2016

Administration de Windows Server 2012

http://aide.informatique1.fr

44011B – FORMATEUR : MAXENCE VAN JONES

REDATEUR : OLIVIER DEHECQ

Table des matières

http://aide.informatique1.fr

1 A propos de PowerShell

L'utilisation de PowerShell s'avère indispensable dans le cadre de l'administration de Windows Server. Afin de ne pas être perdu avec cet interpréteur de commandes, voici un guide de survie.

Liste des commandes chargées (disponibles) :
```
get-command
```

Liste des commandes relatives à DNS (contenant « DNS ») :
```
get-command *dns*
```

Liste des commandes qui ont un verbe get et un noun (nom) dns :
```
get-command -verb get -noun dns
```

Chercher une commande pour vider le cache :
```
get-command -module DnsServer -noun *cache*
```

Trouver l'aide sur la syntaxe d'une commande :
```
get-help nomDeLaCommande
```

Trouver l'aide de la commande clear-DnsServerCache :
```
get-help clear-DnsServerCache
```

Afficher la date du jour (sous le format : mardi 24 mai 2016 10:09:07)
```
get-date
```

Lister toutes les propriétés contenues dans le pipe « | »
```
get-date | get-member
```

Renvoie le nombre de minutes de la date du jour : 09
```
get-date | select minute
(get-date).minute
```

Exécuter une commande sur un poste distant :
```
invoke-command
```

Prérequis pour `invoke-command` :

- Autoriser l'administration à distance (par défaut sous WS2012+)
- CMD : `winrm qc`
- PowerShell : `enable-psRemoting [-skipNetworkProfileCheck]`
  `-skipnetworkprofilecheck` (WS2012+) : pour le faire aussi sur le profil réseau « Public »

Envoyer un mail depuis PowerShell (PS2+)
```
send-mailmessage
```

Équivalent de `ping`, renvoie true si la machine est allumée, sinon renvoie false (pratique dans un script) :
```
test-connection 192.168.10.2 -count 1 -quiet
```

Lister les rôles installés (available veut dire que les sources sont disponibles dans winSxs :
```
get-windowsFeature
```

Installer une fonctionnalité (en local ou à distance) :
```
install-windowsfeature [-computername leNomdeLordiSurLequelInstaller] featàInstaller
```

Pour passer d'une installation Core à une installation graphique (depuis WS2012) :
```
install-windowsFeature server-gui-mgmt-infra
install-windowsFeature server-gui-shell
```

1.1 L'équivalent de SET en PowerShell

```
si ENV:TOTO "essai"                          définir une variable d'environnement de façon temporaire
gci ENV:Path                                 récupérer le contenu de la variable Path
gci ENV:                                     récupérer l'ensemble des variables d'environnement
setx.exe TOTO "essai" -m                     définir une variable d'environnement de façon définitive
```

Prérequis pour setx : exécuter la commande en tant qu'administrateur

```
setx PATH "$env:path;\the\directory\to\add" -m     ajouter un morceau à la variable place de façon définitive
```

Sources : http://stackoverflow.com/questions/714877/setting-windows-powershell-path-variable

http://aide.informatique1.fr

2 Astuces Windows Server 2012

Ne pas afficher la console gestionnaire de serveur :

- Gestionnaire de serveur > gérer > propriétés > ne pas afficher au démarrage
- Tâche planifiée > Microsoft > server manager > server manager > désactiver

A propos des partitions de disques (dans diskmgmt.msc)

- Partition qui contient le secteur de boot = « système »
- Partition qui contient le système d'exploitation = « démarrage »

Emplacement des sources de Windows :

C:\Windows\winSXS

A propos des réseaux d'entreprise :

Eviter les réseaux en 192.168.0/24 et 192.168.1/24. Ainsi, en cas de VPN le réseau entreprise sera différent de celui de la maison

A propos du bureau à distance vers les VM :

vmconnect : programme dans le répertoire d'hyper-v = permet de se connecter à un serveur puis à une de ses VM sans passer par la console d'hypervision

A propos de DFS en entreprise :

Indiquer le contrôleur de domaine (DC) en racine DFS. Ainsi, le DC stocke le partage au niveau du domaine (en plus de Sysvol et de Netlogon), du coup le partage = **\\domaine\partageDFS**

Ajouter aussi un serveur DFS par site, configuré comme serveur racine du domaine

http://aide.informatique1.fr

3 Windows Deployment Services

WDS permet d'exécuter des installations à partir du réseau afin de les simplifier.

Boot PXE : utilisé pour démarrer la machine sur le réseau. Fonctionnalités installées en même temps que WDS :

- Serveur TFTP
- Dossier partagé
- Référentiel d'image

Prérequis WSD : ADDS / DNS / DHCP / Volume NTFS pour les images

Utiliser WAIK pour créer les fichiers de réponses pour le déploiement automatisé

Au niveau du poste client :

- Paramètres de démarrage (afin de booter sur le réseau
- Pilotes (ceux nécessaires à l'installation = contrôleur réseau + contrôleurs de disques)

Notion de « Postes connus » : adresse MAC ou GUID de la carte mère nécessaire

Mise en place :

1. Installer services de déploiement Windows
2. Aller dans les propriétés du serveur pour peaufiner
3. Configurer DHCP (cas où le rôle DHCP est sur un autre serveur ou installé après WDS)
4. Ajouter les images / les manager (pour y ajouter les mises à jour Windows)
    a. Ajouter une image de démarrage : DVD\sources\boot.wim
        i. Image x64 pour déployer OS x64 (noyau équivalent = os plus ancien que l'os dont on extrait le boot.wim)
        ii. Image x86 pour déployer OS 32 bits (noyau équivalent = os plus ancien que l'os dont on extrait le boot.wim)
    b. Ajouter une image d'installation : DVD\install.wim
5. Créer un fichier Uunatend.xml (pour automatiser le processus de configuration de Windows) puis le lier à un fichier d'installation (par les propriétés = cocher « autoriser l'image à s'installer en mode sans assistance)
6. Transmission par multidiffusion

Sources :

- Prestaging Client Computers : http://technet.microsoft.com/en-us/library/cc770832.aspx
- How to Manage Your Server : http://technet.microsoft.com/en-us/library/cc770637.aspx
- How to Manage Client Computers : http://technet.microsoft.com/en-us/library/cc754289.aspx
- Pour WS2008 : https://araihan.wordpress.com/2009/09/24/deploy-windows-7-using-microsoft-deployment-toolkit-2010-life-is-easy-for-systems-admin/

http://aide.informatique1.fr

4 Configuration et résolution des problèmes DNS

Manipulation commune pour tester une résolution DNS :

```
ipconfig /flushdns
ping x.x.x.x
```

