http://www.laboratoire-microsoft.org

Essentiel Exchange 2003

IMPLEMENTATION ET GESTION DE MICROSOFT EXCHANGE 2003

Auteur : Guillaume LHOMEL - Sammy POPOTTE – Antoine RICHET

Version 0.80 – 2004-02-22

Ecole Supérieure d'Informatique de Paris
23. rue Château Landon 75010 – PARIS
www.supinfo.com

Table des matières

1. Installation et mise à jour vers Exchange Server 2003

1.1. Installation d'Exchange Server 2003

1.1.1. Matériel requis pour Exchange Server 2003

Voici ci-dessous le tableau récapitulatif du matériel requis pour l'installation d'Exchange Server 2003.
Nous distinguerons le matériel minimum indispensable, du matériel recommandé par Microsoft.

	Minimum requis	Recommandé
 Processeurs	233 MHz ou plus	1,6 GHz ou plus (exécution sur 8 processeurs au plus)
 Mémoire vive	256Mo minimum	3 à 4Go
 Disque dur	500Mo d'espace libre pour l'installation + 200Mo d'espace libre sur la partition système + un lecteur CD-Rom Les partitions doivent être formatées en NTFS	Partitions supplémentaires pour les transactions de bases de données et de journaux
 Système d'Exploitation	Microsoft Windows 2000 Server, Service Pack 3 (SP3) ou ultérieur Famille Microsoft Windows Server 2003 (sauf édition Web)	Microsoft Windows Server 2003, édition entreprise

Afin de planifier une installation supportant la charge de votre réseau, n'oubliez pas qu'il vous est possible de coupler plusieurs serveurs Exchange 2003. Prenez en compte le nombre d'utilisateurs susceptibles d'utiliser votre ou vos serveurs Exchange afin de calculer les ressources matérielles nécessaires.
La configuration la plus courante consiste à configurer des serveurs Exchange frontaux fournissant les connexions pour les clients, et des serveurs arrières chargés du stockage des boîtes aux lettres.

1.1.2. Environnement requis

Pour installer et configurer votre serveur Exchange, un certain nombre d'éléments sont requis.
Lors de cette installation, un assistant vous demande de vérifier quelques uns des points suivants :

- **Active Directory et DNS sont installés et configurés :** Microsoft Exchange Server 2003 s'appuie entièrement sur Active Directory et sa base de comptes utilisateurs. Votre installation d'Active Directory doit donc être propre et fonctionnelle.

- **Avez-vous les bonnes permissions pour exécuter l'installation ?** Vous devez être administrateur local de la machine afin de pouvoir installer Exchange. Cependant, durant l'installation, un certain nombre d'opération vont devoir être effectuées au sein d'Active Directory, telles que la mise à jour du schéma Active Directory. Pour cette mise à jour de schéma, vous devez être membre du groupe Admin de l'entreprise et du groupe Admin du schéma. Vous pourrez alors exécuter ForestPrep.
  Vous devez également être Admin du domaine afin d'exécuter un DomainPrep pour créer les groupes de permissions pour les serveurs Exchange.
  Vous pourrez alors également exécuter les outils de diagnostique tels que DCDiag et NetDiag vous

permettant de vérifier la connectivité de votre serveur.

- **Le système hébergeant Exchange 2003 fait-il bien partie du domaine ?**

- **Toutes les machines hébergeant Exchange pour une même organisation Exchange doivent faire partie de la même forêt Active Directory.** Effectivement, il ne peut y avoir qu'une organisation Exchange par forêt Active Directory.

- **Vous devez installer Exchange 2003 avant de mettre à jour un système Windows 2000 en Windows 2003 Server.** Lorsque vous ferez la mise à jour du système, il y aura une mise à jour plus logique des éléments liés à Exchange.

- **Vérifiez que vos contrôleurs de domaine et serveurs de catalogue global exécutent bien Windows 2000 SP3 ou Windows 2003 Server.** C'est la seule possibilité pour qu'Exchange Server puisse les contacter.

- **Lorsque vous exécutez ForestPrep, choisissez un compte qui aura les droits administrateur dans l'organisation Exchange.** Ce compte pourra alors administrer Exchange et donner des droits administratifs à d'autres comptes ultérieurement.

- **Lorsque vous exécutez DomainPrep, les groupes de domaine local suivants seront créés :** Exchange Domain Servers, Exchange Enterprise Servers. Même si Exchange 2000 est déjà installé, vous devez exécuter la version 2003 de DomainPrep pour Exchange 2003.
- Vérifiez que les services et applications suivantes sont installés : Microsoft .NET Framework, Microsoft ASP.NET, World Wide Web Publishing service, SMTP service, NNTP service.

1.1.3. Composants pouvant être configurés pendant l'installation

Votre environnement est maintenant prêt à recevoir l'installation d'Exchange. Sachez qu'il vous est possible de sélectionner différents composants pendant l'installation proprement dite.

Ainsi, nous avons :

- **Les services de Collaboration et de Messagerie Microsoft Exchange :** Ce sont les composants de base de messagerie. Lorsque vous sélectionnez ce composant, vous avez trois options disponibles : *Connecteur Microsoft Exchange pour Lotus Notes* (option nécessaire pour partager la messagerie avec les système Lotus Notes au format natif Lotus Notes), *Connecteur Microsoft Exchange pour les groupes Novell* (option nécessaire pour partager la messagerie avec les système Novell au format natif Novell), et *Connecteur Microsoft Exchange Calendrier* (option nécessaire pour le partage des informations de calendrier avec les systèmes Lotus Notes et Novell).

- **Outils d'administration système Microsoft Exchange :** ce composant installe les outils nécessaires à la gestion de votre serveur Exchange. Sont inclus dans ces outils : *Gestionnaire système Exchange* (outil principal vous permettant la gestion de vos objets Exchange) et une version modifiée de l'outil *Utilisateurs et Ordinateurs Active Directory* (cette version vous permet d'activer très simplement les boîtes aux lettres pour vos utilisateurs). En sélectionnant cet outil, vous pourrez également choisir d'installer le composant supplémentaire suivant : *Administrateur Microsoft Exchange 5.5* (outil permettant d'administrer les serveurs Microsoft Exchange 5.5).

1.1.4. Qu'est-ce qu'une installation automatisée ?

En plus de l'installation classique du produit Exchange, il vous est possible de procéder à une installation entièrement automatisée. Aucune interaction ne vous sera alors nécessaire pendant le processus d'installation. Vous devez pour cela préparer au préalable un fichier de réponses (.ini) aux différentes

questions normalement posées pendant l'installation. Vous pourrez alors utiliser ce fichier autant de fois que vous le souhaitez pour réaliser des installations similaire de serveurs Exchange.
Ce mode d'installation vous permet de gagner du temps lors d'un déploiement d'un grand nombre de serveurs Exchange pour votre entreprise.

Vous pouvez utiliser un fichier de réponses dans les cas suivants :

- Installation d'un second ou Xième serveur Exchange dans votre entreprise
- Installation des outils d'administration système Microsoft Exchange
- Exécution de DomainPrep

L'installation automatisée n'est pas possible dans les cas suivants :

- Installation du premier serveur Exchange 2003 dans votre entreprise
- Installation d'un serveur Exchange 2003 dans un cluster Windows
- Installation d'un serveur Exchange 2003 dans un environnement mixte (2003, et 5.5)
- Actions de maintenance, comme par exemple la réinstallation d'un serveur Exchange ayant subit un désastre.

1.1.5. Comment effectuer une installation automatisée ?

Le procédé est simple :

- Créez votre fichier de réponses (.ini)
- Lancez l'installation en utilisant le fichier .ini
- Exchange est alors automatiquement installé sur le ou les ordinateurs cibles

Vous pouvez cependant lancer une installation automatisée avec des options spécifiques :

- **Createunattend :** ce commutateur de ligne de commande vous permet de créer un fichier d'initialisation. Lors d'une installation classique, vos réponses aux différentes questions seront sauvegardées dans ce fichier d'initialisation. Vous pourrez alors réutiliser ce fichier pour l'installation automatisée d'autres machines.

- **Unattendfile :** vous pourrez alors utiliser les réponses fournies dans un fichier de réponses spécifique.

1.1.6. Comment vérifier que votre installation d'Exchange s'est déroulée correctement ?

Une série de tests simples vous permet de vérifier que votre installation d'Exchange s'est effectuée avec succès :

- **Utilisateurs et Ordinateurs Active Directory :** utilisez cette console pour créer un compte d'utilisateur avec boîte aux lettres.

- **Message de test :** Ouvrez une session avec le compte que vous venez de créer, créez un profil de messagerie dans Microsoft Outlook, et envoyez un message de test.

- **Gestionnaire système Exchange :** Ouvrez une session avec le compte pour lequel vous avez délégué les droits d'administration pendant l'installation et ouvrez le gestionnaire système Exchange. Développez tous les sous-conteneurs.

- Si l'une des étapes ci-dessus semble poser problème, vous pouvez alors consulter les outils suivants : *console Services* (afin de vérifier que les services Exchange ont été installés et démarrés), *Observateur d'événements* (regardez les éventuelles erreurs ayant été enregistrées pendant l'installation), *Explorateur Windows* (regardez si le dossier \Exchsrvr existe et qu'il contient les fichiers binaires et de bases de données Exchange).

1.2. Installation d'Exchange Server 2003 dans un environnement en cluster

1.2.1. Matériel requis pour Exchange Server 2003 en cluster

Voici la liste des éléments matériels indispensables pour Exchange Server 2003 en cluster :

- 2 serveurs identiques ou plus, désignés en tant que nœuds de cluster
- Un contrôleur de disque dur pour chaque nœud à partir duquel le système d'exploitation démarrera sur chaque nœud
- Un autre contrôleur séparé du premier (SCSI recommandé) pour un disque partagé
- Un disque partagé (typiquement externe) relié à tous les nœuds du cluster
- 2 cartes réseau pour chaque noeud

1.2.2. Types de configuration en cluster

Il existe 2 configurations possibles pour la mise en cluster : **Actif/Actif**, et **Actif/Passif**.

Actif/Actif : Exchange supporte seulement 2 nœuds de cluster dans cette configuration. Les 2 nœuds traitent activement les requêtes. Chaque nœud est configuré avec au moins 1 **Exchange Virtual Server (EVS)**. Le cluster est toujours considéré comme actif, même si tous les serveurs virtuels restants ne fonctionnent plus que sur un nœud. Exchange supporte jusqu'à 4 serveurs virtuels Exchange dans cette configuration.
Lorsqu'un nœud devient indisponible (panne ou mise hors-ligne), a lieu un **failover**. Les requêtes sont alors toutes traitées par le nœud restant jusqu'à ce que le second nœud redevienne disponible. Dans ce cas, les performances de votre système Exchange sont bien entendu réduites.

Actif/Passif : Dans cette configuration, vous devez avoir au moins un nœud passif, et un ou plusieurs nœuds actifs. Un nœud est considéré comme actif dès lors qu'il exécute une instance de serveur virtuel Exchange. Le nœud considéré comme passif n'exécute pas quant à lui une instance de serveur virtuel Exchange, ni aucune autre application d'ailleurs.
Si l'un des nœuds actif n'est plus à même de traiter les requêtes, un nœud passif prend alors le relais et exécute le serveur virtuel Exchange. Le premier nœud devient alors passif.
Dans cette configuration, les nœuds actifs traitent les requêtes, tandis que les nœuds passifs se tiennent prêts au cas où l'un des nœuds actifs faillirait.

1.2.3. Configuration de cluster recommandée pour Exchange Server 2003

Microsoft recommande l'utilisation d'une configuration **Actif/Passif** pour les raisons suivantes :

- Les serveurs Exchange peuvent détenir autant de boîtes aux lettres que l'on souhaite du moment que les serveurs passifs ont la même configuration matérielle. Dans une configuration **Actif/Actif**, un nœud ne peut héberger que 1900 boîtes aux lettres au maximum afin d'assurer la fiablilité du failover.
- La configuration est plus fiable

- Les performances sont meilleures que dans une configuration **Actif/Actif** où l'un des serveurs aura le double de charge par exemple, en cas de failover.
- Cette configuration permet d'avoir 8 nœuds de cluster, au lieu de 2. → Plus grande fiabilité et performance.

1.2.4. Conseils d'utilisation pour le clustering

Dans une configuration **Actif/Passif**, il est conseillé d'avoir un serveur virtuel Exchange de moins que le nombre de nœuds du cluster, au maximum. Effectivement, dans cette configuration, au moins l'un des nœuds est passif. Voici donc les recommandations selon les versions de Windows que vous exécutez :

Système d'exploitation exécuté	Nombre de noeuds	Nombre maximum de serveurs virtuels Exchange exécutés
 Windows 2000 Advanced Server	2	1
 Windows 2000 Datacenter	4	3
 Windows Server 2003, édition Entreprise ou Datacenter	8	7

Exchange 2003 est limité à 4 groupes de stockage par serveur (ensembles de boîtes aux lettres et de dossiers publics partageant les mêmes journaux de transaction). Cette limitation physique d'Exchange peut poser problème dans le cas d'une configuration **Actif/Actif**. En effet, imaginons que chaque serveur exécute 3 instances de serveur virtuel Exchange (donc 3 groupes de stockage sur chaque nœud). Si l'un des nœuds tombe en panne, l'autre nœud prend le relais. Malheureusement celui-ci ne peut pas supporter 6 groupes de stockage, d'où un problème évident. Dans ce cas, le nœud tombé en panne devra attendre d'être réparé pour rendre à nouveau disponibles ses groupes de stockage.

En réalité, il existe un 5ème groupe de stockage possible sur chaque serveur. Mais ce groupe est réservé aux sauvegardes et récupérations de groupes de stockage. Il n'est pas possible d'y créer des boîtes aux lettres.

1.2.5. Comment se déroulent les failover ?

Le failover se déroule différemment selon une configuration **Actif/Actif** ou une configuration **Actif/Passif.**

Failover Actif/Actif : Dans cette configuration, chaque nœud actif exécute au moins une instance du serveur virtuel Exchange. Lorsqu'un des nœuds devient indisponible, l'autre nœud prend le relais et continue de répondre aux machines clientes.

Failover Actif/Passif : Ici, un ou plusieurs nœuds actifs exécutent des instances de serveur virtuel Exchange, tandis qu'un ou plusieurs restent passifs. Le nœud passif est un serveur dédié en attente permanente d'un failover. Vous devez configurer la liste des nœuds passifs préférés en cas de failover. Ceci signifie juste l'ordre dans lequel seront choisis les nœuds passifs en cas de failover.

C'est dans cette configuration qu'un failover s'effectue le plus rapidement. En effet, le nœud passif récupérant les informations n'exécute aucune application à la base. Au contraire, dans une configuration Actif/Actif, le second nœud récupérant les informations du premier exécute déjà une instance de l'application. Le traitement du failover est donc plus long.

1.2.6. Autorisations requises pour l'installation et la configuration d'un serveur virtuel Exchange

Pour installer Exchange sur chaque nœud, vous devez être Administrateur local.
Pour créer le premier serveur virtuel Exchange de l'organisation, vous devez être administrateur Exchange au niveau de l'organisation.
Pour ajouter, modifier, ou supprimer un serveur virtuel Exchange d'un groupe administratif, vous devez avoir les autorisations d'administration Exchange au niveau du groupe administratif en question.

1.3. Installation et utilisation des outils d'administration Exchange

1.3.1. Les utilitaires de gestion pour administrer Exchange

Le G*estionnaire Système Exchange* et la console *Utilisateurs et Ordinateurs Active Directory* sont les principaux outils d'administration pour Exchange. Cependant, pour bon nombre d'opérations de maintenant, vous pouvez être amené à utiliser d'autres outils Windows et Active Directory.

Gestionnaire Système Exchange : A partir d'une seule console MMC, vous pouvez gérer Exchange pour votre entreprise. Vous l'utiliserez pour gérer les objets tels que : listes d'adresses, dossiers publics, serveurs, routage, stratégies. Il est possible d'installer cet outil sur un poste de travail.

Utilisateurs et Ordinateurs Active Directory : En plus de pouvoir gérer les ressources habituelles de votre domaine, telles que les utilisateurs, ordinateurs, partages …, vous pouvez gérer les destinataires Exchange et créer les boîtes aux lettres pour vos différents utilisateurs.

Administrateur Cluster : Grâce à cet outil, vous pourrez configurer, gérer et surveiller vos clusters.

ADSI Edit : Cet éditeur Active Directory vous permet de visualiser et de modifier les objets Active Directory avec entre autres, les propriétés et les attributs des objets. ADSI Edit se trouve dans les outils de support pour Windows 2000 ou 2003.

Utilitaire LDP : Cet utilitaire vous permet de vous connecter à un annuaire compatible avec le protocole LDAP (protocole d'accès utilisé par Active Directory). Cet utilitaire permet comme le précédent la modification d'objets, et se trouve également dans les outils de support.

Composant logiciel enfichable Schéma Active Directory : Vous pouvez utiliser cet outil pour visualiser la configuration des attributs et classes. La différence avec les 2 outils précédents est que vous ne pouvez pas vous connecter à l'instance d'un objet (un compte utilisateur spécifique par exemple). Vous pouvez par exemple modifier les attributs d'objets qui seront répliqué sur le catalogue global par exemple. Pour pouvoir utiliser ce composant, vous devez enregistrer la librairie DLL suivante : Schmmgmt.

Composant logiciel enfichable IIS : L'installation d'Exchange sur votre serveur se traduit par l'ajout de protocoles Internet pour que vos utilisateurs puissent consulter leurs boîtes aux lettres. L'un de ces protocoles est le HTTP et permet entre autres aux clients de consulter les dossiers public de votre

organisation par le biais d'un navigateur web. Vous pouvez gérer les accès Web sur votre serveur grâce à ce composant.

Composant logiciel enfichable DNS : Après l'installation d'Exchange, vous devez vous assurer qu'il existe des enregistrement de type MX et A pour vos serveurs Exchange au niveau des serveurs DNS de votre domaine.

1.3.2. A partir de quelles plate-formes peut-on administrer Exchange ?

L'essentiel de l'administration des systèmes Exchange va pouvoir se faire grâce à l'outil Gestionnaire Système Exchange. Il est possible d'exécuter cet outil sur les plates-formes suivantes :

- Windows 2000 Server avec le Service Pack 3
- Windows 2000 Professionnel avec le Service Pack 3
- Windows Server 2003 (toutes versions)
- Windows XP avec le Service Pack 1

Certains pré-requis existent tout de même quant à l'exécution de cet outil sur Windows XP :

- la machine doit être jointe à un domaine de la forêt Active Directory où le serveur Exchange est installé
- les outils d'administration Windows Server 2003 doivent être installés sur la machine
- le service SMTP doit également être installé. Par contre, il n'est pas nécessaire que ce service soit démarré. Sa simple installation suffit.

1.3.3. Autorisations requises pour accéder aux objets du Gestionnaire Système Exchange

Pour administrer Exchange, vous devez être membre du même domaine Active Directory que le serveur Exchange. De plus, vous devez avoir les autorisations sur les différents objets Exchange que vous voulez administrer.

Par défaut, seul le compte défini durant l'installation d'Exchange a le droit d'administrer tous les objets Exchange. Vous avez la possibilité de déléguer certaines tâches d'administration sur différents objets à d'autres comptes utilisateurs.

Voici maintenant les 3 autorisations existantes concernant l'administration d'Exchange :

- **Administrateur total Exchange** : cette autorisation donne un accès complet aux objets concernés. Vous pouvez alors ajouter, modifier ou supprimer des éléments de l'objet. Vous pouvez également modifier les autorisations liées à cet objet
- **Administrateur Exchange** : cette autorisation est identique à la précédente sauf que vous n'avez pas la possibilité de changer les autorisations liées à l'objet
- **Administrateur en lecture seule d'Exchange** : cette autorisation permet à un administrateur de lire les propriétés et attributs d'un objet, mais ne peut en aucun cas modifier celui-ci.

Afin de déléguer les tâches d'administration pour Exchange, il existe des assistants simples à exécuter au sein du gestionnaire système Exchange.

1.4. Mise à jour d'Exchange 2000 Server vers Exchange Server 2003

1.4.1. Les différences entre Exchange 2000 Server et Exchange Server 2003

Pour effectuer une comparaison des deux produits, nous allons lister les nouveautés de 2003, puis les éléments qui ont été supprimés.

Voici donc les nouveautés d'Exchange Server 2003 :

- **Accès clients améliorés :** grâce à Outlook 2003, les clients pourront se connecter en utilisant RPC sur http. Un support accrû des périphériques mobiles a également été ajouté.
- **Sécurité améliorée :** un nouveau système d'élimination de spams avec les listes de blocage. Prise en charge d'IPSec entre les serveurs frontaux et les serveurs arrière.
- **Gestion améliorée :** prise en charge des clichés instantanés de Windows Server 2003. Surveillance automatique de serveurs. Support de 8 nœuds de clusters.
- **Nouveaux outils de mise à jour et de déploiement**
- **Connecteurs Active Directory améliorés :** l'amélioration des connecteurs facilite les communications avec les systèmes Exchange 5.5
- **Nouvel outil de migration de dossier public :** l'outil Migration de dossier public Microsoft Exchange permet la migration et la réplication de dossier systèmes et publics vers un autre serveur.

Quels sont les éléments qui ont disparus :

- **Fonctionnalités de collaboration en temps-réel :** les outils de chat ou de messagerie instantanée par exemple, ne sont plus inclus dans Exchange Server 2003. Ces produits font maintenant partie d'une autre suite logicielle Microsoft : Microsoft Office Real-Time Communications Server 2003
- **Connecteurs pour MS Mail et Lotus ccMail**
- **Mappage du lecteur M :** utilisé à l'époque pour le stockage Exchange, ce mappage posait trop de problèmes de corruption des fichiers, avec les anti-virus entre autres.
- **Service de gestion de clé :** le service est pris en charge directement par Windows Server 2003.

1.4.2. Eléments requis pour la mise à jour vers Exchange Server 2003

Un certain nombre de conditions doivent être remplies pour une mise à jour réussie vers Exchange Server 2003. Nous en avons déjà étudié au début du chapitre, en voici d'autres :

- Vous devez effectuer la mise à jour avec un compte ayant les permissions appropriées
- Une connexion possible à un contrôleur de domaine pendant la mise à jour
- Mettez à jour en priorité les serveurs de front d'un groupe administratif
- Désactivez tous les services inutiles à la fin de l'installation si il y en a
- Pensez à mettre à jour les connecteurs Active Directory de votre organisation
- Si Microsoft Mobile Information Server est installé, supprimez-le avant la mise à jour
- Supprimez la messagerie instantanée, le chat, le service de gestion de clé, et les connecteurs MS Mail et Lotus ccMail
- Mettez à jour vos applications tierces susceptibles de communiquer avec vos serveurs Exchange 2003.

2. Configuration et gestion d'Exchange 2003

2.1. Création et application des stratégies Exchange

2.1.1. Qu'est qu'une stratégie Exchange ?

Une stratégie Exchange permet d'appliquer des paramètres communs à un ensemble d'objets Exchange du même type. Si vous avez plusieurs serveurs Exchange au sein de votre organisation, il est possible de modifier la manière dont doit se comporter un objet Exchange sur tous les serveurs en même temps et très simplement.

Ces stratégies sont tout de même différentes des stratégies de groupe que l'on trouve avec Windows Server 2003.
Les stratégies Exchange sont liées aux objets :

- Serveur
- Groupes de stockage
- Destinataires

2.1.2. Types de stratégies Exchange

On distingue deux types de stratégies : les stratégies système et les stratégies de destinataires.

Les stratégies système régissent le comportement et la configuration des serveurs Exchange ainsi que des informations de stockage. On retrouve ces stratégies dans le conteneur *Stratégies système*, créé dans l'objet *Groupe administratif*.
Voici les trois stratégies système :

- **stratégie de stockage de boîtes aux lettres :** grâce à cette stratégie, vous pouvez gérer des ensembles de boîtes aux lettres. Vous pouvez par exemple appliquer des limites de stockage, définir les mappages de dossiers publics, la mise à jour des index, les intervalles de maintenance, les listes d'adresses hors-connexion…
- **stratégie de stockage de dossiers publics :** de même que précédemment, vous pouvez par exemple appliquer des limites de stockage à des dossiers publics, gérer les index, les réplications, les planifications de maintenance…
- **stratégie de serveur :** vous pouvez ici stocker un ensemble d'objets serveur pour activer par exemple la journalisation des événements sur les serveurs.

Les stratégies de destinataires vous permettent de gérer utilisateurs, groupes, contacts, ou encore dossiers. Vous pouvez utiliser ces stratégies pour configurer par exemple le temps pendant lequel des messages peuvent être stockés sur le serveur.
Il existe par défaut une première stratégie qui définit une nomenclature d'adresses mail lors de la création de boîtes pour vos utilisateurs. Ces stratégies sont stockées dans le conteneur *Stratégies de destinataires* de l'objet *Destinataires*.

2.1.3. Quand utiliser les stratégies Exchange

Selon le nombre de serveurs Exchange que détient votre entreprise, il n'est pas toujours nécessaire d'appliquer des stratégies système.
En revanche, vous serez amené à utiliser régulièrement les stratégies de destinataire.

Si vous n'avez qu'un serveur Exchange, il vous semble peut-être inutile de paramétrer des stratégies système. Cependant, il est possible de les configurer dans l'optique où vous seriez amené à ajouter d'autres serveurs Exchange ultérieurement. Avec un seul serveur, la configuration manuelle reste plus précise qu'avec une stratégie système.
Avec plusieurs serveurs Exchange, il est plus facile et rapide d'utiliser les stratégies pour la configuration des serveurs.

Les stratégies de destinaires, quant à elles, sont indispensables pour simplifier l'administration de vos boîtes aux lettres. Qui plus est, peu importe le nombre de serveurs dans votre organisation.
Les 2 utilisations les plus courantes de ces stratégies sont :

- **Gestion des adresses email dans Active Directory :** vous pouvez par exemple définir des adresses SMTP différentes pour un seul utilisateur dans le cas d'un changement d'adresse. Effectivement l'utilisateur recevra toujours ses mails de son ancienne adresse. Par contre lorsqu'il répondra à ces mails, il utilisera sa nouvelle adresse
- **Gestion des paramètres Active Directory pour les boîtes aux lettres :** vous pouvez par exemple définir des informations de stockage selon le type d'employé de l'entreprise (temps de conservation de messages supprimés sur le serveur, …)

2.1.4. Eléments requis pour la création et l'application de stratégies système Exchange

Afin de créer une stratégie système, il est indispensable d'avoir au moins les droits d'administrateur Exchange sur le conteneur *Groupe administratif* dans lequel les stratégies système résideront. Pour appliquer la stratégie, vous devrez avoir le droit d'écriture sur l'objet pour lequel s'appliquera la stratégie.

Le conteneur *Stratégies système* n'existe pas par défaut. Vous devez le créer avant de créer les stratégies système. Il est possible d'avoir plusieurs conteneurs de stratégies système dans chaque groupe administratif.

Il est possible d'appliquer plusieurs stratégies système pour un objet. Mais vous devez vous méfier des conflits possibles. Pour cela, le mieux est de configurer un onglet différent dans chaque stratégie. Par exemple, vous configurer l'onglet *Limites* de la première stratégie, et vous configurer un autre onglet dans une deuxième stratégie.
Vous obtiendrez une certaine clarté dans l'application de vos stratégies, et vous n'aurez pas de conflit particulier.

2.1.5. Comment supprimer et outrepasser des stratégies système

Lorsque vous appliquez une stratégie sur un objet, il ne vous est plus possible de modifier manuellement les propriétés de l'objet. La seule solution pour cela est de modifier la stratégie ou de la supprimer.

Un clic droit sur la stratégie système dans le gestionnaire Exchange vous donne la possibilité de supprimer la stratégie. En revanche les paramètres anciennement configurés par cette stratégie sont toujours actifs. A vous de les modifier manuellement par la suite.

Selon la politique de l'entreprise, certains utilisateurs ne devront peut-être pas bénéficier de la même configuration de boîte aux lettres que la plupart des autres utilisateurs de l'entreprise. Vous devrez peut-être également créer d'autres dossiers publics configurés différemment des autres. Vous avez alors le besoin d'outrepasser les stratégies dans ces 2 cas précis.

Pour outrepasser une stratégie système, vous pouvez le faire soit manuellement directement au niveau d'une boîte aux lettres ou d'un dossier public, ou alors déplacer ceux-ci dans d'autres groupes de stockage avec les nouveaux paramètres.

2.1.6. Critères de recherche et priorités des stratégies de destinataire

Une fois l'installation terminée, une stratégie de destinataire existe par défaut. Vous pouvez créer d'autres stratégies qui outrepasseront celle par défaut.
En effet, celle par défaut a la priorité la plus faible et est lue en premier. La stratégie ayant la plus forte priorité sera lue en dernier dans la liste afin de pouvoir outrepasser toutes les autres.

Lorsque vous créez une stratégie de destinataires, vous devez spécifiez à quels utilisateurs sera appliquée la stratégie. Pour cela, vous devez entrer les critères de recherche grâce à une requête LDAP et un assistant.

2.2. Configuration d'Exchange Server 2003 pour une gestion proactive

2.2.1. Stockage et création des groupes de stockage

Le stockage Exchange est représenté par une base de données regroupant les emails et différents documents de votre organisation Exchange.
Le stockage est organisé en groupes de stockage contenant chacun des banques de boîtes aux lettres et des banques de dossiers publics. Chaque groupe de stockage représente un processus serveur.

Comme nous l'avons vu précédemment, Exchange Server 2003 édition Entreprise prend en charge jusqu'à 5 groupes de stockage dont 1 qui est dédié uniquement à la récupération de groupe de stockage.
Chaque groupe de stockage a son propre fichier de transactions qui permet de récupérer les informations en cas de défaillance.

Voici quelques conseils concernant la gestion du stockage sous Exchange :

- Préférez créer plusieurs petites banques de boîtes aux lettres ou de dossiers publics plutôt qu'une seule grosse banque. Ceci dans le but de rendre plus facile et moins les restaurations en cas de défaillance
- Evaluez la taille maximale de stockage acceptable pour un groupe de stockage afin de pouvoir sauvegarder aisément vos groupes de stockage.
- Evaluez les boîtes aux lettres critiques et regroupez les dans un groupe de stockage que vous administrerez en conséquences.
- Regroupez les utilisateurs ayant des besoins ou des fonctions similaires au sein de l'entreprise dans un même groupe de stockage. Créez par exemple un groupe de stockage pour chaque département de l'entreprise.
- Afin de gagner en performances et en facilité de gestion, n'hésitez pas, si vous en avez la possibilité, d'assigner un rôle spécifique à chaque serveur Exchange de votre organisation. Un serveur gérera exclusivement les dossiers publics, tandis qu'un autre aura en charge les boîtes aux lettres des utilisateurs.

Concernant la création des groupes de stockage :

- Pour des raisons évidentes de performance, préférez un disque différent pour chaque groupe de stockage et son fichier de transactions. De même, si vous hébergez des groupes de stockages pour différentes entreprises sur vos serveurs Exchange.
- En termes de sauvegardes, regroupez en un même groupe de stockage les données aux besoins identiques si possible.

2.2.2. Configuration des banques de boîtes aux lettres

Dans les propriétés d'une banque de boîtes aux lettres, vous retrouvez un certain nombre d'onglets permettant une administration accrue du stockage :

- **Général :** configuration de la banque de dossiers publics par défaut, et configuration de l'archivage des messages.
- **Base de données :** spécification du disque où est stockée la base de données Exchange contenant les messages, la base de données de streaming pour cette banque. Planification de la maintenance de la banque (sauvegarde) afin de minimiser l'impact sur le travail de vos utilisateurs.
- **Limites :** configuration des limites de stockage, et de taille pour les messages.

2.2.3. Configuration des banques de dossiers publics

Dans les propriétés d'une banque de dossiers publics, vous retrouvez un certain nombre d'onglets permettant une administration accrue du stockage :

- **Base de données :** spécification du disque où est stockée la base de données Exchange contenant les messages, la base de données de streaming pour cette banque. Planification de la maintenance de la banque (sauvegarde) afin de minimiser l'impact sur le travail de vos utilisateurs.
- **Réplication :** spécification des intervalles de réplication pour les dossiers publics vers d'autres serveurs. Spécification de la taille limite de message de réplication à travers les connecteurs.
- **Limites :** configuration des limites de stockage, et de taille pour les messages.

2.2.4. Configuration de la surveillance de services et de ressources

Pour assurer un fonctionnement optimal d'Exchange dans votre entreprise, vous devez vous assurez que le produit bénéficie des ressources matérielles nécessaires, ainsi que l'accès aux bons services. Pour identifier ces différentes ressources, vous devez surveiller votre serveur à l'aide de multiples outils, mais attention à ne pas surcharger le serveur avec l'exécution de ces outils.

Automatiquement, un certain nombre de services sont surveillés par Exchange :
- Microsoft Exchange – Banque d'informations
- Microsoft Exchange – Piles MTA
- Microsoft Exchange – Moteur de routage
- Microsoft Exchange – Service de surveillance du système
- Simple Mail Transfer Protocol (SMTP)
- Service de publication World Wide Web

Après avoir établi une ligne de base de performances, pensez à surveiller les ressources de type mémoire virtuelle disponible, utilisation du processeur, espace disque libre … propres au serveur lui-même.

2.2.5. Configuration des notifications

Lorsque vous avez établi des données de référence pour la surveillance de vos différents composants serveur, vous pouvez paramétrez des notifications afin que vous soyez prévenu lorsqu'une ressource est utilisée anormalement. Effectivement, lorsque vous décidez de surveiller l'activité de votre serveur, il vous est possible de paramétrer celui-ci afin qu'il vous envoie un message ou qu'il exécute un script lorsqu'il dépasse un certain seuil pour une ressource.

2.2.6. Objets et compteurs de performance pour Exchange

Lors de l'installation d'Exchange, celui-ci ajoute de nouveaux objets et compteurs de performances : MSExchangeIS, SMTP Server, MSExchangeAL …

2.2.7. Activation du suivi de message

En activant la fonctionnalité de suivi de message, vous avez la possibilité de voir le chemin emprunté par les messages envoyés aux utilisateurs de votre organisation Exchange ou les messages de vos utilisateurs à destination de l'extérieur. Ceci vous permet alors de déterminer le point de défaillance de remise d'un message par exemple.

Par défaut, cette fonctionnalité est désactivée. Vous pouvez l'activer par une stratégie serveur, ou manuellement sur chaque serveur.

Lorsque vous activez cette fonctionnalité, un fichier journal est créé chaque jour avec les informations de suivi de messages : expéditeur, message, destinataire, objet.
Vous avez également la possibilité d'enregistrer les journaux sur un lecteur spécifique dans le cas d'un manque d'espace disque.

2.2.8. Configuration de l'enregistrement des protocoles

Cette fonctionnalité permet d'enregistrer les commandes envoyées par les protocoles Internet durant une connexion entre un client et votre serveur Exchange. Les informations enregistrées sont les suivantes : adresse IP du client, nom de domaine du client, date et heure du message, nombre d'octets envoyés, et toutes les autres commandes renvoyées par le client.
Le fichier journal créé vous permet alors de diagnostiquer d'éventuelles erreurs de connexions ou de protocoles.

Les différents protocoles supportés par Exchange sont :

- **http :** accès web au serveur Exchange
- **POP3 :** ce protocole stocke les messages d'un utilisateur sur le serveur jusqu'à ce que celui-ci les consulte et donc les récupère localement sur sa machine
- **IMAP4 :** ce protocole permet la consultation des dossiers publics et privés pour un utilisateur et les messages peuvent rester stockés sur le serveur
- **ESMTP/SMTP :** protocole étendu de smtp permettant l'envoi de messages sur Internet
- **NNTP :** protocole utilisé pour la lecture de news.

2.3. Ajout, suppression et mise à jour de serveurs Exchange

L'administration de l'organisation Exchange de votre entreprise vous imposera certainement d'ajouter ou supprimer des serveurs Exchange pour répondre aux différents besoins.

Vous pouvez par exemple ajouter des serveurs physiques ou virtuels afin d'héberger plusieurs protocoles sur un serveur. De même, au fil du temps, vous pourrez être amenés à effectuer des mises à jour de vos serveurs Exchange.

2.3.1. Ajout de serveurs virtuels

Vous aurez peut-être besoin de configurations différentes pour un même protocole. Dans ce cas, vous serez amenés à configurer des serveurs virtuels. Voici différents exemples :

- Vous souhaitez un cryptage différent selon que les clients se connectent localement ou à distance
- Vous pouvez réguler le trafic d'un même protocole sur plusieurs ports afin de répondre à des besoins applicatifs par exemple

2.3.2. Suppression de serveurs

Pour des raisons de maintenance et de sécurité, vous pouvez être amenés à supprimer un serveur. Il existe une procédure adaptée :

- déplacer les dossiers publics et systèmes vers un autre serveur du groupe de routage
- déplacer les boîtes aux lettres vers un autre serveur du groupe de routage
- supprimer le serveur d'Active Directory

2.3.3. Suppression du 1er serveur d'un groupe de routage

Le 1er serveur d'un groupe de routage détient des rôles importants. En effet, il est souvent consulté par les autres serveurs du groupe pour les informations suivantes : carnet d'adresses hors connexion, calendrier et autres informations système. Il est donc important de transférer ces rôles avant de supprimer le serveur en question.

Voici la procédure :

- transférer tous les dossiers publics et systèmes à un autre serveur Exchange du même groupe de routage
- transférer le service de mise à jour de destinataire à un autre serveur Exchange du domaine
- si ce serveur est *Maître de groupe de routage*, transférer ce rôle à un autre serveur
- si ce serveur exécute le service de réplication de site pour communiquer avec un serveur Exchange 5.5, créer à nouveau ce service.
- si ce serveur héberge des connecteurs particuliers, penser à transférer ces connecteurs à un autre serveur
- enfin, insérer le CD-Rom d'Exchange Server 2003 pour supprimer tous les composants.

