=WellKnown Security Principals,CN=Configurat CN=NTDS Quotas CN=Dialup foreignSecurityPrincipal CN=Dialup,CN=WellKnown Security Principals,CN=Configurat CN=Partitions CN=Digest Authentication foreignSecurityPrincipal CN=Dialup,CN=WellKnown Security Principals,CN=Configurat CN=Physical Locations CN=Physical Locations foreignSecurityPrincipal CN=Enterprise Domain Controllers CN=Services CN=Everyone foreignSecurityPrincipal CN=Enterprise Domain Controllers
CN=DisplaySpecifiers CN=Console Logon foreignSecurityPrincipal CN=Console Logon, CN=WellKnown Security Principals, CN=Console Logon, CN=Enterprise Domain Controllers CN=Drestribute CN=Console Logon foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Config CN=Services CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Config CN=Services CN=Enterprise Domain Controllers foreignSecurityPrincipal <t< td=""></t<>
CN=Extended-Rights CN=Creator Group foreignSecurityPrincipal CN=Creator Group, CN=WellKnown Security Principals, CN=Cc CN=ForestUpdates CN=Creator Owner foreignSecurityPrincipal CN=Creator Owner, CN=WellKnown Security Principals, CN=Cc CN=LostAndFoundConfig CN=Dialup foreignSecurityPrincipal CN=Creator Owner, CN=WellKnown Security Principals, CN=Cc CN=NTDS Quotas CN=Dialup foreignSecurityPrincipal CN=Dialup, CN=WellKnown Security Principals, CN=Configurat CN=Partitions CN=Dialup foreignSecurityPrincipal CN=Dialup, CN=WellKnown Security Principals, CN=Configurat CN=Partitions CN=Dialup foreignSecurityPrincipal CN=Dialup, CN=WellKnown Security Principals, CN=Configurat CN=Physical Locations CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Configurat CN=Services CN=Everyone foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Configurat
CN=Porestuppates CN=Creator Owner foreignSecurityPrincipal CN=Creator Owner, CN=WellKnown Security Principals, CN=C CN=LostAndFoundConfig CN=LostAndFoundConfig foreignSecurityPrincipal CN=Dialup, CN=WellKnown Security Principals, CN=C CN=NTDS Quotas CN=Drattions foreignSecurityPrincipal CN=Dialup, CN=WellKnown Security Principals, CN=Configurat CN=Partitions CN=Physical Locations foreignSecurityPrincipal CN=Digest Authentication, CN=WellKnown Security Principals, CN=Configurat CN=Physical Locations CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Configurat CN=Services CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Configurat
CN=EbstAndroundcorning CN=Dialup foreignSecurityPrincipal CN=Dialup,CN=WellKnown Security Principals,CN=Configurat CN=NTDS Quotas CN=Dialup,CN=WellKnown Security Principals,CN=Configurat CN=Digest Authentication,CN=WellKnown Security Principals,CN=Configurat CN=Partitions CN=Physical Locations CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers,CN=WellKnown Security Principals,CN=Configurat CN=Services CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers,CN=WellKnown Security Principals,CN=Configurat
CN=NHDS Quotas CN=Digest Authentication foreignSecurityPrincipal CN=Digest Authentication, CN=WellKnown Security Principals, CN=Partitions CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Physical Locations CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security Principals, CN=Services CN=Everyone foreignSecurityPrincipal CN=Everyone, CN=WellKnown Security Principals, CN=Config
CN=Physical Locations CN=Enterprise Domain Controllers foreignSecurityPrincipal CN=Enterprise Domain Controllers, CN=WellKnown Security P CN=Services CN=Everyone foreignSecurityPrincipal CN=Everyone, CN=WellKnown Security Principals, CN=Config
CN=Services CN=Services CN=Services CN=Services CN=Services CN=Cn=Services CN=Cn=ServiceServi
CN-Interactive Sequences of the Sector Sequences of the Sector Se
CN=Sites Interactive Interactive Interactive CN=Interactive, CN=weikhown Security Principals
CN=WellKnown Security Principals CN=IUSR foreignSecurityPrincipal CN=IUSR,CN=WellKnown Security Principals,CN=Configuration
Default naming context [FR92SV0001.newlife.lan]
Schema [FR92SV0001.newlife.lan]
CN=Network Service foreignSecurityPrincipal CN=Network Service,CN=WellKnown Security Principals,CN=
CN=NTLM Authentication foreignSecurityPrincipal CN=NTLM Authentication,CN=WellKnown Security Principals,
CN=Other Organization foreignSecurityPrincipal CN=Other Organization,CN=WellKnown Security Principals,Cl
CN=Owner Rights foreignSecurityPrincipal CN=Owner Rights,CN=WellKnown Security Principals,CN=Co
CN=Proxy foreignSecurityPrincipal CN=Proxy,CN=WellKnown Security Principals,CN=Configurat
CN=Remote Interactive Logon foreignSecurityPrincipal CN=Remote Interactive Logon,CN=WellKnown Security Principal
CN=Restricted foreignSecurityPrincipal CN=Restricted,CN=WellKnown Security Principals,CN=Config
CN=SChannel Authentication foreignSecurityPrincipal CN=SChannel Authentication,CN=WellKnown Security Princip
CN=Self foreignSecurityPrincipal CN=Self,CN=WellKnown Security Principals,CN=Configuration
CN=Service foreignSecurityPrincipal CN=Service,CN=WellKnown Security Principals,CN=Configura
CN=System foreignSecurityPrincipal CN=System,CN=WellKnown Security Principals,CN=Configura
CN=Terminal Server User foreignSecurityPrincipal CN=Terminal Server User, CN=WellKnown Security Principals,
CN=This Organization foreignSecurityPrincipal CN=This Organization,CN=WellKnown Security Principals,CN=

TP: Création d'un domaine 1/2

Renommer la machine suivant la convention de nommage indiquée par le formateur (DCTESTLABX).

Configurer le serveur en adressage IP fixe (valider la configuration DNS).

Installer le rôle serveur DNS.

Installer le rôle Active Directory Domain Services.

Jusqu'à Windows Server 2008 R2, exécuter l'assistant DCPROMO (Domain Controller Promotion).

<u>A partir de Windows Server 2012, utiliser le Server Manager (ajout du rôle Active Directory</u> Domain Services).



\overline Assistant Installation des services de domaine Active Directory

Compatibilité du système d'exploitation

Les paramètres de sécurité étendus dans Windows Server 2008 et Windows Server 2008 R2 affectent les versions précédentes de Windows

Les contrôleurs de domaine Windows Server 2008 et "Windows Server 2008 R2 " offrent un nouveau paramètre par défaut mieux sécurisé, "Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ". Ce paramètre empêche Microsoft Windows et les " clients " non-Microsoft SMB d'utiliser des algorithmes de chiffrement faibles de type NT 4.0 dans des sessions sur canal sécurisé vers des contrôleurs de domaine Windows Server 2008 ou "Windows Server 2008 R2". Désormais, les opérations et applications qui requièrent un canal sécurisé servi par un contrôleur de domaine Windows Server 2008 ou "Windows Server 2008 R2" peuvent échouer.

Les plateformes concernées incluent Windows NT 4.0, ainsi que les " clients " non-Microsoft SMB et les périphériques NAS non compatibles avec les algorithmes de chiffrement forts. Certaines opérations sur les clients exécutant une version de Windows antérieure à Vista avec le Service Pack 1 sont également concernées, notamment les jonctions aux domaines effectuées par l'outil de migration Active Directory ou les Services de déploiement Windows.

Pour plus de détails à ce sujet, voir l'article 942564 (http://go.microsoft.com/fwlink/? LinkId=104751).

TP : Création d'un domaine 2/2

Assistant Installation des services de domaine Active Directo	ry 🐻 As	ssistant Installati	on des services de don	naine Active Directory	\overline Assistant Installation des se	rvices de domaine Active Directory
Choisissez une configuration de déploiement Vous pouvez créer un contrôleur de domaine pour une forêt nouvelle ou existante.		Nommez le domaine racine de la forêt Le premier domaine de la forêt est le domaine racine de la forêt. Il porte é nom de la forêt.		Nom de domaine NetBIOS Il s'agit du nom que les utilisateurs des versions antérieures de Windows utiliseront pour identifier le nouveau domaine.		
Forêt existante Acouter un contrôleur de domaine à un domaine existant Créer un nouveau domaine dans une forêt existante Ce serveur va devens le premier contrôleur de domaine du Créer une nouvelle racine d'arborescence de domaine	nouveau doma se lieu d'un no	Entrez le nom de o Nom de domaine o formation10.lan	domaine complet du nouvea	au domaine racine de forêt. de forêt :	L'Assistant génère un nom N que si vous avez sélectionné le nom par défaut. Acceptez le nom généré par l Suivant. Nom de domaine NetBIOS :	etBIDS par défaut. Cette page de l'Assistant ne s'affiche le mode avancé ou si l'Assistant a détecté un conflit dans 'Assistant ou tapez un nouveau nom, puis cliquez sur IMSREPORTEORMI
domaine entent		Exemple : corp.co	ntoso.com			
Assistant Installation des services de doma Définir le niveau fonctionnel de la forêt Sélectionnez le niveau fonctionnel de la forêt.	Assistant Instal Définir le nivea Sélectionnez l	lation des servic u fonctionnel du le niveau fonctionn	Assistant Installation des Options supplémentaires Sélectionnes des options	services de domaine Active Direc pour le contrôleur de domaine	tory Assistant Installa	sible de créer une délégation pour ce serveur DNS car ente faisant autorité est introuvable ou elle n'exécute sur DNS Windows. Si vous procédez à întégration avec ructure DNS existante, yous devez manuellement créer tion avec ce serveur DNS dans la zone parente pour
Niveau fonctionnel de la forêt : Vindows 2000 Vindows 2000 Windows Server 2003	Niveau fonctio Windows 2 Windows 200 Windows Ser Windows Ser	onnel du domaine : 20 natif 10 natif ver 2003 ver 2008	 Serveur DNS Catalogue global Contrôleur de domai Informations supplément Le premier contrôleur de global et ne peut pas êt Nous vous recommand. 	ne en lecture seule (RODC) taires : e domaine d'une forêt doit être un servet re un contrôleur de domaine en lecture s ons d'installer le service Serveur DNS su	r de catalogue reule (RODC), rr le premier	Solution de hons habe en denors du domaine « J.lan ». Sinon, aucune action n'est requise. s continuer ?
Windows Server 2008 Minister Casuar 2009 D2 Assistant Installation des services de domaine Active D Emplacement de la base de données, des fichiers jour	Windows Ser Directory naux et de SYSVOL	ver 2008 R2 Assistant I Mot de pa	contrôleur de domaine. Installation des services des services des services des services des services des res	de domaine Active Directory stauration des services d'anı	a Assistant Installe Résumé nuaire	tion des services de domaine Active Directory
Active Directory, les fichiers journaux et SYSVDL.					Vérifiez vos sél Configuer ce s d'une nouvelle Le nouveau no	ections : erveur en tant que premier contrôleur de domaine Active Directory forêt. m de domaine est « formation10.lan ». C'est aussi le nom de la
Pour de meilleures performances et une meilleure récupératio données et les fichiers journaux sur des volumes séparés. Dossier de la base de données :	n, stockez la base de	Le com compte Attribue de ce	pte d'administration de restaur d'administrateur de domaine. z un mot de passe au compte ontrôleur de domaine en mode commandens de obaieur un oct	ation des services d'annuaire est d'administrateur qui sera utilisé loi e Restauration des services d'ann t de nesse fort	différent du nouvelle forêt. Le nom NetBIO s du démarrage Niveau fonctior uaire. Nous Niveau fonctior	S du domaine est « MSREPORTFORM ». nel de la forêt : Windows 2000 nel du domaine : Windows 2000 natif
C:W/indows/NTDS Dossier des fichiers journaux : C:W/indows/NTDS	Parcourir	Mot de	passe :		Site : Default-Fi Pour modifier ur sur Suivant.	rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rst-Site-Name rs
Dossier SYSVOL : C:\Windows\SYSVOL	Parcourir	Confirm	er le mot de passe : pir plus sur le <u>mot de passe d</u> e	restauration des services d'annua	Vous pouvez er réponses pour l installation sans En savoir plus s	xporter ces paramètres dans un fichier de es utiliser avec d'autres opérations d' assistance. ut jutilisation d'un fichier de réponse

TP : Ajout d'un second DC 1/3

Définir comme serveur DNS principal, l'IP du premier contrôleur de domaine. Expliquer pourquoi ?

Faire un ping DCTESTLABX.formationX.lan puis ipconfig /displaydns Faire ensuite un ipconfig /flushdns puis ipconfig /displaydns. Expliquer. Lancer l'assistant DCPROMO. Une fois l'écran de bienvenue se lance, aller le gestionnaire de rôle dans la section Rôles de Server. Que constatez vous ? Suivre les indications sur les captures d'écran.

Propriétés de : Protocole Internet version 4 (TCP/IPv4)	<u>न</u> Assistant Installatio	on des services de domaine Active Directory	🚮 Assistant Inst	allation des services de domaine Active Direc
Général Les paramètres IP peuvent être déterminés automatiquement si v réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau. C Obtenir une adresse IP automatiquement C Utiliser l'adresse IP suivante : Adresse IP : 192 . 168 . 0 161 Masque de sous-réseau : 255 . 255 . 0 Densersie au défectue 200 . 00 . 00 . 00 . 00 . 00 . 00 . 00		Assistant Installation des services de domaine Active Directory Cet Assistant vous aide à installer les services de domaine Active Directory (AD DS) sur ce serveur, faisant du serveur un contrôleur de domaine Active Directory. Pour continuer, cliquez sur Suivant.	Choisissez un Vous pouve	e configuration de déploiement z créer un contrôleur de domaine pour une forêt nouv
Passereile par deraut : 192 : 168 . 0 . 254 O Obtenir les adresses des serveurs DNS automatiquement O Utiliser l'adresse de serveur DNS suivante : Serveur DNS préféré : 192 . 168 . 0 . 160 Serveur DNS auxiliaire : 192 . 168 . 0 . 161		 Utiliser l'installation en mode avancé En savoir plus sur les options supplémentaires disponibles dans l'<u>installation en mode avancée</u>. 	 Forêt ex Ajo 	istante uter un contrôleur de domaine à un domaine existant
Assistant Installation des services de domaine Active Directo Informations d'identification réseau Spécifies le nom de la forêt dans laquelle l'installation s'effectuera e d'identification du compte disposant des privilèges nécessaires pou l'installation.	t les informations reffectuer	Assistant Installation des services de domaine Sélectionnez un domaine	e Active Directory	Sélectionnez un site Sélectionnez un site
Tapez le nom d'un domaine de la forêt dans laquelle vous prévoyez contrôleur de domaine : [formation10.lan	d'installer ce			
Spécifiez les informations d'identification de compte à utiliser pour el C Mes informations d'identification de connexion actuelles (SFR2) Impossible de sélectionner les informations d'identification at a cet ordinateur. Des informations d'identification de donain	ffectuer l'installation : Administrateur) ctuelles car elles sont locales e sont nécessaires.	Sélectionnez un domaine pour ce contrôleur de do	omaine supplémentaire.	Utiliser le s _{ite} con ^{espond}
 Autres informations d'identification : administrateur@formation10.lan En savoir plus sur <u>qui peut installer les services de domaine Active f</u> 	Définir	Domaines : formation10.1an (domaine racine de la for	êt)	Site Site Default-First-Site-Name

TP : Ajout d'un second DC 2/3

En mode avancé, il est possible de spécifier depuis quel contrôleur de domaine on réplique. Pour les sites avec une très faible bande passante, il est même possible de répliquer depuis une sauvegarde. Pour plus d'informations : http://www.laboratoire-microsoft.org/articles/win/dcpromo_adv/

Les cases « *Serveurs DNS* » et « *Catalogue Global* » doivent être cochées. Sans catalogue global, seul les administrateur du domaine peuvent ouvrir une session.

Sans serveur DNS, les stations de travail ne peuvent pas localiser les contrôleurs de domaine.

TP : Ajout d'un second DC 3/3

Vérifier le fonctionnement de la réplication avec Sites et Services Active Directory

Si la réplication n'est pas fonctionnelle :

Définir sur tous les DC le même serveur DNS principal.

Vérifier sur ce dernier qu'il existe une zone DNS correspondant au nom de domaine DNS.

Vérifier si cette zone autorise les mises à jour dynamiques.

Taper les commandes suivantes :

Ipconfig /flusddns Ipconfig /registerdns Net stop netlogon Net start netlogon Repadmin /kcc

Les chemins LDAP :

Nom unique relatif LDAP : OU=Production Nom unique LDAP : *CN=sophie mathieu2,Ou=enfant,OU=Migration,DC=ORGA2,DC=LAN* Nom canonique : orga2.lan/Production

Commutateur	Signification
OU=	Unités d'organisation
CN=	Objets
DC=	Domaine
O=	Organisation (Exchange).

Mise en pratique :

Créer deux comptes utilisateurs appelés Sophie Mathieu2 et guillaume.mathieu. Aller dans l'éditeur d'attribut de la console Utilisateurs et Ordinateurs Active Directory. Prendre la valeur du champ *DistinguishedName*.

Les rôles FSMO et le Catalogue Global 1/2

5 rôles FSMO (*Flexible Single Master Operation*) et le Catalogue Global :

- Emulateur PDC : serveur de temps du domaine. Gère les changements de mots de passe. En mode 2000 mixte, permet aux BDC NT4 de se synchroniser avec le DC jouant le rôle d'Emulateur PDC. Gère la création des relations d'approbation. Gère la topologie DFS.
- Maître RID : permet d'allouer des pool de 500 SID. Si ce rôle n'est plus en ligne, les contrôleurs de domaine ne peuvent plus obtenir de nouveau pool de SID. Si leur pool est épuisé, ils ne peuvent plus créer de nouveaux objets.
- Maître d'infrastructure : permet de gérer les objets fantômes (un objet fantôme est créé lorsque l'on joint un objet du domaine B dans un groupe du domaine A).
- Maître d'attribution de noms de domaine : valide s'il n'y a pas de conflit(s) de noms DNS au niveau des domaines de la forêt et des domaines approuvés.
- Maître de schéma : permet de gérer les modifications effectuées au niveau du schéma Active Directory.

Les rôles FSMO et le Catalogue Global 2/2

Le serveur de Catalogue Global : contient une réplique des principaux attributs de tous les objets de la forêt. Permet de faire des recherches dans l'annuaire. Gère les groupes universels. Si plus de serveur de Catalogue global, on ne peut plus ouvrir de sessions (sauf les administrateurs du domaine).

Mettre tous les DC en tant que serveur de « *Catalogue global* » <u>ou</u> ne pas mettre le contrôleur de domaine qui joue le rôle de Maître d'Infrastructure en tant que serveur de Catalogue Global.

http://support.microsoft.com/kb/324801/en-us http://support.microsoft.com/kb/223346/en-us http://support.microsoft.com/kb/839879/en-us http://support.microsoft.com/kb/910202/en-us http://support.microsoft.com/kb/839879/en-us

TP : déterminer qui a les rôles FSMO

Pour déterminer qui a les 5 rôles FSMO en ligne de commande : *netdom query fsmo* Utiliser la commande *Dcdiag*.

📕 dcdiag	- Notepad
File Edit	Format View Help
	Object DN: CN=DFSR-LocalSettings,CN=FR75020DC1,OU=Domain Controllers,DC=newlife,DC=lan Error: 2 (The system cannot find the file specified.) Domain Controller: FR925V0001.newlife.lan Polling Cycle: 60 A warning event occurred. EventID: 0x80001206 Time Generated: 02/18/2013 20:07:04 Event String: The DFS Replication service initialized SYSVOL at local path C:\windows\SYSVOL\domain and is waiting to perform in
	Additional Information: Replicated Folder Name: SYSVOL Share Replicated Folder ID: EF47EB4D-7EFA-48C1-9DBB-20459E8F303F Replication Group Name: Domain System Volume Replication Group ID: 10FA23ED-C540-4043-8FB2-E6D2DC732942 Member ID: 03392200-2E35-41A9-BC6E-A4BE9DEC366 Read-only: 0 FR75020DC1 failed test DESREVent
s	Starting test: SysvolCheck * The File Replication Service SYSVOL ready File Replication Service's SYSVOL is ready File Replication Service's ASYSVOL is ready File Replication Service's SYSVOL Service SysVolCheck Starting test: KccEvent
5	* The KCC Event log test Found no KCC errors in "Directory Service" Event log in the last 15 minutes.
	Role Schema Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan Role Domain Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan Role PDC Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan Role Rid Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan Role Infrastructure Update Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan Role Infrastructure Update Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan Role Infrastructure Update Owner = CN=NTDS Settings,CN=FR92SV0001,CN=Servers,CN=Paris,CN=Sites,CN=Configuration,DC=newlife,DC=lan

TP : transfert du Schema Master via console

Taper la commande "*regsvr32 schmmgmt.dll*" pour afficher la composant logiciel enfichable "Maître de schéma",

Aller dans me menu *Démarrer*, cliquer « *Exécuter* » puis taper MMC. Cela permet de lancer une console MMC vierge. « *Cliquer sur Ajouter un composant logiciel enfichable* ».

Sélectionner le composant « Maître de Schéma ».

<u>Astuce : il faut se connecter sur le DC cible sur lequel on veut transférer le rôle car par défaut la console Maître de Schéma se connecte sur le contrôleur de domaine qui joue le rôle de Maître de Schéma.</u>





Les partitions d'annuaires 1/4 :

Active Directory est découpé en partitions :

- Schéma : contient l'ensemble des attributs et des classes (extensible).
- Configuration : contient la configuration de l'annuaire Active Directory (les sites, les partitions d'annuaires...).
- Domaine (1 par domaine) : contient les données utiles (les comptes utilisateur / ordinateur, les groupes...).
- ForestDnsZones : contient les entrées des zones DNS publiées sur tous les serveurs DNS de la forêt.
- DomainDnsZones (1 par domaine) : contient les entrées des zones DNS publiées sur tous les serveurs DNS du domaine.

Pour se connecter à certaines partitions, il faut se connecter avec un éditeur bas niveau Active Directory : ADSIEDIT.

