Administration système: cours 6 (PP)

- AD: consoles MMC
- AD avancé: forêt, arborescences, relations d'approbation, maîtres d'opérations, serveur de catalogue global
- AD: stratégies de groupe
- AD: Les domaines windows 2000
- Sauvegardes: présentation générale, ntbackup
- Rappel réseau: ethernet, tcp/ip, routage
- SMTP

Création d'une console personnalisée

- L'administration W2K: des consoles MMC pré-créées;
- En standard, un jeu plus riche sur un contrôleur de domaine mais installable sur tout ordinateur W2K (adminpak)
- Administration à distance
- Possibilité de créer des consoles personnalisées

Windows 2000 propose des outils d'administration qui sont des **MMC** (**Microsoft Management console**). Un jeu de consoles standard est livré avec tout ordinateur windows 2000. Le jeu de console est plus riche sur un contrôleur de domaine que sur un ordinateur windows 2000 pro. L'installation des consoles manquantes sur un ordinateur W2K pro ou server non contrôleur de domaine est possible.
Les consoles MMC permettent d'effectuer la majeure partie des tâches d'administration à distance.
Il est possible de modifier les consoles livrées. On peut ainsi ajouter le composant enfichable « utilisateur et ordinateurs Active Directory » à la MMC « gestion de l'ordinateur ».
On peut aussi créer des consoles personnalisées :

- Limitée à un seul outil;
- Limitée aux objets que leurs utilisateurs devront gérer;
- Restreintes à une seule fenêtre;
- Proposant une liste de tâches d'administration pour faciliter le travail de leur utilisateur.

C'est particulièrement pratique dans le cas d'une délégation de l'administration de certains objets.

Création d'une console personnalisée

- Utilisation de mmc.exe
- Ajout de composants enfichables, extensions
- Mode auteurs, mode utilisateur

L'outil mmc.exe permet de créer des consoles personnalisées et de modifier des consoles existantes.
Une console est constituée d'un ou plusieurs composants logiciels enfichables. Un composant logiciel enfichable peut être composé d'extensions. Certains composants peuvent être utilisés à la fois comme composants logiciels enfichable et comme des extensions.
Exemple: « gestion de l'ordinateur » est une console composée de nombreuses extensions (Observateur d'événements, utilisateurs et groupes locaux, ...).
Les consoles personnalisées peuvent être fournies à des utilisateurs ayant des droits d'administration limités. Il est possible de limiter les consoles ainsi livrées pour les rendre non modifiables. Pour cela, on définit le mode d'une console:
•**Mode auteur** (**mode par défaut**) : autorise la modification de la console (ajout/suppression de composants, création de fenêtres, ...)
•**Mode utilisateur accès total**: l 'utilisateur peut se déplacer parmi les objets gérés par la console, créer des nouvelles fenêtres, ... mais ne peut enregistrer ces modifications ni ajouter/supprimer des composants enfichables
•**Mode utilisateur accès limité, fenêtre multiples**: idem mais pas de déplacement possible
•**Mode utilisateur, accès limité, fenêtre unique**: idem mais une seul fenêtre.

Structure logique

- Forêts
- Arborescences
- Domaines
- Unités d'organisation

Il est important de planifier la structure avant de l'implanter. La structure logique: décomposition de l'entreprise en domaines, arborescences, unités d'organisation. Cette décomposition pourra être guidée par la structure de l'entreprise et, surtout, par les besoins d'administrations :

- Limites de sécurité (qui est responsable de quoi) : domaines
- Possibilité de délégation d'administration : unités d'organisation
- Autorisation d'accès aux ressources
- Contraintes ou configurations des comptes et des sessions des utilisateurs
- ...

Nous allons détailler les outils qui sont à la dispositions de l'architecte du réseau pour créer sa structure logique. Plus tard, nous parlerons de éléments qui l'inciteront à adopter une structure plutôt qu'une autre: délégation de tout ou partie de l'administration de tout ou partie d'un ensemble d'utilisateurs et, dans un autre chapitre, les stratégies de groupes (imposer des configurations aux utilisateurs et aux ordinateurs).

Domaine

- Limite de sécurité
- Unité d'administration
- Unité de réplication
- Mode d'un domaine: mixte ou natif (dépend de l'OS des contrôleurs de domaine)

Limite de sécurité: chaque domaine dispose de ses propres stratégies de sécurité.

Unité d'administration: L'administrateur du domaine gère l'ensemble de la sécurité sur son domaine. Il est le seul à pouvoir accorder des permissions sur les objets de son domaine. Sauf autorisation accordée explicitement, il ne gère rien en dehors de son domaine.

Unité de réplication: les données actives directory sont répliquées sur tous les contrôleurs de domaine toutes les 5 mn.

Mode d'un domaine: **mode mixte**: s'il reste des contrôleur de domaine NT4. Certaines fonctionnalités ne sont pas disponibles. **Mode natif**: si tous les contrôleurs de domaine sont en W2K. L'OS des ordinateurs non contrôleur du domaine n'influe pas sur le mode.

Il est possible de passer du mode mixte au mode natif mais pas l'inverse.

Unités d'organisations

- Organisation logique à l'intérieur d'un domaine
- Contient des objet active directory
- Permet
  - De déléguer des pouvoirs
  - De simplifier la sécurité
  - D'appliquer une stratégie à des ordinateurs ou utilisateurs
- Rend obsolète la construction usuelle domaine de compte/domaine de ressources NT4
- Une UO ne peut être créée que dans le domaine ou une autre UO

Une **unité d'organisation** (UO) est un « container » pouvant contenir des utilisateurs, des ordinateurs, des groupes, ... et d'autres unités d'organisation.

Une unité d'organisation doit être utilisée quand on souhaite déléguer des pouvoirs ou appliquer une stratégie particulière à un sous-ensembles des objets du domaine.

Il est possible de donner tout ou partie des droits d'administration sur les objets d'une UO à certains utilisateurs.

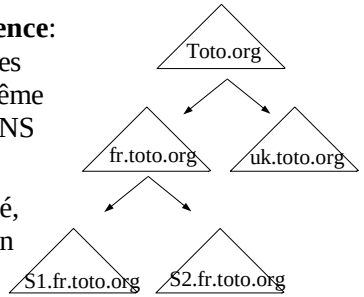
En créant une unité d'organisation regroupant les ordinateurs du domaine, on peut déléguer leur gestion à un utilisateur qui n'aura pas de droit sur les comptes utilisateurs. On évite de mettre en place deux domaines ressources/comptes comme sous NT4.

Sans UO, les utilisateurs sont dans le container *Users* (qui n'est pas une UO) et les ordinateurs dans un container *Computers* qui n'est pas une UO.

Un petit piège: une UO ne peut être créée que dans le domaine ou dans une autre UO. « users » n'est pas une UO et on ne peut donc pas créer d'UO (« unité d'organisation » n'apparait alors pas dans le menu « Nouveau ».