ou

```
nslookup [-serveurDns] ip/nom
```

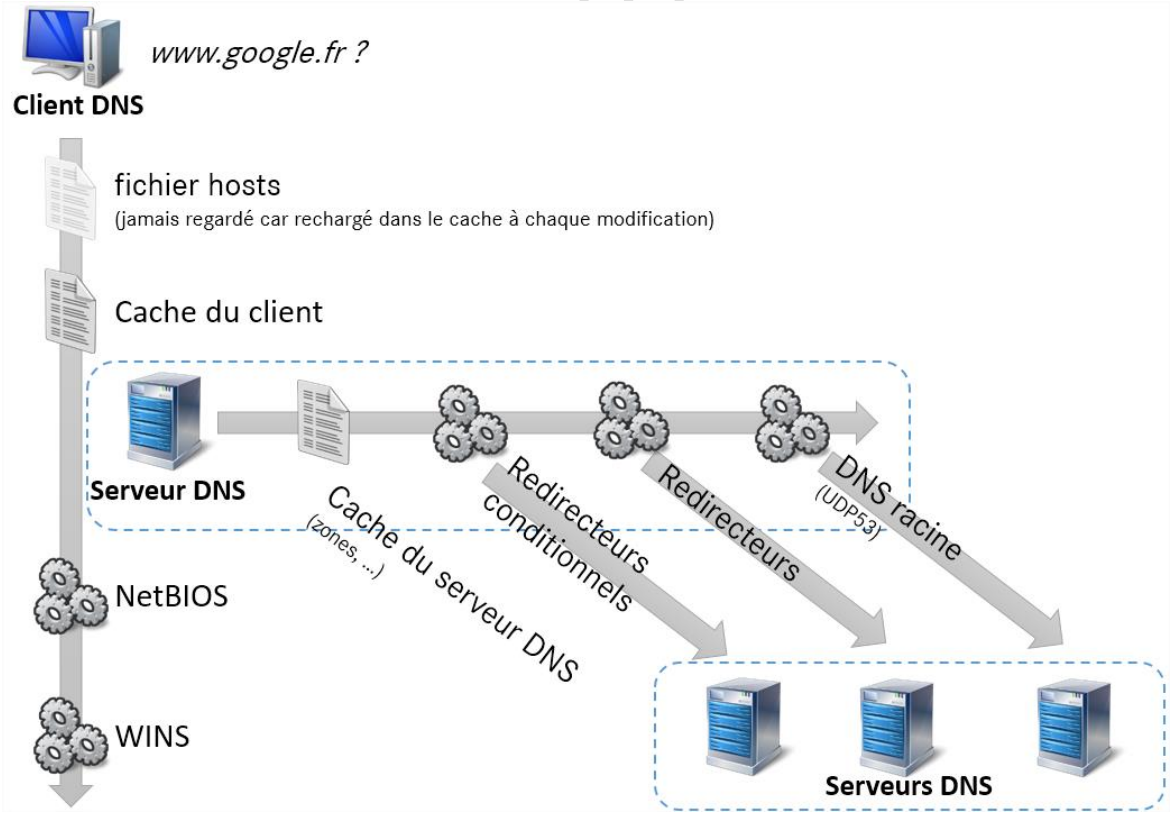
Nota : Eviter .local en nom de domaine interne (.lan ou .priv) car LOCAL est le nom du workgroup de MAC.

Un DNS public contient principalement les enregistrements www et MX des organisations.

Séparation des domaines LAN et WAN d'une organisation :

- Nom de domaine identique (LAN = societe.com ; WAN = societe.com) = split DNS / facilite l'authentification mais attention à ce qui est contenu sur le DNS public
- Nom de domaine unique (LAN = societe.lan ; WAN = societe.com) : préféré, facile à gérer, rajouter les deux domaine dans la conf ip
- Sous-domaine (LAN = interne.societe.com ; WAN = societe.com) = synchroniser la partie societe.com mais pas la partie interne.societe.com

Configuration des redirecteurs : indiquer le serveur DNS du FAI (à minima). Si pas de DNS FAI, c'est le serveur DNS qui interrogera les racines, etc. etc. jusqu'à trouver l'IP du FQDN.



Processus de résolution de nom

Si le DNS ne connait pas le chemin complet (récursif) : demande le chemin complet (récursif) au redirecteur (exemple = DNS FAI). Le redirecteur FAI interrogera par demandes incomplètes (itératives) le DNS racine.

- Itératif : demande une partie du nom. Demande l'adresse IP du DNS de la sous-zone ou l'adresse IP du FQDN (exemple de FQDN : pc1.ouest.societe.com)
- Récursif : demande tout (adresse IP du FQDN) ou rien

Fichier .dns - enregistrement des services Windows :

RessourceWindows	600	SRV	priorite	poids	port	fqdn
_gc.tcp....	600	SRV	0	100	3268	lon-dc1.adatum.com
_ldap					389	

Best practice :

- Autoriser les transferts de zone uniquement vers les serveurs listés / suivants (pour ajouter de la sécurité)

Nota : transfert de zone = TCP53 / résolution de nom = UDP53

Pour migrer des adresses IP de serveurs :

- Vider le cache des serveurs DNS
  - Console dns > sur le serveur : clic droit > vider le cache
  - `clear-DnsServerCache` (en powershell)
- Modifier le TTL pour qu'il soit faible (afin de forcer la recherche DNS sur le serveur principal)

Pour afficher les adresses mises en cache :

  - Console DNS > affichage > affichage détaillé
  - « Recherches mises en cache »

Intérêt de la zone de stub : permet d'avoir les adresse IP des DNS (+ redirecteur) mais dynamique si @IP serveur DNS (du partenaire par exemple) est modifiée

`ipconfig /registerdns` : force le client à s'enregistrer sur DNS (A/AAAA et PTR)

important : répliquer tous les contrôleurs de domaine : `repadmim /syncall`

Types de requêtes de transfert de zones entre les serveurs DNS :

- AXFR = transfert intégral
- IXFR = transfert incrémental

Sécurité de zones :

- Le transfert de zones passe en clair par défaut (le chiffrer) :
  - Configurer DNS-sec (via mmc DNS par une clé partagée entre les serveurs)
- Restreindre le transfert de zone à des serveurs spécifiés
- Envisager d'utiliser des zones intégrées AD (l'AD étant sécurisé)

Activer le nettoyage des enregistrements obsolètes non manuels (pas activé par défaut) :

  - Mmc DNS > serveur > propriétés > onglet avancé > cocher nettoyage
  - Mmc DNS > zone > propriétés > général > vieillissement

http://aide.informatique1.fr

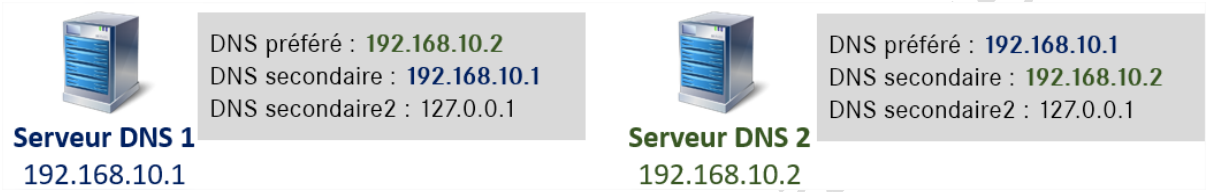
Tester la configuration du DNS avec nslookup

```
nslookup
> www.google.fr                    résolution de nom
> set type=MX                      ne donnera que les enregistrements de type MX
> google.com                       le domaine dont on veut les champs MX
> server=x.x.x.x                   interrogera le serveur dns sélectionné
> set type=all                     pour chercher tous les types d'enregistrements
>
```

Journaux et analyses

Journaux d'événements DNS / applications Windows / gestionnaire de services > DNS > Best Practice Analyzer

Configuration d'un serveur DNS



Configuration par défaut des DNS préférés et secondaires sur les serveurs DNS

Autres outils de de diagnostic DNS :

- netsh
- Microsoft© Network-Monitor : équivalent de Wireshark

http://aide.informatique1.fr

5 ADDS

Vue d'ensemble :

Composants physiques :