Modification ADSI	Paramètres de connexion	Modification ADSI	Modification ADSI
Modification AD5I Fichier Action Affichage ? Modification Affichage ? Modification Affichage Affichage	Paramètres de connexion Nom : Contexte d'attribution de noms par défaut Chemin d'accès : LDAP://SFR1.formation10.lan/Contexte d'attribution de Point de connexion	Modification ADSI Fichier Action Affichage ? Affi	Picher Action ADSI Ficher Action Afribage ? Image: State and State
Actualiser	Contexte Vattribution de noms par défaut Ordin Configuration SRootDSE [:Schéma Configuration Schéma Configuration (• Par défaut (le domaine ou le serveur auquel vous vous êtes connecté) Utiliser le chiffrement SSL	OU=Promation CN=Usanaged Service A CN=Managed Service A CN=MINDS Quotas OU=Production OU=Production OU=Production CN=Program Data CN=Users OU=Vente OU=Vente CN=Vent	Ok-Lotzkhafbund physicaDelwey0ffic 172 Bureau de la coline physicaDelwey0ffic 172 Bureau de la coline Ok-Mr05 Quotas OU-Production OU-Production OU-Production OU-Production Ok-System Ok-Ok-System Ok-Ok-System Ok-System Ok-System Ok-S

Pro	priétés de : OU	=XP					?
É	diteur d´attributs	Sécurit	é				
	Attributs :						
	Attribut		Valeur				
	distinguishedNa	me	OU=XF	P,OU:	=Administrati	on des veni	tes,DC=form
	dSCorePropaga	ationD	08/06/	2010	13:48:02 P	aris, Madrid,	; 08/06/201
	instanceType		0x4 = (WRI	TE)		
	name		XP				
	objectCategory		CN=Or	ganiz	ational-Unit,	CN=Schem	a,CN=Config
	objectClass		top; org	ganiz	ationalUnit		
	objectGUID		08ef33	44-5	106-4c21-9b	71-843b75f	ac2d4
	ou		×Р				
	replPropertyMet	aData	AttID	Ver	Loc.USN	Or	g.DSA
	uSNChanged		14293				
	uSNCreated		14227				
	whenChanged		08/06/	2010	13:47:33 P	aris, Madrid	
	whenCreated		08/06/	2010	13:42:51 P	aris, Madrid	

Les partitions d'annuaires 2/4 :

Modification ADSI			
Fichier Action Affichage ?			
🗢 🔿 🙍 🖬 🖬 🖉			
Modification ADSI Configuration [SFR1.formation: CN=Configuration,DC=forr CN=DisplaySpecifiers CN=Extended-Rights CN=ForestUpdates CN=LostAndFoundConl CN=NTDS Quotas CN=Partitions CN=Services CN=Sites CN=Sites CN=WellKnown Securit*	Nom CN=670bb63f-faaa-48f1-91c8-220c3cbfcfb6 CN=acb0552a-ec6f-46e3-a59e-03cd1b343e31 CN=Enterprise Configuration CN=Enterprise Schema CN=MSREPORTFORM	Nom de la partition du répertoire DC=DomainDnsZones,DC=formation10,DC=lan DC=ForestDnsZones,DC=formation10,DC=lan CN=Configuration,DC=formation10,DC=lan CN=Schema,CN=Configuration,DC=formation10,DC=lan DC=formation10,DC=lan	Clas cros cros cros cros

Modification ADSI			
Fichier Action Affichage ?			
🗢 🔿 🙋 📅 🚺 🗶 🖨 😣			
2 Modification ADSI	Nom	Classe	Nom unique
🖃 📋 Schéma [SFR1.formation10.lar	CN=account	classSchema	CN=account,CN=Schema,CN=Configuration,DC=formal
🙀 CN=Schema, CN=Configura	CN=Account-Expires	attributeSche	CN=Account-Expires, CN=Schema, CN=Configuration, DC
	CN=Account-Name-History	attributeSche	CN=Account-Name-History,CN=Schema,CN=Configurat
	CN=ACS-Aggregate-Token-R	attributeSche	CN=ACS-Aggregate-Token-Rate-Per-User,CN=Schema,
	CN=ACS-Allocable-RSVP-Ban	attributeSche	CN=ACS-Allocable-RSVP-Bandwidth,CN=Schema,CN=Co
	CN=ACS-Cache-Timeout	attributeSche	CN=ACS-Cache-Timeout, CN=Schema, CN=Configuration
	CN=ACS-Direction	attributeSche	CN=ACS-Direction, CN=Schema, CN=Configuration, DC=
	CN=ACS-DSBM-DeadTime	attributeSche	CN=ACS-DSBM-DeadTime,CN=Schema,CN=Configuration
	CN=ACS-DSBM-Priority	attributeSche	CN=ACS-DSBM-Priority,CN=Schema,CN=Configuration,
	CN=ACS-DSBM-Refresh	attributeSche	CN=ACS-DSBM-Refresh,CN=Schema,CN=Configuration
	🛛 🚍 ann agus suithe agus chuidhe		CN ACCELLE ACCELLED ON CLEAR ON CLEAR

Les partitions d'annuaires 3/4 :

Connection Settings × Name: Default naming context Path: LDAP://WIN-2RF3R463H09.orga2.lan/DC=ForestDnsZones,dc=c	✓ ADSI Edit File Action ✓ ➡ ✓ ✓ ➡ ✓			
Connection Point Select or type a Distinguished Name or Naming Context: DC=ForestDnsZones,dc=orga2,dc=lan Select a well known Naming Context: Default naming context Computer Select or type a domain or server: (Server Domain [:port]) Select or type a domain or server: (Server Domain [:port]) Select or type a domain or server that you logged in to) Use SSL-based Encryption Advanced OK Cancel	VDSI Edit Configuration [WIN-2RF3R463H09.orga2.lan] Schema [WIN-2RF3R463H09.orga2.lan] CN=Schema,CN=Configuration,DC=orga2,IC Default naming context [WIN-2RF3R463H09.org DC=ForestDnsZones,dc=orga2,dc=lan CN=LostAndFound CN=MicrosoftDNS DC=_msdcs.msreportexch.local DC=msreportexch.local CN=NTDS Quotas	Name DC=@ DC=_kerberostcp.Default-F DC=_ldaptcp.db7055c3-42 DC=_ldaptcp.dc DC=_ldaptcp.Default-First DC=_ldaptcp.Default-First DC=_ldaptcp.Default-First DC=_ldaptcp.Default-First DC=_ldaptcp.Default-First DC=_ldaptcp.gc DC=_ldaptcp.pdc DC=_ldaptcp.pdc DC=gc	Class dnsNode dnsNode dnsNode dnsNode dnsNode dnsNode dnsNode dnsNode dnsNode dnsNode dnsNode	Distinguished Name DC=@,DC=_msdcs.orga2.lan,CN=MicrosoftDNS DC=_kerberostcp.dc,DC=_msdcs.orga2.lan,Cl DC=_kerberostcp.Default-First-Site-Namesit DC=_ldaptcp.dc,DC=_msdcs.orga2.lan,CN=M DC=_ldaptcp.Default-First-Site-Namesites.di DC=_ldaptcp.Default-First-Site-Namesites.gi DC=_ldaptcp.Default-First-Site-Namesites.gi DC=_ldaptcp.gc,DC=_msdcs.orga2.lan,CN=M DC=_ldaptcp.pdc,DC=_msdcs.orga2.lan,CN=M DC=_ldaptcp.pdc,DC=_msdcs.orga2.lan,CN=M DC=_ldaptcp.pdc,DC=_msdcs.orga2.lan,CN=M

Mise en pratique :

Lancer la console « Utilisateurs et Ordinateurs Active Directory ».

Créer l'OU Test à la racine du domaine.

Créer le compte utilisateur test1 (mot de passe : P@ssword) dans l'OU Test.

Créer le groupe global testgp1 dans l'OU Test.

Ajouter l'utilisateur test1 au groupe global testgp1.

Lancer ADSIEDIT. Se connecter à la partition de domaine.

Localiser la ressource testgp1 et éditer l'objet utilisateur (bouton droit, *Propriétés*). Aller au niveau de l'attribut « *member* » et supprimer l'entrée test1.

Relancer la console « *Utilisateurs et Ordinateurs Active Directory* » et valider que l'utilisateur test1 n'est plus membre du groupe testgp1.

Les partitions d'annuaires 4/4 :

📴 Active Directory Users and Com	puters			
File Action View Help				
🗢 🔿 🖄 📊 🖌 💼	1 🖸 🗟 🛛 🖬	1 🙁 🐮 🍞 .	2 🗽	
Active Directory Users and Comput Active Directory Users and Comput Graphic Saved Queries Graphic Saved Queries Graphic Saved Queries Graphic Saved Queries Graphic Scores Graphic Scores Graphic Saved Queries Graphic Scores Graphic Saved Queries Graphic Scores Graphic Saved Queries Graphic Saved Queries G	Name test1 Testgp1 Testgp1 Object General Members: Name test1	Type D User Security Group ties Security Members Active Directory orga2.lan/Test	escription Attrib Member Of	ute EdilEdi Managnag Ider
Test				



Multi-valued Distinguished Name With Security Principal Editor

х	x
_	

-ie Action View Help		
ADSI Edit Default naming context [WIN-2RF3R463Hi DE=orga2, DC=lan CN=Builtin OU=Cible OU=Cibl	CN=Testgp I Properties Attribute Editor Security Attributes:	
OU=Domain Controllers CN=EoreignSecurityPrincipals CN=LostAndFound CN=Managed Service Accounts OU=Microsoft Exchange Security (CN=Managed Service Accounts OU=Microsoft Exchange System O OU=Microsoft Exchange System O OU=Microsoft Exchange System O CN=Program Data CN=Program Data CN=System OU=Source CN=Test CN=Testgp1 CN=Users	mail (not set) mail (not set) managedBy (not set) mAPIRecipient (not set) member CN=test1,DU=Test,DC=orga2,DC=k memberilid (not set) msDS-AzBizRule (not set) msDS-AzBizRule_ang (not set) msDS-AzEizRule (not set) msDS-AzEizRule (not set) msDS-AzEizRule (not set) msDS-AzEizRule (not set) msDS-AzEoperciData (not set) msDS-AzDipetGuid (not set) msDS-ConsistencyC (not set)	n

🕅 ADST Edi

lici-talucu Discinguis	neu Name mich Securicy Frincipal cultor		l
Attribute: memb Yalues:	ber		
Name	Container	Distinguished Name / SID	
test1	orga2.lan/Test	CN=test1,OU=Test,DC=orga2,D	
Add Windows Account.		Remove	
Add DN		K	
		OK Cancel	
			~

TP : déplacement de zone DNS

Créer une zone DNS appelée google2.fr.

Intégrer la zone dans l'annuaire. Cocher la case « Enregistrer la zone dans Active Directory ...». Sélectionner ensuite « Vers tous les contrôleurs de domaine dans ce domaine... »

Créer un enregistrement de type A appelé www avec l'IP 192.168.0.1. Cela va créer une entrée dans System\Microsoft DNS.

Assistant Nouvelle zone

Type de zone

Publier maintenant cette zone dans la *ForestDnsZones* puis dans la *DomainDnsZones*. Pour cela, aller dans les propriétés de la zone, onglet « Général ». Au niveau de Réplication, cliquer sur Propriétés. Sélectionner choix 1 puis choix 2.



Nom de la zone Quel est le nom de la nouvelle zone ?

> Le nom de la zone spécifie la partie de l'espace de noms DNS pour laquelle ce serveur fait autorité. Il peut s'agir du nom de domaine de votre société (par exemple, microsoft.com) ou d'une partie du nom de domaine (par exemple, nouvelle_zone.microsoft.com). Le nom de zone n'est pas le nom du serveur DNS.

Nom de la zone : google2.fr



Le serveur DNS prend en charge différents types de zones et de stockages.

Assistant Nouvelle zone

Étendue de la zone de réplication de Active Directory

Vous pouvez sélectionner la façon dont les données DNS doivent être répliquées sur votre réseau.

Choisissez la façon dont les données de la zone doivent être répliquées :

- C Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : formation10.lan
- C Vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : formation10.lan
- Vers tous les contrôleurs de ce domaine (compatibilité avec Windows 2000) : formation10.lan
- O Vers tous les contrôleurs de domaine spécifiés dans l'étendue de cette partition d'annuaire :

Nouvel hôte

Nom (utilise le domaine parent si ce champ est vide) :

www

Nom de domaine pleinement qualifié (FQDN) :

www.google2.fr.

Adresse IP :

214.20.1.1

🔀 Créer un pointeur d'enregistrement PTR associé

¹³Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom de propriétaire

Le schéma

Vocabulaires :

- > Attributs : propriétés d'un objet (exemple : description, société, numéro de fax...).
- Méthodes : actions que l'on peut faire sur un objet (déplacer, supprimer..)
- Classes : types d'objets (exemple de classe d'objet : groupe, utilisateur).
- Schéma : ensemble des attributs, des méthodes et des classes.

Le schéma Active Directory est extensible. Cela permet d'ajouter des attributs ou des classes. On ne peut pas modifier les méthodes. Certaines applications comme Exchange (setup.com/PrepareAD) nécessite d'étendre le schéma. <u>http://technet.microsoft.com/fr-fr/library/bb727029.aspx</u> <u>http://technet.microsoft.com/en-us/library/bb727064.aspx</u> <u>http://technet.microsoft.com/en-us/library/cc784557(WS.10).aspx</u>

🚟 Console1 - [Console Root	Active Directory Schema	WIN-2RF3R463	H09.orga2.lan]\Classes]
🚠 File Action View Fav	orites Window Help			
🗢 🔿 🖄 🛅 🙆	2			
🧰 Console Root 🛛 🔺	Name	Туре	Status	Description
🖃 🧱 Active Directory Sch	T account	Structural	Active	The account object class i
🖃 🧮 Classes	T _a acsPolicy	Structural	Active	ACS-Policy
t account	T aCSResourceLimits	Structural	Active	ACS-Resource-Limits
- C aCSPolicy	TacsSubnet	Structural	Active	ACS-Subnet
	■ t addIn	Structural	Active	ms-Exch-Add-In
-La aCSSubnet	T addressBookContainer	Structural	Active	Address-Book-Container
	T addressTemplate	Structural	Active	Address-Template
	T addrType	Structural	Active	ms-Exch-Addr-Type
	T adminExtension	Structural	Active	ms-Exch-Admin-Extension
	T applicationEntity	Structural	Active	Application-Entity
daminexcon		C	A	Aller During

Mise à jour/extension du schéma

Pourquoi mettre à jour son schéma Active Directory :

Installation de produit qui s'appuie sur Active Directory comme Exchange. ADPREP /Forestprep : permet d'ajouter les attributs et les classes permettant l'installation des contrôleurs de domaine de version Windows supérieur (exemple, DC 2008 R2 dans un domaine géré initialement par des DC Windows 2000).

Best Practice :

Effectuer la manipulation sur le maître de Schéma.

Désactiver la réplication entrante et sortante sur le maître de schéma pendant la phase de mise à niveau du schéma (voir commande ci-dessous).

C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 +DISABLE_OUTBOUND_REPL Current DSA Options: IS_GC New DSA Options: IS_GC DISABLE_OUTBOUND_REPL

C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 +DISABLE_INBOUND_REPL Current DSA Options: IS_GC DISABLE_OUTBOUND_REPL New DSA Options: IS_GC DISABLE_INBOUND_REPL DISABLE_OUTBOUND_REPL

C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 -DISABLE_INBOUND_REPL Current DSA Options: IS_GC DISABLE_INBOUND_REPL DISABLE_OUTBOUND_REPL New DSA Options: IS_GC DISABLE_OUTBOUND_REPL

C:\Users\Administrator>repadmin /options WIN-2RF3R463H09 -DISABLE_OUTBOUND_REPL Current DSA Options: IS_GC DISABLE_OUTBOUND_REPL New DSA Options: IS_GC

TP schéma : paramétrage des attributs

Créer une MMC vierge et ajouter le composant logiciel enfichable « *Maître de Schéma* ».

Vérifier si les attributs « *Description* » et « *Department* » sont dans le Catalogue Global (case « Répliquer cet attribut dans le catalogue global).

Sélectionner l'attribut « *Title* ». Cocher la case pour que ce dernier soit conservé lors de la copie d'objet (compte utilisateur).

roprieces de : cicle	
Général	
title	;
Description :	Title
Nom commun :	Title
ID_d´objet X.500 :	2.5.4.12
⊢Syntaxe et étendue-	
Syntaxe :	Chaîne Unicode
Minimum :	1
Maximum :	128
Cet attribut est à val	eur simple.
 L'attribut est actif Indexer cet attribut Résolution de nom Répliquer cet attrib L'attribut est copié Indexer cet attribut 	s ANR (Ambiguous Name Resolution ut dans le catalogue global lors de la duplication de l'utilisateur pour des recherches en conteneur

Les relations d'approbation 1/4

Les relations d'approbations permettent de partager des accès entre deux annuaires différents. Tous les domaines de la même forêt s'approuvent.

A approuve B : on peut définir des permissions sur les ressources du domaine A avec des utilisateurs / groupes du domaine B. Les utilisateurs de la forêt B sont automatiquement membres du groupe « *Utilisateurs authentifiés* » du domaine A.

L'authentification sélective permet de donner aucun droit par défaut entre deux domaines qui s'approuvent. Il faut déléguer au niveau de chaque compte ordinateur les droits « *Lire* » et « *Authentifier* » pour permettre un accès avec des permissions équivalentes à « *Utilisateurs Authentifiés* »

Pas d'approbation entre deux domaines avec un nom de domaine NETBIOS ou un nom de domaine DNS identique.

L'Emulateur PDC de chaque domaine doit être en ligne lorsque l'on crée une relation d'approbation entre deux domaines.

Les relations d'approbations peuvent être :

- Transitive : si A approuve B et que B approuve C, alors A approuve C.
- Implicite : automatique (relation d'approbation entre domaines de la même forêt).
- Bidirectionnelle : A approuve B et B approuve A.

Les relations d'approbations entre domaines de la même forêt sont transitives, implicites et bidirectionnelles.

Les relations d'approbation 2/4

😽 Active Directory Domain	s and Trusts			
File Action View Help				
🗢 🔿 🖄 📅 🗔 🗟				
Active Directory Domains ar 🍈 👘 orga2.lan	nd Trusts [\	Name		
orga2.lan Properties			? ×	
General Trusts Managed I	Зу			
Domains trusted by this doma	ain (outgoing tr	usts):		
Domain Name	Trust Type	Transitive	Properties	
			Remove	
Domains that trust this domai	in (incoming tru	ists):		
Domain Name	Trust Type	Transitive	Properties	
			Remove	
New Trust				
ОК	Cancel	Apply	Help	

New Trust Wizard

Trust Name

You can create a trust by using a NetBIOS or DNS

Type the name of the domain, forest, or realm for this trumust type a DNS name.

Example NetBIOS name: supplier01-int Example DNS name: supplier01-internal.microsoft.com

Name:

msreportexch.local

🍰 DNS Manager	
File Action View Help	
 DNS WIN-2RF3R463H09 Imade Good Logs Forward Lookup Zones Forward Lookup Zones Imades.msreportexch.local Imsreportexch.local Ims	Name dc domains gc pdc (same as p (same as p 7f8bde83-a

Les relations d'approbation 3/4

orga2.lan Properties			? ×
General Trusts Managed B	3y		
Domains trusted by this doma	ain (outgoing tr	usts):	
Domain Name	Trust Type	Transitive	Properties Remove
Domains that trust this domai	n (incoming tru Trust Type	ısts): Transitive	Properties Remove
MAN Trust			
ОК	Cancel	Apply	Help

New Trust Wizard

Trust Name

You can create a trust by using a

Type the name of the domain, forest, must type a DNS name.

Example NetBIOS name: supplier01-in Example DNS name: supplier01-intern

Name:

msreportexch.local

New Trust Wizard

Trust Type

This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.

Select the type of trust you want to create.

C External trust

An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

Eorest trust

A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.

New Trust Wizard

Direction of Trust

You can create one-way or two-way trusts.

Select the direction for this trust.

Two-way

Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

- One-way: incoming Users in this domain can be authenticated in the specified domain, realm, or forest.
- C One-way: outgoing

Users in the specified domain, realm, or forest can be authenticated in this domain.

Les relations d'approbation 4/4

New Trust Wizard

Sides of Trust

If you have appropriate permissions in both domains, you can create both sides of the trust relationship.

To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.

Create the trust for the following:

- C This domain only This option creates the trust relationship in the local domain.
- Soth this domain and the specified domain

This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.

📄 Utilisateurs et ordinateurs Active 🕻 <u>Sélectionnez des utilisateurs, de</u>s ordinateurs, des comptes de service ou c Fichier Action Affichage ? Sélectionnez le type de cet objet : 🎽 📰 🔏 📋 🗙 (= des utilisateurs ou des groupes Utilisateurs et ordinateurs Active Di No À partir de cet emplacement : 🛨 🦳 Requêtes enregistrées formation3.lan 🖃 🚔 formation1.lan 🕀 🚞 Builtin Requêtes communes Computers Domain Controllers -Commence par E ForeignSecurityPrincipals + 📋 LostAndFound Description : Commence par -Managed Service Accounts + + 📔 Program Data Comptes désactivés 🗊 Rhu Mot de passe sans date d'expiration + 📋 System + Users 🛨 🧮 NTDS Quotas Sécurité de Windows X Saisie du mot de passe réseau Entrez le nom et le mot de passe d'un compte avec les autorisations pour formation3.lan. Par exemple Utilisateur, Utilisateur@microsoft.com ou Domaine\Nom d'utilisateur administrateur@formation3.lan Domaine : formation3.lan

Ouvrir le dossier

\\10.0.0.1 n'est pas accessible. Vous ne disposez peut-être pas des autorisations nécessaires pour utiliser cette ressource réseau. Contactez l'administrateur de ce serveur pour savoir si vous disposez des autorisations d'accès.

Échec de l'ouverture de session : l'ordinateur sur lequel vous êtes connecté est protégé par un pare-feu d'authentification. Le compte spécifié n'est pas autorisé à s'authentifier sur l'ordinateur.



X

ropriétés de	: DCFORM1							?
Général Géré par	Système d'exp	bloitation Sécuri	Membr ité	e de 🏼 Appel e	Délégati entrant	on E Éditeu	implacem ur d'attribu	ent Its
Noms de grou	upes ou d'utilisate	urs:						
Administ Administ Cout le r Cout le r Co	rateur (formation3 nonde urs authentifiés du domaine (FORI de certificats (FO	VAdministrate MATION1VA RMATION1V	eur) .dmins du .Éditeurs d	domaine; de certific) cats)			•
					Ajou	ter	Supprin	her
Autorisations	pour Administrate	ur				Autoriser	Refu	ser
Contrôle to	tal							-
Lire						\checkmark		
Écrire								
Créer tous	les objets enfants							
Supprimer	tous les objets enl	fants						
Autorisatio	n d´authentifier					V		-
E orituro un	lidán unra la nom	d'hôto DNE -						

TP : création d'une relation d'approbation

Ouvrir la console DNS.

Autoriser sur toutes les zones le transfert de zones.

Sur le DC1 (domaine 1), ajouter les zones DNS du DC2 (domaine 2).

Ouvrir la console « Domaines et Approbation Active Directory ».

Créer une relation d'approbation bidirectionnelle.

Activer l'authentification sélective.

