Microsoft Windows Server System

Guide de transport et de routage Exchange Server 2003

Dernière mise à jour :	août 2004
Version du produit :	Exchange Server 2003
Révisé par :	Équipe de développement Exchange
Informations récentes :	www.microsoft.com/exchange/library
Auteur :	Patricia Anderson

Guide de transport et de routage Exchange Server 2003

Patricia Anderson

Date de publication : mars 2004

S'applique à : Exchange Server 2003

Copyright

Remerciements

Éditeur du projet : Alison Hirsch

Rédacteurs ayant offert leur contribution : Per Farny, Mohammad Nadeem

Éditeurs ayant offert leur contribution : Katherine Enos, Janet Lowen

Réviseurs techniques : Pretish Abraham, Simon Attwell, Philip Buelow, Max Ciccotosto, Wayne Cranston, Greg Derk, Ade Famoti, Per Farny, Scott Landry, Dominic Lai, Will Martin, Mohammad Nadeem, Colin Nash, Gerald Ramich, Hao Zhang

Conception graphique : Kristie Smith

Production : Joe Orzech, Sean Pohtilla

Table des matières

Introduction

Ce guide explique comment fonctionnent le transport et le routage dans Microsoft® Exchange Server 2003 et comment vous pouvez configurer Exchange pour permettre un flux de messages internes et externes.

Qu'allez-vous apprendre dans ce guide ?

Ce guide fournit essentiellement des réponses détaillées aux questions suivantes :

- Quels sont les composants de base concernés par le transport et le routage et quels sont leurs rôles ?
- Comment fonctionnent les groupes de routage, les connecteurs et les maîtres de groupes de routage dans Exchange Server 2003 ?
- Qu'est-ce que le protocole SMTP (Simple Mail Transfer Protocol) et à quoi sert-il ?
- Comment fonctionne le protocole SMTP dans Exchange ?
- Quels sont les éléments essentiels de SMTP et comment gérer ce protocole dans Exchange ?
- Quels sont les composants sur lesquels repose le transport ? Comment ces composants affectent-ils le fonctionnement du transport et du routage ?
- Quelles sont les topologies de routage courantes et à quel moment sont-elles déployées ?
- Comment faut-il configurer votre topologie de routage ?
- Quels sont les scénarios de déploiement courants permettant de se connecter à Internet ? Comment prendre en charge les différents besoins de l'organisation ou répondre aux diverses exigences comme le partage d'un domaine de messagerie SMTP ou la prise en charge de deux domaines de messagerie SMTP ?
- Comment configurer SMTP, Exchange et le système DNS (Domain Name System) pour prendre en charge la remise des messages Internet ?
- Quelles sont les mesures à prendre pour sécuriser votre infrastructure et vos serveurs Exchange ?
- Quels sont les outils et les processus disponibles pour résoudre et diagnostiquer les problèmes liés au transport et au routage ?

À qui s'adresse ce guide ?

Ce guide s'adresse en particulier aux professionnels suivants :

Architectes système
: Personnes responsables de la planification et de l'élaboration des stratégies et des solutions de l'entreprise.

Administrateurs Exchange de l'entreprise
: Personnes responsables de l'installation, de la maintenance et de l'administration des logiciels dans l'entreprise.

Gestionnaires de comptes d'utilisateur Exchange
: Personnes responsables de la configuration des comptes individuels de messagerie et de la modification des comptes individuels Exchange dans le service d'annuaire Microsoft Active Directory®.

Prise en charge de la messagerie
: Personnes spécialisées dans la résolution des problèmes rencontrés par les utilisateurs finaux avec leur environnement de messagerie.

Opérateurs du support technique

Personnes chargées d'apporter une assistance aux utilisateurs finaux dans divers domaines logiciels et matériels notamment les problèmes de messagerie simples.

Terminologie

Avant de lire ce guide, vous devez connaître les termes suivants :

enregistrement « A »
Enregistrement de ressources d'adresses dans DNS ; de façon spécifique, enregistrement DNS qui associe un nom d'hôte à une adresse IP.

serveur tête de pont
Ordinateur connectant des serveurs à l'aide du même protocole de communication afin d'assurer la transmission des informations d'un serveur à un autre. Dans Exchange 2003 et Exchange 2000 Server, un serveur tête de pont représente un point de connexion entre un groupe de routage et un autre groupe de routage, un système distant ou un autre système externe.

connecteur
Composant permettant aux informations de circuler entre deux systèmes. Les connecteurs prennent, par exemple, en charge le transfert des messages, la synchronisation d'annuaire et l'interrogation du calendrier entre Exchange et d'autres systèmes de messagerie. Lorsque des connecteurs sont en place, les informations utilisateur de base sont préservées sur les deux systèmes de messagerie. L'échange de messages et d'informations diverses entre Exchange et d'autres systèmes de messagerie s'effectue de façon transparente pour l'utilisateur, même si les deux systèmes fonctionnent différemment.

DNS (Domain Name System)
Service de nom standard TCP/IP qui permet aux clients et aux serveurs de résoudre des noms en adresses IP (Internet Protocol) et inversement. Les services de nom de domaine dynamique Microsoft Windows® 2000 Server et Windows Server™ 2003 permettent aux clients et aux serveurs de s'enregistrer eux-mêmes sans que les administrateurs définissent manuellement les enregistrements.

nom de domaine complet
Nom de domaine DNS (Domain Name System) déclaré sans ambiguïté afin d'indiquer avec certitude son emplacement dans l'arborescence d'espace de noms du domaine. Les noms de domaines complets se distinguent des noms relatifs par le fait qu'ils se déclarent généralement à l'aide d'un point (.), par exemple, « host.example.com », pour qualifier leur position à la racine de l'espace de noms. Certaines fonctions Exchange utilisent le nom de l'hôte du serveur Exchange/nom NETBIOS qui correspond au nom de domaine complet sans la partie domaine du nom.

serveur de catalogue global
Contrôleur de domaine qui contient un réplica partiel de chaque domaine dans Active Directory. Un catalogue global contient une copie de chaque objet dans Active Directory, mais un nombre limité des attributs de chaque objet.

enregistrement de ressource de serveur de messagerie (MX)
Enregistrement DNS qui définit un serveur de messagerie pour un domaine donné. Un serveur de messagerie est configuré pour associer un domaine de messagerie au nom de domaine complet d'un ou plusieurs serveurs virtuels SMTP qui servent ce domaine.

protocole SMTP (Simple Mail Transfer Protocol)
Norme Internet pour le transport et la remise des messages électroniques. Basée sur les spécifications dans les RFC (*Request For Comments*) 2821 et RFC 2822, le service SMTP de Microsoft est inclus dans le système d'exploitation Windows 2000. SMTP est le protocole de transport par défaut pour Exchange 2003 et Exchange 2000.

Pour plus d'informations, consultez le *Glossaire Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=24625).

Comment ce guide est-il structuré ?

Ce guide en cinq parties comporte un total de quinze chapitres et trois annexes. Pour obtenir des résultats optimaux, consultez les parties et les chapitres dans l'ordre, car chacun d'eux s'appuie sur des concepts décrits dans les chapitres précédents.

Première partie Composants de transport et de routage

La première partie « Composants de transport et de routage » présente et explique les composants et les dépendances concernés dans le transport :

Chapitre 1, « Présentation du routage »
: Ce chapitre présente une vue d'ensemble du routage. Il explique les fonctions des groupes et des connecteurs de routage ainsi que la manière dont Exchange utilise le routage de l'état des liaisons pour déterminer le moyen optimal de remettre un message.

Chapitre 2, « Présentation du protocole SMTP »
: Ce chapitre présente une vue d'ensemble du protocole SMTP et explique la manière dont il permet le flux des messages dans une organisation Exchange.

Chapitre 3, « Dépendances de transport »
: Ce chapitre explique les composants nécessaires au fonctionnement correct du transport : les services IIS (Internet Information Services), Active Directory, DNS, les stratégies de destinataire, le service de mise à jour de destinataire et le service d'annuaire vers la métabase (DS2MB).

Deuxième partie Configuration du flux des messages

La deuxième partie « Configuration du flux des messages » présente des scénarios de déploiement SMTP et de routage destinés à configurer le flux des messages et explique les processus concernés par l'activation de la remise des messages externes et internes :

Chapitre 4, « Configuration du service DNS »
: Ce chapitre vous guide tout au long du processus de vérification de la configuration correcte du service DNS (Domain Name System) dans votre organisation Exchange.

Chapitre 5, « Configuration de votre topologie de routage »
: Ce chapitre présente des topologies de routage de base, décrit comment et quand utiliser les groupes de routage, et explique comment configurer le flux des messages dans votre organisation Exchange.

Chapitre 6, « Scénarios de déploiement pour la connectivité Internet »
: Ce chapitre présente des scénarios personnalisés et courants pour la connectivité Internet.

Chapitre 7, « Connexion à Internet »
: Ce chapitre contient les procédures permettant de configurer l'envoi et la réception de messages Internet par Exchange.

Troisième partie Sécurisation du transport

La troisième partie « Sécurisation du transport » traite des considérations en matière de sécurité du transport pour votre infrastructure et vos serveurs Exchange.

Chapitre 8, « Sécurisation de votre infrastructure »
: Ce chapitre se penche sur les méthodes dont vous disposez pour protéger votre infrastructure en désactivant certains services superflus dans IIS et en utilisant des pare-feu et des réseaux privés virtuels.

Chapitre 9, « Sécurisation de votre serveur Exchange »
: Ce chapitre explique les méthodes recommandées en matière de sécurité générale vous permettant de protéger vos serveurs Exchange.

Chapitrer 10, « Configuration du filtrage et contrôle du courrier indésirable »
Ce chapitre explique comment contrôler les messages commerciaux non sollicités, également connu sous le nom de courrier indésirable, à l'aide de filtrage au niveau des connexions, des expéditeurs et des destinataires Exchange.

Quatrième partie Résolution des problèmes

La quatrième partie « Résolution des problèmes » présente les problèmes et les techniques de résolution auxquels vous pouvez faire appel pour résoudre les problèmes liés au flux des messages, au routage et aux rapports de non-remise.

Chapitre 11, « Résolution des problèmes de routage »
Ce chapitre se concentre sur les problèmes de routage courants ainsi que les mesures que vous pouvez prendre pour identifier et résoudre ces problèmes.

Chapitre 12, « Résolution des problèmes de flux des messages et SMTP »
Ce chapitre explique les techniques disponibles pour identifier et résoudre les problèmes liés à SMTP et au flux des messages.

Chapitre 13 « Résolution des problèmes de rapports de non-remise »
Ce chapitre explique comment diagnostiquer les codes des rapports de non-remise et décrit les techniques que vous pouvez utiliser pour résoudre les problèmes s'y rapportant.

Partie 5 Informations internes de transport

La cinquième partie « Éléments internes du transport » contient des informations avancées sur l'architecture de transport sous-jacente et les concepts sur l'état des liaisons.

Chapitre 14, « Présentation des composants de transport internes »
Ce chapitre indique comment les composants de transport internes, comme le moteur de routage, le moteur de files d'attente avancé et le catégoriseur de messages, opèrent conjointement pendant la remise des messages.

Chapitre 15, « Concepts avancés sur l'état des liaisons »
Ce chapitre examine les détails du paquet de l'état des liaisons et décrit des concepts avancés relatifs à l'état des liaisons.

Annexes

Annexe A, « Référence »
Cette section contient des documents de référence sur les commandes SMTP, les fonctions des composants de transport SMTP internes et les récepteurs d'événements.

Annexe B, « Ressources »
Cette section contient des liens vers les ressources mentionnées dans ce guide. Cette annexe contient également des liens vers des ressources supplémentaires qui peuvent vous aider à mieux comprendre le routage et le transport ainsi qu'Exchange.

Annexe C, « Accessibilité pour les personnes atteintes de handicaps »
Cette annexe fournit des informations sur les fonctionnalités, les produits et les services qui facilitent l'accès à la famille Microsoft Windows Server™ 2003, la famille Windows® 2000 Server, Microsoft Exchange Server 2003 et Microsoft Office Outlook Web Access® 2003 pour les personnes présentant une incapacité physique.

Première partie Composants de transport et de routage

Le routage et le transport des messages assurent ensemble la remise des messages internes et externes. Le routage des messages définit le mode d'acheminement des messages entre les serveurs au sein de l'organisation et vers les autres serveurs à l'extérieur de l'organisation. Votre topologie de routage, fondée sur les groupes de routage et les connecteurs que vous définissez, détermine le chemin emprunté par les messages pour atteindre leur destination finale. Le transport détermine le mode de remise et de traitement des messages.

Les serveurs Microsoft® Exchange utilisent le protocole de transport SMTP (Simple Mail Transfer Protocol) pour communiquer entre eux et envoyer des messages à l'aide de la topologie de routage. Le protocole SMTP fait partie du système d'exploitation Microsoft® Windows Server™ 2003 ou Microsoft Windows® 2000 Server. Lorsque vous installez Exchange sur un serveur Windows Server 2003 ou Windows 2000 Server, Exchange étend le protocole SMTP pour prendre en charge des commandes SMTP supplémentaires qui offrent des fonctionnalités avancées. Ces fonctionnalités incluent la possibilité de communiquer l'état des liaisons (informations et coûts relatifs aux chemins de routage des messages disponibles) et d'autres fonctionnalités Exchange.

La partie 1 comprend les chapitres suivants :

Chapitre 1 « Présentation du routage »
: Ce chapitre explique le fonctionnement des groupes et des connecteurs de routage, des informations sur l'état des liaisons afin de permettre une remise performante des messages.

Chapitre 2 « Présentation du protocole SMTP »
: Ce chapitre fournit une description détaillée du protocole SMTP et de son fonctionnement dans Exchange 2003, et explique le processus d'envoi et de réception des messages Internet.

Chapitre 3 « Dépendances de transport »
: Ce chapitre décrit les composants dont dépend SMTP et passe en revue l'interaction de chaque composant avec SMTP.

Présentation du routage

Le routage détermine le flux des messages entre les serveurs de votre organisation Microsoft® Exchange et vers les utilisateurs de votre organisation. Pour la remise des messages internes et externes, Exchange fait appel au routage en commençant par déterminer le chemin le plus efficace, puis le chemin disponible le moins coûteux pour la remise des messages. Les composants du routage interne effectuent cette évaluation en fonction des groupes de routage et des connecteurs que vous configurez ainsi que des espaces d'adressage et des coûts associés à chaque chemin.

Le routage assure les fonctions suivantes :

- Déterminer le saut suivant (destination suivante pour un message en route vers sa destination finale) en fonction du chemin le plus efficace.
- Échanger des informations sur l'état des liaisons (état et disponibilité des serveurs et des connexions entre les serveurs) au sein des groupes de routage et entre ces groupes.

Cette section explique le fonctionnement des groupes et des connecteurs de routage, des informations sur l'état des liaisons afin de permettre une remise performante du flux des messages.

Composants du routage

Les composants du routage constituent la topologie et les chemins de routage utilisés pour remettre les messages internes et externes. Le routage repose sur les composants suivants que vous définissez dans votre topologie de routage :

Groupes de routage Ensembles logiques de serveurs utilisés pour contrôler le flux des messages et les redirections de dossiers publics. Les groupes de routage partagent une ou plusieurs connexions physiques. Au sein d'un groupe de routage, tous les serveurs communiquent et transfèrent des messages directement entre eux.

Connecteurs Chemins désignés entre les groupes de routage, vers Internet ou vers un autre système de messagerie. Chaque connecteur définit un chemin à sens unique vers une autre destination.

Informations sur l'état des liaisons Informations sur les groupes et les connecteurs de routage, leurs configurations utilisées par le routage afin de déterminer le chemin de remise le plus efficace pour un message.

Composants de routage interne Composants, notamment le moteur de routage, chargés de fournir et de mettre à jour la topologie de routage pour les serveurs Exchange de votre organisation. Pour plus d'informations sur les composants de routage interne, consultez le chapitre 14 « Présentation des composants de transport internes ».

Description des groupes de routage

Dans son état par défaut, Exchange Server 2003, tout comme Exchange 2000 Server, fonctionne comme si tous les serveurs dans une organisation appartenaient à un groupe de routage unique et étendu. Ainsi, tout serveur Exchange peut envoyer des messages directement à n'importe quel autre serveur Exchange au sein de l'organisation. Toutefois, dans les environnements aux besoins d'administration spécifiques et où la connectivité réseau et la distribution géographique sont variables, vous pouvez accroître l'efficacité du flux des messages en créant des groupes de routage et des connecteurs de groupes de routage conformes à votre infrastructure réseau. En créant des groupes de routage et des connecteurs de groupes de routage, les serveurs au sein d'un groupe de routage peuvent toujours s'envoyer des messages directement entre eux, mais ils

utilisent le connecteur du groupe de routage sur ces serveurs avec la meilleure connectivité réseau pour communiquer avec les serveurs d'un autre groupe.

Pour plus d'informations sur la création de groupes de routage et les considérations associées, consultez le chapitre 8, « Scénarios de déploiement pour la connectivité Internet ».

Présentation des connecteurs

Les connecteurs fournissent un chemin à sens unique pour le flux des messages vers une destination spécifique. Les connecteurs principaux dans Exchange 2003 sont les suivants :

- **Connecteurs de groupe de routage** Ces connecteurs fournissent un chemin à sens unique par lequel sont acheminés les messages entre les serveurs d'un groupe de routage et les serveurs d'un groupe de routage différent. Les connecteurs de groupe de routage utilisent une connexion SMTP (Simple Mail Transfer Protocol) pour activer la communication vers les serveurs dans le groupe de routage connecté. Les connecteurs de groupe de routage sont la méthode préférée de connexion des groupes de routage.
- **Connecteurs SMTP** Les connecteurs SMTP sont utilisés pour définir des chemins isolés pour le courrier destiné à Internet ou une adresse externe ou un système de messagerie non Exchange. L'utilisation du connecteur SMTP pour connecter des groupes de routages n'est ni recommandée ni conseillée. Les connecteurs SMTP sont conçus pour une remise des messages externes.
- **Connecteurs X.400** Les connecteurs X.400 sont conçus principalement pour permettre une connexion entre les serveurs Exchange et les autres systèmes X.400 ou les serveurs exécutant Exchange Server version 5.5 situés à l'extérieur de l'organisation Exchange. Un serveur Exchange 2003 peut alors envoyer des messages à l'aide du protocole X.400 sur ce connecteur.