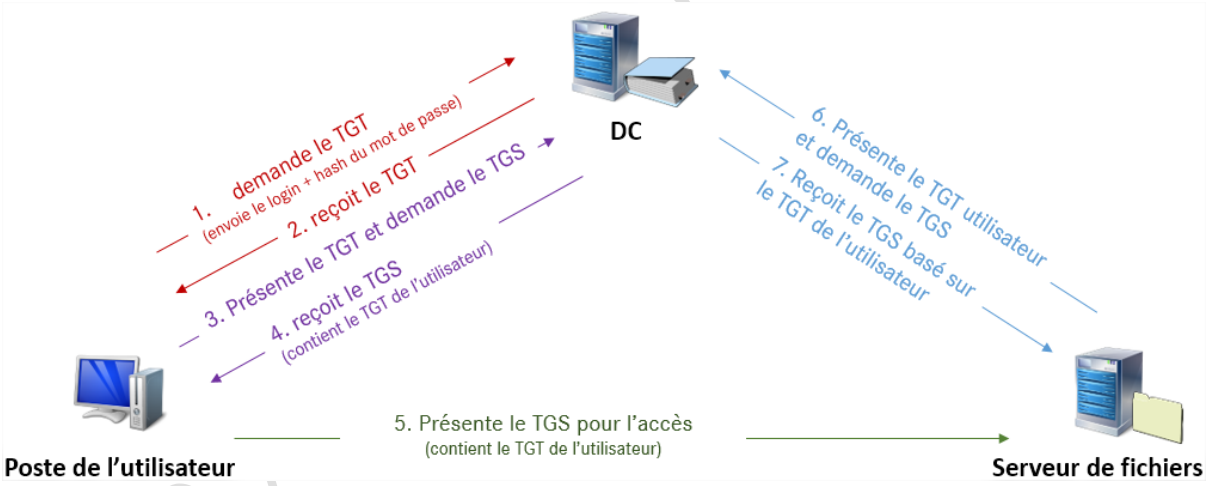
- Magasin de données (ntds.dit)
- Contrôleur de domaine
- Serveur de catalogue global
- Contrôleur de domaine en lecture seule

Composants logiques :

- Partitions : schema (F), conf (F), domaine (D), DNSForestZone (F), DNSDomainZone (D), [applications...] (F = réplique au sein de la forêt / D = réplique au sein du domaine)
  - Schéma : adsi edit (réplique niveau foret)
  - Configuration
- Schéma
- Domaines
- Arborescence de domaine
- Forêts
- Sites (rattachés aux sous-réseaux)
- Unités d'organisation

Au sein de la forêt : relation bidirectionnelle transitive

Si une « relation d'approbation de forêt » lie 2 forêts, dans ce cas il y a relation bidirectionnelle transitive entre tous les domaines des deux forets.



Fonctionnement de l'accès à des ressources dans un domaine

- TGT : SIDuser, SIDgroup1, SIDgroup2, etc.
- TGS : ticket d'accès

Nota : maître infrastructure : pas sur le même serveur que le GC. Sinon on a des sidxxxxxx quand on supprime un compte (car c'est le maître infra qui fait le ménage)

Contrôleurs de domaine virtualisés

WS2012 : clonage sûr / restauration sure depuis un snapshot

Ne pas mettre 2 DC sur un seul hôte physique car cela ne sert à rien si l'hôte tombe

http://aide.informatique1.fr

RODC :

Un RODC est un contrôleur de domaine en lecture seule.

Un RODC ne peut pas authentifier d'utilisateur ni de machine (ne contient pas de hachage de mot de passe = aucun secret). Sinon il faut mettre les utilisateurs ET ordinateurs dans un groupe spécial qui exporte les mots de passe vers le RODC.

Nota : Problème de « relation d'approbation » est causé par un compte machine qui a un mauvais mot de passe :

- Réinitialiser le compte ordinateur puis
- `test-ComputerSecureChannel -repair` (pour réparer la relation d'approbation)

Gestion de l'ADDS

- WS2008R2+ : outils d'administration > centre d'administration active directory
- Utilisateurs & ordinateurs active directory
- Domaines et approbations active directory : relations d'approbation
- Sites & services active directory : catalogues globaux & replication AD inter-sites
- Modification ADSI : modification des partitions
- Activer la gestion du schéma : `regsvr32 schmmgmt.dll` puis mmc.exe > schéma AD

`get-command -module ActiveDirectory | measure` permet de compter le nombre de commandes liées à ADDS

Les rôles FSMO :

- Contrôleur de schéma (1/F) : peut modifier le schéma
- Maître d'attribution des noms de domaine (1/F) : peut ajouter des domaines et DC
- Maître RID (1/D) : peut ajouter des RID (le RID est le nombre à la fin d'un SID)
- Maître d'infrastructure (1/D) : peut vérifier/valider les relations d'approbation, peut faire le ménage dans les SID orphelins. Ne doit pas être sur un CG ou sinon tous les DC doivent être catalogue global
- Émulateur PDC (1/D) : peut faire office de PDC dans le cas du mode mixte (compatibilité NT4), gère le serveur de temps (met à jour l'heure dans le domaine, dans la limite de 5 minutes de décalage), décide des mises à jour urgentes ou pas (verrouillage de compte, etc.)

Les maitres de rôles sont modifiables par `ntdsutil transfer` (si l'actuel est allumé) / `ntdsutil seize` (si l'actuel est éteint)

Le service « Services de domaine Active Directory » :

- À l'arrêt = transforme en membre de l'ADDS jusqu'au redémarrage
- Démarré = contrôleur de domaine
- DSRM = mode de restauration

L'outil ntdsutil :

`ntdsutil` permet :

- sauvegarde / restauration
- snapshot pour monter un AD temporaire pour tester

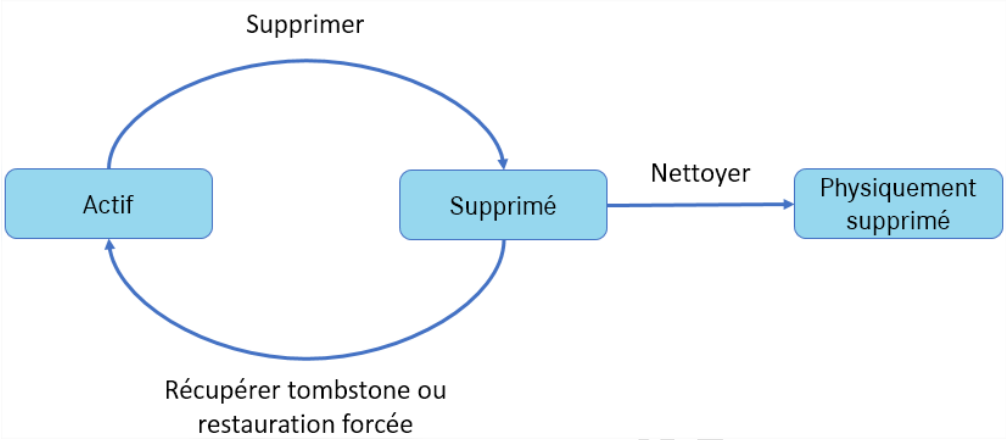
```
ntdslutil > activate instance ntds                    active l'instance NTDS (instance par défaut)
.>ifm> create sysvol full c:\temp                     créé un backup IFM dans C:\temp\ pour transfert
.>list instance                                       liste les instance ADDS
.> files                                              pour copier/déplacer les instances
.> metadata cleanup                                   nettoyer les entrées des serveurs morts
.> roles                                              lister/déplacer les roles fsmo
```

http://aide.informatique1.fr

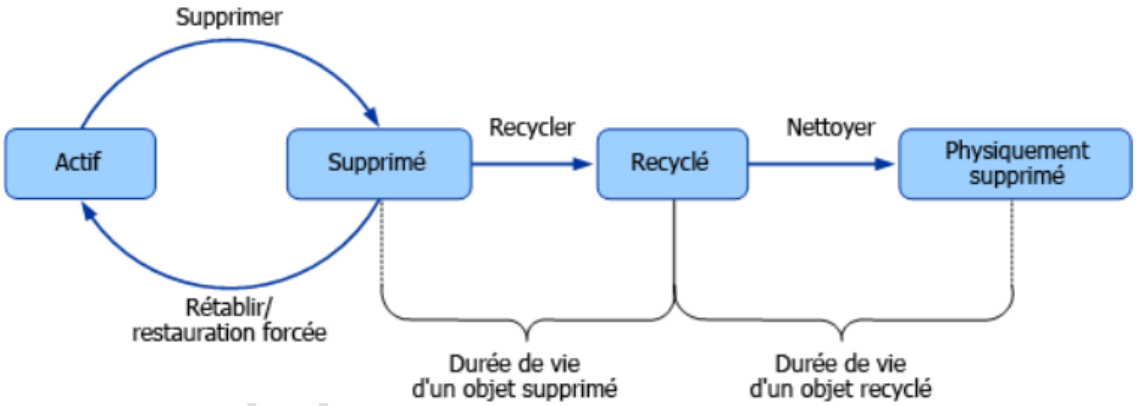
Faire une copie de test d'une instance AD :