_msdcs.orga2.lan Properties		? ×	New Zone Wizard
General Start of A	uthority (SOA)	Name Servers	Zone Type The DNS server supports various types of zones and storage.
A zone transfer sends a copy of Allow zone transfers: To any server Only to servers listed on t Only to the following serv IP Address	the zone to the serve the Name Servers ta rers	b	 Select the type of zone you want to create: Primary zone Creates a copy of a zone that can be updated directly on this server. Secondary zone Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance. Stub zone Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone. Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
New Zone Wizard Zone Name What is the name of the new zone?	New Zone Wizard Zone Name What is the na	New Zo Ma ame of the new zone?	one Wizard Ister DNS Servers The secondary zone is copied from one or more DNS servers.
The zone name specifies the portion o authoritative. It might be your organiz or a portion of the domain name (for a not the name of the DNS server.	The zone nam authoritative, or a portion ol not the name	e specifies the portion It might be your orga the domain name (fo of the DNS server.	Specify the DNS servers from which you want to copy the zone. Ser contacted in the order shown. Master Servers:
Zone name: msreportexch.local	Zone name: msdcs.msre	portexch.local	IP Address Server FQDN Validated <click add="" address="" an="" dns="" here="" ip="" name="" or="" to=""> Ig2,168,0.163 DCSRD1 OK</click>

Les services Active Directory

Services d'un contrôleur de domaine :

- Netlogon (Isass.exe) : client d'authentification
- Active Directory Services / NTDS (Isass.exe) : service d'authentification. Existe sous forme d'un service depuis Windows 2008.
- Kerberos Key Distribution Center : service de distribution de clés Kerberos (délivre les TGTs, tickets de service)
- Service de réplication de fichiers (NTFRS) ou service DFSR : en charge de la réplication du dossier SYSVOL.
- Service DNS : héberge la zone DNS qui dispose des entrées permettant aux clients de localiser les contrôleurs de domaine.
- Client DHCP : ce service permet au contrôleur de domaine d'enregistrer dynamiquement les entrées DNS du fichier netlogon.dns.

Propriétés de Services de domaine Active Directory (Ordinateur lo				
Général Connexion Récupération Dépendances				
Nom du service : NTDS				
Nom complet : Services de domaine Active Directory				
Description : Service de contrôleur de domaine des services de domaine Active Directory. Si ce service est arrêté,				
Chemin d'accès des fichiers exécutables : C:\Windows\System32\Isass.exe				
Type de démarrage : Automatique				
Obtenir de l'aide pour configurer les options de démarrage des services.				
État du service : Démarré				
Démarrer A <u>r</u> rêter Suspendre Regrendre				
Vous pouvez spécifier les paramètres qui s'appliquent au démarrage du				

Le répertoire SYSVOL

Contient les scripts et les fichiers des stratégies de groupe (GPO). L'emplacement de SYSVOL se définit au DCPROMO (modification avec NTDSUTIL).

Réplique sur tous les contrôleurs de domaine.

En mode natif 2003 et antérieur : utilisation du moteur NTFRS

En mode natif 2008 et ultérieur : utilisation du moteur DFSR

(recommandée, procédure de migration en 3 étapes).

Le partage NETLOGON correspond au répertoire

c:\windows\sysvol\sysvol\nom_domaine\scripts.

Le partage SYSVOL correspond au répertoire c:\windows\sysvol\sysvol.



📙 Policies	
~~~	
C:\windows\SYSVOL\sysvol\orga2.la	n\Policies
Organize 👻 Include in library 👻 Share with 💌	New folder
Name ^	Date modified
6AC1786C-016F-11D2-945F-00C04fB984F9}	30/03/2010 19:40
{31B2F340-016D-11D2-945F-00C04FB984F9}	30/03/2010 19:40



## Le répertoire NTDS

Contient l'annuaire (fichier NTDS.DIT)

**Pour sauvegarder l'annuaire, il faut obligatoirement une sauvegarde de l'Etat du système.** Une sauvegarde du lecteur C n'est pas suffisante.

Les modifications sont effectuées dans les logs puis inscrits ensuite dans le fichier NTDS.DIT.

Le fichier .chk permet de connaître le log en cours.

Les fichiers .jrs sont des fichiers de logs utilisaient en cas de saturation de l'espace disque.

Le fichier temp.edb est une base de données temporaire utilisée pour certaines opérations.

Pour réparer la base de données Active Directory, il faut utiliser l'utilitaire ESEUTIL (défragmentation....). Windows effectue tous les soirs une défragmentation en ligne de l'annuaire. Cette dernière ne permet cependant pas de récupérer de l'espace disque. Il faut une défragmentation hors ligne.

C:\windows	
File Edit View Tools H	Help
Organize 🔻 🛛 Include in libr	ary 🔻 Share
Name *	Size
🔊 edb.chk	8 KB
🙀 edb.log	10 240 KB
🐴 edb00007.log	10 240 KB
🏹 edb00008.log	10 240 KB
🏹 edb00009.log	10 240 KB
🛕 edbres00001.jrs	10 240 KB
🛕 edbres00002.jrs	10 240 KB
🛕 ntds.dit	45 072 KB
🗛 temp.edb	2 064 KB

## TP SYSVOL & NTDS 1/2

Prérequis : Un domaine avec deux contrôleurs de domaine.

Sur le premier contrôleur de domaine, créer un fichier test.txt (contenu test1) dans c:\windows\sysvol\sysvol\nom_domaine. Attendre environ 5 minutes.

Valider que ce dernier est apparu dans le même répertoire sur le second contrôleur de domaine.

Sur les deux contrôleurs de domaine, éditer le même fichier, le modifier (mettre une valeur différente) et l'enregistrer au même moment. Que se passe t'il ?

Arrêter le service « *DFS Replication* » sur le second contrôleur de domaine. Créer un nouveau fichier sur le premier contrôleur de domaine. Que se passe t'il ?

## TP SYSVOL & NTDS 2/2

#### Taper les commandes suivantes :

Ntdsutil Activate Instance NTDS Files Info Compact to c:\Windows\NTDS\temp Remplacer le fichier NTDS.DIT.