Arborescences

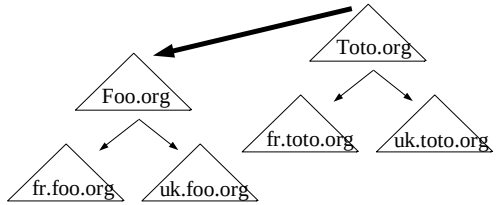
- **Arbre ou arborescence**: ensemble de domaines appartenant à une même hiérarchie de nom DNS
- **Domaine racine**: premier domaine créé, non renommable, non supprimable
- **Domaine enfant**



L'ajout d'un nouveau domaine se fait en créant un domaine enfant à un domaine existant de l'arborescence. Le nom complet (DNS) du nouveau domaine est obtenu en concaténant son nom au nom du domaine parent. Ainsi, le nom de S1 est S1.fr.toto.org.

Forêts

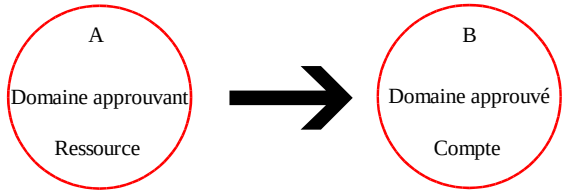
- **Forêt**: ensemble d'arborescences



Une **forêt** est un ensemble d'arborescences ayant des noms appartenant à des espaces non contigus. Les arborescences d'une forêt partagent une configuration, un schéma et un catalogue global communs. Le nom de la forêt est le nom de l'arborescence racine (première arborescence créée dans la forêt).
Une forêt peut ne contenir qu'une seule arborescence.

Relations d'approbation

- Déléguer l'authentification
- Permettre d'autoriser des utilisateurs d'un autre domaine à utiliser des ressources de son domaine



Une relation d'approbation permet à l'administrateur d'un domaine A de déléguer l'authentification de certains utilisateurs à un autre domaine B.

L'administrateur du domaine A peut accorder l'accès à certaines ressources (ouvrir une session, accès à des ressources, ...) aux utilisateurs validés par le domaine B. Cet accès doit être explicitement donné par l'admin de A qui reste donc maître chez lui.

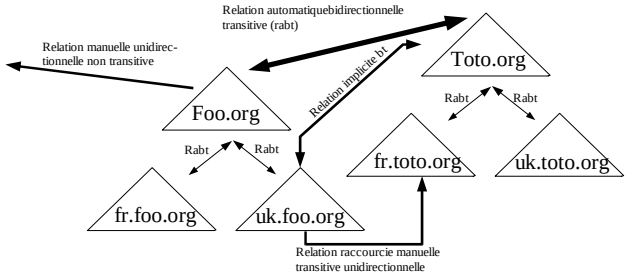
Parallèle avec la vie courante : une médiathèque départementale peut accepter les cartes délivrées par les bibliothèques municipales pour identifier certains de ses lecteurs. Dans ce cas, la médiathèque joue le rôle du domaine approuvant et les bibliothèques municipales jouent le rôle du domaine approuvé.

La médiathèque est libre de décider l'accès à ses ressources qu'elle laisse aux membres des bibliothèques municipales tout comme l'administrateur du domaine A est libre de décider l'accès qu'il laisse aux membres du domaines B (en général, l'accès est donné aux membres d'un groupe de B, pas à des utilisateurs individuels).

Une carte de bibliothèque locale permet à la médiathèque de vous authentifier (elle sait qui vous êtes) mais son règlement intérieur peut ensuite vous refuser l'accès (vous n'êtes pas autorisé).

Relation d'approbation sous W2K

- Relation bidirectionnelles/unidirectionnelles, transitives, implicites, manuelles/automatiques, raccourcies



Une relation entre un domaine A et un domaine B est **bidirectionnelle** si A approuve B et si B approuve A.

Une relation est **transitive** si A approuve B, B approuve C alors A approuve C même s'il n' y a pas de relation d'approbation explicite entre A et C.

Au sein d'un forêt, des relations d'approbations bidirectionnelles transitives entre domaine parent et domaines enfantset entre arborescences et racine sont automatiquement mises en place lors de la création des arborescences et des domaines.

Il est possible de créer manuellement des **relations raccourcies** qui évitent le parcours complet du chemin entre deux domaines. De telles relations sont unidirectionnelles et transitives.

Les **relations d'approbations externes** peuvent être créées manuellement entre deux domaines de deux forêts différentes ou entre un domaine W2K et un domaine non W2K. Ces relations externes sont unidirectionnelles et non transitives.

Structure physique

- Sites
- Contrôleurs de domaines

La structure physique d'active directory est distincte de sa structure logique. La structure physique vous permet de gérer et d'optimiser le trafic de votre réseau. Elle se compose de deux éléments: les contrôleurs de domaine et les sites:

Un **site** est un ensemble de plusieurs sous réseaux IP reliés entre eux par des liaisons à haut débit. Les liaisons entre sites peuvent être plus lentes ou plus coûteuses.

Définir des sites, c'est donner des informations à windows 2000 qui lui permettront d'optimiser le trafic lié à la duplication entre contrôleurs de domaines et la vitesse de la liaison entre les utilisateurs et leur contrôleur de domaine.

La notion de site est indépendante de la notion de domaine: un domaine peut contenir plusieurs sites e un site peut contenir plusieurs domaines.

Un **contrôleur de domaine** est un ordinateur sous windows 2000 server qui stocke et gère une copie de la base d'active directory. Il duplique les modifications de l'annuaire vers les autres contrôleurs. Le processus d'ouverture de session des 'utilisateurs met forcément en jeux au moins un contrôleur de domaine. Il est donc important que tout utilisateur puisse avoir une liaison rapide et fiable avec au moins un contrôleur de domaine.

Pour concevoir une structure physique cohérente, il faut maîtriser le fonctionnement de la réplication entre contrôleurs de domaine et les rôles des maîtres d'opérations.

Exécution multimaîtres (W2K) vs maître unique (NT 4)

- Sous NT4: un contrôleur principal (original en lecture/écriture) et des contrôleurs secondaires (copie en lecture)
- Sous W2K: des contrôleurs de domaines identiques, une base en lecture/écriture sur chaque contrôleur
- W2K: Opérations en maîtres unique : maitres d'opérations

Sous windows NT4, un contrôleur de domaine particulier appelé le **contrôleur principal** du domaine hébergeait les informations du domaine (sécurité, ...) et y avait un accès en lecture/écriture. Les **contrôleurs secondaire** avaient une copie de ces informations. Un contrôleur secondaire pouvait servir à consulter les informations mais pas à les modifier. Les modifications devaient avoir forcément lieu sur le contrôleur principal (changement de mot de passe, création d'utilisateurs, ...)

Sous W2K, les contrôleurs de domaines sont globalement tous équivalents et hébergent une copie des informations de la base d'annuaire accessible en lecture/écriture. La base d'annuaire est dupliquée et distribuée sur chaque contrôleur de domaine (**réplication multimaîtres)**. Les opérations usuelles (créations de comptes, changement de mot de passe, ...) peuvent être réalisées sur n'importe quel contrôleur du domaine. Dans certains cas, si des modifications incompatibles sont réalisées sur des contrôleurs à un moment où ils sont coupés du réseau, seule l'une de ces modification sera prise en compte. W2K a été conçu pour limiter au maximum ce type de problèmes.