1. Faire un snapshot de l'AD via ntdsutil
2. Monter la nouvelle instance via ntdsutil
3. Exposer l'instance via U&OAD > changer de domaine : FQDN:port
    - Si on indique le port 389 (port par défaut), c'est l'instance par défaut qui est montée
    - Si on indique le port donné à la nouvelle instance (via l'étape 2), c'est cette instance qui est montée (cela ne démonte pas l'instance actuelle, cela permet juste de la gérer)

Fonctionnement de la suppression d'objets dans l'AD :



Fonctionnement sans la corbeille Active Directory



Fonctionnement avec la corbeille Active Directory

Nota : adrestore de sysinternal est un outil pour restaurer des objets supprimés

Pour activer la corbeille Active Directory :

```
Enable-ADOptionalFeature -Identity 'CN=Recycle Bin Feature,CN=Optional
Features,CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
DC=contoso,DC=com' -Scope ForestOrConfigurationSet -Target 'contoso.com'
```

6 Gestion des comptes d'utilisateurs et de service

6.1 Utilisation de ldifde et csvde

CSVDE

Format CSV avec entête (`csvde -f` = export / `csvde -i` = import)

```
csvde -f nomDeFichier [-d aPartirDe] [-p [base]|OneLevel|sous-arborescence] [-r
filtre] [-l attributsAImporterOuExporter]
```

Astuce : indiquer l'extension .txt en fichier, ensuite ouvrir Excel puis « ouvrir fichier » sélectionner le fichier .txt. Dans ce cas Excel demandera de lui-même les séparateurs de champs. Sinon Excel a du mal à gérer les fichiers .csv

`csvde -i nomDeFichier [-k]` `-k` : continuer malgré les erreur (exemple : l'objet existe déjà)

LDIFDE

```
ldifde [-i] [-f nomDeFichier] [-k]
```

`-i` : importer (si rien n'est indiqué = exporte par défaut)

`-k` : continuer malgré les erreurs

Nota non officiel : pour récupérer les mots de passe, il faut être loggé en SYSTEM

Exporter les utilisateurs en csv par PowerShell :

```
get-aduser -filter * | convertTo-Csv -delimiter "`t" | out-file c:\temp\toto.csv [-
append]
get-aduser -filter * | convertTo-Csv -delimiter "`t" > c:\temp\toto.csv
get-aduser -filter * | export-Csv -delimiter "`t" -path c:\temp\toto.csv
```

Importer les utilisateurs en csv :

```
get-content -path c:\temp\toto.csv | convertFrom-csv -delimiter "`t" | new-aduser
```

`new-aduser` (ramène les infos) `| set-aduser` [`get-credential as plaintext` (génère le hash du mdp)]

6.2 Configuration des paramètres des mots de passe :

Pour définir la stratégie de mot de passe sur le domaine : GPO « DefaultDomainPolicy »

- Cette GPO ne devrait servir qu'à configurer la stratégie de mot de passe du domaine
- Complexité de mot de passe : majuscules, minuscules, chiffres, caractères spéciaux (au moins 3 sur les 4)

Outils :

- Stratégie de sécurité LOCALE : secpol.msc
- Stratégie de sécurité AD : gpmc.msc

Stratégies de mots de passe affinées (PSO) :

Pour faire des différences entre les utilisateurs. Mettre les utilisateurs dans des groupes de sécurité globaux. Ces stratégies sont liées à des groupes de sécurité globaux (pas sur une OU, pas sur des groupes de Domaine Local)

- Si plusieurs stratégies concernent un utilisateur, le poids le plus faible gagne
- `new-adFineGrainedPasswordPolicy`
- `add-adFineGrainedPasswordPolicy`

http://aide.informatique1.fr

6.3 Configuration des comptes de service (MSA)

Comptes de services : depuis WS2008R2+ (WS2008R2 : en ligne de commande)

Prérequis pour un compte de service géré :

- NF de domaine 2008R2+ (ou `prepareshema` sur un des serveurs 2008R2 + passerelle web pour AD : permet de ne pas modifier le niveau fonctionnel de domaine)
- Au moins un DC en WS2008R2+ (ou en PDC et CG si `prepareshema`)
- .net Framework 3.5.x (l'ajouter si WS2012+)
- Module active directory pour Windows PowerShell (>= PowerShell 3)
    - Management Network v3+ (pour ws2008R2)

Deux types de comptes de service :

- Compte de service géré : fonctionne seulement sur une seule machine
- Compte de service géré du groupe : fonctionne sur plusieurs machines
    - **MAIS NECESSITE AU MOINS UN DC EN WS2012 (en plus des autres prérequis)**

Ajouter un compte de service :

Dans la fenêtre « Module Active Directory pour Windows PowerShell » :

```
Add-KdsRootKey -effectiveTime ((get-date).addHours(-10))                    créer certificat

New-ADServiceAccount -name NomMSA -DNSHostname HostnameduDC -
PrincipalsAllowedToRetrieveManagedPassword LON-DC1$                         créer un compte de service

Add-ADComputerServiceAccount -identity HostnameHote -serviceAccount NomMSA
                                        lier un service à un ordinateur (à faire sur l'ordinateur qui doit être lié)

Get-ADServiceAccount -filter *                                              lister tous les comptes de service

Install-ADServiceAccount -identity NomMSA
```

http://aide.informatique1.fr

7 Gestion des stratégies de groupe

Mise à jour d'applications (seulement celles qui ont été installées par GPO)

Redirection des dossiers (bureau + mes documents au moins pour les portables)

Lier des GPO à des groupes de sécurité **globaux** ou des comptes utilisateurs ou des comptes machine

Mise à jour des GPO :

- Ordinateur à l'allumage ordinateurs
- Utilisateur à l'ouverture de session
- Vérification et mise à jour toutes les 90 à 120 minutes sur les clients
- Vérification et mise à jour toutes les 5 minutes sur les contrôleurs de domaine
- Le service CSE est utilisé pour appliquer les GPO

Astuces diverses :

Tester les GPO (et sauvegarder la version n-1) avant de mettre en place

Lier une GPO à un site : utile pour mapper les imprimantes propres au sites

Publier une appli : visible pour installation dans ajout/suppression de programme (ou bien installable en cliquant sur un fichier lié à l'appli (exemple : document .docx)

Fermeture de session : vider le cache IE, vider le dossier temp

On ne peut pas configurer la stratégie de mot de passe dans les GPO hors DefaultDomainPolicy (les GPO DefaultDomainPolicy et DefaultDomainControlerPolicy ne doivent pas être modifiées sauf pour la stratégie de mot de passe du domaine)

Liste non exhaustive du détail des possibilités

Emplacement dans l'éditeur de GPO	Permet de
Ordi > strat > param.secu > strat locales > strat audit	Pour faire de l'audit simple
Ordi > strat > param.secu > journal d'évènement	Gestion des journaux Windows
Ordi > strat > param.secu > groupes restreints	Pour ajouter un user admin local des postes
Ordi > strat > param.secu > services système	Pour activer/désactiver des services en auto
Ordi > strat > param.secu > pare-feu	Pour configurer le serveur (possibilité d'exporter/importer des règles faites depuis le panneau de config/pare-feu)
Ordi > strat > param.secu > strat de rso sans fil	Ajouter les wifi entreprise
Ordi > strat > param.secu > strat de clé publique	Pour ajouter un certificat auto
Ordi > strat > param.secu > config avancée audit	Pour faire de l'audit affiné
Ordi > strat > modèle admin >	Plein de choses