```
ntdsutil: activate Intance ntds
Error parsing Input - Invalid Syntax.
ntdsutil: activate Intance NTDS
Error parsing Input - Invalid Syntax.
ntdsutil: Activate Instance NTDS
Active instance set to "NTDS".
ntdsutil: fils
Error parsing Input - Invalid Syntax.
ntdsutil: Activate Instance NTDS
Active instance set to "NTDS".
ntdsutil: files
file maintenance: info
Drive Information:
        C:\ NTFS (Fixed Drive ) free(31.3 Gb) total(39.8 Gb)
DS Path Information:
        Database : C:\Windows\NTDS\ntds.dit - 44.1 Mb
Backup dir : C:\Windows\NTDS
Morking dir : C:\Windows\NTDS
Log dir : C:\Windows\NTDS
```

It is recommended that you immediately perform a full backup of this database. If you restore a backup made before the defragmentation, the database will be rolled back to the state it was in at the time of that backup.

Compaction is successful. You need to: copy "c:\Windows\NTDS\temp\ntds.dit" "C:\Windows\NTDS\ntds.dit" and delete the old log files: del C:\Windows\NTDS*.log

file maintenance: _

# 3. Les comptes utilisateurs

### Présentation compte utilisateur 1/3

Les comptes utilisateurs sont identifiés par le SID / GUID et non par le login. Il est donc possible de changer le login / renommer un compte utilisateur. Il existe deux types de login (un pour nom NETBIOS et un pour nom DNS).

Toujours cocher la case « *Le mot de passe n'expire jamais pour un compte de service* » ou utiliser la nouvelle fonctionnalité de « *Compte de services gérés* ».

ropriétés de : guillaume.mathieu	? ×	Propriétés de : guillaume.mathieu
Membre de Réplication de mot de passe Environnement Sessions Profil des services Bureau à distance Bureau vi Général Adresse Compte Profil Télé guillaume.mathieu	Appel entrant Objet Sécurité Contrôle à distance tuel personnel COM+ Éditeur d'attributs phones Organisation Certificats publiés	Membre de       Réplication de mot de passe       Appel entrant       Objet       Sécuri         Environnement       Sessions       Contrôle à distance         Profil des services Bureau à distance       Bureau virtuel personnel       COM+       Éditeur d'attrib         Général       Adresse       Compte       Profil       Téléphones       Organisation       Certificats pub         Nom d'ouverture de session de l'utilisateur :       gmathieu       @proservia.fr       Image: Compte       Image: Compte       Image: Compte       Image: Compte       Compte
Prénom : Guillaume Nom : Mathieu	Initiales :	Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :         MSREPORTFORM\         guillaume.mathieu         Horaires d'accès         Se connecter à
Description : Consultant Pôle Archite Bureau : 172 Bureaux de la colli	ecture & Intégration	Options de compte :
Numéro de téléphone :     01.41.31.69.00       Adresse de messagerie :     msreport@free.fr       Page Web :     http://msreport.free.fr	Autre Autre	✓ Le mot de passe n'expire jamais         ✓ Enregistrer le mot de passe en utilisant un chiffrement réversible         ✓ Date d'expiration du compte         ✓ Jamais         ✓ Fin de :       jeudi         8       juillet       2010

### Présentation compte utilisateur 2/3

Pour le chemin des profils itinérants, il est possible d'utiliser la variable %username% et faire une sélection multiple.

Indiquer juste le nom du script de login. Ce dernier doit se trouve dans c:\windows\sysvol\sysvol\nom_domaine_dns\scripts

Depuis Windows Server 2008, il est possible de protéger les comptes utilisateurs contre une suppression accidentelle. Cela positionne des permissions « Refusé » pour l'opération de suppression au niveau de l'onglet « Sécurité » du compte utilisateur (il faut être en mode d'affichage « Fonctionnalités avancées ».

Avec les RODC, il est possible de dire si le mot de passe peut être mis en cache (en mémoire) ou non.

P	ropriétés de : guillaume.mat	hieu		? ×	Propriétés de : qui	illaume.mathieu
	Membre de Réplication d	le mot de passe 🃋 App	el entrant 📔 Objet	Sécurité	i roprietes de riga	
	Environnement	Sessions	Contrôle à	a distance	Environnei	ment
	Profil des services Bureau à dist	ance Bureau virtuel per	sonnel COM+	Éditeur d'attributs	Profil des services	Bureau à distance
	deneral   Adlesse   Comple	Trelephones		ceruncaus publies	Général Adres	se   Compte   F
	Profil utilisateur	1			Membre de	Réplication de mo
	Chemin du profil :	 				
	Script d'ouverture de session :				Membre de :	
	Dossier de base				Nom	Dossier S
	<ul> <li>Chemin d'accès local :</li> </ul>	[			Administrateurs	formation
		ъ.			Utilisateurs	formation1
		a. [			Utilisateurs du c	Jomaine formation"

Environnen	nent	1	Se	ssions
Profil des services	Bureau à dis	tance	Bure	eau virl
Général Adress	e Compti	e   Pr	ofil	Téléj
Membre de	Membre de Réplication de mot de passe			
Membro do :				
Nom	Dos	sier Se	rvices	de don
Nom Administrateurs	Dos	sier Se ation1(	rvices ).lan/B	de don uiltin
Nom Administrateurs Utilisateurs	Dos form form	sier Se ation1( ation1(	rvices ).lan/B ).lan/B	de don uiltin uiltin

P	Propriétés de : guillaume.mathieu				? >
	Membre de Réplication de m	ot de passe 🎽	Appel entra	nt Ob	jet Sécurité
	Environnement	Sessions	1	Contrôl	e à distance
	Général Adresse Compte	Profil   Télép	hones   Org	anisation	Certificats publiés
	Profil des services Bureau à distance	Bureau virtu	el personnel	COM+	Éditeur d'attributs
	Vous pouvez attribuer dans les serv ordinateur virtuel spécifique à un uti virtuel personnel. Vous devez utiliser l'outil G Bureau à distance sour les Bureau à distance pour me disposition des utilisateurs.	ices de domaine lisateur qui l'utilis estionnaire de c erveur du service ettre des bureaux	Active Direc era en tant qu onnexions au Broker pour virtuels perso	tory un ue bureau x services les connexi innels à la	ons
	Attribuer un bureau virtuel perso	innel à cet utilisa	teur		
	Entrez le nom de domaine comple	et de l'ordinateur	à attribuer à c	et utilisateu	и.
	Le nom de l'ordinateur vir correspondre au nom de	tuel dans l'outil ( domaine comple	iestionnaire H t de l'ordinate	lyper-V doit ur.	
	Nom de l'ordinateur :		[	Parcouri	·

prices ac i gai	laume.mati	nieu				
Environner	nent	9	essions	: 1		Con
Profil des services	Bureau à dist	ance   Bi	ureau vi	rtuel perso	nnel	СОМ
iénéral 📔 Adress	e Compte	Profil	Télé	éphones	Orga	anisatio
Membre de	Réplication d	e mot de p	asse	Appel	entrani	t
Nom canonique d	e l'objet :					
formation10.lan/4	Administration	des ventes	s/Utilisal	eurs/guilla	ume.n	nathieu
Classe d'objets :	Utilisateur					
Créé le :	07/06/2010	) 23:04:43				
Modifié le :	08/06/2010	) 14:48:49				
Nombres de séqu	ences de mise	e à jour (US	5N):			
Actuel :	14423					

Protéger l'objet des suppressions accidentelles

## Présentation compte utilisateur 3/3

La console Utilisateurs et Ordinateurs Active Directory intègre maintenant une éditeur ADSIEDIT (onglet « *Editeur d'attributs* »).

Les deux captures de droite montrent les permissions positionnées par la case « *Protéger contre la suppression accidentelle* ».

L'onglet « *Bureau Virtuel* » est lié à la solution Microsoft Virtual Desktop Infrastructure (VDI).

http://www.laboratoire-microsoft.org/articles/Microsoft-VDI/4/

Il est possible de visualiser les certificats associés aux comptes utilisateurs comme pour EFS (clé publique uniquement)

Propriétés de : g	uillaume.mat	hieu						?
Environr	nement	) s	essions		1	Contr	ôle à dis	stance
Membre de	Membre de 📔 Réplication de mot de pa			Appel	entrant	j c	Ibjet	Sécurité
Profil des service	es Bureau à dist	ance   Bu	ireau vii	tuel perso	onnel 🗍	COM+	🗍 Édit	teur d'attributs
Général Adre	esse 📔 Compte	Profil	∫ Télé	phones	0rga	nisation	Cert	tificats publiés

Liste des certificats X509 publiés pour le compte d'utilisateur

ropriétés de : guillaume.mathieu	? ×
Environnement Sessions Profil des services Bureau à distance Bureau virtuel personr Général Adresse Compte Profil Téléphones Membre de Réplication de mot de passe Appel er	Contrôle à distance nel COM+ Éditeur d'attributs Organisation Certificats publiés htrant Objet Sécurité
Noms de groupes ou d'utilisateurs : Tout le monde SELF SUtilisateurs authentifiés Système Admins du domaine (MSREPORTFORM\Admins du domai Éditeurs de certificats (MSREPORTFORM\Éditeurs de cert Administrateurs de l'entreprise (MSREPORTFORM\Admini	ine) ttřícats) strateurs de l'entreprise)
Autorisations pour Tout le monde	Autoriser Refuser
Écrire Options de messagerie et de téléphone Lire Restrictions de compte Écrire Restrictions de compte Lire Serveur de licences Terminal Server Écrire Serveur de licences Terminal Server	
Autorisations speciales	
Autorisations speciales Pour les autorisations spéciales et les paramètres avancés, cliqu Avancé. Informations sur le contrôle d'accès et les autorisations	uez sur <u>Avancé</u>

ntrées d'a Type	r ou modimer les details o une au utorisations :	Nom : Tout le monde Appliquer à : Cet objet uniquement		Modifier
Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser Autoriser	Tout le monde     S       Utilisateurs authentifiés     S       Administrateurs (MSREP     S       Administrateurs de l'entre     S       Administrateurs de l'entre     S       Administrateurs de l'entre     S       Administrateurs de l'entre     S       Accès compatible pré-Wi     S       Groupe d'accès d'autori     Serveurs de licences de       Serveurs de licences de     L       SELF     S       r     Modifier	Autorisations : Contrôle total Lister le contenu Lire toutes les propriétés Écrire toutes les propriétés Supprimer Supprimer la sous-arborescence Autorisations de lecture Modifier les autorisations Modifier le propriétaire Toutes les écritures validées Tous les droits étendus	Autoriser	Refuser
Ajoute Inclure I estion des	r Modifier	Tous les droits étendus           Appliquer ces autorisations unique           aux objets et/ou aux conteneurs frapartie de ce conteneur           Gestion des autorisations	nent aisant .	Efface

### **Modifications multiples**

Il est possible d'effectuer des modifications sur plusieurs comptes en même temps en appuyant sur la touche contrôle et en sélectionnant les comptes utilisateurs. On peut aussi utiliser un outil comme *ADMODIFY*.


#### Les modèles de comptes utilisateurs

Modèle de compte : on passe par la fonction Copier. L'assistant classique se lance ensuite et demande de saisir les informations spécifiques au compte utilisateur. On peut modifier dans la console « Schéma », les valeurs des attributs qui sont conservés lors d'un copie.

Intérêt : permet de conserver la valeur de certains attributs (appartenances aux groupes, certains champs de l'adresses...). D'où un gain de temps.

Best Practice : les modèles de comptes utilisateurs doivent être des comptes désactivés

📴 Utilisateurs et ordinateurs Active Directory		Copier l'objet - Utilisateur 🛛 🗙
Fichier Action Affichage ?		
🗢 🔿 🙍 📊 🠇 📋 💥 🖬 🧟 📄	🛿 🖬 🗏 📚 🛅 🍸 🗾 📚	Créer dans : formation10.lan/Administration des ventes/Utilisateurs
📔 Utilisateurs et ordinateurs Active Directory [SFR	Nom Type Description	
🕀 🚞 Requêtes enregistrées	👗 guillaume.m <del>a – Utilicatour – Concultant</del> Pôle Archity	ect
🖃 🚔 formation10.lan	Copier	Prénom : Initiales :
🕀 🧰 Builtin	Ajobilizer à un groupe	
🕀 🚞 Computers	Désactiver le compte	Nom :
🕀 🧾 Domain Controllers	Réinitialiser le mot de passe	
ForeignSecurityPrincipals	Déplacer	Nom complet :
Formation	Ouvrir la page de démarrage	
🗄 🔜 Managed Service Accounts	Envoyer un message	Nom d'ouverture de session de l'utilisateur :
🗄 🔜 Users	Toutes les tâches	Qproservia fr
Comptabilité		
	Couper	Nom d'ouverture de session de l'utilisatel Nantérieur à Windows 2000) :
	Supprimer	
Ressources humaines	Renommer	
	Propriétés	
📑 Seven		· ·
💼 Groupes	Aide	
💼 Utilisateurs		< Precedent Survant > Annuler

#### Best Practice compte utilisateur :

Valider avec la direction la convention de nommage et la stratégie de mots de passe.

Intégrer si possible une chaîne de caractère aléatoire dans le login pour éviter les attaques par verrouillage (en déterminant le login d'un utilisateur). Créer des modèles de comptes utilisateurs.

**Désactiver les comptes au lieu de les supprimer.** En effet en cas de suppression, il ne sera pas possible de récupérer le SID sauf si l'on effectue une restauration autoritaire (avec NTDSUTIL).

Ne pas activer le verrouillage de comptes avec une seuil trop faible (mettre environ 50 échecs avant le verrouillage).

Pour les comptes de services, cocher la case « *Le mot de passe n'expire jamais* » afin d'éviter que le mot de passe des comptes de services n'expire. Cela bloquera en effet le démarrage du service. Il est aussi possible d'utiliser les nouveaux comptes de services gérés.

Il existe des outils comme *Active Roles* qui permettent de forcer la saisie de certains champs lors de la création des comptes utilisateurs ou qui permettent d'imposer un certain formalisme lors de la saisie des champs.

## TP : création compte utilisateur

Créer un compte utilisateur sans mot de passe. On obtient le message d'erreur cidessous. Réessayer en utilisant le mot de passe « *P@ssword* ».

Ouvrir une session avec ce compte sur une machine membre du domaine. Un nouveau profil est généré.

Lancer l'éditeur de base de registre (REGEDT32). Faire une recherche sur la valeur « *profileimagepath* ». Cette clé permet de mapper le SID du compte au profil utilisateur. Personnaliser le profil (fond d'écran, création de fichiers sur le bureau...). Fermer la session.

Renommer le compte utilisateur (champ prénom, nom, description, **login).** Ouvrir la session. Vous devez récupérer votre profile. Pourquoi ?

http://msreport.free.fr/?p=86



#### La gestion des mots de passe 1/2

#### Les paramètres de stratégies de mots de passe :

- Historique des mots de passe / durée de vie minimale du mot de passe : permet d'empêcher les utilisateurs de réutiliser le même mot de passe. Le paramètre durée de vie minimale du mot de passe empêche l'utilisateur de changer X fois son mot de passe jusqu'a pouvoir ressaisir son ancien mot de passe.
- Durée de vie maximale du mot de passe : le mot de passe devra être changer tous les X jours.
- Longueur minimum du mot de passe : le mot de passe doit faire au minimum X caractères.
- Les mots de passe doivent respecter les exigences de complexité : permet d'obliger les utilisateurs à saisir un mot de passe avec un caractère spécial ou une majuscule ou un chiffre. Les paramètres de complexité ne sont pas configurables. La complexité des mots de passe est géré via le fichier passfit.dll.

Des outils tiers comme *One Identity Password Manager* permettent de disposer d'une Passfit.dll personnalisée (dictionnaire de mots de passe interdit, charactères interdits...). Il existe aussi une solution gratuite alternative :

https://blog.scrt.ch/2017/08/23/passfilt-dll-complexifier-sa-politique-de-mot-de-passewindows/

#### Quelle stratégie de mots de passe adoptée ?

Depuis Windows Server 2008, les « *Fine Grained Password Policy* » permettent de définir des stratégies de mots de passe spécifique pour un utilisateur ou un groupe. <u>http://technet.microsoft.com/en-us/library/cc770842(WS.10).aspx</u>

#### La gestion des mots de passe 2/2

#### Les risques :

Une politique de mots de passe trop faible risque de compromettre le niveau de sécurité de la société tout comme une politique de mots de passe trop complexe (les utilisateurs écrivent sur papier leur mot de passe).

#### Réinitialisation de mots de passe ≠ Changement de mot de passe :

Attention la réinitialisation de mot de passe fait perdre l'accès aux données chiffrées avec EFS dans certains cas (si compte de la base SAM local par exemple).

#### Self Service Password Reset :

De nombreux outils comme *One Identity Password Manager ou* Microsoft Azure AD Premium (SSPR) permettent aux utilisateurs de réinitialiser eux même leur mot de passe via des questions réponses, l'envoie de Passcode par SMS ou messagerie personnelle. L'utilisation de questions / réponses peut abaisser fortement le niveau de sécurité ou générer des problèmes de conformité avec le RGPD. L'envoie de Passcode sur téléphone portable Pro est donc à privilégier.

#### Quel politique adoptée ?

Toujours faire valider la stratégie de mots de passe par la direction. Il faut trouver un juste milieu (complexité activé, historique : 5 mots de passe, durée de vie minimale du mot de passe : 1 journée, durée de vie maximale du mot de passe : 42 jours).

#### L'option « Le mot de passe n'expire jamais » :

A définir <u>uniquement</u> pour les comptes de services (pas pour les autres comptes)

## MSA et gMSA

#### MSA:

- Prise en charge avec machine Windows Server 2008 R2 / Windows Seven.
- Un Managed Service Account par machine (pas de partage d'un même « Managed Service Account » entre machines).
- Pas de pris en charge des cluster (services mis en haute disponibilité).
- msDS-ManagedServiceAccount : nouvelle classe pour gérer les Managed Service Accounts.
- Managed Service Account : c'est une sorte d'intermédiaire entre un compte utilisateur et un compte ordinateur.
- Changement du mot de passe : même fonctionnement qu'un compte ordinateur (changement tous les 30 jours). Nécessite mode 2008 R2 pour changement automatique du mot de passe.
- Pas de login interactif ou de verrouillage de compte.
- Possibilité d'ajouter un Managed Service Account à un groupe (pour le contrôle des accès). <u>http://blogs.technet.com/b/askds/archive/2009/09/10/managed-service-accounts-understanding-implementing-best-practices-and-troubleshooting.aspx</u>

#### gMSA :

Disponible depuis Windows Server 2012.

https://blogs.technet.microsoft.com/askpfeplat/2012/12/16/windows-server-2012-groupmanaged-service-accounts/

#### Toujours vérifier que l'application supporte l'usage des MSA ou gMSA !

## 4. Les comptes ordinateurs

#### Les comptes ordinateurs 1/2

Les comptes ordinateurs disposent d'un mot de passe.

Permet d'authentifier la machine dans le domaine. La machine envoie le mot de passe du compte ordinateur (qui est mis en cache) au contrôleur de domaine. Ce dernier le compare au mot de passe contenu dans l'annuaire. Permet d'attribuer des GPO de type « *Configuration Ordinateur* ». Le mot de passe du compte ordinateur change par défaut tous les 30 jours (configurable via registre / GPO).

Lorsque l'on joint une machine au domaine, par défaut le compte ordinateur est ajouté dans le conteneur « Computer » à la racine du domaine.

En cas de problème avec le compte ordinateur, une erreur NETLOGON apparaît sur la station de travail et le contrôleur de domaine.

Il est possible de pré-créer le compte ordinateur dans une OU spécifique. Quand la machine joint le domaine, elle complète les informations (version de l'OS...).

Propriétés de : SFR	3 ? ×
Emplacement Général S	Géré par Objet Sécurité Appel entrant Éditeur d'attributs système d'exploitation Membre de Réplication de mot de passe
SFR3	
Windows 2000) :	SFR3
Nom DNS :	SFR3.formation10.lan
Type de contrôleu de domaine :	Ir Station de travail ou serveur

Pr	opriétés de :	SFR3		
ĺ	Emplacement	Géré par Objet	Sécurité	Appel entra
	Général	Système d'exploitation	Membre o	de Ì Rép
	Nom :	Windows Server 2008	R2 Entreprise	
	Version :	6.1 (7600)		

## Les comptes ordinateurs 2/2

Propriétés de : SFR3 ? 🗙	Propriétés de : Membre de domaine : désactive les modifications <mark>?</mark> 🗙
Propriétés de : SFR3       ? ×         Emplacement       Géré par       Objet       Sécurité       Appel entrant       Éditeur d'attributs         Général       Système d'exploitation       Membre de       Réplication de mot de passe         Les mots de passe des utilisateurs et des ordinateurs sont stockés de manière permanente sur tous les contrôleurs de domaine en lecture seule (RODC). Le mot de passe de ce compte est mis en cache sur les contrôleurs de domaine en lecture seule suivants.       Contrôleurs de domaine en lecture seule :         Nom       Site         Propriétés de : SFR3       Emplacement       Géré par       Dbjet       Sécurité       Appel         Emplacement       Géré par       Dbjet       Sécurité       Appel       Géréral       Système d'exploitation         Membre de :       Nom       Dossier Services de domaine Activ       Implacement       Géré par       Objet         Nom       Dossier Services de domaine Activ       Membre de       Nom :       Modifier         Utilisateurs et ordnateurs Active Directory       Mappages des noms       Désactiver le compte       Réinitialiser le compte         Explaces enregistrées       Formation10.lan       Mappages des noms       Désactiver le compte       Déplacer         Béritaliser le compte       Réinitialiser le compte       Mappages des noms       Dépl	Propriétés de : Membre de domaine : désactive les modifications ?         Paramètre de stratégie de sécurité Expliquer         Membre de domaine : désactiver les modifications de mot de passe du compte ordinateur         Détermine si un membre de domaine doit périodiquement modifier son mot de passe de compte d'ordinateur. Si ce paramètre est désactivé, le membre de domaine e tente pas de modifier son mot de passe de compte d'ordinateur. Si ce paramètre est désactivé, le membre de domaine essaie de modifier son mot de passe de compte d'ordinateur. Si ce paramètre est désactivé, le membre de domaine essaie de modifier son mot de passe de compte d'ordinateur le qu'il est spécifié par le paramètre Membre de domaine : antériorité maximale du mot de passe du compte ordinateur, qui est fixé par défaut à 30 jours.         Valeur par défaut : Désactivé.         Remarques         Il est recommandé de ne pas activer ce paramètre de sécurité. Les mots de passe de compte d'ordinateur sont utilisés pour établir des communications via le canal sécurisé entre des membres et des contrôleurs de domaine et, au sein du domaine, entre les contrôleurs de domaine eux-mêmes. Une fois qu'il est établi, le canal sécurisé est utilisé pour transmettre des informations sensibles qui rendent nécessaires le processus d'authentification et la vérification des autorisations.         Pour obtenir plus d'informations sur la stratégie de sécurité et les fonctionnalités de Windows, wisitez le site Web de Microsoft         DK       Annuler       Appliquer
Réinitialiser le compte   Seven   Utilisateurs   Utilisateurs   Seven   Utilisateurs   Seven   Utilisateurs   Seven   Utilisateurs   Seven   Supprimer   Computers   Computers   Couper   Supprimer   Supprimer   ForeignSecurityPrincipals   Formation   Propriétés   Aide	OK Annuler Appliquer

## TP : Les comptes ordinateurs

Installer Windows 10 Pro ou Enterprise. Ne pas mettre de serveur DNS. Joindre la machine avec le nom DNS de domaine. Cela échoue. Pourquoi ?

Mettre vos contrôleurs de domaine comme serveur DNS sur la machine Windows 10. Pourquoi faut il définir plusieurs serveurs DNS ?

- Sortir la machine du domaine. Redémarrer la machine.
- Créer un compte utilisateur standard.

Joindre la machine au domaine en utilisant le nom de DNS de domaine. Utiliser le compte standard pour vous authentifier. Redémarrer la machine.

Ouvrir la console « *Utilisateurs et Ordinateurs Active Directory* ». Aller dans le conteneur « *Computers* ».

Aller dans les propriétés du compte ordinateur et parcourir les différents onglets. A quoi sert le groupe « *Ordinateurs du domaine* ».

Supprimer le compte ordinateur. Redémarrer la station de travail . Essayer d'ouvrir une session avec le compte utilisateur. Cela échoue. Pourquoi ? Ouvrir les observateurs d'événements et chercher une erreur Netlogon.

Joindre de nouveau la machine dans le domaine (la repasser en workgroup au préalable).

Réinitialiser le mot de passe du compte ordinateur. Redémarrer la station de travail. Ouvrir les observateurs d'événements. Une erreur NETLOGON apparaît de nouveau. Pourquoi ?

# 5. Les groupes

#### Présentation générale des groupes

#### Qu'est ce qu'un groupe ?

Un groupe est un ensemble de ressources.

Un groupe n'est pas un conteneur (ne pas confondre avec les OU).

On ne peut pas affecter de GPO à un groupe. On peut cependant filtrer l'application des GPO à des groupes en définissant les droits « *Lire* » et « *Appliquer les stratégies de groupes* » à un groupe (dans l'onglet Sécurité).

#### 2 types de groupes :

Les groupes de sécurité : utilisés pour la messagerie et gérer les droits. Les groupes de distribution : utilisés pour la messagerie (liste de diffusion)

#### 3 étendues différentes :

Les groupes globaux de domaine Les groupes locaux de domaine Les groupes universels

#### Fonctionnement selon le niveau fonctionnel de domaine / forêt :

Pour créer des groupes universelles : mode natif 2000 obligatoire.

Pour encapsuler des groupes globaux (groupes globaux membres d'autres groupes globaux) : mode natif 2000 obligatoire.

A partir du mode natif 2003, si l'on ajoute un objet comme membre d'un groupe, seul l'ajout du membre réplique. Auparavant l'objet groupe répliquait complètement.

On va pouvoir changer l'étendue d'un groupe à partir du mode natif 2000.

## Les étendues de groupes

Etendue	Membres	Visibilité	Intérêt
Globale	Objet du même domaine Ne peut pas contenir de groupe universel.	Visible sur le domaine locale et tous les domaines approuvées.	Groupe d'utilisateurs
Locale	Objet du domaine locale et de tous les domaines approuvées.	Visible sur le domaine locale uniquement.	Pour définir des permissions.
Universelle	Objet de tous les domaines de la forêt (pas sur les domaines approuvées hors de la forêt)	Visible sur le domaine locale et tous les domaines approuvées	Liste des distributions pour Exchange.

## Notions avancées sur les groupes

Les propriétaires d'un groupe : peut gérer les appartenances aux groupes. L'imbrication des groupes : un groupe peut avoir comme membre d'autres groupes selon le niveau fonctionnel du domaine.

Pour modifier l'étendue d'un groupe : convertir un groupe globale en groupe universel puis le repasser en groupe local. **Attention aux permissions définis sur les serveurs à l'aide des groupes !** Un groupe globale est visible depuis le domaine locale et tous les domaines approuvées. Un groupe locale n'est visible que depuis son domaine ! Attention aux incohérences.

On peut aussi changer le type d'un groupe. Attention si l'on passe un groupe de sécurité en groupe de distribution, toutes les permissions définies ne fonctionneront plus mais elles continueront de s'afficher dans l'onglet « *Sécurité* ».

Pas de synchronisation entre le système de fichiers et l'annuaire.

Permission accès partage = cumul le plus restrictif permissions Partages / NTFS.



#### Les Best Practice

Eviter de convertir les groupes de sécurités en groupe de distribution.