3. Sécurisation d'Exchange Server 2003

3.1. Préparation et Protection du serveur contre les attaques virales

Aujourd'hui, les attaques virales sont incessantes et de divers formes. Les virus peuvent être diffusés en pièces jointes à des messages. Lorsque ceux-ci sont ouverts par un utilisateur, ils sont généralement capables d'infecter très rapidement de nombreux fichiers qui transiteront plus tard sur le réseau et infecteront alors d'autres machines.

Les infections peuvent alors se traduire par des problèmes ou lenteurs matérielles.

Les vers, contrairement aux simples virus, n'ont pas besoin de programme hôte pour se répliquer. La diffusion est alors encore plus rapide et plus large.

Les chevaux de troie, quant à eux, se font passer pour ce qu'ils ne sont pas, tel un jeu vidéo par exemple. La diffusion est simple et trompeuse. Les chevaux de troie sont très largement diffusés par messagerie Internet de nos jour.

3.1.1. Comment se diffusent les virus ?

Il est très courant qu'un utilisateur Internet ouvre un pièce jointe ou un fichier téléchargé sur Internet contenant un virus. Le virus est chargé en mémoire dans la machine de l'utilisateur et tente alors d'infecter d'autres programmes de l'utilisateurs.

Si jamais le programme de messagerie est infecté, certains virus sont capables d'utiliser le carnet d'adresses de l'utilisateur pour se diffuser.

3.1.2. Choix d'une stratégie antivirus

Pour protéger votre système de messagerie et vos utilisateurs, il est essentiel de mettre en place une stratégie antivirus adéquate. La stratégie se compose de 3 étapes :

- **Avertissement des utilisateurs :** vous devez vous assurez que vos utilisateurs n'ouvrent pas n'importe quelle pièce jointe provenant d'expéditeurs qui leur sont inconnus.
- **Choix de l'installation antivirus :** vous avez la possibilité de vous protéger des virus de divers manières : antivirus côté client, antivirus côté serveur et antivirus pare-feu.
  Vos utilisateurs ouvrent les pièces jointes et sont directement exposés au danger. Vous pouvez installer une application antivirus sur les postes clients qui analyseront par exemple toutes les pièces jointes des messages arrivant.
  Vous avez également la possibilité de protégér vos utilisateur en amont en installant une application antivirus sur le serveur. L'application analysera les banques de boîtes aux lettres et de dossiers publics et empêchera les virus de se diffuser sur le réseau. Cependant, vous devez installer un antivirus spécialement conçu pour les serveurs Exchange.
  Enfin, vous pouvez installer l'application au niveau du pare-feu de votre entreprise et analyser tout le trafic entrant et sortant.
- **Antivirus à jour :** de nouveaux virus apparaissent chaque jour et il est important de mettre à jour les applications antivirus avec les nouvelles bases de données de virus pour s'en protéger.

3.1.3. Que sont les mises à jour de sécurité ?

Les mises à jour de sécurité permettent de réparer des failles de sécurité de votre système soit créées par des virus, soit exploitées par des virus.

Les mises à jour de sécurité se font souvent par l'intermédiaire d'une interface web.

Soyez prudents, si le système d'exploitation est vulnérable, votre système Exchange le sera également. Il est donc important de faire toutes les mises à jour de sécurité, que ce soit pour votre système Exchange ou pour votre système d'exploitation (Windows Server 2003 par exemple).

3.2. Sécurisation des boîtes aux lettres

3.2.1. Le filtrage de messages pour réduire le nombre de messages commerciaux non sollicités

Les messages commerciaux non sollicité polluent bon nombre de serveurs de messagerie de nos jours. En plus de faire perdre du temps aux utilisateurs, ils consomment un pourcentage de bande passante réseau considérable.

Le processus de filtrage de messages consiste en l'analyse de l'entête et du corps des messages afin de déterminer si le message est légitime ou non, auquel cas, celui-ci peut alors être supprimé.

Outlook 2003, Exchange 2003 et Microsoft Outlook Web Access implémentent plusieurs fonctionnalités de filtrage de messages pour le confort des utilisateurs :

- **Courrier indésirable Outlook :** un certain nombre de filtres existent pour identifier les messages commerciaux non sollicités. Les utilisateurs peuvent alors choisir les expéditeurs fiables ou non, ainsi que les destinataires fiables. Cette fonctionnalité de courrier indésirable est activée par défaut dans Outlook et Microsoft fournit régulièrement des mises à jour de filtres
- **Blocage de contenu Outlook :** vous avez le blocage de contenu activé par défaut qui n'exécutera alors pas de codes malicieux cachés dans les messages et désactivera le téléchargement de code HTML par exemple.
- **Filtrage Exchange :** vous pouvez configurer un certain nombre de règles dans votre organisation Exchange qui permettront de filtrer les messages selon leur entête par exemple. Pour cela, vous devez configurer l'objet *Remise de messages* puis configurer SMTP pour utiliser ces filtres globaux.

Vous pouvez utiliser les listes de blocage qui recensent des noms de domaines et des adresses IP connus pour envoyer des messages commerciaux en masse. Vous pouvez créer une liste vous-même ou vous abonner à une liste fournie par un organisme extérieur. Vous devez alors configurer votre Exchange pour qu'il utilise les services d'une société tiers.
Cependant, certains messages légitimes peuvent être bloqués dans le cas d'erreurs dans cette liste.

Une autre fonctionnalité d'Exchange 2003 concerne le filtrage de connexion qui vérifie les adresses IP des serveurs SMTP se connectant à votre serveur avec la liste de blocage. Effectivement lorsqu'une connexion est établie avec votre serveur Exchange qui regarde la liste de blocage, celui-ci vérifie l'adresse IP correspondant au nom DNS pour vérifier si ce n'est pas une adresse habituellement bloquée.
Vous pouvez configurer plusieurs règles de filtrage qui seront lues dans l'ordre dans lequel elles apparaissent. Vous pouvez également configurer plusieurs règles pour une même adresse, dans le cas où vous avez plusieurs listes de blocage par exemple.
Vous avez aussi la possibilité de créer une liste d'exceptions.

3.2.2. Le filtrage de destinataires et d'expéditeurs

Vous avez plusieurs possibilités de filtrer les messages : par connexion, par domaines, expéditeurs … Vous pouvez également créer des listes pour accepter ou refuser les messages selon expéditeurs et destinataires. Pour cela, vous devez configurer l'objet *Remise de message* pour créer des listes selon chaque serveur virtuel.

Filtrage de destinataires : en configurant cette fonctionnalité, vous pouvez rejeter les messages adressés à des utilisateurs n'existant pas dans votre annuaire Active Directory, les messages adressés à un nombre défini d'utilisateurs ou dont l'expéditeur n'a pas le droit d'écrire à tel ou tel utilisateur.

Filtrage d'expéditeur : vous pouvez rejeter les messages de certains expéditeurs précis, ou les message qui n'ont pas d'expéditeur.

3.3. Implémentation de la signature numérique et du cryptage

3.3.1. Définitions du cryptage et de la signature numérique

Les systèmes de messagerie ont besoin d'être sécurisés, mais également les transmissions entre les différents expéditeurs et destinataires.

La signature numérique certifie à un destinataire de message que l'expéditeur est bien celui qu'il prétend être. Un code numérique est apposé au message lors de son envoi et certifie au destinataire que le message provient bien d'une source sûre et qu'il n'a pas été modifié lors de son transfert.

Vous avez également la possibilité de crypter le contenu d'un message afin de le rendre illisible pour les personnes désirant intercepter le message lors de son transfert sur le réseau. Pour implémenter le cryptage, Exchange utilise l'infrastructure de clé publique / clé privée : la clé publique est connue par tous, tandis que la clé privée n'est détenue que par le destinataire du message qui pourra alors lire le contenu du message.

Exemple : John souhaite envoyer un message crypté à Sarah. Il va utiliser la clé publique de Sarah pour crypter le message. La seule clé privée qui sera capable de décrypter le message sera celle de Sarah qui n'est détenue que par elle.

3.3.2. Définition d'une infrastructure de clé publique (PKI)

Une infrastructure de clé publique est un ensemble de composants permettant la gestion du cryptage d'informations ainsi que la garantie de l'identité d'un utilisateur.
Cette infrastructure s'appuie sur 2 clés (clé publique, clé privée) et permet de sécurises les communications Exchange.

3.3.3. Composants de PKI pour la signature numérique et le cryptage

Voici une liste des différents composants utilisés pour signature numérique et cryptage :

- **Certificat numérique :** authentifie utilisateurs et ordinateurs
- **Modèles de certificats :** il existe des modèles prédéfinis de certificats pour divers utilisation, dont les signatures numériques et le cryptage de messages
- **Liste de révocation de certificats :** liste des certificats révoqués par une autorité de certification
- **Points de publication de certificats :** ces points rendent disponibles au public les certificats

- **Outils de gestion de certificats :** ils permettent de gérer les autorités de certification et les certificats délivrés ou à délivrer
- **Serveurs de certificats :** ils permettent de créer, délivrer et gérer les certificats.

Les processus de délivrance de certificats sont identiques à ceux utilisés pour d'autres services, tel que l'utilisation d'IPSec. (l paire de clés est générée pour un utilisateur, celui-ci fait la demande de certificat auprès d'une autorité, l'administrateur accepte la demande et l'autorité crée le certificat pour le délivrer à l'utilisateur).

3.4. Configuration de pare-feu

Le pare-feu est utilisé afin d'interdire l'accès d'un réseau à un utilisateur non autorisé. Ceci permet de protéger votre réseau de l'extérieur. Vous pouvez ainsi par exemple, analyser les messages entrants et sortant de votre entreprise et les traiter selon des règles bien précises.

Vous pouvez configurer votre pare-feu pour filtrer les paquets et en tant que serveur proxy afin de masquer vos adresses réseau.
Une autre possibilité consiste à filtrer les ports TCP utilisés par vos applications. Ceci permet de réduire et limiter les différents types de trafic sur votre réseau et provenant de l'extérieur.

3.4.1. Les ports utilisés par Exchange

La liste des ports utilisés par Exchange est relativement longue. Effectivement les protocoles utilisés par Exchange sont variés. Cependant, il est intéressant de filtrer que les ports que vous utilisez réellement et de rejeter tout le reste du trafic à destination des autres ports.

Voici la liste des ports :

25	SMTP
80	HTTP
88	Protocole d'authentification Kerberos
102	MTA – X400
110	POP3
119	NNTP
135	RPC
143	IMAP
389	LDAP
443	HTTP (SSL)
563	NNTP (SSL)
636	LDAP (SSL)
993	IMAP4 (SSL)
995	POP3 (SSL)

3.4.2. Ports IIS utilisés par Exchange

Avant d'installer Exchange, vous devez installer IIS avec les protocoles HTTP, SMTP et NNTP. Une fois l'installation d'Exchange faite, celui-ci peut manipuler ces protocoles et ajoute encore 2 protocoles qui sont POP3 et IMAP4.

Ces protocoles d'accès Internet sont alors utilisés par les clients pour se connecter à votre organisation Exchange.

HTTP fournit aux clients Microsoft Outlook Web Access et Outlook Mobile Access.

SMTP est le protocole par défaut utilisé pour l'envoi de messages au sein même de l'organisation et sur Internet.
NNTP donne des accès publics et privés aux groupes de news.
POP3 et IMAP4 sont 2 protocoles permettant la récupération de messages pour les clients. Ils seront détaillés plus loin dans cet essentiel.

3.4.3. Connexion de client MAPI

Lorsque vous paramétrez un pare-feu sur votre réseau, vous devez définir une configuration particulière permettant la connexion de vos clients Outlook au serveur Exchange de l'entreprise et à Active Directory.

Voici les différentes possibilités :
- **Ports statiques**
- **RPC sur http**
- **Connexion VPN**
- **Configuration d'ISA Server**

3.4.4. Recommandations pour la connexion de client MAPI

Avec Exchange 2003 s'exécutant sur Windows Server 2003, vous avez la possibilité de configurer RPC sur http ce qui évite de paramétrer une connexion VPN pour la connexion directe d'un client à un serveur Exchange en passant par Internet.

Lorsque vous paramétrez cette connectivité, vous configurez un serveur Exchange frontal qui va agir en tant que serveur proxy RPC. Ce proxy va spécifier les à utiliser pour communiquer avec les contrôleurs de domaine, serveurs de catalogue global et les autres serveurs Exchange clients RPC.

Lors du déploiement de RPC, vous avez 2 configurations possibles :
- **Le serveur proxy RPC derrière le pare-feu de votre entreprise :** c'est le déploiement le plus recommandé. Effectivement, vous pouvez installer ISA Server sur le réseau périphérique de votre entreprise et celui se chargera d'ouvrir les ports nécessaires au trafic RCP sur http. Votre serveur proxy, lui, derrière le pare-feu sera protégé et pourra ouvrir tous les ports nécessaires aux communications Exchange
- **Le serveur proxy RPC dans le réseau périphérique :** Dans ce cas, il est impératif de limiter le nombre de ports ouverts sur votre serveur proxy pour les communications Exchange.

3.5. Configuration des autorisations d'administration

3.5.1. Que sont les groupes administratifs ?

Les groupes administratifs regroupent un ensemble d'objets ayant des besoins communs en terme d'administration. Ils regroupent les serveurs, groupes de routage, stratégies et hiérarchies de dossiers publics.

En répartissant les serveurs et autres objets Exchange dans différents groupe administratifs, il est plus aisé de répartir des tâches et déléguer l'administration à différents administrateurs de l'entreprise.

3.5.2. Où est ajouté un nouveau serveur Exchange ?

Lorsque vous installé un nouveau serveur Exchange, celui-ci est automatiquement ajouté à un groupe administratif :

- Si c'est votre premier serveur Exchange, celui crée automatiquement le conteneur *Premier groupe administratif* et ajoute le serveur à celui-ci
- Si un seul groupe administratif existe, chaque nouveau serveur sera automatiquement ajouté à ce groupe
- Si vous avez plusieurs groupes administratifs, il vous sera demandé durant l'installation de choisir le groupe administratif dans lequel vous souhaitez ajouter le nouveau serveur.

3.5.3. Configurer les autorisations d'administration

Grâce aux assistants de délégation d'administration, vous avez la possibilité de définir des autorisations à des utilisateurs ou groupes d'utilisateurs pour administrer certains objets Exchange.

Cet assistant peut être démarré à partir de l'objet *Organisation* afin de définir des autorisations sur tous les objets de l'organisation ou à partir d'un objet *Groupe administratif* afin de gérer tous les objets d'un groupe administratif particulier.

Comme nous l'avons déjà vu, il existe 3 autorisations : **Administrateur total Exchange, Administrateur Exchange** et **Administrateur d'Exchange en lecture seule.**
Par contre, la dernière autorisation n'est pas disponible par défaut dans le gestionnaire système Exchange. Vous pouvez retrouver cette autorisation grâce à l'outil adsiedit.exe.

De plus, si vous donnez l'autorisation à un utilisateur de modifier des objets Exchange, il est nécessaire que cet utilisateur soit administrateur local de la machine où est installé Exchange.

Enfin, lorsque vous installé Exchange, deux groupes sont automatiquement créés :

- **Exchange Domain Servers**
- **Exchange Enterprise Servers**

Ces deux groupes permettent aux serveurs Exchange d'accéder à la configuration Exchange et les informations de destinataires dans Active Directory. Ils ne doivent pas être utilisés pour donner d'autres autorisations à des groupes ou utilisateurs de votre organisation.

3.5.4. Modifier et empêcher l'héritage

Pour des raisons de sécurité, vous pouvez être amené à désactiver l'héritage des autorisations. En effet, lorsque vous créez par exemple un groupe de routage dans un groupe administratif, le groupe de routage hérite des autorisations définies au niveau du groupe administratif.
Pour diverses raisons, vous pouvez désactiver l'héritage afin de définir des autorisations différentes pour le groupe de routage en question.

3.6. Services requis pour exécuter Exchange Server 2003

3.6.1. Services utilisés par Exchange 2003

Un serveur Exchange a besoin de communiquer avec d'autres serveurs Exchange, des contrôleurs de domaine et différents clients. Un certain nombre de composants et services sont alors nécessaire pour l'exécution correcte de toutes ces tâches et connexions.

Pour chaque environnement de fonctionnement, les services nécessaires sont différents, voici un tableau récapitulatif :

Installation	SMTP, NNTP, Service de publication World Wide Web, Service d'admin IIS
Administration	Microsoft Exchange – Surveillance du système, Gestion de Microsoft Exchange, Windows Management Instrumentation
Routage	Microsoft Exchange – Moteur de routage, Service d'Admin IIS, SMTP
Compatibilité avec les versions précédentes	Microsoft Exchange – Service Evénement, Microsoft Exchange – Service de réplication de sites, Microsoft Exchange – Piles MTA
Fonctionnalités supplémentaires	Microsoft Search, Service de publication World Wide Web

3.6.2. Pourquoi limiter les services ?

Pour chaque étape et rôle de votre serveur Exchange, différents services sont requis. Certains peuvent alors certainement être désactivés dans certains cas.

Ceci permet une amélioration des performances pour votre serveur mais cela permet également de désactiver l'accès à certains ports de votre serveur, et donc de protéger votre serveur d'éventuelles attaques.

3.6.3. Services requis sur un serveur Exchange frontal

Dans le cas d'un serveur Exchange frontal, c'est celui-ci qui va accepter les différentes connexions de clients et il va alors transmettre les requêtes à traiter à des serveurs Exchange arrière.

Certains services peuvent alors être désactivés.

Voici la liste des services minimums dans le cas où vous devez activer *Outlook Web Access* sur votre serveur frontal :

- **Microsoft Exchange – Moteur de routage**
- **Services IPSec**
- **Service d'admin IIS**
- **Service de publication World Wide Web**

Les autres services lies à Exchange peuvent alors être désactivés.

Si vous souhaitez activer les connexions POP3, IMAP4 ou SMTP, les services correspondant sont alors nécessaires.

3.6.4. Services requis sur un serveur Exchange arrière

Voici maintenant les services que vous pouvez désactiver sur un serveur Exchange arrière :

- **Microsoft Exchange – IMAP4**
- **Microsoft Exchange – POP3**
- **Microsoft Search**
- **Microsoft Exchange – Service Evénement**
- **Microsoft Exchange – Service de réplication de sites**
- **Localisateur d'appels de procédure distante (RPC)**
- **NNTP**

4. Gestion des destinataires

4.1. Les destinataires Exchange

4.1.1. Les types de destinataires Exchange

Les destinataires Exchange sont des objets Active Directory utilisés par Exchange pour leur délivrer des messages. Il existe 3 types de destinataires :

- **Les destinataires utilisateur :** parmi ces utilisateurs, on distingue encore 2 catégories. La 1ère catégorie « utilisateur avec boîte aux lettres » concerne les utilisateurs Active Directory ayant une boîte aux lettres Exchange et une adresse de messagerie. Ils peuvent envoyer et recevoir des messages par l'intermédiaire de l'infrastructure Exchange. La 2nde catégorie « utilisateur de messagerie » concerne les utilisateurs ayant une boîte aux lettres extérieure à votre organisation Exchange. Les adresses peuvent êtres listées dans les listes d'adresses globales (GAL) mais ces utilisateurs n'utilisent pas l'organisation Exchange pour recevoir et envoyer des messages. Leur adresse de messagerie est liée à leurs identifiants Windows.
- **Les destinataires contact :** ce sont des destinataires n'ayant pas d'accès spécifiques à votre réseau et donc votre organisation Exchange. Il est intéressant d'inclure des adresses de messagerie de contacts extérieures dans les listes d'adresses Exchange parfois pour que vos utilisateurs internes retrouvent rapidement les adresses de différents contacts externes (partenaires, clients …).
- **Les destinataires groupe :** il est possible de définir des adresses de messagerie pour des groupes Active Directory. La condition réside toutefois dans le fait que chaque utilisateur faisant partie du groupe en question est une adresse de messagerie valide. Par exemple, pour le groupe de comptabilité de l'entreprise Supinfo.com, il est plus facile d'envoyer un message à l'adresse comptabilite@supinfo.com plutôt qu'à chaque membre du groupe individuellement. Le message sera alors distribué automatiquement à chaque membre du groupe. Dans ces listes, vous pouvez ajouter des destinataires utilisateurs et des contacts.

4.1.2. Les types de groupe et étendue Active Directory

Au niveau d'Active Directory, nous savons déjà qu'il existe 2 types de groupe :

- **le groupe de sécurité :** ce groupe est utilisé afin de donner des accès aux différentes ressources de l'entreprise à des utilisateurs. Vous pouvez utiliser ce type de groupe pour la messagerie et pour définir des autorisations sur des dossiers publics.
- **Le groupe de distribution :** vous ne pouvez pas utiliser ce type de groupe pour donner des accès particuliers à des ressources de l'entreprise. Cependant ce groupe sera utilisé pour l'envoi de messages à des groupes d'utilisateurs.

Concernant les étendue, nous avons toujours les mêmes, mais cette-fois ci il est important de comprendre l'impact des étendues sur l'utilisation d'Exchange pour les utilisateurs :

- **Groupe de domaine local et groupe global:** le contenu de ces groupes n'étant pas publié au niveau du serveur de catalogue global, les utilisateurs Exchange ne pourront pas voir les contacts et utilisateurs inclus dans ces groupes si ils ne font pas partie du domaine dans lequel ces groupes ont été créés.
- **Groupe universel :** le contenu de ce groupe est publié dans tous les serveurs de catalogue global de la forêt. Les utilisateurs de tous les domaines de la forêt pourront alors voir les différents contacts et utilisateurs inclus dans ce groupe. Dans un forêt disposant de nombreux domaines, il est alors recommandé d'utiliser des groupes universels.

Afin de pouvoir utiliser tout de même les groupes globaux et de domaine local dans un environnement multi-domaines, vous devez installer un serveur d'expansion dans chaque domaine où est créé ce type de

groupe. Ce serveur aura pour objectif de résoudre le contenu de tels groupes lorsque ces groupes ne font pas partie du même domaine que l'utilisateur qui en fait la demande.

4.1.3. Les différentes tâches Exchange concernant les destinataires

Dans la console *Utilisateurs et Ordinateurs Active directory*, vous disposez d'un assistant Exchange pour effectuer un certain nombre de tâches d'administration :

- Créer ou supprimer une boîte aux lettres
- Créer ou supprimer une adresse de messagerie
- Déplacer une boîte aux lettres
- Cacher ou non le contenu d'un groupe
- Configurer certaines fonctionnalités Exchange
- Supprimer des attributs Exchange

4.2. Création, modification et suppression des utilisateurs et contacts

4.2.1. Création d'une boîte aux lettres

Pour permettre à un utilisateur d'envoyer et recevoir des messages grâce à votre organisation Exchange, il est nécessaire de créer une boîte aux lettres pour cet utilisateur. Pour cela, 2 possibilités s'offrent à vous :

- Si vous créez un utilisateur, à partir d'un ordinateur ayant le gestionnaire système Exchange d'installé, une boîte aux lettres sera automatiquement créée si un serveur Exchange fait partie de la même forêt Active Directory
- Si vous souhaitez créer une boîte aux lettres pour un utilisateur existant, un assistant vous demandera de spécifier le serveur Exchange, le groupe de stockage et la banque de boîte aux lettres pour la boîte aux lettres de cet utilisateur.

Dans les propriétés de compte d'utilisateurs, de nouveaux onglets spécifiques à Exchange apparaissent alors et vous permettent alors d'affiner la configuration Exchange pour cet utilisateur.

Lorsque vous créez une boîte aux lettres pour un utilisateur, un alias est automatiquement créé à partir du nom d'utilisateur. Par défaut, l'adresse de messagerie créée pour un utilisateur sera de type *alias@nomdedomainepleinementqualifié.xyz*
Vous avez la possibilité de paramétrer la création automatique d'adresses SMTP.

4.2.2. Suppression d'une boîte aux lettres

A l'aide de l'assistant Exchange de la console *Utilisateurs et Ordinateurs Active Directory*, vous pouvez supprimer une boîte aux lettres.
Dans un premier temps, celle-ci sera juste déconnectée et pourra alors être restaurée à tout moment. A la fin de la période de rétention définie dans les propriétés de la banque de boîtes aux lettres, cette boîte aux lettres sera réellement supprimée.

Par défaut, cette période de rétention (laps de temps pendant lequel une boîte est désactivée avant d'être supprimée) est de 30 jours.

4.2.3. Modification des alias et adresses de messageries pour les destinataires

Ce type de modification intervient généralement lorsqu'un utilisateur change de nom. Effectivement, imaginons que Barbie Matel change de nom pour s'appeler Barbie Ken. Il est nécessaire qu'elle ait une nouvelle adresse de messagerie reflétant son nom, mais elle ne doit pas perdre les mails encore envoyés à son ancienne adresse.

Il est possible de définir plus adresses de messagerie SMTP. Dans le cas ci-dessus, nous allons garder l'adresse barbie.matel@mydomain.com et ajouter une nouvelle adresse SMTP barbie.ken@mydomain.com . Elle recevra toujours les messages à l'ancienne adresse, mais lorsqu'elle répondra aux messages, ou lorsqu'elle enverra de nouveaux messages elle utilisera l'adresse SMTP barbie.ken@mydomain.com , et les utilisateurs prendront note de cette nouvelle adresse petit à petit.

4.2.4. Cacher des boîtes aux lettres

Par défaut, tous les destinataires Exchange apparaissent dans les listes d'adresses Exchange. Cependant, il peut être nécessaire de masquer une boîte aux lettres qui est utilisés pour des tâches spécifiques par exemple.

Lorsque vous masquez une boîte aux lettres, celle-ci est toujours accessible par son adresse de messagerie SMTP, mais par contre elle n'apparaît plus dans les listes d'adresses Exchange. De même, les utilisateurs de l'entreprise ne pourront plus résoudre l'adresse de messagerie en entrant simplement l'alias de cette boîte aux lettres dans le champ destinataire « A… » de Outlook.

4.2.5. Reconnecter une boîte aux lettres à un compte Active Directory

Nous avons vu que par défaut une boîte aux lettres est d'abord déconnectée durant 30 jours lorsque l'on décide la supprimer.

Pendant cette période de rétention, vous pouvez restaurer la boîte aux lettres, mais vous pouvez aussi décider de la reconnecter à un autre compte utilisateur Active Directory qui n'a pas déjà de boîte aux lettres.

Cette procédure s'effectue à partir du gestionnaire système Exchange.

4.3. Administration des boîtes aux lettres

4.3.1. Configuration des limites de stockage

Il est important de paramétrer des limites de stockage pour les boîtes aux lettres des utilisateurs pour diverses raisons :

- Economie d'espace disque sur les serveurs Exchange
- Temps de sauvegarde et de restauration des banques de boîtes aux lettres
- Maintenance des serveurs

Vous pouvez également paramétrer des messages d'avertissement qui seront envoyés sous forme de notifications à vos utilisateurs. Il existe 3 types de notification :

- **Avertissement :** signale juste à un utilisateur que sa boîte aux lettres est pleine
- **Envoi interdit :** l'utilisateur ne peut plus envoyer de messages

- **Envoi et réception interdits :** l'utilisateur ne plus ni envoyer, ni recevoir de messages tant que sa boîte aux lettres sera aussi grosse.

Vous pouvez paramétrer ces limites sur chaque boîte aux lettres individuellement, ou sur des banques de boîtes aux lettres. De même, afin de faciliter l'administration, il vous est possible de paramétrer des stratégies de banques de boîtes aux lettres.

4.3.2. « Envoyer de la part de » et « Envoyer en tant que »

Pour une raison ou une autre, vous souhaiteriez que votre assistant puisse envoyer du courrier à votre place. Il est possible de paramétrer ceci de 2 manières :

- **Envoyer de la part de :** les destinataires recevront un message dont l'expéditeur sera « Assistant de la part de Manager »
- **Envoyer en tant que :** les destinataires recevront un message dont l'expéditeur sera « Manager ». Les destinataires ne sauront donc pas que c'est votre assistant qui a envoyé un mail à votre place.

Afin de paramétrer ceci, il suffit d'aller dans les propriétés du compte utilisateur (dans *Utilisateurs et Ordinateurs Active Directory*) pour lequel vous voulez déléguer l'envoi de courrier.

4.3.3. Autorisations sur les boîtes aux lettres

Si les autorisations précédentes ne suffisent pas et que vous souhaitez déléguer d'autres tâches à d'autres personnes sur différentes boîtes aux lettres, il est possible également de le paramétrer à partir d'Active Directory.

4.3.4. Déplacement de boîtes aux lettres

Plusieurs raisons peuvent vous pousser à déplacer une ou plusieurs boîtes aux lettres : changement de service d'un employé, équilibrage de charge entre différents serveurs, …

Pour déplacer une boîte aux lettres, vous devez être administrateur sur le serveur source, ainsi que sur le serveur cible. 2 outils sont à votre disposition :

- **L'assistant de Tâches Exchange :** outil vous permettant de déplacer des boîtes aux lettres au sein de la même organisation Exchange
- **Exmerge.exe** : dans le cas de déplacement de boîtes aux lettres et de fusions de données de boîtes aux lettres entre différentes organisations Exchange. Cet outil est également intéressant pour extraire des messages par exemple d'une banque de boîtes aux lettres endommagée et les réimporter dans une banque saine.

4.3.5. Configuration d'une adresse de transfert

Cette fonctionnalité est intéressante dans le cas où un utilisateur souhaiterait par exemple centraliser tous ses messages sur un compte externe. Tous les messages reçus à son adresse Exchange seront automatiquement transférés à une autre de ses adresses (ex : hotmail).

Attention : les messages transférés ne bénéficient alors plus de la sécurité implémentée dans votre organisation Exchange.

4.4. Administration des groupes de distribution

4.4.1. Création de groupes de distribution à partir de requêtes

Le groupe de distribution basé sur une requête est une nouveauté Exchange 2003. Ces groupes bénéficient des mêmes fonctionnalités que les groupes de distribution classiques.

La différence réside dans le fait que les utilisateurs faisant partie d'un groupe de distribution basé sur une requête sont assignés dynamiquement à ce groupe et non plus statiquement. Effectivement lors de la création d'un tel groupe, il vous suffit par exemple de spécifier que ce groupe contiendra tous les employés du département comptabilité. A chaque fois qu'un nouvel employé arrivera dans le département comptabilité, il sera automatiquement ajouté au groupe de distribution basé sur une requête.

Ce type de groupe simplifie et réduit grandement l'administration des groupes de distribution. Néanmoins, ce type de groupe est coûteux en termes de performances. Effectivement, chaque fois qu'un mail est envoyé à ce type de groupe, une requête LDAP est exécutée sur le serveur.

4.4.2. Limiter l'accès aux groupes de distribution

Vous pouvez restreindre le nombre de personnes autorisées à envoyer des messages ou à recevoir des messages d'un groupe de distribution.
De même, il est possible de cacher un groupe de distribution de sorte à ce que celui-ci n'apparaisse pas dans les listes d'adresses Exchange.

5. Gestion des dossiers publics

5.1. Gestion des données de dossier public

5.1.1. Que sont les dossiers publics ?

Les dossiers publics peuvent regrouper un certain nombre d'informations telles que des messages, des documents ou des fichiers multimédia. Ce contenu peut alors être accédé grâce aux protocoles NNTP et HTTP pour les utilisateurs externes à l'organisation mais aussi par les utilisateurs internes de l'organisation Exchange.

Les dossiers publics sont situés dans des banques de dossiers publics. Ils sont présentés sous forme d'arborescence de dossiers publics dans une application cliente telle qu'Outlook pour vos utilisateurs. On peut alors parler de dossier parent contenant des dossiers enfants.

Avec le gestionnaire système Exchange, vous avez le contrôle total des dossiers publics. Avec Outlook 2003, vous avez accès à la création et à la configuration basique des dossiers publics.

5.1.2. Quel est l'intérêt des dossiers publics ?

Les dossiers publics sont utilisés dans un but de partage d'informations entre utilisateurs. Ils sont alors utilisés pour le travail collaboratif ou en tant que groupes de discussion.
Les utilisateurs de votre organisation Exchange peuvent accéder à ces dossiers publics grâce à un client MAPI tel qu'Outlook.

Les utilisateurs ne faisant pas partie de votre domaine Active Directory peuvent quant à eux accéder à ces dossiers grâce aux protocoles http et nntp. Dans ce cas, vous devez donner un accès anonyme possible aux dossiers publics.

Les dossiers publics permettent alors :
- envoyer des messages vers des dossiers publics
- poster des messages directement dans les dossiers publics
- stocker des dossiers publics dans plusieurs arborescences différentes
- accéder aux dossiers publics à l'aide d'un navigateur web et d'une simple URL
- activer la recherche de texte intégral sur le contenu des dossiers publics
- avoir un accès public à des ressources d'entreprise

5.1.3. Quelles sont les autorisations de dossiers publics ?

Les autorisations permettent aux utilisateurs de créer, gérer et utiliser le contenu des dossiers publics. Ces autorisations sont soit affectées par l'administrateur, soit obtenues par héritage de permissions.

L'héritage des autorisations a lieu de la manière suivante :
- pour les dossiers publics de 1er niveau, les autorisations sont héritées des autorisations présentes sur le groupe administratif contenant le dossier
- pour les dossiers publics enfants, les autorisations sont héritées du dossier parent (dossier de 1er niveau)

En tant qu'administrateur Exchange, il vous incombe de définir les autorisations pour vos différents utilisateurs lorsque vous créez un dossier public.

Il existe 3 types d'autorisations pour les dossiers publics :

- **Autorisations clientes :** permet de contrôler les utilisateurs accédant aux dossiers publics
- **Droits d'annuaire :** permet de contrôler les utilisateurs pouvant manipuler un dossier public stocké dans Active Directory
- **Droits administratifs :** permet de déléguer des tâches d'administration à d'autres utilisateurs ou administrateurs de l'entreprise, comme par exemple la réplication de dossiers publics.

5.1.4. Types d'arborescences de dossiers publics

Il existe 2 types d'arborescences :

- **l'arborescence de dossier public par défaut :** cette arborescence est créée automatiquement lors de l'installation du 1er serveur Exchange de votre organisation. Il est trouvable dans Outlook en tant que **Tous les dossiers publics**. Cette arborescence est répliquée sur chaque serveur Exchange contenant une banque de dossiers publics associée à cet arbre.
- **L'arborescence de dossier public à contenu général :** ce sont des arborescences que vous créez par la suite. Le processus de réplication est identique à celui utilisé par l'arborescence de dossier public par défaut.

Il est conseillé d'utiliser le second type d'arborescence lorsque vous souhaitez faciliter le travail collaboratif selon les centres d'intérêts ou fonctions des différents employés de l'entreprise.

Les 2 arborescences peuvent être consultées par les clients http et nntp. Par contre, seule l'arborescence par défaut peut être consultée par des clients MAPI (Outlook 2003).

5.1.5. Configuration des autorisations pour accéder aux dossiers publics

Par défaut, tous les utilisateurs ont les autorisations d'Auteur dans l'arborescence de dossiers publics par défaut. Par contre, vous avez la possibilité de modifier ces autorisations clientes.
Cependant, pour modifier des autorisations sur les arborescences de dossiers publics à contenu général, vous devez passer par le gestionnaire système Exchange, car vous ne pouvez pas vous connecter à ces arborescences avec Outlook.

Lorsque vous décidez d'affecter des autorisations sur l'arborescence par défaut, vous affecter en fait un rôle avec en ensemble d'autorisations prédéfinies.
En revanche, pour les arborescences à contenu général, ce sont des autorisations similaires aux autorisations Windows.

Les autorisations fonctionnent selon les principes suivants :

- si l'on définit des autorisations pour un utilisateur sur un dossier public, seulement ces autorisations seront appliquées pour cet utilisateur
- si un utilisateur fait partie d'un groupe de sécurité ayant des autorisations définies sur un dossier public, les autorisations effectives de l'utilisateur seront les moins restrictive entre les autorisations du groupe et les autorisations par défaut sur le dossier public

5.2. Gestion de l'accès réseau aux dossiers publics

5.2.1. Qu'est-ce que la réplication de dossier public ?

Lorsque vous créez un dossier public dans votre organisation, vous pouvez choisir de n'en garder qu'une copie, ou d'en avoir plusieurs copies (répliquas).

Le processus de réplication de dossiers publics s'appuie sur les mêmes protocoles et connecteurs utilisés au sein de votre organisation pour envoyer des messages. Vos répliquas peuvent alors être hébergés dans plusieurs banques de dossiers publics sur différents serveurs Exchange de votre réseau local.

Le fait d'avoir plusieurs copies de vos dossiers publics permet d'avoir une tolérance de panne et une répartition de la charge réseau lors de l'accès à ces dossiers.

La réplication Exchange utilise un modèle multi maître, ce qui signifie que tout changement de contenu d'un dossier public sur un serveur entraîne une réplication sur les autres serveurs. Il n'y pas de serveur maître de réplication.

5.2.2. Processus de réplication

Le processus se compose de 4 étapes :

- **La réplication hiérarchique :** cette étape correspond à la réplication de l'arborescence de dossiers publics avec le *Folder ID* (FID) pour tous les dossiers liés à toutes les banques de dossiers publics de l'organisation Exchange.
- **La réplication du contenu :** cette étape constitue la réplication du contenu des dossiers publics.
- **Le retour de réplication :** cette étape permet de vérifier les banques de dossiers publics qui auraient raté une mise à jour, une synchronisation avec les autres banques. Lorsqu'une banque est repérée comme n'étant pas à jour, un retour de réplication a lieu pour mettre à jour cette banque.
- **Résolution de conflit de contenu :** lorsqu'un même objet est modifié par 2 utilisateurs sur 2 serveurs différents simultanément, nous rentrons en situation de conflit. Il existe précisément 2 types de conflit :
  - conflit de message : lorsqu'un message est modifié simultanément sur 2 répliquas différents, il y a conflit et un message est envoyé au contact responsable du dossier afin que celui-ci choisisse la version à conserver
  - conflit de dossier : lorsque les paramètres d'un dossier sont modifiés simultanément sur 2 répliquas différents. La toute dernière sauvegarde des paramètres est prise en compte et écrase les précédentes.