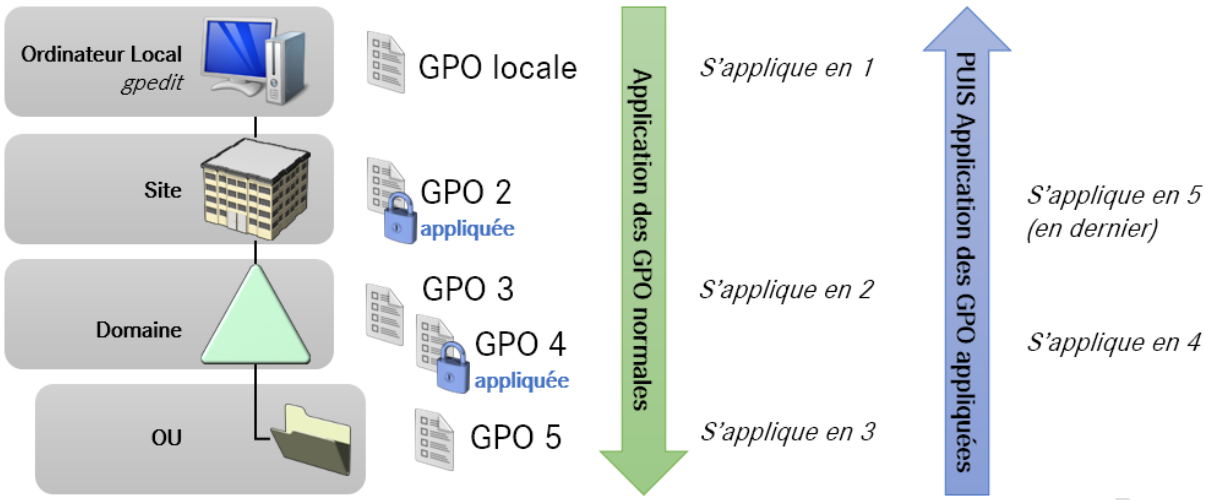
Important :

- Ordi > strat > : non modifiable (grisé coté interface)
  - L'utilisateur ne peut donc pas modifier les paramètres de lui-même
- Ordi > préférence > : modifiable côté interface
  - L'utilisateur peut donc modifier les paramètres de lui-même

Commandes PowerShell :

- `new-gpo` : créer une GPO
- `import-gpo` : importer une GPO
- `get-command *GPO*`

http://aide.informatique1.fr



Ordre d'application des GPO – avec des GPO « appliquées / enforced »

Ordre d'application : "GPO normales" du haut vers le bas PUIS "GPO appliquée" du bas vers le haut

Filtres WMI (outil Wmi Explorer, gratuit) exemples :

- https://msdn.microsoft.com/fr-fr/library/jj717288(v=ws.11).aspx
- https://technet.microsoft.com/fr-fr/library/cc754488(v=ws.10).aspx

Traitement par boucle de rappel :

Objectif : forcer la partie Utilisateur d'une GPO à s'appliquer pour des ordinateurs (pratique pour les serveurs TS / Citrix)

1. Créer une OU nommée « RDS » et y mettre les comptes ordinateurs : RDS1, RDS2 …
2. Créer une GPO dont la partie Utilisateur doit s'appliquer pour les objets Ordinateur
3. La lier à l'OU « RDS »
4. Activer le traitement par boucle de rappel : la GPO Utilisateur s'applique pour les objets Ordinateurs

Conf ordi > strat >modele admin > composants windows > système > stratégie de groupe > configurer le mode de traitement par boucle de rappel

Pour activer la GPO on peut soit « **fusionner** » soit « **remplacer** » :

- **Bouclage avec remplacement.** Dans ce cas, la liste des objets de stratégie de groupe de l'utilisateur est entièrement remplacée par la liste des objets de stratégie de groupe déjà établie au démarrage de l'ordinateur (à l'étape 2 de la section Traitement et priorité de la stratégie de groupe). Les paramètres Configuration utilisateur de cette liste sont appliqués à l'utilisateur.
- **Bouclage avec fusion.** Dans le cas d'un **Bouclage avec fusion**, la liste des objets de stratégie de groupe est une concaténation. La liste par défaut des objets de stratégie de groupe de l'objet utilisateur est obtenue comme normalement, mais ensuite la liste des objets de stratégie de groupe de l'ordinateur (obtenue au démarrage de l'ordinateur) y est ajoutée. Comme les objets de stratégie de groupe de l'ordinateur sont traités après ceux de l'utilisateur, ils sont prioritaires en cas de conflit de paramètres.

Dépannage de l'application des GPO :

1. Réplication des objets de GPO sur les DC du domaine
2. Forcer l'application des GPO sur le poste client `invoke-gpupdate` = `gpupdate /force`
3. Ouverture de session / redémarrage de l'ordinateur (ou WS2012+ : clic droit sur l'OU > mise à jour de la stratégie de groupe)
4. Vérifier le jeu de stratégie résultant : RSOP ou `gpresult -R`
5. Vérifier le journal des GPO : Journaux évènement > journaux et applications > Microsoft > Windows > Group Policy

http://aide.informatique1.fr

8 Gestion des bureaux des utilisateurs avec la stratégie de groupe

Modèles d'administration utilisés :

- GPO > conf ordinateur > strat > modèles d'admin
- GPO > conf utilisateur > strat > modèles d'admin (dont bureau et menu démarrer)

Gestion par des fichiers ADMX (fonctionne avec un fichier de langue ADML) : permet de gérer les programmes tiers avec des GPO. Exemples : Microsoft Office 2016, Google Chrome, Adobe Reader DC, etc.

Redirection des dossiers (vers un emplacement réseau) : Rediriger « documents » redirige aussi par défaut les répertoires suivants : *bureau, accueil, documents, images, appdata\roaming, contacts, téléchargements, favoris, parties enregistrées, recherches, liens, musique et videos*. Il est donc utile de faire de la granularité car rediriger le répertoire *Téléchargements* peut être consommateur d'espace disque inutilement. Il est cependant recommandé de le faire pour les postes nomades.

Autorisations NTFS du dossier racine des profils des utilisateurs :

- Administrateur (aucun)
- Groupe des utilisateurs qui sauvegardent des données sur le partage : (RW)
- Système local (CT)

Partage du dossier racine des profils des utilisateurs :

- Groupe des utilisateurs qui sauvegardent des données sur le partage : (CT)

Autorisations NTFS pour le dossier redirigé de chaque utilisateur :

- %username% (CT + propriétaire)
- Administrateurs (aucun)
- Système (CT)

Nota utile :

Pour transformer un .exe en .msi (afin de le déployer par GPO) : Wise LE ou InstallShield Studio

http://aide.informatique1.fr

9 Configuration et résolution des problèmes d'accès à distance

VPN par défaut : port 500 (VPN IPSec) et 4500 (IPSec over NAT-T)

Nota : Direct access : disponible dans les version entreprise (pas dans les version pro)

Nota2 : préférer d'autres solutions telles que OpenVPN patché, etc.

Configuration des réseaux dans le cadre d'utilisation de VPN

- DMZ : Serveur VPN
- LAN : Serveur NPS (Radius), NAP, Autorité HRA, DHCP, ADDS, PKI ...
- Réseau Restreint : Serveur de mise à jour (pour NAP/HRA)

Stratégies d'accès réseau (NAP/NPS) :

- Contrôle d'intégrité
- Sécurisation SansFil et cablé
- Gestion de la stratégie réseau

Serveur RAS :

- Routage, natage (entrée/sortie), directAccess

Authentification VS Autorisation

- Authentification se fait en 1er
- Autorisation, une fois que l'authentification est autorisée, vérifie l'accès

Protocoles d'authentification :

- ~~PAP : pourri (login & mdp en clair)~~
- ~~CHAP : pourri (hachage MD5)~~
- MS-CHAPv2 : le minimum (authentification bidirectionnelle)
- EAP le top (très sécurisé avec clés temporaires, biométrique ...)