Eviter d'utiliser les groupes universels. Les groupes universels augmentent la taille du « *Catalogue globale* ».

Utiliser les groupes locaux de domaine pour définir des permissions sur les serveurs de fichiers et au niveau de l'annuaire.

Utiliser les groupes globaux comme des groupes d'utilisateurs.

Définir une topologie de groupe globaux sur papier. Elle doit correspondre à la structure administrative de l'entreprise. Un groupe par sous-services par exemple...

Pas plus de 5 niveaux d'encapsulation (pour des raisons de performance).

Convenir avec la direction d'une convention de nommage.

#### Pour gérer les accès à une ressource :

L'administration des accès doit se faire depuis la console *Utilisateurs et Ordinateurs du domaine* ou *Centre d'administration Active Directory*.

Créer 3 groupes locaux de domaine, un pour l'accès en lecture, un pour l'accès en lecture et écriture (Modifier), un pour l'accès en Contrôle Totale.

Définir les permissions à ces 3 groupes au niveau de la ressource (onglet Sécurité).

Ajouter « Contrôle Total » aux groupes SYSTEM et au groupe Administrateurs.

Créer vos groupes d'utilisateurs (groupes globaux).

Pour définir des accès à la ressource, ajouter des groupes globaux ou des comptes utilisateur / ordinateur en tant que membres des groupes locaux de domaine.

## TP : Gestion accès avec les groupes 1/2

Créer 3 dossiers imbriqués les uns dans les autres (Niveau1, Niveau 2 et Niveau 3).

Désactiver l'héritage au niveau du dossier Niveau 1.

Partager Niveau 1 (contrôle Total pour tout le monde).

Sécuriser le répertoire Niveau 1 selon les Best Practice (utiliser les groupes locaux de domaine pour définir des permissions). Création groupes

GDL_Niveau1_L, GDL_Niveau1_M et GDL_Niveau1_CT.

Créer des comptes utilisateurs compta1 et compta2 et le groupe globale (GG_Comptaibilité). Ajouté les utilisateurs compta1 et compta2 dans ce groupe globale.

Définir des permissions « Modifier » sur le répertoire Niveau1 à l'utilisateur « *Compta1* ».

Supprimer le compte Compta1. Observer ce qui se passe au niveau des groupes et des permissions de la ressource Niveau1, Niveau 2 et Niveau 3.

Ajouter le groupe GG_Compatibilité en tant que membre du groupe « *GDL_Niveau1_M* ».

Se loguer avec le compte Compta2 sur une machine membre du domaine et accéder au partage Niveau1.

## TP : Gestion accès avec les groupes 2/2

Peut on sauvegarder un répertoire sur lequel on a pas d'accès. La réponse est oui si on est opérateur de sauvegarde, Opérateur de Server et administrateurs. Voir la capture de droite. Expliquer ?

Partage avancé	×
✓ Partager ce dossier	
Paramètres	1
Nom du partage :	
dossiers	
Ajouter Supprimer	
Limiter le nombre d'utilisateurs simultanés à : 16777:	
Commentaires :	
Autorisations Mise en cache	
OK Annuler Appliquer	
Propriétés de : dossiers	×
Général Partage Sécurité Versions précédentes Personnaliser Partage NFS	
Nom de l'objet : C:\dossiers	
Noms de groupes ou d'utilisateurs : RECREATEUR PROPRIETAIRE Système Compte inconnu (S-1-5-21-1241569958-1998640802-1357695591-1002) Administrateurs (FORMATION3\Administrateurs)	
Pour modifier les autorisations, cliquez sur Modifier.	

Autorisations pour Administrateurs

Pour les autorisations spéciales et les paramètres avancés, cliquez sur

Informations sur le contrôle d'accès et les autorisations

Contrôle total

Modification

Lecture Écriture

Avancé.

Lecture et exécution Affichage du contenu du dossier

×
r
r
- 11

#### Propriétés de : Sauvegarder les fichiers et les r

Paramètre de stratégie de sécurité Expliquer



Modifier.

Avancé

Autoriser

Refuser

Sauvegarder les fichiers et les répertoires

Définir ces paramètres de stratégie :

Administrateurs Opérateurs de sauvegarde Opérateurs de serveur

## Les groupes BUILTIN 1/2

Ne pas déplacer.

Equivalent des groupes locaux de domaine.

Ne pas utiliser si possible car on ne peut pas les migrer avec des outils comme ADMT.

📔 Utilisateurs et ordinateurs Activ	e Director <del>y</del>	
Fichier Action Affichage ?		
🗢 🔿 🗾 🖬 🗐 💁 🧔	) 🛛 🖬 🗏 📚 🖆 🔻 🔼 🍇	
Utilisateurs et ordinateurs Active Di	Nom	Description
<ul> <li>              € Requêtes enregistrées          </li> <li>             formation3.lan         </li> <li>             Builtin             Computers             </li> <li>             Domain Controllers             </li> <li>             ForeignSecurityPrincipals             </li> <li>             formation</li></ul>	<ul> <li>Accès compatible pré-Windows 2000</li> <li>Accès DCOM service de certificats</li> <li>Administrateurs</li> <li>Duplicateurs</li> <li>Générateurs d'approbations de forêt entrante</li> <li>Groupe d'accès d'autorisation Windows</li> <li>IIS_IUSRS</li> <li>Invités</li> <li>Lecteurs des journaux d'événements</li> <li>Opérateurs d'impression</li> <li>Opérateurs de compte</li> <li>Opérateurs de compte</li> <li>Opérateurs de sauvegarde</li> <li>Opérateurs de serveur</li> </ul>	Un groupe de compatibilité descendante qui autorise un accès en lecture sur tous les utilisateurs et groupes dans le Les membres de ce groupe sont autorisés à se connecter à des autorités de certification d'entreprise. Les membres du groupe Administrateurs disposent d'un accès complet et illimité à l'ordinateur et au domaine Prend en charge la réplication des fichiers dans le domaine Les membres de ce groupe peuvent créer des approbations à sens unique entrantes vers cette forêt Les membres de ce groupe ont accès à l'attribut tokenGroupsGlobalAndUniversal sur les objets Utilisateur Groupe intégré utilisé par les services Internet (IIS). Les membres du groupe Invités disposent par défaut du même accès que les membres du groupe Utilisateurs, à l'ex Des membres de ce groupe peuvent lire les journaux des événements à partir de l'ordinateur local Les membres sont autorisés à effectuer des opérations de chiffrement. Les membres sont autorisés à effectuer des opérations de chiffrement. Les membres peuvent administrer les comptes utilisateur et groupe du domaine Les membres de ce groupe peuvent disposer de certaines autorisations d'administration pour la configuration des fo Les membres du groupe Opérateurs de sauvegarde peuvent passer outre les restrictions de sécurité uniquement da Les membres peuvent administrer les serveurs de domaine
	<ol> <li>Serveurs de licences des services Terminal Server</li> <li>Utilisateurs</li> <li>Utilisateurs de l'Analyseur de performances</li> <li>Utilisateurs du Bureau à distance</li> <li>Utilisateurs du journal de performances</li> <li>Utilisateurs du modèle COM distribué</li> </ol>	Les membres de ce groupe peuvent mettre à jour des comptes d'utilisateurs dans Active Directory avec des informa Les utilisateurs ne peuvent pas effectuer de modifications accidentelles ou intentionnelles à l'échelle du système ; pa Les membres de ce groupe peuvent accéder aux données de compteur de performance localement et à distance. Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance Les membres de ce groupe peuvent planifier la journalisation des compteurs de performance, activer les fournisseur Les membres sont autorisés à lancer, à activer et à utiliser sur cet ordinateur les objets COM distribués.

## Les groupes BUILTIN 2/2

#### Rôle de ces groupes :

Builtin\Administrateurs : administrateur local sur tous les contrôleurs de domaine. Droits presque équivalents à *Admins du domaine*. Les membres de ce groupe ne sont pas administrateur local des stations de travail membrew du domaine.

- BUILTIN\Duplicateurs
- Builtin\Opérateurs de compte : peut créer des comptes. Peut être utilisé pour faire un premier niveau
- Builtin\Opérateurs de sauvegarde : peut sauvegarder des données même si ce dernier n'a pas d'accès.

#### Propriétés de : Permettre l'ouverture d'une session locale

Pa	ramètre de stratégie de sécurité Expliquer
	Permettre l'ouverture d'une session locale
	Détermine quels utilisateurs peuvent se connecter à l'ordinateur
	Important
	La modification de ce paramètre peut affecter la compatibilité avec des clients, des services et des applications. Pour obtenir des informations de compatibilité sur ce paramètre, voir l'article sur cet aspect de compatibilité (http://go.microsoft.com/fwlink/?LinkId=24268) sur le site Web Microsoft.
	Valeur par défaut :
	<ul> <li>Sur les stations de travail et les serveurs : Administrateurs, Opérateurs de sauvegarde, Utilisateurs avec pouvoir, Utilisateur et Invité</li> </ul>
	Sur les contrôleurs de domaine : Opérateurs de compte, Administrateurs, Opérateurs de sauvegarde et Opérateurs

 Builtin\Opérateurs de Server : peut effectuer certaines actions au niveau des contrôleurs de domaine comme changer la configuration IP.

Seul les groupes BUILTIN Opérateurs de sauvegarde, Administrateurs, Opérateurs de comptes et Opérateurs d'impression peuvent ouvrir une session sur un contrôleur de domaine (configurable via GPO).

#### Les groupes dans conteneur Users :

Admins du domaine : n'a des droits que sur le domaine. Il n'a que des droits partiels sur la partition de configuration. Il est administrateurs de tous les serveurs et stations de travail du domaine.

Administrateur de l'entreprise : administrateur de tous les domaines de la forêt Administrateur du schéma : seul groupe habilité à modifier le schéma Active Directory

📔 Utilisateurs et ordinateurs Activ	e Directory	
Fichier Action Affichage ?		
🗢 🔿 🖄 🖬 🖌 🗊	) 🧟 🗟 🔻 🔝 📷 🗏 🐍 📚 🖀 🖉 🧕 🍇	
<ul> <li>Utilisateurs et ordinateurs Active Dir</li> <li>Requêtes enregistrées</li> <li>formation 10.lan</li> <li>Administration des ventes</li> <li>Builtin</li> <li>Comptabilité</li> <li>Computers</li> <li>Domain Controllers</li> <li>DSI</li> <li>ForeignSecurityPrincipals</li> <li>Formation</li> <li>LostAndFound</li> <li>Managed Service Accounts</li> <li>Production</li> <li>Program Data</li> <li>System</li> <li>Users</li> <li>Vente</li> </ul>	Nom Administrateur Administrateurs de l'entreprise Administrateurs du schéma Administrateurs du schéma Administrateurs du schéma Administrateurs du domaine Contrôleurs de domaine Contrôleurs de domaine d'entreprise en lect Contrôleurs de domaine en lecture seule DnsAdmins DnsUpdateProxy Éditeurs de certificats Groupe de réplication dont le mot de passe Groupe de réplication dont le mot de passe Invité Invité Notificateurs du domaine Krbtgt Contributeurs du domaine	Description         Compte d'utilisateur d'administration         Administrateurs désignés de l'entreprise         Administrateurs désignés du schéma         Administrateurs désignés du domaine         Tous les contrôleurs de domaine du domaine         Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans l'entreprise.         Les membres de ce groupe sont des contrôleurs de domaine en lecture seule dans le domaine         Groupe des administrateurs DNS         Les clients DNS qui sont autorisés à effectuer des mises à jour dynamiques en tant que clients différe         Les membres de ce groupe ont l'autorisation de publier des certificats dans le répertoire         Les mots de passe des membres de ce groupe peuvent être répliqués sur tous les contrôleurs de don         Les mots de passe des membres de ce groupe ne peuvent pas être répliqués sur des contrôleurs de (         Compte d'utilisateur invité         Tous les invités du domaine         Compte de service du centre de distribution de clés         Toutes les stations de travail et les serveurs joints au domaine
	<ul> <li>Propriétaires créateurs de la stratégie de gr…</li> <li>Serveurs RAS et IAS</li> <li>Utilisateurs du domaine</li> </ul>	Les membres de ce groupe peuvent modifier la stratégie de groupe pour le domaine Les serveurs de ce groupe peuvent accéder aux propriétés d'accès distant des utilisateurs Tous les utilisateurs du domaine

#### Les entités système

Tout le monde : tout le monde.

<u>Utilisateurs authentifiés :</u> tout ordinateur ou tout utilisateurs qui a ouvert une session est membre du groupe « *utilisateurs authentifiés* ». Groupe avec privilège important comme créer des dossiers / fichiers sur la partition C des serveurs.

<u>Créateur propriétaire :</u> par défaut le créateur d'un fichier et d'un dossier est le propriétaire. Il a le droit de modifier les permissions.

<u>System :</u> droit presque équivalent à administrateur local. C'est par exemple le seul à pouvoir modifier le contenu de la base SAM dans la base de registre.

💣 Éditeur du Registre				🕌 Autorisations pour SAM
Fichier Edition Affichage Favoris ?				
	Nom	Туре	Données	Sécurité
HKEY_CLASSES_ROOT	(par défaut)	REG_SZ	(valeur non	Nome de groupes ou d'utiliezteurs :
	Autorisations pour SAM		×	
	(Cérural)			Système .
HARDWARE	Securite		1	Administrateurs (XP-GMAT3\Administrateurs)
	Noms de groupes ou d'utilisateurs	:		
SECURITY	Système .			
	Administrateurs (XP-GMAT3)	Administrateurs)		
E. SYSTEM				1
				Aiouter Supprimer
		Ajouter	Supprimer	Autorisations pour Administrateurs
	Autorisations pour Système			Autoriser Refuser
	Autonationa pour ayateme	Autoriser	Refuser	
	Contrôle total			
	Lecture			
	Autorisations spéciales			Autorisations spéciales

# 6. Les unités d'organisation

## Présentation générale des OU 1/2

OU = unité d'organisation

C'est un conteneur (rien à voir avec les groupes).

On peut créer dans une OU tout type d'objet dont d'autres OU.

La topologie d'unités d'organisation doit correspondre à l'organisation administrative de l'entreprise. Elle est à faire sur papier et doit être validée par la direction.

Les OU permettent aussi de faire de la délégation d'administration et de créer des GPO.

Depuis Windows 2008, la console « *Gestion des stratégies de groupe* » est installé par défaut. On ne peut donc plus créer d'objets stratégies de groupe depuis la console « *Utilisateurs et Ordinateurs Active Directory* ».

#### Nouveauté sur les contrôleurs de domaine :

Quand on crée une nouvelle OU sur un DC 2008 / 2008, par défaut la protection renforcée contre la suppression accidentelle est activée. Cette protection met des permissions « Refusé » à Tout le monde pour la suppression d'objet.

Si on essaie de déplacer ou supprimer une OU, on a donc un message « *Accès Refusé* ».

Passer en mode d'affichage « *Fonctionnalités avancées* » pour cocher ou décocher cette case.

## Présentation générale des OU 2/2

Utilisateurs	et ordinateurs Active Direct
Fichier Action	Affichage ?
待 🔿 🖄 🚺	Ajouter/supprimer des color
Utilisateurs e E Carlos Requêtes E Formation Builtir	Grandes icônes Petites icônes GListe Détails
	Utilisateurs, contacts, grou ir Fonctionnalités avancées tion
Général Géré par C	)bjet   Sécurité   COM+   Éditeur d'attributs
Général   Géré par   C Nom canonique de l'o	Dbjet   Sécurité   COM+   Éditeur d'attributs
Général Géré par C Nom canonique de l'o formation3.1an/forma	)bjet Sécurité COM+Éditeur d'attributs objet : tion
Général Géré par C Nom canonique de l'o formation3.lan/forma Classe d'objets : U	Dbjet Sécurité COM+Éditeur d'attributs objet : tion nité d'organisation
Général Géré par C Nom canonique de l'o formation3.lan/forma Classe d'objets : U Créé le : 0	Dbjet Sécurité COM+Éditeur d'attributs objet : tion nité d'organisation 3/06/2010 10:42:28
Général Géré par C Nom canonique de l'o formation3.lan/forma Classe d'objets : U Créé le : 0 Modifié le : 0	Dbjet Sécurité COM+Éditeur d'attributs objet : tion nité d'organisation 3/06/2010 10:42:28 3/06/2010 10:43:06
Général       Géré par       C         Nom canonique de l'o       formation3.lan/forma         Classe d'objets :       U         Créé le :       0         Modifié le :       0         Nombres de séquence       0	Dbjet Sécurité COM+Éditeur d'attributs objet : tion nité d'organisation 3/06/2010 10:42:28 3/06/2010 10:43:06 es de mise à jour (USN) :

Utilisateurs et ordinateurs Active Directory Fichier Affichage Action -? П × Q - 📾 ? Þï Utilisateurs et ordinateurs Active Di Nom. Requêtes enregistrées N TESTSYSRAIL2 + 🟥 formation3.lan -Å user Builtin CHH Délégation de contrôle... Coll Déplacer. 💦 Do + Rechercher... Foi + for + Nouveau Mal + Toutes les tâches Usi + Autorisations pour formation X Objet Propriétés Tout le monde Modifier... Nom : Cet objet uniquement Appliquer à : • Autorisations : Refuser Autoriser Contrôle total 

Lister le contenu

Supprimer

Lire toutes les propriétés

Écrire toutes les propriétés

Supprimer la sous-arborescence

☑ ☑

Protéger l'objet des suppressions accidentelles

20644

Original :

## TP : délégation d'administration 1/4

Il est possible de déléguer des droits au niveau de chaque attribut (chaque champ) pour chaque type d'objet.

**Méthode 1 :** utilisateurs membres d'*Opérateur de Comptes*. Ces comptes utilisateur peuvent créer des groupes / comptes utilisateur / ordinateur dans l'AD.

**Méthode 2 :** Utilisateur l'assistant « *Délégation d'administration* » en mode basique. Cette méthode permet de déléguer des tâches basiques au niveau d'un OU particulière. Il n'est pas possible de déléguer les droits pour un ou plusieurs attributs.

**Méthode 3 :** Utiliser l'assistant Délégation en mode avancé « *Créer une tâche personnaliser à déléguer* ». Cette méthode permet de déléguer la gestion de certains attributs pour certains types d'objets.

**Méthode 4 :** lancer la console « *Utilisateurs et Ordinateurs Active Directory* » en mode d'affichage « *Fonctionnalités avancées* ». Aller au niveau d'une OU, cliquer sur « *Propriétés »* et aller dans l'onglet « *Sécurité* » puis passer en mode *Advanced*.

Microsoft propose maintenant une méthode appelée Tier 0, Tier 1 et Tier 2 pour déléguer l'administration Active Directory. L'idée principale est de séparer l'administration du service Active Directory (Tier 0), l'administration des serveurs (Tier 1) et l'administration des stations de travail et des comptes standards (Tier 2).

https://www.petri.com/keep-active-directory-secure-using-privileged-access-workstations https://social.technet.microsoft.com/wiki/contents/articles/37509.active-directory-red-forestdesign-aka-enhanced-security-administrative-environment-esae.aspx

## TP : délégation d'administration 2/4

Créer une OU appelée Msreport1.

Créer un compte utilisateur dans cette OU appelé admin1_msreport.

Faire un clic droit au niveau de l'OU CHU et cliquer « *Délégation de contrôle* ». Ajouter le utilisateur ou le groupe à qui vous souhaitez déléguer des droits d'administration.

Sélectionner le ou les droits à déléguer.

Se loguer sur une station de travail membre du domaine avec le compte *admin1_msreport*.

Installer les outils d'administration (RSAT) sur la station d'administration https://www.microsoft.com/en-us/download/details.aspx?id=45520 Tester la création d'un compte utilisateur.



## TP : délégation d'administration 3/4

Créer une OU appelée MSREPORT2.

Créer un compte utilisateur dans cette OU appelé *admin2_msreport*.

Clic droit sur l'OU CHU et cliquer « *Délégation de contrôle* ». Ajouter le utilisateur ou le groupe à qui vous souhaitez déléguer des droits d'administration.

Sélectionner « Créer une tâche d'administration personnalisée à déléguer ».

Sélectionner « Seulement les objets suivants dans le dossier ».

Cocher les cases « Créer et supprimer des objets ».

Sélectionner « générales » dans la fenêtre « Afficher les autorisations ».

Si vous souhaitez déléguer l'accès en écriture que pour certains attributs, cocher la case « *Spécifique aux propriétés* ».

Sélectionner les propriétés de votre choix.

Se loguer sur une station de travail membre du domaine avec le compte *admin2_msreport*.

Installer les outils d'administration (RSAT) sur la station d'administration

https://www.microsoft.com/en-us/download/details.aspx?id=45520 Tester la création d'un compte utilisateur.





Éc	rire N	lumé	éro	de té	léph	ione	
		,					

Lire Numéro de téléphone (Autres)
Carine Manager als 1414-14 and 1644

Écrire Numéro de téléphone (Autres)

Lire Numéro de téléphone domicile (Autres)

Écrire Numéro de téléphone domicile (Autres)

#### Autorisations :



## TP : délégation d'administration 4/4



# 7. Les stratégies de groupe

## La base de registre 1/2

#### La base de registre est la base de configuration de Windows.

Pour éditer la base de registre, on utilise REGEDIT ou REGEDT32 (c'est le même exécutable depuis Windows XP).

Ruche : ensemble de clés et de valeurs qui correspondent à un fichier au niveau du système.

Clés : c'est un conteneur de valeur.

Valeur : variable. Il existe différent type de valeur (binaire, chaîne de caractères, tableaux de chaines de caractères...).

La base de registre est organisée en deux grandes sections HKEY LOCAL MACHINE et HKEY USERS.

La ruche HKEY_CURRENT_CONFIG est une sous ruche de HKEY_LOCAL_MACHINE

Il est possible de charger des ruches (fichier *NTUSER.DAT* d'un autre utilisateur...).

Il est possible de définir des permissions au niveau des clés de registre



🙀 Editeur du Registre					
Fichier	Edition	Affichage	Favoris	?	
Continueur  Conti					
😭 Éditeu	ır du Regi	stre			
Fichier E	dition Af	fichage Favo	oris ?		
Image: Same series     Image: Same series     Image: Same series     Image: Same series       Image: Same series     Image: Same series     Image: Same series     Image: Same series					
	SECU SECU SOFT	Déveloj Nouveau Recherch	pper J her	×	
HKEY_USE Supprimer     HKEY_CUI     Renommer					
Exporter					
		Autorisa	tions		

Autorisations pour SAM				
Sécurité				
Noms de groupes ou d'utilisateurs :				
& Système				
& Administrateurs (FORMATION3\Administrateurs)				
<u> </u>				
	Ajouter	Suppri		
Autorisations pour Sustème				
Hatonodione pour oyeteme	Autoriser	Refu		
Contrôle total	V			
Lecture				
Autorisations spéciales				

## La base de registre 2/2

Les paramètres de *HKEY_USERS* correspondent à la configuration spécifique au niveau des utilisateurs. Les paramètres de *HKEY_LOCAL_MACHINE* correspondent à la configuration de la machine (commune pour tous les utilisateurs).

Dans *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services*, on retrouve la configuration des services. Dans *HKEY_LOCAL_MACHINE* | *SOFTWARE*, on retrouve la configuration des logiciels commun à tous les utilisateurs. Dans *HKEY_USERS* | *SOFTWARE*, on retrouve la configuration des logiciels commun spécifique à un utilisateur.





#### TP : base de registre

Sur une station de travail Windows XP Pro, lancer l'éditeur de base de registre. Aller dans HKEY_LOCAL_MACHINE | SAM | SAM.

Faire un clic droit sur le dossier SAM et cliquer sur « Autorisation ».

Ajouter les droits *Control Total* au groupe *Administrateurs* de la base SAM locale. Vous pouvez maintenant visualiser le contenu de la base SAM locale.

Créer un compte utilisateur appelé « *testregistre* » au niveau du domaine et se loguer avec ce compte sur la station de travail. Personnaliser puis fermer la session (ajout imprimante réseau...).

Ouvrir une session avec le compte administrateur local sur cette station de travail. Lancer l'éditeur de base de registre.

Sélectionner « *HKEY_USERS* » puis aller dans le menu « *Fichier* » et cliquer sur « *Charger la ruche* ». Aller dans « *c:\Documents and settings\testregistre* » et sélectionner le fichier « *NTUSER.DAT* ». A quoi correspond ce fichier ? Faire une recherche au niveau de « *HKEY_LOCAL_MACHINE* » sur la clé « PROFILEIMAGEPATH ». A quoi sert cette clé. On se rend compte que toute la sécurité est basé sur le SID. Il est possible de réassocier un compte utilisateur avec le profil d'un autre utilisateur. Pour plus d'informations, voir <u>http://msreport.free.fr</u>. Aller dans c:\windows\system32\config. On y retrouve tous les fichiers des ruches de la base de registre.

## Qu'est ce qu'une stratégie de groupe ?

Les stratégies de groupes (GPO) : se sont des clés et valeurs de registre.

Deux sections pour les stratégies de groupe : Configuration ordinateur (modifie

HKEY LOCAL MACHINE) et Configuration utilisateur (modifie HKEY_USERS).

Les stratégies de groupe se décomposent en deux composants, les fichiers de stratégie de groupe (dans le répertoire

SYSVOL\SYSVOL\nomdomainedns\Policies), un objet stratégie de groupe (dans le conteneur SYSTEM au niveau de la partition de domaine).

📙 Policies	🕌 {31B2F340-016D-11D2-94	
C:\windows\SYSVOL\sysvol\formation10.lan\Policies	GOV 🖟 16D-11D2-945	USER
Fichier Edition Affichage Outils ?	Fichier Edition Affichage C	🕤 🖓 🔰 1D2-9
Organiser 👻 Inclure dans la bibliothèque 👻 Partager avec 💌	Organiser 👻 🛛 Inclure dans la t	Fichier Edition Affich
Nom * Modifié le	Nom *	Organicar 💌 Jochwa
{6AC1786C-016F-11D2-945F-00C04fB984F9} 07/06/20		Organiser + Inclure
🔑 {31B2F340-016D-11D2-945F-00C04FB984F9} 07/06/20		Nom *
4946D8591-D291-4947-BC5F-1F12B993A627} 10/06/20		
B4A67723-01B4-48C6-AC5F-A314B6A945D4} 10/06/20		Registry.pol





## Présentation de la console GPMC

La console *Gestion des stratégies de groupe* : permet d'ajouter, lier, modifier et supprimer les GPO.

Il est possible d'ajouter de créer des stratégies de groupes personnalisées (fichier ADM ou ADMX).

A la création du domaine, deux GPO, la « *Default Domain Policy* » (configuration du domaine ) et la *Default Domain Controller Policy* (configurer des DC). **Ne pas supprimer ces deux GPO. Eviter de les modifier.** 

Possibilité d'exporter / importer des GPO via GPMC.

🛃 Gestion de stratégie de groupe					
🕌 Fichier Action Affichage Fenêtre ?					
Image: Section de stratégie de groupe         Image: Section de stratégie de groupe <t< th=""><th>Default Domain Controllers Policy Étendue Détails Paramètres Délégation</th><th></th></t<>	Default Domain Controllers Policy Étendue Détails Paramètres Délégation				
<ul> <li>Initiation Control and Policy</li> <li>Image: State of the state</li></ul>	Default Domain Controllers Policy Données recueillies le : 10/06/2010 19:47:01 Configuration ordinateur (activée)	<u>afficher tout</u> <u>masquer</u>			
🖃 💼 Domain Controllers	Stratégies	masquer			
🛒 Default Domain Controllers I 💼 Formation	Paramètres Windows	masquer			
🕀 🖬 Production	Paramètres de sécurité	masquer			
∃ 20 Vente ∃ 20 Vente ∃ 20 Vente	Stratégies locales/Attribution des droits	utilisateur <u>masquer</u>			
🗄 📑 Filtres WMI	Stratégie	Paramètre			
<ul> <li></li></ul>	Accéder à cet ordinateur à partir du réseau	BUILTIN/Accès compatible pré-Windows 2000, AUTORITE NT/ENTERPRISE DOMAIN CONTROLLERS, AUTORITE NT/Utilisateurs authentifiés,			

## Les stratégies de groupe

Déployer des logiciels (installeur au format .MSI obligatoire). Pas de rapport, risque saturation réseau si gros logiciels.

Déposer les exécutables dans le partage NETLOGON ou SYSVOL.