Certaines opérations critiques sont prises en charges par un seul contrôleur de domaine. Pour ces quelques opérations, on retrouve un fonctionnement en maître unique (mais une copie en lecture est accessible sur tout ou partie des autres contrôleurs). Les ordinateurs réalisant ces opérations critiques sont appelés des **maîtres d'opérations** (ou **FSMO** : Flexible Single Master Operation).

Partition d'annuaire

- Partition d'annuaire : portion de l'espace de noms de l'annuaire
- Sert à répartir les données de l'annuaire
- Sous arbres :
  - Configuration
  - Schema
  - Domaine

Consultez le tome 6 du kit de ressources techniques pour plus d'information sur la parition d'annuaire: reskit tome 6 page 99 et suivantes

Voir cours3-AF pour une présentation de LDAP.

Maîtres d'opérations

- Maître de schéma
- Maître d'attribution de noms de domaine
- Le maître émulateur CPD
- Le maître de RID (identifiants relatifs)
- Le maître d 'infrastructure

Maître de schéma: modification sur le schéma d'annuaire. Un par forêt.

Maître d'attribution de nouveau noms de domaine:permet d'ajouter/retirer un domaine de la forêt et les objets de référence croissée avec les annuaires externes. Un par forêt. S'il est indisponible, les fonctions qu'il assure ne sont plus assurée. Le rôle peut être transféré définitivement à un autre contrôleur.

Maître émulateur CPD: sert de contrôleur principal de domaine aux ordinateurs w9x ou NT membres du domaines sur lesquels le client Active Directory n'a pas été installé. Il y en a un par domaine. S'il est indisponible, les changements de mot de passe depuis des ordinateurs w9x et NT sans client active directory seront impossibles. Certaines ouvertures de sessions seront perturbées (cf reskit chap. 7).

Maître des identificateurs relatifs : distribue des paquets d'identificateurs relatifs aux contrôleurs de domaine. Les contrôleurs de domaines peuvent ainsi utiliser ces identifiants relatifs lors de la création des principaux de sécurité (utilisateurs, groupes ou ordinateurs). Quand un contrôleur de domaine a épuisé son stock d'identifiants relatifs, il doit contacter le maître RID pour en obtenir de nouveaux. Si le maître RID est indisponible, il ne sera plus possible de créer de nouveaux principaux sur ce contrôleur. Il y a un maître RID par domaine. Le maître RID sert aussi lors du transferts de principaux d'un domaine dans un autre à l'aide de l'utilitaire movetree. L'utilitaire DCDIAG permet d'afficher l'allocation des paquets (option /v, test RidManager, cf reskit tome 6, chapitre 10 et dcdiag /?) -> cf diapo suivante pour la suite.

Exemple

- Arborescence de domaines : toto.fr, s1.toto.fr et s2.toto.fr
- Indiquez les rôles de maître d'opération de cette forêt (11 rôles)

Maître d'infrastructure:Quand un utilisateur et un groupe sont dans deux domaines différents, le changement de nom de l'utilisateur n'est pas pris en compte tout de suite au niveau du groupe. le maître d'infrastructure est responsable de la référence transdomaine groupe-à-utilisateur de façon à mettre à jour le nom de l'utilisateurs là où il est utilisé dans les autres domaine. Il y a un maître d'infrastructure par domaine.

Le maître d'infrastructure compare ses données à celles du serveur de catalogue global. Les deux rôles ne doivent pas être assurés par le même ordinateur.

En cas d'indisponibilité du maître d'infrastructure, les mises à jour seront retardées.

Réponse de l'exemple: au niveau de la forêt toto.fr: 1 maître de schéma et un maître d'appellation de domaines. Au niveau de chaque domaine : un émulateur CPD, un maître d'infrastructure et un maître des RID (soit 3*3=9 rôles).

Placement des rôles de maître d'opération

- 3 soucis :
  - Contrôler la charge réseau
  - Augmenter les performances et la fiabilité
  - Permettre un remplacement rapide en cas de défaillance
- Transfert de rôle:
  - Ntdsutil: pour transférer un rôle en ligne de commande
  - Repadmin: diagnostique de la réplication (vérification de la mise à jour)

En cas de défaillance d'un rôle, il est possible de transférer le rôle à un contrôleur existant. Pour éviter les pertes d'informations, il est utile de repérer les contrôleurs de domaines qui sont partenaires de réplication de chaque maître d'opération. En tant que partenaire direct, ces ordinateurs auront la base de données la plus à jour possible et sont des remplaçants idéaux.

Le placement par défaut des rôles convient bien aux domaines de petite taille. Pour les domaines de grande taille, on peut planifier le placement des rôles :

La planification prendra en compte la topologie du réseau et les actions à mener en cas de défaillance.

Pour plus d'information, consultez le kit de ressources techniques, tome 6 pages 400 et suivantes.

Serveurs du catalogue global

- Mémorise une copie partielle des données Active Directory de tous les domaines de la forêt
- Utile pour l'ouverture de session des utilisateurs :
  - Appartenance aux groupes universels
  - Domaine d'un nom principal d'utilisateur
- Localisation d'objets dans la forêt
- Un contrôleur de domaine peut devenir serveur de catalogue global (action manuelle)
- Conseil: au moins un serveur de catalogue global par site et par domaine

Un **serveur de catalogue global** est un contrôleur de domaine possédant une copie en lecture seule des attributs les plus utilisés de **tous** les objets de la forêt.

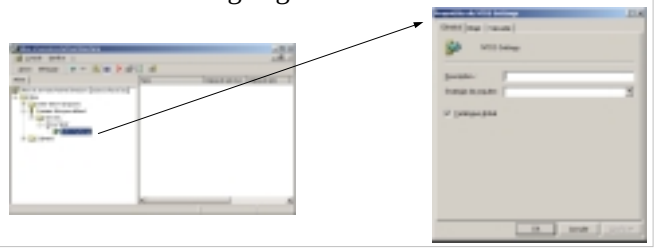
Le premier contrôleur de la forêt est serveur de catalogue global. Les administrateurs de domaines peuvent transformer n'importe quel contrôleur de domaine en serveur de catalogue global. Le serveur de catalogue global va être utilisé pour des recherches à l'échelle de la forêt. Il est conseillé d'avoir un serveur de catalogue global par site pour éviter l'utilisation de liaison lentes et d'avoir un serveur de catalogue global par domaine. Sans serveur de catalogue global, les recherches s'effectuent sur chaque contrôleur de domaine de la forêt.

Le serveur de catalogue global est consulté pendant l'ouverture de session des utilisateurs. Il fournit les informations sur l'appartenance de l'utilisateur à des groupes universels nécessaires à la création du jeton de sécurité de l'utilisateur. Si l'utilisateur a fourni un nom principal (petit@ueve.world) pour l'ouverture de session au lieu du couple identifiant/domaine ou nom SAM (UEVE\petit), c'est le serveur de catalogue global qui fournit le nom de domaine (UEVE) associé au nom principal.

Le serveur de catalogue global est consulté en cas d'ajout d'un utilisateur ou d'un groupe d'un domaine différent à un groupe du domaine.