5.2.3. Comment les clients se connectent-ils aux dossiers publics ?

Lorsqu'un client désire accéder à des données de dossier public, il doit se connecter à un serveur détenant un répliqua de ce dossier public. Ce serveur peut être soit dans le même groupe de routage que le client, mais peut également être dans un autre groupe de routage et dans ce cas, les connexions réseau ne sont pas forcément permanentes.

Dans le cas où le répliqua existe dans le même groupe de routage que le client, celui-ci tentera de trouver le répliqua dans la banque de dossiers publics par défaut associée à sa banque de boîte aux lettres. Si le répliqua ne se trouve pas dans cette banque, le client tentera aléatoirement de se connecter à une autre banque faisant partie du même groupe de routage.

Dans le cas où le répliqua n'existe pas dans le même groupe de routage, le client se connectera à un autre groupe de routage en utilisant les coûts des connecteurs de groupe de routage pour déterminer le groupe vers lequel l'utilisateur doit être redirigé.

En effet, chaque connecteur a un coût (entre 1 et 100) qui lui est associé. Les messages empruntent les chemins ayant les coûts les plus faibles. Lorsqu'un client tente de se connecter à un répliqua, Exchange détermine le chemin le plus rapide pour afficher l'information grâce aux coûts des connecteurs.

Afin que le client soit redirigé d'un groupe de routage à un autre, il est impératif d'indiquer une référence :

- il faut implémenter un connecteur entre 2 groupes de routage. Les connecteurs sont unidirectionnels. Ce qui signifie que si vous souhaitez une communication dans les 2 sens, vous devez configurer 2 connecteurs
- vous pouvez indiquer une liste de références pour être certain que l'utilisateur sera redirigé vers l'un des serveurs de référence.

5.2.4. Qu'est-ce que l'indexage de texte intégral ?

En utilisant le gestionnaire système Exchange, vous pouvez activer l'indexage de texte intégral qui permet à vos clients d'effectuer des recherches plus rapides et plus précises au sein de votre organisation.
Grâce à cette fonctionnalité, vos clients pourront également rechercher du contenu tel que les pièces jointes par exemple (.doc, .xls, .txt …).

La recherche fonctionne également avec des mots apparentés et donc la recherche est élargie en cas d'erreur de frappe dans les termes à rechercher par exemple.

Vous pouvez activer l'index pour chaque banque individuellement. Cependant, ne perdez pas de vue que la création d'un index exploite fortement le processeur et peut prendre un certain nombre d'heures. De même, l'espace disque occupé par l'index peut-être considérable.

5.2.5. Où stocker les fichiers d'indexage de texte intégral ?

Par défaut, les fichiers d'index sont stockés dans le répertoire *Exchsrvr\ExchangeServer_servername* où vous avez installé Exchange.
Pour des raisons de performance et de tolérance de panne, il est conseillé de stocker ces fichiers sur des disques durs en configuration de RAID matériel.

5.3. Publication d'un formulaire Outlook 2003

5.3.1. Que sont les formulaires Outlook ?

Les formulaires Outlook permettent d'uniformiser des informations mises à disposition par les utilisateurs par exemple.
On peut aisément imaginer un formulaire permettant de poster un message dans un dossier public.

Chaque objet Outlook est considéré comme étant un formulaire (contact, message, …).
Il vous est possible d'en personnaliser afin de les rendre disponibles pour d'autres utilisateurs.

Voici les différents formulaires à votre disposition : Contact, liste de distribution, tâche, message, post, rendez-vous, entrée de journal, formulaire de bureau.

5.3.2. Rendre disponible un formulaire pour les autres utilisateurs

Outlook utilise les librairies de formulaire pour stocker les formulaires personnalisés. Celles-ci sont stockées sur le serveur Exchange en tant que dossiers systèmes, qui peuvent être répliqués.

Lorsque vous créez un formulaire, vous avez la possibilité de l'enregistrer dans l'une des 3 librairies suivantes :

- **Librairie de formulaires personnels** : les formulaires créés et stockés dans cette librairie ne sont accessibles que par l'utilisateur local, pour un usage personnel

- **Dossiers Outlook** : les formulaires stockés ici seront accessibles soit par tout le monde par l'intermédiaire d'un dossier public, soit par un seul utilisateur si ils sont dans un dossier privé. On utilise cette méthode pour enregistrer des formulaires dans un dossier particulier.
- **Librairie de formulaires d'organisation** : les formulaires sont stockés sur le serveur et accessibles par tous les utilisateurs de l'organisation. Cette librairie n'existe pas par défaut. Vous devez la créer pour chaque langue nécessaire pour les formulaires.

Afin de rendre disponible un formulaire pour d'autres utilisateurs, il suffit d'en créer un, et de le rendre disponible grâce à Microsoft Outlook Web Access. Vous pouvez également distribuer un formulaire par simple mail.
Dans Outlook, ouvrez le formulaire que vous souhaitez publier. Dans le menu *Outils*, vous trouverez une boîte de dialogue *Publier le formulaire en tant que* et il ne vous reste plus qu'à définir un nom et la librairie dans laquelle vous souhaitez stocker le formulaire.

6. Gestion des listes d'adresses

6.1. Une liste d'adresses, c'est quoi ?

6.1.1. Introduction aux listes d'adresses

Le but d'une liste d'adresse est de faciliter la recherche de destinataires dans votre organisation. Il n'est donc pas nécessaire de connaître l'adresse de messagerie du destinataire mais de consulter la liste d'adresses. De plus, si les différents attributs des utilisateurs sont remplis, certains clients de messagerie (Outlook, par exemple) vous permettent d'afficher d'autres informations comme le numéro de téléphone ou l'adresse d'une personne.

Une liste d'adresse est une collection de destinataires fondée par une requête LDAP. Une liste d'adresse peut donc contenir les éléments suivants :

- Utilisateurs
- Contacts
- Groupes
- Dossiers publics

Etant basé sur une requête LDAP, un liste d'adresse est un élément dynamique basé sur des attributs permettant d'administrer l'organisation des objets Active Directory possédant une adresses e-mail afin d'en simplifier la recherche.

6.1.2. Quand doit-on utiliser les différents types de listes d'adresses

Depuis Exchange 2000, quatre types de listes d'adresses sont disponibles :

- **Listes d'adresses par défaut** : Ces listes d'adresses sont créées automatiquement en se basant sur des attributs spécifiques d'objets Active Directory et sont disponible sans aucune intervention de l'administrateur. Par défaut, vous allez retrouver quatre listes d'adresses : Tous les Contacts, Tous les Groupes, Tous les Utilisateurs et Dossiers Publics. Il est conseillé d'utiliser ces listes si vos utilisateurs ne nécessitent pas une utilisation plus complexe.
- **Liste d'adresse globale** (GAL : Global Access List) : Cette liste contient tous les destinataires Exchange de l'organisation. Les GAL sont fondées à partir de serveurs de catalogue global d'Active Directory puis sont utilisées par les clients Exchange pour adresser des e-mails ou pour trouver des informations relatifs aux destinataires dans l'organisations. Lors de l'installation d'Exchange, la liste d'adresses globale est créée par défaut. Cette liste est utilisée par défaut dans le carnet d'adresses des utilisateurs.
- **Liste d'adresses hors connexion** : Cette liste est disponible aux utilisateurs qui travail en mode déconnecté. A l'aide de ce type de liste d'adresses, un administrateur peut choisir quelles adresses sont disponibles hors connexion. Un utilisateur peut pour sa part préparer ces messages sans être connecter à l'aide des emails disponibles sur le serveur de messagerie. Par défaut la liste d'adresses hors connexion est une copie de la GAL.
- **Liste d'adresses personnalisées** : Vous pouvez créer de nouvelles listes d'adresses personnalisées pour respecter les nécessités de votre organisation. Vous pouvez de ce fait simplifier au maximum la recherche de destinataires en respectant l'organisation des services de votre entreprise par exemple.

6.2. Gestion et personnalisation de liste d'adresses

6.2.1. Pourquoi plusieurs listes d'adresses ?

Votre organisation Exchange peut contenir plusieurs milliers d'employés. C'est pourquoi, il est utile de créer vos propres listes d'adresses permettant de limiter le nombre de critères de recherche pour trouver un destinataire.

Il est nécessaire de créer des listes d'adresses globales quand vous souhaitez :

- Masquer l'affichage de certaines GAL : Vous pouvez modifier les permissions de la liste d'adresses par défaut et créer de nouvelles GAL avec des permissions spécifiques.
- Vous assurer que les différentes sociétés que vous hébergez voient uniquement leurs GAL : La liste d'adresses globale par défaut permet à tous les utilisateurs de voir tous les destinataires Exchange de votre organisation.

Lors de la création de listes d'adresses globales, il est nécessaire de prendre en considération les éléments suivants :

- Vous pouvez utiliser des filtres personnalisés pour vos requêtes LDAP. Exemple : les adresses emails finissant par « @supinfo.com » ou par rapports à des attributs spécifiques.
- Vous pouvez ajouter les dossiers publics que vous avez créé afin qu'ils apparaissent dans votre GAL. Par défaut les dossiers publics ont leur email activé.
- Configurer les permissions spécifiques pour chaque GAL.
- Comprendre quelle liste va apparaître dans le carnet d'adresses. Si vous fournissez plusieurs GAL, une seule d'entre elle serra utilisée par les clients de messagerie. La liste suivante fournit ordre à partir duquel la liste va être sélectionnée :
    - Les listes d'adresses globales auxquelles l'utilisateur a accès (permissions)
    - Les listes d'adresses globales auxquelles l'utilisateur est membre
    - La liste d'adresses globale la plus volumineuse

6.2.2. Personnaliser l'affichage des noms

Il est utile de modifier l'affichage des noms pour respecter les besoins de votre organisation. Par exemple, vous souhaitez afficher la liste des personnes par leur nom suivant de leur prénom. Par défaut, Exchange utilise le champ nom détaillé qui est formaté avec le Prénom, l'initial et le nom.

Dans ce cas vous devez modifier la façon dont est généré cet attribut. Pour ce faire vous devez utiliser le composant logiciel enfichable **ADSI Edit** et le parcourir jusqu'à l'attribut **user-display** (Configuration Container, CN=Configuration., CN=DisplaySpecifiers, CN=40c) et éditer l'élément **createDialog** comme suit %<sn> %<givenName>.

6.2.3. Service de mise à jour de destinataire ?

Le service de mise à jour de destinataire (RUS : Recipient Update Service) est le service qui construit et met à jour les listes d'adresses. Par défaut, RUS questionne Active Directory toutes les minutes afin d'être au courant de toutes les modifications ou ajout liés au contact, groupes ou utilisateurs. De ce fait il tient à jour les listes d'adresses.

Le service de mise à jour de destinataire tient aussi à jour les adresses e-mail des objets Exchange basé sur les stratégies de destinataires.

Par défaut, il existe deux objets RUS :

- **Recipient Update Service (Entreprise Configuration)** : Cet objet construit et met à jour les adresses emails des objets qui sont situés dans la partition configuration d'Active Directory (MTA, Store…).
- **Recipient Update Service (*Nom du domaine*)** : Cet objet existant pour chaque domaine de votre entreprise, met à jour les destinataires s'y trouvant.

Vous pouvez mettre à jour manuellement la liste d'adresse au lieu de patienter la mise à jour planifiée. La mise à jour permet de prendre en compte les modifications apportées à l'appartenance des listes d'adresses. Vous avez la possibilité de forcer la mise à jour des listes en utilisant le service de mise à jour destinataire (RUS).

Lors de l'utilisation du service de mise à jour de destinataire, vous pouvez mettre à jour ou reconstruire totalement la liste d'adresse :

- Mettre à jour : Cette option permet de mettre à jour les listes de destinataires de manière incrémentielle depuis la dernière mise à jour.
- Reconstruire : Cette option permet de vérifier toutes les listes d'adresses. Il faut utiliser cette option lors d'une modification de la stratégie de destinataires afin d'accélérer les changements d'adresse.

7. Implémentation et gestion des accès clients avec les protocoles Internet

7.1. Introduction aux protocoles d'accès client

Exchange 2003 et Internet Information Service (IIS) se sont associées pour fournir une connectivité sécurisée aux utilisateurs qui accèdent à Exchange Server 2003 en utilisant l'un de ces protocoles :

- Post Office Protocol version 3 (POP3)
- Internet Message Access Protocol version 4 (IMAP4)
- Hypertext Transfer Protocol (HTTP)
- Network News Transfer Protocol (NNTP)
- Lightweight Directory Access Protocol (LDAP)

Les clients de messagerie Internet comme Outlook Express peuvent être configuré pour utiliser POP3 ou IMAP4 pour accéder à Exchange. POP3 fournit le processus le plus simple d'accès à la messagerie et IMAP4 fournit plus de fonctionnalités. Un navigateur Web comme Internet Explorer utilise le protocole HTTP pour accéder à Exchange en fournissant un client plus robuste. NNTP est utilisé pour envoyer et recevoir des messages sur les groupes de discussion. LDAP fournit une connectivité client et serveur avec le service d'annuaire Active Directory.

7.1.1. Protocoles d'accès client Internet supportés par Exchange Server 2003

Exchange utilise des serveurs virtuels pour fournir un accès à partir des protocoles POP3, IMAP4, SMTP, NNTP et HTTP sur le même serveur physique. Lors de l'installation, un serveur virtuel est créé pour chaque protocole. En créant tous ces serveurs, Exchange vous laisse la possibilité de choisir le type de client que vous souhaiter utiliser pour vous connecter à Exchange. En configurant plusieurs serveurs virtuels pour le même protocole, vous pouvez, par exemple, configurer différentes méthodes d'authentification ou de cryptage.

7.1.1.1. HTTP

Exchange Server 2003 supporte le protocole HTTP pour fournir un accès aux données d'Exchange à l'aide d'Outlook Web Access (OWA). OWA autorise les utilisateurs à accéder à leur boîte de messagerie par l'intermédiaire d'un navigateur Web comme Internet Explorer. OWA référence les objets Exchange en utilisant des URLs (Uniform Resource Locators) comme http://nom_du_server/exchange/mailbox/inbox. L'utilisation des URLs simplifie l'accès à Exchange pour les utilisateurs. OWA permet aux utilisateurs d'accéder à leurs données à partir d'ordinateurs Unix, Macintosh et Microsoft. Par l'intermédiaire d'OWA, les utilisateurs peuvent voir et travailler avec les dossiers publics, leur boîte aux lettres, la GAL et le calendrier.

7.1.1.2. LDAP

Exchange utilise LDAP version 3 pour effectuer des requêtes de lecture et de modification. LDAP est un protocole qui fournit un accès aux services d'annuaire pour le serveur et les quelques clients Exchange. La plupart des clients de messagerie comme Outlook Express, inclus un client LDAP.

7.1.2. Clients permettant l'accès à Exchange 2003

Suivant les besoins de votre entreprise vous avez la possibilité de choisir différents clients vous permettant d'accéder à votre messagerie. Les différents types de client de messagerie fournissent des accès et des fonctionnalités différentes.

7.1.2.1. Client POP3

POP3 (Post Office Protocol version 3) est un protocole simple qui possède des commandes limitées. Un client POP3 fournit l'accès le plus basic à un serveur Exchange en autorisant les utilisateurs d'accéder à leur boîte de messagerie. Une fois authentifié, le protocole télécharge les messages non lus pour les traiter en local.

Le principal inconvénient de ce protocole est qu'il est dépendant du poste sur lequel il est utilisé. Si vous utilisez ce protocole sur un réseau, vous devez toujours consulter vos messages sur le même poste de travail et si celui-ci venait à tomber en panne vous risquez de perdre l'intégralité de vos messages.

Par défaut, le service POP3 est désactivé sur le serveur Exchange 2003. Il faut donc activer dans la console **services.msc** le service **Microsoft Exchange – POP3.**

Techniquement, le protocole POP3 est défini par la RFC 1939/1737 et utilise les ports **TPC 110** et **SSL 995.**

7.1.2.2. Client IMAP4

IMAP4 (Internet Message Access Protocol version 4) est un protocole plus récent que POP3 possédant des commandes avancées. IMAP4 vous permet de stocker et gérer vos messages sur le serveur, contrairement à POP3 qui nécessite le téléchargement. En utilisant IMAP4, vous avez la possibilité de créer des dossiers sur le serveur, d'organiser vos messages et apercevoir le contenu de vos messages avant d'en télécharger les pièces jointes.

Par le simple fait que le contenu des messages reste sur le serveur, IMAP4 est supérieur à POP3 dans le cas d'une utilisation réseau sur des postes de travail partagé.

Un client IMAP4, comme Outlook Express fournit un accès à une boîte aux lettres et aux dossiers publics d'Exchange.

Par défaut, le service IMAP4 est désactivé sur le serveur Exchange 2003. Il faut donc activer dans la console **services.msc** le service **Microsoft Exchange – IMAP4.**

Techniquement, le protocole IMAP4 est défini par la RFC 2060 et utilise les ports **TPC 143** et **SSL 993.**

7.1.2.3. Client NNTP

NNTP (Network News Transfer Protocol) est utilisé pour accéder aux groupes de discussion. Vous avez la possibilité de configurer Exchange pour publier une partie de la hiérarchie de ses dossiers publics pour les rendre disponible aux clients NNTP.

7.1.2.4. Client Outlook Web Access

Microsoft Outlook Web Access permet à un utilisateur d'accéder à sa boîte aux lettres via un navigateur Web. Cet accès via le web peut se révéler très utile lorsque l'on dispose de serveurs

Exchange dans un environnement hétérogène. Ainsi, n'importe quel client UNIX, Macintosh ou Windows pourra accéder au serveur Exchange.
Il offre une alternative à beaucoup de problèmes lorsqu'il s'agit d'offrir un accès à la messagerie n'importe où au sein de l'entreprise.

OWA est installé et activé par défaut sur tous les serveurs de votre organisation. Pour y accéder, saisissez l'url http://serveur/Exchange (où serveur représente le nom de votre serveur Exchange) dans la barre d'adresse de votre navigateur.

7.1.3. Pourquoi utiliser la technologie du serveur frontal et dorsal ?

Les deux éditions de Microsoft Exchange Server 2003 (standard et entreprise) supportent la topologie serveur frontal/dorsal pour répartir votre organisation Exchange afin de vous adapter à une forte population d'utilisateur.

Les serveurs frontaux exécutent Exchange Server 2003 mais n'hébergent ni les boîtes aux lettres ni les banques d'informations de dossiers publics. Les serveurs dorsaux exécutent Exchange Server 2003 et contiennent au moins une banque de boîtes aux lettres ou de dossiers publics.

Dans une topologie serveur frontal/dorsal, chaque serveur frontal détermine le serveur dorsal qui contient la ressource voulu en interrogant Active Directory avec une requête LDAP.

7.1.3.1. Les avantages

Les clients HTTP, POP3 et IMAP4 profite de la topologie frontal/dorsal. Certains clients MAPI comme Outlook 2002 ou ultérieur, accèdent à la banque de stockage directement, ils ne peuvent donc pas profiter de cette topologie. Cependant, Outlook 2003 utilise la connexion RPC sur HTTP lui permettant d'accéder aux banques d'information via cette topologie.

L'implémentation de la topologie frontal/dorsale fournit les avantages suivants :

- Il est possible de configurer le système DNS avec l'équilibrage de charge réseau Windows 2003 pour n'avoir qu'un nom unique pour tous les frontaux. De cette façon, les utilisateurs peuvent utiliser la même URL pour configurer l'accès à Outlook Web Access, POP3 et IMAP4
- Si vous choisissez d'activer le cryptage de vos connexions entre les clients et les serveurs frontaux, le traitement du chiffrage et déchiffrage serra exécuté par ces mêmes serveurs frontaux. Ce qui vous permet de libérer des ressources sur les serveurs dorsaux qui traitent la gestion de banques d'informations.
- Vous pouvez améliorer la sécurité de votre messagerie en déplaçant par exemple le serveur frontal dans une DMZ ou en publiant son accès sur votre pare-feu, sachant que si une personne mal intentionné arrive à accéder au serveur malgré la protection, il aura accès à aucunes boîtes aux lettres.
- Il est possible de faire une expansion facile du système de messagerie d'une entreprise car il suffit d'ajouter des serveurs frontaux supplémentaires pour répondre à la croissance de charge. De même, la suppression de serveurs dorsaux est complètement transparente pour les clients en ayant au préalable déplacé les banques informations contenues sur ces serveurs.

7.1.4. Pourquoi implémenter la répartition de charge réseau ?

La répartition de charge réseau (Network Load Balancing) est un service fournit par Windows Server 2003. Ce service répartit dynamiquement et de manière transparente la charge réseau (trafic IP) aux multiples serveurs frontaux.

Avec la répartition de charge réseau, si un serveur ne fonctionne pas, les autres serveurs frontaux prennent automatiquement la charge réseau du serveur manquant. Donc, la répartition de charge réseau fournit à la fois une répartition du trafic réseau afin de répartir la charge de travail et ajoute un niveau de tolérance de panne en assurant l'accès aux serveurs frontaux malgré le disfonctionnement de l'un d'entre eux.

Si vous souhaitez fournir un accès client aux ressources d'Exchange Server 2003 en utilisant Outlook Web Access, POP3 et IMAP4 en souhaitant rendre ces services le plus disponibles possible, vous devez considérer les éléments suivants :

- Déployer au minimum 2 serveurs frontaux pour chaque protocole.
- Implémentez une solution de cluster sur les serveurs dorsaux.
- N'autorisez pas l'accès direct aux utilisateurs d'Internet aux serveurs dorsaux.

7.2. Implémentation d'une topologie serveur frontal/dorsal

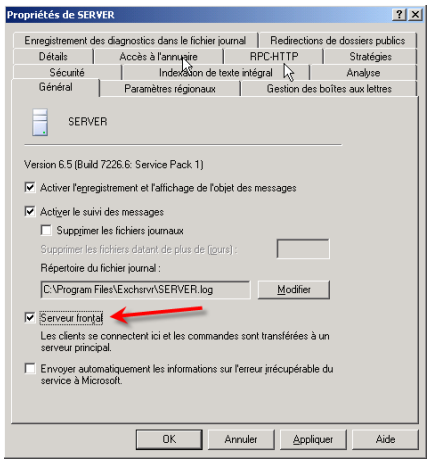
Une fois avoir décidé le ou les protocoles de connexion clients que vous allez utiliser dans votre organisation, vous devez configurer votre topologie Exchange. La topologie frontal/dorsal est la plus sécurisée et la plus robuste.

7.2.1. Comment configurer un serveur Exchange en serveur frontal

Un serveur frontal doit absolument faire parti de la même organisation Exchange que les serveurs dorsaux et donc de la même forêt.

Les étapes à suivre pour configurer un serveur frontal :

1. Installer au moins deux serveurs Exchange dans votre organisation.
2. Utiliser le gestionnaire système Exchange pour afficher les propriétés de votre premier serveur Exchange.
3. Activer la case **Serveur frontal.**
4. Pour commencer à utiliser le serveur frontal, vous devez redémarrer l'ordinateur ou redémarrer les services HTTP, POP3 et IMAP4.

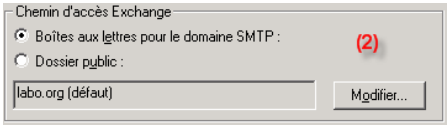


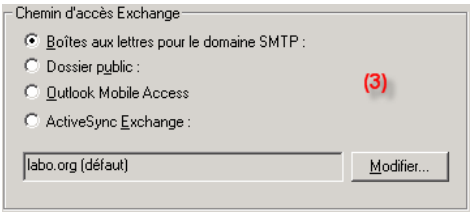
7.2.2. Comment configurer Outlook Web Access avec des serveurs frontaux

Par défaut, aucunes modifications ne sont requises sur le serveur frontal. Cependant, Si vous utilisez Outlook Web Access et que vous hébergez plusieurs domaines, organisations ou arborescences de dossiers publics, vous devez créer plusieurs serveurs ou répertoires virtuels.

Comment configurer votre serveur frontal hébergeant plusieurs domaines avec les serveurs virtuels ?

1. Utiliser le gestionnaire de système Exchange pour créer un serveur virtuel pour chaque domaine.
2. Associer chaque serveur virtuel avec un domaine SMTP. (En faisant cette association, Exchange n'autorisera l'accès qu'aux utilisateurs qui ont le même domaine SMTP)
3. Créer les dossiers virtuels Exchange et Public sous le serveur virtuel.





Lorsque vous avez plusieurs serveurs virtuels avec différents noms de domaines en implémentant SSL, vous devez ajouter un certificat pour chaque domaine.

Si vous souhaitez implémenter SSL en réduisant le coût d'acquisition de plusieurs certificats SSL représentant les diverses entreprises hébergées par votre entreprise, vous avez la possibilité d'utiliser des répertoires virtuels. En configurant des répertoires virtuels supplémentaires, les clients peuvent accéder à leurs données par l'intermédiaire d'un seul domaine. L'avantage ici est de réduire le coût des certificats et la charge de configuration.

Comment configurer votre serveur hébergeant plusieurs domaines en utilisant les dossiers virtuels ?

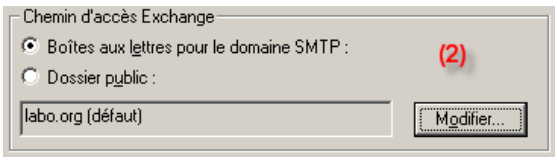
1. Utiliser le gestionnaire système Exchange pour ajouter un dossier virtuel sous le serveur virtuel HTTP par défaut.
2. Sélectionner la fonction du répertoire virtuel.
3. Dans le cas d'un dossier de boîte aux lettres, sélectionnez le domaine SMTP correspondant.
4. Dans le cas d'un dossier public, sélectionnez le dossier public correspondant.

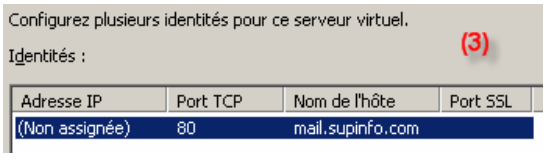
7.2.3. Comment configurer Outlook Web Access avec des serveurs dorsaux

Dans le cas d'une utilisation simple d'Exchange, aucunes modifications ne sont requises sur le serveur dorsal. Par contre si vous avez configuré des serveurs ou des répertoires virtuels supplémentaires sur le serveur frontal, vous devez apporter la même configuration à vos serveurs dorsaux.

Configuration des serveurs virtuels Exchange (HTTP) supplémentaires sur les serveurs dorsaux :

1. Créer et indiquer un nom spécifique au serveur virtuel comme *supinfo.com (serveur dorsal).*
2. Sélectionner le domaine SMTP approprié.
3. Ajouter le nom d'hôte approprié, mail.supinfo.com par exemple.





Configurer un répertoire virtuel supplémentaire sur un serveur dorsal :

1. Configurer la même structure de répertoires virtuels sur le serveur dorsal correspondante au serveur frontal.
2. Spécifier le domaine SMTP approprié pour le ou les répertoires virtuels puis associer les avec les banques de boîtes aux lettres.

Quand les serveurs dorsaux sont en cluster et si vous avez besoin d'ajouter un serveur ou un répertoire virtuel, vous devrez utiliser la combinaison de l'outil d'administration du cluster et le gestionnaire système Exchange pour ajouter cet élément.

Le serveur Exchange Server 2003 ne requière pas la modification du nom d'hôte du serveur virtuel par défaut. Lors de l'utilisation du cluster, le nom d'hôte du serveur virtuel par défaut doit rester vierge comme pour l'utilisation sans cluster.

Comment configurer un serveur virtuel Exchange (HTTP) dans l'Exchange Virtual Server :

1. Créer un serveur virtuel Exchange dans le gestionnaire système Exchange.
2. Créer un répertoire virtuel pour faire la correspondance avec la configuration du serveur frontal.
3. Ajouter un nouveau serveur virtuel Exchange (HTTP) à l'Exchange Virtual Server (EVS) du cluster à l'aide de l'outil d'administration du cluster.

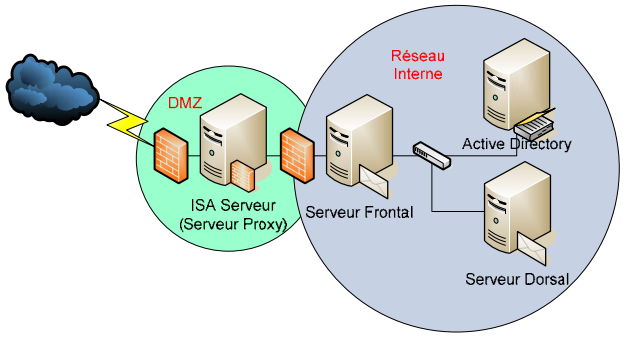
7.2.4. Configuration du pare-feu pour sécuriser la structure serveur frontal/dorsal

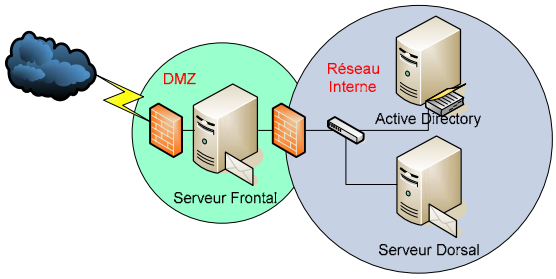
Lors du déploiement de la topologie serveur frontal/dorsal, vous devez alors vous interroger sur le placement et la configuration du ou des pare-feu.

7.2.4.1. Type de topologie avec un pare-feu

Quatre configurations de pare-feu sont possibles lors de l'implémentation de la topologie serveur frontal/dorsal :

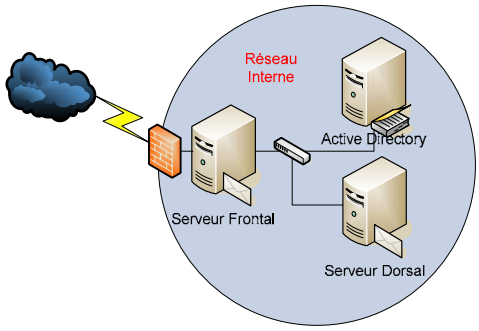
1) ISA Serveur en mode Proxy est situé entre deux Pare-feu : Dans ce mode, les serveurs frontaux et dorsaux sont situés dans la partie interne du réseau (la partie la plus sécurisée). Dans ce cas, ISA serveur transmet seulement toutes les requêtes entre les clients et le serveur frontal et empêche les clients d'accéder aux serveurs dorsaux. En plaçant les serveurs frontaux et dorsaux dans le réseau interne, on se retrouve dans le cas le plus sécurisé venant du fait que le nombre de port ouvert sur le pare-feu interne est minimisé.

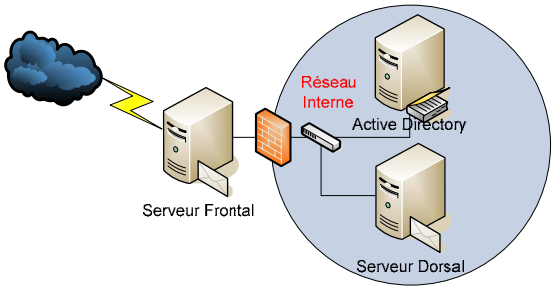




2) Le serveur frontal est situé dans le réseau périphérique (DMZ) : Dans ce mode, le serveur frontal est isolé entre deux pare-feu, ce qui signifie que si une personne arrive à compromettre la sécurité du serveur frontal, il restera isolé du reste du réseau de l'entreprise vous laissant par la même occasion le temps de détecter l'intrusion et d'y mettre fin.

3) Le serveur frontal est situé derrière un unique pare-feu : Dans ce mode, vous devez limiter l'ouverture des ports sur le pare-feu à ceux requit par le serveur frontal (HTTP 80, HTTPS 443, POP3 110, etc.) et seulement à destination de celui-ci.





4) Le serveur est situé en dehors du pare-feu : Ce mode de fonctionnement est déconseillé. Ici, le serveur frontal est totalement vulnérable aux accès non autorisés.

7.2.4.2. Configuration des différents ports

Selon le type de topologie choisi, vous devez ouvrir certains ports afin de permettre la communication entre les différentes machines. Les clients communiquent avec les serveurs frontaux au travers d'Internet, les serveurs frontaux communiquent avec les serveurs dorsaux et les contrôleurs de domaines.

Lorsque vous placer un serveur frontal derrière un pare-feu, vous devez ouvrir certains ports (correspondant aux services que vous utilisez) sur le pare-feu qui est situé entre Internet et le serveur frontal :

Services	Port TCP	Port TCP avec SSL
POP3	110	995
IMAP4	143	993
SMTP	25	25
NNTP	119	563
HTTP (Outlook Web Access)	80	443

Lorsque vous avez placé votre serveur frontal dans une DMZ et votre serveur dorsal dans le réseau interne, vous devez ouvrir certains ports (correspondant aux services que vous utilisez) sur le pare-feu qui est situé entre la DMZ et le réseau interne :

Services de messagerie	Port TCP
POP3	110
IMAP4	143
NNTP	119
HTTP	80

Le serveur frontal doit aussi communiquer avec des contrôleurs de domaines Active Directory (ou des catalogues globaux) situés derrière le pare-feu en utilisant des requêtes LDAP en s'authentifiant à l'aide du protocole Kerberos.

Communication AD	Port TCP	Port UDP
LDAP → Contrôleur de domaine	389	389
LDAP → Catalogue global	3268	X
Kerberos	88	88

Le serveur frontal doit pouvoir résoudre les noms d'hôtes locaux. Si votre serveur DNS est situé dans le réseau interne alors il faudra ouvrir le port suivant :

DNS	Port TCP	Port UDP
DNS Lookup	53	53

Le serveur frontal utilise aussi des RPCs pour authentifier les clients auprès des catalogues globaux. Pour permette la connectivité entre ces services vous devez ouvrir les ports suivant :

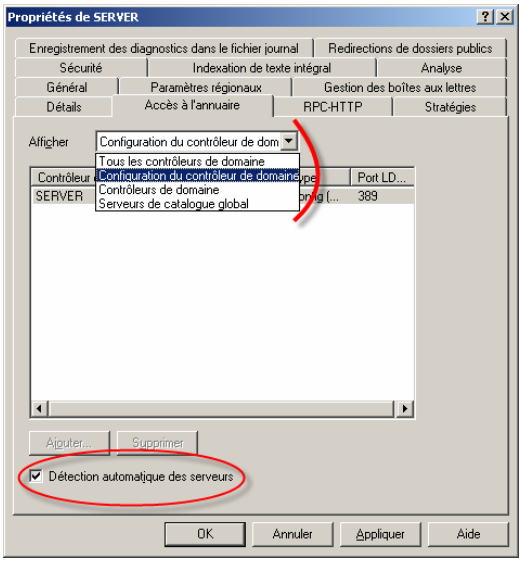
RPC Services	Port TCP
RPC endpoint mapper	135
RPC services ports	1024-65535

- Si vous utilisez IPSec dans votre réseau, vous devez opter pour le filtrage de paquets IP au lieu du filtrage de ports.

- Si vous déployez la connexion **RPC sur HTTP** avec un serveur proxy RPC dans la DMZ, vous devrez ouvrir les ports **80** ou **443** sur le pare-feu externe pour permettre à vos clients Outlook 2003 de communiquer avec votre serveur proxy RPC. Vous devez aussi autoriser le port **593** sur votre pare-feu interne pour autoriser le service RPC endpoint mapper encapsulé dans le protocole HTTP.

Pour éviter l'ouverture des ports DNS ou RPC entre le réseau périphérique et le réseau interne, vous devez :

- Pour le **DNS** : Configurer un serveur DNS dans le réseau périphérique
- Pour le **RPC** : Configurer le serveur frontal pour qu'il n'utilise pas RPC pour localiser le contrôleur de domaine dans l'intranet. Vous pouvez utiliser l'onglet Accès à l'annuaire dans les propriétés de votre serveur à partir du gestionnaire système Exchange pour spécifier le nom du contrôleur de domaine et celui du catalogue global.



7.2.4.3. Comment configurer DSAccess pour les réseaux périphériques ?

Le composant DSAccess dans Exchange fourni un support pour les réseaux périphériques dans lesquels le trafic RPC n'est pas autorisé sur le pare-feu interne. Cependant pour des soucis de performances, vous devez ajouter deux clefs de registre sur le serveur frontal afin de désactiver **NETLogon** et **Directory Access ping**.

DSAccess se connecte à Active Directory pour vérifier l'espace disque disponible, la synchronisation du temps et la réplication de partition en utilisant le service **NetLogon** avec RPC.

Pour arrêter le service **Netlogon** vous devez créer la clef de registre **DisableNetlogonCheck** de type **DWORD** avec la valeur **1** sur le serveur frontal à l'emplacement suivant : ***HKEY_LOCAL_MACHINE\System\CurrentContràlSet\Services\MSExchangeDSAccess\.***

Pour arrêter le **Directory Access ping**, vous devez créer la clef de registre **LdapKeepAliveSecs** de type **DWORD** avec la valeur **0** sur le serveur frontal à l'emplacement suivant : ***HKEY_LOCAL_MACHINE\System\CurrentContràlSet\Services\MSExchangeDSAccess\.***

7.2.4.4. Comment implémenter IPSec entre les serveurs frontaux et dorsaux

Les réseaux sont de nos jours protéger d'accès non autorisé sur des données qui transitent en dehors de l'intranet sur des lignes publiques. Cependant, une grande partie des réseaux communique en interne de façon clair (non crypté). Une personne munie d'un accès à ce réseau et d'un analyseur de trame pourrait facilement récupérer des données importantes.