D'exécuter des scripts au démarrage / arrêt de la machine (sous compte SYSTEM).

De configurer les stratégies de mots de passe, Kerberos et de verrouillage de comptes. Les paramètres de stratégie de mot de passe pour les comptes du domaine se définissent uniquement au niveau de la « *Default Domain Policy* ». Si on définit ce paramètre dans une autre stratégie, cela s'applique pour les comptes locaux. Voir <u>http://msreport.free.fr/?p=156</u>.

De configurer les paramètres et options de sécurité (qui peut ouvrir une session localement, arrêter la machine, accéder à la machine via le réseau, changer l'heure, les protocoles d'authentification autorisés...).

De configurer les paramètres des logiciels et du système (configuration Windows Update, panneau de configuration, pare feu). Il est possible d'ajouter des fichiers ADM / ADMX supplémentaires pour ajouter de nouvelles stratégies (configuration Adobe, Citrix, Office...) : <a href="http://www.microsoft.com/downloads/details.aspx?familyid=92d8519a-e143-4aee-8f7a-e4bbaeba13e7&displaylang=en">http://www.microsoft.com/downloads/details.aspx?familyid=92d8519a-e143-4aee-8f7a-e4bbaeba13e7&displaylang=en</a>

Depuis Windows 2008, L incluse GPO de préférences. Nécessite déploiement d'un correctif sur Windows XP / Vista / 2003. Voir <u>http://support.microsoft.com/kb/943729/en-us</u>

#### Les paramètres de stratégie de groupe


# Comment s'appliquent les GPO ?

Une GPO « *Configuration Ordinateur* » s'applique à une machine (si compte ordinateur est dans OU où est liée la GPO et si le compte ordinateur a les droits « *Lire* » et « *Appliquer la stratégie de groupe* »).

Une GPO « *Configuration Utilisateur* » s'applique aux utilisateurs (si compte utilisateur est dans OU où est liée la GPO et si le compte utilisateur a les droits « *Lire* » et « *Appliquer la stratégie de groupe* »).

Par défaut « *Utilisateurs authentifiés* » (toutes les comptes ordinateurs et utilisateurs qui ont ouvert une session) a les droits « *Lire* » et « *Appliquer la stratégie de groupe* ». Possibilité filtrage en supprimant cet entité de sécurité.





### Ordre d'application des GPO

Possibilité de fixer des GPO avec des paramètres contradictoires à différents niveaux.

Pour gérer les conflits, les GPO s'appliquent dans un certains ordre :

Local, Site, Domaine, unités d'organisation, unités d'organisation enfant

En cas de conflit c'est la dernière stratégie qui s'applique qui l'emporte sauf si les paramètres « *Appliquer* » (ne pas passer outre) et « *Bloquer l'héritage* » ont été définis.

Paramètre « *Appliquer* » : force l'application de la GPO.

Paramètre « Bloquer l'héritage » : si ce paramètre est fixé au niveau d'une OU enfant, les GPO au niveau des sites, domaines et des OU parent ne s'appliquent pas (sauf les paramètres de sécurité).

Le paramètre « Appliquer » prime sur le paramètre « Bloquer l'héritage ».



### Les stratégies de mots de passe 1/2

Paramètres de stratégies de mots de passe : configurable au niveau de la stratégie « *Default Domain Policy* ».

Utiliser les *Fine Grained Password Policy / Granular Password Policy* pour créer des stratégies de mots de passe spécifiques pour un groupe d'utilisateurs : Permet d'attribuer une stratégie de mots de passe à un compte utilisateur ou à un groupe. Nécessite domaine en mode Fonctionnalité Windows 2008. <u>http://technet.microsoft.com/en-us/library/cc770394(WS.10).aspx</u>

🧾 Éditeur de gestion des stratégies de groupe		
Fichier Action Affichage ?		
🧇 🧼 🙎 📊 🔒 👔 🗊		
🧾 Stratégie Default Domain Policy [SFR1.FORMATION10.LA	Stratégie 🔺	Paramètres de stratégie
<ul> <li>Image: Configuration ordinateur</li> <li>Image: Stratégies</li> </ul>	Conserver l'historique des mots de passe	24 mots de passe mémorisés 42 jours
<ul> <li>              ■ Paramètres du logiciel      </li> <li>             ■ Paramètres Windows         </li> <li>             ■ Stratégie de résolution de noms</li></ul>	<ul> <li>Durée de vie minimale du mot de passe</li> <li>Durée de vie minimale du mot de passe</li> <li>Enregistrer les mots de passe en utilisant un chiffrem</li> <li>Le mot de passe doit respecter des exigences de co</li> <li>Longueur minimale du mot de passe</li> </ul>	1 jours Désactivé Activé 7 caractère(s)

### Les stratégies de mots de passe 2/2

Modification ADSI

Attribute	Value	Quick explanation
Cn	PassPolAdmins	This is the name of the policy. Try to come up with a naming convention for these policies if you will have lots of them.
msDS-PasswordSettingsPrecedence	10	This number is used as a 'cost' for priority between different policies in case a user is hit by multiple PSOs. Be sure to leave space below and above for future use. The stronger the PSO password settings are, the lower the 'cost' should be.
msDS-PasswordReversibleEncryptionEnabled	False	Boolean value to select if passwords should be stored with reversible encryption (usually not a good idea).
msDS-PasswordHistoryLength	32	How many previously used passwords should the system remember?
msDS-PasswordComplexityEnabled	True	Should the users use a complex password? (Boolean value)
msDS-MinimumPasswordLength	16	What should be the minimum number of characters in the user accounts password?
msDS-MinimumPasswordAge	-86400000000 (9 zeros)	What is the minimum password age? (in this case 1 day) NB! Minus sign
msDS-MaximumPasswordAge	-3628800000000 (9 zeros)	What is the maximum password age? (in this case 42 days) NB! Minus sign

msDS-LockoutTreshold	30	How many failed attempts before the user account will be locked?
msDS-LockoutObservationWindow	-1800000000 (9zeros)	After how long should the counter for failed attempts be reset? (in this case 6 minutes) NB! Minus sign
msDS-LockoutDuration	-1800000000 (9zeros)	For how long should the user account object be locked in case of too many bad passwords entered? (in this case 6 minutes) NB! Minus sign

#### Fichier Action Affichage ? | 🖄 📰 🗙 🗊 🤕 🐟 🛛 🖬 (= Nom OU=Formation CN=LostAndFound Aucun él CN=Managed Service Accounts CN=NTDS Quotas OU=Production 🦲 CN=Program Déplacer 🖃 🧮 CN=System Nouvelle connexion à partir d'îci CN=Admir CN=ComF Nouveau ы Objęt.. CN=ComF Affichage CN=Defai CN=Dfs-C Supprimer CN=Doma Renommer CN=File R Actualiser CN=FileLi( Exporter la liste... CN=IP Se CN=Meet Propriétés CN=Micro Aide CN=Pass CN=Policies CN=PSPs CN=RAS and IAS Servers Acces CN=RpcServices CN=WinsockServices 📋 CN=WMIPolicy CN=Users 🣔 OU=Vente

# Bloquer les applications non autorisées

Permet de définir quels sont les applications que l'on peut exécuter sur une station de travail.

APPLOCKER ne fonctionne qu'avec Windows Seven ou Windows 2008 R2.

Utiliser le mode d'inventaire avant de mettre des stratégies restrictives.

http://technet.microsoft.com/fr-fr/library/ee424367(WS.10).aspx

# Dépannage des stratégies de groupes 1/2

Utiliser l'outil GPRESULT ou le composant logiciel enfichable « *Jeu de stratégies résultants* » pour déterminer quels sont les paramètres de stratégies de groupe qui s'appliquent.

Toujours consulter l'onglet « *Aide* » au niveau d'un paramètre de stratégie de groupe (désactiver une stratégie qui masque le panneau de configuration active le panneau de configuration...).

Pour les scripts de déploiement réseau, configurer la stratégie « *Ouverture de session : attendre les connexions réseau* » pour forcer l'application des scripts de démarrage avant l'ouverture de session.

http://support.microsoft.com/kb/887303

http://technet.microsoft.com/en-us/library/bb727058.aspx

http://support.microsoft.com/kb/555982/en-us

Pour bloquer l'application des stratégies pour les administrateurs : supprimer l'entité « *Utilisateurs authentifiés* » et ajouter les droits lire et appliquer la stratégie à des groupes utilisateurs et des groupes d'ordinateurs. Pour plus d'informations, voir <u>http://support.microsoft.com/kb/816100/en-us</u>

En cas de suppression des stratégies *Default Domain Policy* et *Default Domain Controller Policy*, appliquer l'article : <u>http://support.microsoft.com/kb/555647/en-us</u> Pour réinitialiser stratégie sécurités :

http://support.microsoft.com/kb/324800/en-us

# Dépannage des stratégies de groupes 2/2

Bug GPRESULT : <u>http://support.microsoft.com/kb/837129/en-us</u> et http://support.microsoft.com/kb/927908/en-us

Pour afficher les stratégies de mots de passe : *net accounts /domain* Les stratégies de préférence : <u>http://support.microsoft.com/kb/943729/en-us</u>

🛜 Console1 - [Racine de la console]		🔚 Console1 - [Racine de la console\Adminis	strateur on SFR1 - RSoP\Configuration ordinateur\Paramètres	s Windows\Param
Fichier Action Affichage Favoris Fenêtre ?		🚠 Fichier Action Affichage Favoris Fer	être ?	
		🗢 🔿 📶 🗙 🗐 😽 🚺 🗊		
		Carle de la console	Stratégie 🔺	Paramètre de l'ordii
Racine de la console Nom		Administrateur on SFR1 - RSoP     Administrateur on ordinateur	Conserver l'historique des mots de passe     Durée de vie maximale du mot de passe	24 mots de passe n 42 jours
Ajouter ou supprimer des composants logiciels enfichable	:5	🕀 🧾 Paramètres du logiciel	i Durée de vie maximale du not de passe	1 jours
Vous pouvez sélectionner des composants logiciels enfichables part composants logiciels enfichables extensibles, vous pouvez spécifier	mi ceux disponibles sur votre ordinat r quelles extensions doivent être act	<ul> <li>Paramètres Windows</li> <li>Paramètres de sécurité</li> <li>Paratégies de comptes</li> <li>Stratégie de mot de p</li> </ul>	Enregistrer les mots de passe en utilisant un chiffrement réversible Le mot de passe doit respecter des exigences de complexité Longueur minimale du mot de passe	Désactivé Activé 7 caractère(s)
Composants logiciels enrichables disponibles :	Composants logicleis enn. selectionn	🕀 📑 Stratégie de verrouill.	Propriétés de : Conserver l'historique des mots de passe	? ×
Composant logicler enn Pournisseur	Jeu de stratégie résultant	E i Stratégies locales I filosofie d'audit	Paramètre de stratégie de sécurité Priorité Expliquer	
Lien vers une adress Microsoft Cor		H Attribution des droits	Conserver l'historique des mots de passe	
🚟 Console1 - [Racine de la console\Jeu de stratégie résultant]				
🚡 Fichier Action Affichage Favoris Fenêtre ?				
		c:/>gpresult /R		
Cacine de la console     Seu de stratégie résultant     Jeu de stratégie résultant		Outil de résultat du système Copyright (C) Microsoft Corr	: d'exploitation Microsoft (R) Windows (F ). 1981–2001	l> v2.0
Generer les données Roop r obtenir une		Jeu créé le 10/06/2010 à 21:	26:39	
Nouvelle fenêtre à partir d'îci	Action requise			
Nouvelle vue de la liste des tâches	tionner 'Générer les données RSoP…' à partir	Données RSOP pour MSREPORTFO	PRM\Administrateur sur SFR1 : mode journa	lisation
Assistant Jeu de stratégie résultant Assistant Jeu de stratég	Assistant Jeu de stratégie résulta	Configuration du système d'e Version du système d'exploit Nom du site Parfi itiréurat	xploitation : Contrôleur principal de do ation : 6.1.7600 	omaine
Selection du mode         Selection des ordinal           Vous pouvez afficher les paramètri utilisateur sélectionné, ou simuler u         Vous pouvez affiche	Sélection de l'utilisateur Vous pouvez afficher les param l'ordinateur sélectionné.	Profil local Connexion via une liaison le	nrn : C:\Users\Administrateur nte ? : Non	
		Paramètre de l'ordinateur		
Quel mode voulez-vous utiliser ? Sélectionnez l'ordinateur		CN=SFR1,OU=Domain Contro Heure de la dern <u>ière ap</u> r	llers,DC=formation10,DC=lan llication de la stratégie de gr <u>oupe : 10/</u>	′06/2010 à 21
Mode de journalisation Cet ordinateur	<ul> <li>Afficher les paramètres de la stra</li> </ul>	:23:25		
Vérifier les paramètres de strat utilisateur spécifique	Otilisateur actuel			
	O Utilisateur spécifique :			

# 8. Les mécanismes de réplication :

### Les sites Active Directory

Réplication Active Directory : basée sur numéro USN (Unique Séquence Number). La restauration autoritaire (avec NTDSUTIL) permet d'augmenter numéro USN. Par défaut, les DC <u>d'un même site</u> réplique toutes les 15 secondes entre eux.

Intérêt de créer plusieurs sites Active Directory : définir avec quels DC les stations de travail s'authentifient et configurer l'intervalle de réplication entre contrôleurs de domaine.

Chaque site est associé à un ou plusieurs sous réseaux IP. Un sous réseau IP ne peut pas être associé à deux sites Active Différents.

Pour configurer 2 sites AD différents, il faut 2 sous réseaux IP (un pour chaque site).

Les DC répliquent entre eux via des objets « *Connexion* » (unidirectionnel). Les objets « *Connexion* » sont générés par le KCC (DC dans même site) et par l'ISTG entre 2 sites. Pour forcer la génération objets « Connexion » : *repadmin /KCC.* Best Practice : prévoir un serveur de Catalogue Global dans chaque site ou activer la mise en cache des groupes universels. <u>http://support.microsoft.com/kb/242780/en-us</u> <u>http://support.microsoft.com/kb/305179/en-us</u>

http://www.tech-faq.com/lang/fr/active-directory-replication.shtml

### TP: Les sites Active Directory 1/5

Le service RRAS permet de transformer Windows Server en routeur IP, serveur NAT, serveur VPN et en serveur RAS.

Depuis Windows Server 2008 R2, il est nécessaire d'installer le rôle « Services de stratégies et d'accès distants » et de configurer ensuite le service RRAS en tant que routeur IP.

Installer le rôle « Services de stratégies et d'accès réseau » avec les services de rôles « Service de routage et accès distant ».

Aller dans les outils d'administration et lancer la console « *Routage et Accès distants* ».



### TP : Les sites Active Directory 2/5

Démarrer la console « *Routage et Accès distant* » (dans les outils d'administration). Cliquer sur « Configurer et activer le routage et l'accès distant ». Sélectionner « *Configuration personnalisée* » puis « *Routage IP »*. Cliquer sur « *Démarrer le service* ». Valider que les deux contrôleurs de domaine peuvent communiquer ensemble (ping).



Assistant Installation d'un serveur Routage et accès distant	Assistant Installation d'un serveu	🚊 Routage et accès distant	
Configuration Vous pouvez activer l'une des combinaisons de services suivantes ou vous pouvez personnaliser ce serveur.	Configuration personnalisée À la fermeture de l'Assistant, vo	Fichier Action Affichage ?	2 ==
<ul> <li>Accès à distance (connexion à distance ou VPN) Autoriser les clients distants à se connecter à ce serveur via une connexion d'accès à distance ou via Internet au moyen d'une connexion sécurisée à un réseau privé virtuel (VPN).</li> <li>NAT (Network address translation) Autoriser les clients internes à se connecter à Internet en utilisant une adresse IP publique.</li> <li>Accès VPN (Virtual Private Network) et NAT Autoriser les clients distants à se connecter à ce serveur par Internet et les clients locaux à se connecter à Internet en utilisant une seule adresse IP publique.</li> <li>Connexion sécurisée entre deux réseaux privés Connecter ce réseau à un réseau distant tel que celui d'une succursale.</li> <li>Configuration personnalisée Sélectionner une combinaison de fonctionnalités disponibles dans Routage et accès distant.</li> </ul>	Sélectionnez les services que vous Accès VPN Accès réseau à distance Connexions à la demande NAT Routage réseau	<ul> <li>Routage et accès distant</li> <li>Statut du serveur</li> <li>SFR4 (local)</li> <li>Interfaces réseau</li> <li>Connexion et stratégies (</li> <li>IPv4</li> <li>Général</li> <li>Itinéraires statiques</li> <li>Général</li> <li>Itinéraires statiques</li> </ul>	Général         Inter       Adresse IP         Lan2       192.168.2.254         Lan       192.168.1.254         Interne       Non disponible         Bouclage       127.0.0.1

### TP : Les sites Active Directory 3/5

Définir 1^{er} DC avec IP : 192.168.1.1 /24 et 2^{ème} DC avec IP : 192.168.2.1 /24. Changer les adresses de serveur DNS et indiquer une passerelle (routeur RRAS). Supprimer les anciennes entrées dans le DNS (anciennes IP des DC).

Taper les commandes suivantes :

Ipconfig /registerdns

Net stop netlogon & Net start netlogon

Ipconfig /flushdns

Valider que les deux DC peuvent communiquer ensemble (PING).

Lancer « Sites et Services Active Directory » . Forcer la réplication entre les 2 DC.

Renommer le site par défaut en « Nemours ». Créer un second site appelé

« Meudon ». Créer 2 SUBNETs 192.168.1.0./24 et 192.168.2.0 /24. Lier 1^{er} SUBNET au site Nemours, lier 2^{ème} SUBNET à Meudon.

Renommer le lien inter-sites par défaut en Nemours-Meudon. Configurer la

réplication sur 15 minutes. Permettre la réplication à toutes heures.

Déplacer le 2^{ème} contrôleur de domaine dans le site Meudon. Lancer la commande repadmin /kcc pour forcer l'ISTG à générer les objets Connexion.

Supprimer les liens connexions. Désactiver le KCC / ISTG :

http://support.microsoft.com/kb/242780/en-us

Taper la commande repadmin /KCC. Que se passe t'il ? Créer les liens de connexion manuellement.

### TP : Les sites Active Directory 4/5

Fichier Action Affichage ?	📲 Sites et services Activ <u>e Directo</u>	Y			
	Fichier Action Affichage ?				
Sites et cervices Active Directory [SFR 1. formation 10.lan]     Nom     Depuis le serveur       Sites     Sites     Sites		2 🖬 🗾			
Constant     Constant	Sites et services Active Directory [Sites et services Active Direc	R 1. formation 10.lan]	Nom	Site	Empla
Remours     Servers     SFR1     SFR1     SFR1     SFR1	Sites     Subnets     Inter-Site Transports     Nemours	Nouvel objet - Sous-r	éseau		
Image: Services         Image: Services         Image: Services	Servers     SFR1	Créer dans	s : formation 10.lan/	'Configuration/Sites/	Subnets
Fichier       Action       Affichage       ?         Image: Image and the second secon	Imposized angle     I	Entrez le préfixe d'ad (adresse/longueur du nombre de bits fixes. IPv4 ou IPv6. En savoir plus sur l'er	lresse en utilisant la n u préfixe), où la longu Vous pouvez entrer u ntrée des préfixes d'a	otation de préfixe rés eur du préfixe indique un préfixe de sous rés <u>idresse.</u>	eau : le :eau
Sites et services Active Directory [SFR1.formation 10.lan]       Nom       Type         Sites       Supers       Conteneur de s         Sites       Inter-Site Transports       Wouvel objet - Site		Exemple IPv4 : 157 Exemple IPv6 : 3FF Préfixe :	:54.208.0/20 E:FFFF:0:C000::/64		
Image: Servers         Imaget		192.168.1.0/24 Nom du préfixe des s	ervices de domaine /	Active Directory :	
Nom : Meudon		192.168.1.0/24			
Sélectionnez un objet lien de sites pour ce site. Les objets lien de situés dans le conteneur Transports sites/inter-sites.		Nom du site	a du site pour ce pren		
DEFAULTIPSITELINK		Nemours			
sites et services Active Directory					
Fichier Action Affichage ?					
(= e) 🖄 🗊 📴 🔂 📷 🔟					
Sites et services Active Directory [SFR 1. formation 10. lan] Nom Site Type					



192.168.1.0/24 Nemours

192,168,2.0/24 Meudon

Sous-réseau

Sous-réseau

### TP : Les sites Active Directory 5/5

y∯Sites et services Active Directory	Sites et services Active Directory
Fichier Action Affichage ?	Sites et services Active birectory
Sites et services Active Directory [SFR1.formation 10.lan] Nom Type Descri	Fichier Action Affichage ?
Sites  Subnets  Propriétés de : Nemours-Meudon  Lien du site  Propriétés de : Nemours-Meudon	🗢 🔿 🙋 📅 🖌 🗶 🗊 🧔 🐟 📝 🗊 💆
Image: Servers       Image: Servers         Image: Servers       Image: Se	Sites et services Active Directory [SFR1.formation 10.lan]   Sites   Subnets   Subnets   Inter-Site Transports   Meudon   Servers   Servers   Servers   Nemours   Serve   Serve   Serve   Serves   Serve   Serve   Serves   Serve   Serves   Serve   Serve   Serves   Serve   Serves     Serves
Modifier la planification	Attichage
Planification pour Nemours-Meudon	Sites et services Active Directory
	Fichier Action Affichage ?
0 · 2 · 4 · 6 · 8 · 10 · 12 · 14 · 16 · 18 · 20 · 22 · 0	
Tous Annuler	Sites et services Active Directory [SFR1.formation10.lan]
	Image: Subsets     Répliquer maintenant
mardi C. Réplication non	Inter-Site Transports
mercredi disponible	<ul> <li>□ Servers</li> <li>□ I SFR2</li> <li>Une ou plusieurs de ces connexions des services de domaine</li> <li>Active Directory sont partagées entre plusieurs contrôleurs de</li> </ul>
jeudi	domaine dans des sites différents. Les services de domaine Active Directory vont essayer de répliquer ces connexions. Pour plus
	Generation d'informations sur la verification de la replication, consultez Aide et support.
	E SFR1
Du lundi au dimanche, de 00:00 à 00:00	E Services

9. Sauvegarde et restauration Active Directory

# Windows Server Backup 1/5

NTBACKUP a été replacé par « Windows Server Backup ».

Windows Server Backup permet prend en charge la déduplication quand on sauvegarde sur une partition dédiée. On peut donc exécuter des sauvegardes complètes toutes les heures. Seuls les blocs modifiés sont sauvegardés. Windows Server Backup ne permet pas de sauvegarder sur bande. Pour faire une sauvegarde sur bande, sauvegarder vers un partage et sauvegarder ensuite les fichiers produits par « *Windows Server Backup* ».

Quand on fait une sauvegarde sur disque local, le disque est formaté en NTFS mais n'est pas monté. Il est alors réservé par Windows Server Backup.

### Mise en pratique :

Prérequis : Il faut disposer d'un second disque sur le serveur (dédié).

Lancer la détection des disques et à le mettre en ligne.

Installer la fonctionnalité « *Windows Server Backup* » (avec la partie PowerShell). Lancer la console « *Windows Server Backup* » et cliquer sur Planifier une sauvegarde. Cliquer sur sauvegarde complète (inclue la sauvegarde de l'Etat du système). Faire une sauvegarde plusieurs fois par jour vers un disque dédié. Aller dans les tâches planifiées, dans la section backup. Modifier la tâche pour qu'elle autorise les actions manuelles et lancer une sauvegarde.

Ouvrir la console Windows Server Backup et valider l'état d'avancement de la sauvegarde.

### Windows Server Backup 2/5

🚆 Gestionnaire de serveur	Gestionnaire de serveur		Assistant Ajout de fonctionnalit	és	
Fichier     Action     Affichage       Image: Section are de serveur (SFR1)	Gestonnare de serveur (SFRI)	stion des disques Liste ume (C:) GRMSXEVAL FR. DVD (D:)	Sélectionner o	les fonctionnalités	
<ul> <li>Rôles</li> <li>Fonctionnalités</li> <li>Diagnostics</li> <li>Configuration</li> <li>Stockage</li> <li>Sauvegarde de Windows Server</li> <li>Gestion dos dissuos</li> <li>Actualiser</li> <li>Analyser les disques de nouveau</li> </ul>	Configuration     Configuration     Sourcegarde de Windows Server     Section des disques     Gestion des disques     Configuration     Configuration	Réservé au système Disque 0 100 Mo h ligne Disque 1 Disque 1 Disque 1 Correction 1 Propriétés	Fonctionnalités Confirmation État d'avancement Résultats	Sélectionnez une ou plus Fonctionnalités : Fonctionnalités Sauvegarde Outils en lig Econtionnalités	sieurs fonctionnalités à installer sur ce serv de la Sauvegarde de Windows Server e de Windows Server <mark>ne de commande</mark> du NET Framework 3 5 1 (Toctallá)
	Fichier       Action       Affichage       ?         Image: Image and the second secon			_ [] ×	
	Gestionnaire de serveur (SFR1) Contionnailtés Diagnostics Configuration Stockage Sauvegarde de Windows Server Gestion des disques	Sauvegarde de Windows S Sauvegarde de Wi Cette application réguliers. Aucune sauvegarde régu Messages (Activité de la Durée 👻	Server /indows Server ▲ n permet d'effectuer une sauvegarde ponctuelk n'a été configurée sur cet ordinateur. Utilisez l'Assistant Planifica lière ou ponctuele. semaine dernière, double-cliquez sur le message pour Message Description	Actions       Sauvegarde de Windows Server       Planification de sauvegarde       Sauvegarde unique       Récupérer       Configurer les paramètres de perform       Affichage       Alde	

h Assistant Planification (	le sauvegarde 🛛 🔀
Sélectionr	ner la configuration de la sauvegarde
Mise en route	Quel type de configuration voulez-vous planifier ?
Sélectionner la configu	Serveur entier (recommande)
Spécifier l'heure de la s	Je veux sauvegarder toutes les données et les applications présentes sur le serveur, ainsi que l'état du système.
Spécifier le type de de	Taille de la sauvegarde : 8,49 Go
Confirmation	C Personnalisé
Résumé	Je veux choisir des volumes et des fichiers personnalisés pour la sauvegarde.

#### 🐜 Assistant Planification de sauvegarde



#### Spécifier l'heure de la sauvegarde

Mise en route Sélectionner la configu Spécifier l'heure de la s	À quelle fréquence et à quel moment voule C Tous les jours Sélectionnez une heure : 21:00	z-vous exécut
Spécifier le type de de	Plusieurs fois par jour	
Confirmation	Cliquez sur une heure disponible, puis s	ur Ajouter pou
Résumé	planification de sauvegarde.	Herme else i
	remps asponible :	
	00:30	22:30
	01:30	23:00
	02:00 Ajouter >	23:30

### Windows Server Backup 3/5

🍇 Assistant Planification	de sauvegarde 🛛 🔀
Spécifier	le type de destination
Mise en route Sélectionner la configu Spécifier l'heure de la s Spécifier le type de de	Où voulez-vous stocker les sauvegardes ? Sauvegarder vers un disque dur dédié aux sauvegardes (recommandé) Sélectionnez cette option pour stocker de la manière la plus sûre les sauvegardes. Le disque dur utilisé sera formaté, puis utilisé uniquement pour stocker les sauvegardes.
Sélectionner le disque Confirmation Résumé	Sauvegarder vers un volume Sélectionnez cette option si vous ne pouvez pas dédier tout un disque à la sauvegarde. Notez que cette option peut réduire les performances du volume de 200 pour cent durant le stockage des sauvegardes. Il est recommandé de ne pas stocker d'autres données de serveur sur le même volume.
	Sauvegarder sur un dossier réseau partagé Sélectionnez cette option uniquement si vous ne voulez pas stocker les sauvegardes sur le serveur lui-même. Notez que vous ne disposerez que d'une sauvegarde à la fois lorsque vous créez une nouvelle sauvegarde, car celle-ci remplace la précédente.

#### 👆 Assistant Planification de sauvegarde



S S Sélectionner le disque de destination

lise en route électionner la configu pécifier l'heure de la s	Sélectionnez un ou plusieurs disques pour stocker vos sauvegardes. Vous pouvez utiliser plusieurs disques de sauvegarde si vous souhaitez stocker des disques hors site. Disques disponibles :				
pécifier le type de de…	Disque	Nom	Taille	Espace uti	Volumes prés
électionner le disque	✓ 1	Msft Virtual	50,00 Go	0 Ko	
onfirmation					
ésumé					
				Afficher tous les d	disques disponibles