Les PKI (Infrastructure de clés publiques = certificats) :

AIA / CPD : point de récupération des informations sur les autorités de certifications

aide.informatique1.fr

Intégration de DHCP au service routage et accès distant :

- Un pool statique créé sur le serveur de routage et accès à distance
- Un serveur DHCP
- Les serveur DHCP exécutant WS2012 :
    - Fournissent une classe d'utilisateur appelée "classe de routage et d'accès distant par défaut"
    - Pour affecter des options fournies uniquement aux client de routage et d'accès à distance

Configuration de l'accès VPN (IP Sec, PPTP, L2TP = PPTP L2F, SSTP = VPN SSL = DirectAccess, IKEv2)

En **IKEv2** : permet le multibornes sans perdre la connexion VPN (permet le changement d'adresse IP à la volée) = Roaming

Atelier WS2012 config VPN :

Prérequis : 2 interfaces RSO (Une dans le WAN, une dans le LAN)

Rôle accès à distance

- Console "Serveur NPS"
- Console "Routage et accès distant"

1. Membre du domaine
2. Console NPS > inscrire dans Active Directory
3. Console Routage et accès à distance (si modification de l'adresse réseau : reconfigurer RAS)
    a. Configurer VPN & accès à distance
    b. VPN et Accès à distance
    c. Configurer VPN avec une plage d'adresse DHCP pour les clients
4. Console NPS > ajouter les stratégies réseau

Pour pouvoir être connecté :

- Stratégie d'accès réseau (accès à distance)
- Stratégie de connexion (NPS)

Installer le kit CMAK RAS sur le client (fonctionnalité de Windows)

- Le chercher dans les outils d'administration
- Permet de créer des installeurs de profils de connexions VPN personnalisés à déployer ou à fournir au client

http://aide.informatique1.fr

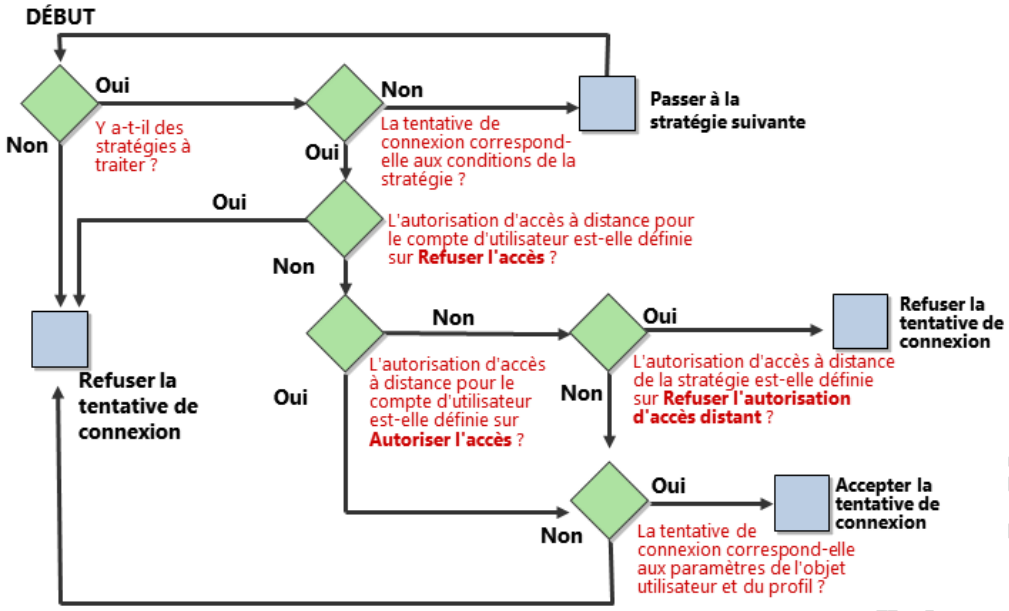


Diagramme de traitement des stratégies dans NPS

Activer les traces :

```
netsh ras diagnostics set rastracing * enabled
```

ou regedit.exe puis HKLM\Software\Microsoft\Tracing\

Configuration de DirectAccess :

- Coté poste client, il faut au moins une Edition Enterprise (contrat OpenSA, la licence OEM fournie ne sert à rien ou alors <90jours pour appeler le service licences de M$ pour transfert une licence pro en EE)
- Les flux réseaux ne doivent pas être analysés en sortie ou en entrée (tester en entrée : demander le certificat d'un site https et vérifier que c'est SON certificat qui apparait, sinon il y a man in the middle)
- Pare-feu : Attention aux ports : 1723 pour L2TP ...
- Direct Access est transparent : essaye de se connecter au réseau dès qu'il y a un accès internet
- Besoin d'une PKI, d'un serveur DirectAccess, de NLS, de IPv6 (ou de 6to4)

http://aide.informatique1.fr

10 Installation, configuration et résolution des problèmes du rôle de serveur NPS

Serveur NPS WS2012 (fourni dans les rôles d'accès distant) permet :

- Serveur RADIUS
- Proxy RADIUS
- Serveur de stratégie NAP

Outils de gestion/configuration :

- Mmc "Serveur NPS"
- `Netsh` (pour NPS, RADIUS, stratégies, groupes de serveurs RADIUS distants, stratégie réseau, NAP, comptes)
- PowerShell

Proxy Radius (peut être un switch 802.1x) :

- Sous traite les services accès distant / VPN / sans fil
- Authentifie et autorise les comptes utilisateurs

Stratégie de demande de connexion :

- Permet des conditions (trames, services, tunnel, heures/jour de restriction)
- Permet des paramètres (type d'authentification, gestion de compte, manipulation d'attributs, paramètres avancés)

Ports par défaut :

- UDP 1812/1645 (entrée standard / sortie sécurisée)
- UDP 1813/1646 (sortie standard / sortie sécurisée)

Méthodes d'authentification NPS :

- Méthode d'authentification par mot de passe : CHAP / MS-CHAPv2 / PAP / non authentifié
- Certificat : besoin de PKI, mettre une clé d'au moins 2048. Remplace l'auth par mdp. Sont acceptés les certificats de type :
    - Autorité de certification (ajouter la confiance par GPO)
    - Certificat ordinateur et/ou certificat utilisateur (sur les clients)
    - Certificat de serveur (sur le(s) NPS + sur les clients)
- Déploiement de certificats pour authentifier (PEAP et EAP) :
    - Inscription + récupération certificats via GPO (client en domaine et en LAN)
    - Inscription de l'autorité via le web + récupération certificats (clients hors domaine mais dans le LAN)
    - Ajouter certificats utilisateur/ordinateur via support amovible (clients hors domaine et hors LAN)
- Journalisation

http://aide.informatique1.fr

11 NAP

Les version XPsp2 et antérieures ne sont pas restrictibles (avant le pare-feu Windows intégré/centre de sécurité)