Pour fournir un conduit sécurisé entre les serveurs frontaux et dorsaux, vous pouvez utiliser IPSec. IPSec authentifie les ordinateurs et crypte les données transmises entre deux ordinateurs.

> ☞ Pour implémenter IPSec entre des serveurs frontaux et dorsaux en cluster, vous devez utiliser Exchange Server 2003 sur Windows Server 2003.

Vous créez et configurez les stratégies IPSec locales en utilisant la MMC Stratégie de sécurité locale. Utilisez la stratégie de sécurité du domaine pour créer et configurer les stratégies IPSec pour tout le domaine. Vous avez aussi la possibilité de créer votre propre MMC pour utiliser IPSec à l'aide du composant logiciel enfichable **Gestion de la stratégie de sécurité IP**.

Les étapes pour configurer les stratégies IPSec sont les suivantes :

1. Démarrer une MMC.
2. Ajouter le composant logiciel enfichable **Gestion de la stratégie de sécurité IP** dans la MMC.
3. Configurer la stratégie IP : Il existe 3 types de stratégies IPSec par défaut : **Server**, **Client**, **Secure Server**. Server permet par défaut d'utiliser le cryptage IPSec mais accepte aussi les communications non cryptées. Client accepte le cryptage si on lui demande, il ne peut initier une communication cryptée. Secure Server accepte seulement les communications cryptées. Vous pouvez donc configurer votre serveur frontal afin qu'il communique toujours en IPSec et configurer votre serveur dorsal afin qu'il n'utilise IPSec que lorsqu'un ordinateur lui demande.
4. Assigner la stratégie aux serveurs frontaux et dorsaux.

Les stratégies IPSec permet à l'aide de filtre IP une configuration pointue. Par exemple, vous pouvez utiliser IPSec en cryptant seulement le trafic émanant du port 80.

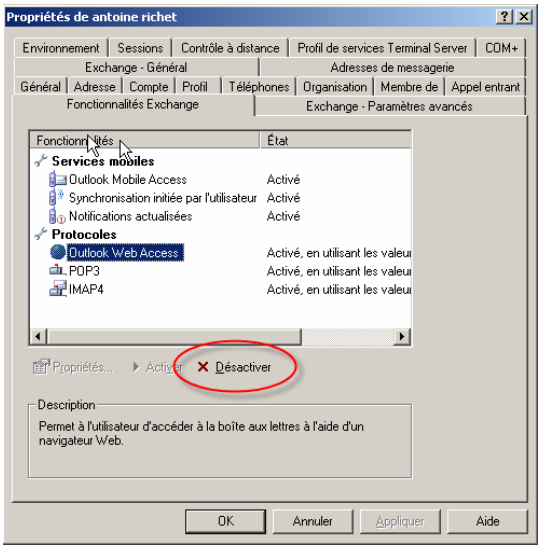
7.3. Implémentation et gestion d'Outlook Web Access

7.3.1. Comment gérer Outlook Web Access ?

Par défaut, Outlook Web Access (OWA) est configuré pour autorisé les utilisateurs à accéder à leurs boîtes aux lettres et à l'arborescence de dossier public par défaut. Cependant vous pouvez configurer le serveur Exchange pour qu'il fournisse un accès personnalisé en HTTP ou WebDAW.

Par défaut, OWA est activé pour tous les utilisateurs. Les tâches suivantes indiquent comment désactiver cette fonctionnalité :

1. Ouvrer la console Utilisateurs et ordinateurs Active Directory.
2. Dans les propriétés d'un utilisateur, vous pouvez désactiver l'accès à OWA dans l'onglet **Fonctionnalités Exchange**.



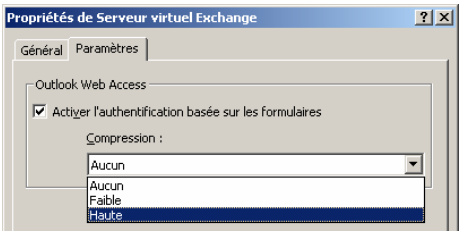
Vous pouvez configurer Outlook Web Access avec les outils suivants :

- **Gestionnaire Système Exchange** : Avec cet outil vous pouvez créer de nouveaux serveurs ou répertoires virtuels. Ces serveurs et ces répertoires apparaissent dans la console IIS. Les modifications effectuées avec cet outil, surchargent celles inscrites par IIS.
- **Internet Services Manager (IIS)** : Utilisez cet outil uniquement pour faire des modifications que vous ne pouvez pas faire avec le Gestionnaire Système Exchange : SSL, Activer le l'audit des événements.

7.3.2. Comment sélectionner une version d'Outlook Web Access ?

Outlook Web Access permet aux clients de choisir entre deux versions lors de l'authentification de l'utilisateur basé sur la connexion et la version du navigateur web.

Exchange Server 2003 fournit une nouvelle page d'authentification qui permet à l'utilisateur de choisir sa version d'Outlook Web Access. Pour activer cette fonctionnalité, vous devez activer l'authentification basée sur les formulaires dans les propriétés du serveur virtuel et utiliser un certificat SSL. Une fois activé, vous avez la possibilité de choisir le niveau compression des réponses HTTP implémenté par GZip (GNU zip).



Voici les deux versions :

- **Expérience de base (OWA Basic)** : Conçu pour fonctionner avec la plupart des navigateurs (HTML 3.2). Son interface est plus simple et nécessite moins de trafic réseau. Par contre certaines fonctionnalités ne sont pas disponibles.
- **Expérience étendue (OWA Premium)** : Conçu pour fournir toutes les fonctionnalités d'OWA Exchange 2003. Certaines fonctionnalités nécessitent l'utilisation d'Internet Explorer 6 mais peuvent être utilisé en grande partie avec Internet Explorer 5.

7.3.3. Options pour sécuriser les communications Outlook Web Access ?

Vous pouvez configurer différentes options pour fournir une meilleure sécurité pour les environnements dans lesquels vous ne souhaitez pas stocker les informations d'authentifications de l'utilisateur sur l'ordinateur client et vous souhaitez utiliser un moyen de communication sécurisé entre le client et le serveur.

7.3.3.1. Les cookies

Un cookie stocke les informations d'authentifications de l'utilisateur quand l'authentification basée sur les formulaires est activé sur le serveur Exchange. Lorsque d'un utilisateur se déconnecte d'Outlook Web Access, le cookie est vidée et n'est plus valide pour l'authentification.

La page d'authentification (vu au dessus) permet à l'utilisateur de sélectionner l'option de sécurité la plus adaptée dans son cas :

- **Ordinateur public ou partagé** : Rend le cookie invalide au bout de 15 minutes d'inactivité.
- **Ordinateur privé** : Configure le time out du cookie à 24 heures d'inactivité. Ce mode est à utiliser sur une machine dont vous êtes le seul utilisateur.

✍ La fonctionnalité de time out n'est disponible que dans le mode étendue d'Outlook Web Access.

7.3.3.2. Mise en cache de l'authentification

Pour les utilisateurs accédant à OWA à l'aide du navigateur Internet Explorer 6 SP1 ou ultérieur, les informations d'authentification sont supprimées lorsque l'utilisateur appuie sur le bouton *Se déconnecte*. La fermeture du navigateur n'est pas nécessaire pour vider le cache des informations d'authentification.

7.3.3.3. Support S/MIME

Le protocole ***Secure Multipurpose Internet Mail Extensions*** (S/MIME) autorise les utilisateurs à envoyer des messages sécurisés par une signature digitale ou par un cryptage. Dans Outlook Web Access d'Exchange Server 2003, l'utilisateur peut signer un message en utilisant le contrôle Outlook Web Access S/MIME. Ce contrôle travail conjointement avec l'infrastructure de clef public de l'entreprise (PKI) pour fournir les capacités de signer et crypter un message.

7.3.4. Comment sécuriser les communications Outlook Web Access ?

7.3.4.1. Time Out des cookies

Lors de l'utilisation de l'option de sécurité Ordinateur public ou partagé, on a vu que la valeur par défaut du time out d'inactivité du cookie est par défaut de 15 minutes.

Exchange vous permet de changer cette valeur en créant une nouvelle clef dans le registre, comme suit :

1. Ouvrer l'éditeur de registre et déployer la clef suivante : ***HKey_local_machine\system\CurrentControlSet\Services\MSExchangeWeb\OWA***
2. Créer une clef DWORD nommé **PublicClientTimeout** ou **TrustedClientTimeout** avec une valeur **Décimal** en minutes comprise entre 1 et 432000.

7.3.4.2. Outlook Web Access S/MIME

Pour pouvoir bénéficier de la signature et du cryptage, vous devez déployer S/MINE avec OWA comme suit :

1. Installer une autorité de certification racine d'entreprise.
2. Configurer la façon permettant à vos utilisateurs de récupérer un certificat.
3. Installer le contrôle Outlook Web Access S/MIME sur les postes clients.
4. Configurer les paramètres de sécurité de la messagerie.
5. Envoyer des messages de tests.

7.3.4.3. Cryptage SSL

Les étapes suivantes montrent comment sécuriser les communications avec OWA en utilisant SSL :

1. Installer un certificat à votre serveur Web : Ce certificat inclus une stratégie d'authentification d'application pour le cryptage SSL. Vous pouvez utiliser un simple certificat de serveur Web pour toutes les communications SSL de votre Exchange.
2. Activer le filtrage de port sur votre serveur : Attribuer ce certificat à chaque protocole pouvant fonctionner avec SSL (HTTP, SMTP, …) et activer le cryptage.
3. Configurer SSL dans les applications de messagerie clientes : Configurer les logiciels clients afin qu'il utilise le port SSL au lieu du port par défaut. Une fois SSL activé, le serveur n'acceptera plus de communications sur le port par défaut.

8. Gestion de la configuration et de la connectivité client

8.1. Configurer et personnaliser Outlook 2003

8.1.1. Comment s'installe Outlook 2003

Outlook est installé automatiquement avec le pack Microsoft Office 2003. Vous avez la possibilité de l'installer seul ou avec d'autres outils d'un pack de différente version. Par contre vous ne pouvez avoir qu'un seul Outlook par poste.

Lorsque l'installation est terminée, lors de la première exécution, un assistant de configuration se lance, permettant de finir la configuration initiale du profil outlook. Le profil définit l'adresse du le serveur de messagerie utilisé, l'emplacement des mails reçu et la méthode de connexion (authentification, cryptage, VPN,…). Outlook 2003 peut se connecter aux serveurs Exchange, POP3, IMAP, HTTP. Cette partie peut être effectuée par l'administrateur ou directement par l'utilisateur.

Ensuite lorsqu'Outlook 2003 est installé et que votre profil est créé, il est possible d'effectuer des taches de personnalisations. Par exemple, les utilisateurs peuvent configurer le degré de fonctionnement du courrier indésirable, changer le format des messages. Généralement, les utilisateurs font ces taches directement.

8.1.2. Modes de connexion d'Outlook 2003 avec Exchange

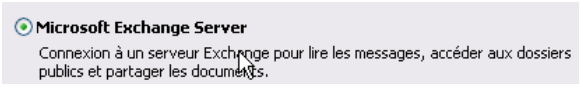
Avant que les utilisateurs n'accèdent à leur boîte aux lettres, l'ordinateur doit être connecté sur le réseau et authentifié. Les utilisateurs peuvent configurer Outlook 2003 dans 3 modes de connexions :

Mode	Description
Mise en cache	Ce mode est le mode par défaut, il stock une copie de la boîte aux lettre de l'utilisateur localement dans un fichier .ost. Ce dossier est mis à jour fréquemment avec le serveur Exchange. Dans ce mode, l'état de connexion est gérer directement et de manière transparente par Outlook.
En ligne (Connecté)	Dans ce mode, la boîte aux lettres reste stockée sur le serveur Exchange et l'utilisateur doit être connecté en permanence pour accéder à ces messages.
Hors connexion	Ce mode est utile pour les utilisateurs ne possédant pas de connexion permanente ou qui utilise une connexion VPN pour joindre le serveur Exchange. Là aussi les messages sont stockés dans un fichier .ost qui est synchronisé par la commande Envoyer/Recevoir. Ce mode est différent du mode cache car les utilisateurs peuvent ici spécifier à quel moment et quelles dossiers doivent être synchronisés avec le fichier .ost.

8.1.3. Comment configurer Outlook pour le connecter à Exchange Server 2003

Il n'est pas nécessaire de configurer cette connexion lors de la première exécution d'Outlook, vous avez la possibilité de la configurer à tous moment.

Pour se faire, il vous suffit d'accéder aux options d'Outlook et de créer un nouveau profil de connexion et de choisir la connexion **Microsoft Exchange Server**



Une seule connexion Microsoft Exchange Server est possible par profil.

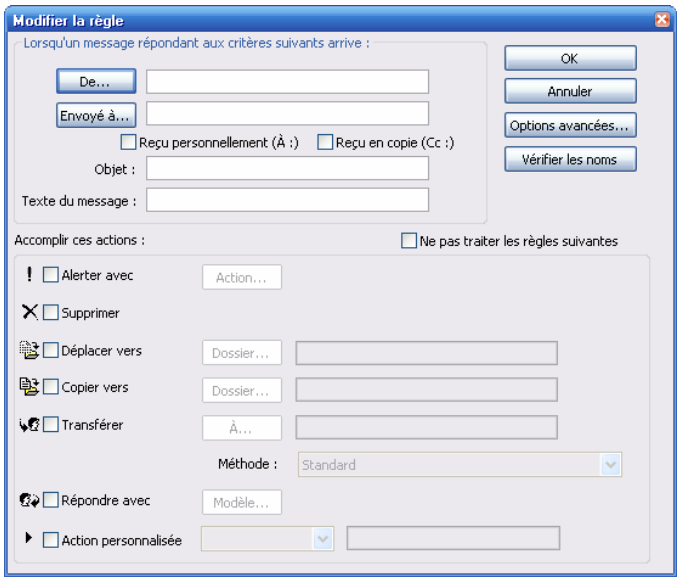
8.1.4. Comment utiliser le gestionnaire d'absence du bureau ?

Les deux tâches les plus courantes où les administrateurs doivent aider les utilisateurs à configurer Outlook sont : Les règles et alertes de messages et le gestionnaire d'absence du bureau.

Le gestionnaire d'absence du bureau, comme son nom l'indique, va gérer les messages que vous réceptionnez lorsque justement vous n'étés pas présent pour les lire. (Congés, déplacements, maladie…).

Pour configurer le gestionnaire faites comme suit :

1. Dans Outlook, ouvrir le **Gestionnaire d'absence du bureau…** qui se situe dans le menu **Outils**.
2. Configurer le message qui va être envoyé aux personnes qui vous envoient un message pendant votre absence.
3. Configurer des règles si vous souhaiter accomplir des actions et/ou d'envoyer des messages personnalisés en fonction de l'expéditeur.



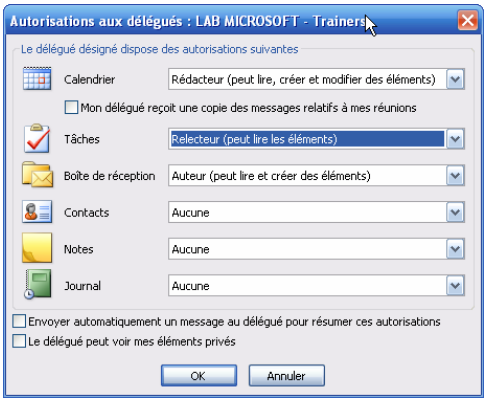
8.1.5. Comment donner la permission à un délégué d'accéder à votre boîte aux lettres ?

Pour utiliser la fonctionnalité de délégation vous devez être connecté au serveur Exchange, avoir déjà reçu un message dans la boîte aux lettres sur le serveur et possédez le complément de Microsoft Exchange Client Dlgsetp.ecf (qui est installé par défaut).

Vous pouvez déléguer trois différents rôles d'accès avec Outlook :

Rôles	Le délégué peut faire
Auteur	Lire, créer, modifier et supprimer des éléments que le délégué a créés.
Rédacteur	Tous ce que faire l'auteur, plus modifier et créer des éléments créés par le propriétaire de la boîte.
Rélecteur	Lire des éléments.

Pour déléguer un de ces rôles dans Outlook, vous devez aller dans le menu Outils et cliquez sur Options. Une fois dans le menu options, cliquez sur l'onglet délégations. A partir de cet onglet vous allez pouvoir sélectionner le ou les délégués puis leurs affecter les bons rôles.



8.1.6. Comment configurer Exchange Server 2003 et Outlook 2003 pour utiliser le protocole RPC sur HTTP ?

Sans la fonctionnalité qu'offre Exchange Server 2003 d'utiliser RPC sur HTTP, les utilisateurs doivent se connecter en VPN afin d'utiliser un client Exchange depuis un emplacement Internet. Grâce à cette fonctionnalité les utilisateurs peuvent se connecter sans utiliser le VPN et toutes les données transférées sont encryptées à l'aide de Secure Sockets Layer (SSL) sur la connexion HTTP.

Pour appliquer l'utilisation de RPC sur HTTP vous devez apporter des modifications à la fois coté serveur et client.

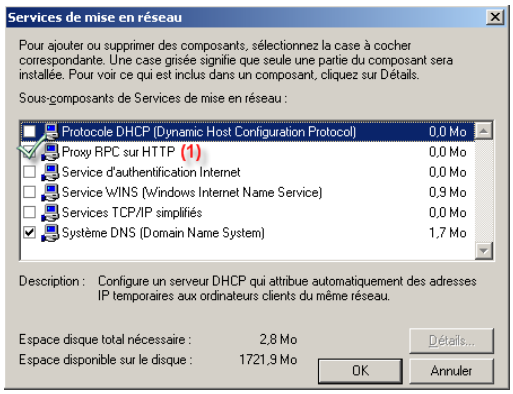
8.1.6.1. Eléments requis pour utiliser RPC sur HTTP

Ordinateurs	Requis
Client	- Outlook 2003 - Windows XP avec le service pack 1 - Windows XP correctif Q331320
Serveur	- Exchange 2003 sur Windows Server 2003 pour les serveurs frontaux

	- Exchange 2003 sur Windows Server 2003 pour les serveurs dorsaux - Exchange 2003 sur Windows Server 2003 pour les dossiers publics - Exchange 2003 sur Windows Server 2003 pour les dossiers systèmes - Windows Server 2003 pour le catalogue global.

8.1.6.2. Configuration d'Exchange 2003 pour le RPC sur HTTP

1. Configurer le serveur frontal comme serveur Proxy RPC en ajoutant le composant **Proxy RPC sur HTTP** dans les Services de mise en réseau.



2. Configurer la méthode d'authentification du répertoire virtuel RPC dans le gestionnaire IIS sur **authentification de base**.

3. Configurer le serveur **proxy RPC** pour qu'il utilise les ports spécifiques à RPC sur HTTP : Modifier la clef de registre **HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\RpcProxy\ValidPorts** sur le **serveur proxy RPC** en y ajoutant les informations suivantes sans aucuns espaces ni saut de ligne :

   « ***ExchangeServer*:593;*ExchangeServerFQDN*:593;**
   ***ExchangeServer*:6001-6002;*ExchangeServerFQDN*:6001-6002;**
   ***ExchangeServer*:6004;*ExchangeServerFQDN*:6004;**
   ***GlobalCatalogServer*:593;*GlobalCatalogServerFQDN*:593;**
   ***GlobalCatalogServer*:6004;*GlobalCatalogServerFQDN*:6004** »

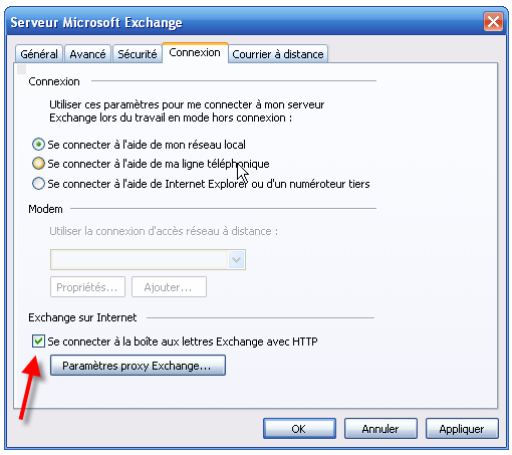
   Sachant que les variables **ExchangeServer** et **GlobalCatalogServer** sont les noms NetBIOS de votre serveur Exchange et de votre catalogue global. **ExchangeFQDN** et **GlobalCatalogServerFQDN** sont les noms DNS complets de votre serveur Exchange et de votre catalogue global.

4. Configurer le serveur de **catalogue global** afin qu'il utilise les ports spécifiques pour RPC sur HTTP :
   Créez la clef de registre **NSPI interface protocol sequences** (Valeur de chaînes multiples) avec la valeur **ncacn_http:6004** dans l'arborescence ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters***

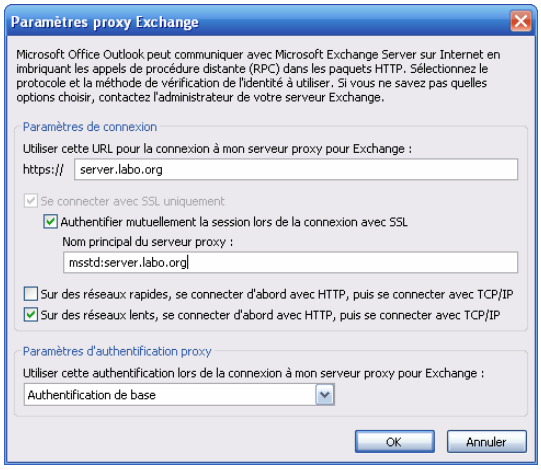
8.1.6.3. Configurer Outlook 2003 pour utiliser le RPC sur HTTP

1. Mettez à jour Outlook et créez-vous un nouveau profil pour utiliser le RPC sur HTTP.

2. Configurer le compte de message du profil Outlook pour se connecter à Exchange Server et spécifier l'utilisation mode cache.
3. Dans les paramètres avancés de votre compte, spécifiez l'utilisation du protocole HTTP.



4. Configurer la connexion avec l'url complète du serveur Proxy et utilisez le protocole SSL avec l'authentification de base.



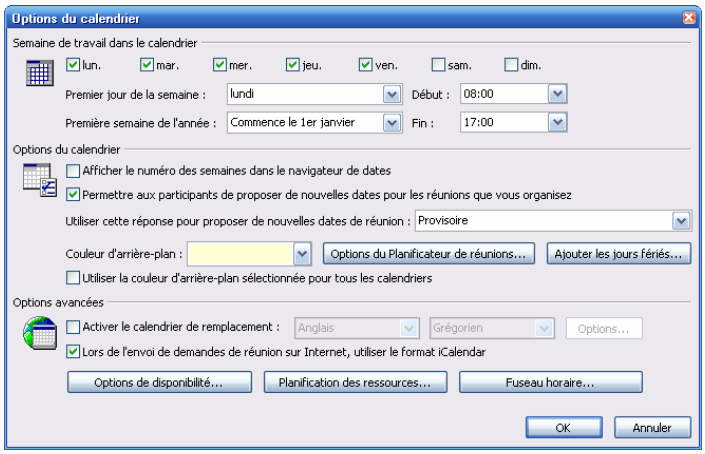
8.2. Utilisation du calendrier d'Outlook 2003

Les utilisateurs utilisent le calendrier d'Outlook pour gérer leur calendrier et créer des rendez-vous, événements et des réunions rapidement et facilement.

8.2.1. Comment organiser une réunion ?

Créer une réunion est la tâche la plus utilisé du calendrier Outlook 2003.

La première étape pour utiliser le calendrier est de le configurer : (Outils → Options… → Options du calendrier…).



Ensuite pour créer une demande de réunion :

- Il suffit d'aller dans le menu fichier d'Outlook et sélectionner Demande de réunion.
- Entrer les participants et les informations concernant cette réunion.
- Envoyer la demande de réunion.

8.2.2. Méthode de partage de calendrier avec Exchange Server 2003

Si votre compagnie utilise Exchange Server 2003, vous avez plusieurs choix pour partager les calendriers :

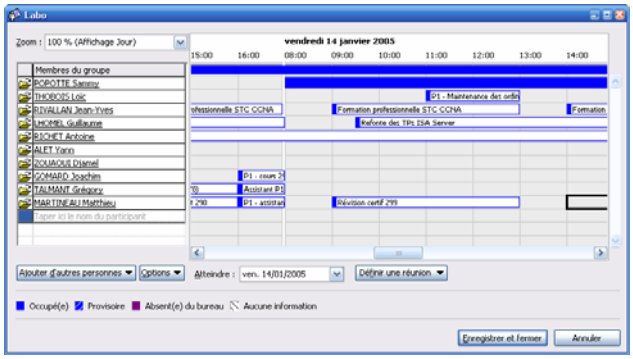
- **Les utilisateurs peuvent modifier les permissions d'accès de leur calendrier** : Un utilisateur possédant les bonnes permissions d'accès peut facilement voir le calendrier d'une autre personne.
- **Les utilisateurs peuvent déléguer la gestion de leur calendrier** : Un utilisateur à qui vous déléguez certains droits peut exécuter des actions de votre part.
- **L'administrateur peut utiliser un dossier public** : L'administrateur créé un calendrier de groupe dans un dossier publique et assigne les permissions pour les utilisateurs.

8.2.3. Comment créer un agenda de groupe ?

Pour faciliter le travail en groupe, vous avez la possibilité de créer des agendas de groupe permettant de faciliter la visibilité des tous les calendriers du groupe.

Pour créer un agenda de groupe, il faut se situer dans la rubrique Calendrier d'Outlook 2003, aller dans le menu Actions et cliquer sur Agendas de groupe…

Vous allez avoir la possibilité de créer votre propre agenda de groupe comme le suivant.



8.3. Installer et configurer Outlook Express

8.3.1. Pourquoi utiliser Outlook Express ?

Du fait qu'Outlook Explorer soit intégré à Microsoft Internet Explorer, il est devenu un logiciel de messagerie très courant. Outlook Express n'étant pas le logiciel de messagerie le plus utilisé en entreprise, il est plus apprécié sur les ordinateurs personnels.

Outlook Express est installé dans chaque système Windows car il est contenu dans l'installation de Internet Explorer et nécessite une configuration pour fonctionner avec un serveur de messagerie avant de pouvoir recevoir des messages via le protocole POP3 ou IMAP4. De plus, il permet de se connecter à des serveurs de news.

8.3.2. Comment configurer Outlook Express ?

Lors de la première utilisation d'Outlook Express, l'Assistant Nouvelle connexion s'exécute pour vous aidez à établir une connexion à Internet et si besoin à un réseau d'entreprise. Il va vous permettre de choisir votre type de connexion Internet, de définir les paramètres du Proxy et les paramètres du compte de messagerie. Les administrateurs et les utilisateurs peuvent accomplir cette tâche.

Ensuite, si un utilisateur veut modifier certains paramètres de sa messagerie, il peut faire cette modification directement dans Outlook Express ou dans un environnement d'entreprise, les administrateurs peuvent effectuer certaines modifications à l'aide d'outils de déploiement.

8.3.3. Configuration Initial d'Outlook Express

Le tableau suivant indique comment configurer votre compte de messagerie dans Outlook Express à l'aide de l'Assistant Nouvelle connexion.

Configurer	Faire
Courrier entrant	Sélectionner le protocole utilisé par votre serveur de messagerie et tapez le nom complet de celui-ci dans le champ Serveur de messagerie pour courrier entrant.
Courrier sortant	Tapez le nom complet du serveur SMTP utilisé dans votre réseau.
Compte de messagerie	Tapez votre nom de compte et votre mot de passe puis si votre serveur de messagerie nécessite une authentification avec un mot de passe sécurisé à partir d'un SSPI comme NTML, cocher la case concernant l'utilisation de l'authentification SPA.

8.3.4. Configuration supplémentaire dans Outlook Express

En supplémentant de la configuration initiale, vous avez la possibilité de configurer Outlook Express correspondant à l'utilisation dont vous avez besoin au sein de votre entreprise.

Tâche	Considération
Configurer Outlook Express pour un fonctionne hors connexion	Les utilisateurs téléchargent les en-têtes de messages puis télécharge le contenu du message qu'il souhaite. Ensuite lorsque les utilisateurs travaillent hors ligne, ils peuvent utiliser leurs messages comme s'il était en ligne. Une synchronisation s'effectuera directement lorsque l'utilisateur sera en ligne.
Configurer un compte supplémentaire.	Lors de la configuration initiale, vous pouvez créer qu'un seul compte de messagerie. Vous pouvez en créer d'autres à l'aide d'Outlook Express lui-même.
Utiliser POP3 pour consulter vos messages.	POP3 vous permet de télécharger vos messages à partir de n'importe quel ordinateur possédant une connexion Internet. Si vous souhaitez utiliser le protocole POP3 en tant qu'utilisateur itinérant, vous devez spécifier au serveur de conserver une copie de votre boîte de messagerie.
Utiliser IMAP pour consulter les informations à partir de dossiers de boîtes aux lettres	IMAP permet de consulter des boîtes de réception et des dossiers publics qui sont stockés sur des serveurs de messagerie à partir de n'importe quel ordinateur possédant une connexion Internet. Vous avez la possibilité de spécifier les dossiers que vous souhaitez voir et changer les paramètres de synchronisation pour ne télécharger que les en-têtes.
Utiliser WebDAV pour connecter à Outlook Express à Exchange	Une version d'Outlook Express permettant d'accéder à Exchange 2000 ou 2003 en WebDAV est incluse à partir de la version 5 d'Internet Explorer. En utilisant WebDAV, vous pouvez accéder à tous vos dossiers (Boîte de réception, Contacts, Calendrier, Courrier Indésirable, Tâches). Pour configurer Outlook Express avec WebDAV, vous devez configurer le serveur de courrier entrant avec le protocole HTTP.

8.3.5. Déployer Internet Explorer et Outlook Express automatiquement

Il n'est pas pratique de configurer toutes les fonctionnalités d'Outlook Express lorsque votre société possède beaucoup d'employée. Pour se faire, Microsoft met à votre disposition des outils vous permettant d'automatisé ces actions et d'effectuer leurs déploiement.

Le IEAK (*Internet Explorer Administration Kit*) est une collection d'outil vous permettant de personnaliser Internet Explorer et Outlook Express dans un environnement d'entreprise, par exemple :

- Etablir un contrôle de version.
- Distribution centralisé pour l'installation
- Configuration automatique des profiles en fonction de l'utilisateur
- Personnaliser les aspects d'IE, les fonctionnalités, la sécurité et les autres éléments importants.

Pour effectuer ces tâches vous devrez vous familiariser avec les outils suivants :

- *Internet Explorer Customization Wizard :* Un assistant que vous allez utiliser pour créer des packages de personnalisation pour IE.
- *IEAK Profile Manager :* Un outil qui vous permet de modifier les paramètres des utilisateurs automatiquement lorsqu' Internet Explorer est déjà installé.
- *IEAK Toolkit :* La trousse à outils de IEAK regroupe des outils, des programmes et des fichiers d'exemple tous aussi utiles les uns que les autres. Vous y trouvez notamment des outils permettant de créer des images animées et des fichiers d'exemple pour la procédure

d'inscription et l'ajout de modules complémentaires. Libre à vous de les utiliser pour faire bénéficier l'ensemble de votre entreprise des fonctionnalités d’IEAK.

9. Gestion du routage

9.1. Comment fonctionne le routage des messages dans une organisation Exchange ?

9.1.1. Les groupes de routages

Beaucoup de sociétés requièrent l'utilisation de plusieurs serveurs Exchange 2000 ou 2003 dans leur organisation Exchange. Lorsqu'un utilisateur étant connecté à un de ces serveurs et souhaite envoyer un message à un utilisateur situé sur un autre serveur, Exchange doit transférer le message entre ces deux serveurs. Le transfère de message entre des serveurs s'appel le *routage de message*.

Les administrateurs rassemble les serveurs Exchange en différents groupe de routage afin rendre plus efficace le routage de message entre les serveurs :

- Un **groupe de routage** est un groupe de serveurs exécutant Exchange interconnectés par des liaisons réseaux permanentes.
- Le **maître de groupe de routage** est le serveur qui stocke les informations d'état de liaison pour un groupe de routage. Il y en a un par groupe de routage. Lorsqu'il y a une modification de l'état d'une liaison (nouvelle liaison, liaison hors service ou modification de coût), le serveur sur lequel est défini le connecteur envoie une mise a jour au maître du groupe de routage qui va la notifier à tous les autres serveurs Exchange.

Au sein d'un groupe de routage, les messages sont transférés directement du serveur source au serveur de destination via le protocole SMTP. On parle alors d'envoi de messages en un saut unique. Aucune planification n'est requise. Par contre entre groupes de routage, les messages transitent entre les groupes de routage en passant par des serveurs pont (reliés par des connecteurs).

9.1.2. Les connecteurs de groupe de routage

Les connecteurs de groupe de routage sont des composants utilisés pour lier des groupes de routage pour que les messages puissent transiter de façon efficace et fiable entre les groupes. Vous pouvez créer un ou plusieurs connecteurs et les configurer et utiliser ces connecteurs pour contrôler :

- **Options de remise** : Permet à l'administrateur de créer des connecteurs qui transmettront les messages seulement pendant les périodes de temps spécifiées. Très utile lors de l'utilisation de liaisons non permanentes coûteuses.
- **Priorités autorisées** : Permet à l'administrateur de créer des connecteurs qui transmettront les messages possédant une priorité spécifique (Haute, Normal, Faible).
- **Types autorisés** : Permet à l'administrateur de créer des connecteurs qui transmettront les messages d'un type particulier (système ou non système).
- **Tailles autorisées** : Permet à l'administrateur de créer des connecteurs qui transmettront les messages inférieurs à la taille spécifié.
- **Restrictions de remise** : Permet à l'administrateur de créer des connecteurs qui transmettront les messages provenant de groupes d'utilisateurs spécifiés.
- **Coût** : Permet à l'administrateur d'assigner une valeur comprise en 1 et 100 indiquant le coût d'utilisation de ce connecteur pour l'envoi du message. Lorsque plusieurs routes existent pour envoyer un message, Exchange va sélectionner la route ayant le coût le plus **faible**.
- **Redirections de dossiers publics** : Permet à l'administrateur de créer des connecteurs qui autorisent les utilisateurs MAPI, OWA et IMAP d'accéder à des dossiers publics situés dans un autre groupe de routage. Par défaut, cette option est activée.

9.1.3. Utilisation de plusieurs groupes de routage

Vous pouvez utiliser seulement un groupe de routage si les serveurs Exchange que vous utilisez :
- possèdent une liaison permanente et faible reliant chaque serveur entre eux.
- sont membres de la même forêt Active Directory.
- sont connectés au maître du groupe de routage.

Plusieurs groupes de routage peuvent être nécessaire si l'un des paramètres suivant est rencontré :
- Les connections réseaux sont lentes et intermittentes.
- Le réseau est peu fiable ou instable.
- Le transfert de messages est complexe et indirect, il nécessite plusieurs sauts dans le réseau.
- La transmission de messages doit respecter différentes plages horaires suivant les différents emplacements.
- La structure de groupe de routage est créée pour empêcher des utilisateurs d'accéder aux répliquas de dossiers publics.

9.2. Configurer le routage dans votre organisation Exchange

9.2.1. Les connecteurs supportés

Exchange support 3 types de connecteurs :
- **Connecteur de groupe de routage** : Ce connecteur est le plus simple à configurer et permet de connecter des groupes de routages de la même organisation. Ce connecteur utilise le protocole SMTP pour transférer les messages aux autres serveurs. Lors de l'implémentation de ce connecteur, il faut savoir qu'il est unidirectionnel et donc le créer par paires (entrant et sortant). Le gestionnaire système Exchange simplifie le processus en créant et configurant automatiquement le second connecteur quand le premier est créé.
- **Connecteur SMTP** : Etablit une route pour transférer les messages SMTP entre deux groupes de routage ou entre un groupe de routage et un serveur SMTP. Comme le connecteur de groupe de routage, ce connecteur utilise le protocole SMTP qui fournit les avantages suivants :
  - Interconnecte une organisation Exchange avec un serveur SMTP non Exchange
  - Interconnecte des organisations Exchange indépendantes
  - Permet des configurations plus pointues entre des groupes de routage notamment en termes de planification et de routage.
- **Connecteur X.400** : Etablit une route pour transférer les messages X.400 entre deux groupes de routage ou entre un groupe de routage et un système X.400. Comme les connecteurs précédant, vous pouvez relier deux groupes de routage par contre ce connecteur fournit les avantages suivants :
  - Interconnecte un groupe de routage avec un système X .400.
  - Fournit une méthode efficace pour envoyer des messages de fortes tailles lorsque la connexion entre les deux groupes est lente mais fiable.
  - Créer une connexion réseau lorsque la connexion entre les deux groupes est en X.25.