Serveurs du catalogue global

- Sites et services Active Directory pour passer un contrôleur de domaine serveur de catalogue global
- Ouverture de session en cas d'indisponibilité des serveurs du catalogue global.



Pour passer serveur de catalogue global un contrôleur de domaine, il faut utiliser **Sites et Services Active Directory** et cocher l'option ad hoc dans les propriétés de **NTDS Settings**.

En cas d'indisponibilité de tous les serveurs de catalogue global :

- Un membre du groupe administrateurs du domaine peut ouvrir une session
- Pour les autres utilisateurs, la connexion s'appuie sur les informations mises en cache : si l'utilisateur s'est déjà connecté sur le domaine, il peut ouvrir une session. S'il ne s'est jamais connecté sur le domaine, il ne peut y ouvrir de session. Il peut néanmoins ouvrir une session sur l'ordinateur local.

Bibliographie

- Structure logique AD: reskit tome 6 chap. 1
- Maîtres d'opération, catalogue global : reskit tome 6, chapitre 1, chapitre 7
- Les RFC concernant LDAP : cf http://www.rfc-editor.org/ pour le texte des RFCs et l'annexe B du tome 6 du reskit pour la liste des RFCs concernées.

Bibliographie (2)

- Sécurité: reskit tome 6 chap. 12
- Sécurité: "Modèle de sécurité windows », Joel Marchand (hsc), MISC No 2

Stratégie de groupes

- Permet d'imposer à des ordinateurs ou à des utilisateurs des configurations, des paramètres
- 2 types de stratégies:
  - Stratégies locales : propre à un ordinateur
  - Stratégies non locales: s'appuient sur Active Directory

Les stratégies de groupes permettent d'imposer des paramètres de configuration (menus, paramètres des programmes (proxy, ...), paramètres de sécurité, limitations (pas de chgt de mot de passe, pas d'ouverture de session sur le cotrôleur de domaine, ...) à des utilisateurs ou à des ordinateurs. C'est un outil extrèmement utile qui permet de tout gérer au niveau du domaine (stratégies non locales).
Stratégie locale:
gérée par l'outil « stratégie de sécurité locale »
Stockée dans *%systemRoot%\System32\GroupPolicy*
la stratégie locale est écrasée par les stratégies non locales.
Stratégies non locales:
s'appuie sur active directory.
Une stratégie non locale consiste à définit un objet de stratégie de groupe et à le lier à un ou plusieurs conteneur (site, domaine, unité d'organisation. On peut ainsi appliquer des paramètres identiques à plusieurs conteneurs. On peut désactiver l'application de paramètres à un conteneur en détruisant le lien sans détruire l'objet GPO. On peut les réactiver en recréant le lien. Ainsi, on ne perd tout le travail de configuration réalisé sur l'objet GPO.

- **Un objet GPO peut être lié à plusieurs conteneurs**
- **Un conteneur peut être lié à plusieurs objets GPO**

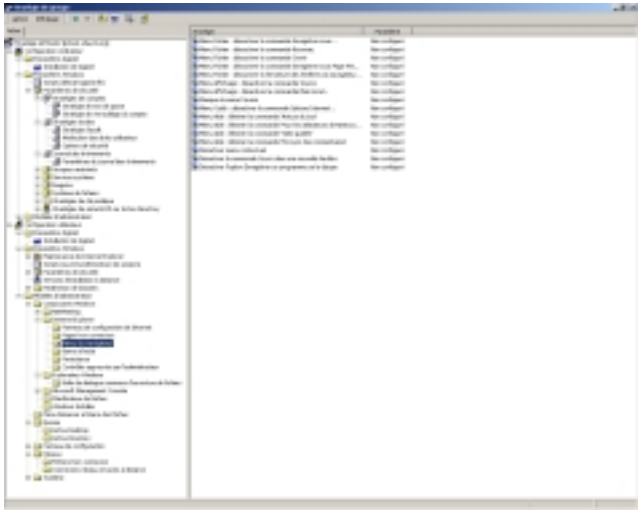
Paramètres contrôlés

- Modèle d'administration: paramètres basé sur le registre
- Sécurité: paramètres de sécurité locale, de site, domaine ou UO
- Installation des logiciels
- Scripts: démarrage/arrêt d'ordinateur ou de session utilisateur
- Redirections de dossiers

Modèles d'administration: paramètres s'appuyant sur le registre configurant les paramètres d'application (proxy internet explorer par exemple), la présentation des sessions utilisateurs, le comportement des services système.
Sécurité: configuration des options de sécurité locale, de domaine, de site. Par exemple: stratégie de sécurité des contrôleurs de domaine pour autoriser un utilisateur à ouvrir une session sur un contrôleur de domaine
installation des logiciels:gestion centralisée de la mise à jour des logiciels
Scrips:scrips exécutés à l'ouverture ou à la fermeture de session utilisateur, scripts exécuté au démarrage ou à l'arrêt de l'ordinateur
Redirection de dossiers: rediriger les dossiers de l'utilisateurs (Mes Documents, ...) sur le réseau. Permet à un utilisateur de voir ses dossiers quelque soit la machine sur laquelle il travaille.

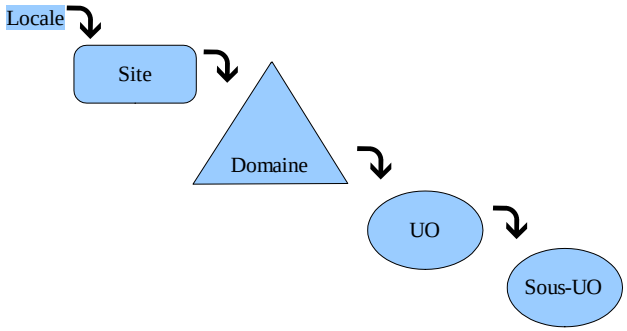
Objets stratégie de groupe (GPO)

- 2 parties :
  - Conteneur de stratégie de groupe (Group Policy Container) : objet AD
  - Modèle de stratégie de groupe (Group Policy Template GPT) : dossier
- Peut-être lié à plusieurs conteneurs
- Un conteneur peut être lié à plusieurs GPOs
- La stratégie s'applique aux objets du conteneur



Ordre d'applications des stratégies de groupes

- Héritage cumulatif des paramètres



Conflits entre GPOs

- Les paramètres de la dernière GPO sont appliqués :
  - Ordre d'application via l'héritage
  - Ordre d'application des GPOs liés à même conteneur.
- Dans un GPO, paramètres de l'ordinateur prioritaires sur ceux de l'utilisateur

Puis +sieurs diapo avec des exemples (cf ENI par 310ss)

DEMO (1)

- On crée un utilisateur etu1 sur le contrôleur de domaine
- On vérifie qu'il est correctement authentifié mais qu'il n'a pas le droit d'ouvrir une session interactive sur le contrôleur de domaine
- On modifie la stratégie de sécurité du contrôleur de domaine pour qu'il ait le droit d'ouvrir une session dessus
- On vérifie que ça ne marche pas
- On attend 5 mn et on vérifie que ça marche.