Méthode	Points clés
Contrainte de mise en conformité IPsec pour les communications protégées par IPsec	• L'ordinateur doit être conforme pour pouvoir communiquer avec d'autres ordinateurs conformes • Il s'agit du type de contrainte de mise en conformité NAP le plus puissant, qui peut être appliqué en fonction d'une adresse IP ou d'un numéro de port de protocole
Contrainte de mise en conformité 802.1X pour les connexions câblées ou sans fil authentifiées par le protocole IEEE 802.1X	• L'ordinateur doit être conforme pour pouvoir obtenir un accès illimité via une connexion 802.1X (commutateur d'authentification ou point d'accès)
Contrainte de mise en conformité VPN pour les connexions d'accès à distance	• L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité via une connexion de service d'accès à distance
DirectAccess	• L'ordinateur doit être conforme pour pouvoir obtenir un accès réseau illimité • Pour les ordinateurs non conformes, l'accès est restreint à un groupe défini de serveurs d'infrastructure
Contrainte de mise en conformité par DHCP pour la configuration d'adresse basée sur DHCP	• L'ordinateur doit être conforme pour pouvoir recevoir une configuration d'adresse IPv4 à accès illimité de DHCP • Il s'agit de la forme de contrainte de mise en conformité NAP la plus faible

Configuration de NAP

1. Mise en place des programmes d'intégrité
2. Stratégie de contrôle d'intégrité
3. Groupes de serveurs de mises à jour
4. Configuration du client NAP (netsh ou GPO)

Demonstration :

1. Installation : Rôle "Service de stratégie et d'accès réseau"
2. Ajouter NAP et HRA

Résoudre les problèmes :

```
netsh NAP client show state|config|group
```

Journaux d'évènements :

ID d'événement	Signification
6272	L'authentification a réussi
6273	L'authentification n'a pas réussi
6274	Un problème de configuration existe
6276	Le client NAP est mis en quarantaine
6277	Le client NAP est en période d'essai
6278	Le client NAP bénéficie d'un accès complet

http://aide.info

12 Optimisation des services de fichiers

FSRM File Server Resource Manager : gestion des quotas par répertoire (WS2008R2+), restriction d'écriture d'extension de fichiers, gestion DFS

Installation :

- Rôle "Service de fichiers et de stockage" (plusieurs services de role dont "gestionnaire de ressources du serveur de fichiers", "déduplication de données", "réplication DFS")
- A installer sur le(s) serveur(s) contenant les données

Gestion :

- "Gestionnaire de ressources du serveur de fichiers"
  - Gestionnaire de ressources du serveur > Clic droit : options de rapports, d'assistance fichier refusé ...
  - Quotas : "modèles de quotas" permet d'appliquer les modifications sur les quotas basés sur ces modèles. Notification mail ou obs d'evnt
- PowerShell
  - `Get-FSRMQuotas` lister les quotas activés (disabled = false)
  - `get-command -module FileServerResourceManager` lister les commandes liées à FSRM
- Commandes DOS deprecated (n'existe plus en WS2016)

Gestion du filtrage :

- Par extension, par groupe de fichiers
- Utilisation de modèles (cf. quotas)
- Les fichiers déjà présents ne seront pas modifiés
- Passif = avertir, Actif = bloquer

Rapports de stockage :

- Fichiers en double, volumineux, quotas, propriété des dossiers, fichiers les moins / plus souvent ouverts ...
- Planification ou manuel
- Format des rapports
- Base de registre : changer la nomination des rapports (pour les mettre sur un intranet par exemple)

`fsutil file createnew c:\toto.txt 130000000` créer un fichier (taille en octets = 130Mo)

Règle de classification (WS2008R2+) :

- Modifier des flux NTFS liés fichiers (propriétés) selon certains critères (nom) : seulement sous NTFS (sauf pour les fichiers MSOffice car stocké dans les métadata)
  - La valeur Oui de la propriété booléenne l'emporte sur les Non (si plusieurs règles)
- Possibilité ensuite d'effectuer des actions selon ces propriétés
- Possibilité de gérer à distance (sauf classification de fichiers) pour les serveurs distants : WS2003+

http://aide.informatique1.fr

13 DFS Distributed FileSystem

Présentation

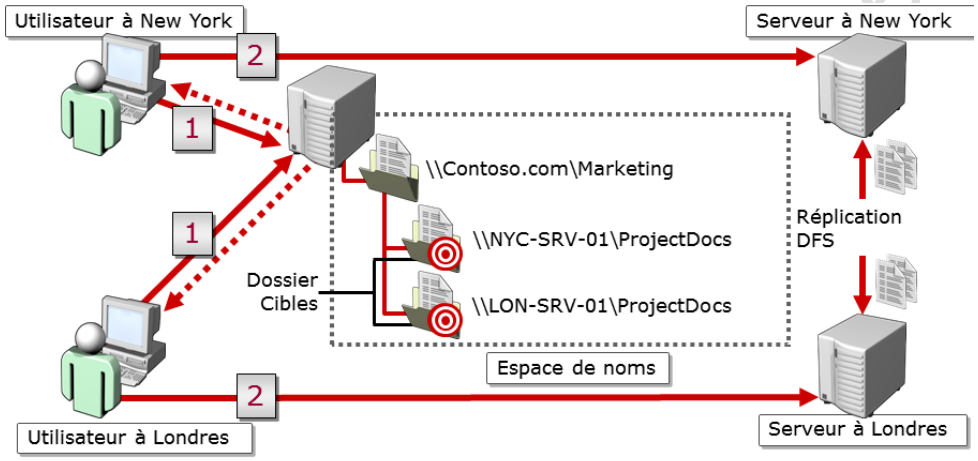
- Pratique pour les migrations de serveurs
- Utilise DFS-N (espace de nom) et DFS-R (réplication)

Espace de nom (DFS-N) :

- Basé sur un domaine : stocké dans ADDS tolérance des espaces de nom.
  Préféré : au moins une racine sur les contrôleurs de domaine pour attaquer avec \\nomDeDomaine\
- Autonome : besoin d'un cluster de basculement

Réplication DFS (DFS-R) :

- Compression des données sur les réseaux
- Surveille le journal USN (journal d'accès au disque) = réplication par détection de fichiers (sauf si réplications inter-sites désactivées en journée par exemple)



1. Types d'utilisateur : \\contoso.com\marketing
   Les ordinateurs clients contactent un serveur d'espace de noms et reçoivent une référence
2. Les ordinateurs clients mettent en cache la référence puis contactent le premier serveur dans cette référence

Fonctionnement de DFS

Nota pour le schéma : les utilisateurs ne voient que \\contoso.com\marketing / espace de nom = DFS-N / Réplication DFS = DFS-R / Détection par les sous-réseaux -> contacte le serveur DFS le plus proche (si ne repond pas, contacte l'autre au bout de qlq secondes)

Installation

- "Services de fichiers et de stockage" > Services de role "Espace de nom DFS" et "Réplication DFS"

Outils

- Console mmc "Gestion du système de fichiers distribués DFS"
  Nota : depuis WS2008R2+ l'ADDS est répliqué par DFS : ne pas toucher à la réplication sysvol
- `dfsradmin.exe` : gérer la réplication DFS
- `get-command *DFS*`
- `dfsrdiag.exe` : surveiller l'était de la réplication

Pour un partage :

- Autorisations du partage : Utilisateurs authentifiés = CT
- Autorisations NTFS : paufiner les accès

14 Configuration du chiffrement et de l'audit avancé

14.1 EFS – Encrypted FileSystem

EFS : fonctionnalité du NTFS – permet de chiffrer les fichiers (qu'en NTFS)

- Utilise le certificat utilisateur, sinon utilise un certificat auto-signé (à ne pas utiliser !)
- Recouvrement : pas défaut l'admin local
- Utiliser ADCS + autorité de certification + déploiement GPO

Marche à suivre :

- Sauvegarder les certificats utilisateur
- *Autorité de certification entreprise (certsvr.msc) (génère la clé de recouvrement)*
- Configurer un agent de récupération et la rendre portable pour la sauvegarder ailleurs
- Détail sur les propriétés du fichier crypté > avancé > détail :
  - Infos sur qui a crypté
  - Sauvegarder les clés
  - Ajouter des utilisateurs pouvant accéder

Commandes utiles :