  Important Les connecteurs X.400 sont uniquement disponibles dans Exchange Server 2003 Édition Entreprise.

À chaque connecteur correspondent un coût et un espace d'adressage associés ou un groupe de routage connecté désigné comme le point de destination du connecteur. Lors de la détermination du chemin de routage le plus performant, la logique de routage d'Exchange commence par examiner l'espace d'adressage ou le groupe de routage connecté défini sur chaque connecteur afin de trouver la destination qui correspond le mieux à la destination du message, puis le routage évalue le coût associé à chaque connecteur. Le routage n'utilise les coûts que lorsque deux connecteurs possèdent le même espace d'adressage défini ou les mêmes groupes de routage connectés. La section suivante explique la manière dont Exchange utilise ces informations.

Présentation des informations sur l'état des liaisons

Exchange Server 5.5 repose sur la table de routage d'adresses de la passerelle pour déterminer le choix de routage dans une organisation Exchange. Cette méthode utilise un algorithme de routage de vecteur de distance, ce qui peut donner lieu à des boucles de routage dans certaines situations. Exchange 2003, comme Exchange 2000, utilise un algorithme de routage d'état des liaisons pour propager des informations sur l'état des liaisons sous la forme d'une table d'état des liaisons stockée en mémoire sur tous les serveurs Exchange 2000 et Exchange 2003 dans l'organisation. Un algorithme d'état des liaisons offre les avantages suivants :

- Chaque serveur Exchange peut sélectionner le routage optimal des messages à la source ce qui évite d'envoyer des messages sur un chemin de routage où un lien (ou chemin) n'est pas disponible.
- Les messages ne rebondissent plus entre les serveurs car chaque serveur Exchange dispose d'informations à jour sur l'état de disponibilité ou non des chemins de routages alternatifs ou redondants.

- Les boucles au niveau des messages ne se produisent plus.

La table d'état des liaisons contient des informations sur la topologie de routage de l'ensemble de l'organisation Exchange et indique l'état de disponibilité ou non de chaque connecteur dans la topologie. Par ailleurs, cette table contient les coûts et les espaces d'adressage associés à chaque connecteur disponible. Ces informations permettent à Exchange de déterminer le chemin de routage le moins onéreux pour l'adresse de destination. Si un connecteur n'est pas disponible pour le chemin de routage qui offre le coût le plus faible, Exchange détermine un autre chemin présentant les mêmes avantages au niveau du coût et de la disponibilité du connecteur. Entre les groupes de routage, les informations sur l'état des liaisons sont communiquées de manière dynamique à l'aide du verbe SMTP étendu, X-LINK2STATE.

Utilisation des informations sur l'état des liaisons pour la remise des messages internes

Pour comprendre le fonctionnement des informations sur l'état des liaisons et des coûts des connecteurs, observez la topologie de routage présentée à la figure 1.1 qui comporte quatre groupes de routage : Seattle, Bruxelles, Londres et Tokyo. Les connecteurs existent entre chaque groupe de routage et sont affectés à des coûts basés sur la vitesse du réseau et la bande passante disponible.

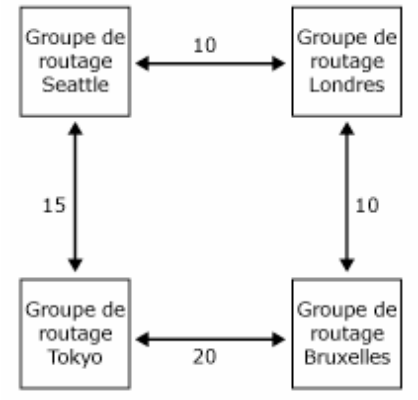


Figure 1.1 Topologie et coûts de routage

Si toutes les connexions entre les groupes de routage sont disponibles, un serveur du groupe de routage Seattle envoie toujours un message au groupe de routage Bruxelles en transmettant d'abord le message par l'intermédiaire du groupe de routage Londres. Le coût de ce chemin de routage est de 20, ce qui représente le coût le plus faible. Toutefois, si le serveur tête de pont à Londres n'est pas disponible, les messages provenant de Seattle et destinés à Bruxelles sont acheminés par l'intermédiaire du groupe de routage Tokyo dont le coût est supérieur à 35.

Il est important de comprendre que pour qu'un connecteur soit marqué comme non disponible, tous les serveurs têtes de pont de ce connecteur doivent être arrêtés. Si vous avez configuré votre connecteur de groupe de routage pour qu'il utilise l'option par défaut de **Tous les serveurs locaux peuvent envoyer des messages via ce conn.**, le connecteur de groupe de routage est toujours considéré en service. Pour plus d'informations sur la configuration des connecteurs de groupes de routage, consultez le chapitre 5 « Connexion de groupes de routage ».

Utilisation des informations sur l'état des liaisons pour la remise des messages externes

Pour une remise des messages externes, le routage utilise les informations dans la table d'état des liaisons pour évaluer le connecteur dont l'espace d'adressage correspond le plus possible à la destination, puis le routage évalue le coût. La figure 1.2 illustre une entreprise dont la topologie est la suivante :

- Un connecteur SMTP avec un espace d'adressage *.net et un coût de 20.
- Un connecteur SMTP avec un espace d'adressage * comprenant toutes les adresses externes et un coût de 10.

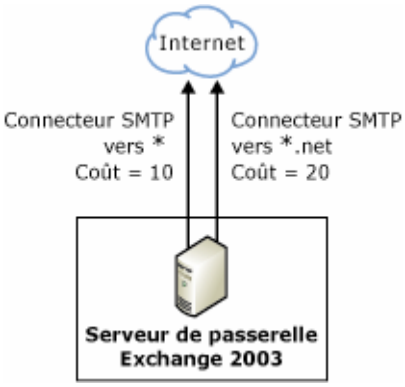


Figure 1.2 Utilisation de l'espace d'adressage pour le routage des messages par Exchange

Dans la topologie présentée à la figure 1.2, lorsque le courrier est envoyé à un utilisateur externe avec l'adresse de messagerie pierre@treyresearch.net, le routage commence par rechercher un connecteur dont l'espace d'adressage correspond le mieux à la destination de treyresearch.net. Le connecteur SMTP avec l'espace d'adressage *.net correspond le mieux à la destination, le routage utilise donc ce connecteur quel que soit le coût.

Cependant, si du courrier est adressé à un utilisateur externe avec une adresse bernard@contoso.com, le routage utilise le connecteur SMTP avec l'espace d'adressage * car il s'agit de la correspondance la plus proche. Le routage n'évalue pas le coût. Si deux connecteurs SMTP existant possèdent un espace d'adressage * mais des coûts différents, le routage utilise les informations dans la table d'état des liaisons et sélectionne le connecteur SMTP le moins onéreux. Le routage utilise le connecteur le plus onéreux uniquement si le connecteur moins onéreux n'est pas disponible.

> **Remarque** Pour plus d'informations sur les informations de liaison et leur propagation, consultez le chapitre 15, « Concepts avancés sur l'état des liaisons ».

Le routage ne bascule pas d'un connecteur avec un espace d'adressage spécifique vers un connecteur avec un espace d'adressage moins spécifique. Dans le scénario ci-dessus, si tous les utilisateurs peuvent utiliser les deux connecteurs et qu'un utilisateur tente d'envoyer du courrier à un utilisateur à treyresearch.net, le routage considère le connecteur avec l'espace d'adressage .net comme sa destination. Si ce connecteur n'est pas en service ou n'est pas disponible, le routage ne tente pas de trouver un connecteur avec un espace d'adressage différent, moins restreint tel que * car il considère cet espace d'adressage comme une destination différente.

Cependant, dans cette même topologie, tenez compte du fait que des restrictions existent sur le connecteur avec l'espace d'adressage *.net et que celles-ci ne permettent qu'aux utilisateurs du service commercial d'envoyer du courrier par l'intermédiaire de ce connecteur. Dans ce cas, si ce connecteur n'est pas en service, le routage ne redirige pas le courrier envoyé par un utilisateur du service commercial et destiné à une adresse .net par l'intermédiaire du connecteur avec l'adresse *. Le courrier est mis en file d'attente jusqu'à ce que l'adresse *.net soit disponible. Cependant, les utilisateurs en dehors du service commercial ne sont jamais affectés lorsque ce

connecteur n'est plus disponible car leurs messages sont toujours routés par l'intermédiaire du connecteur SMTP avec l'espace d'adressage *.

Utilisation des groupes de routage en mode natif et en mode mixte

Dans Exchange 2003 et Exchange 2000, les fonctions d'administration et de routage sont divisées en différentes unités :

- Les groupes d'administration définissent la limite administrative logique des serveurs Exchange.
- Les groupes de routage définissent les chemins de routage physiques empruntés par les messages sur le réseau.

Si votre organisation Exchange fonctionne en mode natif, tous les serveurs exécutent Exchange 2000 ou toute version ultérieure, cette division entre les groupes d'administration et les groupes de routage vous permet de créer des groupes de routage qui s'étendent aux groupes d'administration et de déplacer les serveurs entre les groupes de routage qui existent dans différents groupes d'administration. Cette fonctionnalité vous permet également de séparer les fonctions de routage et d'administration. Par exemple, vous pouvez administrer des serveurs dans deux groupes d'administration centraux, en plaçant les serveurs de chaque groupe d'administration dans des groupes de routage différents, basés sur la topologie de votre réseau et les besoins des utilisateurs.

Toutefois, les fonctionnalités des groupes de routage dans un environnement en mode mixte, où certains serveurs exécutent Exchange 2003 ou Exchange 2000 tandis que d'autres utilisent Exchange 5.5, sont différentes du mode natif. En mode mixte :

- Un groupe de routage ne peut pas s'étendre à plusieurs groupes d'administration.
- Vous ne pouvez pas déplacer des serveurs entre les groupes de routage qui existent dans les différents groupes d'administration.

Cette situation tient au fait que la topologie de routage dans Exchange 5.5 est définie par site, sous la forme de combinaisons logiques de serveurs connectés par l'intermédiaire d'un réseau fiable à bande passante élevée. Les sites assurent les fonctionnalités du groupe d'administration et du groupe de routage dans Exchange 2003 et Exchange 2000. Cette différence dans la topologie de routage limite les fonctionnalités des groupes de routage dans un environnement en mode mixte.

Présentation du protocole SMTP

Avant de configurer l'envoi et la réception des messages dans votre organisation Exchange, vous devez vous sensibiliser sur la manière dont le protocole SMTP permet le flux des messages dans Microsoft® Exchange Server 2003. Exchange Server 2003 utilise ce protocole pour remettre les messages internes entre des serveurs Exchange et des groupes de routage. De manière similaire, Exchange 2003 utilise le protocole SMTP pour la remise des messages Internet en dehors de l'organisation Exchange. Ce chapitre fournit une description détaillée du protocole SMTP ainsi que de son fonctionnement dans Exchange 2003 et explique le processus d'envoi et de réception des messages Internet.

Procédures du chapitre 2

Le tableau 2.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 2.1 Procédures du chapitre 2 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Restreindre les dépôts sur un serveur SMTP en fonction d'un groupe de sécurité	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Restreindre les relais en fonction d'un groupe de sécurité	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Description du service SMTP et d'Exchange

Le service SMTP est la norme Internet pour le transport et la remise de messages électroniques. Basée sur les spécifications des RFC (*Request For Comments*) 2821 et RFC 2822, le service SMTP de Microsoft est inclus dans le système d'exploitation Microsoft Windows® 2000 Server et Windows Server™ 2003.

Le service SMTP de Windows est un composant des services IIS (Internet Information Services) et s'exécute dans le cadre du programme Inetinfo.exe. Exchange 2003 utilise le service SMTP de Windows comme protocole de transport natif ; par conséquent Exchange utilise SMTP pour le routage de l'ensemble des messages internes et externes.

Une fois Exchange installé, il étend les fonctionnalités SMTP sous-jacentes de la manière suivante :

- En déplaçant la gestion du service SMTP (à l'aide de serveurs virtuels SMTP) de la console d'administration IIS vers le Gestionnaire système Exchange.
- En mettant en œuvre la prise en charge des informations de l'état des liaisons. À l'aide des informations de l'état des liaisons, Exchange détermine la meilleure méthode d'envoi des messages entre les serveurs, en fonction de l'état actuel de la connectivité et du coût de la messagerie ainsi que des coûts correspondants de routage définis à partir de votre topologie.

- En étendant SMTP pour qu'il prenne en charge les verbes de commande utilisés dans la prise en charge du routage de l'état des liaisons et d'autres fonctionnalités Exchange. Les commandes suivantes sont ajoutées à l'installation d'Exchange :
  - X-EXPS GSSAPI
  - X-EXPS=LOGIN
  - X-EXCH50
  - X-LINK2STATE

    Remarque Pour obtenir une liste contenant toutes les commandes SMTP et leurs définitions, consultez la section « Commandes SMTP » dans l'annexe A.
- En configurant un lecteur de banque d'informations IFS (Installable File System) Exchange pour permettre la remise des messages vers la banque Exchange et leur récupération.
- En définissant l'emplacement disque \exchsrv\mailroot\vs 1\queue où les messages sont mis en file d'attente. Il s'agit de l'emplacement du premier serveur virtuel SMTP sur le serveur Exchange. Si vous ajoutez un deuxième serveur virtuel SMTP, Exchange crée un emplacement supplémentaire (\exchsrv\mailroot\vs 2\queue).
- En mettant en œuvre la prise en charge des files d'attente avancées. Exchange améliore les fonctionnalités de mise en file d'attente de Windows 2000 et Windows Server 2003. Le moteur de files d'attente avancé traite les fonctions de transport sous-jacentes dans Exchange.
- En améliorant la catégorisation des messages. La catégorisation des messages est un processus effectué par le catégoriseur de messages, un composant du moteur de files d'attente avancé. Le catégoriseur envoie des requêtes LDAP (Lightweight Directory Access Protocol) au serveur de catalogue global pour récupérer des informations de configuration et utilisateur stockées dans le service d'annuaire Microsoft Active Directory®. Le catégoriseur de messages récupère des informations de stratégie de destinataire et des informations de serveur virtuel Exchange pour activer la remise des messages. Il utilise ces informations pour valider l'adresse des destinataires, pour vérifier que les limites des messages ne sont pas dépassées et pour déterminer le mode de livraison finale du message à l'aide de SMTP et du routage Exchange. Pour plus d'informations sur le catégoriseur et les autres composants de transport interne, consultez le chapitre 14, « Présentation des composants de transport internes ».

Dans le cadre de SMTP et Exchange 2000 et des versions ultérieures, il est important de comprendre le concept d'interaction entre Exchange, Active Directory et la métabase IIS. Grâce au Gestionnaire système Exchange, toutes les modifications de configuration apportées (par exemple à vos stratégies de destinataire et à vos serveurs virtuels SMTP) sont inscrites dans Active Directory, ce qui permet une administration simple et à distance. Toutefois, comme le service SMTP lit ses paramètres depuis la métabase IIS, le service DS2MB, un composant du système de Surveillance Exchange, réplique ces informations depuis Active Directory dans la métabase IIS du serveur local.

Réception de messages Internet

Si les conditions suivantes existent, Exchange 2003 est en mesure de recevoir des messages Internet dans sa configuration par défaut :

- Vous disposez d'une connexion constante à Internet.

  Remarque Les connexions d'accès à distance à Internet nécessitent une configuration particulière. Pour plus d'informations sur les connexions d'accès à distance, consultez la section « Définition d'un calendrier de connecteur pour la connexion à un fournisseur de services réseau » au chapitre 7.
- Les serveurs DNS (Domain Name System) externes de votre domaine doivent avoir les enregistrements de ressource de serveur de messagerie (MX) qui pointent vers vos serveurs de messagerie ou, si vous utilisez

un fournisseur d'accès Internet ou un système externe, ce système externe doit avoir un enregistrement MX pour votre domaine et un mécanisme de transfert des messages vers vos serveurs Exchange. Pour plus d'informations sur la vérification de vos enregistrements MX, consultez la section « Configuration du service DNS pour la remise de messages Internet » au chapitre 4.

- Votre serveur de messagerie doit être accessible aux autres serveurs sur Internet. Pour plus d'informations sur la vérification de l'accessibilité de votre serveur de messagerie à Internet, consultez la section « Utilisation de Telnet pour garantir l'accessibilité à Internet » au chapitre 4. Si vous utilisez un fournisseur d'accès Internet ou un système externe pour recevoir votre courrier, ce système externe doit pouvoir contacter vos serveurs Exchange pour la remise de vos messages.
- Vos stratégies de destinataire doivent être configurées correctement. Pour recevoir des messages Internet, vous devez configurer une stratégie de destinataire qui contient un espace d'adressage correspondant au domaine SMTP. Également, votre organisation Exchange doit être responsable de la remise des messages vers cette adresse (paramètre par défaut) Par exemple, pour accepter des messages Internet pour pierre@example.com, vous devez disposer d'une stratégie de destinataire qui contient @example.com. Cependant, il existe des exceptions à cette règle. Par exemple, vous pouvez créer un connecteur qui autorise le relais des messages vers un domaine spécifié. Pour plus d'informations sur la configuration de vos stratégies de destinataire, consultez la section « Configuration des stratégies de destinataire » au chapitre 7.

Les messages Internet entrants circulent par l'intermédiaire d'un serveur Exchange de la manière suivante :

1. Le serveur SMTP d'envoi interroge le serveur DNS pour localiser l'adresse IP du serveur de messagerie SMTP du destinataire.
2. Le serveur SMTP d'envoi démarre ensuite une conversation sur le serveur SMTP du destinataire (sur le port 25). Sur une passerelle Exchange, le serveur SMTP du destinataire correspond au serveur virtuel SMTP configuré pour accepter les messages Internet entrants.
3. Dans le meilleur des cas, le serveur SMTP entrant accepte uniquement le message entrant si celui-ci est destiné à un destinataire de son domaine de messagerie SMTP. Ces destinataires sont définis dans les stratégies de destinataire (sauf si le serveur est ouvert au relais, ce qui est fortement déconseillé).