Exemple

- Une UO LicASR, une UO LicMiage toutes deux dans le domaine.
- Sur le site: GPO imposant un fond d'écran château de chambord
- Sur le domaine: GPO imposant de ne pas avoir d'item « Executer » dans le menu démarrer
- Une GPO empéchant le changement de mot de passe liée aux deux UO LicASR et LicMiage
- Une GPO imposant la photo d'un prof barbu en fond d'écran liée à l'UO LicASR
- Qu'est-ce qui s'applique réellement à LicASR ?

Les GPO vont s'appliquer dans l'ordre suivant :

- GPO de site: fond d'écran chambord
- GPO de domaine : pas d'Exécuter dans « Démarrer »
- GPO d'UO: pas de changement de mot de passe et fond d'écran barbu

Quand un paramètre est redéfini, c'est le dernier appliqué qui l'emporte. On obtient donc :

- pas d'Exécuter dans « Démarrer »
- pas de changement de mot de passe
- fond d'écran barbu

Demo2:

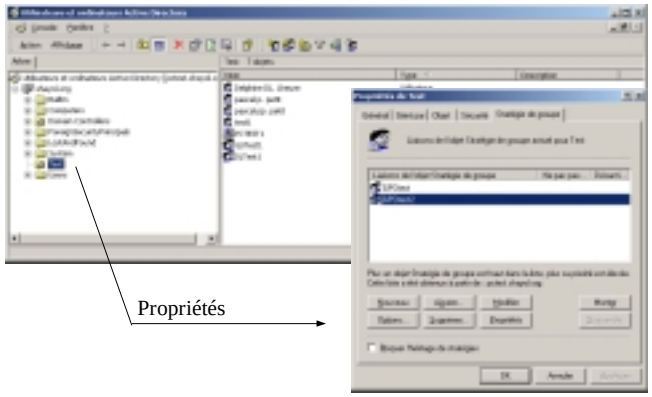
- On applique l'exemple
- On force la propagation des stratégies de groupe avec un « secedit /refreshpolicy machine_policy » et « secedit /refreshpolicy user_policy ». Souswindows XP, on utilisera gpupdate à la place de secedit.
- On le vérifie
  - soit avec le compte étu1 sur le contrôleur de domaine,
  - Soit avec le compte étu1 sur une des stations du domaine

Application des objets stratégie de groupe

- Paramètres utilisateurs: à l'ouverture de session
- Paramètre ordinateur: au démarrage de l'ordinateur
- Actualisation toutes les 90 mn (+/- 30mn)
- Actualisation toutes les 5 mn sur les contrôleurs de domaine
- Forcer l'actualisation: scedit /refreshpolicy ...

Pour forcer la mise à jour :
Scedit /refreshpolicy machine_policy ou Scedit /refreshpolicy user_policy
Sous windows Xp: utiliser la commande gpupdate

Création d'un objet stratégie de groupe



Bibliographie

- Kit de ressource technique tome 6
- « Active Directory, les services d'annuaires windows 2000 » de V. Cottin, édition ENI

Sauvegarde

- Sauvegarde / archivage
- Sauvegarde des données / du système
- Sauvegarde des postes individuels / des données sur un serveur
- Sauvegarde hors site

Le terme achivage est utilisé dans deux contextes :

- on souhaite sauvegarder les évolutions dans le temps des données sauvées, pouvoir revenir à une version passée et pas seulement restaurer la version courante.
- Stocker les données anciennes et peu ou plus utilisées de façon à libérer de l'espace disque. Son évolution est la notion de stockage étendue où l'on définit un hiérarchie de moyen de stockage. Les données courantes sont stockées sur des périphériques rapides, celles qui servent moins sur des périphériques moins rapide et moins coûteux, celles qui ne servent plus jamais sont stockées sur bandes (moins cher mais l'accès est plus long, le temps que le robot charge la bonne bande).

Sauvegarde des données/du système: les données sont des choses vitales à sauvegarder. Sauvegarder le système peut permettre de gagner du temps en cas de crash: on le restaure au lieu de le réinstaller. Dans ce cas, on utilise un logiciel de restauration qui ne nécessite pas la réinstallation préalable du système.

Solutions qui ont prouvé leur inefficacité

- Faire faire les sauvegardes par les utilisateurs : pour dégager sa responsabilité mais aucune garantie qu'elles seront faites
- Sauvegardes sur des supports peu fiables (disquettes, DAT, ...)
- Sauvegarde en lecture seule : il faut valider sauvegarde et procédures de restauration
- Sauvegarde d'un système en cours d'exécution
- Un seul support de sauvegarde
- Sauver sur une partition du même disque
- Pas de sauvegarde hors site (incendie, ...)

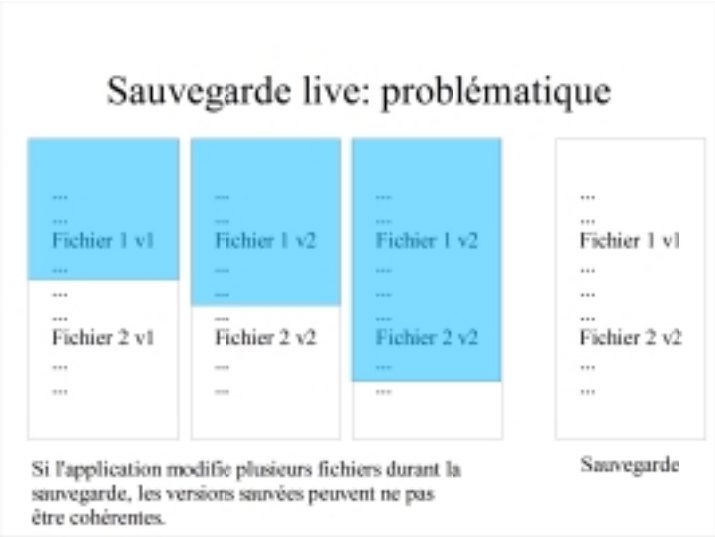
Cette page liste quelques exemples de choses à ne pas faire si on veut des sauvegardes fiables.

On peut être amené à en mettre certaines en place pour des raisons administratives (pour dégager sa responsabilité par exemple). Il faut avoir concience dans ce cas que les sauvegardes sont purement théoriques.

Sauvegarde par les utilisasateurs: mis à part dans des contextes où il y a des procédures rigoureuses, les utilisateurs ne réalisent pas les sauvegardes régulièrement. Leur faire réaliser les sauvegarde ne peut servir qu'à leur faire supporter la responsabilité. Ce n'est pas un moyen fiable. **Les seules sauvegardes fiables sont les sauvegardes automatisées qui ne dépendent pas des utilisateurs**.

Sauvegardes en lecture seule: il est important de **définir une procédure de restauration des sauvegarde et de la tester régulièrement pour éviter de se retrouver avec des sauvegardes que l'on peut restaurer**. Le principe est le même que pour les alertes incendie: seuls des tests en vrai permettent de valider les procédures.

Support de sauvegarde (partion d'un autre disque, un seul support): il faut faire en sorte qu'à tout moment, quoi qu'il se passe, on ait au moins une sauvegarde en état. Les sauvegardes stressent les disques qui ont tendance à casser pendant la sauvegarde. Si on a un seul support; on efface la sauvegarde précédente quand on en fait une autre. En cas de crash pendant la sauvegarde; on a plus le disque, on a plus la sauvegarde précédente et on n' a pas en core celle qui est en cours.