9.2.2. Considération d'utilisation des connecteurs de groupe de routage

Avant d'implémenter des connecteurs de groupe de routage, vous devez considérer les caractéristiques suivantes :

- Peut être configuré pour utiliser zéro, un ou plusieurs serveurs de tête de pont. Comment configurer le nombre de serveurs de tête de pont :
    - **Aucun** : Utilisez cette configuration quand vous souhaitez que chaque serveur du groupe de routage agisse en tant que serveur de tête de pont.
    - **1** : Utilisez cette configuration quand vous souhaitez que tous vos emails circulent par un seul serveur afin de surveiller et d'archiver les messages.
    - **Plusieurs** : Utilisez cette configuration quand vous souhaitez assurer une certaine tolérance de panne. Lorsque que l'un d'entre eux tombe en panne, Exchange envoie tous les messages aux autres serveurs de têtes de ponts disponibles. L'autre avantage est que vous pouvez spécifier le serveur qui va envoyer et recevoir des messages avec d'autres groupes de routage.
- Doit être utilisé en combinaison avec TLS ou une stratégie de sécurité. Les serveurs utilisant Exchange fournissent un processus d'authentification quand ils effectuent le routage de messages par contre aucunes encryptions. Si vous nécessitez une couche de sécurité supplémentaire durant le transfert de messages, utilisez une des solutions suivantes :
    - **Configurez TLS** : Vous pouvez fournir un cryptage des messages en utilisant TLS (transport Layer Security) sur le serveur virtuel SMTP. Cependant, si vous configurez cette option sur un serveur virtuel SMTP, vous devez configurer TLS sur tous les serveurs de têtes de pont.
    - **Créez une stratégie de sécurité** : Vous pouvez fournir un cryptage des messages en utilisant une stratégie de sécurité d'Active directory qui va activer l'utilisation du protocole IPSec.
- Doit résoudre l'adresse IP du serveur de tête de pont : Lorsque un serveur de tête de pont qui support le connecteur de groupe de routage reçoit un message transmit par l'intermédiaire du connecteur, il le transmet à un autre serveur de tête de pont aléatoire et doit résoudre sont IP en utilisant les méthodes suivantes :
    1. Le serveur de tête de pont local tente de résoudre le serveur de tête de pont de destination définit dans le groupe de routage en interrogeant les enregistrements MX du serveur DNS.
    2. Si, ce qui est souvent le cas, l'enregistrement MX n'existe pas pour le serveur de destination, le serveur de tête de pont local interroge Active Directory pour trouver le FQDN du serveur de tête de pont destinataire.
    3. Le serveur local de tête de pont interroge ensuite le serveur DNS pour résoudre l'IP du FQDN récupéré dans Active Directory.
    4. Si la requête DNS pour le FQDN ne propose aucune réponse, le serveur de tête de pont local tente de résoudre l'adresse IP en utilisant le processus de résolution de nom standard en réseau local.

9.2.3. Considération d'utilisation des connecteurs SMTP

Avant d'implémenter des connecteurs SMTP, vous devez considérer les caractéristiques suivantes :

- Peuvent être utilisé pour identifier plusieurs serveurs de tête de ponts locaux : Le connecteur SMTP délivre tous les messages entre les groupes de routage en utilisant le serveur de tête de pont local. Contrairement aux options de configurations d'un connecteur de groupe de routage, vous ne pouvez pas configurer un serveur de tête de pont du groupe de routage distant.
- Peut être configuré pour utiliser le cryptage TLS des messages en partance : Les paramètres de sécurités configurés dans le connecteur SMTP surchargent les paramètres de sécurités du serveur virtuel SMTP.
- Doit obligatoirement résoudre le serveur de tête de pont distant en utilisant les enregistrements MX ou A dans le serveur DNS :
    1. Quand vous connectez des groupes de routage, le connecteur SMTP résout l'adresse de tête de pont en utilisant l'enregistrement DNS MX.

2. Vous ne pouvez pas spécifier les serveurs de tête de pont spécifique. Le connecteur SMTP tente premièrement de résoudre l'adresse IP du serveur de destination.
3. Si un enregistrement MX n'existe pas, le serveur émetteur tente de résoudre le serveur de destination en utilisant le processus de résolution de nom d'hôte, ce qui inclut les requêtes DNS pour les enregistrements de noms d'hôtes (A).

- Doit être configurer avec la plage d'adresses que vous pouvez utiliser pour contrôler quels messages peut transiter par ce connecteur SMTP : Chaque connecteur SMTP a au moins une plage d'adresses et peut y avoir un ou plusieurs groupes de routage associés. Par exemple, si vous utilisez deux connecteur SMTP dans votre organisation, vous pouvez en configurer un pour transmettre les messages à destinations des domaines *.fr et l'autres à destinations des domaines *.com.

9.2.4. Considération d'utilisation des connecteurs X.400

Avant d'implémenter des connecteurs X.400, vous devez considérer les caractéristiques suivantes :

- **Nécessité la configuration d'une pile de transport pour le service X.400 X.25 ou X.400 TCP/IP avec la création du connecteur** : Cette pile de transport va définir le type de réseau que va utiliser le connecteur X.400.
- **Ne supporte pas l'utilisation de multiples serveurs de tête de pont de chaque connecté du connecteur** : Pour assurer de la tolérance de panne ou un minimum de répartition de charge, vous devez créer plusieurs connecteur X.400.
- **Nécessite un espace d'adressage pour contrôler le routage des messages**.

9.2.5. Comment créer un groupe de routage

Lorsque vous installez le premier serveur Exchange, un groupe nommée *Premier groupe de routage* est automatiquement créé. Tous les autres serveurs qui exécutent Exchange sont installés dans ce groupe de routage tant que vous ne créez pas un nouveau groupe de routage.

Vous pouvez créer un nouveau groupe de routage à l'aide du gestionnaire système Exchange puis installer un nouveau serveur Exchange dans ce groupe ou alors déplacer un serveur existant dans ce groupe.

Pour créer un groupe de routage, vous devez effectuer les étapes suivantes :

1. Déployez le dossier groupe de routage dans la console gestionnaire système Exchange
2. Faites un clic droit sur ce dossier, cliquez sur **Nouveau** puis sur **Groupe de routage**.

9.2.6. Comment créer un connecteur de groupe de routage ?

Pour créer un connecteur de groupe de routage, vous devez au préalable avoir un serveur virtuel SMTP lié à au groupe de routage, plusieurs groupe de routage et suivre les étapes suivantes :

1. Déployez le dossier **Connecteurs** se trouvant dans le groupe de routage voulu.
2. Faites un clic droit sur ce dossier, cliquez sur **Nouveau** puis sur **Connecteur de groupe de routage.**
3. Dans la boîte de dialogue, spécifiez un nom et les serveurs locaux et distants de tête de pont.
4. Configurez les options de remise, les restrictions de remise et les restrictions sur le contenu dans les onglets nécessaires si besoin.

9.2.7. Surveiller l'état des serveurs, des connecteurs et des ressources.

L'outil **analyse et état** est un outil d'administration contenu dans le gestionnaire système Exchange que vous pouvez utiliser pour surveiller l'état et les performances des serveurs, des connecteurs et des ressources. Cet outil possède deux composants :

- **Notifications** : Permet de créer des notifications par email ou par script qui se déclanchent automatiquement lorsque l'état du serveur ou de ces connecteurs change.
- **Etat** : Permet de voir l'état de fonctionnement du serveur, des ressources et des connecteurs.

9.3. Concept et protocole pour la connectivité Internet

9.3.1. Fonctionnement du protocole SMTP

Quand un serveur Exchange communique avec un autre serveur, il envoi des commandes SMTP standard sur le port 25. Ce protocole fonctionne sur le système question/réponse, lorsque un serveur envoi une commande, il attend la réponse avant d'envoyer la prochaine commande.

Voici les étapes exécutées par un utilisateur lorsque celui-ci veut envoyer un message :

1. L'utilisateur initialise la communication avec le serveur SMTP, le serveur SMTP indique qu'il accepte la communication en renvoyant le code **220** suivit du **FQDN** du serveur (Service Mail + Version) **Ready** et la date du jour.
2. L'utilisateur répond à l'initialisation de communication en envoyant la commande **HELO.** Le serveur SMTP répond avec le code **250 <*FQDN*> Hello.**
3. L'utilisateur identifie l'envoyeur du message avec la commande **MAIL FROM:** Le serveur répond par le code **250**.
4. L'utilisateur identifie le destinateur du message avec la commande **RCPT TO:** Le serveur répond par le code **250**.
5. L'utilisateur indique qu'il est prêt à écrire le contenu du message avec la commande **DATA**. Le serveur réponde par le code **354**.
6. L'utilisateur clos la session avec la commande **QUIT**. Le serveur retourne alors le code **221** indiquant la fin de la session.

9.3.2. Principales commandes et codes de retour SMTP

SMTP se compose de différentes commandes transitant par le port TCP 25 et permet l'échange de données entre deux serveurs.

Commande	Description
HELO domaine_complet (FQDN, Fully Qualified Domain Name)	Identifie l'hôte expéditeur SMTP.
MAIL FROM:<expéditeur>	Identifie l'expéditeur du message.
RCPT TO:<destinataire>	Identifie le destinataire du message. Cette commande est utilisée pour chaque destinataire du message.
DATA	Indique que l'hôte expéditeur est prêt à envoyer le message.

RSET	Abandonne la transaction de messagerie en cours.
VRFY	chaîne Permet à l'hôte expéditeur de vérifier la validité du destinataire avant d'envoyer le message.
HELP	Énumère les commandes SMTP prises en charge par l'ordinateur destinataire.
QUIT	Déconnecte la session TCP.
TURN	Déclenche le serveur destinataire pour qu'il envoie les messages de la file d'attente destinés au serveur expéditeur. Cette commande est utilisée dans des environnements d'accès à distance pour interroger un hôte sur les messages de la file d'attente.

Pour chaque commande envoyée, un code de réponse SMTP est retourné pour informé de l'état de la transaction en cours.

Code de réponse	Description
220 domaine_complet (FQDN)	Le service est prêt.
221 domaine_complet (FQDN)	Le service ferme le canal de transmission.
250	L'action demandée est acceptée et a été exécutée.
354	Tapez le message. Terminez par <CRLF>.<CRLF>
450	Action demandée non exécutée : boîte aux lettres occupée.
451	Action demandée abandonnée : erreur locale lors du traitement.
452	Action demandée non exécutée : mémoire système insuffisante.
500	Erreur de syntaxe, commande non reconnue.
550	Action demandée non exécutée : boîte aux lettres indisponible ou introuvable.
552	Action demandée abandonnée : allocation de mémoire dépassée.
554	Échec de la transaction.

9.3.3. Fonctionnement de la connexion ESMTP

ESMTP est un protocole étendu des fonctionnalités SMTP en fournissant des options supplémentaires. ESMTP support des commandes supplémentaires comme l'authentification d'hôtes et le cryptage.

ESMTP autorise le serveur destinataire d'informer le client (ou serveur) émetteur des extensions qu'il support. Il n'est pas nécessaire d'effectuer des modifications sur l'émetteur ou le récepteur pour utiliser ESMTP. Comme Windows 2000 et 2003, certains serveurs SMTP supporte les connexions ESMTP.

Comment ESMTP se connecte :

1. le poste émetteur initialise la connexion avec le serveur destinataire. Le serveur doit retourner le code **220**, indiquant qu'il a ouvert la connexion.
2. Le poste émetteur va envoyer la commande **EHLO** au lieu de **HELO**. Le serveur peut répondre de deux façons :
    a. Si le serveur support les commandes ESMTP, il va retourner le code **250** indiquant qu'il accepte la session et propose au poste émetteur de continuer. Le serveur va ensuite envoyer la liste de extensions SMTP qu'il support.
    b. Si le serveur ne support pas les commandes ESMTP, il va tout simplement retourner le code **500** correspondant à une commande inconnue. Dans ce cas, le post émetteur n'a plus qu'à envoyer la commande **HELO** pour initier une communication **SMTP**.

9.3.4. Principales commandes ESMTP

Certain serveur prennent en charge le jeu de commande ESMTP qui étend le nombre de commandes de messagerie disponibles.

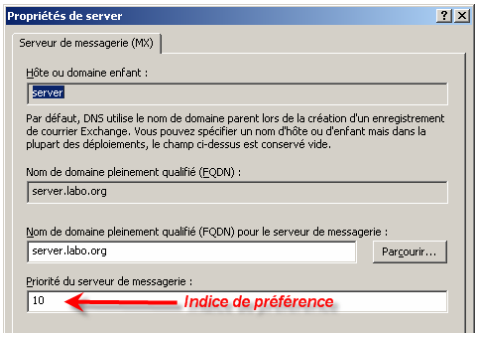
Commande du serveur	Description
ATRN	La commande Authenticated TURN n'est exécutée que si la session a été authentifiée. Cette commande est décrite dans la RFC 2645.
ETRN	Fonction identique à TURN, mais spécifie l'hôte distant auquel sera remis le message. Cette commande est décrite dans la RFC 1985.
PIPELINING	Permet l'envoi par lot des commandes SMTP sans attendre la réponse de l'ordinateur destinataire. Le protocole est ainsi plus efficace.
CHUNKING	Permet d'envoyer plus efficacement des messages MIME *(Multipurpose Internet Mail Extensions*) de grande taille par segmentation des données lors du transport entre les hôtes SMTP.
X-EXPS GSSAPI NTLM LOGIN	Utilise un mécanisme d'authentification qui prend en charge Kerberos et NTLM (Windows NT LAN Manager). Cette commande prend en charge le même mécanisme d'authentification que AUTH.
X-EXPS=LOGIN	Utilise un mécanisme d'authentification spécifique à Exchange Server 5.5 prenant en charge NTLM pour assurer la compatibilité avec Exchange Server 5.5.
X-LINK2STATE	Spécifie la prise en charge des commandes d'état des liens Exchange 2000.
XEXCH50	Utilisée lors de l'établissement d'une connexion à un autre serveur exécutant Exchange. La commande XEXCH50 permet de transférer un contenu Exchange spécifique dans des messages.
STARTTLS	Établit une connexion SSL (*Secure Sockets Layer*) entre le client et le serveur SMTP. Le système client doit établir une connexion TLS (*Transport Layer Security*).
AUTH mécanism SASL	Fournit une forme d'authentification SASL (*Simple Authentication and Security Layer*) pour authentifier les hôtes SMTP à l'aide de Kerberos et NTLM.
AUTH=LOGIN	Fournit une forme d'authentification SASL pour les clients tels que Netscape et Exchange Server 5.5 qui nécessitent cette authentification de base SMTP.
HELP	Demande la liste des commandes prises en charge par l'hôte SMTP. Cette commande est décrite dans la RFC 821.
VRFY	Désactivée par défaut, elle permet de déterminer si un compte de messagerie existe. De nombreux administrateurs considèrent que l'activation de cette commande représente un risque en matière de sécurité. Cette commande est décrite dans la RFC 821.
DSN	Génère et envoie une notification d'état de remise (DSN, *Delivery Status Notification*) à l'ordinateur expéditeur en cas d'échec de la remise. Cette commande constitue une amélioration par rapport au mécanisme du rapport de non-remise (NDR, *Non-Delivery Report*). Cette commande est décrite dans la RFC 1891.
SIZE	Détermine la taille d'un message avant de l'accepter. Auparavant, un message devait être transmis totalement ou partiellement au système de réception avant de pouvoir être rejeté pour des raisons de dépassement de la taille maximale. Cette commande est décrite dans la RFC 1870.

9.3.5. Enregistrement MX

Un enregistrement MX (*mail exchanger*) est un enregistrement DNS qui indique l'adresse IP d'un serveur de messagerie dans votre domaine. Il existera autant d'enregistrement MX dans votre serveur DNS que de serveurs disponible dans votre entreprise.

Si un serveur SMTP devient inaccessible pour une raison quelconque, que se passe-t-il ?

1. L'émetteur SMTP cherche tous les enregistrements MX disponible sur le serveur DNS et résout l'enregistrement ayant la préférence la plus faible. Si celui-ci n'est pas accessible, la même action sera effectuée sur l'enregistrement suivant dans l'ordre des préférences.
2. Lorsque l'adresse d'un serveur est résolue, le client SMTP va tenter d'établir une session avec ce serveur.



9.4. Gérer la connectivité à Internet

9.4.1. Etapes que vous pouvez réaliser pour contrôler l'accès Internet au e-mail

Il n'est pas nécessaire de créer un connecteur pour les emails, pour connecter des serveurs dans votre organisation, pour relier votre serveur Exchange à Internet. C'est le serveur SMTP par défaut qui est créé lors de l'installation d'Exchange qui effectue toutes ces tâches.

Vous pouvez interagir avec la configuration de ce serveur virtuel afin de contrôler comment ce connecte Exchange à Internet. Vous pouvez :

- Créer des serveurs virtuels supplémentaires et configurer un connecteur SMTP pour utiliser l'utiliser en tant que serveur de tête de pont : Vous pouvez effectuer cette configuration domaine par domaine afin de contrôler les options de remise, les restrictions de remise, l'Espace d'adressage et les restrictions sur le contenu. Dans ce scénario, le connecteur SMTP vient surcharger les paramètres du serveur virtuel.
- Limiter l'étendue d'un connecteur SMTP au groupe de routage : Si vous souhaitez que les messages dans un autre groupe de routage soient délivrés par ce connecteur SMTP.
- Configurer l'utilisation d'un compte sur le connecteur SMTP si celui est configuré pour délivrer les messages sur serveur SMTP nécessitant une authentification.
- Configurer le connecteur SMTP seulement pour qu'il reçoive et envoie des emails : Par exemple, si votre serveur Exchange ne parvient pas effectuer de requête DNS inversé pour les adresses Internet et que vous voulez désigner ce serveur comme étant la passerelle Internet. Vous devez donc configurer un connecteur SMTP et lui désigner un serveur de tête de pont à utiliser ainsi que configurer l'étendu du connecteur, le routage des messages et l'espace d'adressage.
- Configurer les paramètres de formats des messages Internet et la remise des messages : Vous avez la possibilité de configurer un format de message spécifique par domaine de destination par exemple.

9.4.2. Méthodes de sécurisation du trafic SMTP

Vous avez la possibilité de sécuriser le trafic SMTP en utilisant les méthodes d'authentification, de cryptage des données qui transitent sur le réseau et le contrôle effectué par requête DNS inversée.

Le principe de l'authentification est de vérifier que l'utilisateur est bien celui qu'il prêtant être. Exchange support trois méthode d'authentification permettant de s'adapter à votre environnement :

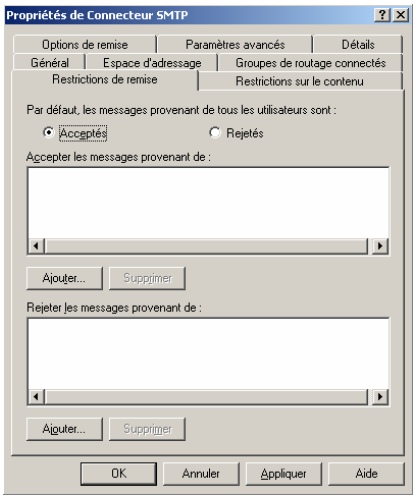
- ***Authentification anonyme*** : Cette méthode qui justement ne propose aucune authentification, considère que vous êtes connecté en tant utilisateur anonyme et la solution qui fournit un accès limité au dossier public. Cette méthode est supportée par tous les types de clients.
- ***Authentification de base*** : Permettant d'authentifier un utilisateur, cette méthode est la plus simple et la moins sécurisé car le login et le mot de passe de la personne transite en clair sur le réseau. Cette méthode est supportée par la plupart des clients.
- ***Authentification intégrée à Windows*** : Cette méthode est la plus sécurisée, efficace et transparente des méthodes proposées. L'avantage de cette méthode est quelle utilise l'authentification que vous avez effectuée pour ouvrir une session sur votre ordinateur.

Le cryptage permet de dissimuler le contenu du message en y appliquant un algorithme permettant de rendre ce message totalement illisible aux personnes ne possédant pas la clef pour le décoder. Sachant que l'authentification ne permet pas de rendre le message totalement sécurisé lors de son transfert sur le réseau, vous allez pouvoir utiliser TLS pour crypter le contenu de celui-ci entre le client et le serveur. TLS nécessite l'utilisation d'un certificat SSL X.509 qui va crypter l'intégralité de la session TCP/IP entre le client et le serveur permettant de sécurisé une méthode d'authentification envoyant les mots de passe en clair.

Un des problèmes majeurs associés à Internet est l'IP *Spoofing*, cette attaque consiste à utiliser l'adresse IP d'une machine considéré comme de confiance et de tenter d'accès à des ressources sur le réseau. Pour palier à ce genre d'attaque, vous pouvez utiliser les requêtes DNS inversé permettant de vérifier sur le serveur DNS de l'émetteur du message si l'adresse utilisé est bien une adresse de son réseau.

9.4.3. Comment restreindre un utilisateur d'envoyer des messages sur Internet?

Certaines entreprises ne nécessitent pas que tous ces employés possèdent une adresse email utilisable sur Internet. Par exemple, une entreprise qui utilise beaucoup d'intérimaire peut souhaiter que ces personnes temporaires n'aient accès qu'à une messagerie interne afin d'échanger des informations avec les autres employés de l'entreprise. L'administrateur peut alors configurer un connecteur SMTP n'autorisant que à certains groupes ou personnes l'envoie de messages sur Internet.



Pour contrôler qui peut envoyer des messages, vous devez utiliser les options de l'onglet restrictions de remise pour spécifier l'action des utilisateurs par défaut, quels sont ceux qui peut envoyer et ceux qui ne peuvent pas.

9.4.4. Comment configurer un relais SMTP dans Exchange ?

Un relais SMTP est un serveur SMTP qui transmet les messages à un autre serveur SMTP sans résoudre l'adresse du destinataire. Vous pouvez créer un connecteur SMTP pour transférer des messages à partir d'Exchange vers n'importe quel système de messagerie compatible SMTP. C'est le serveur de tête de pont ou le serveur que vous définissez qui va se charger de délivrer le message au serveur contenant la boîte aux lettres de destinations.

La liste ci-dessous décrit les six différentes méthodes pour configurer un relais SMTP :

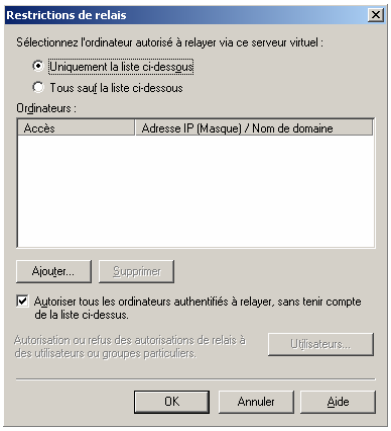
- ***Configurer un serveur virtuel SMTP pour utiliser un hôte actif*** : Par défaut, le serveur Exchange utilise DNS pour router vers les espaces d'adressage du connecteur. Vous avez la possibilité de transférer tous les courriers via un connecteur spécifié dans l'onglet général d'un connecteur SMTP aux hôtes actifs sans tenter de résoudre le domaine SMTP du destinataire. Pour spécifier l'emplacement de l'hôte actif, vous pouvez entrer le FQDN ou l'adresse IP (entre []).
- ***Configurer un connecteur SMTP pour utiliser un hôte actif*** : Le connecteur SMTP aussi utilise par défaut la résolution DNS pour transférer les messages vers le bon serveur SMTP. Vous pouvez aussi spécifier l'hôte actif à utiliser dans le menu Remise avancée de l'onglet Remise des propriétés sur serveur virtuel SMTP.
- ***Configurer le serveur virtuel SMTP pour transférer les messages non résolus à un hôte actif*** : Vous configurez le serveur virtuel SMTP pour transférer tous les messages dont les destinataires n'ont pas été résolus vers l'hôte spécifié dans l'onglet Messages des propriétés d'un serveur virtuel SMTP. Si l'hôte actif n'arrive pas à résoudre le nom du destinataire, le message sera retourné avec un NDR.
- ***Configurer un serveur virtuel SMTP comme serveur relais*** : Pour utiliser un serveur SMTP en tant que relais, vous devez l'autoriser à relayer les messages provenant de serveurs spécifiques dans le menu restrictions de relais dans l'onglet Accès. Vous allez pouvoir bloquer ici les serveurs qui utilisent votre serveur SMTP comme relais SMTP.
- ***Configurer les domaines vers lesquelles le connecteur SMTP va relayer les messages*** : Vous souhaitez que votre serveur reçoive des messages à partir de n'importe quel domaine mais vous souhaitez restreindre les domaines vers lesquelles votre serveur peut relayer des messages. Pour ce faire utilisez l'onglet Espace d'adressage dans les propriétés du connecteur SMTP.

9.4.5. Quand utiliser et restreindre le relais dans Exchange.

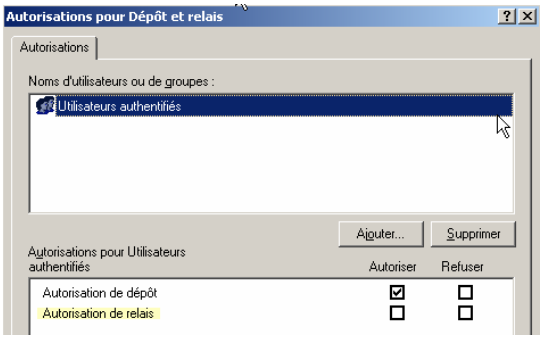
Des restrictions de relais peuvent être définies afin d'empêcher que certaines personnes mal intentionnées utilisent votre serveur SMTP comme relais pour des envois en masse (bulk) ou de messages polluants (spam). Pour cela, vous pouvez autoriser un ordinateur, un groupe d'ordinateur, ou un domaine à relayer les messages ou limiter les domaines vers lesquels vous allez relayer les messages.

Pour empêcher Exchange d'être utiliser par tous les utilisateurs en tant que relais de messages, il faut :

- modifier dans l'onglet Accès du serveur SMTP par défaut de votre serveur les restrictions de relais.
- Puis, vérifier que vous avez sélectionné l'option **Uniquement la liste ci-dessous** et que la liste des ordinateurs est vide. (Configuration par défaut).
- Ne pas sélectionner la case **Autoriser tous les ordinateurs authentifiés à relayer, sans tenir compte de la liste ci-dessus** si vous utilisez des clients POP3 et IMAP4.



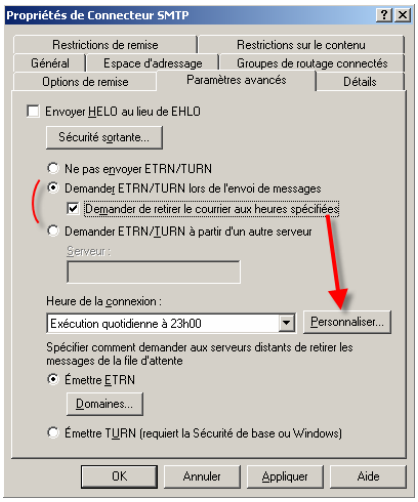
Pour empêcher des groupes d'utilisateurs à utiliser votre serveur en tant que relais de messages, il faut, ne pas sélectionner la case **Autoriser tous les ordinateurs authentifiés à relayer, sans tenir compte de la liste ci-dessus** et cliquez sur le bouton **Utilisateurs…** pour spécifier les utilisateurs ou les groupes auxquels vous donnez l'autorisation de relais.



9.4.6. Comment configurer Exchange pour qu'il récupère des e-mails à stocker chez le FAI

Vous pouvez utiliser un connecteur SMTP pour mettre en place une relation « Tirer » avec des serveurs (souvent employé lorsque la sécurité de la messagerie confiée à un fournisseur d'accès charger de filtrer les virus). Il faut dans ce cas passer par une requête TURN ou ETRN (que l'on peut planifier) sur le serveur distant pour transférer les messages en file d'attente vers le serveur local.

Ces options se configurent dans l'onglet Paramètres avancés des propriétés du connecteur spécifique.



9.4.7. Comment identifier les problèmes de messageries liées aux domaines

Il existe deux outils permettant d'identifier des problèmes de messageries liées aux domaines :

- **Telnet** : Cette commande permet de se connecter et d'ouvrir une session sur un serveur en utilisant un port TCP de son choix. Par exemple, pour un client ayant un problème de connectivité POP3, il faut taper la commande : ***TELNET serveur 110***. Une fois connecté, il suffit de s'authentifier et de lister les messages de la boîte de réception.
- **Nslookup** : L'utilitaire NSLOOKUP vous permet d'accéder aux informations de messagerie fournies par le serveur DNS (nslookup –querytype=mx *domaine*) ce qui permet de vérifier l'existence des enregistrements MX et A sur le serveur DNS pas exemple.

10. Prise en charge des périphériques mobiles par Exchange Server 2003

10.1. Gérer les composants des services mobiles

10.1.1. Quels sont les composants des services mobiles d'Exchange Server 2003

Exchange prend en charge un accès spécifique dédié aux périphériques mobiles, sans fil comme les téléphones mobiles, les PDA ou les smartphones. Les utilisateurs nomades utilisent Exchange ActiveSync et Outlook Mobile Access qui sont deux des composants qui sont inclus directement dans Exchange 2003 pour synchroniser leur calendrier, leurs contacts et leurs messages.

Les périphériques compatible ActiveSync comme les Pockets PC 2002, les smartphones 2002 et ceux fonctionnant sous Windows Mobiles 2003, utilisent le service ActiveSync pour synchroniser leurs informations (Boîte de réception, sous-dossier, calendrier, contact, tâches).

10.1.1.1. Exchange ActiveSync

Les deux types de synchronisation proposés aux utilisateurs qui sont supporté par Exchange ActiveSync sont manuels et planifié. Par contre, Exchange peut initialiser la synchronisation en envoyant des notifications de mise à jour pour indiquer aux périphériques mobiles que de nouveaux éléments sont disponibles.

Pour pouvoir bénéficier des notifications de mise à jour, il faut en premier lieu activer les notifications actualisées dans les propriétés de service mobiles, effectuer une synchronisation complète avec le périphérique mobile puis spécifier les dossiers susceptibles de déclencher une notification. Ensuite lorsque d'un nouvel événement serra créer dans l'un de ces dossiers, Exchange Server créera une notification SMTP à destination du périphérique. Une fois cette notification reçu le périphérique déclenchera une synchronisation avec le serveur.

10.1.1.2. Outlook Mobile Access

Le service Outlook Mobile Access fournit une interface web permettant un accès aux serveurs Exchange aux utilisateurs possédant des périphériques mobiles. Les périphériques téléphoniques ou les PDA utilisant un navigateur XHTML, compact HTML ou standard peuvent accéder par ce service à leur boîte de réception, leur calendrier, leurs tâches et faire des recherches dans la liste d'adresses globale. Outre les téléphones mobiles, les périphériques Windows Mobile utilisant Internet Explorer 6.0 ou ultérieur accède à ce service.

Si votre entreprise utilise Microsoft Mobile Information Server 2001 ou 2002 Edition entreprise, vous devez faire attention au problème de compatibilité avec le service d'Exchange 2003 :

- Mobile Information Server communique avec Exchange 5.5 pour fournir le service Outlook Mobile Access et avec Exchange 2000 pour fournir les services Outlook Mobile Access et ActiveSync.
- Seuls les composants mobiles Exchange 2003 peuvent fournir un accès aux boîtes aux lettres aux périphériques mobiles.

10.1.2. Que nécessite Exchange Server 2003 pour utiliser les services mobiles

Le service Outlook Mobile Access a été développé pour fonctionner et pour tirer avantage du Framework .NET 1.1 et de l'ASP.NET. Les périphériques supportés par Exchange Serveur 2003 sont définit par mise à jour à l'aide du service ASP.NET Device Update (http://www.asp.net/mobile/).

Vous avez la possibilité de développer des applications Web pour périphérique mobiles grâce à Microsoft Mobile Internet Toolkit.

10.1.3. Utilitaire que vous pouvez utiliser pour administrer les composants mobiles

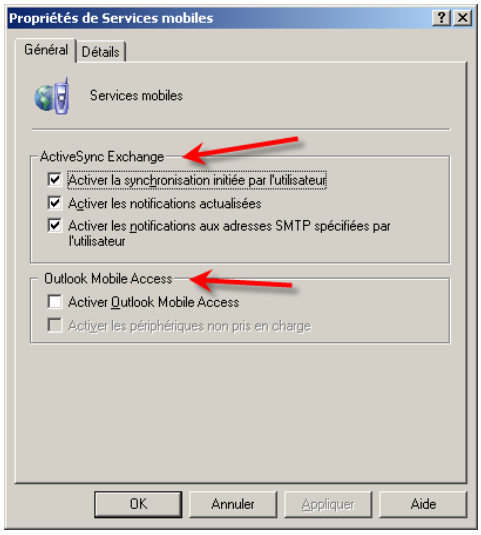
Pour configurer tous les paramètres liés aux services mobiles, vous pouvez utiliser les utilitaires suivants :

- ***Gestionnaire Système Exchange*** : Utilisé dans un premier temps pour configurer les services Outlook Mobile Access et ActiveSync au sein de l'organisation, il sera utilisé dans un second temps pour configurer le connecteur SMTP pour qu'il transmette les notifications vers les mobiles.
- ***Gestionnaire IIS*** : Utilisé pour configurer les options de sécurité lié aux connections des périphériques mobiles. Le paramétrage de ces options revient à effectuer les mêmes actions que de configurer les options pour Microsoft Outlook Web Access en utilisant le gestionnaire IIS.
- ***Utilisateurs et ordinateurs Active Directory*** : Utilisé pour contrôler l'accès mobile pour chaque utilisateur individuellement. Exchange ActiveSync et Outlook Mobile Access sont autorisé par défaut pour tous les utilisateurs mais Outlook Mobile Access est désactivé sur le serveur Exchange 2003.

10.1.4. Comment configurer les propriétés des services mobiles dans le gestionnaire système Exchange

Par défaut, seul le service ActiveSync est activé dans les paramètres globaux d'Exchange avec toutes ces options.

Pour modifier les paramètres globaux des services mobiles, vous devez utiliser le gestionnaire système Exchange puis naviguer dans les propriétés des services mobiles situés dans le dossier paramètres globaux.



10.1.4.1. Configuration d'ActiveSync

- ***Activer la synchronisation initiée par l'utilisateur*** : Les utilisateurs ont la possibilité d'utiliser leur périphérique mobile pour démarrer une synchronisation des données.
- ***Activer les notifications actualisées*** : Exchange Server va pouvoir envoyer des notifications aux périphériques mobiles afin de les inciter à se synchroniser lors de la réception d'un nouvel élément.
- ***Activer les notifications aux adresses SMTP spécifiées par l'utilisateur*** : Permet aux utilisateurs utilisant n'importe quel opérateur téléphonique de synchroniser sa boîte de réception. Utilisez cette option si vous ne souhaitez pas spécifier des opérateurs mobiles dans Exchange.

10.1.4.2. Configuration De Outlook Mobile Access

- ***Activer Outlook Mobile Access*** : Cette fonctionnalité autorise les utilisateurs à se connecter à partir d'un périphérique Windows Mobile, iMode ou n'importe quel téléphone compatible XHTML pour accéder à leurs emails, leurs contacts, leur calendrier et leurs tâches.
- ***Activé les périphériques non pris en charge*** : Cette fonctionnalité permet d'autorisé les téléphones portables non pris en charge comme le WAP 1.0. Il n'est pas impossible que lors de connexions, ces téléphones affichent des résultats non attendus.

10.1.5. Comment configurer Exchange ActiveSync et les mises à jour par notifications ?

Les modifications apportées à Active Directory concernant les services mobiles ActiveSync et Outlook Mobile Access sont effectués durant le ForestPrep. L'installeur d'Exchange quand à lui se charge d'installer Exchange Event Source (EES) permettant d'envoyer les notifications de mise à jour.

Pour envoyer des notifications à destinations des téléphones portables, vous allez créer un objet Opérateur Mobile soit en utilisant le gestionnaire système Exchange ou soit en important des données de configuration au format LDIF fournit par un opérateur mobile comme MSN Mobile qui est l'opérateur mobile de Microsoft. MSN Mobile est en accord avec de nombreux opérateurs téléphoniques dans le monde (en France, MSN Mobile couvre le réseau Bouygues Telecom), ce qui peut vous permettre de créer un unique point de sortit pour les notifications en direction des appareils téléphoniques.

Une fois les opérateurs mobiles créés dans Active Directory, les utilisateurs Windows Mobile 2003 vont être autorisé à choisir leur opérateur parmi ceux disponibles.

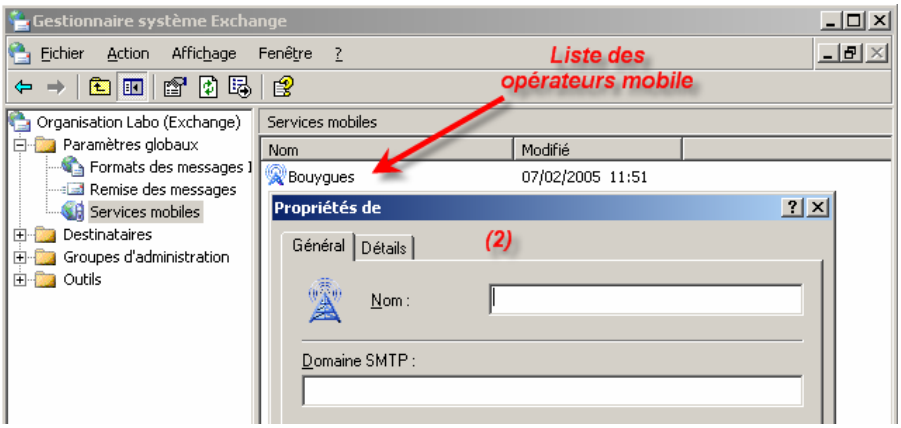
Pour permettre à votre organisation Exchange de transmettre tous les messages à destination de vos téléphones portables par l'intermédiaire d'un seul opérateur, vous devez utiliser MSN Mobile :

1. Connectez-vous sur le site MSN Mobile en utilisant votre compte .Net passeport, puis sélectionnez dans les opérateurs disponibles ceux dont vous avez besoin.
2. Configurer Active Directory pour qu'il utilise MSN Mobile en important le fichier LDIF fournit par celui-ci.
3. Créez un connecteur SMTP sur votre serveur de tête de pont en direction de MSN Mobile en utilisant les informations d'authentifications reçu lors de l'inscription.