   Remarque Si vous laissez votre système ouvert pour un relais, des utilisateurs non autorisés peuvent utiliser vos serveurs pour envoyer des messages à des adresses externes. Votre système peut se retrouver sur une liste d'interdiction — processus qui bloque les messages en provenance de serveurs soupçonnés d'envoyer du courrier commercial non sollicité (courrier indésirable). Pour plus d'informations sur les relais, consultez la section « Restrictions de relais », plus loin dans ce chapitre. Pour plus d'informations sur la vérification de vos restrictions de relais, consultez la section « Vérification des restrictions de relais par défaut sur votre serveur virtuel SMTP entrant » au chapitre 7.
4. Une fois le message accepté, le serveur virtuel SMTP utilise les mécanismes de transport dans Exchange pour déterminer la méthode de remise du message. Exchange localise le destinataire dans Active Directory et détermine quel serveur de l'organisation Exchange va remettre le message.
5. Enfin, le serveur virtuel SMTP utilise ses mécanismes de transport interne pour remettre le message au serveur Exchange approprié.

   Pour plus d'informations sur les mécanismes de transport interne, consultez le chapitre 14 « Présentation des composants de transport internes ».

Envoi de messages Internet

Dans le cas d'une connexion constante à Internet, Exchange envoie des messages Internet grâce aux méthodes suivantes :

- Utilise le service DNS directement pour contacter le serveur de messagerie distant.
- Route les messages par l'intermédiaire d'un hôte actif chargé de la résolution de noms DNS et de la remise des messages.

Avant la description approfondie de chacune de ces méthodes, vous devez posséder une connaissance générale du fonctionnement du flux des messages sortants dans une organisation Exchange.

Les messages Internet sortants circulent par l'intermédiaire d'un serveur Exchange 2003 de la manière suivante :

1. Un utilisateur interne envoie un message à un destinataire dans un domaine distant.
2. Pour déterminer si le destinataire est local ou distant, le serveur virtuel SMTP sur le serveur Exchange de l'expéditeur utilise des fonctions de transport interne pour interroger le serveur de catalogue global afin d'obtenir l'adresse du destinataire. Si l'adresse du destinataire sur le message ne figure pas dans une stratégie de destinataire, celle-ci n'est pas stockée dans Active Directory ; par conséquent, Exchange détermine que le message est destiné à un domaine distant.
3. Si nécessaire, le serveur Exchange remet le message au serveur virtuel SMTP approprié.
4. Le serveur virtuel SMTP utilise ses informations de métabase IIS pour déterminer la méthode de remise d'un message à un domaine distant.
5. Le serveur virtuel SMTP sur le serveur Exchange effectue ensuite l'une des deux actions suivantes :
   - Utilise le serveur DNS pour vérifier l'adresse IP du domaine cible, puis tente de livrer le message.
   - Transmet le message à un hôte actif chargé de la résolution DNS et de la remise du message.

   Pour plus d'informations sur les mécanismes de transport interne, consultez le chapitre 14 « Présentation des composants de transport internes ».

Éléments SMTP

Cette section décrit les composants essentiels du service SMTP. Ces composants sont les suivants :

Serveurs virtuels SMTP

Les serveurs virtuels SMTP fournissent les mécanismes Exchange permettant de gérer SMTP. Chaque serveur virtuel SMTP représente une instance du service SMTP qui s'exécute sur le serveur Exchange. À l'aide du Gestionnaire système Exchange, vous pouvez configurer les serveurs virtuels SMTP chargés de contrôler le comportement de SMTP.

Connecteurs SMTP

Un connecteur SMTP sert à désigner un chemin de routage isolé pour les messages. Vous pouvez utiliser les connecteurs SMTP pour établir une passerelle pour les messages Internet ou un hôte actif, ou pour connecter les groupes de routage en interne. Les connecteurs vous permettent de définir des options spécifiques pour le chemin de routage des messages défini.

Serveur virtuel SMTP

Un serveur virtuel SMTP est essentiellement une pile de protocole SMTP, c'est à dire un processus ou un serveur qui reçoit des messages électroniques et fonctionne en tant que client pour l'envoi de ces messages. Chaque serveur virtuel SMTP représente une instance du service SMTP sur un serveur. Un serveur virtuel SMTP est défini par une combinaison unique composée d'une adresse IP et d'un numéro de port. Le serveur virtuel SMTP par défaut utilise toutes les adresses IP disponibles sur le serveur et utilise le port 25 pour les connexions entrantes. Un serveur physique unique peut héberger un grand nombre de serveurs virtuels.

Le Gestionnaire système Exchange vous permet de contrôler la plupart des paramètres SMTP. Les paramètres de propriété du serveur virtuel SMTP contrôlent les messages entrants et, à un niveau inférieur, les paramètres des messages sortants.

> **Important** Comme un serveur virtuel SMTP joue un rôle critique dans la remise des messages, modifiez avec prudence les paramètres de ses propriétés. Par exemple, le serveur virtuel SMTP par défaut envoie des messages au sein d'un groupe de routage. De plus, si le serveur est un contrôleur de domaine, Active Directory utilise ce serveur virtuel pour la réplication d'annuaire SMTP. Ainsi, au lieu de modifier le serveur virtuel SMTP par défaut, il est recommandé soit de créer un serveur virtuel SMTP supplémentaire, soit de créer un connecteur SMTP pour annuler les paramètres par défaut du serveur virtuel.

Erreurs à propos de serveurs virtuels SMTP multiples

Un malentendu courant est de croire que la création de plusieurs serveurs virtuels SMTP sur un serveur Exchange unique augmente le débit. Il est important de comprendre que chaque serveur virtuel SMTP est multithread. La création de serveurs virtuels SMTP supplémentaires sur un serveur Exchange unique n'accroît pas les performances et complique votre organisation Exchange. Un exemple de cas où plusieurs serveurs virtuels SMTP sont nécessaires est une configuration de serveur à double hébergement. Dans la plupart des autres scénarios, l'utilisation d'un serveur virtuel SMTP par défaut avec ses paramètres par défaut est généralement suffisante.

> **Remarque** Pour plus d'informations sur la configuration d'un serveur à double hébergement, consultez la section « Utilisation d'un serveur Exchange à double hébergement comme passerelle Internet » au chapitre 6.

Paramètres des messages entrants sur le serveur virtuel SMTP

Vous pouvez utiliser les paramètres de propriété du serveur virtuel pour configurer les paramètres des messages entrants suivants :

Ports entrants et adresses IP

Le serveur virtuel SMTP écoute sur l'adresse IP qui lui est assignée les communications entrantes et accepte les connexions entrantes sur le port qui lui est assigné. Pour configurer ces paramètres, utilisez l'onglet **Général** des propriétés du serveur virtuel SMTP.

> **Important** Le service SMTP définit le port 25 comme son port standard. Ne changez pas ce paramètre.

> **Remarque** Une fois installé dans sa configuration initiale, le serveur virtuel par défaut se connecte au serveur SMTP distant sur le port 25 pour envoyer des messages sortants. Ce paramètre est différent du paramètre de port entrant. Pour configurer ce paramètre, utilisez le bouton **Connexions sortantes** sous l'onglet **Remise**.

Restrictions de relais

Pour empêcher les utilisateurs non autorisés d'utiliser votre serveur pour envoyer des messages à des adresses externes, utilisez le bouton **Relais** sous l'onglet **Accès**. Par défaut, le serveur virtuel SMTP par défaut relaie les messages uniquement pour les utilisateurs authentifiés. Pour plus d'informations sur les restrictions de relais, consultez la section « Restrictions de relais », plus loin dans ce chapitre.

Limiter les envois et les autorisations de relais à des utilisateurs et à des groupes spécifiques

Dans Exchange 2003, vous pouvez limiter les expéditeurs de messages vers un serveur virtuel SMTP à l'aide des boutons **Relais** et **Authentification** sous l'onglet **Accès**. Pour plus d'informations sur les limites

s'appliquant aux expéditeurs de messages vers un serveur virtuel SMTP, consultez la section « Restriction des autorisations de dépôt et de relais pour un serveur virtuel SMTP interne » au chapitre 9.

Sécurité
Vous pouvez exiger le service TLS (Transport Layer Security), une implémentation de SSL (Secure Sockets Layer), sur les connexions entrantes.

Vous pouvez également configurer d'autres paramètres tels que les restrictions de connexions entrantes, le paramétrage des performances et le traitement des notifications de rapports de remise.

Restrictions de relais

Le relais des messages permet de transférer des messages vers les domaines différents du vôtre. En particulier, le relais des messages a lieu lorsqu'une connexion entrante vers votre serveur SMTP est utilisée pour envoyer des messages électroniques à des domaines externes. Par défaut, votre serveur Exchange accepte les messages envoyés par des utilisateurs authentifiés ou internes et les envoie vers un domaine externe. Si votre serveur est ouvert pour le relais des messages ou si le relais n'est pas sécurisé, des utilisateurs non autorisés peuvent utiliser votre serveur pour envoyer du courrier commercial non sollicité (courrier indésirable). Par conséquent, pour sécuriser votre serveur virtuel SMTP, il est essentiel de définir des restrictions de relais.

Il est important de comprendre la différence entre le relais authentifié et le relais ouvert ou anonyme :

Relais authentifié
Le relais authentifié permet à vos utilisateurs internes d'envoyer des messages aux domaines situés à l'extérieur de votre organisation Exchange. En revanche, il nécessite une authentification avant l'envoi des messages. Par défaut, Exchange autorise uniquement le relais authentifié.

Relais anonyme
Le relais anonyme permet à n'importe quel utilisateur de se connecter à votre serveur Exchange et de l'utiliser pour envoyer du courrier à l'extérieur de votre organisation Exchange.

Les exemples suivants illustrent la manière dont Exchange 2003 accepte et relaie le courrier en utilisant les relais authentifiés :

- Un utilisateur anonyme se connecte au serveur virtuel SMTP et tente de remettre du courrier à un utilisateur interne dans l'organisation Exchange.

  Dans ce cas, le serveur virtuel SMTP accepte le message parce qu'il est destiné à un domaine interne et que l'utilisateur existe dans Active Directory.

- Un utilisateur anonyme se connecte au serveur virtuel SMTP et cherche à remettre du courrier à un utilisateur externe dans un domaine externe.

  Dans ce cas, le serveur virtuel SMTP rejette le message car il est destiné à un domaine externe dont le serveur Exchange n'est pas responsable. Comme l'utilisateur n'est pas authentifié, le serveur virtuel SMTP ne relaie pas ce message en dehors de l'organisation Exchange.

- Un utilisateur se connecte au serveur virtuel SMTP à l'aide du protocole POP (Post Office Protocol) ou du client IMAP (Internet Message Access Protocol), par exemple Microsoft Outlook® Express, puis tente d'envoyer un message à un utilisateur d'un domaine externe.

  Dans ce cas, le client de messagerie se connecte directement au serveur virtuel SMTP et authentifie l'utilisateur. Même si le message est destiné à un domaine distant, le serveur virtuel SMTP accepte et relaie ce message car l'utilisateur est authentifié.

Grâce aux fonctionnalités de contrôle de relais d'Exchange 2003, vous pouvez empêcher des tiers de relayer des messages par l'intermédiaire de votre serveur. Le contrôle de relais vous permet de spécifier une liste d'adresses IP et des paires de masques de sous-réseau distantes entrantes qui sont autorisées à relayer les messages par l'intermédiaire de votre serveur. Exchange vérifie l'adresse IP d'un client SMTP entrant par rapport à la liste de réseaux IP qui sont autorisés à relayer des messages. Si le client n'est pas autorisé à relayer

de messages, seuls les messages adressés aux destinataires locaux sont autorisés. Vous pouvez également mettre en œuvre le contrôle de relais par domaine — Cependant, cette approche nécessite la mise en œuvre d'une résolution DNS inversée qui est contrôlée au niveau du serveur virtuel SMTP.

Restrictions de relais par défaut

Par défaut, le serveur virtuel SMTP autorise le relais des messages uniquement en provenance d'utilisateurs authentifiés. Cette configuration est conçue pour empêcher des utilisateurs non autorisés d'utiliser votre serveur Exchange pour relayer des messages. Comme l'illustre la figure 2.1, la configuration par défaut du serveur virtuel autorise uniquement des ordinateurs authentifiés à relayer des messages.

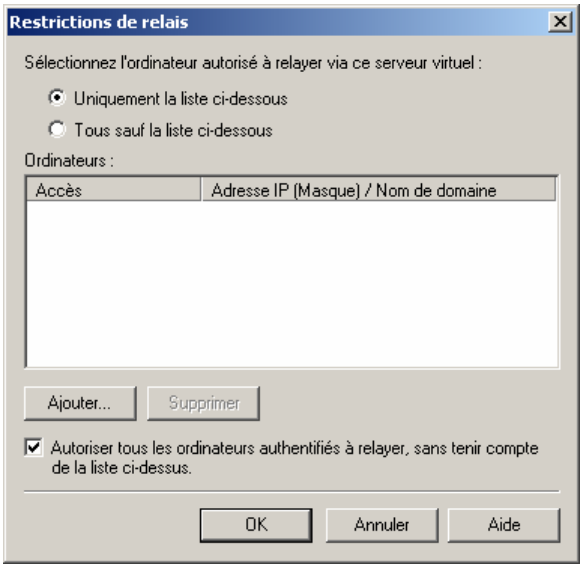


Figure 2.1 Restrictions de relais par défaut

Les messages électroniques commerciaux non sollicités proviennent généralement d'une adresse usurpée ou falsifiée et sont souvent relayés par un serveur non sécurisé pour le relais. C'est pour cette raison qu'Exchange 2003, par défaut, autorise uniquement les utilisateurs authentifiés à relayer des messages. Modifiez ce paramètre avec prudence — de nombreux fournisseurs d'accès Internet bloquent les serveurs qui autorisent le relais ouvert.

Paramètres des messages sortants sur le serveur virtuel SMTP

Si vous souhaitez que votre serveur virtuel SMTP envoie des messages directement vers Internet, vous pouvez configurer les paramètres de messages sortants. Plus particulièrement, vous pouvez configurer votre serveur virtuel pour qu'il utilise un serveur DNS externe pour la résolution d'adresses externes et l'envoi de courrier directement aux serveurs de messagerie situés en dehors de votre organisation.

> **Important** Comme un serveur virtuel SMTP joue un rôle critique dans la remise des messages, modifiez avec prudence les paramètres de ses propriétés. Par exemple, le serveur virtuel SMTP par défaut envoie des messages au sein d'un groupe de routage. De plus, si le serveur est un contrôleur de domaine, Active Directory utilise ce serveur virtuel pour la réplication d'annuaire SMTP. Ainsi, au lieu de modifier le serveur virtuel SMTP par défaut, il est recommandé soit de créer un serveur virtuel SMTP supplémentaire, soit de créer un connecteur SMTP pour annuler les paramètres par défaut du serveur virtuel.

Dans de nombreux cas, il est préférable (sans que cela soit nécessaire) de configurer un connecteur SMTP pour qu'il traite les messages sortants. Pour plus d'informations sur les connecteurs SMTP, consultez la section « Connecteurs SMTP », plus loin dans ce chapitre.

> **Remarque** Si vous utilisez un connecteur SMTP, celui-ci ignore certains paramètres et contrôles des messages sortants pour la remise des messages sortants.

Pour contrôler la remise des messages sortants sur votre serveur virtuel, vous pouvez configurer les paramètres suivants :

- Port sortant
- Restrictions sortantes
- Options de remise de messages sortants
- Sécurité sortante
- Paramétrage des performances
- Notification des rapports de remise

Pour plus d'informations sur la configuration de ces paramètres, consultez la section « Configuration des paramètres des messages sortants sur les serveurs virtuels SMTP » au chapitre 7.

Connecteurs SMTP

Les connecteurs SMTP permettent principalement la connexion à d'autres systèmes de messageries ou la définition d'options supplémentaires pour une passerelle Internet SMTP. Les connecteurs SMTP peuvent également servir à connecter un groupe de routage à un autre groupe de routage en interne. Toutefois, cette utilisation n'est pas recommandée. Les connecteurs SMTP vous permettent essentiellement de désigner un chemin de routage isolé pour permettre aux messages de circuler vers un domaine spécifique ou sur Internet.

L'avantage d'utiliser un connecteur SMTP est de pouvoir spécifier des paramètres de configuration supplémentaires pour modifier la remise des messages. Ces paramètres sont les suivants :

Remise de messages sortants

Lorsque vous configurez un connecteur, vous pouvez router les messages des deux façons suivantes :

- Utilisez le DNS pour router tous les messages sortants par l'intermédiaire du connecteur. Si vous utilisez le DNS pour router les messages sortants, le connecteur SMTP utilise le DNS pour résoudre l'adresse IP du serveur SMTP distant, puis il remet les messages.
- Spécifiez un hôte actif (un autre serveur vers lequel le connecteur route l'ensemble des messages). L'hôte actif est chargé de la résolution DNS et de la remise des messages.

Serveurs têtes de pont locaux

Un serveur virtuel SMTP héberge un connecteur. Lorsque vous créez un connecteur, désignez au moins un serveur Exchange et un serveur virtuel SMTP en tant que serveurs têtes de pont. Le connecteur hérite des restrictions de taille et des autres paramètres du serveur virtuel SMTP ; cependant, vous pouvez remplacer ces paramètres sur le connecteur. Vous pouvez également désigner plusieurs serveurs têtes de pont pour équilibrer la charge, les performances et la redondance.

Espace d'adressage

L'espace d'adressage définit les adresses ou les domaines de messagerie pour les messages électroniques que vous souhaitez router par l'intermédiaire d'un connecteur. Par exemple, l'espace d'adressage * (astérisque) englobe tous les domaines externes — ce connecteur est utilisé pour router tous les messages électroniques externes. Si vous avez créé un deuxième connecteur avec un espace d'adressage *.net, Exchange route tous les messages destinés au domaine qui comporte l'extension .net par l'intermédiaire du second connecteur. Cette action se produit car Exchange sélectionne le connecteur dont l'espace

d'adressage est le plus proche. Vous pouvez configurer ce paramètre sous l'onglet **Adresse** des propriétés du connecteur SMTP.

Portée

Vous pouvez sélectionner une organisation entière ou un groupe de routage pour la portée du connecteur. Vous pouvez également définir la portée sous l'onglet **Adresse** des propriétés du connecteur SMTP.

Restrictions de remise

Vous pouvez restreindre les types d'expéditeur habilités à envoyer des messages par l'intermédiaire d'un connecteur. Par défaut, les messages de tous les utilisateurs sont acceptés. Vous pouvez configurer ces paramètres sous l'onglet **Remise** des propriétés du connecteur SMTP.

> **Remarque** Par défaut, vous ne pouvez par restreindre les messages sauf si vous changez les paramètres de la clé de Registre. Si vous avez choisi d'activer la restriction de remise, sachez que cette opération nécessite beaucoup de ressources processeur et peut avoir une incidence négative sur les performances du serveur. Pour plus d'informations sur la manière d'activer les restrictions de remise, consultez la section « Définition de restrictions de remise » au chapitre 7.