#### Sauvegarde de Windows Server

Une fois que vous avez terminé cet Assistant, les disques sélectionnés seront reformatés et tous les volumes et données des disques seront supprimés. Pour permettre aux utilisateurs de déplacer les sauvegardes hors site à des fins de protection en cas d'urgence et pour garantir l'intégrité des sauvegardes, l'intégralité des disques sera dédiée au stockage des sauvegardes et ne sera pas visible dans l'Explorateur Windows.

Oui.

Non.

Cliquez sur Oui pour utiliser le ou les disques sélectionnés.



### Windows Server Backup 4/5

Une fois la sauvegarde terminée, relancer une seconde fois la sauvegarde. L'espace disque évolue t'il ? Le fait de faire une seconde sauvegarde nous fait passer de 7,01 Go à 7,03 Go.

Lancer PowerShell et taper la commande suivante : *add-pssnapin* 

*windows.serverbackup*. Cela ajoute les CMDLET Windows Server backup à PowerShell.

Taper ensuite la commande get-command -module windows.serverbackup pour afficher les commandes Windows Server Backup.





Durée 👻	Message	Description	
10/06/2010 22:52	Sauvegarde	Réussite	
itatut			
)ernière sauvegarde		Prochaine sauvegarde	Toutes les sauvegardes
ítat : 👩 Réussite		État : Planifiée	Total des sauvegardes : 1 copies
Ourée : 10/06/2010 22:52		Durée : 10/06/2010 23:00	Copie la plus récente : 10/06/2010 22:52
Afficher les détails		Afficher les détails	Copie la plus ancienne : 10/06/2010 22:52
			Afficher les détais

Paramètres		11	<ul> <li>Utilisation de la destination</li> </ul>	
Éléments de sauvegarde :	Récupération complète; État du système; Réservé au s		Nom :	SFR1 2010_06_10 22:49 DISK_01
Fichier exclus :	Aucun		Canada	49.98.60
Option avancée :	Sauvegarde complète VSS		Espace utilisé :	7.01.60
Destination :	SFR1 2010_06_10 22:49 DISK_01		Sarvenardes disponibles :	1 String
Heure de la sauvegarde :	Tous les jours 00:00; 22:30; 23:00; 23:30			- copies
			Afficher les détails	



### Windows Server Backup 5/5

Pour externaliser la sauvegarde, faire une sauvegarde sur un LUN hébergé sur un SAN (Fibre Channel / DAS obligatoire). Cela permet de conserver la déduplication.

Vérifier qu'il est possible de charger le pilote de la carte Fibre / DAS depuis le CD d'installation (en mode récupération).

http://technet.microsoft.com/en-us/library/ee849849(WS.10).aspx http://technet.microsoft.com/en-us/library/cc771290(WS.10).aspx http://www.winserverhelp.com/2010/03/windows-server-2008-r2-backup-and-restore/ http://unifiedit.wordpress.com/2009/12/17/forest-recovery-ad-2008/

#### Sauvegarde planifiée

Une sauvegarde planifiée à intervalles réguliers est configurée pour ce serveur.

— Daramétrec —	
Farametres	
Éléments de sauvegarde :	Récupération complète; État du système; Réservé au s
Fichier exclus :	Aucun
Option avancée :	Sauvegarde complète VSS
Destination :	SFR1 2010_06_10 22:49 DISK_01
Heure de la sauvegarde :	Tous les jours 00:00; 22:30; 23:00; 23:30

-Utilisation de la destination	
Nom :	SFR1 2010_06_10 22:49 DISK_01
Capacité :	49,98 Go
Espace utilisé :	7,03 Go
Sauvegardes disponibles :	2 copies
Afficher les détails	
Actualiser les informat	ions

# Restauration Windows Server Backup 1/2

On ne peut pas restaurer un DC à une date antérieure à la période de Tombstone

Depuis Windows 2008, il est possible de faire une restauration complète d'un DC en démarrant depuis le DVD d'installation. Vérifier une fois que la restauration est effectuée que tout réplique bien et qu'il n'y a pas d'erreurs dans les logs. Faire un DCDIAG /V /E pour valider le bon fonctionnement de l'annuaire.

Pour faire une restauration autoritaire (restaurer un objet supprimé par exemple), il faut redémarrer en mode « *Restauration des services d'annuaire* ».

http://technet.microsoft.com/en-us/library/cc816878(WS.10).aspx

### Mise en pratique :

Démarrer sur le CD d'installation et cliquer sur « Réparer l'ordinateur ». Restaurer avec la sauvegarde disque.

	<b>2</b> 1	
	vvindows Server 2008	
	Inst <u>a</u> ller maintenant 🗧	
À lire avant d'installer <u>W</u> indov Rénarer Pordinateur		
À lire avant d'installer <u>W</u> indov <u>Réparer l'ordinateur</u>		
À lire avant d'installer <u>W</u> indov <u>Réparer l'ordinateur</u> Copyright © 2009 Microsoft Corporatio		
À lire avant d'installer <u>W</u> indov Réparer tordinateur Cepylight o 2009 Microsoft Corporate	WS an. Taus droits réservés.	
À lire avant d'installer <u>W</u> indov <u>Réparer</u> Copyright & 2009 Microtoft Corporate Options de récupération syst	WS an. Tous droits réservés. <b>Lème</b>	
À lire avant d'installer <u>W</u> indor <u>Réparer</u> l'ordinateur Copyright & 2009 Microsoft Corporate P <b>ytions de récupération syst</b>	WS an. Taus droits réservés. <b>Lème</b>	
À lire avant d'installer <u>W</u> indov <u>Réparer l'ordinateur</u> Copyright © 2009 Microsoft Corporate <b>Options de récupération syst</b> Utiliser des outils qui peuvent de Windows, Sélectionnez le s	ws an. Tous droits réservés. <b>Lème</b> vous aider à résoudre les problèmes r	de déma
À lire avant d'installer <u>W</u> indov Réparer l'ordinateur Copyright 6 2009 Microsoft Corporate <b>Options de récupération syst</b> Utiliser des outils qui peuvent de Windows. Sélectionnez le s	WS on. Tous droits réservés. <b>tème</b> vous aider à résoudre les problèmes ré système d'exploitation à réparer.	de déma
À lire avant d'installer <u>W</u> indor <u>Réparer lordinateur</u> Copyright e 2009 Microsoft Corporate <b>Pptions de récupération syst</b> Utiliser des outils qui peuvent de Windows. Sélectionnez le s Si votre système d'exploitatio et installe les plotes sur vos	ws on. Tous drots réservés. <b>tème</b> vous aider à résoudre les problèmes o système d'exploitation à réparer. In ne s'affiche pas, ciquez sur Charge disques durs.	de déma r des pilo
À lire avant d'installer <u>W</u> indov Réparer fordinateur Copyright saves Microsoft Corporate <b>Ditions de récupération syst</b> Utiliser des outils qui peuvent de Windows. Sélectionnez le s Si votre système d'exploitatio et installez les pilotes sur vos	ws on Tous drots réservés: tème : vous aider à résoudre les problèmes ( système d'exploitation à réparer, in ne s'affiche pas, cliquez sur Charge disques durs,	de déma r des pilo
À lire avant d'installer <u>W</u> indov <u>Réparer</u> l'ordinateur Copyright & 2009 Microtof Corporate <b>Dytions de récupération syst</b> Utiliser des outils qui peuvent de Windows, Sélectionnez le s Si votre système d'exploitatio et installez les pilotes sur vos Système d'exploitation	ws on Tous droits réservés. tème vous aider à résoudre les problèmes s système d'exploitation à réparer. In ne s'affiche pas, cliquez sur Charge disques durs. Taille de la pa Emplacement	de démai r des pilo

Restaurer votre ordinateur avec une image système créée précédemment.

Charger des pilotes

#### Suivant >

#### **Réimager** l'ordinateur

Chercher une image système sur le réseau
 Établit une connexion au réseau pour rechercher l'image

#### Installer un pilote

Rechercher et installer un plote pour un périphérique qu pas dans la liste des images système disponibles.

#### 🛽 Réimager l'ordinateur

Sélectionnez l'emplacement de la sauvegarde pour l'ordinateur que vous voulez rest Si l'image système se trouve sur un périphérique externe, connectez-la à cet ordinateur, puis diquez sur Actualiser.

Si l'image système est sur DVD, insérez le dernier DVD de la sauvegarde de l'image système. Cliquez sur Avancé pour ajouter un emplacement réseau ou installer un pilote pour un périphérique de sauvegarde s'il ne figure pas dans la liste d-dessous.

#### Fuseau horaire actuel : GMT+01:00

[	Emplacement	Image système la plus récente	
	SFR1 2010_06_10 22:49 DISK_01 (F:)	10/06/2010 22:30:06	



#### Sélectionner une sauvegarde d'image système

Cet ordinateur sera restauré à l'aide de l'Image système. Tout ce qui se trouve sur cet ordinateur sera remplacé par les informations incluses dans l'Image système.

#### O Utiliser la dernière image système (recommandé)

Emplacement :	SFR1 2010_06_10 22:49 DISK_01 (F:)
Date et heure :	10/06/2010 22:30:06 (GMT+01:00)
Ordinateur :	SFR1

Sélectionner une image système

### Restauration Windows Server Backup 2/2

#### 🚈 Réimager l'ordinateur X Réimager l'ordinateur X Votre ordinateur sera restauré depuis l'image système Sélectionnez la date et l'heure de l'image système à restaurer suivante : Si plusieurs images système sont disponibles et si vous ne savez pas laquelle /06/2010 22:30:06 (GMT+01:00) restaurer, choisissez la plus récente. Date et heure : 📐 Ordinateur : SFR 1 Lecteurs à restaurer : \\?\Volume{a427cd07-7200-11df-i Sauvegardes disponibles pour SFR1 sur SFR1 2010 06 10 22:49 DISK 01 (F:) Fuseau horaire actuel : GMT+01:00 Date et heure Lecteurs dans la sauvegarde \\?\Volume{a427cd07-7200-11df-a227-806e6f6e6963}, C: 10/06/2010 22:30:06 Réimager l'ordinateur $\times$ \\?\Volume{a427cd07-7200-11df-a227-806e6f6e6963}, C: 10/06/2010 21:58:23 \\?\Volume{a427cd07-7200-11df-a227-806e6f6e6963}, C: 10/06/2010 21:52:33 Tous les disques à restaurer seront formatés et remplacés par la disposition et les données de l'image système. Êtes-vous sûr de vouloir continuer? • Þ Non Réimager l'ordinateur X 🔚 Réimager l'ordinateur X Windows restaure votre ordinateur depuis l'image système. Cette opération peut durer de plusieurs minutes à plusieurs heures. Choisir des options de restauration supplémentaires Restauration du disque (C:)... Formater et repartitionner les disques Sélectionnez cette option pour supprimer toutes les partitions Exclure les disques... Arrêter la restauration existantes et reformater tous les disques sur cet ordinateur afin de correspondre à la disposition de l'image système.

### **TP** : restauration autoritaire

Au redémarrage, appuyer sur F8.

Démarrer en mode « Restauration des services d'annuaire ».

Lancer Windows Server Backup et faire une restauration classique.

Lancer l'utilitaire NTDSUTIL pour marquer les objets qui sont à restaurer de

manière autoritaire (cela incrémente le numéro USN de l'objet).

Appliquer la procédure suivante : <u>http://technet.microsoft.com/en-</u>

us/library/cc816878(WS.10).aspx

Attention aux problèmes d'appartenance des groupes. Préférer utiliser la corbeille Active Directory quand cela est possible.

👰 SFR1 on localhost - Virtual Machine Connection
File Action Media Clipboard View Help
🕸 🔍 💿 💿 💿 🛞 😒
Options de démarrage avancées
Choisissez les options avancées pour : Windows Server 2008 R2 (Utilisez les touches fléchées pour mettre votre choix en surbrillance.)
Réparer l'ordinateur
Mode sans échec Mode sans échec avec prise en charge réseau Invite de commandes en mode sans échec
Inscrire les événements de démarrage dans le journal Activer la vidéo basse résolution (640x480) Dernière configuration valide connue (option avancée) Mode restauration des services d'annuaire

# La corbeille Active Directory 1/3

Avant la corbeille Active Directory, il était déjà possible de récupérer les objets qui étaient en mode Tombstone. Lorsque un objet est supprimé, il passe en mode Tombstone pendant 60 jours ou 180 jours. Il est alors possible de le restaurer. Cependant, lors de la restauration on ne pouvait récupérer que 5 attributs dont le SAMACCOUNTNAME (login pré Windows 2000), le SID et le GUID. Les appartenances aux groupes étaient perdues.

L'activation de la corbeille est irréversible

La forêt doit être en mode natif 2008 R2 pour activer cette fonctionnalité.

La durée de vie pendant laquelle les objets peuvent être restaurés est contrôlés par le paramètre « *msDS-deletedObjectLifetime* ». Ne pas oublier de définir la valeur souhaitée.

http://www.hyperv.fr/blog/2009/04/11/windows-server-2008-r2-et-powershellrestauration-dobjets-active-directory-1273.html

### TP : la corbeille Active Directory 1/2

Vérifier que la forêt est en mode natif 2008 R2 (en PowerShell)

Activer la corbeille Active Directory en tapant la commande suivante (remplacer le nom de domaine, ici *formation10.lan* par le nom de votre domaine) :

Enable-ADOptionalFeature - Identity 'Recycle Bin Feature' – Scope ForestOrConfigurationSet -Target formation10.Lan

Configurer la durée de vie de la corbeille.

Set-ADObject -Identity "CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration, DC=formation10, DC=Lan" -Partition "CN=Configuration, DC=formation10, DC=Lan" -Replace: @{"msDS-DeletedObjectLifeTime" = 365}

Créer un compte utilisateur testsuppr1 et un groupe Testlab2. Ajouter l'utilisateur dans le groupe. Ouvrir une session avec ce compte et personnaliser la session.

Supprimer ce compte utilisateur. Lister les objets supprimés :

Get-ADObject -Filter 'isdeleted -eq \$true -and name -ne "Deleted Objects" -IncludeDeletedObjects -Properties *

*Get-ADObject -filter 'samaccountname -eq « guillaume.mathieu''' – IncludeDeletedObjects* Restaurer l'objet en tapant la commande suivante :

Get-ADObject -filter 'samaccountname -eq "dominique.mathieu"

-IncludeDeletedObjects | Restore-ADObject

http://www.hyperv.fr/blog/2009/04/11/windows-server-2008-r2-et-powershell-restauration-dobjetsactive-directory-1273.html http://blogs.technet.com/b/askds/archive/2009/08/27/the-ad-recycle-bin-understandingimplementing-best-practices-and-troubleshooting.aspx

### TP : la corbeille Active Directory 2/2

_ 0

#### 💹 Administrateur : Module Active Directory pour Windows PowerShell 👘

PS C:\Users\Administrateur> Set-ADForestMode -Identity formation10.Lan -ForestMo de Windows2008Forest

#### Confirmer

Êtes-vous sûr de vouloir effectuer cette action ? Opération « Set » en cours sur la cible « CN-Partitions,CN=Configuration,DC=formation10,DC=lan ». [O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide(la valeur par défaut est « 0 ») : o PS C:\Users\Administrateur> _

PS C:\Users\Administrateur> Enable-ADOptionalFeature -Identity 'Recycle Bin Feat ure' -Scope ForestOrConfigurationSet -Target formation10.lan AVERTISSEMENT : L'activation de « Recycle Bin Feature » sur « CN=Partitions,CN=Configuration,DC=formation10,DC=lan » est une action irréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur « CN=Partitions,CN=Configuration,DC=formation10,DC=lan » si vous continuez.

#### Confirmer

Etes-vous sûr de vouloir effectuer cette action ? Opération « Enable » en cours sur la cible « Recycle Bin Feature ». [O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide(la valeur par défaut est « 0 ») : o Enable-ADOptionalFeature : La méthode spécifiée n'est pas prise en charge Au niveau de ligne : 1 Caractère : 25 + Enable-ADOptionalFeature <<<< -Identity 'Recycle Bin Feature' -Scope ForestO rConfigurationSet -Target formation10.lan + CategoryInfo : NotSpecified: (Recycle Bin Feature:ADOptionalFea ture) [Enable-ADOptionalFeature], ADException + FullyQualifiedErrorId : La méthode spécifiée n'est pas prise en charge,M icrosoft.ActiveDirectory.Management.Commands.EnableADOptionalFeature

PS C:\Users\Administrateur> Enable-ADOptionalFeature -Identity 'Recycle Bin Feat ure' -Scope ForestOrConfigurationSet -Target formation10.lan AVERTISSEMENT : L'activation de « Recycle Bin Feature » sur « CN=Partitions,CN=Configuration,DC=formation10,DC=lan » est une action irréversible ! Vous ne pourrez pas désactiver « Recycle Bin Feature » sur « CN=Partitions,CN=Configuration,DC=formation10,DC=lan » si vous continuez.

#### Confirmer

Êtes-vous sûr de vouloir effectuer cette action ? Opération « Enable » en cours sur la cible « Recycle Bin Feature ». [O] Oui [T] Oui pour tout [N] Non [U] Non pour tout [S] Suspendre [?] Aide(la valeur par défaut est « 0 ») : o PS C:\Users\Administrateur> _

PS C:\Users\Administrateur> Set-ADObject -Identity "CN=Directory Service,CN=Wind ows NT,CN=Services,CN=Configuration,DC=formation10,DC=Lan" -Partition "CN=Config uration,DC=formation10,DC=Lan" -Replace:@{"msDS-DeletedObjectLifeTime" = 365} PS C:\Users\Administrateur> _

# 10. Notions avancées Active Directory :

### Les paramètres avancées

Compléments d'informations sur les paramètres de sécurité Active Directory (quotas...) : <u>http://www.serverwatch.com/tutorials/article.php/3075971/Exploring-Windows-2003-Security-More-Active-Directory-Security-Improvements.htm</u>

Réinitialiser le mot de passe administrateur du domaine depuis le mode Restauration des services d'annuaire :

http://blog.portail-mcse.net/index.php?post/2008/02/27/Reset-du-mot-de-passe-Admin-dudomaine-sous-Windows-Server-2003

Visibilité du champ UserPassword :

http://blog.portail-mcse.net/index.php?post/2009/11/23/I-attribut-UserPassword-en-clear-text

Configuration des paramètres KERBEROS :

Lorsque l'on rencontre des problèmes de désynchronisation horaire sur les stations de travail, il peut être intéressant d'augmenter le paramètre « *Maximum tolerance for computer clock synchronisation* » à plus de 5 minutes.



# Méthodologie dépannage AD 1/2

### Etape 1 : Faire une sauvegarde de l'Etat du Système avant toutes modifications.

Avant d'effectuer la moindre modification, valider qu'il existe une sauvegarde de l'Etat du système pour chaque contrôleur de domaine (au moins un DC par domaine). Valider le bon fonctionnement de la sauvegarde en lançant la console « *Windows Server Backup* ».

### Etape 2 : reproduction du problème :

Reproduire le problème : généralement quand on arrive à reproduire le problème, l'incident à 90% de chance d'être résolu.

### Etape 3 : Vérification préliminaire :

Valider que les services suivants sont démarrés sur tous les DC :

Appel de procédure distante (RPC), Assistance NetBIOS sur TCP/IP, Centre de Distribution de Clés Kerberos, Client DHCP (gère la mise à jour dynamique DNS, Explorateur d'ordinateurs (pour le voisinage réseau), Messagerie Inter-site Netlogon, Registre à distance, Réplication de fichiers (si niveau fonctionnelle domaine < 2008 natif), Réplication DFS (si niveau fonctionnelle domaine > 2003 R2), Serveur DNS, Services de domaine Active Directory, Services Web Active Directory

Désactiver temporairement UAC et le pare Windows.

Vérifier que les stations de travail peuvent communiquer avec les contrôleurs de domaine (ping).

# Méthodologie dépannage AD 2/2

### Etape 4 : Analyse :

Analyser les observateurs d'événements. Filtrer sur les erreurs et les avertissements uniquement dans un premier temps. Attention, de nombreuses erreurs risquent de remonter. Il faut trouver la cause du problème et ne pas se focaliser sur les conséquences.

Validation la configuration DNS (tous les DC ont le même serveur DNS principal).

Valider le bon fonctionnement de la réplication Active Directory (NTDS) et SYSVOL. Pour cela, lancer la console « *Sites et Services Active Directory* » et forcer la réplication. Copier un fichier dans c:\windows\sysvol\sysvol et valider que ce fichier apparaît dans sur tous les DC.

Valider qu'il n'y a pas plus de 5 minutes de décalage horaire entre les différentes machines (DC comme stations de travail).

Lancer les outils de diagnostics DCDIAG, REPADMIN, MPSREPORT, REPLMON...

### **Etape 5 : recherche et validation solution :**

Vous pouvez vous appuyer sur les sites communautaires (<u>www.google.fr/microsoft</u>), les NEWGROUP et la base de connaissance Microsoft (<u>http://support.microsoft.com/search</u>) . Pour plus d'informations, voir l'article « *A la découverte de la communauté Microsoft* » sur <u>http://msreport.free.fr</u>.

Une fois la solution trouvée, il faut monter une maquette pour valider la solution.

Faire une sauvegarde avant toute application de la solution sur l'environnement de production.

### Les observateurs d'événements 1/2

Analyser le contenu des journaux Systèmes, Application, Key Management Service, Réplication DFS (pour SYSVOL et le DFS), Service DNS, Services d'annuaire, Services Web Active Directory.

Configurer les filtres pour n'afficher que les avertissements, les erreurs et les messages critiques.

Quelques erreurs à rechercher : USERENV, NTDS REPLICATION, NETLOGON, SAM, NTDS, DNS-SERVER-SERVICE, DFS-REPLICATION, SCECLI.

De nombreuses erreurs vont remonter. Chercher les causes pas les conséquences. Astuces : Aller sur <u>www.google.fr</u> et taper la source de l'événement et le code d'erreur après (exemple : NETLOGON 5722).

Pour les recherches dans la base de connaissance Microsoft

(<u>http://support.microsoft.com/search</u>, toujours en anglais).

🛃 Observateur d'événements	🛃 Observateur d'événements	
Fichier     Action     Affichage     ?       Image: Construction of the state of t	Fichier       Action       Affichage       ?         Image: State of the stat	Système Nombre d'événements : 4 075
☐       Affichages personnalisés         Rôles de serveurs       Information         ⑦       Événements d'administratio         〕       Journaux Windows         ☐       Application         ☐       Sécurité		Filtré : Journal: System; Niveaux: Critique, Erreur, Avertissement; Source: . Nombre d'événemer         Niveau       Date et heure       Source       ID de       Catégorie de la         Image: Construint of the structure
Installation Information Systè Événk Journaux Abonnem Ouvrir le journal enregistré Créer une vue personnalisée Importer une vue personnalisée Effacer le journal Filtrix le journal actuel	<ul> <li>Durnaux des applications et des services</li> <li>Internet Explorer</li> <li>Key Management Service</li> <li>Microsoft</li> <li>Réplication DFS</li> <li>Serveur DNS</li> <li>Service d'annuaire</li> <li>Services Web Active Directory</li> </ul>	Événement 5722, NETLOGON         Général       Détails         Échec de l'authentification de la configuration de session de l'ordinateur FORMA06. Le nom du compte référencé dans la base de données de la sécurité est FORMA06\$. L'erreur suivante s'est produite :         Accès refusé.

### Les observateurs d'événements 2/2

### Pour afficher les événements de plusieurs journaux, passer par les vues !

🐻 Observateur d'événements	Créer une vue personnalisée 🛛 🗙
Fichier Action Affichage ?	Filtrer       XML         Connecté :       À tout moment         Niveau d'événement :       Image: Critique image: Avertissement image: Commentaires
<ul> <li>Observateur d'événements (Local)</li> <li>Affichages personnalisés         <ul> <li>Rôles de serveurs</li> <li>Événements d'administration</li> <li>Jour</li> <li>Ouvrir le journal enregistré</li> <li>Créer une vue person alisée</li> <li>Importer une vue person alisée</li> <li>Affichage</li> <li>Affichage</li> <li>Affichage</li> <li>Actualiser</li> <li>Aboi</li> </ul> </li> </ul>	Image: Par journal       Journaux d'événements :         Par source       Sources d'événements :         Par source       Sources d'événements :         Inclut/exclut des ID d'événements :       Application         Inclut/exclut des ID d'événements :       Application         Séparant par des virgules. Pour exclure des critères, f       Installation         Par exemple 1,3,5-99,-76       Système         Image: Catégorie de la tâche :       Internet Explorer         Mots clés :       Internet Explorer         Utilisateur : <tous les="" utilisateurs="">         Ordinateur(s) :       <tous les="" ordinateurs="">         Services Web Active Director       Windows PowerShell         Windows PowerShell       Événements matériels</tous></tous>



# Les outils de dépannage 1/3

NTDSUTIL :

- Réinitialisation du mot de passe compte restauration des services d'annuaire.
- Supprimer un contrôleur de domaine ou un domaine.
- Permet de défragmenter l'annuaire.
- Permet de faire une restauration autoritaire.
- Permet de forcer le transfert d'un rôle.
- Permet de créer des SNAPSHOT d'Active Directory (que l'on peut monter en lecture seule).
- Permet de créer des partitions d'application.

DCDIAG /V /E > c:\DCDIAG.TXT :

- Permet de valider la configuration des contrôleurs de domaine de toute la forêt. Attention ce dernier s'appuie sur les noms NETBIOS. Donc il faut pouvoir résoudre tous les contrôleurs de domaine avec leurs noms NETBIOS.
- Faire une recherche sur le mot « Fail » ou « Echec » au niveau du fichier de sortie.

DCPROMO /FORCEREMOVAL :

Permet de forcer la suppression d'un contrôleur de domaine. Ce dernier ne contacte pas les autres DC qui référencent donc toujours le DC. Il faut faire ensuite un NTDSUTIL METADATACLEANUP

### Les outils de dépannage 2/3

DFSDIAG :

Permet de valider le bon fonctionnement de la réplication DFS-R (SYSVOL).

### **REPADMIN:**

- Repadmin /KCC : permet de forcer l'ISTG / KCC a régénérer la topologie de réplication (liens connexions dans la console Sites et Services Active Directory).
- Repadmin /showrepl : permet de valider le bon fonctionnement de la réplication.
- Repadmin /options nom_serveur +Disable_Outbound_REPL
- Repadmin /options nom_serveur +Disable_Inbound_REPL

🙀 Administrateur : C:\Windows\system32	\cmd.exe - ntdsutil
Microsoft Windows Eversion 6.1 Copyright (c) 2009 Microsoft C	.7600] orporation. Tous droits réservés.
C:\Users\administrateur.FORMAT ntdsutil: ?	ION3>ntdsutil
? Activate Instance %s ifique	- Afficher ces informations d'aide - Définissez « NTDS » ou une instance AD LDS spéc
Authoritative restore	comme l'instance active. - Restauration faisant autorité de la base de données NIT
Change Service Account %s1 %s	2 - Changez le compte de service AD DS/AD LDS en nom d'utilisateur xs1 et mot de passe xs2. Itilisez « NULL » pour un mot de passe vide *
20112	otilisez « Nobh » pour un Not de passe vide, *
Configurable Settings DS Behavior	entrer un mot de passe depuis la console. - Gérer les paramètres configurables - Afficher et modifier le comportement AD DS/AD I
DS Files DS	- Gère les fichiers de base de données AD DS/AD I
Group Membership Evaluation ur ou un groupe	- Évaluer des SID dans un jeton pour un utilisate
Help IFM LDAP policies LDAP Port %d	donné - Afficher ces informations d'aide - Création d'un support IPM - Gérer les stratégies de protocole LDAP - Configurez le port LDAP pour une instance AD LI
s. List Instances es	- Répertorie toutes les instances AD LDS installé
Local Roles Metadata cleanup Partition management Popups off Quit Roles Security account management	sur cet ordinateur. - Gestion des rôles RODC locaux - Mettoyer les objets des serveurs désaffectés - Gérer des partitions de répertoire - Désactiver les messages - Activer les messages - Quitter l'utilitaire - Gérer les jetons du propriétaire du rôle NTDS - Gérer les jetons de geomées de comptes de
Semantic database analysis Set DSRM Password	sécurité — nettoyage des SID en double — Vérificateur sénantique — Réinitialise le mot de passe du compte Administrateur du mode Restauration du service d'annuaire
Snapshot SL Port %d	- Gestion des captures instantanées - Configurez le port SSL pour une instance AD LDS
ntdsutil:	

#### c:∖>repadmin ∕showrepl