Pour autoriser l'envoi des notifications directement à vos téléphones portables, vous devez créer le suffixe SMTP des opérateurs téléphoniques :

1. Dans le gestionnaires système Exchange, faites un clic droit sur l'icône services mobiles et cliquez sur nouveau → Opérateur mobile…
2. Entrez le domaine SMTP de l'opérateur.

3. Dites à vos utilisateurs mobiles de sélectionner leur opérateur téléphonique en utilisant Exhange ActiveSync.



10.1.6. Considération pour sécuriser les composants mobiles

Afin de pouvoir sécuriser les communications avec les mobiles, il est nécessaire de configurer un accès sécurisé aux serveurs frontaux et d'appliquer la topologie la mieux adaptée à nos besoins (ISA Server, DMZ).

Vous pouvez sécuriser la connexion entre le serveur Exchange et le client mobile en utilisant un certificat SSL (Secure Sockets Layer). Pour y parvenir, vous devez placer un certificat sur les répertoires virtuels IIS Outlook Mobile Access et Exchange ActiveSync sachant que pour que la communication fonctionne avec Exchange ActiveSync, vous devez utiliser un certificat reconnu par les périphériques Windows Mobile. Windows Mobile fait confiance aux certificats les plus populaires et ne risque de ne pas marcher lors de la synchronisation si vous déployez votre propre certificat.

Outlook Mobile Access est utilisé comme Outlook Web Access. Il fonctionne avec une topologie serveur frontal/dorsal, c'est pourquoi lors du déploiement du serveur frontal, vous pouvez assurer la protection de celui-ci à l'aide d'ISA serveur.

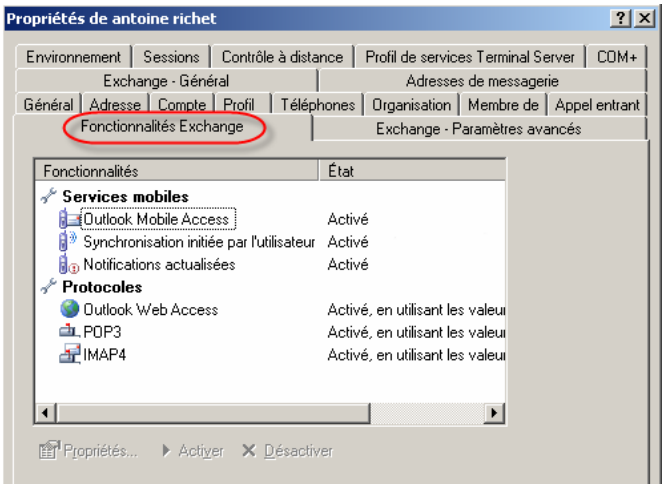
Les clients Windows Mobile Pocket PC, Windows Mobile PC Phone Edition et les périphériques Smartphone étant basés sur Windows CE peuvent se connecter à l'aide de VPN ou RAS. C'est deux technologies permettent de se connecter à votre réseau interne de manière sécurisée avant d'initier la connexion avec Exchange Server.

10.2. Activer les comptes utilisateurs pour un accès mobile

Lorsque vous autorisez un compte utilisateur à utiliser l'accès mobile, vous l'autorisez à afficher sa boîte de réception sur son périphérique mobile.

Utiliser l'onglet Fonctionnalités Exchange pour activer Outlook Mobile Access utilisateurs par utilisateurs.

Pour permettre les synchronisations et les notifications, activés les deux autres services mobiles.



10.2.1. Comment configurer les périphériques pour la synchronisation

Après avoir autorisé un utilisateur à synchroniser sa boîte de réception avec son périphérique mobile, vous devez configurer celui-ci pour qu'il puisse utiliser ActiveSync et les notifications de mise à jour.

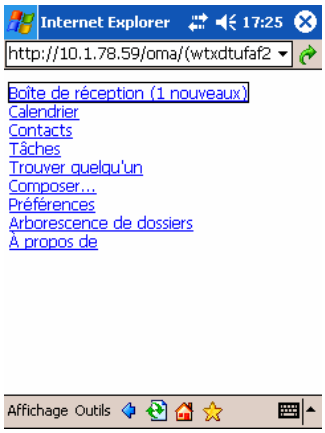
Les étapes suivantes indiquent comment configurer un périphérique Windows Mobile 2003 pour utiliser Exchange ActiveSync :

1. Ouvrez **ActiveSync** sur le périphérique.
2. Dans l'onglet Serveur :
    a. Spécifiez le nom du serveur.
    b. Si votre Exchange Server est configuré pour utiliser SSL, sélectionnez **Ce serveur util. des connexions SSL**.
3. Cliquez sur **Options…** spécifiez un nom d'utilisateur, un mot de passe, et un nom de domaine.
4. Sélectionnez l'option **Enregistrer le mot de passe** si vous ne voulez pas renseigner les informations d'authentification à chaque synchronisation.
5. Sélectionnez les éléments que vous souhaitez synchroniser.
6. Configurez les options de synchronisation pour chaque élément sélectionné.
7. Configurer l'adresse du périphérique.

Pour utiliser les notifications de mise à jour, vous devez utiliser un périphérique utilisant le système d'exploitation Windows Mobile 2003. La fonctionnalité de synchronisation apparaîtra une fois la première synchronisation effectuée. Suivez les démarches suivantes pour pouvoir configurer les notifications :

1. Ouvrez **ActiveSync** sur le périphérique
2. Dans l'onglet Planification du mobile, choisissez les intervalles de synchronisation pendant les heures de pointes et en dehors des heures de pointes.
3. Synchronisez votre périphérique avec Exchange afin qu'il sauvegarde ces paramètres.

10.2.2. Comment configurer le périphérique pour utiliser Outlook Mobile Access



Effectuez ces étapes pour configurer le périphérique Windows Mobile afin qu'il utilise Outlook Mobile Access :

1. Sur le périphérique, démarrez Microsoft Internet Explorer.
2. Tapez l'URL suivante correspondant à votre Exchange Server : http://*server*/oma
3. Dans la page d'authentification, tapez votre login et votre mot de passe.

Les étapes suivantes permettent d'utiliser un périphérique compatible XHTML pour se connecter au serveur Outlook Mobile Access :

1. Sélectionnez le service WAP
2. Tapez l'url https://Serveur_Exchange/oma

11. Gestion du stockage des données et des ressources matérielles

Pour optimiser les performances d'un serveur Exchange 2003 durant les transactions des utilisateurs et tâches administratives, les administrateurs ont besoin d'avoir une visibilité parfaite sur la gestion de l'espace de stockage et l'utilisation de celui par le système Exchange.

Quelle est la meilleure configuration matérielle pour le stockage de vos boîtes aux lettres ?
Devez vous utiliser du RAID5 plutôt que du RAID 0+1 ?
Quelles sont les étapes pour migrer matériellement un serveur Exchange 2003 ?

11.1. La technologie ESE

La gestion des données Exchange 2003 est gérée par le moteur ESE (Extensible Storage Engine), cette technologie fait le lien entre Exchange et Active Directory ; ESE est un moteur de base de données régulant la lecture /écriture entre les différentes opérations sur le serveur Exchange afin de les valider en tant que transaction.

-Une opération est une simple opération, comme supprimer ou ajouter une donnée, comme il est possible de le faire dans une base de données SQL classique avec la fonction (INSERT VALUE)

-Une transaction est un ensemble d'opérations aboutissant à une action portant vers le même but.

Le moteur ESE d'Exchange se base sur le procédé ACID afin de garantir l'intégrité des données.

ACID est composé de 4 étapes :

-**Atomique (Atomic):** Processus qui valide une transaction uniquement après l'exécution de toutes les opérations.
-**Conformité (Consistent)** : Processus vérifiant que la base de données passe d'un état fiable à un autre après exécution des transactions
- **Isolation (Isolated)** : Les changements de la base de données seront appliqués uniquement après que les transactions soient validées (COMMIT)
-**Durable (Durable)** : Les transactions validées sont conservés au cas où le serveur Exchange serai en panne.

11.2. Le stockage des données Exchange

Exchange stocke les données dans des bases de données logiques appelé banques. Exchange peut avoir plusieurs banques stockées dans des bases de données, elles-mêmes contenues dans des groupes de stockage.

11.2.1. Les groupes de stockage :

Exchange utilise des conteneurs appelés « groupe de stockage » pour regrouper des banques de boîtes aux lettres et dossiers publics partageant le même espace de fichier de log. Un groupe de stockage peut contenir jusqu'à 5 banques utilisant un seul jeu de fichiers journaux.
Les banques au sein d'un groupe de stockage peuvent être administré individuellement ou en groupe.

11.2.2. Les banques :

- Les banques de boîtes aux lettres : contenant les mails privés des utilisateurs
- Les dossiers publics : contenant des informations non privées partagées accessible par un grand nombre d'utilisateurs selon les droits attribués.

Chaque banque est composée de deux fichiers :

- Le premier fichier porte l'extension **EDB,** ce fichier contient les données utilisées par les clients MAPI (Microsoft Outlook); les mails, les répertoires. Ces informations sont consultées depuis un client MAPI accédant au fichier EDB contenant les informations. Ce fichier est également appelé Rich Text database file.

- Le deuxième fichier porte l'extension **STM,** ce fichier contient toutes les informations non relatives aux clients MAPI (Outlook express, HTTP via OWA, NNTP, POP3). Ce fichier est également appelé Streaming database file.

Néanmoins ces deux fichiers sont emmenés à travailler ensemble car le fichier **STM** contient uniquement des documents de type RAW, et le fichier **STM** a besoin de lire des méta données dans le fichier EDB pour formater correctement le contenu des documents RAW.

11.2.3. Les fichiers journaux :

Exchange conserve un historique des transactions dans des fichiers journaux. En cas de défaillance du serveur Exchange, il sera alors possible de restaurer les données en exécutant les dernières transactions présentes dans les fichiers journaux.

11.3. Processus de stockage des données Exchange

Le moteur ESE a la charge d'écrire et de lire les données dans les groupes de stockage, et de gérer les messages avec le fichier EDB et/ou STM. Ce processus se fait en fonction du client utilisé, MAPI ou non MAPI.

11.3.1. Connexion avec un client MAPI

Lorsqu'un client MAPI Microsoft Outlook se connecte à un serveur Exchange pour envoyer un mail M1, alors le mail M1 est directement stocké dans le fichier Rich Text EDB. Lorsque le destinataire du message ouvre le mail avec son client Outlook, le mail est directement ouvert depuis le fichier EDB.

11.3.2. Connexion avec un client Non-MAPI

Lorsqu'un client non MAPI, comme un utilisateur Outlook Web Access, POP3, NNTP ou IMAP4 ouvre une session sur le serveur Exchange pour lire le mail M1 préalablement envoyé par le client MAPI ; le contenu du mail M1 est automatiquement converti au format approprié avant d'être lu par le client par le processus de « **conversion à la demande** ».
Lorsqu'un client non MAPI, comme un utilisateur Outlook Web Access, POP3, NNTP ou IMAP4 ouvre une session sur le serveur Exchange pour envoyer un mail M2, alors les données du mail M2 sont enregistrés dans le fichier Streaming STM et les propriétés du mail M2 sont enregistrés dans le fichier Rich Text EDB.

11.3.3. Connexion avec un client MAPI et Non-MAPI

Lorsqu'un client MAPI, ouvre une session sur le serveur Exchange pour lire le mail M2 préalablement envoyé par le client non MAPI ; le client MAPI lit des propriétés du mail M2 dans le fichier Rich Text EDB pour trouver le message dans le fichier STM.
La conversion est ensuite effectuée entre le fichier STM et le fichier EDB.

Si le client MAPI effectue une modification sur le mail M2, alors celui-ci sera sauvegardé dans le fichier EDB Rich Text, de ce fait le processus de conversion n'aura pas besoin de s'exécuter lors de la prochaine ouverture de ce mail M2 par un client MAPI.

11.3.4. Le processus de stockage des transactions en mémoire

Lorsqu'une modification est fait sur une banque, les transactions sont effectuées dans un espace de mémoire vive spécialement allouée pour l'occasion dans le but d'accroître les performances, cependant ce procédé de stockage en mémoire peut causer des pertes de donnée ; par exemple si un votre serveur subi une panne de courant, alors les données non validées (Commit) présentes en mémoire seront perdues.

11.3.5. Les fichiers journaux et checkpoint

Pour palier à ce problème de transactions perdues, ESE crée des fichiers de journaux portant l'extension **.LOG** contenant toutes les transactions qui ont été effectuées.
Exchange crée des fichier CHECKPOINT portant l'extension **.CHK**, dans le but de consigner les transactions des fichiers journaux qui ont été validés (COMMIT) dans la base de données pour un groupe de stockage et par conséquent présent sur le disque et non plus en mémoire.

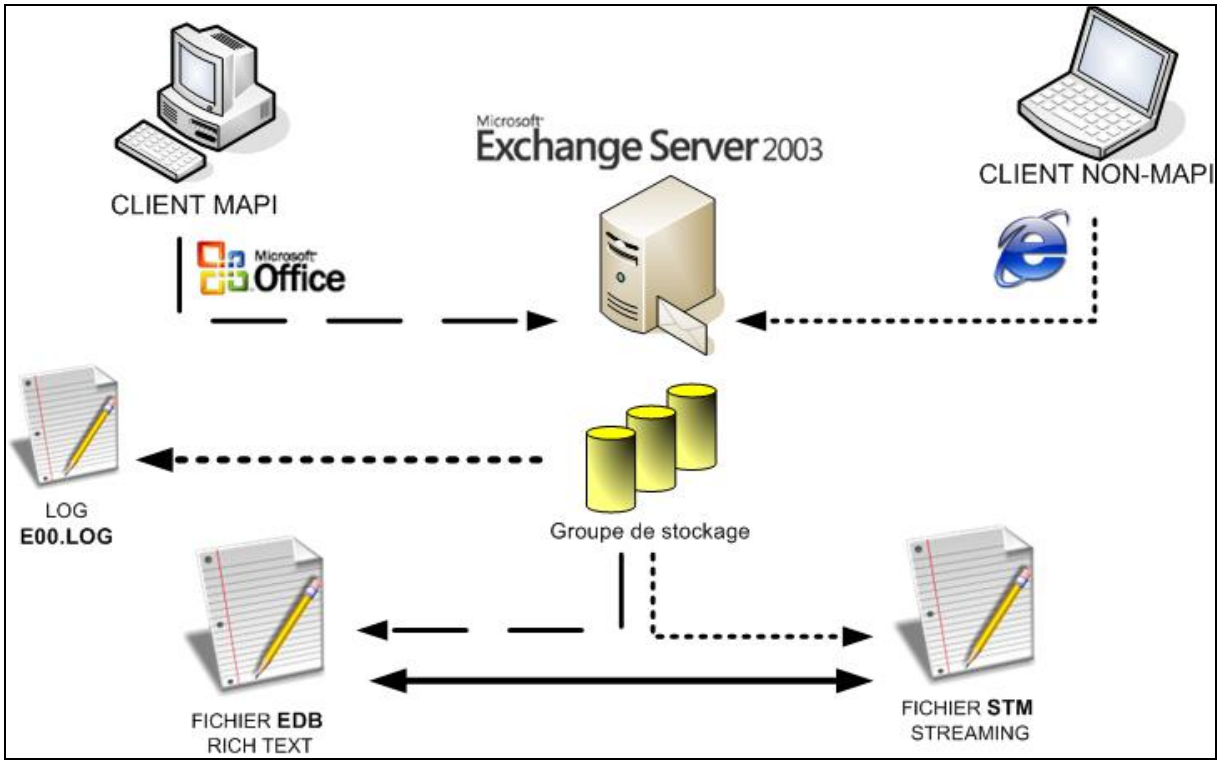
Reprenons notre exemple avec une coupure de courant, dans ce cas là, lorsque Exchange redémarre, alors le moteur de base de données ESE utilise le dernier fichier CHECKPOINT pour connaître les jeux de transactions à ré-exécuter et permet ainsi de restaurer l'état de la base de données avant la coupure de courant. Bien entendu les transactions déjà validées ne seront pas exécuter à nouveau.

Lorsqu' Exchange démarre pour la première fois, un fichier journal nommé **E00.log** est crée automatiquement, sa taille est de 5MB. Lorsque le fichier de log est plein alors Exchange le renomme en tant que **E00*000001.log*** et crée un nouveau fichier **E01.log** prêt à enregistrer les transactions de la base de données, lorsque ce nouveau sera à son tour plein celui-ci sera renommé en tant que **E01*00001.log***, et un nouveau fichier E02.log sera crée.

11.3.6. Les fichiers de journaux réservés

Lorsque votre serveur n'a plus de place pour stocker les fichiers journaux (moins de 5 MB) et que votre serveur ne peut plus créer de fichier E00.log ; alors Exchange se sert des fichiers journaux réservés, en effet il existe 2 fichiers nommé res1.log et res2.log, qui est en fait un espace réservé pour journaliser les transactions en cas de manque de place sur les fichiers journaux normaux.
Dans le cas de l'utilisation des fichiers journaux réservés, aucune opération exécutée en mémoire n'est stockée dans les fichiers journaux réservés et le groupe de stockage démonté.

SCHEMA RECAPITULATIF.



11.3.7. Qu'est ce que le mode circulaire pour les fichiers journaux Exchange ?

Dans ce mode de configuration les fichiers journaux ne sont pas tous stockés sur le disque, les transactions sont effacées au fur et à mesure.

En effet lorsque le dernier fichier journal est plein, alors Exchange continue la journalisation des transactions dans le premier fichier journal, et supprime les données de celui-ci.

Ce mode réduit l'espace disque utilisé par les fichiers journaux, mais ne permet pas de restaurer toutes les transactions, car il nécessaire d'avoir tous les fichiers journaux pour pouvoir reconstituer l'historique de toutes les transactions sur la base de données Exchange. Le mode circulaire limite le niveau de restauration des opérations non validées en cas de défaillance de la base données ; mais permet de faire un gain d'espace disque.

Pour implémenter ce mode, le choix doit se faire sur :

- le nombre de transactions
- la stratégie de sauvegarde mis en place
- la gestion de votre espace disque

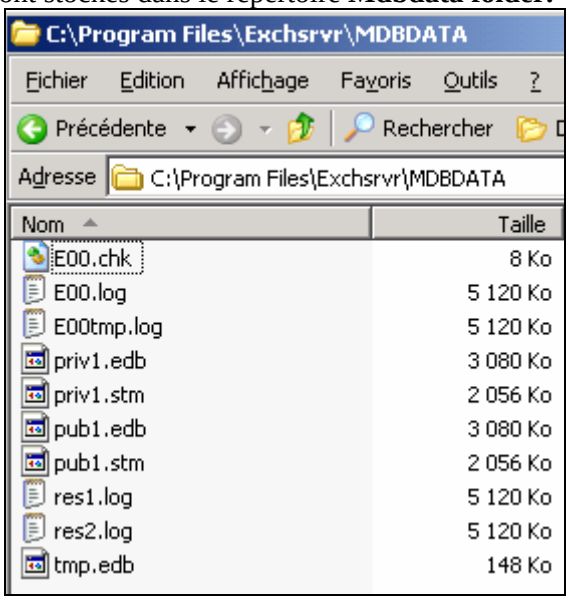
11.4. Gestion du stockage des données

11.4.1. Où sont stockés les fichiers ?

Par défaut lorsque vous installez pour la première fois Exchange 2003 Serveur, un groupe de stockage est créé. Ce groupe s'appelle – **Premier groupe de stockage** - , ce groupe contient les boîtes aux lettres et les dossiers publics.

Ce dossier est physiquement stocké sur le disque à l'emplacement suivant :
C:\PROGRAM FILES\EXCHSRVR\MDBDATA FOLDER

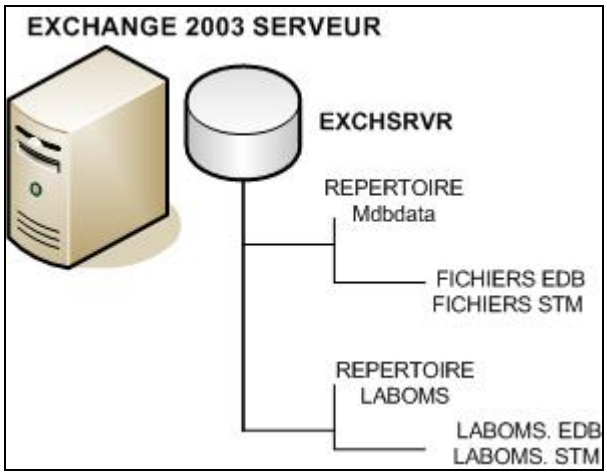
Les fichiers STM et EDB sont stockés dans le répertoire **Mdbdata folder.**



Tous les emails sont stockés dans une base de données, cette base de données adopte le moteur **E**xtensible **S**torage **E**ngine basé sur les transactions **ACID**.

Lorsque vous créez des nouveaux fichiers de stockage, par défaut ceux-ci prennent le nom du répertoire de stockage dans lequel ils se situent.

Exemple : Vous créez un nouvel espace de stockage nommé **LABOMS.** Par défaut les fichiers s'appelleront LABOMS.EDB et LABOMS.STM



11.4.2. Comment effacer des banques de boîtes aux lettres ?

Avant d'effacer le fichier de stockage de boîtes aux lettres, vous devez stocker les boîtes aux lettres contenues dans le fichier de stockage dans un autre fichier de stockage.

Si vous utilisez un **SMTP** sur un serveur frontal, vous ne pourrez pas supprimer toutes les banques de boîtes aux lettres.

11.4.3. Comment effacer des banques de dossiers publics ?

Avant d'effacer les banques de dossiers publics qui sont utilisés par des répertoires système, vous devez vous assurer des sélectionner une nouvelle banque de dossiers publics pour stocker les répertoires systèmes.

Si la banque de dossiers publics que vous souhaitez effacer contient uniquement un répliqua d'un ou plusieurs répertoires, alors vous perdrez toutes les données présentes dans ces répertoires.

Vous ne pouvez pas effacer la dernière banque de dossiers publics qui héberge une arborescence de dossier publics ou qui est la banque de dossiers publics par défaut pour une banque de boîte aux lettres ou pour les utilisateurs.

11.4.4. Comment effacer des fichiers de groupe de stockage ?

Vous pouvez uniquement effacer un groupe de stockage si celui-ci n'héberge plus aucunes banques. En revanche vous devrez effacer manuellement les fichiers logs liés au groupe de stockage après suppression de celui-ci.

Ouvrez le Gestionnaire de système Exchange, sélectionnez le groupe de stockage désiré, click droit et cliquez sur « **Effacer** ». Effacer ensuite tous les fichiers de transactions de logs sur votre serveur liés au groupe de stockage que vous venez d'effacer.

11.5. Gestion de l'espace disque

Nous allons à présent décrire les différentes technologies de stockage qu'il est possible d'implémenter et nous ferons également l'étude des besoins en terme d'espace de stockage.

11.5.1. Où sont stockées les ressources des clients ?

11.5.1.1. Environnement sans clustering

Dans un environnement où il n'y a pas de clustering, lorsqu'un client Exchange envoie une requête à un serveur Exchange. Le serveur recherche les informations pour répondre à la requête du client dans son disque dur local.

11.5.1.2. Environnement avec clustering

Dans un environnement où des serveurs Exchange sont en cluster, chaque serveur est appelé nœud (*node* en anglais) lorsqu'un client Exchange se connecte à serveur Exchange, la connexion se fait via un serveur virtuel. Le serveur virtuel redirige ensuite la requête du client vers le nœud contrôlant la ressource adéquat. Le nœud va ensuite lire et /ou écrire les informations sur la baie de disque partagées et les renvoyer au client via le serveur virtuel.

☞ Pour plus d'informations sur le clustering, lire l'article :
http://www.laboratoire-microsoft.org/articles/win/clustering/

11.5.2. Les technologies de stockage utilisées

Pour stocker les bases de données, il est nécessaire d'utiliser une technologie de stockage performante, fiable et rapide.
Evidement, plus la charge de vos requêtes client sera croissante, plus le besoin d'avoir un stockage performant, rapide et à tolérance de panne deviendra indispensable.
A l'heure actuelle, pouvez-vous vous permettre d'interrompre le service de messagerie pendant 5h de temps dans une multinational, sans avoir de conséquence néfaste sur les performances de l'entreprise ?
La performance d'Exchange passe également par le choix que vous souhaitez implémenter pour le stockage de vos données.

Voici les différentes implémentations de stockage possible :

Baie de stockage externe	 Cette solution de stockage est utilisée avec un boîtier SCSI contenant plusieurs disques SCSI ou autre matériel. Les disques sont généralement configurés en RAID. Le boîtier est directement connecté via un câble SCSI au serveur Exchange. Ce type de stockage offre de bonne performance, mais reste limité lors de montée en charge. Ce type de stockage peut être retenu pour les petites structures.
Stockage relié au réseau (NAS)	 Le NAS permet d'avoir une entité de stockage indépendante avec sa propre adresse IP. Il n'y a pas besoin dans ce cas de figure d'avoir un lien avec un serveur. Le NAS est relié directement au réseau et une adresse IP lui a été assignée. Les requêtes reçues par le serveur Exchange principal sont redirigés vers le NAS pour que celui-ci puisse les traiter. Vous devez vérifier que le niveau de bande passante des données entrée/sortie transitant entre le NAS et le serveur Exchange est suffisant de façon assurer une qualité de service au moins correcte. Au quel cas il est possible de brancher le NAS directement sur le serveur Exchange.
Espace de stockage réseau (SAN)	 La solution SAN permet de connecter plusieurs serveurs à différents périphériques de stockage sur un réseau. Le SAN permet de stocker des données pour l'ensemble de votre infrastructure. Le SAN utilise la Fibre Channel dans le but d'avoir une rapidité et une connectivité optimale entre les données stockées et les applications. Ce qui permet à un grand nombre de clients de se connecter. Ce type de stockage est utilisé dans les grandes structures ayant besoin de matériel ultrarapide et pouvant résister à une montée en charge.

Il est recommandé d'utiliser la solution de stockage SAN, lorsque vous aurez le choix. En effet la solution du SAN répond à plusieurs problématiques que sont :

- La montée en charge
- L'optimisation des performances
- La vitesse en entrée/sortie

- L'ajout de serveurs supplémentaire si besoin est
- La gestion de *backup*, *snapshot* et de niveau de RAID

11.5.3. La configuration des disques dur

Microsoft recommande d'utiliser cette répartition des données sur vos disques pour votre serveur Exchange de façon à optimiser au maximum les performances de celui-ci.

TYPE DE FICHIERS	DISQUE	AVANTAGES
Système et fichiers de boot (C:\)	RAID 1	Tolérance de panne Séparation des partitions
Fichier de pagination (D:\)	Volume simple	Séparation de partition
Queue SMTP (E:\)	RAID 1	Séparation de partition Tolérance de panne
Fichiers .EDB et .STM (F:\)	RAID 5	Séparation de partition Tolérance de panne Optimisation des performances et de la capacité
Fichiers journaux (G:\)	RAID 0+1	Séparation de partition Tolérance de panne avec une meilleure performance

11.5.4. Quel type de RAID choisir ?

Chaque environnement Exchange est différent et ne requiert pas les mêmes besoins en termes de performance et de tolérance de panne. Vous devez donc prendre tous ses paramètres avant de pendre une décision sur le type de stockage à implémenter et quel type de RAID choisir.

- Evaluez l'impact d'une panne de disque dans votre environnement de système d'informations.
- Evaluez le coût en calculant le nombre de disques dont vous avez besoin pour faire fonctionner la chaîne de disque RAID.
- Déterminez le temps maximum de restauration souhaité pour déterminer le type de RAID à implémenter.

11.6. Gestion de la mise à jour matérielle

11.6.1. Les espaces d'adressage virtuels

Le processus STORE.EXE gère l'allocation de l'espace d'adressage en mémoire en fonction du nombre de bases de données et du nombre d'utilisateurs connectés à Exchange.
Cette allocation est appelé **espace d'adressage virtuel.**

La plupart du temps, l'espace d'adressage virtuel est paramétré de façon à obtenir des performances et une montée en charge. Dans le cas de petites et moyennes infrastructures Exchange, l'un des services Exchange ajustera automatiquement l'espace d'adressage virtuel.
Dans le cas d'une plus grande infrastructure, vous devrez procéder à un ajustement manuel des paramètres de l'espace d'adressage virtuel.

11.6.2. Optimiser les espaces d'adressage virtuels

Si votre serveur Exchange a plus d'un gigabyte de mémoire vive, il faut alors ajouter le commutateur **/3GB** sur la ligne correspondant à votre serveur dans le fichier **BOOT.INI.**

Lorsque vous utilisez ce commutateur, vous permettez l'allocation de 3GB dans le mode utilisateur.
Ce commutateur doit être utilisé uniquement pour les serveurs Windows 2003 et Windows 2000 Advanced Server.

✍ Ne jamais utiliser le commutateur /3GB pour un serveur Windows 2000 standard

Dans le cas où vous utilisez Windows 2003 serveur avec Exchange 2003 serveur, utilisez le commutateur **/USERVA=3030** dans le fichier **boot.ini.**
Ce paramètre permettra d'augmenter les entrées dans la table système pour Exchange serveur.

11.6.3. Le cache de base de données

Le moteur ESE utilise un cache de grande capacité où sont stockées les transactions avant leur validation et leur écriture sur le disque.
Par défaut Exchange alloue **896 MB** de mémoire vive pour son cache lorsque le commutateur /3GB est spécifié.
Au quel cas, Exchange alloue **576 MB** de mémoire vive pour son cache lorsque le commutateur /3GB n'est pas spécifié.

Lorsque le serveur Exchange 2003 a de forte montée en charge ou lorsque que les performances des disques ne sont pas optimales, vous devrez la plupart du temps augmenter ou diminuer la capacité de la mémoire.
A vous de calibrer la taille de cache nécessaire pour optimiser la lecture/écriture sur votre serveur tout en respectant la charge de travail de votre serveur Exchange 2003.

11.6.4. Modifier la taille du cache

Pour modifier la taille du cache :

1. Utiliser Active Directory Services Interface (ADSI) Edit et parcourir le chemin suivant :
Configuration Container | CN=Information Store,CN=<*server*>,
CN=Servers,CN=<*Admin Group*>,CN=Administrative Groups,
CN=<*org*>,CN=Microsoft Exchange,CN=Services,CN=Configuration

2. Click droit sur **Information Store** object, et sélectionnez **Properties**.
3. Sélectionnez l'attribut **msExchESEParamCacheSizeMax** attribute, adjuster la valeur souhaité et cliquez sur **Set**.

> - Attention à ne pas faire d'erreur avec la valeur **msExchESEParamCacheSizeMin**
> -La valeur du cache doit être un multiple de 8 192.

4. Fermez l'utilitaire ADSI Edit et attendre les réplications, si besoin est.
5. Redémarrez le service Banque d'Information

11.6.5. L'utilitaire de Migration de dossier Public Microsoft Exchange

Il existe un nouvel utilitaire vous permettant de faire des migration de dossier Public.
Cet utilitaire s'appelle : **pfMigrate.**

PfMigrate vous permet de :

- Créez un réplica de dossiers publics sur un autre serveur
- Supprimez un réplica depuis le serveur source après avoir répliqué les dossiers publics
- Générez un rapport détaillé pour déterminer les dossiers publics qui ont besoin d'être répliqués
-Générez un rapport détaillé après l'exécution du processus **pfMigrate** pour vérifier que vous n'avez eu aucun problèmes pendant la migration.

11.6.5.1. Où trouver l'utilitaire pf Migrate ?

L'utilitaire **PfMigrate** est disponible dans le répertoire ExDeploy du CD-ROM Exchange 2003.

12. Planification d'une restauration après un sinistre

12.1. Planification d'une restauration

Identification des risques est la première chose à étudier lorsque vous mettez en place un plan contre un incident.

12.1.1. Quels sont les risques potentiels ?

La perte d'informations comme :

-Un message, une boîte aux lettres, un dossier public
-Une base de données
-Un groupe de stockage
-Un index

La perte d'un serveur Exchange

La perte d'un service essentiel à l'exécution du serveur Exchange comme :

- Le service DNS
- Le service Internet Information Services

La perte ou la détérioration d'un service dû à une configuration inadéquate comme :

- une brèche de sécurité
  - un déni de service
  - un virus ou cheval de Troie

Une fois les risques identifiés, vous devez recenser tous les composants et services requis afin d'optimiser et prévenir les risques d'instabilité ou de panne sur le serveur Exchange 2003.

12.1.1.1. Qu'est que l'analyse des risques ?

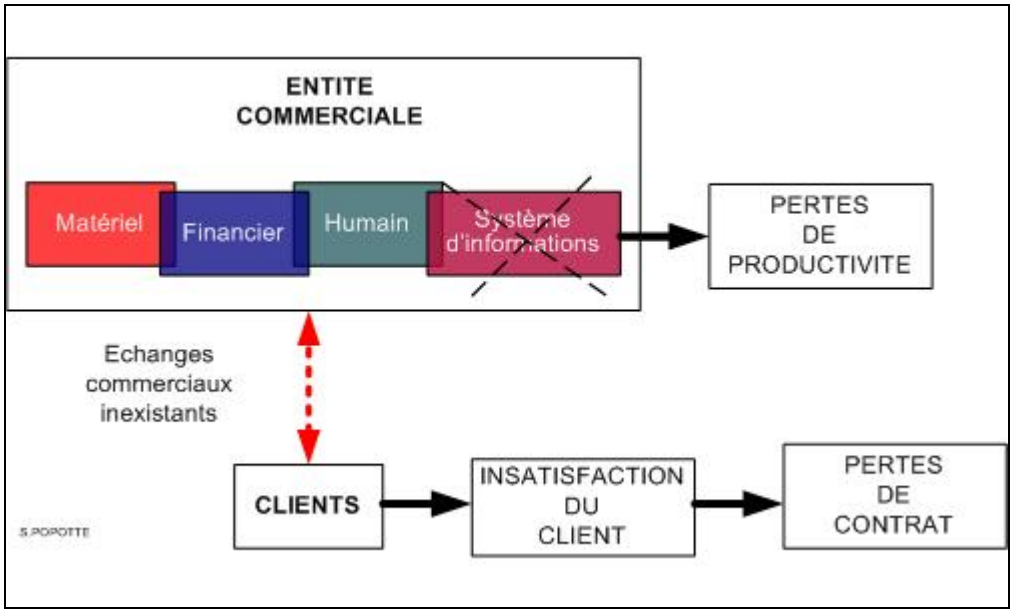
L'analyse des risques est la conversion du risque de pertes de données en prise de décision pour protéger les données. Une analyse permet de d'identifier les failles et faiblesses de votre système d'informations.
L'analyse permet également d'identifier les potentiels risques extérieurs comme les désastres naturels ; incendie, tremblement de terre, vol physique du serveur, sabotage ou erreurs humaines.

L'impact ne sera pas seulement technique ; mais pourra fortement influencer les résultats de l'entreprise, à tout niveau.

Exemple : Le serveur de messagerie Exchange Serveur 2003 ne fonctionne plus pendant une journée suite à une défaillance électrique, le temps de réparer les installations électrique et de vérifier l'intégrité des données sur le serveur; le service commercial ainsi que la direction ne peuvent plus répondre aux appels d'offres, le service clients ne peut pas faire le suivi des réclamations, le service technique ne peut plus passer de commandes. La structure est paralysée pour tous les échanges de

courrier électronique, qui représente un pourcentage conséquent de la gestion des activités au sein d'une structure à but lucratif.

Résultat : des contrats perdus, des bénéfices en moins, des heures de travail perdues, une réputation égratignée auprès des clients, des sanctions pour l'équipe de commerciaux et pour le service informatique...



Pour plus d'informations concernant la méthodologie pour l'analyse des risques, consultez la documentation officielle Microsoft à l'adresse suivante **http://www.microsoft.com/technet** Effectuez une recherche pour trouver le document : ***MSF Risk Management Discipline***

12.1.2. Comment minimiser les risques ?

Les mesures à prendre pour minimiser les risques et les anticiper se basent sur le rapport coût d'implémentation / pertes d'argent. Vous devrez déterminer le niveau acceptable de panne pour les services de votre compagnie et le temps pendant lequel la ou les pannes peuvent durer.
Puis-je me permettre d'avoir un panne d'une demi-heure ou dois-je impérativement implémenter une solution de basculement comme un cluster ?

12.1.2.1. Installation et matériel

Le fait de minimiser les risques commence dès l'installation d'Exchange, vous devez prendre en compte et respecter le minimum matériel requis et calculer la charge maximale +20% pour déterminer le matériel à utiliser sur le serveur de messagerie.
L'impact sur une infrastructure Exchange s'exécutant dans un environnement Active Directory requiert une solution matérielle fiable et robuste ainsi qu'une solution avec tolérance de panne matérielle. Les clusters restent une des meilleures solutions pour contrer les risques de paralysie.
En ce qui concerne Active Directory, il est important d'installer au moins 2 contrôleurs de domaine pour la tolérance de panne d'Active Directory.

12.1.2.2. Etablir des procédures

L'établissement de procédure vous aidera à limiter et minimiser les désastres matériels ou le dysfonctionnement sur certains services et composants.
Il est important de faire des procédures pour :

- Appliquer des services packs, hotfix et mise à jour de firmware
- Surveiller les fichiers journaux d'événements
- Maintenir les fichiers journaux des serveurs
- Effectuer une stratégie de sauvegarde journalière efficace

12.1.2.3. Planifier les directives pour Active Directory

Les serveurs Exchange serveur 2003 se servent du processus de réplication d'Active directory pour répliquer les propriétés des objets et les méta-données de l'infrastructure Exchange à travers la forêt. Les serveur Exchange 2003 communiquent avec les contrôleurs de domaine Active directory pour accéder aux informations dont ils ont besoin pour faire fonctionner les processus d'envoi/réception de messages, d'autorisations, de gestion de listes, sécurité et autres composants.