Restrictions sur le contenu

Vous pouvez spécifier les types de messages remis par l'intermédiaire d'un connecteur. Vous pouvez configurer ces paramètres sous l'onglet **Restriction sur le contenu** des propriétés du connecteur SMTP.

Options de remise

Si vous vous connectez à un fournisseur de services réseau pour récupérer vos messages, vous pouvez configurer l'exécution du connecteur selon un calendrier défini et mettre en œuvre les fonctionnalités de file d'attente et de retrait avancées. Vous pouvez configurer ces paramètres sous l'onglet **Options de remise** des propriétés du connecteur SMTP.

Communication SMTP

Vous pouvez contrôler la manière dont le connecteur utilise SMTP pour communiquer avec les autres serveurs SMTP. Vous pouvez en particulier spécifier si le connecteur utilise les commandes SMTP ou ESMTP (Extended Simple Mail Transfer Protocol) pour initialiser une conversation avec un autre serveur et contrôler l'utilisation des commandes ERTN et TURN (ces commandes sont utilisées pour demander à un autre serveur SMTP d'envoyer les messages qu'il possède). Vous pouvez configurer ces paramètres sous l'onglet **Paramètres avancés** des propriétés du connecteur SMTP.

Sécurité sortante

Vous pouvez également vérifier que les messages transmis par l'intermédiaire du connecteur sont authentifiés. Ce paramètre permet d'établir un chemin de routage sécurisé pour communiquer avec une société partenaire. Il vous permet de définir une méthode d'authentification et de requérir le cryptage TLS (Transport Layer Security). Vous pouvez configurer ces paramètres à l'aide du bouton **Sécurité sortante** sous l'onglet **Paramètres avancés** des propriétés du connecteur SMTP.

Fonction d'un connecteur SMTP

Le service SMTP s'appuie sur le DNS pour déterminer l'adresse IP de son serveur de destination suivant. Pour envoyer des messages directement à un serveur de messagerie externe, un connecteur SMTP doit faire appel au serveur DNS pour la résolution des noms de domaine externes. Le connecteur peut également se contenter de transmettre les messages vers un hôte actif chargé de la remise et de la résolution de noms DNS. Pour plus d'informations sur la dépendance du service SMTP par rapport au service DNS, consultez la section « DNS » au chapitre 3.

Après avoir configuré un connecteur SMTP, tant que l'adresse de destination correspond à l'espace d'adressage configuré sur le connecteur SMTP, les serveurs ne routent plus les messages directement ; en fait, les serveurs routent les messages par l'intermédiaire du connecteur SMTP. (Ces serveurs s'appellent soit des serveurs de passerelle, soit des serveurs têtes de pont.)

Pour illustrer cette notion, supposez que vous voulez router tous les messages externes par l'intermédiaire d'un connecteur vers un serveur tête de pont (le seul serveur qui communique avec Internet). Pour ce faire, créez un connecteur sur le serveur tête de pont avec un espace d'adressage * (astérisque) qui spécifie tous les domaines externes. Lors de l'envoi de messages à un domaine externe, Exchange route automatiquement ces messages vers ce connecteur, ce qui évite à un serveur virtuel SMTP d'envoyer les messages externes directement. Si vous disposez de plusieurs connecteurs, Exchange tente d'abord de router les messages par l'intermédiaire du connecteur dont l'espace d'adressage est le plus proche (espace d'adressage le plus restrictif).

> **Remarque** Dans un environnement en mode mixte, si vous disposez d'un connecteur IMC (Internet Mail Connector) d'Exchange Server version 5.5, Exchange 2003 considère ce connecteur comme le chemin de routage valide. Si vous rencontrez des difficultés lors de l'envoi ou de la réception de messages Internet, vérifiez les files d'attente MTA du serveur Exchange Server 5.5 et les files d'attente X.400 du serveur Exchange 2003. Exchange 2003 utilise le service MTA pour communiquer avec les versions héritées d'Exchange.

Fonctions d'un connecteur SMTP

Grâce aux fonctionnalités de serveur virtuel d'Exchange 2003, il n'est pas nécessaire de créer un connecteur SMTP pour permettre le flux des messages, pour connecter celui-ci à d'autres serveurs dans une organisation Exchange ou pour le connecter à Internet. De plus, vous n'avez pas besoin d'un connecteur si tous vos serveurs Exchange 2003 se connectent à Internet et effectuent correctement des recherches DNS des adresses Internet.

Toutefois, bien qu'il ne soit pas essentiel pour la remise de messages Internet, les avantages offerts par l'utilisation d'un connecteur SMTP sont les suivants :

- simplifie l'administration ;
- réduit l'exposition à Internet ;
- établit un routage isolé pour la communication avec un autre domaine ou un autre système de messagerie ;
- route les messages vers un autre système de messagerie ou relaie les messages vers un autre domaine ;
- autorise plusieurs serveurs têtes de pont pour l'équilibre de la charge ;
- vous permet de contrôler l'utilisation de SMTP pour communiquer avec d'autres serveurs ;
- autorise les heures de connexion planifiées avec des paramètres personnalisés.

Les sections suivantes fournissent des informations détaillées sur chacun de ces avantages. Pour plus d'informations sur les connecteurs SMTP, consultez l'article 294736 (en anglais) de la Base de connaissances Microsoft, « When to Create SMTP Connectors in Exchange 2000 and Later » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=294736).

Simplifier l'administration du flux des messages

Un connecteur SMTP permet un contrôle administratif accru du trafic Internet sortant de votre organisation. Vous pouvez faire appel à un connecteur SMTP ou à un ensemble de connecteurs pour limiter les chemins de routage disponibles pour les messages Internet sortants. Également, comme vous ne vérifiez que les files d'attente SMTP et les autres configurations sur un serveur unique, l'utilisation d'un serveur unique comme serveur tête de pont simplifie la résolution des problèmes.

Limiter l'exposition à Internet

L'un des avantages offerts par la création d'un connecteur SMTP est de vous permettre le routage de l'ensemble des messages SMTP externes sortants ou entrants par l'intermédiaire d'un serveur ou un ensemble de serveurs têtes de pont particulier. En désignant un routage isolé pour les messages Internet qui utilisent un connecteur, vous limitez l'exposition de votre organisation Exchange à Internet.

Pour utiliser un connecteur SMTP pour router les messages Internet, définissez un serveur ou un ensemble de serveurs comme votre passerelle Internet, créez un connecteur SMTP, puis désignez ces serveurs comme les serveurs têtes de pont source du connecteur.

Isoler un chemin de routage pour la communication avec d'autres domaines

Vous pouvez également utiliser un connecteur SMTP pour établir un chemin de routage isolé permettant de communiquer avec d'autres domaines. Cette approche est utile lorsque vous souhaitez utiliser des communications sécurisées avec une entreprise particulière.

Dans les versions antérieures d'Exchange, vous pouvez configurer des paramètres par domaine de messagerie. Même si ces options ne sont pas disponibles dans Exchange 2003, vous pouvez créer plusieurs connecteurs SMTP, définir des espaces d'adressage pour ces connecteurs, puis spécifiez les paramètres souhaités pour ces domaines.

Par exemple, supposons que vous souhaitez utiliser SSL pour sécuriser tous les messages électroniques envoyés aux forces armées sans toutefois utiliser SSL pour d'autres communications électroniques. Pour ce faire, vous avez besoin de deux connecteurs SMTP :

- Un connecteur avec un espace d'adressage SMTP:*.mil
- Un connecteur avec un espace d'adressage SMTP:*

Comme Exchange route tous les messages par l'intermédiaire du connecteur qui est le plus proche de l'espace d'adressage, tous les messages destinés au domaine .mil cherchent initialement à passer par le connecteur *.mil. Vous pouvez indiquer que le connecteur *.mil envoie du courrier à un seul serveur (un hôte actif), qu'il utilise SSL et nécessite une authentification. Comme le routage traite *.mil et * comme deux destinations séparées, si le connecteur *.mil n'est pas disponible, les messages sont mis en file d'attente jusqu'à ce que le connecteur soit disponible. Les messages ne sont pas redirigés par l'intermédiaire du connecteur SMTP qui utilise l'espace d'adressage *.

Équilibrage de charge avec plusieurs serveurs têtes de pont

Lorsque vous disposez d'un seul connecteur hébergé par plusieurs serveurs têtes de pont, les serveurs qui font appel au connecteur de manière aléatoire choisissent le serveur tête de pont qu'ils utilisent, ce qui permet d'équilibrer la charge des requêtes sur l'ensemble des serveurs têtes de pont. La situation est différente si vous disposez de plusieurs connecteurs avec le même espace d'adressage, chacun avec un serveur tête de pont unique. Les serveurs qui utilisent ces connecteurs utilisent une méthode basée sur le serveur GUID pour déterminer quels connecteurs disponibles ils vont utiliser. L'algorithme peut ne pas répartir de façon équitable les choix de serveur parmi les connecteurs disponibles. Aussi, pour garantir l'équilibrage de la charge, il est recommandé d'utiliser un connecteur unique connecté à plusieurs serveurs têtes de pont.

Utiliser des commandes SMTP ou ESMTP spécifiques

Vous pouvez utiliser un connecteur pour contrôler la manière dont vos serveurs Exchange font appel à SMTP pour communiquer avec d'autres serveurs. Pour initier des sessions SMTP, vous pouvez choisir si votre serveur utilise les commandes ESMTP ou les commandes SMTP, et vous pouvez contrôler le type de commandes émises par votre serveur.

Lorsque vous configurez une connexion SMTP, vous disposez des options de communications suivantes :

- Envoyer ou non des commandes ETRN/TURN côté serveur ou côté client.

  TURN est une commande SMTP qui permet au client et au serveur d'inverser leurs rôles et d'envoyer des messages dans la direction opposée sans avoir à établir une nouvelle connexion. ETRN est une commande

ESMTP envoyée par un serveur SMTP pour demander à autre serveur d'envoyer les messages qu'il contient. Vous pouvez faire appel à ces commandes si vous dépendez d'un fournisseur de services réseau pour la conservation et la remise de votre courrier à la demande.

- Demander ETRN/TURN à des serveurs spécifiques.
- Envoyer HELO (commande SMTP) à la place d'EHLO (commande ESMTP).

  HELO est une commande SMTP envoyée par un client afin de s'identifier le plus souvent auprès d'un nom de domaine ; EHLO est une commande ESMTP qui permet à un serveur d'identifier sa prise en charge des commandes ESMTP.

Planifier et personnaliser des connexions sortantes

Vous pouvez utiliser un connecteur pour ouvrir une connexion sortante à des moments définis. Cette fonctionnalité vous permet d'utiliser un fournisseur de services réseau pour la remise de votre courrier ou si votre bande passante est limitée et que vous souhaitez contrôler le moment où votre courrier externe est envoyé.

Vous pouvez également configurer un connecteur pour :

- autoriser des propriétés de message hautes, normales ou basses pour un domaine ;
- autoriser les messages système ou non système ;
- utiliser des temps de remise différents pour les messages de taille limite ;
- mettre les messages en file d'attente pour une remise déclenchée à distance ;
- définir des restrictions de remise spécifiques.

Dépendances de transport

Pour fonctionner correctement, le service SMTP (Simple Message Transfer Protocol) repose sur les composants suivants :

- Services IIS (Internet Information Services), une fonctionnalité de Microsoft® Windows Server™ 2003
- Service d'annuaire Microsoft Active Directory®
- DNS (Domain Name System)
- Stratégies de destinataire
- Service de mise à jour de destinataire
- Service d'annuaire vers la métabase (DS2MB)

Ce chapitre fournit des informations détaillées sur chacun de ces composants et sur leur interaction avec le service SMTP.

Procédures du chapitre 3

Le tableau 3.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre, ainsi que les autorisations requises pour les effectuer.

Tableau 3.1 Procédures du chapitre 3 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Ajouter une adresse SMTP supplémentaire pour vos utilisateurs	Membre du groupe d'administrateurs locaux et membre d'un groupe auquel le Rôle Administrateurs intégral Exchange a été appliqué au niveau du groupe de l'organisation

Services Internet IIS (Internet Information Services)

Les services IIS (Internet Information Services) fournissent un processus d'infrastructure pour les services Internet tels que le service de publication sur le World Wide Web (W3SVC), le service SMTP (SMTPSVC) et le service du protocole NNTP (Network News Transfer Protocol - NntpSvc). Ne confondez pas le service IIS avec les services Web car plusieurs autres services tels que SMTP dépendent du service IIS pour fonctionner.

L'installation du service IIS fournit les éléments suivants :

- Le processus d'infrastructure connu sous le nom de service d'administration IIS (IISADMIN) qui permet l'administration des services par l'intermédiaire du composant logiciel enfichable IIS.
- Les consoles d'administration ou les composants logiciels enfichables pour Microsoft Management Console (MMC).
- La métabase IIS qui est le référentiel de configuration pour IIS.
- Les fichiers communs qui sont des bibliothèques partagées qui fournissent des groupements de connexion de sockets, l'inscription et la gestion de ces services Internet.

L'installation de Microsoft Exchange 2000 Server et Exchange Server 2003 nécessite l'installation du service de publication du World Wide Web ainsi que des service SMTP et NNTP. Cette exigence garantit que tous les composants nécessaires sont installés avant l'installation d'Exchange. Exchange exploite le service SMTP principal par l'intermédiaire d'une infrastructure d'événements. (Pour plus d'informations sur les infrastructures d'événements, consultez le site MSDN® http://msdn.microsoft.com/.) Une fois Exchange installé, le service SMTP ne dépend que du service d'administration IIS. Vous pouvez désactiver le service de publication sur le World Wide Web sans affecter le service SMTP ; cependant, vous ne pouvez pas utiliser l'option **Ajouter/Supprimer des composants Windows** dans **Ajout/Suppression de programmes** pour désactiver le service d'administration IIS ou pour supprimer le composant IIS entièrement.

L'installation du service IIS crée plusieurs répertoires virtuels sous le service de publication sur le World Wide Web qui ne sont pas nécessaires pour les composants Exchange, notamment Microsoft Outlook® Web Access. Pour sécuriser le service IIS, Microsoft fournit les outils suivants :

- URLScan version 2.5 pour Windows Server 2003

  URLScan version 2.5 est un outil de sécurité qui limite les types de demandes HTTP que traite le service IIS. Pour accroître la sécurité sur votre serveur qui exécute Windows Server 2003, exécutez URLScan. Vous pouvez télécharger URLScan à partir du Centre de téléchargement Microsoft. Pour plus d'informations sur URLScan, consultez l'article 823175 (en anglais) de la Base de connaissances Microsoft, « Fine-Tuning and Known Issues When You Use the Urlscan Utility in an Exchange 2003 Environment » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=823175).

- Assistant IIS Lockdown pour Windows® 2000 Server

  L'Assistant IIS Lockdown est un outil de sécurité qui supprime les répertoires virtuels superflus, améliore la sécurité des fichiers et traite les demandes d'URL en temps réel en fonction des configurations définies par l'utilisateur. Pour optimiser la protection dans le cas peu probable du démarrage par erreur du service de publication sur le World Wide Web, si vous exécutez Exchange sur des serveurs Windows 2000, vous devez déployer l'Assistant IIS Lockdown sur chaque serveur et chaque contrôleur de domaine Exchange. Vous pouvez télécharger l'Assistant IIS Lockdown à partir du Centre de téléchargement Microsoft (http://go.microsoft.com/fwlink/?LinkId=12281). Pour plus d'informations sur l'utilisation de l'Assistant IIS Lockdown, consultez la section « Utilisation de l'Assistant IIS Lockdown sur Windows 2000 Server » au chapitre 8.

Active Directory

Exchange 2003 est fortement intégré à Windows 2000 et Windows Server 2003 ainsi qu'à Active Directory. Exchange enregistre toutes les informations de configuration dans Active Directory, y compris celles relatives aux stratégies de destinataire, à la configuration du connecteur et du routage, à la configuration du serveur virtuel SMTP, aux boîtes aux lettres des utilisateurs ainsi que beaucoup d'autres informations. Toutefois, SMTP lit ses paramètres à partir de la métabase IIS. Ainsi, pour fournir au service IIS les informations requises pour la fonctionnalité SMTP, le Service de surveillance du système Exchange (un service des Services d'Exchange par défaut) réplique les informations de configuration d'Active Directory vers la métabase IIS.

En outre, le routage dépend d'Active Directory pour obtenir des informations sur la topologie de routage actuelle. Au démarrage, chaque serveur Exchange lit les informations d'Active Directory sur la topologie de routage, telles que la configuration du connecteur existant, les groupes de routage, les serveurs têtes de pont locaux et distants. Si un objet comme un groupe de routage ou un connecteur est endommagé, il n'est pas lu depuis Active Directory. Dans ce cas, les serveurs ont un affichage incomplet de la topologie. Surveillez l'événement 929 dans l'Observateur d'événements pour détecter cette situation. Pour plus d'informations sur l'Observateur d'événements, consultez la section « Utilisation de l'Observateur d'événements » au chapitre 12.

Après le démarrage, le maître du groupe de routage (serveur chargé de maintenir et de communiquer les informations sur la topologie de routage dans son groupe de routage) de chaque groupe de routage s'inscrit auprès d'Active Directory et reçoit du contrôleur de domaine de configuration la notification des modifications

de version de routage importantes. Lorsqu'un maître du groupe de routage reçoit une mise à jour de la topologie de routage, celui-ci envoie les informations mises à jour à tous les serveurs membres dans son groupe de routage et avertie tous les serveur têtes de pont dans les groupes de routage distants. Ces serveurs avertissent ensuite leurs maîtres de groupe de routage respectifs. En outre, le catégoriseur, composant de transport interne, accède à une version mise en cache des informations dans Active Directory à l'aide de DSAccess ou en interrogeant Active Directory directement à l'aide des requêtes LDAP. Pour plus d'informations sur le catégoriseur, consultez le chapitre 14 « Présentation des composants de transport internes ».

DNS

Même si une analyse et une discussion complètes sur le service DNS sortent du cadre de ce guide, cette section fournit des informations sur les relations entre les services DNS et SMTP dans Exchange. Comme Exchange 2003 repose sur le service DNS pour la résolution de noms, ce service joue un rôle crucial dans le flux des messages Internet.