Crypter en PowerShell : sur le dossier voulu : `get-childitem -file | foreach Encrypt`
Crypte les fichiers contenus dans le dossier voulu

14.2 Audit avancé

Configuration de l'audit avancé :

Audit les accès aux fichiers, ouverture de session, changement de compte ou objet dans l'ADDS, attribution de droits utilisateurs

Plus on audite, plus ça ralentit. Ne donne pas le nom du fichier audité

Mise en place :

- Activer l'audit dans les stratégies de groupe
  - Audit simple : GPO > config. ordi > Param. Windows > Param. sécurité > Stratégies locales > Stratégies d'audit -> réussite / échec = audit de l'accès global
  - Audit avancé (WS2008R2+) : GPO > config. ordi > Param. Windows > Param. securité > Configuration avancée de la stratégie d'audit -> affiner
  - Active la fonction d'audit sur les postes mais n'audite rien
  - gpupdate /force + redémarrer
- Se configure dans l'onglet des ACL
  - Propriétés > avancé > audit
  - Choix des utilisateurs à auditer
  - Choix des accès à auditer (modifications, lectures, écritures)
- Observateur d'évènements > journal de sécurité

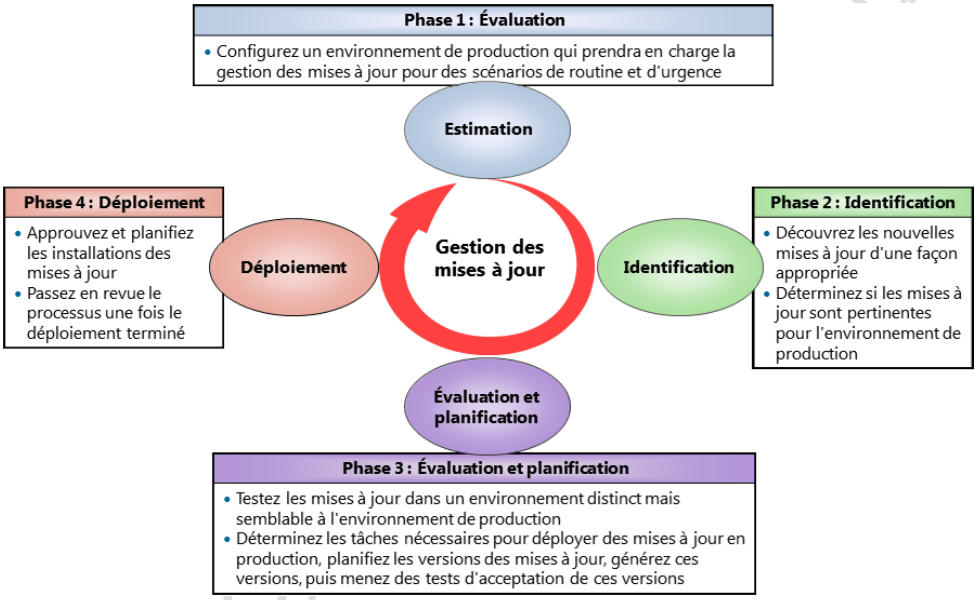
http://aide.informatique1.fr

15 WSUS - Implémentation de la gestion des mises à jour

Serveur de mises à jour internalisé

Mise en œuvre :

- Mise à jour approuvées. Par défaut affiche les mises à jour disponibles. Doit être autorisée pour les télécharger
- Par GPO des ordinateurs : définir le serveur "Windows update" = serveur wsus
    - Ordi > Strat > Modèle Adm > Comp Windows > Windows update
        - Autoriser l'installation immédiate : désactiver
        - Autoriser le ciblage coté client : activé + nomDuGroupeCible (celui du wsus)
        - Autoriser les non-admin à recevoir les màj : activé
        - Config des màj : installer auto : désactivé, tous les mardi 12h
        - Ne pas modifier l'option par défaut activé
        - Pas de redémarrage auto pour les utilisateurs connectés : activé
        - Redemander un redémarrage pour les installations planifiées : activé
        - Vérifier l'emplacement intranet... : http://serveur.fqdn:8530 pour les deux
        - (Mode de traitement par bouclage de la strat de groupe utilisateur : activé)
    - Mettre l'ordi dans une OU



Prérequis (tout sera automatiquement installé en même temps que WSUS) :

- Configuration logicielle requise :
    - Services Internet (IIS) version 6.0 ou ultérieure
    - Microsoft .NET Framework 2.0 ou version ultérieure
    - Microsoft Management Console 3.0
    - Microsoft Report Viewer Redistributable 2008 ou version ultérieure
    - SQL Server 2012, SQL Server 2008, SQL Server 2005 SP2 ou Base de données interne Windows
- Configuration matérielle requise :
    - Processeur x64 de 1,4 GHz ou supérieur
    - Au moins 2 Go de mémoire RAM
    - 10 Go d'espace disque disponible (40 Go ou plus est recommandé)

Nota : les 2GO de RAM seront utilisés **en plus** de ce qui est déjà utilisé. **Report Viewer Redistributable 2008**+ est à télécharger

Installation :

- Rôle "Services WSUS"

Outils :

- Service WSUS

- `get-command *wsus*`

http://aide.informatique1.fr

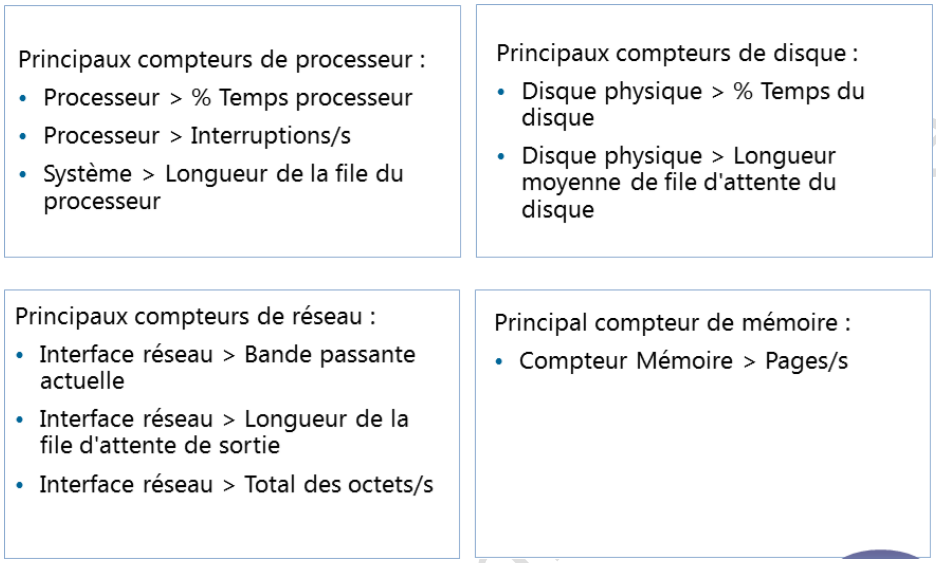
16 Surveillance de Windows Server 2012

Outils d'analyse :

- Gestionnaire des tâches
- Analyseur de performances (savoir quoi analyser)
- Moniteur de ressources (à peu près équivalent à perfmonitor de Sysinternal)
- Observateur d'évènements

Analyseur de performances : "Analyseur de perf" ou `perfmon` :

- Files d'attentes représentatives de ce qui n'est pas traité assez vite



Nota : Compteur mémoire : bande passante = indique si la ram a été mal installée

Observateur d'évènement :

- Abonnements : permet d'envoyer les journaux d'évènements d'une autre machine
  - Apparait des "évènements transférés"
  - Utilise les ports TCP5985 (ou TCP5986 en https)

Surveillance des services d'infrastructure réseau

- Syslog / snmp

Surveillance des ordinateurs virtuels :

- Surveillance de la VM + surveillance de l'hôte

http://aide.informatique1.fr