La sauvegarde prend un certain temps. Si le système continue à fonctionner, les fichiers peuvent être modifiés pendant la sauvegarde et on risque de se retrouver avec des version incohérentes sur la sauvegarde. Exemple avec une application qui va modifier deux fichiers:

la zone bleue indique le niveau d'avancement de la sauvegarde. A droite, on a les fichiers sauvegardés.

- La sauvegarde sauvegarde la version 1 du fichier 1
- Pendant qu'elle avance, l'application modifie ses fichiers : les fichiers 1 et 2 sont modifiés (passent en version 2)
- Quand la sauvegarde arrive au fichier 2, c'est al version 2 qu'elle sauvegarde.

Bilan: dans la sauvegarde, on a la version 1 du fichier 1 et la version 2 du fichier 2. Si ces deux fichiers sont liés (par exemple;: le fichier 1 est un index des informations du fichier 2), il est possible que la restauration de versions différentes ne permettent pas à l'application de redémarrer.

Sauvegarde live: solutions

- Arrêt de l'application pendant la sauvegarde;
- Snapshot: image des blocs du sgf, en cas d'effacement de fichier, les blocs ne sont pas réalloués tant que la sauvegarde n'est pas finie
  - Suppose un support dans le sgf
  - Proposé par les NAS, par afs, ...
  - Application: proposer aux utilisateurs une image de l'état antérieur de leur compte (la veille ?) à moindre coût.

Le plus simple consiste à arrêter l'application pendant la sauvegarde mais ce n'est pas forcément compatible avec les impératifs de l'entreprise.

Une autre solution consiste à prendre une image du disque à un instant donné et à sauver cette image. Prendre l'image de l'ensemble des données n'est pas possible (sinon on saurait faire une sauvegarde instantannée). Pour cela, on prend une image des pointeurs vers les blocs de données et on garantit que les blocs de données ne seront pas détruits par la suite..

Sauvegarde live: snapshot

- Là, on mettra une illustration du fonctionnement des snapshot
- Fait en live au tableau.

Sauvegarde : démarche

- Nécessité d'un cahier des charges
- Plan de sauvegarde
- Plan de restauration
- Que sauve-t-on ?
- Pour se protéger de quoi ?
- Sécurité vs confidentialité

La sauvegarde, c'est une chose critique qui nécessite un cahier des charges précis, des plan de restauration, une définition précise de ce contre quoi on se protège.

Certains éléments du cahier des charges peuvent être contradictoire: avoir une sauvegarde hors site est une bonne chose pour se protéger d'un incendie. C'est aussi s'exposer au vol de cette sauvegarde et donc 'est une mauvaise chose pour la confidentialité des données.

Exemple de l'incendie du crédit lyonnais qui avait des sauvegardes hors site et un site informatique de secours qui a pu prendre le relais dans un délai très bref sans attendre la remise en état du centre informatique brulé. D'un point de vue coût, on dépasse évidemment ce que peut se permettre une entreprise de taille moyenne. :-)

Problèmes liés à la volumétrie:

- Coût
- Charge réseau
- Durée des sauvegardes
- Indisponibilité des serveurs/applications

Le volume des disques et des données augmente tout le temps. Un gros volume de données à sauvegarder, cela implique:

- Un coût plus important (périphériques de sauvegarde plus gros, ...)
- Une charge réseau plus importante
- Des sauvegardes plus longues
- Une indisponibilité plus longue des serveurs/applications si on ne fait pas de la sauvegarde live.

Les sauvegardes incrémentales ou différentielles sont une solution pour limiter le volume des données à sauvegarder.

Sauvegardes incrémentales/différentielles

- Sauvegarde incrémentielle : fichiers créés ou modifiés depuis la sauvegarde précédente
  - Diminue le volume à sauver
  - Restauration nécessite toutes les sauvegardes, restaure toutes les versions d'un même fichier
  - Peu adapté si la totalité des fichiers changent
- Sauvegarde différentielle : fichiers créés/modifiés depuis la dernière sauvegarde de référence
  - Diminue le volume à sauver
  - Plus de volume qu'en incrémental
  - Restauration nécessite la sauvegarde de référence et la dernière sauvegarde différentielle

Ràf: prendre le cas d'un fichier qui ne change pas, d'un fichier qui change souvent, d'un fichier qui change rarement et commenter :

- Le volume des sauvegardes
- La procédure de restauration (quelles sauvegardes impliquées, quel volume restauré)

Exemple:

- Comparer la taille des sauvegardes et les procédures de restauration dans les cas suivants : (ST: sauvegarde totale, I: sauvegarde incrémentale, D: sauvegarde Différentielle)
- Cas 1) ST, I1, I2, I3, I4, I5, I5
- Cas 2) ST, D1, D2, D3, D4, D5
- Cas 3) ST, I1, I2, I3, D1, I4, I5

Cas 1): ST sauve toutes les données et chaque sauvegarde incrémentale sauve les données modifiées/créées depuis l'incrémentale précédente. Un fichier modifié le lendemain de ST sera sauvé seulement dans I1
La restauration nécessite de restaurer ST puis toutes les incrémentales dans l'ordre. Si un fichier a été modifié plusieurs fois, ses différentes version seront présentes dans I1, I2, ... et chaque version sera restaurée puis écrasée par la version suivante.
Cas2) ST sauve toutes les données. Chaque différentielle sauve les données créées/modifiées depuis la sauvegarde totale. Un fichier modifié le lendemain de ST sera sauvé dans chaque différentielle.
La restauration nécessite de restaurer ST et la dernier incrémentale.
Cas 3): ST sauve toutes les données. D1 sauve toutes les données créées/modifiées depuis ST. I4 sauve les données modifiées depuis D1, I5 depuis I4.
La restauration nécessite soit de restaurer ST, I1, I2 et I3 (si le crash a lieu avant D1), soit ST, D1, I4 et I5 s'il a lieu après D1.

Dump: un outil de sauvegarde sous unix

- Dump est un outil unix
- Il est efficace (travail directement au niveau du sgf)
- Sauvegarde non portable d'un unix à un autre (lié au sgf)
- Niveau (0 à 9) permettant un gestion très souples des sauvegarde incrémentales/differentielles:
  - Une sauvegarde niveau *n* sauvegarde tous les fichiers modifiés depuis la dernière sauvegarde de niveau *n-1*

Ràf:

- Citer l'option -u
- Donner un exemple de cycle de sauvegarde et comparer avec différentielle/incrémentale à loa ntbackup

Ntbackup: un outil de sauvegarde sous windows

- Un outil apparu avec windows 2000
- Pratique et polyvalent
- Supporte les sauvegarde incrémentales et différentielles
- Permet de sauver les données (au choix) et/ou les fichiers systèmes
- Utile pour des sauvegardes « artisanales »
- Pour des sauvegardes lourdes, la pratique est d'utiliser des logiciels dédiés (cf cours sauvegarde AF)

Ntbackup

- La restauration nécessite que w2k soit installé
- NT Backup est installé par défaut sous windows 2000/XP pro et serveur.
- Ntbackup est fourni avec windows Xp home (cf VALUEADD\MSFT\NTBACKUP)

Windows: droit requis pour les sauvegardes

- Dans la prochaine version de ce document

Rappels réseau: notion de couche

- Couche application: flux tcp/message udp
- Couche tranport (tcp/udp): segment tcp, paquet udp
- Couche internet (IP) : datagramme
- Couche accès au réseau (trame ethernet par exemple)

Rappel réseau (ipv4): adresse ip, sous-réseau, ...