Le service SMTP dépend du service DNS pour déterminer l'adresse du protocole Internet (IP) de son prochain serveur de destination interne ou externe. En général, les noms DNS internes ne sont pas publiés sur Internet. Aussi, le service SMTP doit pouvoir contacter un serveur DNS capable de résoudre les noms DNS externes pour envoyer les messages Internet, ainsi qu'un serveur DNS capable de résoudre les noms DNS internes pour la remise des messages au sein de l'organisation. Pour des informations sur la configuration du service DNS pour l'envoi et la réception des messages, consultez « Configuration du service DNS » au chapitre 4.

Les sections suivantes fournissent une vue d'ensemble générale des requêtes DNS et une explication du rôle que joue le service DNS dans l'envoi et la réception des messages.

Fonctionnement des requêtes DNS externes

Lorsqu'un client DNS doit résoudre le nom d'un serveur, il interroge les serveurs DNS. Chaque requête envoyée par le client demande essentiellement au serveur DNS de fournir ces informations. Le client spécifie le type de la requête, il peut s'agir soit d'un enregistrement de ressource par type, soit d'un type spécialisé d'opération de requête. Par exemple, pour rechercher des serveurs de messagerie SMTP depuis Internet, spécifiez le type de requête MX (enregistrement de ressource de serveur de messagerie).

Par exemple, le nom spécifié peut correspondre à un domaine externe, tel qu'example.microsoft.com., et la définition du type de requête à rechercher peut être un enregistrement MX de ce nom. Il faut se représenter une requête DNS comme un client posant à un serveur une question en deux parties : Premièrement, « Avez-vous des enregistrements de ressource MX pour un domaine intitulé 'example.microsoft.com.' ? », deuxièmement, « Si oui, pouvez-vous convertir cet enregistrement MX en enregistrement A (hôte) et résoudre son adresse IP ? » Lorsque le client reçoit une réponse du serveur, il lit et interprète l'enregistrement MX et reçoit l'enregistrement A, ce qui résout l'adresse IP de l'ordinateur.

Interrogation d'un serveur DNS

Lorsqu'un serveur DNS reçoit une requête, le serveur commence par vérifier s'il peut répondre à la requête avec autorité en fonction des informations d'enregistrement MX contenues dans une zone configurée localement sur le serveur. Si le nom interrogé correspond à un enregistrement MX dans la zone locale, le serveur répond avec autorité et utilise ces informations pour résoudre le nom interrogé.

Si aucune information de zone n'existe pour le nom interrogé, le serveur vérifie ensuite pour déterminer s'il peut résoudre le nom en utilisant des informations mises en cache localement issues de requêtes précédentes. Si une correspondance est trouvée, le serveur répond par ces informations. Une fois de plus, si le serveur préféré peut fournir au client demandeur une réponse correspondante positive depuis son cache, la requête est terminée.

Si aucune information mise en cache ou de zone n'existe pour le nom interrogé, le processus d'interrogation utilise la récursivité pour résoudre complètement le nom. La récursivité est le processus durant lequel un serveur DNS interroge d'autres serveurs DNS pour le compte du client demandeur afin de résoudre complètement le nom, puis renvoie une réponse au client. Par défaut, le service du client DNS nécessite que le serveur fasse appel à la récursivité pour résoudre complètement les noms pour le compte du client avant de renvoyer une réponse. Dans la plupart des cas, le serveur DNS est configuré (par défaut) pour prendre en charge le processus de récursivité comme l'illustre la figure 3.1.

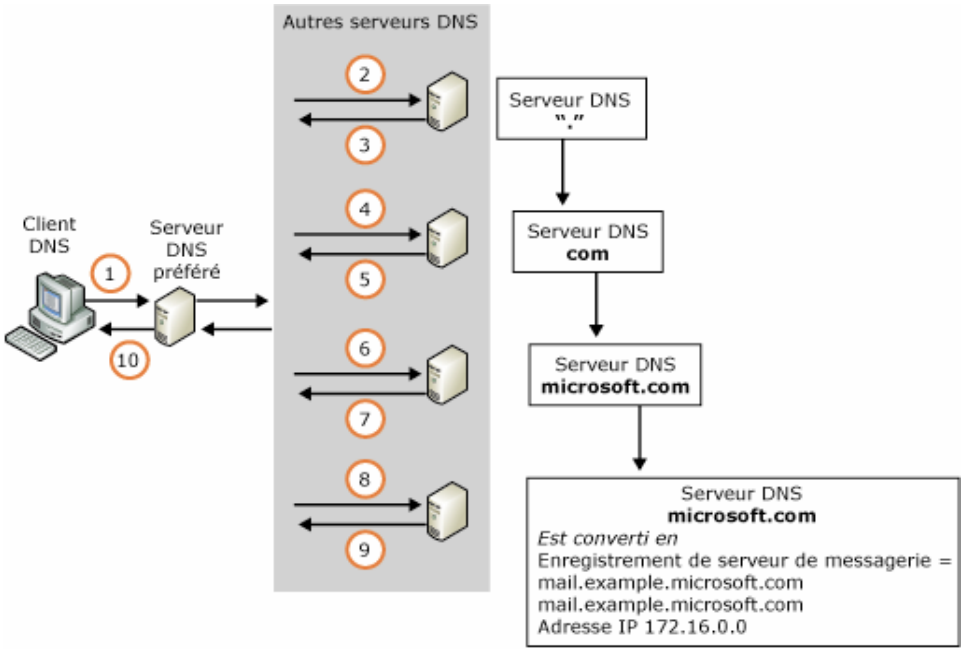


Figure 3.1 Résolution par le service DNS d'une demande d'un enregistrement MX et recherche de l'adresse IP

Pour plus d'informations sur le service DNS, consultez l'aide de Microsoft Windows 2000 ou Windows Server 2003.

Rôle du service DNS dans l'envoi ou la réception des messages internes

Windows 2000 et Windows Server 2003 enregistrent le nom de domaine complet (FQDN) de chaque serveur auprès du DNS dynamique. Votre serveur Exchange et vos serveurs virtuels SMTP utilisent également le nom de domaine complet. Si vous modifiez le nom de domaine complet utilisé par votre serveur virtuel SMTP, veillez à ajouter manuellement un enregistrement pour ce nom de domaine complet dans le service DNS.

Rôle du service DNS dans la réception des messages Internet

Pour recevoir des messages Internet, vos serveurs DNS externes doivent posséder un enregistrement MX qui pointe vers un enregistrement A et contient l'adresse IP de vos serveurs de messagerie ou un serveur en mesure de transférer des messages vers vos serveurs de messagerie. Pour vérifier que vos enregistrements MX sont configurés correctement, vous pouvez utiliser l'utilitaire Nslookup. À l'aide de Telnet, vous pouvez vérifier que votre serveur est accessible sur le port 25 aux autres serveurs sur Internet.

Pour plus d'informations sur Nslookup, consultez la section « Utilisation de Nslookup pour vérifier la configuration DNS » au chapitre 4. Pour plus d'informations sur Telnet, consultez la section « Utilisation de Telnet pour garantir l'accessibilité à Internet » au chapitre 4.

Rôle du service DNS dans l'envoi des messages Internet

Exchange utilise l'une des deux méthodes suivantes pour l'envoi des messages Internet :

- Utilisation du service DNS pour la résolution de noms externes.
- Transmission des messages à un hôte actif chargé de la résolution des noms et de la remise des messages.

Pour envoyer des messages Internet à l'aide du service DNS au lieu de les transmettre vers un hôte intelligent, le serveur Exchange résout le domaine de réception et l'adresse IP du serveur SMTP du destinataire. Le serveur utilise ensuite le service SMTP pour établir une connexion avec le serveur SMTP du destinataire et pour remettre les messages.

Utilisation du service DNS pour envoyer des messages Internet

Lorsque vous utilisez le service DNS, il est essentiel de se rappeler que tous les serveurs DNS dans l'ordre de recherche DNS doivent pouvoir résoudre des domaines externes (également appelés domaines Internet). Comme il est probable que vous ferez appel à des serveurs internes pour la résolution de noms internes, vous avez trois options de configuration possibles :

- **Configurez vos serveurs DNS internes comme serveurs de mise en cache qui utilisent des indications de racine pour les domaines Internet**. Les indications de racine pointent vers des serveurs DNS qui font autorité pour la zone contenant la racine du domaine et les domaines supérieurs. Les indications de racine permettent aux serveurs DNS de localiser le serveur correct permettant de résoudre un nom de domaine.
- **Configurez les serveurs DNS internes avec des redirecteurs vers les serveurs DNS externes**. Un redirecteur est un serveur DNS désigné par un serveur interne pour résoudre les noms DNS externes (pour configurer un redirecteur, dans la console DNS, sélectionnez le serveur DNS. Dans le menu **Action**, cliquez sur **Propriétés**, sur l'onglet **Redirecteurs**, puis activez la case à cocher **Activer les redirecteurs**. Ajoutez les adresses IP pour les autres serveurs DNS qui fonctionnent en tant que redirecteurs pour ce serveur).
- **Configurez le service SMTP pour utiliser les serveurs DNS externes**. Pour configurer un serveur DNS externe, cliquez avec le bouton droit sur votre serveur virtuel SMTP, cliquez sur **Propriétés**, puis sur l'onglet **Remise**. Cliquez sur **Options avancées**, puis sur **Configurer** pour configurer un serveur DNS externe.

Par exemple, supposons qu'un client interne du domaine example.com envoie un message à un destinataire du domaine distant contoso.com. Pour router le message, Exchange utilise le service DNS pour résoudre l'adresse IP du serveur SMTP du domaine Contoso et pour remettre le message au destinataire à contoso.com. La figure 3.2 illustre ce processus. La séquence suivante explique également la manière dont Exchange fait appel au service DNS pour la résolution d'une adresse IP externe :

1. Une fois que le serveur SMTP dans le domaine example.com a reçu le message destiné au destinataire à contoso.com, le serveur virtuel SMTP contacte le serveur DNS approprié et envoie une requête MX pour le domaine externe de contoso.com.
2. Le serveur DNS localise un enregistrement A associé à l'enregistrement MX pour contoso.com, puis utilise cet enregistrement A pour déterminer l'adresse IP. Pour plus d'informations sur la manière dont le

serveur DNS localise l'enregistrement A, consultez la section « Interrogation d'un serveur DNS » plus haut dans ce chapitre.

3. Le serveur DNS renvoie l'adresse IP 172.234.234.23 pour le serveur de messagerie dans contoso.com au serveur virtuel SMTP.
4. Le serveur virtuel SMTP ouvre une connexion sur le port 25 du serveur SMTP distant à l'adresse IP 172.234.234.23 et remet les messages.

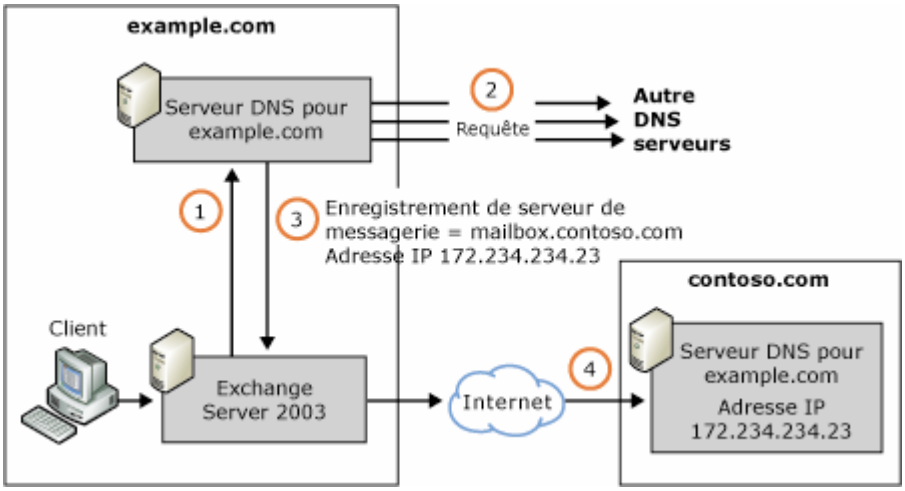


Figure 3.2 Utilisation par Exchange du service DNS pour la résolution des adresses IP externes

Transfert des messages Internet vers un hôte actif

Un hôte actif est un serveur ou un processus de messagerie qui traite la remise des messages Internet. Il n'est pas nécessaire que l'hôte actif soit un serveur Exchange — il peut s'agir d'un processus ou d'un serveur SMTP chargé de la remise des messages, soit en envoyant ces derniers à un autre serveur SMTP, soit en faisant appel au service DNS pour remettre les messages directement. Dans les cas où la connexion à Internet est permanente, un hôte actif n'est pas nécessaire. Cependant, il arrive souvent que l'hôte actif soit un antivirus ou un service SMTP de Windows 2000 ou de Windows Server 2003 qui se trouve dans un réseau de périmètre.

L'utilisation d'un hôte actif pour la résolution DNS est semblable à l'utilisation d'un serveur DNS, hormis le fait que l'hôte actif est chargé de la résolution de l'adresse IP et de l'envoi des messages (comme cela est expliqué de l'étape 2 à l'étape 4 dans la section « Utilisation du service DNS pour envoyer des messages Internet » plus haut dans ce chapitre).

Pour plus d'informations sur la configuration du service SMTP de Windows 2000 dans un réseau de périmètre, consultez l'article 293800 (en anglais) de la Base de connaissances Microsoft, « XCON: How to Set Up Windows 2000 as a SMTP Relay Server or Smart Host » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=293800).

Pour plus d'informations sur la configuration d'Exchange derrière un serveur Microsoft ISA (Internet Security and Acceleration), consultez l'article technique (en anglais) *Microsoft ISA Server 2000 – Configuring and Securing Exchange 2000 Server and Clients* (http://go.microsoft.com/fwlink/?LinkId=10733).

Stratégies de destinataire

Une stratégie de destinataire définit les adresses de messagerie par défaut qui utilisent un protocole spécifique (tel que SMTP) pour un ensemble d'utilisateurs. Les adresses de messagerie permettent de définir les formats d'adresses valides pour les messages électroniques entrants destinés au système Exchange. La stratégie de

destinataire par défaut établit le domaine de messagerie pour lequel le serveur virtuel accepte les messages électroniques entrants. Elle spécifie les adresses SMTP et X.400 par défaut pour tous les objets à boîte aux lettres activée, basés sur Exchange 2003.

Tous les domaines SMTP spécifiés dans les stratégies de destinataire sont répliqués dans la métabase IIS et définis en tant que domaines locaux faisant autorité. Par conséquent, le service SMTP accepte les messages entrants pour ces domaines. Une adresse SMTP n'est pas considérée comme étant locale uniquement lorsque vous désactivez la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse** dans **Propriétés de Adresse SMTP** et ajoutez cette adresse à la stratégie de destinataire.

Une stratégie de destinataire peut contenir plusieurs adresses de messagerie pour un protocole spécifié (tel que SMTP ou X.400). Par exemple, si tous les utilisateurs dans votre organisation Exchange possèdent une adresse de messagerie externe @example.com, mais que vous souhaitez que tous vos utilisateurs de Seattle disposent de deux adresses de messagerie externes — l'une avec @example.com et l'autre avec l'adresse @seattle.example.com — vous pouvez configurer une stratégie de destinataire pour tous les utilisateurs de votre bureau de Seattle et ajoutez une adresse supplémentaire @seattle.example.com. Pour ce faire, effectuez la procédure suivante.

Pour ajouter une adresse SMTP supplémentaire pour vos utilisateurs

1. Dans le Gestionnaire système Exchange, créez une nouvelle stratégie de destinataire : Dans l'arborescence de la console, développez **Destinataires**, cliquez avec le bouton droit sur **Stratégies de destinataire**, pointez sur **Nouveau**, puis cliquez sur **Stratégie de destinataire**.
2. Dans **Nouvelle stratégie**, cliquez sur **Adresses de messagerie**, puis sur **OK**.
3. Dans les propriétés de stratégie de destinataire, dans l'onglet **Général**, sous **Règles de filtrage**, cliquez sur **Modifier** pour créer un filtre qui définit tous les utilisateurs du service commercial.
4. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur **Nouvelle**.
5. Dans **Nouvelle adresse de messagerie**, cliquez sur **Adresse SMTP**.
6. Dans **Propriétés de Adresse SMTP**, **Adresse**, tapez **@seattle.example.com**. Cette opération ajoute une adresse SMTP @seattle.example.com à l'adresse SMTP @example.com.
7. Définissez une adresse principale.

   Lorsque vous disposez de plusieurs types d'adresse, vous devez définir une adresse comme adresse principale. L'adresse principale est celle qui apparaît par défaut dans la ligne **De** des messages sortants (sauf si l'utilisateur spécifie un suffixe d'adresse différent).
   Si vous voulez que l'adresse électronique de retour des utilisateurs de Seattle s'affichent toujours sous la forme de @seattle.example.com, définissez cette adresse comme l'adresse principale.

Pour plus d'informations sur la création des stratégies de destinataire, consultez la section « Configuration des stratégies de destinataire » au chapitre 7.

Service de mise à jour de destinataire

Le service de mise à jour de destinataire fait partie du service Surveillance du système Microsoft Exchange (MSExchangeSA) qui surveille les nouveaux destinataires dans Active Directory et inscrit l'adresse de messagerie appropriée et d'autres propriétés Exchange pour l'utilisateur dans Active Directory. Le service de mise à jour de destinataire utilise les informations définies dans les stratégies de destinataire pour mettre à jour Active Directory avec les informations utilisateur correctes destinées aux destinataires inclus dans chaque stratégie de destinataire.

Vous devez disposer d'un service de mise à jour de destinataire pour chaque domaine de votre organisation. Dans les grandes organisations, plusieurs services de mise à jour de destinataires sont recommandés. Vous

pouvez envisager un service de mise à jour de destinataire pour chaque site Active Directory. Si ce n'est pas le cas, la réplication des nouveaux destinataires et de leurs informations à jour peut nécessiter jusqu'à 30 minutes dans une topologie de réplication simple. Tant que cette réplication n'est pas terminée, ces destinataires ne sont pas en mesure d'envoyer ou de recevoir des messages.

Service d'annuaire vers la métabase

Le service DS2MB (service d'annuaire vers la métabase), un composant du service Surveillance du système Exchange est chargé de la propagation des informations depuis Active Directory vers la métabase IIS. Le service DS2MB est essentiel pour le fonctionnement des services SMTP, IMAP4 (Internet Message Access Protocol 4), POP3 (Post Office Protocol 3), le service de publication sur le World Wide Web (W3SVC) et le service de Microsoft Outlook® Web Access.