En cas de dysfonctionnement ou de panne, assurez vous que :

-Les administrateurs Exchange travaillent avec les administrateurs Windows 2003 pour assurer une tolérance de panne avec un domaine multi-contrôleur.

- Les administrateurs Exchange doivent avoir des droits sur Active directory pour qu'ils puissent restaurer des données en cas de panne, lire, créer, modifier et supprimer tous les objets liés à Exchange présent dans Active directory.

-Les administrateurs Exchange doivent avoir des forêts Active Directory séparées pour pouvoir utiliser les serveurs de restauration. Pour restaurer une boîte aux lettres endommagée ou un dossier public depuis un serveur de restauration qui ne fait pas parti de l'organisation Exchange, les administrateurs doivent utiliser une forêt Active Directory séparée.

12.1.3. Les outils de restauration

Lors d'une panne, le temps de recherche d'outils de dépannage et de restauration, peut influer fortement sur le temps de restauration et de remise en production de votre serveur, donc implicitement sur le bénéfice net de l'entreprise.
Il sera donc plus sage de se confectionner par avance une boîte à outils avec tous les utilitaires et informations nécessaire dont vous avez besoin pour répondre rapidement à une demande de dépannage en cas de crash de votre organisation Exchange 2003, en moins de temps possible.

Votre boîte à outils personnalisées doit comprendre :

- Un ordinateur prêt- à l'emploi
- Un câble null modem pour connecter votre ordinateur directement sur le serveur défaillant
- Des utilitaires de debogage pour vos serveurs
- Les droits appropriés
- Les sauvegardes sur média des derniers fichiers logs si besoin est
-Une installation de Windows serveur
-Une installation d'Exchange serveur
-Les utilitaires fournis par votre fabricant de matériel serveur
-Le programme anti-virus
-Le programme de sauvegarde
-Les autres programmes tierce-partie
-Les documents concernant la version de Windows ainsi que les services pack et hotfix installés
-Les documents concernant la version d'Exchange ainsi que les service pack et hotfix installés
-Le détail du calendrier de sauvegarde
-Le détail sur la configuration de vos disques RAID
-Les archives des fichiers journaux système et applications

-Les numéros de téléphone d'urgence du département informatique
-Le numéro de client de support Microsoft si vous en avez un
-Le numéro de support de votre fabricant de matériel
-Un accès direct à la base de connaissance Microsoft (support.microsoft.com)
-Un accès direct à des articles technique pour vous aider dans les tâches de restauration
-Des « white papers »

12.1.4. Le plan de restauration

Un plan de restauration est un guide qui permettra aux administrateurs Exchange de suivre une procédure pas à pas en cas de dysfonctionnement du serveur Exchange 2003.
Lorsque vous rédigez un plan de restauration Exchange vous devez prendre en compte les ressources logistiques et système.

-Installez une des médias externes compatibles et performants
-Prévoyez sur chaque serveur un nombre de cassette pouvant répondre au flux de données
-Configurez votre serveur pour ne pas redémarrer automatiquement après une erreur
-Configurez votre serveur pour qu'il enregistre tous les événements et qu'il envoie les alertes appropriées
-Faire une copie des procédures de sauvegardes
-Vérifiez que vous avez assez de capacité sur vos disques pour restaurer les base de données et les fichiers journaux
-Mettez en place le système de fichiers log circulaire uniquement si besoin est
-Planifiez les sauvegardes des boîtes aux lettres aussi souvent que possible
-Maintenez une copie des sauvegardes en dehors du lieu où se trouve les serveurs Exchange

12.2. La sauvegarde Exchange 2003

La première défense à avoir contre les erreurs fatales, pertes de données ou autres désastres est une bonne sauvegarde.
Avant tout chose, il est important de choisir la bonne technologie de déploiement aussi bien en matériel et logiciel, cette décision aura un impact non négligeable sur votre sauvegarde et restauration.

Quels sont les critères de sélection et considérations à prendre lors du choix final du système de sauvegarde ?

- Si vous choisissez un logiciel de sauvegarde, prenez garde à ce que celui-ci ne vous limite pas dans les fonctionnalités Exchange, en effet la fonctionnalité de sauvegarde en ligne n'est pas inclut dans toutes les solutions de logiciel de sauvegarde. Certaines API ne sont pas implémentées, renseignez vous au préalable sur les sites techniques et faites de la prise de renseignement sur des salons, forum,site web comparatif, support techniques, collègues ou autres pour obtenir tous les renseignements concernant le logiciel de sauvegarde.

- Architecture des médias est-elle compatible avec votre logiciel de sauvegarde ? Pouvez-vous mettre en réseau cette solution de stockage de sauvegarde pour d'éventuel serveur de secours ?

- Votre logiciel de sauvegarde vous procure-t-il toute la flexibilité en termes de planification de sauvegarde, tous les modes y sont-ils représentés ?

- Vérifiez que le logiciel de sauvegarde supporte toutes les API pour la sauvegarde est restauration d'Exchange Server mais également le Volume Shadow Copy

- Vérifiez que votre logiciel de sauvegarde peut automatiquement identifier les médias insérés, cela vous facilitera le travail en cas d'oubli de marquage sur la cassette de sauvegarde et/ou en cas de grosse quantité de données.

- Vérifiez que les vendeurs de votre logiciel de sauvegarde et de vos périphériques matériels de sauvegarde disposent d'un support techniques et d'un FAQ en ligne.

- Choisissez un logiciel pouvant gérer les Redundant Array of Independent Tapes (RAIT), le clustering ou le stockage réseau (SAN). Même si vous n'utilisez pas lors de la première mise en production ce type de stockage de sauvegarde, soyez prévoyant en cas de montée en charge de vos base de données et fichiers journaux Exchange.

☞ Pour plus d'informations concernant la sauvegarde et la restauration sur un serveur à l'aide de l'utilitaire NTBACKUP, lire l'article suivant sur le site du Laboratoire SUPINFO des technologies Microsoft :
http://www.laboratoire-microsoft.org/articles/server/exchange%5Frestaure/

12.2.1. Les types de données à sauvegarder

Que devez-vous sauvegarder ? Ceci-ci est une très bonne question :o)
A vrai dire, la meilleure solution serait de sauvegarder toutes les données et méta-données du serveur Exchange. Voici une liste non exhaustive des données à sauvegarder sur le serveur :

Bien évidement et obligatoirement, vous devrez sauvegarder :

- Les bases de données Exchange (EDB, STM)
- Les fichiers journaux Exchange (LOG)
- Les journaux d'événements relatifs à Exchange
- Les bases de données di service de réplication (SRS) en cas de réplication inter site.
- Le quorum si vos serveurs sont en cluster

Outre mesures, mais à ne pas négliger vous devrez sauvegarder :

- Les données d'Active Directory
- Le magasin de certificats
- L'état du système
- Utilitaire tierce-partie liés à Exchange

12.2.2. Les types de stratégies de sauvegardes

La stratégie de sauvegarde à adopter dépend du volume de données que vous avez, ainsi que l'importance des données.

Stratégie de sauvegarde	Description
COMPLETE	-Sauvegarde en ligne les fichiers des bases de données et journaux -Un média suffit pour faire cette sauvegarde ainsi la restauration
COMPLETE + INCREMENTIELLE	-Sauvegarde uniquement les données modifiées depuis la dernière sauvegarde -Pour effectuer la sauvegarde vous devez vous procurez la cassette de sauvegarde complète ainsi que toutes les cassettes de sauvegardes incrémentielles jusqu'au point de temps de l'incident
COMPLETE + DIFFERENTIELLE	- Sauvegardes uniquement les fichiers journaux ayant changés depuis la dernière sauvegarde complète - Pour effectuer la sauvegarde, une cassette suffit généralement, tout dépend de la taille des transactions journalière
COPIER	-A l'instar de la sauvegarde complète, ce type de sauvegarde copie toutes les données, excepter les fichiers qui n'ont pas le bit d'archivage à 1.
COPIER + INCREMENTIELLE	-Cette sauvegarde vous permet de restaurer des données depuis un point précis dans le temps via la sauvegarde « copier » et d'avancer à un point précis dans le temps en rejouant les transactions de la base de données via les fichiers de sauvegarde incrémentielles.

12.2.3. Choisir le type de sauvegarde

Pour choisir quel type de sauvegarde implémenter, vous devez prendre en compte et évaluer le temps de sauvegarde et de restauration que cela prendra.

Voici un tableau récapitulatif avec toutes les propriétés des sauvegardes :

Stratégie de sauvegarde	Temps de sauvegarde	Journaux de transactions	Nombre média nécessaire	Temps de restauration
Complète	La plus longue plage de temps	Effacés	1	Intermédiaire
Complète + incrémentielle	Le plus rapide	Effacés	1 pour la complète + 1 pour chaque incrémentielle	Long
Complète + différentielle	Progressivement plus longue que la complète	Non effacés	1 pour la complète + 1 pour chaque différentielle	Intermédiaire
Copier	Selon le volume de données	Non effacés	1	Rapide

12.2.4. La sauvegarde en ligne

12.2.4.1. Qu'est ce qu'un sauvegarde en ligne ?

Le processus de sauvegarde en ligne consiste à sauvegarder les données sans arrêter les services courants ; en effets tous les services continuent à fonctionner correctement, et les utilisateurs peuvent continuer à consulter leurs boîtes mail pendant la sauvegarde.

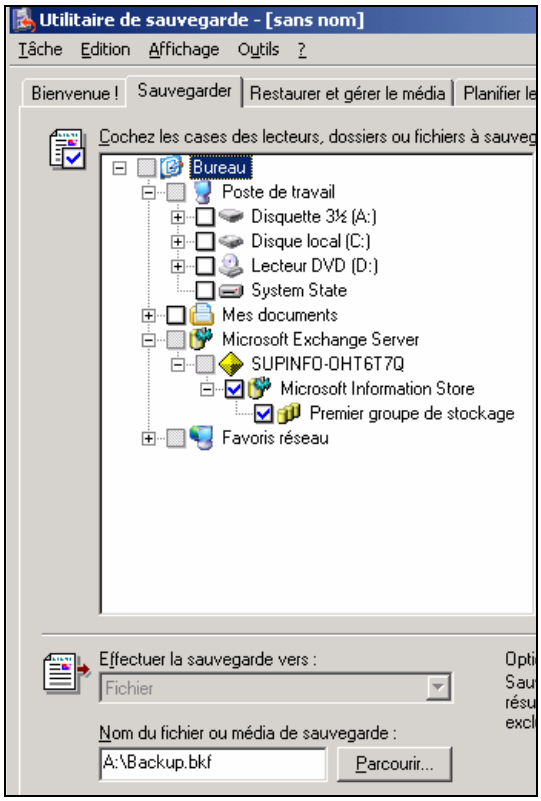
Durant la sauvegarde en ligne, les fichiers .EDB, .STM et .LOG sont sauvegardés et leur intégrité est vérifiée.
Le contrôle d'intégrité (CHECKSUM) se fait tous les blocs de 4ko dans la base de données.
Si la vérification de l'intégrité échoue, le processus de sauvegarde est alors stoppé ; normal, on ne prend pas le risque de sauvegarder des données potentiellement corrompues, imaginez le désastre en cas de restauration de cette sauvegarde ; rassurez vous, même si vous testez de restaurer une sauvegarde corrompue Exchange ne vous laissera pas faire car le processus de restauration effectue une vérification de l'intégrité avant de restaurer.

Pour vérifier que votre sauvegarde s'est bien effectuée avec une intégrité non corrompue, lisez le journal d'événements.

12.2.4.2. Comment effectuer une sauvegarde en ligne ?

Pour effectuer une sauvegarde en ligne, procédez ainsi :

- Ouvrez la console de sauvegarde à l'aide de la commande NTBACKUP.EXE
- Dans l'arborescence sélectionnez Microsoft Exchange Server et développez
- Développez le nom de votre serveur, Microsoft Information Store
- Sélectionnez le groupe de stockage que vous souhaitez sauvegarder
- Cliquez sur le bouton « Parcourir » pour sélectionner un emplacement de sauvegarde
- Nommez votre sauvegarde
- Démarrez votre sauvegarde



12.2.5. La sauvegarde hors ligne

La sauvegarde en ligne, consiste à arrêter tous les services utilisés avant de sauvegarder les fichiers adéquats.
Pour effectuer une sauvegarde hors ligne, vous devez en premier lieu démonter les banques de boîtes aux lettres et dossiers publics avant de sauvegarder manuellement les fichiers de base de données et de transactions.
Il est tout de même recommandé de procéder aux sauvegardes **en ligne** le plus fréquemment possible, la sauvegarde hors ligne n'est pas une solution recommandée.

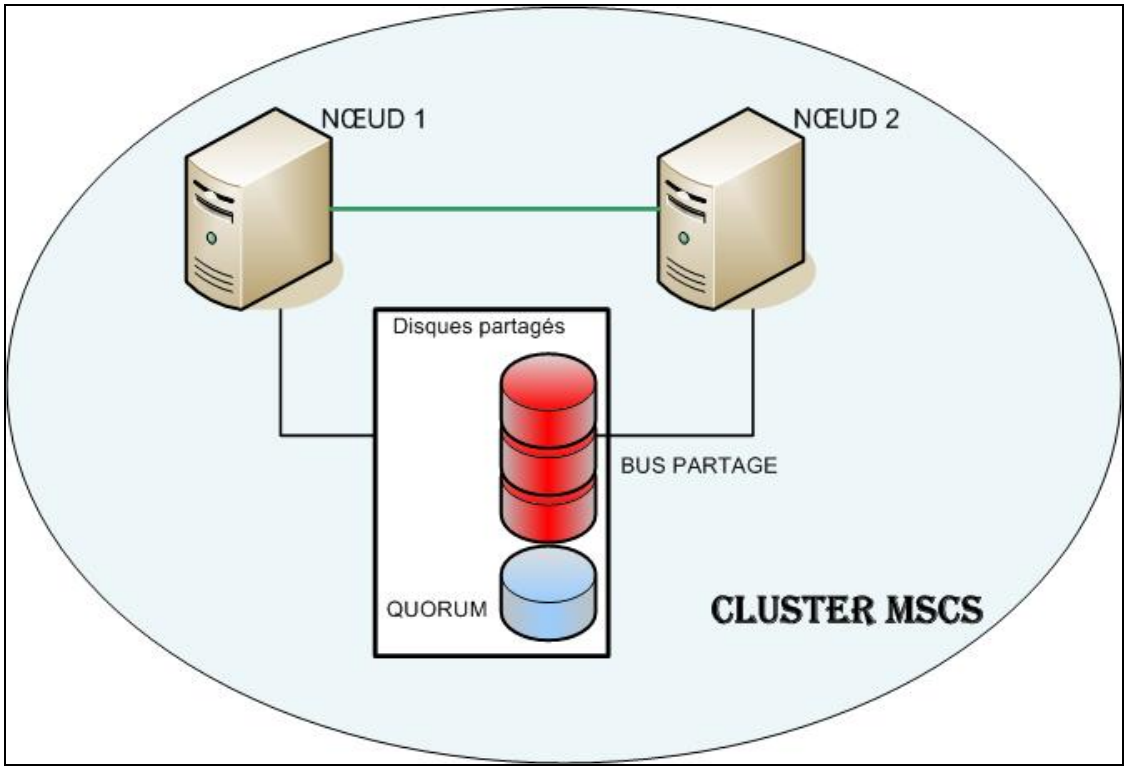
Cependant une sauvegarde hors ligne s'envisage indispensable lorsque :

-La sauvegarde en ligne ne fonctionne pas
-Le logiciel de sauvegarde tierce-partie ne supporte pas ou n'a pas l'API de sauvegarde en ligne

12.2.6. Sauvegarde d'un cluster Exchange 2003

Le principe de sauvegarde et de restauration est le même lorsque vous dans une architecture en cluster ; néanmoins la différence est portée au niveau du Quorum, la signature des disques et partitions.

Rappel : un cluster est composé de plusieurs serveur appelés nœuds, un cluster à pour but de fournir une tolérance de panne et équilibrage de charge aux clients.
Au sein du cluster, la lecture et l'écriture des données se fait sur un bus partagé entre les nœuds, tous les nœuds ont accès à ce bus partagés où réside les disques partagées ; les disques partagés contiennent les ressources ainsi que le quorum.
Le quorum est une partie des disques partagés contenant toutes les méta donnés du cluster, configuration, droits et autres.



✍ Pour plus d'informations à propos du cluster MSCS, lire l'article :

Pour sauvegarder les données Exchange en cluster vous devez inclure dans votre sauvegarde :
- La première chose à sauvegarder est la configuration de la signature des disques et des partitions présents sur votre bus partagé, pour ce faire utilisez des disquettes ASR, à l'aide l'assistant natif NTBACKUP.
- Les fichiers de base de données les fichiers de transactions présent sur les disques partagés
-Le quorum contenant les informations physique et logique du cluster, ainsi que toutes les propriétés et configuration des objets composant le cluster.

✍ Il est également possible d'utiliser le service **Volume Shadow Copy** intégré à Windows pour faire des sauvegardes. Certains éditeurs de logiciels de sauvegarde ce serve de cette API native pour accroître et sécuriser les performances de leurs sauvegardes.

12.3. La restauration des banques Exchange 2003

Lors du processus de restauration, 2 questions sont posées « combien de temps va durer la restauration ? – Quelle est la méthode la plus efficace a utilisé ? »
La procédure de restauration va dépendre de votre architecture Exchange et bien évidement de a méthode entreprise lors du processus de sauvegarde.

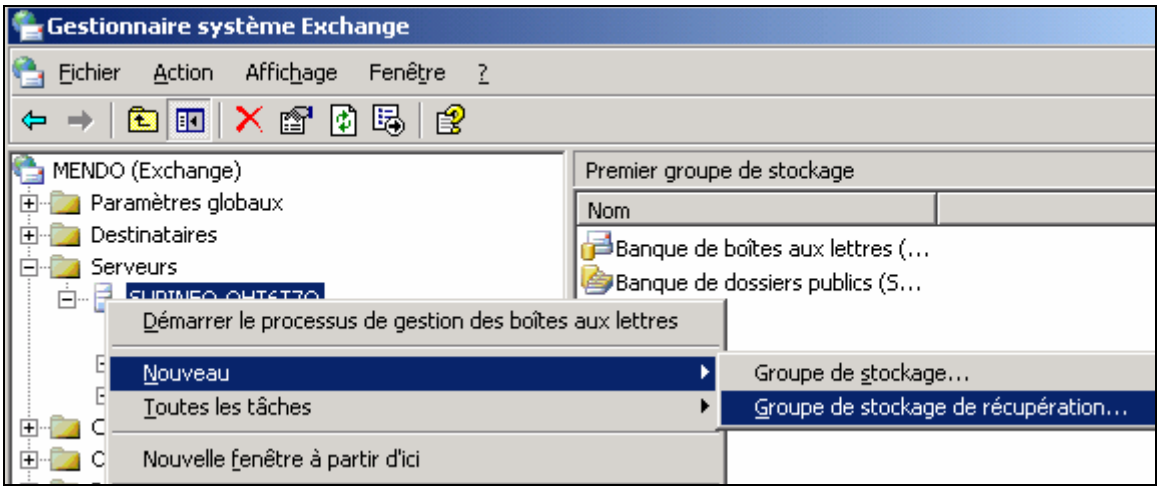
12.3.1. Restauration d'un groupe de stockage

12.3.1.1. Les types de stratégies de restauration

Les stratégies les plus utilisées sont les stratégies de restauration de groupe de stockage et de restauration partielle de forêt.
Vous choisirez la bonne stratégie ou une autre stratégie en fonction de la politique de restauration adoptée par votre entreprise.

12.3.1.2. La restauration via le groupe de stockage de récupération

Exchange possède un groupe de stockage spécial nommé **groupe de stockage de récupération.** Pour le créer, ouvrez le gestionnaire système Exchange, sélectionnez votre serveur Exchange dans le conteneur *Serveurs*, click droit Nouveau\Groupe de stockage de récupération.



Après création ce nouveau groupe, un nouvel item Groupe de stockage de récupération apparaît dans l'arborescence du conteneur serveur nommé *« Groupe de stockage de récupération »*

Ce groupe de stockage est un conteneur qui servira de tampon, de conteneur intermédiaire dans le cadre d'une restauration d'un des quatre autres groupes de stockage.

> ✍ La version Exchange Entreprise prend en charge 4 groupes de stockage, la version standard prend en charge un seul groupe de stockage.

Vous pouvez alors restaurer un groupe de stockage via le groupe de stockage de restauration si :

- Toutes les bases de données sont stockées sur un même jeu de sauvegarde
- Le serveur héberge les groupes de stockage dans le même groupe administratif que le serveur hébergeant le groupe de stockage de récupération.

Pour restaurer une base de données à l'aide ce groupe de stockage :

- Click droit, ajouter une base de données

- Sélectionnez dans la liste de recherche la base de données à récupérer
- Vérifiez les propriétés de la banque de boîtes aux lettres, validez avec OK
- Exécutez votre utilitaire de sauvegarde
- Sélectionnez le bon fichier de base de données à restaurer
- Procédez à la restauration
- Une fois terminé, ouvrez de nouveau le Gestionnaire système Exchange
- Cliquez ensuite dans l'arborescence de votre groupe de stockage de restauration sur « Monter la banque d'informations »

Ce type de restauration réduit l'indisponibilité des boîtes aux lettres pour vos utilisateurs. Lors du processus de restauration, seul les utilisateurs ayant leurs boîtes aux lettres dans la banque à restaurer seront affectés.

En revanche, il sera obligatoire de vérifier que vous possédez assez d'espace disque sur le serveur pour procéder à la restauration.

Assurez-vous également que vos sauvegardes ont été effectuées sur la même version de serveur Exchange. En effet le format des fichiers journaux change d'une version de serveur à l'autre.

✍ La restauration des dossiers publics et le Volume Shadow Copy n'est pas prise en compte dans ce type de sauvegarde

12.3.1.3. La restauration de la forêt Active Directory

Il s'agit ici de procéder à une restauration via une autre forêt Active Directory possédant les mêmes propriétés système Windows serveur contrôleur de domaine, DNS et Exchange.
Grossièrement, il s'agit d'un dump de votre forêt Active Directory en miniature.
Dans cette copie vous vous servirez du serveur Exchange répliqué avec l'original pour procéder à la restauration, il s'agit donc du procédé de serveur de secours.

Ce type de restauration peut également vus permettre de simuler une panne et restauration dans un environnement qui n'est pas en production, ce qui implique aussi que vous pourrez tester dans cette zone les services packs ou autres modifications avant déploiement dans un environnement de production.

Il sera possible avec ce procédé de restaurer les banques de dossiers publics et d'utiliser le Volume Shadow Copy service.

L'inconvénient majeur de cette solution est au niveau matériel, il vous faudra au moins 1 serveur pour simuler votre forêt avec DNS, contrôleur de domaine et serveur de messagerie Exchange 2003.

12.3.2. Restauration des banques de boîtes aux lettres

Avant toutes choses, vérifiez que la banque de boîtes aux lettres que vous souhaitez restaurer est démontée.
Vérifiez également que le service **Microsoft Exchange –Banque d'informations** est démarré car c'est ce service qui gère la restauration des données pour le serveur Exchange.

- Munissez vous des fichiers de bases de données restaurés et remplacez les fichiers de base de données actuels corrompus par les fichiers de bases de données restaurés contenu sur votre sauvegarde.
- Copiez les fichiers journaux stockés sur le média de sauvegarde dans un répertoire temporaire
- Vérifiez la signature et l'intégrité de tous les fichiers logs
- Rejouez tous les fichiers journaux présent sur le média de sauvegarde
- Rejouez tous les fichiers journaux actuels non sauvegardés

12.3.3. La restauration d'une sauvegarde hors ligne

Il existe 2 méthodes de restauration de sauvegarde hors ligne :

12.3.3.1. La restauration d'un point dans le temps

Une restauration d'un point dans le temps est effectuée lorsque la base de données est restaurée mais que les fichiers journaux ne sont pas rejoués dans la base de données.
Ainsi toutes les données crées après la dernière sauvegarde hors ligne effectuée seront perdues.
Ceci est la méthode à utiliser lorsque le mode circulaire pour les fichiers journaux est activé.

12.3.3.2. La restauration « Roll-Forward »

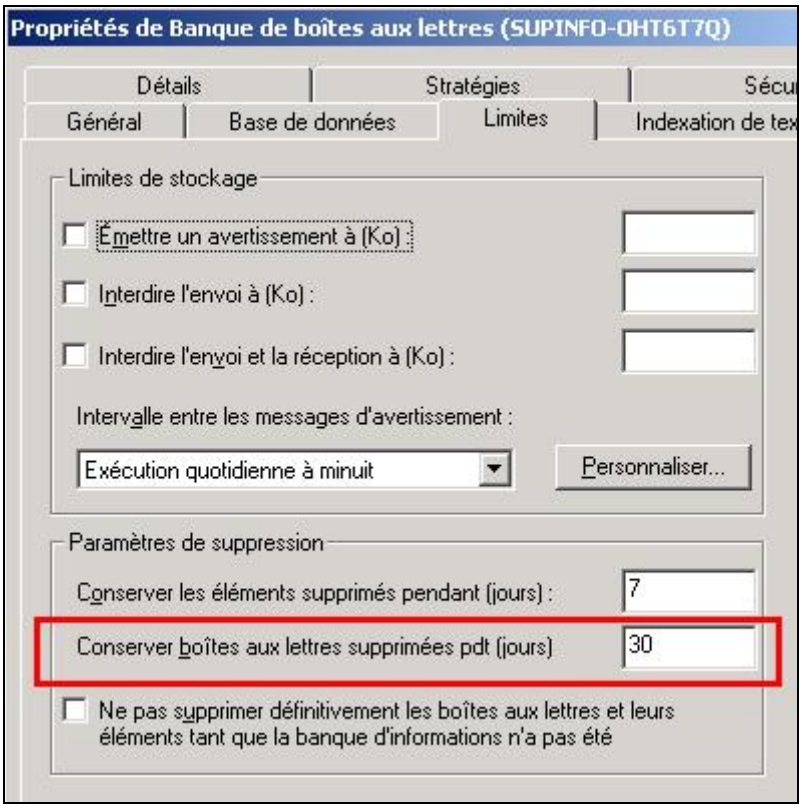
Une restauration d'un point dans le temps est effectuée lorsque la base de données est restaurée et que les fichiers journaux sont rejoués dans la base de données, contrairement à la restauration d'un point dans le temps.
Si tous les fichiers journaux sont intègres alors toutes les données pourront être rejoués et restaurés dans la base de données.
Ceci est la méthode à utiliser lorsque le mode circulaire pour les fichiers journaux n'est pas activé, vous ne pourrez pas utiliser cette méthode si le mode circulaire est activé.

12.3.4. La restauration des boîtes aux lettres et des messages

12.3.4.1. Restauration d'une boîte aux lettres

Par défaut, il existe une période de rétention de 30 jours pour vous permettre de récupérer une boîte aux lettres supprimée. Vous pouvez alors restaurer la boîte aux lettres et la reconnecter à nouveau.

Pour ajuster cette période, ouvrez les propriétés de la banque de boîte aux lettres, dans l'onglet **« Limites »** dans la section **« Paramètres de suppression »,** ajustez le temps pour l'item : **« Conserver boîtes aux lettres supprimées pdt »**



Malheureusement, si vous vous trouvez hors de cette période de rétention, vous devrez alors procéder à une restauration à l'aide d'un serveur de restauration dit également serveur de secours.
Pour ce faire :

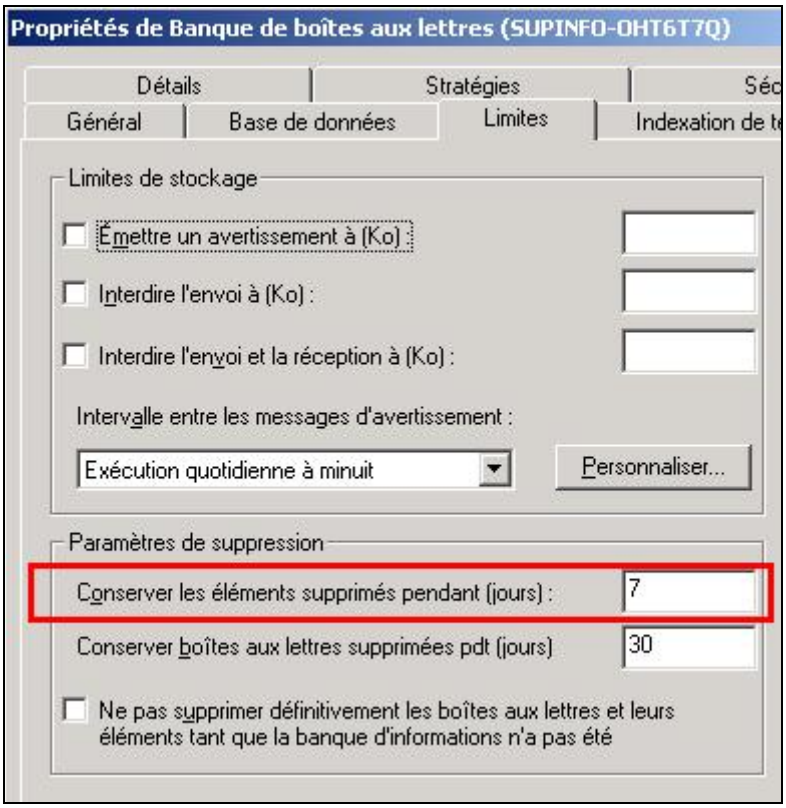
- Installez le serveur de restauration dans une autre forêt Active Directory que le serveur endommagé
- Installez Exchange 2003 sur le serveur de restauration en utilisant le même nom d'organisation qui a été utilisé pour l'organisation à restaurer
- Restaurer la base de données dans un groupe administratif ayant le même attribut **legacyExchangeDN** que la base de données d'origine sur le serveur de restauration
- Nommez le groupe de stockage de restauration et les bases de données de restauration avec les noms d'origine
- Créez un fichier PST, déplacez toutes les données dont vous avez besoin dans ce fichier.
- Ouvrez le fichier sur le serveur de production et déplacez de nouveau les données à l'emplacement voulu

12.3.4.2. Restauration des messages

Il se peut que certains messages soient effacés par inadvertance, malgré un envoi dans la corbeille et le vidage des éléments supprimés de la corbeille, il est tout de même possible de récupérer ces messages.

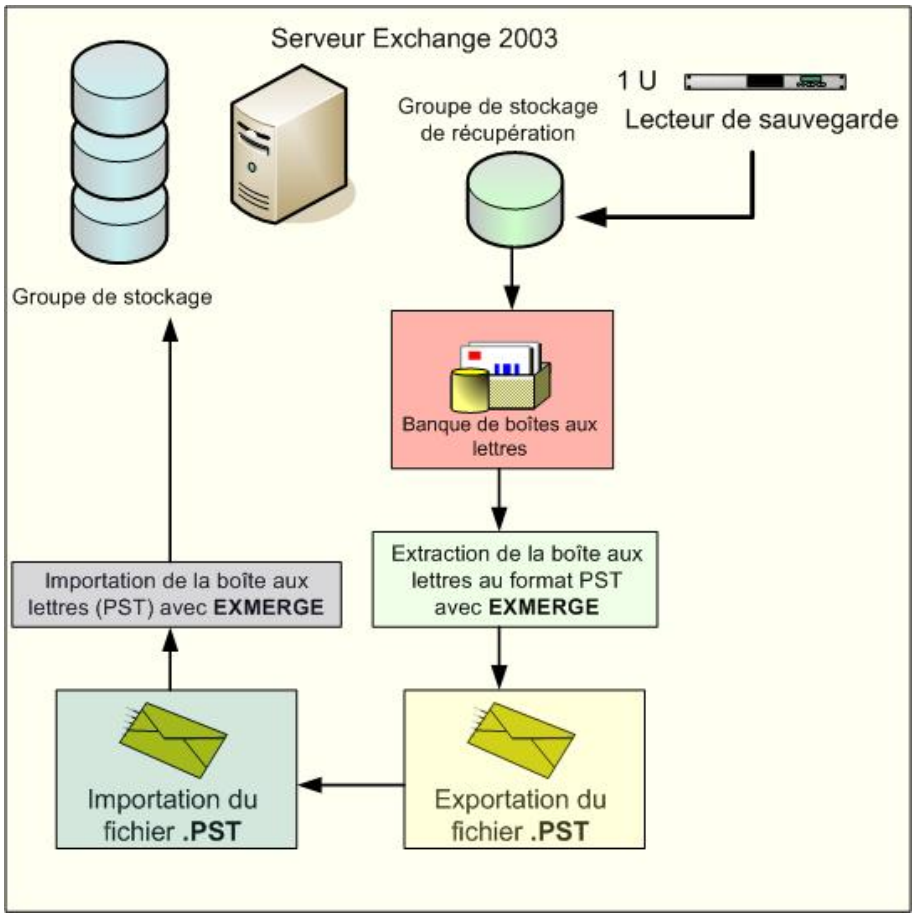
En effet Exchange serveur est doté d'une fonctionnalité lui permettant d'ajuster la conservation des éléments supprimés pendent une période de temps déterminée.

Pour ajuster cette période, ouvrez les propriétés de la banque de boîte aux lettres, dans l'onglet **« Limites »** dans la section **« Paramètres de suppression »,** ajustez le temps pour l'item : **« Conserver les éléments supprimées pdt »**



12.3.5. Utilisation de l'utilitaire EXMERGE avec un groupe de stockage de récupération

Pour avoir une plus grande flexibilité dans le processus de restauration, Microsoft Exchange 2003 serveur intègre la fonctionnalité « Groupe de stockage de récupération ».
Après avoir utilisé les groupes de stockage de récupération, vous devez utiliser l'utilitaire EXMERGE pour déplacer les boîtes aux lettres du groupe de stockage de récupération vers le groupe de stockage d'origine.



13. La maintenance préventive Exchange

L'AFNOR définit la **maintenance** comme « un ensemble d'actions permettant de maintenir et de rétablir un bien dans un état spécifié ou en mesure d'assurer un service déterminé.
Il existe deux types de maintenance :
- la maintenance corrective ou curative
- la maintenance préventives

Afin d'assurer la pérennité de votre système de messagerie, il sera obligatoire d'effectuer des opérations de maintenance, pour contrôler, analyser et optimiser le système (préventif).
Mis à part ces contrôles réguliers, il se peut que vous rencontriez des problèmes précis sur un composant Exchange ; vous devrez alors effectuer un dépannage immédiat pour rétablir la situation.

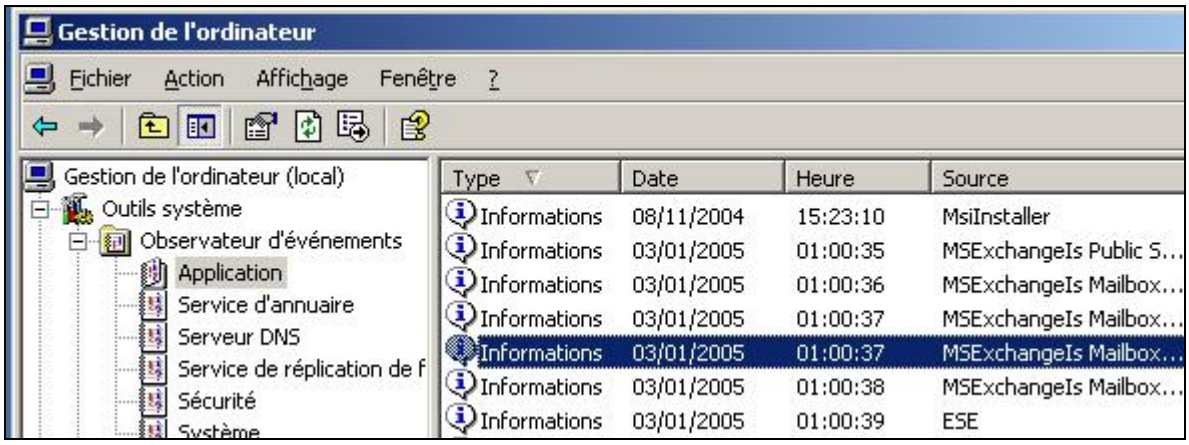
13.1. La maintenance journalière d'Exchange serveur

La maintenance journalière vous assure que les services critiques d'Exchange serveur fonctionnent correctement. Cette maintenance permet de traiter en amont les éventuels problèmes avant répercussions sur les utilisateurs.

Voici les points de contrôle à effectuer le plus régulièrement possible :

13.1.1. L'observateur d'événements

L'observateur d'événements permet d'obtenir des informations sur les dysfonctionnements de votre système, que ce soit des erreurs ou des avertissements, il sera nécessaire de prendre des mesures correctives pour stabiliser le système.

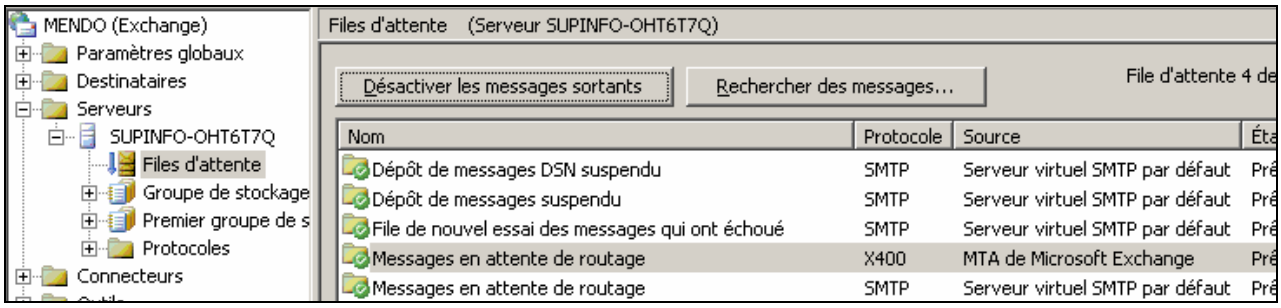


Vérifiez les numéros d'erreurs inscrits dans l'observateur d'événement, cherchez ensuite une solution à votre problème. Au quel cas vous ne trouvez pas de solution visitez les sites suivants :
- http://support.microsoft.com
- http://www.winerrors.com

Les événements contenant les erreurs:
1018 JET_errReadVerifyFailure
1019JET_errPageNotInitialized
1022 JET_errDiskIO sont des erreurs critiques concernant l'endommagement de la base de données Exchange 2003.