```
Repadmin : exécution de la commande /showrepl sur le contrôl<u>eur de domaine compl</u>
et localhost
Default-First-Site-Name\DCFORM2
Options DSA : IS_GC
Options de site : (none)
GUID de l'objet DSA : 7bcfcca4-576f-4c82-a883-ca67c10cc68e
ID de l'invocation DSA : df34aaad-b849-4055-96e8-3bb61cecdc91
 DC=formation3,DC=lan
      Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.
CN=Configuration,DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.
CN=Schema,CN=Configuration,DC=formation3,DC=lan
      Default-First-Šite-Name\DCFORM3 via RPC
            GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
            La dernière tentative, le 2010-06-11 13:55:28, a réussi.
DC=DomainDnsZones,DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : Ø8d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.
DC=ForestDnsZones,DC=formation3,DC=lan
Default-First-Site-Name\DCFORM3 via RPC
GUID de l'objet DSA : 08d9a86b-2714-46f5-a4b6-82cf919b4016
La dernière tentative, le 2010-06-11 13:55:28, a réussi.
```

### Les outils de dépannage 3/3

#### 📕 dcdiag.txt - Bloc-notes

Fichier Edition Format Affichage ?

Diagnostic du serveur d'annuaire Ex,cution de l'installation initialeÿ: Tentative de recherche de serveur associ,... * V,rification que l'ordinateur local DCFORM2 est un serveur d'annu Serveur associ,ÿ: DCFORM2 * Connexion au service d'annuaire sur le serveur DCFORM2. * For^t AD identifi,e. Collecting AD specific global data * Collecte des informations sur le site. Calling ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=forr (objectCategory=ntDSSiteSettings),..... The previous call succeeded Iterating through the sites Looking at base site object: CN=NTDS Site Settings, CN=Default-Firs1 Name,CN=Sites,CN=Configuration,DC=formation3,DC=lan Getting ISTG and options for the site * Identification de tous les serveurs. Calling ldap_search_init_page(hld,CN=Sites,CN=Configuration,DC=forr (objectClass=ntDSDsa),...... The previous call succeeded.... The previous call succeeded Iterating through the list of servers Getting information for the server CN=NTDS Settings,CN=DCFORM3,CN=S Name,CN=Sites,CN=Configuration,DC=formation3,DC=lan objectGuid obtained InvocationID obtained dnsHostname obtained 6 site info obtained All the info for the server collected Getting information for the server CN=NTDS Settings,CN=DCFORM2,CN=S Name,CN=Sites,CN=Configuration,DC=formation3,DC=lan objectGuid obtained InvocationID obtained dnsHostname obtained site info obtained All the info for the server collected * Identification de toutes les r,f,rences crois,es NC. * 2 contr"leurs de domaine ont ,t, trouv,s. Test de 2 d'entre eux. Collecte des informations initiálés termín,e.

Attention, en Français il y a un bug avec l'invite de commande quand on redirige une commande vers un fichier de sortie. En fait le fichier est chiffré en UTF8. Il faut donc l'enregistrer dans le bon format.

# Suppression d'un DC et nettoyage AD 1/2

### Pré-requis :

Disposez de 2 DC qui répliquent et qui sont serveur de « Catalogue Global ». Déterminer sur quel DC les rôles FSMO sont installés. Si les rôles sont répartis, les transférer sur un unique contrôleur de domaine.

### Mise en pratique :

Sur le contrôleur de domaine qui dispose de tous les rôles FSMO, taper la commande : *DCPROMO /FORCEREMOVAL.* 

De nombreux messages apparaissent expliquant quels sont les conséquences de la suppression en mode forcée du contrôleur de domaine qui héberge les rôles FSMO / Catalogue global.

Saisir un nouveau mot de passe administrateur local (la base SAM va être recréée).

#### 🔣 Assistant Installation des services de domaine Active Directory 🚽

- 🔔

Ce contrôleur de domaine Active Directory tient actuellement le rôle de maître d'opérations de l'émulateur du contrôleur de domaine principal (PDC). Si vous supprimez les services de domaine Active Directory (AD DS) de cet ordinateur, les opérations réalisées par l'émulateur PDC, telles que les mises à jour des stratégies de groupes et les réinitialisations de mots de passe four les comptes ne faisant pas partie des services de domaine Active Directory, ne fonctionneront pas correctement.

Avant de continuer, transférez le rôle de maître d'émulateur PDC vers un contrôleur de domaine appartenant au même domaine que ce contrôleur de domaine.

Si le transfert est impossible, supprimez d'abord les services de domaine Active Directory de cet ordinateur, puis utilisez Ntdsutil.exe pour prendre le rôle. Ntdsutil.exe s'utilise sur le contrôleur de domaine qui va prendre le rôle ; si possible, utilisez un partenaire de réplication récent appartenant au même site que ce contrôleur de domaine.

Important : le rôle de maître d'émulateur PDC est le seul rôle que vous pouvez prendre avant de supprimer les services de domaine Active Directory. Pour tous les autres rôles de maître d'opérations, vous devez supprimer les services de domaine Active Directory avant de prendre le rôle.

Pour plus d'informations sur le transfert et la prise de rôles de maître d'opérations, voir l'article 255504 de la Base de connaissances Microsoft (http://go.microsoft.com/fwlink/?LinkId=80395).

Voulez-vous poursuivre la suppression des services de domaine Active Directory de cet ordinateur ?
## Suppression d'un DC et nettoyage AD 2/2

🔜 Assistant Installation des services de domaine Active Directory 🚽



Ce contrôleur de domaine Active Directory est un serveur de catalogue global. Si vous supprimez les services de domaine Active Directory (AD DS) de cet ordinateur, les utilisateurs risquent de rencontrer des problèmes lors de la connexion aux domaines de la forêt. Avant de continuer, assurez-vous qu'un nombre suffisant de serveurs de catalogue global se trouve dans cette forêt et dans ce site pour répondre aux connexions des utilisateurs. Si nécessaire, désignez un autre serveur de catalogue global et mettez à jour les clients et les applications avec les nouvelles informations.

Voulez-vous poursuivre la suppression des services de domaine Active Directory de cet ordinateur ?

#### nt Installation des services de domaine Active Directory



Assistant Installation des services de domaine Active Directory

Cet ordinateur est déjà un contrôleur de domaine Active Directory. Vous pouvez utiliser cet Assistant pour désinstaller les services de domaine Active Directory sur ce serveur.



#### \overline Assistant Installation des services de domaine Active Directory

Forcer la suppression des services de domaine Active Directory

Envisagez cette option uniquement après avoir tenté de supprimer normalement les services de domaine Active Directory.

88			122
	-		200
			122
_			
		-	-

#### \overline Assistant Installation des services de domaine Active Directory

Mot de passe Administrateur

Entrez un mot de passe pour le nouveau compte Administrateur sur ce serveur.

Mot de passe :

-	-	-	-	-	-	×
-	-	-	-	-	-	1

Confirmer le mot de passe :

.....

ces derniers de ce contrôleur de domaine, ainsi que de tous les catalogues globaux et données de partitions d'applications. Toutefois, les métadonnées de la forêt ne seront pas mises à jour. Sauf s'il s'agit du

En forçant la suppression des services de domaine Active Directory, vous supprimez

dernier contrôleur de domaine de la forêt, vous devez effectuer un nettoyage manuel des métadonnées.

Par conséquent, essayez de supprimer les services de domaine Active Directory normalement en exécutant l'Assistant Installation des services de domaine Active Directory (dcpromo.exe) sur le contrôleur de domaine, avant de tenter de forcer leur suppression.

Cliquez sur Suivant pour continuer.

En savoir plus sur la procédure de nettoyage des métadonnées

## Suppression d'un DC en mode forcé

A ne faire que si la suppression du contrôleur de domaine échoue !

Toujours faire une sauvegarde de l'annuaire (sauvegarde complète avec Windows Server Backup).

Configurer l'ancien DC en tant que serveur en groupe de travail : Exécution de la commande *DCPROMO /FORCEREMOVAL* 

Ouvrir un invite de commande et lancer l'utilitaire NTDSUTIL. Utiliser l'utilitaire NTDSUTIL pour supprimer les références à l'ancien contrôleur de domaine. Attention une simple suppression du compte ordinateur en suffit pas! Pour cela appliquer l'article Microsoft suivant : http://support.microsoft.com/kb/216498/en-us

Ne pas se tromper au niveau de la partie « *Select Operation target* ». On sélectionne le DC que l'on veut supprimer.

Forcer le transfert des rôles FSMO (avec l'outil NTDSUTIL). Pour cela appliquer l'article Microsoft suivant : <u>http://support.microsoft.com/kb/255504</u>

Procédure à appliquer avec les DC 2012 et versions ultérieures : <u>https://www.petri.com/demoting-a-windows-server-2016-domain-controller</u>

## Les outils de migration / restructuration 1/2

### Migration de ressources entre forêts / fusion de deux forêts en une seule :

Utilisation de l'outil ADMT 3.1 / ADMT 3.2 (pas de prise en charge des annuaires gérés par des contrôleurs de domaine Windows 2000).

Utilisation de l'attribut SID History.

Les ressources sont copiés entre le domaine source et le domaine cible. Commencer par migrer tous les groupes, puis tous les comptes utilisateurs. Migrer ensuite les comptes ordinateurs par lots.

Attention lors de la suppression de l'ancien domaine, les anciens SID ne sont plus résolus. Il faut donc lancer l'assistant translation des SID sur tous les serveurs. Voir outil tiers pour les NAS NETAPP / EMC...

L'agent ADMT exécute un script qui va permettre de changer la machine de domaine et de translater les SID. Lancer l'outil avec un compte utilisateur du domaine source (compte membre du groupe administrateur du domaine source et BUILTIN\Administrateurs dans le domaine cible).

http://msreport.free.fr/?p=131

http://msreport.free.fr/?p=145

## Les outils de migration / restructuration 2/2

### Fusion de deux domaines dans la même forêt :

Outils : Microsoft ADMT (gratuit) ou Quest Migration Manager (payant).

Les ressources sont déplacées avec ADMT. Il faut migrer les groupes (les passer en groupes universelles) puis migrer par les lots les comptes utilisateurs / comptes ordinateurs.

L'agent ADMT exécute un script qui va permettre de changer la machine de domaine et de translater les SID. Lancer l'outil avec un compte utilisateur du domaine source (administrateur du domaine source et BUILTIN\Administrateurs dans le domaine cible).

http://www.microsoft.com/downloads/details.aspx?familyid=6D710919-1BA5-41CA-B2F3-C11BCB4857AF&displaylang=en

### Mise à jour des contrôleurs de domaine :

Utilisation de l'outil ADPREP pour mettre à jour le schéma Active Directory.

Migration par ajout et suppression de contrôleurs de domaine.

http://technet.microsoft.com/en-us/library/cc731728(WS.10).aspx

http://www.petri.co.il/windows-server-2008-adprep.htm

# 11. Les services réseaux :

## Le service DHCP

Permet d'affecter dynamiquement une adresse IP à des stations de travail. Réservation IP : affectation d'une IP à une adresse MAC (utile pour les imprimantes ou les éléments dont l'IP ne doit pas changer).

Le service DHCP de Windows s'interface avec le service DNS. Le serveur DHCP peut mettre à jour les enregistrements DNS dynamiques à la place des stations de travail.

Il est nécessaire d'autoriser le serveur DHCP sur une machine membre / contrôleur d'un domaine (nécessite les droits administrateur de l'entreprise).

Activer la détection des conflits IP (au niveau des propriétés du serveur DNS). Cocher la case « Ignorer les enregistrements A et PTR lorsque le bail est supprimé ».

Pour les problèmes avec les mises à jour dynamiques DNS : voir <u>http://msreport.free.fr/?p=208</u>

### **Quelques problèmes connus :**

Croix rouge au niveau des baux DHCP : <u>http://msreport.free.fr/?p=120</u> Erreurs DCHP 1010 / 1014 : <u>http://msreport.free.fr/?p=95</u> Doublons dans les zones DNS : <u>http://msreport.free.fr/?p=75</u>

## **TP**: le service DHCP

Déconnecter la salle du cours du réseau d'entreprise ou faire sur des machines virtuelles dans un réseau isolé.

Faire ce TP par groupe de 2.

Installer le service DHCP (ajout du rôle depuis le Gestionnaire de Server). Créer une étendue DHCP avec deux adresses (voir formateur) et la configurer pour affecter une adresse de serveurs DNS / Wins / passerelle). Tester le fonctionnement de l'étendue. Que se passe t'il ? Tester les commandes ipconfig /release et ipconfig /renew et ipconfig /all Arrêter tous les serveurs DHCP. Faire un ipconfig /release et un ipconfig /renew. Que se passe t'il ?

Créer une réservation IP.

## Le WINS / LMHOST

Wins : Windows Internet Naming Service

Protocole permettant de résoudre des noms NETBIOS (toto) en adresse IP. Utiliser aujourd'hui encore pour accélérer l'affichage du voisinage réseau.

### Mise en pratique :

Avec le bloc Note, ouvrir le fichier C:\WINDOWS\system32\drivers\etc\ Imhosts.sam. A quoi sert ce fichier ?

Installer le service WINS (Ajout de fonctionnalités dans le Gestionnaire de Server).

Configurer le serveur pour s'enregistrer dans la base WINS (paramètres TCP / IP, paramètres avancées).

Créer un enregistrement www avec comme IP 192.168.0.1. Faire un ping de www puis un nbstat -n puis nbtstat -R. Qu'est ce qu'est le cache Wins.

Configurer votre serveur WINS pour être partenaire de réplication avec un autre serveur WINS.

Renommer le fichier LMHOST.SAM en LMHOST et configurer Windows pour utiliser ce fichier. Créer une entrée dans ce fichier et conclure.

Présenter le fonctionnement du voisinage réseau et exécuter la commande « *Browstat status* ». Qu'est ce qu'un master browser ?

Lire article <a href="http://msreport.free.fr/?p=129">http://msreport.free.fr/?p=129</a>.

# 11. Sécuriser son annuaire Active Directory :

### La sécurité en 2019 : quelques chiffres

- > 280 jours : délais pour détecter une attaque
- > 63 jours : délais pour s'en remettre
- > 20 minutes (Petya) : 2000 machines, 100 serveurs, sauvegarde HS
- > 81 % : les entreprises françaises ciblées par une attaque informatique en 2015.
- **35** % : source de l'incident de sécurité, l'équipe IT
- > 800 000 euros : prix (moyenne) pour s'en remettre

### La méthodologie pour sécuriser son AD



## Faire un état des lieux de la sécurité de son AD

### Avec Ping Castle, c'est gratuit et automatique ! https://www.pingcastle.com/



#### **Risk model**

Stale Objects Privileged accounts Trusts Anomalies nactive user or computer Old trust protocol lackup SID Filtering Certificate take over Network topograph SIDHistory Object configuration rreversible change Golden ticket Privilege control Obsolete OS Trust impermeability Local group vulnerability Old authentication protocol Trust inactive Network sniffing ass-the-credentia Password retrieval Replication Unfinished migration Reconnaissance Vulnerability management Temporary admins Veak password

#### Leaend:

score is 0 - no risk identified but some improvements detected score between 1 and 10 - a few actions have been identified score between 10 and 30 - rules should be looked with attention score higher than 30 - major risks identified

#### Privileged Accounts rule details [3 rules matched]

Presence of Admin accounts which have not the flag "this account is sensitive and cannot be delegated": 1

The native administrator account has been used recently: 0 day(s) ago

#### Check for Native administrator usage

#### Description

The purpose is to verify if the Native Administrator account is used.

#### **Technical explanation:**

The Native Administrator account is the main administrator account, and it is sharing its password with Directory Services Restore Mode password. Since it is the same password, it can be used to take control of the domain even if the account is disabled, notably through a DSync attack. The last login date is retrieved through the LastLogonTimestamp LDAP attribute retrieved from the Active Directory. There is an exception for 35 days to avoid this rule to be triggered at the domain creation.

+ 20 Point(s)

+ 20 Point(s)

#### Advised solution:

To mitigate the security risk, a good practice is to use the Native Administrator account only for emergency, while the daily work is performed through other accounts

It is indeed strongly recommended to not use this account but to use nominative account for administrators and dedicated account for services. Do note that the anomaly will be removed 35 days after the last native administrator login

To track where the administrator account has been used for the last time, we recommend to extract the attribute LastLogon of the administrator account on ALL domain controllers

It can be done with tools such as ADSIEdit or ADExplorer.

Then, for each domain controller, extract the events 4624 at the date matching the LastLogon date. You will identify the computer and the process at the origin of the logon event.

Please note that PingCastle relies on the attribute LastLogonTimestamp to perform this check. The LastLogonTimestamp attribute is replicated but has a latency of a maximum of 14 days, while LastLogon is updated at each logon and is more accurate but not replicated.

#### Points:

20 points if the occurence is strictly lower than 35

#### Documentation:

## Outils pour faire des tests d'intrusion Active Directory

### Principaux outils de tests d'intrusion :

Cain, DSInternal, Metasploit, Mimikatz, PowerSploit, PSEXEC

### Méthodologie d'attaques :

Elévation de privilèges, mouvement latéral, social engineering, altération des fichiers du système.

### Scénario d'attaque :

Je deviens administrateur local de la machine (via une faille de sécurité, en copiant / renommant *CMD.EXE* par *SETHC.EXE* en console de récupération).

Une fois administrateur local, j'escalade en tant que SYSTEM (PSEXEC -i -s cmd).

Une fois *SYSTEM*, je me connecte à la mémoire du processus *LSASS.EXE* de la machine pour des Hash de mots de passe de compte à fort privilège.

Je me connecte via ses comptes à fort privilèges à d'autres machines.

Je fouille la mémoire du processus *LSASS.EXE* d'autres machines jusqu'à devenir *Domain Admins / Enterprise Admins*.

Je me crée un Golden Ticket pour disposer d'une porte dérobée pour rentrer sur l'annuaire AD quand je le souhaite.

### Les actions pour sécuriser son AD

Visionner les vidéos suivantes :

Msreport - durcissement de la sécurité Active Directory - vue d'ensemble <u>https://youtu.be/RoD1w5nQck4</u>

Msreport - les élévations de privilèges Active Directory et comment les détecter https://youtu.be/qHKVQ76lpAU

Lire le guide "*Tester la sécurité de son annuaire Active Directory*". <u>http://msreport.free.fr/articles/Securite-</u> <u>AD/TESTER_SECURITE_ACTIVE_DIRECTORY_V_2.0.pdf</u>