Le service DS2MB réplique les informations suivantes depuis Active Directory vers la métabase IIS :

- Les serveurs virtuels SMTP et la plupart de leurs propriétés configurables.
- Les espaces d'adressage du connecteur SMTP pour permettre le routage correct des messages par la métabase du moteur de files d'attente avancé.
- Les domaines faisant autorité des stratégies de destinataire (répliqués vers la sous-clé SMTPSVC/x/Domain et utilisés par le moteur de files d'attente avancé).

Au démarrage, le service DS2MB vérifie tous les objets répliqués par le passé ainsi que les modifications apportées depuis la dernière réplication. Si le service DS2MB détecte qu'aucune réplication n'a eu lieu, il initialise et réplique tous les objets.

Après le démarrage, le service DS2MB s'inscrit auprès du contrôleur de domaine de configuration pour que le contrôleur notifie ce service de toute modification apportée à la configuration d'Exchange et au conteneur Objets supprimés. Par conséquent, dès qu'une modification est répliquée sur le contrôleur de domaine de configuration, le service DS2MB réplique cet objet sur la métabase.

Si le service DS2MB rencontre des problèmes, il enregistre un événement avec un ID de 1040. Dans ce cas, augmentez l'enregistrement des diagnostics au niveau 5 pour MSExchangeMU (service de mise à jour de la métabase). Vous pouvez activer l'enregistrement des diagnostics dans le Gestionnaire système Exchange en cliquant avec le bouton droit sur votre serveur Exchange, en cliquant sur **Propriétés**, sur l'onglet **Enregistrement des diagnostics** et en sélectionnant MSExchangeMU sous **Services**. Pour plus d'informations sur cette procédure, consultez la section « Configuration de l'enregistrement des diagnostics pour le protocole SMTP » au chapitre 12.

Deuxième partie Configuration du flux des messages

La deuxième partie « Configuration du flux des messages » explique les facteurs à prendre en compte et les procédures concernées par la configuration du flux des messages au sein de votre organisation. Elle comprend les chapitres suivants :

Chapitre 4 « Configuration du service DNS »
: Ce chapitre explique comment vérifier la configuration correcte du service DNS pour la résolution des noms internes et externes. Ce chapitre explique également comment vérifier que les autres serveurs sur Internet peuvent localiser votre serveur de messagerie et remettre les messages dans votre organisation.

Chapitre 5 « Configuration de votre topologie de routage »
: Ce chapitre présente les topologies de routage courantes. Il explique également comment définir et configurer les groupes de routage et les connecteurs de groupe de routage et comment désigner un maître de groupe de routage.

Chapitre 6 « Scénarios de déploiement pour la connectivité Internet »
: Ce chapitre présente des scénarios personnalisés et courants utilisés par les organisations pour se connecter à Internet.

Chapitre 7 « Connexion à Internet »
: Ce chapitre vous guide dans le processus de connexion à Internet et de configuration de votre organisation pour l'envoi et la réception de messages Internet.

Configuration du service DNS

Ce chapitre vous guide tout au long des processus de vérification de la configuration correcte du service DNS (Domain Name System) dans votre organisation Exchange. Il comporte deux sections principales :

- Vérification de la configuration DNS interne
- Configuration du service DNS pour la remise des messages Internet

Procédures du chapitre 4

Le tableau 4.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre, ainsi que les autorisations requises pour les effectuer.

Tableau 4.1 Procédures du chapitre 4 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Vérifier que vos enregistrements MX ne pointent ni vers le nom de domaine complet de vos serveurs Exchange, ni vers un domaine interne	Membre du groupe Administrateurs local.
Vérifier que vos serveurs Exchange sont en mesure de résoudre les noms DNS internes	Membre du groupe Administrateurs local.
Vérifier que vos enregistrements MX sont configurés correctement	Membre du groupe Administrateurs local.
Vérifier que votre serveur est accessible sur Internet	Membre du groupe Administrateurs local.
Accéder aux propriétés du protocole Internet (TCP/IP) pour un serveur	Membre du groupe Administrateurs local.
Configurer des serveurs DNS externes sur un serveur virtuel SMTP sortant	Membre du groupe Administrateurs local.
Utiliser dnsdiag pour vérifier que votre serveur DNS est en mesure de résoudre les noms DNS externes	Membre du groupe Administrateurs local.
Utiliser nslookup pour vérifier que votre serveur DNS est en mesure de résoudre les noms DNS externes	Membre du groupe Administrateurs local.

Conception DNS

Avant de vérifier votre configuration DNS, assurez-vous que votre conception DNS est conforme aux conditions suivantes :

- Chaque contrôleur de domaine doit exécuter le service DNS.
- La résolution de noms récursifs existants est utilisée selon sa configuration pour l'organisation. Si aucune méthode n'est en place, utilisez des indications de racine sur tous les serveurs.

Le tableau 4.2 illustre la méthode préférée de configuration du service DNS. Il existe plusieurs autres configurations valides ; toutefois, la configuration figurant dans le tableau correspond à la méthode préférée. Le tableau 4.2 explique également la configuration de la zone pour chaque domaine Exchange.

Tableau 4.2 Configuration DNS préférée

Élément de conception	Conception
Type de zone	Intégré à Active Directory
Mises à jour dynamiques	Mises à jour dynamiques sécurisées uniquement
Nettoyage	Activé

Outils disponibles

L'outil DNS Resolver (Dnsdiag.exe) peut s'utiliser sur des serveurs Exchange exécutant Microsoft Windows Server™ 2003. Cet outil simule le chemin de code interne du service SMTP et génère des messages de diagnostic qui indiquent comment se déroule la résolution DNS.

Exécutez DNS Resolver sur l'ordinateur pour lequel vous souhaitez vérifier la configuration DNS. Votre chemin doit inclure %WINDIR%\System32\Inetsrv pour garantir le bon fonctionnement de l'outil.

Vous pouvez télécharger l'outil DNS Resolver à partir du site Web Microsoft (http://go.microsoft.com/fwlink/?LinkId=25097).

Si vous exécutez Exchange sur Microsoft Windows® 2000, vous pouvez utiliser l'outil Nslookup pour diagnostiquer et résoudre les problèmes du service DNS.

Vérification de la configuration DNS interne

Lorsque le service SMTP interroge le service DNS, celui-ci commence toujours par rechercher les enregistrements MX. Si un enregistrement MX interne existe et/ou est configuré de manière incorrecte, la remise de vos messages internes peut ne pas fonctionner.

Pour vérifier que vos enregistrements MX ne pointent ni vers le nom de domaine complet de vos serveurs Exchange, ni vers un domaine interne

1. À l'invite de commandes, tapez **nslookup**, puis appuyez sur ENTRÉE.
2. Tapez **server <*adresse IP*>** où *adresse IP* correspond à l'adresse IP de votre serveur DNS interne.
3. Tapez **set q=mx**, puis appuyez sur ENTRÉE.
4. Tapez **<*fqdn*>**, où *fqdn* correspond au nom complet de votre serveur virtuel SMTP (et de votre serveur Exchange), puis appuyez sur ENTRÉE.
5. Vérifiez qu'il n'existe aucun enregistrement MX pour votre serveur interne. Vos résultats doivent être similaires aux informations suivantes :

```
> set q=mx
> server1.example.local
example.local
        primary name server = server01.example.local
        responsible mail addr = hostmaster.example.local
```

```
        serial  = 6225703
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
```

6. Tapez **set q=a**, puis appuyez sur ENTRÉE.
7. Tapez **<*fqdn*>**, où *fqdn* correspond au nom complet de votre serveur virtuel SMTP (et de votre serveur Exchange), puis appuyez sur ENTRÉE.
8. Vérifiez que les résultats retournés correspondent à l'adresse IP de l'ordinateur. Sur un ordinateur multi-hébergement, l'adresse IP doit correspondre à l'adresse IP du serveur virtuel SMTP (sauf dans le cas d'un serveur virtuel unique avec une adresse IP de type « Non assignée »). Vos résultats doivent être similaires aux informations suivantes :

   ```
   set q=a
   > server1.example.local
   Name:    server1.example.local
   Address:  192.168.1.10
   ```

   Si le seul résultat renvoyé est l'enregistrement A correct, la résolution de noms internes doit aboutir. S'il n'y a aucun enregistrement ou si un enregistrement MX est renvoyé et pointe vers le nom de domaine complet ou l'adresse IP incorrects, d'autres serveurs peuvent ne pas être mesure d'envoyer des messages à ce serveur Exchange.

Exécutez l'outil DNS Resolver sur l'ordinateur pour lequel vous souhaitez vérifier la configuration DNS. Votre chemin doit inclure %WINDIR%\System32\Inetsrv pour garantir le bon fonctionnement de l'outil.

Pour vérifier que vos serveurs Exchange sont en mesure de résoudre les noms DNS internes

1. Sur votre serveur Exchange, ouvrez une invite de commandes, accédez au répertoire suivant et tapez les informations ci-dessous :

   ```
   <drive letter>:\WINDOWS\system32\inetsrv
   ```

2. Tapez ensuite :

   ```
   dnsdiag internal host name –v 1
   ```

   Où :

   internal host name est le nom de domaine complet d'un autre serveur Exchange dans votre organisation.

3. Vérifiez que l'adresse IP correcte du serveur Exchange est renvoyée. Vos résultats doivent être similaires aux informations suivantes :

   ```
           QNAME = example.microsoft.com
           Type = MX (0xf)
           Flags =  UDP default, TCP on truncation (0x0)
           Protocol = UDP
           DNS Servers: (DNS cache will not be used)
           172.16.1.101
   Connected to DNS 172.16.1.101 over UDP/IP.
   Received DNS Response:
   ----------------------
           Error: 9501
           Description: No records could be located for this name
   ```

```
        These records were received:
        microsoft.com   SOA

Querying via DNSAPI:
--------------------
        QNAME = example.microsoft.com
        Type = A (0x1)
        Flags =  DNS_QUERY_TREAT_AS_FQDN, (0x1000)
        Protocol = Default UDP, TCP on truncation
        Servers: (DNS cache will be used)
        Default DNS servers on box.
Received DNS Response:
----------------------
        Error: 0
        Description: Success
        These records were received:
        example.microsoft.com    A    172.16.1.106
1 A record(s) found for example.microsoft.com
Target hostnames and IP addresses
---------------------------------
HostName: "example.microsoft.com"
        172.16.1.106
```

Configuration du service DNS pour la remise des messages Internet

Cette section explique comment configurer le service DNS pour activer la remise des messages Internet. Il vous guide tout au long des tâches suivantes :

- Vérification de la configuration du service DNS pour les messages entrants
- Configuration du service DNS pour les messages sortants

Vérification de la configuration du service DNS pour les messages entrants

Le service DNS joue un rôle essentiel pour la remise des messages Internet. Pour recevoir des messages Internet, les paramètres suivants sont requis :

- Un enregistrement de serveur de messagerie (MX) pour votre serveur de messagerie doit figurer sur votre serveur DNS externe. Pour vérifier que vos enregistrements MX sont configurés correctement, utilisez l'utilitaire Nslookup. Vérifiez que les serveurs de messagerie que vous utilisez comme serveurs têtes de pont ou serveurs de messagerie Internet disposent d'un enregistrement MX sur vos serveurs DNS externes.
- Pour permettre aux serveurs DNS externes de résoudre l'enregistrement MX de votre serveur de messagerie et de contacter ce dernier, votre serveur de messagerie doit être accessible depuis Internet.

Vous pouvez faire appel au programme Telnet pour déterminer si les autres serveurs peuvent accéder à votre serveur de messagerie.

- Votre serveur Exchange doit être configuré pour contacter un serveur DNS ou pour résoudre les noms DNS.
- Votre serveur DNS doit être configuré correctement.

Les sections suivantes expliquent comment vérifier chacun de ces paramètres.

Remarque Il est recommandé, sans que cela soit obligatoire, d'utiliser le service Serveur DNS dans Microsoft Windows® 2000 ou Windows Server 2003. D'autres suites logicielles Serveur DNS sont disponibles, mais Microsoft a procédé à des tests rigoureux du service Serveur DNS ; par conséquent, celui-ci représente un choix fiable pour Windows 2000 et Windows Server 2003. Les instructions dans les sections suivantes s'appliquent au service Serveur DNS dans Windows 2000 et Windows Server 2003.

Utilisation de Nslookup pour la vérification de la configuration d'enregistrement MX

Si vous exécutez Exchange sur un serveur Windows 2000, vous pouvez utiliser l'outil Nslookup sur le serveur de messagerie qui accepte les messages Internet afin de vérifier que vos enregistrements MX sont configurés correctement.

Pour vérifier que vos enregistrements MX sont configurés correctement

1. À l'invite de commandes, tapez **nslookup**, puis appuyez sur ENTRÉE.
2. Tapez **server <*adresse IP*>** où *adresse IP* correspond à l'adresse IP de votre serveur DNS externe.
3. Tapez set **q=MX**, puis appuyez sur ENTRÉE.
4. Tapez <***nom de domaine***>, où *nom de domaine* est le nom de votre domaine, puis appuyez sur ENTRÉE.

L'enregistrement MX pour le domaine entré doit s'afficher. S'il ne s'affiche pas, le service DNS n'est pas configuré correctement.

L'exemple ci-dessous illustre l'affichage des enregistrements MX pour le domaine fictif, example.com :

```
C:\> nslookup
Default Server:  pdc.corp.example.com
Address:  192.168.6.13
> server 172.31.01.01
Default Server:  dns1.example.com
Address:  172.31.01.01
> set q=mx
> example.com.
Server:  dns1.example.com
Address:  10.107.1.7
example.com   MX preference = 10, mail exchanger = mail1.example.com
example.com   MX preference = 10, mail exchanger = mail2.example.com
example.com   MX preference = 10, mail exchanger = mail3.example.com
example.com   MX preference = 10, mail exchanger = mail4.example.com
example.com   MX preference = 10, mail exchanger = mail5.example.com
mail1.example.com     internet address = 172.31.31.01
mail2.example.com     internet address = 172.31.31.02
mail3.example.com     internet address = 172.31.31.03
```

```
mail4.example.com     internet address = 172.31.31.04
mail5.example.com     internet address = 172.31.31.05
```

Dans cet exemple, le serveur DNS configuré au préalable se trouve derrière un serveur proxy. De ce fait, un serveur DNS Internet ou externe avec une adresse IP connue 172.31.01.01 a été utilisé pour effectuer la requête. Puis, MX a été attribué au type de requête pour localiser les serveurs de messagerie pour example.com. Dans cet exemple, cinq serveurs SMTP sont parfaitement équilibrés chacun possédant sa propre adresse IP. Cependant, votre domaine peut ne contenir qu'une seule entrée comme le montre cet exemple :

```
contoso.com   MX preference = 10, mail exchanger = mailbox.contoso.com
mailbox.contoso.com     internet address = 10.57.22.3
```

Utilisation de Telnet pour garantir l'accessibilité à Internet

Si les serveurs sur Internet ne peuvent pas atteindre votre serveur de messagerie, vous ne pouvez pas recevoir de messages Internet. Vous pouvez utiliser Telnet pour vérifier que votre serveur de messagerie est accessible par d'autres serveurs sur Internet.

Une fois que vous avez vérifié la configuration correcte de vos enregistrements MX, vous pouvez ensuite vérifier que d'autres serveurs sur Internet peuvent accéder à votre serveur Exchange. Pour ce faire, à partir d'un emplacement situé en dehors de votre intranet, utilisez Telnet pour vous connecter à votre serveur de messagerie sur le port 25. Vous devez utiliser un ordinateur avec un accès direct à Internet afin de valider la connectivité lorsque vous vous connectez. Si le serveur possède plusieurs cartes d'interface réseau ou plusieurs adresses IP, vous devez utiliser Telnet pour vous connecter à l'adresse IP avec accès Internet.

Pour vérifier que votre serveur est accessible sur Internet

- À l'invite de commandes, tapez **telnet <*votre serveur de messagerie*> 25**, puis appuyez sur ENTRÉE.

Vérifiez que vous recevez une réponse similaire aux informations suivantes qui affichent les résultats d'une session Telnet vers le serveur de messagerie pour Contoso, mailbox.contoso.com.

```
C:\> telnet mailbox.contoso.com 25
220 corp.contoso.com Microsoft ESMTP MAIL Service, Version: 5.0.
2195.1600 ready at Tue, 5 Sep 2002 11:52:36 -0400
```

Configuration du service DNS pour les messages sortants

Vous pouvez utiliser l'une des deux méthodes pour configurer le service DNS pour les messages entrants :

Méthode 1

Vous pouvez configurer Exchange de manière à ce qu'il dépende de vos serveurs DNS internes. Ces serveurs résolvent les noms externes de manière autonome ou utilisent un redirecteur vers un serveur DNS externe.

Méthode 2

Vous pouvez configurer Exchange afin qu'il utilise un serveur DNS externe dédié.

Méthode 1: Utilisation des serveurs DNS internes pour la résolution des noms externes

Dans la méthode 1, Exchange s'appuie sur vos serveurs DNS pour la résolution des noms de domaine. Généralement, vous configurez vos serveurs Exchange comme clients DNS de votre serveur DNS interne. Sur votre serveur DNS interne, configurez un redirecteur externe pour pointer vers des serveurs DNS externes approuvés.

Les sections suivantes expliquent comment procéder à la configuration des éléments suivants :

- Paramètres DNS sur le serveur Exchange
- Paramètres sur le serveur DNS

Configuration des paramètres DNS sur le serveur Exchange

Le serveur Exchange doit généralement spécifier un serveur DNS local, autrement dit, le serveur Exchange doit pointer vers un serveur DSN interne dans son propre domaine.

Pour spécifier le serveur DNS vers lequel pointeront les serveurs Exchange, vous devez accéder à la boîte de dialogue **Propriétés du protocole Internet (TCP/IP)**.

Pour accéder aux propriétés du protocole Internet (TCP/IP) pour un serveur

1. Cliquez sur **Démarrer**, pointez sur **Paramètres**, puis cliquez sur **Connexions réseau et accès à distance**.
2. Double-cliquez sur **Connexion au réseau local,** puis dans **État de Connexion au réseau local**, cliquez sur **Propriétés**.
3. Dans **Propriétés de connexion au réseau local,** sous **Les composants sélectionnés sont utilisés par cette connexion**, double-cliquez sur **Protocole Internet (TCP/IP)**.
4. Dans **Propriétés du protocole Internet (TCP/IP)**, vérifiez que le service DNS est configuré correctement.