13.1.2. La file d'attente

La visualisation de la file d'attente du serveur vous permettra de déterminer la charge des messages sur votre serveur et éventuellement détecter les goulots d'étranglement.
La version de la console de la file d'attente Exchange 2003 a été amélioré par rapport à la version Exchange 2000, en effet cette console offre toutes les informations nécessaires pour repérer rapidement un blocage ou un mauvais routage dans votre organisation Exchange.



Surveillez attentivement les files suivantes :

Messages en attente de routage : cette file indique le nombre de messages en attente de routage, s'il y a un trop grand nombre de messages dans cette file, il faudra vous assurez de ne pas avoir de problème de routage au niveau de votre architecture que ce soit pour la file X400 ou SMTP.

Dépôt de messages suspendu : cette file héberge les messages transmis par Exchange ; s'il y a un trop grand nombre de messages dans cette file, il faudra vous assurez de ne pas avoir de problème avec une banque d'informations.

13.1.3. Espace disque

Exécuter la commande : **DISKMGMT.MSC** pour obtenir l'affichage de la console de management des disques. La console de management des disques permet d'obtenir des informations sur l'espace disponible sur vos partitions et/ou volumes.
En fonction des valeurs indiquées et du volume de données quotidien vous serez en mesure de déterminer si l'espace disque est suffisant pour stocker les bases de données et les fichiers journaux Exchange, sans oublier le système d'exploitation et autres programmes et données.
Comparez l'espace disque libre sur chacun des volumes Exchange, comparez ces valeurs en fonction de :

- votre croissance
- la taille individuelle de chaque boîte aux lettres
- la taille de l'index, le nombre de documents indexés
- la taille du dossier public et sa croissance

En fonction de toutes ces mesures, vous déterminerez si vous avez besoin d'ajouter de l'espace de stockage.

13.1.4. Les services

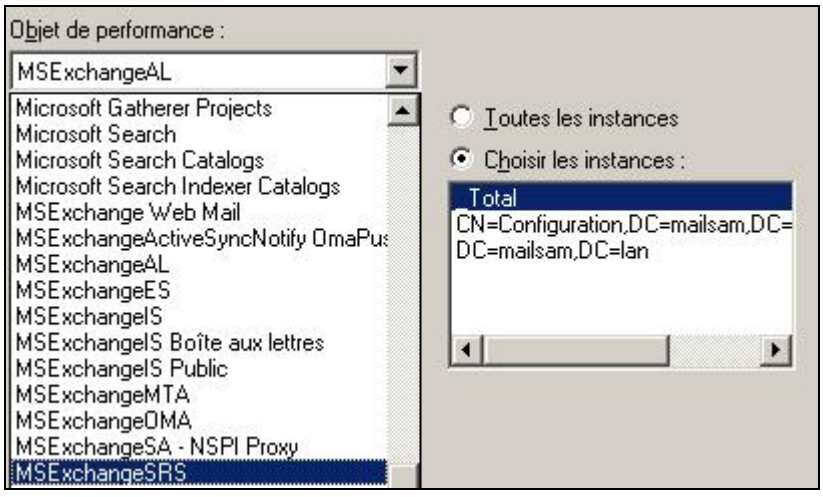
Il vous faudra également vous assurer que tous les services essentiels pour le fonctionnement d'Exchange Serveur, Windows 2003 et Active Directory sont démarrés.
Le service de réplication Active Directory, le service de publication Web pour OWA, le service SMTP et tous les services liés à Exchange.

Messagerie inter-sites	Permet l'éc...	Démarré	Automatique	Système local
Microsoft Exchange - Banque d'informa...	Gère la ba...	Démarré	Automatique	Système local
Microsoft Exchange - Connecteur de c...	Autorisez l...		Manuel	Système local
Microsoft Exchange - Contrôleur de co...	Fournit des...		Manuel	Système local
Microsoft Exchange - IMAP4	Fournit les ...		Désactivé	Système local
Microsoft Exchange - Moteur de routage	Fournit des...	Démarré	Automatique	Système local
Microsoft Exchange - Piles MTA	Fournit les ...	Démarré	Automatique	Système local
Microsoft Exchange - POP3	Fournit les ...		Désactivé	Système local
Microsoft Exchange - Service de réplic...			Désactivé	Système local
Microsoft Exchange - Service Événement	Analyse les...		Manuel	Système local
Microsoft Exchange - Surveillance du s...	Fournit les ...	Démarré	Automatique	Système local
Microsoft Search	Crée des in...	Démarré	Automatique	Système local

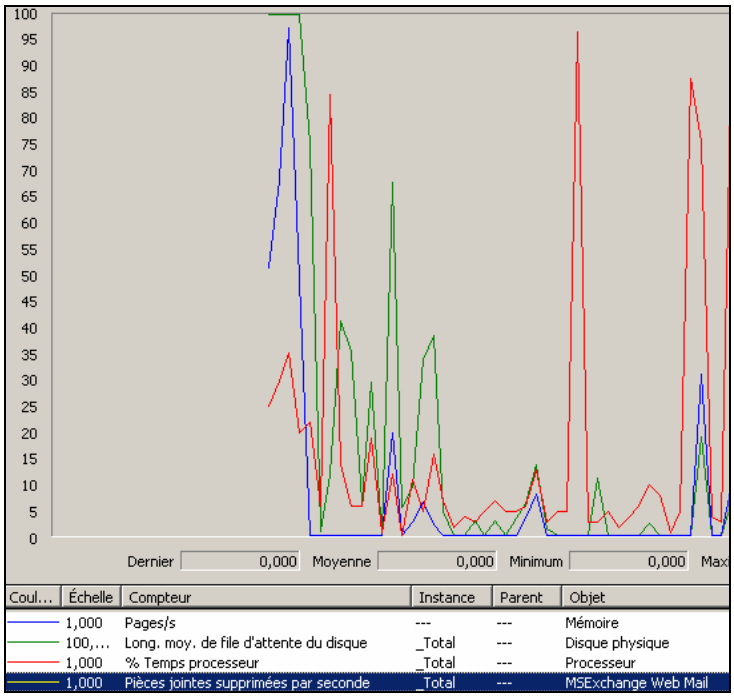
13.1.5. Les performances

Exécuter la commande : **PERFMON.EXE** pour obtenir l'affichage de la console du moniteur de performance.
A l'aide de cette console vous pourrez obtenir des mesures en temps réel de l'activité de votre serveur Exchange, lorsque vous installez Exchange serveur à l'instar de SQL serveur de nouveau Objet de performance relatif au serveur sont crées dans le moniteur de performance.
Sélectionnez ces nouveaux objets pour mesurer les performances du serveur, détecter les goulots d'étranglement et optimiser le serveur Exchange.

Ci-dessous une partie de la liste des objets Exchange à *monitorer*.



Représentation graphique du monitoring du serveur Exchange



13.1.6. Les fichiers journaux

Il sera également nécessaire de vérifier le contenu des différents fichiers journaux stockés sur votre serveur :

- les journaux de performances
- les journaux de protocoles
- les journaux des logiciels de sauvegarde
- les journaux du logiciel d'anti-virus
- les journaux du logiciel de pare-feu

13.1.7. La console HTTPMON

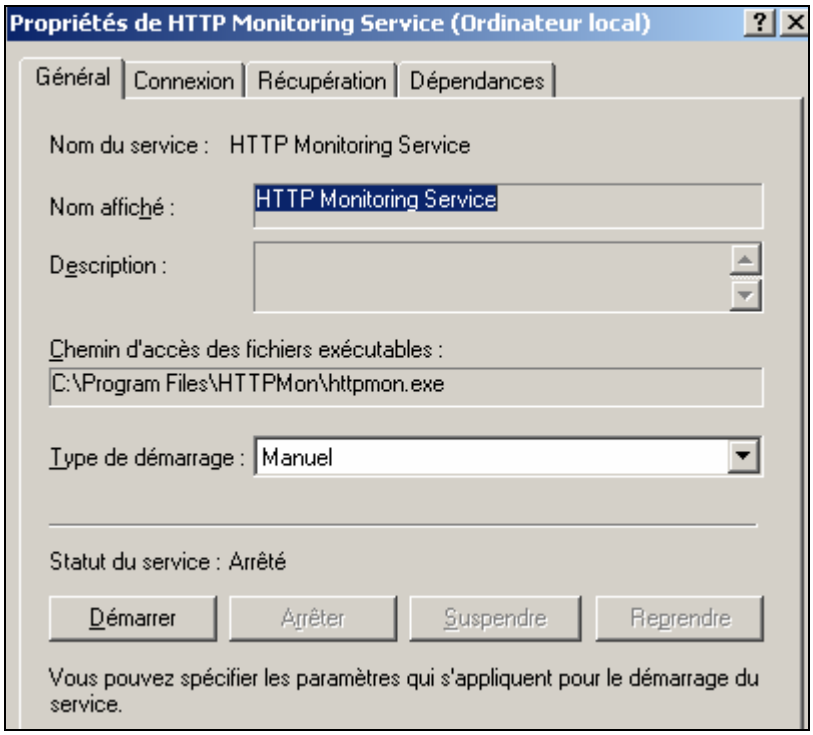
HTTPMon est un outil qui permet de surveiller les paramètres de sites ou d'applications Web et d'exporter les résultats au format standard CSV, afin d'exploiter ceux-ci dans une application de type Excel, SQL report services ou une application tierce-partie.

HTTPMon est disponible dans le kit de ressources techniques Windows 2000 et NT4.

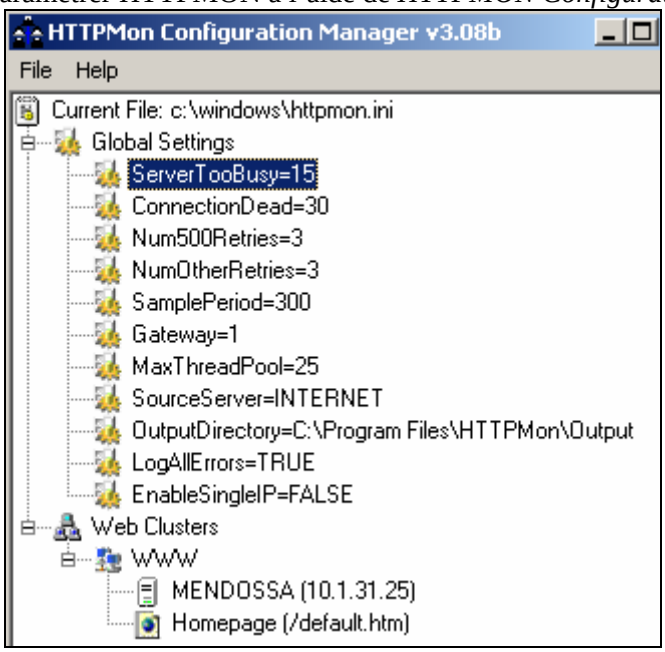
HTTPMon a 3 composants :

-Service temps réel : Permet de faire de l'analyse en temps réel
-Service rapport SQL server : Permet de gérer l'export/import des données dans SQL serveur
-Moniteur client : Permet d'afficher les résultats de votre analyse sous forme de pages Web

L'utilitaire HTTPMON est disponible dans le kit de ressources techniques Windows 2000.
Après installation, ouvrez la console des services à l'aide de la commande **SERVICES.MSC.**
Sélectionnez le service HTTP Monitoring Service dans la liste des services, affichez les propriétés de celui-ci, et assurez vous que le service est bien démarré.



Vous pourrez ensuite paramétrer HTTPMON à l'aide de *HTTPMON Configuration Manager*



L'utilisation du moniteur HTTPMon s'avère utile lorsque vos utilisateurs utilisent Outlook Web Access et que votre infrastructure est composée de cluster Web NLB.

13.1.8. Défragmenter la base de données à l'aide de l'outil ESEUTIL

Il existe un outil nommé ESEUTIL, cet outil permet de défragmenter, compresser, déplacer et réinitialiser les fichiers de la base de données d'Exchange serveur.

Grâce à cet utilitaire il est possible d'effectuer une défragmentation hors ligne pour réduire la taille de la base de données et créer une nouvelle base de données.

ESEUTIL est un utilitaire en ligne de commande qui est utilisé pour défragmenter les boîtes aux lettres et les dossiers publics, une analyse des tables et des enregistrements sont effectués lors du lancement de l'utilitaire.

L'outil ESEUTIL se trouve à l'emplacement suivant:
%lettre_de_lecteur%:\SETUP\I386\EXCHANGE\BIN

Voici les principaux commutateurs à utiliser avec cet utilitaire :

Eseutil /d - Effectuer la défragmentation hors ligne de la base de données Exchange
Eseutil /k - Effectuer la vérification du checksum
Eseutil /p - Effectuer la réparation d'une base de données endommagée
Eseutil /g - Effectuer la vérification de l'intégrité de la base de données.

13.1.9. Vérifier l'intégrité des données Exchange à l'aide de l'outil ISINTEG

L'utilitaire Isinteg détecter les problèmes liés à l'intégrité dans une banque d'informations hors ligne. Vous pouvez également réparer les problèmes détectés par Isinteg. L'utilitaire Isinteg s'exécute à partir d'une invite de commandes.

Avant l'utilisation de cet utilitaire vous devez arrêter le service de gestion de banques d'informations.

Démontez la banque d'information que vous souhaitez analyser.

Pour vérifier l'intégrité de votre banque d'informations et l'intégrité des répertoires : exécutez la ligne de commande suivante :
-isinteg -s %votre nom de serveur% -test allfoldertests

L'outil ISINTEG se trouve à l'emplacement suivant:
C:\PROGRAM FILES\EXCHSRVR\BIN

☞ Pour plus d'informations sur l'utilitaire ISINTEG, veuillez consulter la *Microsoft knowledge database* à l'adresse suivante : **http://support.microsoft.com/kb/182081**

14. Migration Exchange 5.5 vers Exchange 2003

Microsoft a fait des efforts considérables pour limiter le temps d'indisponibilité du serveur Exchange 5.5 lors de la migration de celui-ci vers la version 2003.

Il existe plusieurs méthodes de migration, vous choisirez la votre en fonction des ressources à votre disposition.

Ce document ayant pour but de vous montrer les différentes techniques de migration, certains détails de l'installation ou options des outils utilisés ne vous seront pas présentés, tous ces détails peuvent être trouvés sur le site de Microsoft ou sur le site du laboratoire SUPINFO des technologies Microsoft.

Rappel : La différence entre Exchange 5.5 et 2003 réside dans le fait de l'utilisation d'Active Directory.
En effet le couple Exchange 5.5 et Windows NT4.0, ne se base pas sur Active Directory inexistant et ne partage pas le même annuaire pour effectuer la concordance des comptes de domaine et compte de messagerie. Chaque entité possède sa propre gestion d'annuaire.

A contrario, le couple Exchange 2003 – Windows 2003 se base sur Active Directory pour créer et paramétrer les comptes de messagerie. Tout compte de messagerie créé sera directement associé à un compte Active Directory.
De fait Exchange 2003 bénéficie de tous les avantages d'Active Directory, en matière d'administration centralisée, de tolérance de panne, équilibrage de charges, réplication, sécurité et autres.

La première chose à faire sera donc la migration Windows NT4 vers Active Directory de façon à ce que les objets Exchange 5.5 restent encore accessibles.

Lorsque vous tenterez ensuite de créez une nouvelle boîte aux lettres pour un nouvel utilisateur directement depuis la console Utilisateurs et Ordinateurs Active Directory, cette action sera tout simplement impossible dans le fait que Active Directory n'a aucune visibilité détenue par le serveur Exchange 5.5 et tout comme Exchange 5.5 n'a aucune connaissance des informations contenues dans Active Directory.

Vous devrez alors créez un lien vers les 2 entités à l'aide de **connecteur Active Directory**.

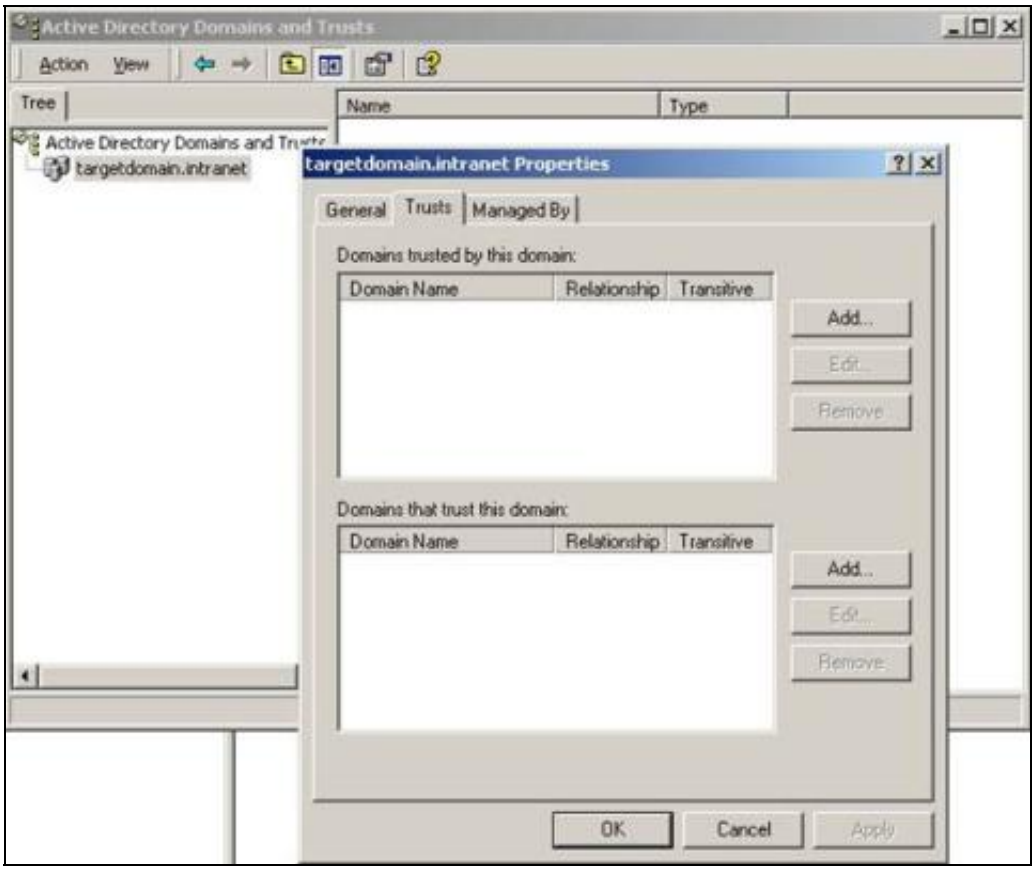
14.1. Préparation du système

Le partitionnement des données n'est pas obligatoire mais reste tout de même une partie très importante, pour l'optimisation de votre système. Vous prendrez alors une attention particulière au choix d'installation des partitions, que ce soit pour votre système Windows 2003 ou Exchange 2003.

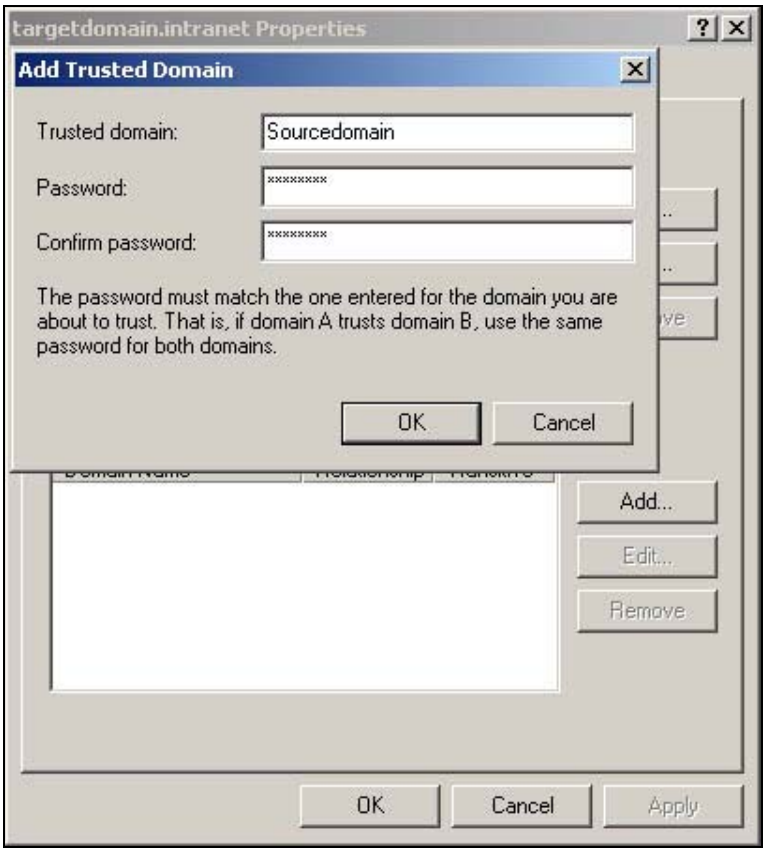
Voici les étapes à suivre lors de la migration d'un serveur Exchange 5.5 vers Exchange 2003.

14.1.1. Création d'une approbation entre les domaines

Sur le 2003 serveur:
Dans l'outil d'administration domaine et approbation Active Directory, dans les propriétés du domaine, choisir l'onglet approbation puis cliquez sur le bouton ajouter au niveau des domaines approuvés pour approuver l'ancien domaine. Le mot de passe que vous devez entrer vous servira pour approuver l'ancien domaine.



Sur le serveur intermédiaire.
Dans le gestionnaire des utilisateurs, allez dans relations d'approbations, puis cliquez sur le bouton ajouter pour les domaines approuvés puis entrez le nom du nouveau domaine, et un mot de passe pour l'approbation du domaine, je vous conseille d'utiliser le même mot de passe que précédemment. Ensuite cliquez sur le bouton ajoutez pour les domaines approuvant, spécifiez le nouveau domaine puis le mot de passe que vous avez entrés auparavant.

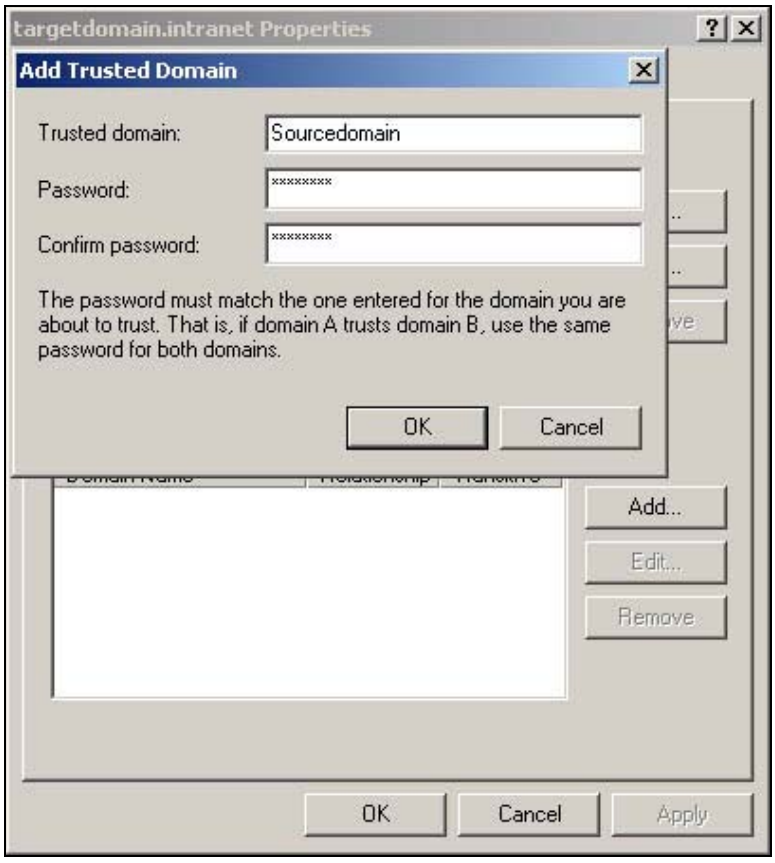


Sur le 2003 serveur:

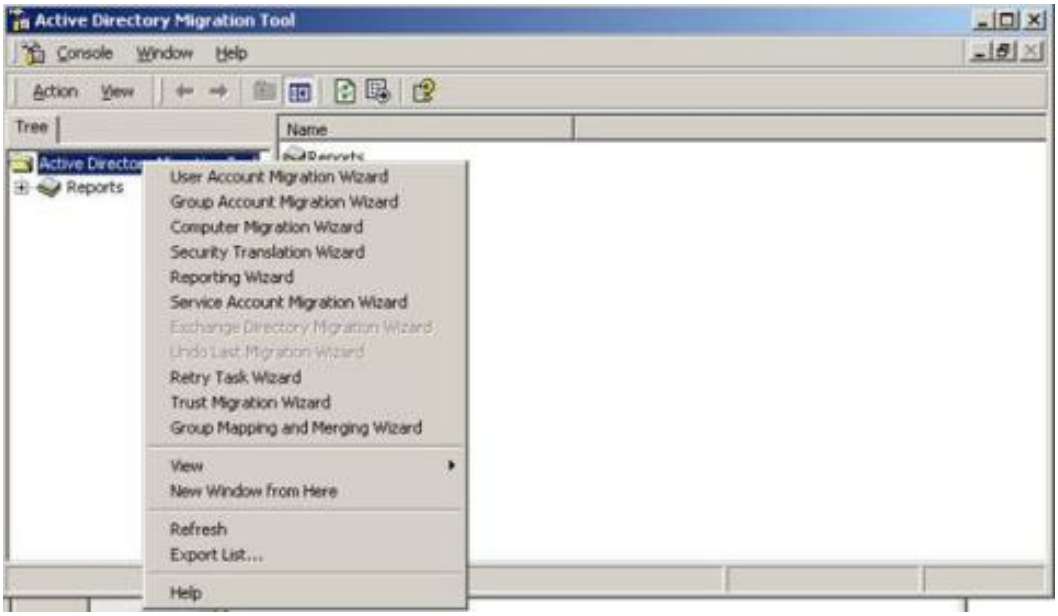
Toujours dans domaine et approbation active directory, cliquez sur le bouton ajoutez pour les domaines approuvant, spécifiez l'ancien domaine puis le mot de passe que vous avez entrés auparavant.

14.1.2. Mise en place d'un connecteur entre active directory et Exchange 5.5

Installez le connecteur active directory qui se trouve sur le cd dans le dossier **ADC\I386**
Dans l'arborescence du Service de connecteur active directory, choisissez outils ADC puis effectuez chacune des quatre étapes sans oublier de vérifier que les étapes 3 et 4 ont été effectuées correctement.
Dans l'arborescence du Service de connecteur active directory, choisissez connecteurs active directory et vérifiez que vous disposez bien de deux connecteurs, un pour les utilisateurs et un pour les dossiers publics. Si ce n'est pas le cas, il vous faut les créer en faisant un clic droit sur connecteurs active directory puis cliquez sur le nom du connecteur qui vous manque ou le cas échéant des deux connecteurs, l'un après l'autre, l'ordre n'est pas important. Il ne vous reste plus qu'à suivre les indications fournies par l'assistant.



14.1.3. Migration des utilisateurs avec ADMT2



Nous allons utiliser l'utilitaire Active Directory Migration Tool 2 pour la migration des utilisateurs car cet outil est le seul qui va permettre la migration des mots de passe des utilisateurs depuis un serveur NT4 ce qui dans le cas d'un nombre important d'utilisateurs est un avantage non négligeable.
Installation d'admt2, sur le cd de Windows 2003 serveur, notez bien le dossier d'installation d'ADMT.
Installation du PES (Password Export Server)
Mettez une disquette vierge dans le lecteur.

Dans le dossier d'installation d'ADMT2, lancez la commande:
"ADMT.exe key %Nom du domaine source% %Lettre du lecteur de disquette%: %Mot de passe optionnel%"
Dans l'éditeur de registre sur le serveur NT4 dans
\ SYSTEM\CurrentControlSet\Control\Lsa
Changez la valeur de la clé **AllowPasswordExport a 1.**

14.2. Migration des comptes utilisateurs

Vous allez devoir accorder à l'utilisateur qui effectue la migration, le plus souvent il s'agit de l'administrateur du nouveau domaine les droits sur les sites et objets Exchange sur le serveur intermédiaire. Pour cela vous allez devoir aller dans l'administrateur Exchange du serveur intermédiaire et ajouter les droits a l'utilisateur faisant la migration sur le site, et sur l'ancien domaine.
Choisir de joindre une organisation déjà existante (si les droits ne sont pas correctement accordés à l'utilisateur effectuant la migration, l'installateur ne vous autorisera pas à rejoindre l'organisation existante.
Poursuivez avec l'installation.
Lorsque l'installation est terminée, les utilisateurs que vous avez migré devraient avoir leur boites mail ajoutées, ces boites mails se trouvent sur le serveur intermédiaire.

Installation du serveur Exchange 2003
Avant de commencer l'installation d'Exchange 2003, vous allez devoir installer les composants suivants a l'aide de l'assistant de composants Windows qui se trouve dans ajout suppression de programmes:
Le framework .net
IIS avec le support pour asp.net
Le service NNTP
Le service SMTP
Installez le serveur Exchange 2003 en choisissant l'option avec les connecteurs déjà installés dans l'assistant d'installation.
Lancer les installations avec **/forestprep** et **/domainprep** comme indiqué dans la procédure d'installation.
Lancez l'installation d'Exchange.

14.2.1. Installation dans une organisation existante

Vous allez devoir accorder à l'utilisateur qui effectue la migration, le plus souvent il s'agit de l'administrateur du nouveau domaine les droits sur les sites et objets Exchange sur le serveur intermédiaire. Pour cela vous allez devoir aller dans l'administrateur Exchange du serveur intermédiaire et ajouter les droits a l'utilisateur faisant la migration sur le site, et sur l'ancien domaine.
Choisir de joindre une organisation déjà existante (si les droits ne sont pas correctement accordés à l'utilisateur effectuant la migration, l'installateur ne vous autorisera pas à rejoindre l'organisation existante.
Poursuivez avec l'installation.
Lorsque l'installation est terminée, les utilisateurs que vous avez migré devraient avoir leur boites mail ajoutées, ces boites mails se trouvent sur le serveur intermédiaire.

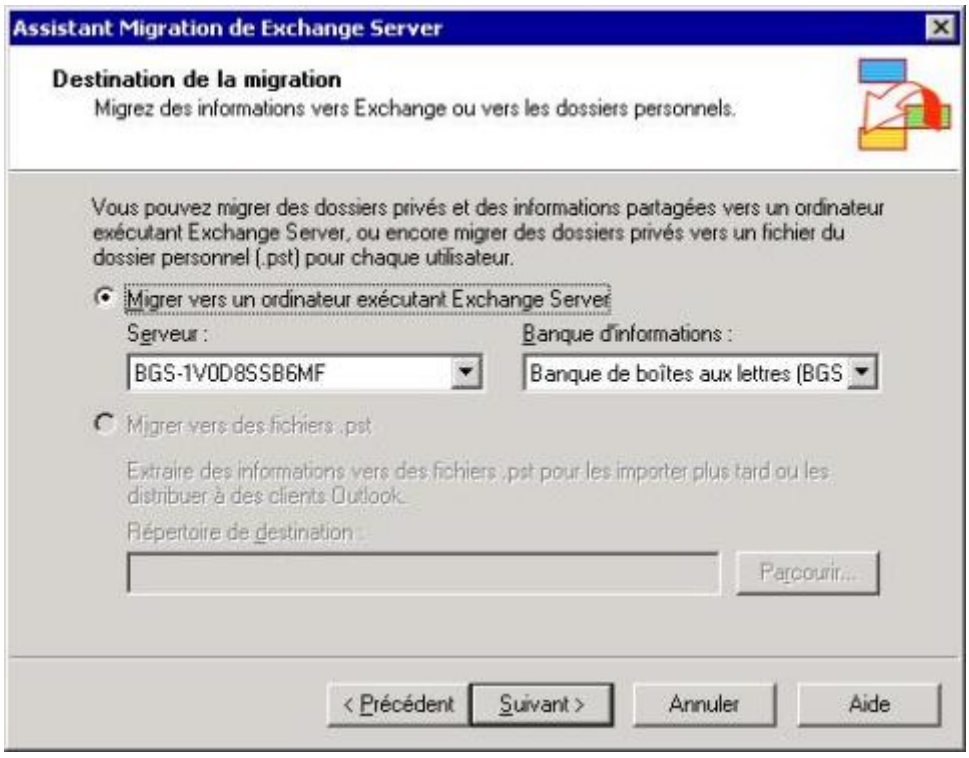
14.2.2. Installation inter organisationnelle

Pour cette option vous n'allez pas avoir besoin de donner de droits particuliers sur le serveur Exchange se trouvant sur le serveur intermédiaire à l'utilisateur effectuant l'installation.
Choisissez l'option « *créer une nouvelle organisation* ». Vous pouvez mettre n'importe quel nom pour l'organisation a l'exception du nom de l'ancienne organisation.

Poursuivez avec l'installation.
Lorsque l'installation est terminée, les utilisateurs que vous avez migré devraient avoir leur boites mail ajoutées, ces boites mails se trouvent sur le serveur intermédiaire

Migration des boites mail vers le nouveau serveur:
Vérifiez que vos boites mails ont bien été connectées avec les utilisateurs, si ce n'est pas le cas, sauter les deux étapes suivantes et passez à la migration des boites mails avec les outils de migration Exchange.
Sur le nouveau serveur, dans utilisateurs et ordinateurs active directory vous allez sélectionner tous les utilisateurs pour lesquels vous souhaitez migrer les boites mails.
Faites un clic droit sur les utilisateurs sélectionnés et sélectionnez taches Exchange puis choisissez déplacer une boite au lettre, il ne reste plus qu'à vous laisser guider et les boites mails sont migré (Cette opération peut être longue en fonction de la taille et du nombre de boite aux lettres que vous allez avoir à déplacer)

14.2.3. Migration des boites mails à l'aide des outils de migration Exchange.



Utilisez l'outil de migration de Microsoft Exchange pour migrer les comptes Exchange vers le nouveau serveur
il est possible que l'outil de migration ait crée des doublons avec des noms proches, cela est du au fait que l'outil de migration n'a pas réussi à mapper la boite mail au compte existant. Pour résoudre ce problème, il faut utiliser l'outil assistant nettoyage de compte Active Directory qui va vous permettre de fusionner les deux comptes créés par les différents outils de migration.

14.3. Migration des dossiers publics

14.3.1. Migration dans une organisation déjà existante

A l'aide d'une version d'Outlook vérifiez que vos dossiers publiques sont bien accessibles, si ce n'est pas le cas, revenez à l'étape de l'installation du connecteur ADC et recréez une connection pour les dossiers publiques, n'oubliez pas que la connection doit être bidirectionnelle pour les dossiers publiques.
Migration des dossiers publiques à l'aide de pfmigrate.wsf:
A l'aide de la commande **pfmigrate.wsf /S: /T: /N:20 /A /SF** vous allez pouvoir migrer les dossiers publiques vers le nouveau serveur.
A l'aide de la commande **pfmigrate.wsf /S: /T: /N:20 /R /SF** vous allez pouvoir supprimer les dossiers publiques du serveur intermédiaire.
Les options /s et /t représentent repectivement les serveurs sources et destination, il va vous falloir rajouter leur nom à la suite de ces options pour que ces commandes puissent fonctionner.

14.3.2. Migration inter organisationnelle:

Installez **Outlook 97**, il vous permettera de créer les dossiers publiques, certains conflits peuvent apparaître avec des versions ultérieures d'Outlook
Sur le serveur intermédiaire Créer un utilisateur PFPublisher avec un compte Exchange associé.
Créer un Dossier publique ExchsyncSecurityFolder affecter à PFPublisher les droits owner et spécifier aucune permission pour anonyme et défaut
Donner les droits owner sur tous les dossiers avec la commande **"pfadmin %profilename% setacl all PFPublisher O"**, vous pouvez également affecter tous ces droits à la main, mais si vous avez un grand nombre de dossiers publiques cette commande à un intérêt certain.
Sur le serveur 2003 Créer un utilisateur PFSubscriber
Créer un Dossier publique ExchsyncSecurityFolder affecter à PFSubscriber les droits owner et spécifier aucune permission pour anonyme et défaut
A partir de Exscfg pour Exchange 2003 (utilitaire se trouvant sur le cd d'installation d'Exchange 2003), configurez les fichiers de configuration de la réplication.
A partir de Exscfg pour Exchange 2003: Lancer la réplication.
Consulter le fichier de log pour s'assurer du bon déroulement de l'installation.

14.3.3. Suppression des connecteurs

Maintenant que vos boites mail et vos dossiers publiques ont été migrés, votre serveur est prêt à être mis en production, il ne vous reste plus qu'a supprimer les connecteurs que vous avez créés auparavant.
Pour ce faire vous allez de voir aller dans l'outil connecteur active directory et cliquez sur connecteurs active directory, ensuite supprimez les connecteurs.
Votre migration est terminée.