- Adresse ip: 4 octets, à une adresse correspond une interface réseau unique
- Sous-réseau, CIDR

Alexandre Fernandez a eu l'occasion de fair equelques rappels sur tcp/ip lors du cours précédent. On se limite ici à ce qui est nécessaire pour comprendre le routage IP.

Rappel rapide sur les adresses IP: à une adresse correspond une seule interface (carte) réseau. L'inverse n'est paa vrai. Une machine peut avoir plusieurs cartes réseau et chaque carte réseau peut avoir plusieurs adresse IP.
Une adresse ip est constituée d'une partie identifiant le réseau et d'une partie identifiant l'hote sur son réseau.
Exemple: 192.168.202.1 et 192.168.202.23 sont deux hôtes sur le même réseau. Le réseau est 192.168.202.0/24. Les parties hotes sont 1 et 23.
CIDR: permet d'indiquer le nombre de bits dont est constitué la partie réeeau d'une adresse IP.
Exemple: 192.168.202.0.24 : les 2' premiers bits (ou les trois premiers octets) sont la partie réseau: 192.168.202. Le reste est la partie hôte.

ARP

- Lien couche liaison/couche IP
- Cache arp, commande arp

Arp permet de faire le lien entre la couche IP et la couche liaison.
Si un datagramme IP a IPDest comme adresse IP de destination, arp permettra de trouver l'adresse ethernet de l'interface ayant IPDest comme adresse IP.
Les requètes arp permettent de découvrir les adresses ethernet des machines présentes sur le même réseau ethernet.
Pour éviter de faire cela à chaque envoi de datagramme, les machines maintiennent un cache qui contient les associations adresse MAC/adresseIP déjà trouvées.
On peut consulter ce cache avec la commande arp.
Exemple:
consulter le cache avant tout accès réseau (il est vide)
envoyer un datagramme à une machine (ping machine par exemple)
consulter le cache arp (arp -n): il contient l'adresse ethernet de la machine que l'on a contacté.
Ràf: faut-il parler de sécurité ? De corruption de cache arp ? D'entrée statique & Co ?

Ports, sockets

- Port: /etc/services
- Socket: (ipSource, portSource, ipDest., portDest)

Fait par A. Fernandez dans le cours précédent.

Rappel réseau: routage

- Une machine sait transmettre les datagrammes sur les sous-réseaux de ses interfaces (réseaux locaux)
- Les autres datagrammes sont envoyés à un routeur directement joignable (situé sur un réseau local)
- Une machine qui sait transmettre un datagramme reçu sur l'une de ses interface sur une autre de ses interface est appelée routeur ou passerelle.
- Table de routage (netstat -nr)
- Routage dynamique : un programme externe modifie la table de routage

Une machine ne sait transmettre directement des datagrammes qu'à des machines situées sur les sous-réseaux de ses interfaces.
Une routeur est une machine reliée à plusieurs réseaux et qui accepte de faire transiter un datagramme d'un réseau à un autre.
Pour aller d'une machine A à une machine B non sitées sur un même sous-réseau, un datagramme passera par une suite de routeurs. Chaque routeur ayant un réseau commun avec le routeur suivant.
Par exemple: A -> R1 -> R2 -> R3 -> B
Le routage, c'est donc ce qui fait que des machinesqui ne sont pas situées sur le même réseau local arrivent à communiquer. L'un des problèmes du routage, c'est pour une machine de déterminer à quelle machine/routeur, directement relié à elle, il faut transmettre le datagramme pour faire en sorte qu'il arrive à destination.
La table de routage d'une machine contient les passerelles permettant de joindre certains hôtes ou réseaux. Elle contient au moins une entrée précisant que les réseaux locaux à la machine sont directement joignables ainsi qu'une entrée pour l'interface de bouclage.
On peut afficher la table de routage avec la commande « netstat -rn ».
Dans les cas les plus complexes (plusieurs routes pour joindre une machine, route changeante, ...), des programmes se chargent de modifier dynamiquement la table de routage. On parle alors de routage dynamique.

Routage: cas classiques

- Réseau isolé
- Machine à une seule interface réseau
- Quelques réseaux avec des routeurs connus et fixes : routage statique
- Nombreux réseaux, interconnexion changeante: routage dynamique

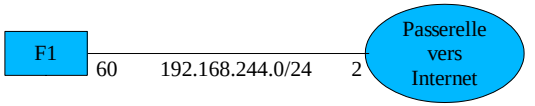
Les machines d'un réseau isolé n'ont pas de passerelle par défaut définie. Elles ne peuvent communiquer qu'avec les autres machines de leur réseau local. Lors de la configuration de l'interface réseau de la machine, une route sera définie pour le sous-réseau local. A l'heure d'internet, c'est un cas de plus en plus rare.

Machine à une seule interface réseau dans un site ayant accès à internet: c'est le cas de figure le plus courant. Comme dans le cas précédent, lors de la configuration de l'interface réseau, une route permettant de joindre les machines du sous-réseau local sera créée automatiquement. Tous les datagrammes qui ne sont pas à distination d'une machine locale seront envoyés à une passerelle par défaut. Une route par défaut sera définie. Cette route par défaut se définit en donnant l'adresse IP de la passerelle par défaut dans les outils configuration réseau.

Quelques réseaux avec des routeurs connus : c'est le cas du réseau interne d'entreprises de taille moyenne. Dans ce cas, les routes vers ces réseaux sont définies statiquement.

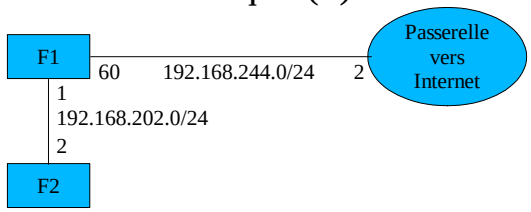
Nombreux réseaux avec interconnexion changeante: dans un réseau où certains hôtes sont joignables par plusieurs routes, où les routes changent parfois (certains liens tombent, d'autres apparaissent, ...), il faut utiliser des protocoles de routage dynamiques. Des programmes comme routed, gated vont modifier la table de routage en fonction des informations que leur donnent leurs homologues sur les autres routeurs.

Rappel réseau: exemples de routage statique



La machine F1 d'adresse IP 192.168.244.60 a une passerelle par défaut qui a comme adresse 192.168.244.2.
Elle enverra directement à leur destinataire les datagrammes dont l'ip de destination est sur 192.168.244/24
Elle enverra les autres datagrammes à sa passerelle par défaut.