Le serveur Exchange doit pointer vers le serveur DNS principal pour votre domaine. Si vous disposez de plusieurs serveurs DNS locaux, vous pouvez configurer Exchange pour qu'il pointe vers l'un d'entre eux. Toutefois, il est recommandé qu'Exchange pointe vers le serveur DNS principal de ce domaine.

Configuration des paramètres sur le serveur DNS

Observez les instructions suivantes pour la configuration de votre serveur DNS. (Pour accéder à la console DNS, cliquez sur **Démarrer**, pointez sur **Outils d'administration**, puis cliquez sur **DNS**).

> **Remarque** Les paramètres de configuration dans cette section partent du principe que vous exécutez le service DNS sur vos contrôleurs de domaine.

- Vérifiez que le serveur DNS pointe vers son adresse IP. Pour confirmer ce paramètre, accédez à la boîte de dialogue **Propriétés du protocole Internet (TCP/IP)** pour le serveur DNS. Pour plus d'informations sur la manière d'accéder à cette boîte de dialogue, consultez la section « Accéder aux propriétés du protocole Internet (TCP/IP) pour un serveur » plus haut dans ce chapitre.

  > **Remarque** Il est fortement recommandé, lorsque vous utilisez l'ordinateur comme serveur DNS, de configurer TCP/IP manuellement et d'utiliser une adresse IP statique.

- Le serveur DNS doit contenir des zones de recherche directes pour chacun des domaines hébergés. Pour configurer ces zones, dans la console **DNS**, développez le serveur DNS, puis **Zones de recherche directes**, cliquez avec le bouton droit sur la zone de recherche directe souhaitée, cliquez sur **Propriétés**, puis utilisez les paramètres sous l'onglet **Général**. Pour chaque zone de recherche directe :

  - Attribuez la valeur **Oui** à **Autoriser les mises à jour dynamiques**.
  - Attribuez **Intégrées à Active Directory** à **Type**.
- Le serveur DNS doit contenir des zones de recherche indirectes pour chaque intervalle de sous-réseau IP hébergé. Pour configurer ces zones, dans la console **DNS**, développez le serveur DNS, puis **Zones de recherche indirectes**, cliquez avec le bouton droit sur la zone de recherche indirecte souhaitée, cliquez sur **Propriétés**, puis utilisez les paramètres sous l'onglet **Général**. Pour chaque zone de recherche indirecte :
  - Attribuez la valeur **Oui** à **Autoriser les mises à jour dynamiques**.
  - Attribuez **Intégrées à Active Directory** à **Type**.

    Remarque Si les zones de recherche indirectes ne sont pas activées sur vos serveurs DNS internes, le service DNS pourra encore fonctionner correctement.
- Configurez votre serveur DNS pour inclure des redirecteurs vers des serveurs DNS externes (Internet). Ce paramètre permet à votre serveur DNS de recevoir une requête pour des noms externes, de transmettre la requête au serveur distant, puis de remettre la réponse au demandeur. Pour configurer ce paramètre, ouvrez la console **DNS**, cliquez avec le bouton droit sur votre serveur DNS, cliquez sur **Propriétés**, sur l'onglet **Redirecteurs**, puis configurez les redirecteurs en serveurs DNS externes.

  Remarque Si la case à cocher **Activer les redirecteurs** sous l'onglet **Redirecteurs** n'est pas disponible, le serveur DNS a été configuré comme serveur DNS racine. Si tel est le cas, pour configurer les redirecteurs, vous devez supprimer la zone "**.**" (point), redémarrez la console DNS, puis configurez les redirecteurs.

Pour plus d'informations sur le service DNS en relation à Windows 2000 et le service d'annuaire Microsoft Active Directory®, consultez l'article 298448 (en anglais) de la Base de connaissances Microsoft, « Windows 2000 DNS and Active Directory Information and Technical Resources » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=298448).

Méthode 2 : Configuration des serveurs DNS externes sur un serveur virtuel SMTP

Cette section explique comment configurer les serveurs DNS externes sur un serveur virtuel SMTP. En configurant les serveurs DNS externes, vous spécifiez un serveur DNS différent du serveur configuré dans les propriétés TCP/IP de l'ordinateur exécutant Exchange. Ce serveur DNS est utilisé par le service SMTP pour la résolution des noms DNS externes et la remise des messages.

Pour configurer des serveurs DNS externes sur un serveur virtuel SMTP sortant

1. Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, **< *Nom serveur* >**, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur **<*votre serveur virtuel SMTP sortant*>**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Remise**, puis sur **Options avancées**. La boîte de dialogue **Remise avancée** apparaît (Figure 4.1).

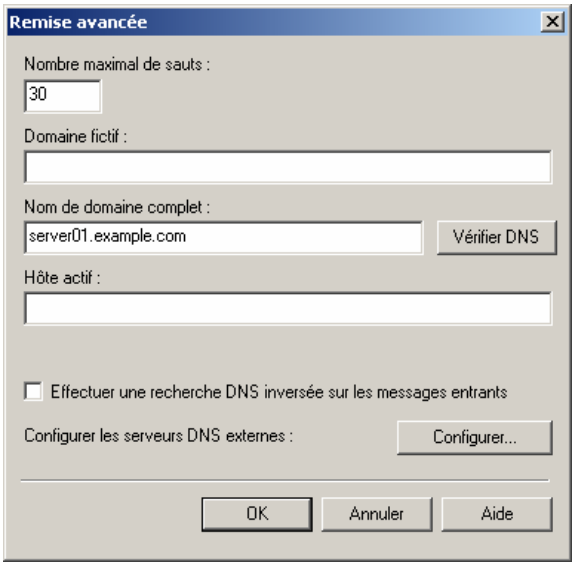


Figure 4.1 Boîte de dialogue Remise avancée

5. Dans **Remise avancée**, cliquez sur **Configurer**. La boîte de dialogue **Configuration** apparaît (Figure 4.2).

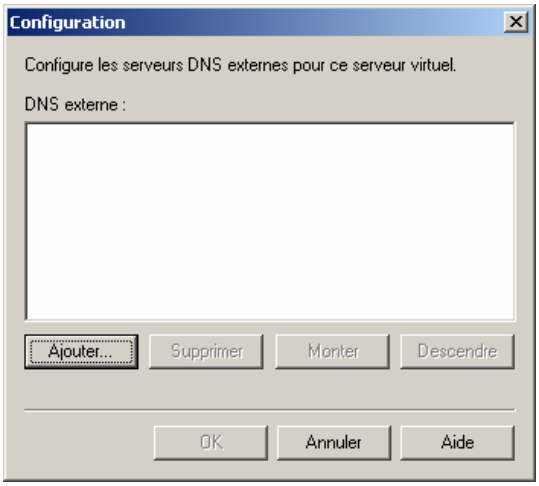


Figure 4.2 Boîte de dialogue Configuration

6. Dans **Configuration**, cliquez sur **Ajouter**, tapez l'adresse IP du serveur DNS externe que vous souhaitez utiliser, puis cliquez sur **OK**.
7. Dans **Configuration**, sous **DNS externe**, vérifiez que l'adresse IP est correcte, puis cliquez sur **OK** deux fois pour appliquer les paramètres.

Utilisation de DNS Resolver pour vérifier la configuration DNS

Pour qu'Exchange envoie des messages Internet, les serveurs DNS utilisés par Exchange pour votre domaine doivent pouvoir résoudre les noms de domaines externes. Pour vérifier que vos serveurs DNS peuvent résoudre les noms de domaines externes, utilisez l'outil DNS Resolver si vous exécutez Exchange 2003 sur Windows Server 2003.

Pour utiliser dnsdiag pour vérifier que votre serveur DNS est en mesure de résoudre les noms DNS externes

- Sur votre serveur Exchange, ouvrez une invite de commandes et tapez les informations suivantes :

  ```
  dnsdiag contoso.com –s 172.16.1.1 –v 1
  ```

  où :

  contoso.com est un domaine externe

  172.16.1.1 est l'adresse IP des serveurs DNS que vous souhaitez utiliser

  1 est le numéro d'instance du serveur SMTP que vous souhaitez utiliser

L'enregistrement de ressource de serveur de messagerie (MX) pour le domaine entré doit s'afficher. Si ce n'est pas le cas, le service DNS n'est pas configuré pour la résolution des noms de domaines externes.

L'exemple suivant illustre comment le serveur DNS pour example.com résout l'adresse IP du domaine externe contoso.com :

```
Created Async Query:
--------------------
        QNAME = contoso.com
        Type = MX (0xf)
        Flags =  UDP default, TCP on truncation (0x0)
        Protocol = UDP
        DNS Servers: (DNS cache will not be used)
        172.16.1.1
Connected to DNS 172.16.1.1 over UDP/IP.
Received DNS Response:
----------------------
        Error: 0
        Description: Success
        These records were received:
        contoso.com    MX    10    mail.contoso.com
        mail.contoso.com    A    172.16.1.2

Processing MX/A records in reply.
Sorting MX records by priority.

Target hostnames and IP addresses
---------------------------------
HostName: "mail.contoso.com"
        172.16.1.2
```

Utilisation de Nslookup pour vérifier la configuration DNS

Pour qu'Exchange envoie des messages Internet, les serveurs DNS utilisés par Exchange pour votre domaine doivent pouvoir résoudre les noms de domaines externes. Pour vérifier que vos serveurs DNS peuvent résoudre les noms de domaines externes, utilisez l'outil Nslookup si vous exécutez Exchange 2003 sur des serveurs Windows 2000.

Pour utiliser nslookup pour vérifier que votre serveur DNS est en mesure de résoudre les noms DNS externes

1. À l'invite de commandes, tapez **Nslookup**, puis appuyez sur ENTRÉE.
2. Tapez **server <*adresse IP*>** où *adresse IP* correspond à l'adresse IP de votre serveur DNS externe.
3. Tapez **set q=MX**, puis appuyez sur ENTRÉE.
4. Tapez <***nom de domaine***>, où *nom de domaine* est le nom d'un domaine de messagerie externe, puis appuyez sur ENTRÉE.

L'enregistrement de ressource de serveur de messagerie (MX) pour le domaine entré doit s'afficher. Si ce n'est pas le cas, le service DNS n'est pas configuré pour la résolution des noms de domaines externes.

L'exemple suivant illustre comment le serveur DNS pour example.com résout l'adresse IP du domaine externe contoso.com :

```
C:\> nslookup
Default Server:  pdc.corp.example.com
Address:  192.168.6.13
> server 10.255.255.255
Default Server:  dns1.example.com
Address:  10.255.255.255
> set q=mx
> contoso.com.
Server:  dns1.example.com
Address:  192.168.10.10
contoso.com   MX preference = 10, mail exchanger = mail1.contoso.com
contoso.com   MX preference = 10, mail exchanger = mail2.contoso.com
contoso.com   MX preference = 10, mail exchanger = mail3.contoso.com
mail1.contoso.com     internet address = 192.168.255.011
mail2.contoso.com     internet address = 192.168.255.012
mail3.contoso.com     internet address = 192.168.255.013
```

Dans cet exemple, le serveur DNS configuré au préalable se trouve derrière un serveur proxy. De ce fait, un serveur DNS Internet ou externe avec une adresse IP connue 10.255.255.255 a été utilisé pour effectuer la requête. Puis, MX a été attribué au type de requête pour localiser les serveurs de messagerie pour contoso.com. Dans cet exemple, trois serveurs SMTP sont parfaitement équilibrés chacun possédant sa propre adresse IP.

Configuration de votre topologie de routage

Ce chapitre explique la planification, les concepts et les procédures concernés par la configuration de votre topologie de routage. Elle comprend les sections suivantes :

> **Remarque** Si vous exécutez Microsoft® Exchange sur un serveur unique, la plupart des rubriques relatives aux groupes de routage ne s'appliquent pas à votre organisation. Toutefois, ces rubriques peuvent vous être utiles si vous envisagez l'extension de votre système de messagerie pour prendre en charge plusieurs serveurs.

Considérations générales sur la planification
Cette section explique les informations que vous devez rassembler avant de configurer votre topologie de routage ainsi que les variables qui influencent celle-ci.

Topologies de routage courantes
Cette section présente les deux topologies de routage les plus courantes, une topologie de routage centralisée et une topologie de routage distribuée. Elle explique les scénarios d'utilisation courants de ces topologies.

Définition des groupes de routage
Cette section explique comment créer des groupes de routage, des connecteurs de groupe de routage et comment connecter des groupes de routage.

Description des restrictions et de la portée du connecteur
Cette section explique les décisions relatives à l'utilisation des restrictions et de la portée du connecteur.

Désignation d'un maître de groupe de routage
Cette section définit le maître de groupe de routage, explique son fonctionnement ainsi que les critères permettant de désigner un maître de groupe de routage.

Configuration de routage avancée
Cette section présente des rubriques relatives à la configuration de routage avancée. Elle décrit comment utiliser les connecteurs pour l'équilibrage de la charge et le basculement, et comment supprimer le trafic d'état des liaisons.

Procédures du chapitre 5

Le tableau 5.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 5.1 Procédures du chapitre 5 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Créer un groupe de routage	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Configurer les options pour un connecteur de groupe de routage	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange

Procédure	Autorisations ou rôles requis
	a été appliqué au niveau du groupe d'administration.
Spécifier un serveur tête de pont distant pour un connecteur de groupe de routage	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Activer les clés de Registre pour les restrictions de remise	Membre du groupe Administrateurs local.
Spécifier un autre serveur maître du groupe de routage	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Supprimer les informations sur l'état des liaisons sur un serveur	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Considérations générales sur la planification

Une topologie de routage bien conçue est essentielle pour permettre un flux des messages fiable et efficace. Avant de concevoir votre topologie de routage, tenez compte des limites suivantes qui s'appliquent à une seule organisation Exchange. Une seule organisation Exchange ne peut pas dépasser les paramètres suivants :

- Plus de 1000 groupes d'administration.
- Plus de 1000 serveurs.

Avant de configurer votre topologie de routage, vous devez effectuer une évaluation détaillée de votre environnement actuel en prenant en compte les variables suivantes :

Topologie réseau et utilisateurs dans chaque emplacement
: La connectivité entre les emplacements et la bande passante disponible en tenant compte également des applications qui utilisent actuellement le réseau ainsi que des futurs projets qui utiliseront la bande passante existante.

Numéro d'utilisateur, emplacement et usages du réseau
: Le nombre d'utilisateurs qui envoient des messages sur le réseau est une considération importante. Par ailleurs, la distribution des utilisateurs et leur communication ou non avec les autres utilisateurs à leur emplacement, ou avec d'autres utilisateurs à des emplacements différents. Également, vous devez tenir compte de la taille des messages envoyés par les utilisateurs situés dans des emplacements spécifiques. Par exemple, un bureau d'études peut envoyer des messages avec des pièces jointes contenant des fichiers graphiques volumineux à divers partenaires commerciaux. Ce trafic aura une plus grande incidence sur le réseau que le trafic provenant d'un service qui envoie peu de pièces jointes sur le réseau.

Type d'applications utilisé par votre entreprise
: Types d'application utilisés par le réseau et l'utilisation durant les heures de pleine activité du réseau.

Emplacements des centres de données
: Emplacement de vos centres de données et la connectivité disponible pour les bureaux régionaux et autres centres de données.

Éléments disponibles/occupés
: Utilisation des informations actuelles de type disponible/occupé dans différents emplacements géographiques. La réplication des dossiers publics comprend la réplication des informations de type

disponible/occupé. Est-ce que les utilisateurs situés dans différents emplacements géographiques nécessitent des informations actuelles de type disponible/occupé destinées aux utilisateurs en dehors de leurs emplacements géographiques ou est-ce que les utilisateurs nécessitent généralement des informations actuelles uniquement pour les utilisateurs situés à leur emplacement ?

Conception actuelle du service d'annuaire Microsoft Active Directory®
Le positionnement des serveurs de catalogue global et des contrôleurs de domaine, la conception de vos sites Microsoft Windows® et la manière dont ils répondent à vos groupes de routage.

Topologies de routage courantes

Cette section décrit deux topologies de messagerie couramment déployées :

- Une topologie de messagerie centralisée dans laquelle tous les serveurs possèdent une connectivité « full-meshed » (maillage intégral) et communiquent de point à point.
- Une topologie de messagerie distribuée dans laquelle un concentrateur ou un centre de données unique se connecte aux nombreux sites de succursales.

Topologie de messagerie centralisée

Dans une topologie de messagerie centralisée, vous disposez d'un concentrateur ou d'un centre de données unique où tous les serveurs sont connectés par une bande passante fiable à grande vitesse. Même si ce site couvre une zone géographique importante, tant que l'ensemble de vos serveurs est connecté par la même bande passante fiable, vous pouvez utiliser un groupe de routage unique.

Les avantages d'une topologie de messagerie centralisée incluent une administration simplifiée et un flux des messages plus efficace car tous les serveurs communiquent de point à point.

Toutefois, si certains de vos serveurs situés dans un emplacement central sont connectés par un réseau plus lent, il est préférable de regrouper ces serveurs dans un groupe de routage séparé. Un serveur dont la connectivité réseau n'est pas fiable au sein d'un seul groupe de routage peut générer un trafic d'état des liaisons. Comme tous les autres serveurs doivent être notifiés si ce serveur ou un connecteur de groupe de routage sur ce serveur n'est plus disponible, le maître de groupe de routage (serveur chargé de communiquer les informations sur la topologie de routage vers des serveurs au sein d'un groupe de routage) doit propager les modifications concernant l'état de ce serveur vers tous les serveurs dans le groupe de routage. Pour plus d'informations sur le maître de groupe de routage, consultez la section « Désignation d'un maître de groupe de routage » plus loin dans ce chapitre.

Topologie de messagerie distribuée

Dans une topologie de succursale ou de messagerie distribuée, généralement un ou plusieurs centres de données sont connectés à plusieurs emplacements de succursale plus petits qui utilisent une conception réseau « hub-and-spoke ». Dans ce scénario, vos serveurs dans le concentrateur central sont regroupés dans un groupe de routage unique où tous les serveurs ont une connectivité réseau fiable. Chaque emplacement de succursale représente son propre groupe de routage.

Généralement, dans le site du concentrateur central, vous disposez de serveurs têtes de pont qui se connectent aux groupes de routage de la succursale. Ces groupes de routage sont souvent des *groupes de routage de nœud feuille* c à d des groupes de routage qui possèdent un seul connecteur de groupe de routage entrant et un seul connecteur de groupe de routage sortant dans des connexions parfaitement opposées. Aucun autre connecteur ne peut figurer dans un groupe de routage de nœud feuille.