Rappel réseau: exemples de routage statique (2)



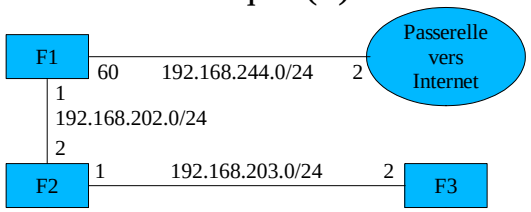
La machine F2 d'adresse IP 192.168.202.2 a une passerelle par défaut qui a comme adresse 192.168.202.1.
Elle enverra directement à leur destinataire les datagrammes dont l'ip de destination est sur 192.168.202/24
Elle enverra les autres datagrammes à sa passerelle par défaut.
La passerelle vers internet aura F1 définie comme passerelle vers 192.168.202.24

Pour joindre Internet, F2 devra passer par F1. Cela implique:

- Que F1 soit un routeur (elle doit accepter de router les datagrammes d'une interface à une autre)
- Que F2 ait F1 comme passerelle par défaut. Ainsi tout paquet qui n'est pas à destination du réseau 192.168.202.0/24 sera envoyé à F1. On peut noter que F1 est sur un réseau local de F2. F2 pourra donc effectivement lui envoyer directement les paquets: une passerelle doit être directement joignable par la machine.

On garantit ainsi que les datagrammes pourront transiter de F2 vers internet.
F1 aura la passerelle vers internet comme passerelle par défaut.
Dans l'autre sens, c'est plus complexe mais il faut que les datagramme à destination du réseau 192.168.202.0/24 finissent par aboutir à F1. Cela impose notamment que la passerelle internet sache que F1 est le routeur vers 192.168.202.0/24.

Rappel réseau: exemples de routage statique (3)



La machine F3 d'adresse IP 192.168.203.2 a une passerelle par défaut qui a comme adresse 192.168.203.1.
Elle enverra directement à leur destinataire les datagrammes dont l'ip de destination est sur 192.168.203/24
Elle enverra les autres datagrammes à sa passerelle par défaut.
La machine F1 aura F2 définie comme passerelle vers 192.168.203.24

Un datagramme de F3 à destination d'internet devra passer par F2 puis par F1. Cela implique:

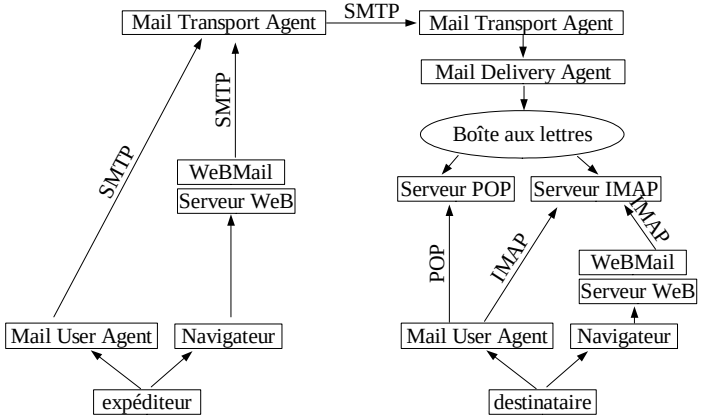
- Que F1 et F2 soient un routeur
- Que F2 ait F1 comme passerelle par défaut. Ainsi tout paquet qui n'est pas à destination du réseau 192.168.202.0/24 ou à destination du réseau 192.168.203.0/24 sera envoyé à F1.
- Que F3 ait F2 comme passerelle par défaut

On garantit ainsi que les datagrammes pourront transiter de F3 vers internet ou vers F1.
F1 aura la passerelle vers internet comme passerelle par défaut.
Dans l'autre sens, que faut-il pour qu'un datagramme puisse transiter de F1 à F3 ?
Si on ne fait rien, comme le réseau où est F3 n'est pas un réseau local de F1, F1 enverra le paquet à sa passerelle par défaut (passerelle internet) ce qui n'est pas ce que l'on veut.
Il faut donc indiquer à F1 que les datagrammes à destination de 192.168.203.0/24 doivent être envoyés à F2. On peut par exemple utiliser une commande route de la forme suivante (la syntaxe exacte dépend du système d'exploitation):
route add -net 192.168.203.0 192.168.202.2 255.255.255.0
La passerelle internet devra savoir que F1 est routeur pour 192.168.202.0/24 et que F2 est routeur pour 192.168.203.0/24

SMPT: notions de base

- L'envoi et la réception d'un courrier mettent en jeu de nombreux outils et protocoles. Notamment :
  - MUA: Mail User Agent ou agent utilisateur (mail, mutt, thunderbird (mozilla), eudora, voire même Outlook express si n'a peur de rien),
  - MTA: Mail Transport Agent ou agent de transport (serveur smtp: sendmail, postfix, qmail, exim, voire exchange),
  - MDA: Mail Delivery Agent ou agent de délivrance du courrier, chargé par le MTA de déposer le courrier dans la boîte aux lettre de l'utilisateur (exemple: procmail, ...)
  - POP3, IMAP : protocole permettant au MUA d'accèder aux boîtes aux lettres

SMPT: architecture



SMTP:

- Rfc821 puis 2821: protocole SMTP
- Rfc822 puis 2822: format des courriers
- D'autres documents concernent le courrier: POP3, IMAP, ETRN, MIME, ...

SMTP: commandes

- Contrôle de session
  - HELO/EHLO
  - RSET/QUIT
  - NOOP
- Traitement des courriers
  - MAIL From:<adresse>
  - RCPT To:<adresse>
  - DATA
  - VRFY/EXPN

SMTP: DEMO (1)

- On se connecte sur le port 25 d'un serveur existant et on envoie un courrier:
  - Un courrier raisonnable
  - Un courrier avec un expéditeur bidon et des entêtes bidon
- On commente les codes d'acquittement (il est de bon ton de faire quelques fautes de frappe pour générer des erreurs)
- On montre un refus de relais

SMTP: acquittement

- 2xy: acquittement positif
- 4xy: acquittement négatif provisoire
- 5xy: acquitement négatif définitif

SMTP: demo (2)

- Un serveur mal configuré qui retourne un code en 4xy en cas d'utilisateur inexistant
- Conséquence: pas de courrier d'erreur pour l'expéditeur dans que son MTA n'a pas fini d'essayer d'envoyer le courrier

Entête des messages (rfc 2822)

- Notion d'enveloppe
- Champs de traçage
  - Return-path
  - Received
- Adresses et champs utilisateur
  - From:,Sender,Reply-To:
  - To:, CC:, BCC:
- Champs informationnels souvent optionnels
  - Date, Subject, X-...
  - Message-ID
  - In-Reply-To:, References:

SMTP: DEMO

- On prend les courriers envoyés dans la première demo.
- On met en évidence les champs de traçage (Received) et les informations récupérées de l'enveloppe (Return-path)
- On commente les autres champs

MIME (RFC2045 à 2049)

Accusé de non-réception

Bibliographie

- Unix Administration, Jean-Michel Moreno, Dunod
- BSD, Emmanuel Dreyfus, Eyrolles
- TCP/IP Administration de réseau, Craig hunt, O'Reilly