Il existe trois configurations possibles pour un groupe de routage de nœud feuille :

- Un groupe de routage avec un connecteur entrant vers un groupe de routage unique et aucun connecteur sortant.
- Un groupe de routage avec un connecteur sortant vers un groupe de routage unique et aucun connecteur entrant.
- Un groupe de routage avec un connecteur sortant vers un groupe de routage unique. Voir la figure 5.1 pour des exemples de groupes de routage de nœud feuille.

Dans Exchange Server 2003, si aucun autre chemin n'existe pour un connecteur qui se connecte à ou depuis un groupe de routage de nœud feuille, l'état du connecteur est toujours signalé comme en service. Exchange Server 2003 ne modifie plus l'état indisponible du connecteur si aucun autre chemin n'existe. En revanche, Exchange place les messages en file d'attente pour les envoyer quand le chemin de routage est disponible. Ce changement améliore les performances car il réduit la propagation des informations sur l'état des liaisons ce qui est particulièrement utile dans un environnement de messagerie distribuée utilisant une topologie « hub-and-spoke ». Supposons que vous disposez d'un connecteur de groupe de routage unique qui connecte le site distant, le groupe de routage de nœud feuille vers le concentrateur et un autre connecteur de groupe de routage qui connecte le concentrateur au site distant. Si le connecteur de groupe de routage n'est plus disponible, soit au niveau du concentrateur, soit au niveau du site distant, les messages sont mis en file d'attente jusqu'à ce que le connecteur soit disponible. Aucun trafic d'état des liaisons n'est généré et le réseau n'est pas affecté.

La figure 5.1 illustre une topologie de messagerie distribuée dans une configuration « hub-and-spoke » standard. Dans cette topologie, chaque site physique renvoie à un groupe de routage. Dans le site central, tous les serveurs se trouvent dans un groupe de routage et communiquent de point à point. Comme chacun des sites de bureau distants ne dispose que d'un seul chemin de routage vers le site central, si un connecteur n'est pas disponible dans un site distant, les messages sont en files d'attente tant que ce dernier n'est pas disponible et qu'aucune modification de l'état des liaisons n'est propagée.

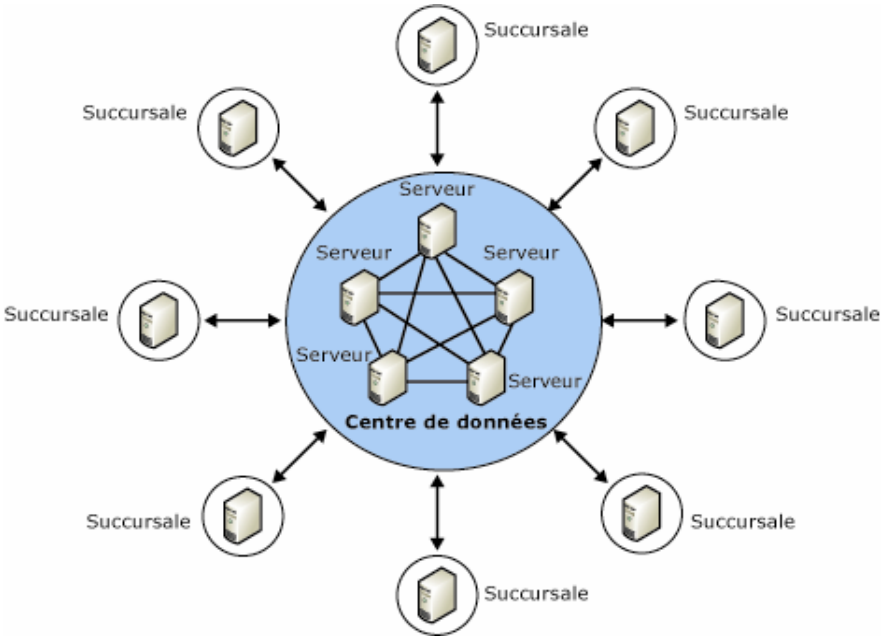


Figure 5.1 Topologie de messagerie distribuée dans une configuration « hub-and-spoke » standard

Définition des groupes de routage

La consigne générale est de définir un groupe de routage et d'en ajouter d'autres uniquement lorsque cela est nécessaire. Moins votre environnement comporte de groupes de routage, plus sa gestion s'en trouve simplifiée.

Toutefois, pour des besoins administratifs et géographiques, ainsi que de disponibilité du réseau, la création de groupes de routage supplémentaires peut s'avérer obligatoire.

Les groupes de routages sont créés généralement pour une des deux raisons suivantes :

- Pour tenir compte de la diversité de la connectivité du réseau entre les serveurs.
- Pour restreindre l'utilisation d'un connecteur aux utilisateurs d'une zone particulière. Pour plus d'informations sur l'utilisation des groupes de routage afin de restreindre l'utilisation du connecteur, consultez la section « Description des restrictions et de la portée du connecteur » plus loin dans ce chapitre.

Avant de définir vos groupes de routage, tenez compte des avantages et des inconvénients que présentent plusieurs groupes de routage comme cela est illustré dans le tableau 5.2.

Tableau 5.2 Avantages et inconvénients de plusieurs groupes de routage

Avantages de plusieurs groupes de routage	Inconvénients de plusieurs groupes de routage
• Permet la planification et le contrôle du flux des messages. Vous pouvez limiter l'utilisation du connecteur à un groupe de routage particulier ou planifier l'utilisation d'un connecteur. • Vous permet de contrôler l'utilisation en fonction de la taille des messages ou du contenu à l'aide des restrictions du connecteur.	• Introduit davantage de saut dans le routage vers la destination finale, ce qui réduit l'efficacité de la remise. • Complique votre environnement de messagerie. • Peut réduire la fiabilité de la messagerie en raison des sauts supplémentaires dans le routage et du plus grand risque de points de défaillance. • Le protocole SMTP (Simple Mail Transfer Protocol) traite la latence dans un environnement TCP/IP correctement connecté, ce qui évite souvent d'avoir à utiliser plusieurs groupes de routage. • Deux chemins de routages utilisent généralement le même réseau et le réseau possède la même stabilité ou fiabilité inhérente.

Le graphique représenté dans la figure 5.2 peut vous aider à déterminer comment définir des limites de groupes de routage.

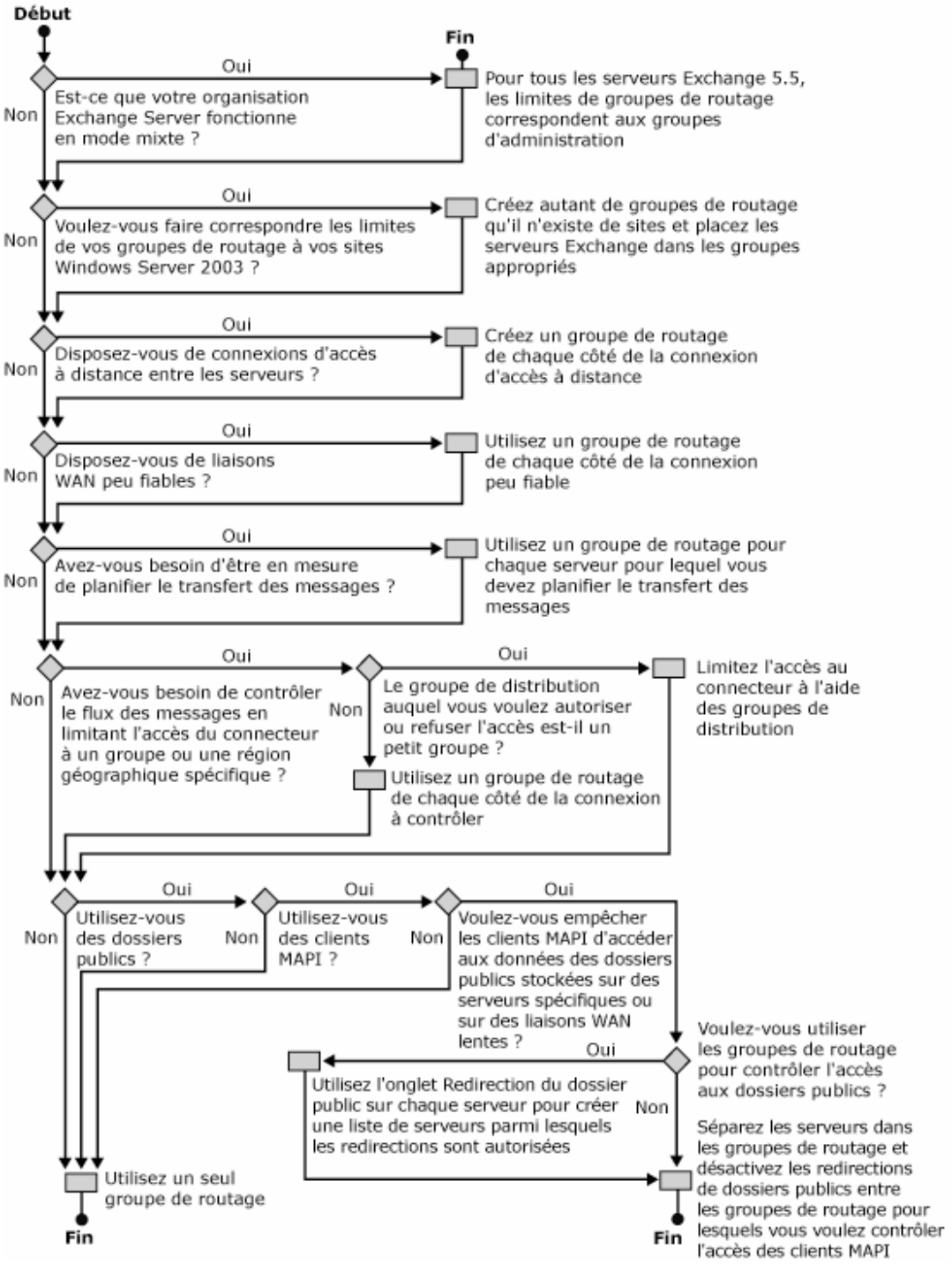


Figure 5.2 Détermination des limites des groupes de routage

Création de groupes de routage

Par défaut, Exchange fonctionne comme si tous les serveurs étaient dans un groupe de routage unique. En fonction de vos besoins d'administration, de la topologie de votre réseau et des raisons qui sont expliquées au tableau 5.2, vous pouvez grouper des serveurs dans des groupes de routage pour permettre à Exchange de maximiser le flux des messages efficacement.

Par défaut, dans une organisation Exchange en mode natif, tous les serveurs sont placés dans un seul groupe de routage appelé Premier groupe de routage, et ces serveurs communiquent directement entre eux. Dans un environnement en mode mixte (où certains serveurs exécutent Exchange Server 5.5 ou une version antérieure), chaque site Exchange Server 5.5 devient un groupe de routage.

> **Remarque** Pour plus d'informations sur la différence entre les groupes de routage en mode mixte et en mode natif, consultez la section « Utilisation des groupes de routage en mode natif et en mode mixte » au chapitre 1.

Après l'installation, vous pouvez créer des groupes de routage supplémentaires dans votre organisation Exchange. Lorsque vous installez des serveurs Exchange supplémentaires dans une organisation existante, vous pouvez ensuite désigner les groupes de routage appropriés pour ces serveurs. Après l'installation, vous pouvez également déplacer des serveurs entre les groupes de routage.

Lorsque vous créez un groupe de routage, deux conteneurs s'affichent sous le groupe de routage :

- **Connecteurs** Ce conteneur affiche tous les connecteurs installés sur les serveurs au sein du groupe de routage. Cette liste inclut les connecteurs d'accès aux systèmes de messagerie tiers, notamment le connecteur Lotus Notes ou Novell GroupWise, ainsi que tous les autres connecteurs de groupes de routage, les connecteurs X.400 et SMTP que vous configurez.
- **Membres** Ce conteneur affiche les serveurs au sein de ce groupe de routage. Par défaut, le maître du groupe de routage est le premier serveur ajouté à un groupe de routage.

  > **Remarque** Avant de pouvoir créer des groupes de routage, vous devez configurer votre organisation Exchange afin qu'elle affiche les groupes de routage. Dans le Gestionnaire système Exchange, cliquez avec le bouton droit sur votre organisation Exchange, cliquez sur **Propriétés,** puis activez la case à cocher **Afficher les groupes de routage**.

Pour créer un groupe de routage

1. Dans le Gestionnaire système, cliquez avec le bouton droit sur **Groupes de routage**, pointez sur **Nouveau**, puis sélectionnez **Groupe de routage**.
2. Sous l'onglet **Général** (figure 5.3), dans la zone **Nom**, entrez le nom du groupe de routage, puis cliquez sur **OK**.

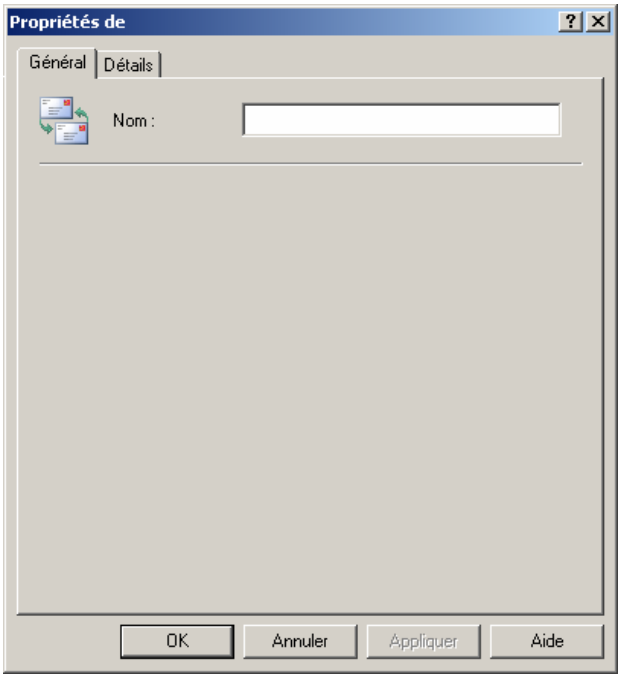


Figure 5.3 Onglet Général du groupe de routage

Définition des connecteurs de groupe de routage et des serveurs têtes de pont

Tous les serveurs communiquent entre eux directement au sein d'un groupe de routage, mais non pas avec un autre groupe de routage. Pour permettre aux serveurs de communiquer avec des serveurs situés dans d'autres groupes de routage, vous devez créer un *connecteur de groupe de routage*. Bien qu'il soit possible d'utiliser un connecteur X.400 ou SMTP pour connecter des groupes de routage, il est recommandé d'utiliser le connecteur de groupe de routage spécifiquement conçu à cet effet dans la plupart des cas.

Par défaut, tous les serveurs au sein d'un groupe de routage peuvent envoyer des messages par l'intermédiaire d'un connecteur de groupe de routage. Les serveurs capables d'envoyer des messages par l'intermédiaire d'un connecteur de groupe de routage sont appelés *serveurs têtes de pont*. Un serveur tête de pont représente une combinaison entre un serveur virtuel SMTP et un serveur Exchange chargé de la remise de tous les messages par l'intermédiaire d'un connecteur.

Lors de la création d'un connecteur de groupe de routage, vous avez la possibilité de conserver tous les serveurs en tant que serveurs têtes de pont pour ce connecteur ou de spécifier un seul ensemble de serveurs sélectionnés à cet effet. Le tableau 5.3 compare les avantages de ces deux approches.

Tableau 5.3 Sélection du nombre de serveurs têtes de pont dans un groupe de routage

Nombre de serveurs têtes de pont	Avantages
Tous les serveurs dans un groupe de routage	• Permet le flux efficace des messages, car tous les serveurs dans le groupe de routage peuvent directement remettre les messages aux autres groupes de routage. • Fonctionne dans les configurations où tous les serveurs dans un groupe de routage utilisent la même connectivité réseau vers les serveurs situés dans d'autres groupes de routage. • Peut ajouter de la complexité dans les grandes organisations où tous les serveurs communiquent de point à point. Les problèmes concernant le flux des messages peuvent être plus difficiles à résoudre. • La connectivité point à point peut fournir l'équilibrage des charges.
Seuls quelques serveurs sélectionnés dans un groupe de routage	• Facilite le dépannage du flux des messages en raison du nombre limité de points de contact entre les groupes de routage. • Distribue la messagerie si vous anticipez un flux de messages important entre les groupes de routage. • Vous permet de spécifier les rôles des serveurs têtes de pont et des serveurs de boîte aux lettres dans des environnements de grande taille où vous ne voulez pas que les serveurs de boîte aux lettres traitent le trafic envoyé par l'intermédiaire d'un serveur tête de pont. • Renforce la fiabilité et l'efficacité du flux des messages dans les configurations où certains serveurs disposent d'une meilleure connectivité réseau que d'autres.

La figure 5.4 illustre les composants de base du routage décrits plus haut. La figure 5.4 illustre le flux des messages entre les serveurs au sein d'un groupe de routage et entre les groupes de routage. Elle représente également une topologie qui utilise uniquement un seul serveur tête de pont dans chaque groupe de routage.

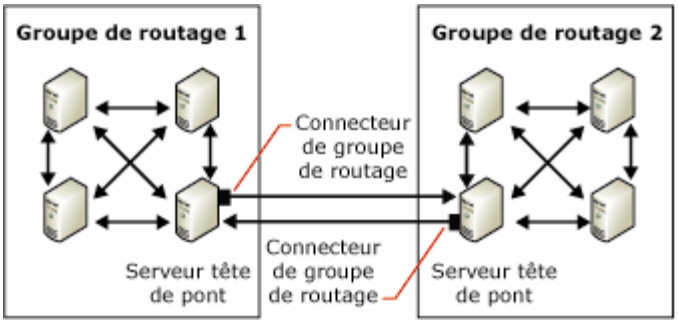


Figure 5.4 Communication au sein d'un groupe de routage et entre les groupes de routage

Dans le cas d'une topologie simple, telle que celle présentée à la figure 5.4, vous n'avez pas besoin de vous préoccuper du mode d'acheminement des messages entre les groupes. Lorsque les topologies deviennent plus complexes et que des nombres importants de groupes de routage s'étendent sur des distances géographiques variables, le routage des messages entre les groupes devient critique.

Vous configurez le routage dans les groupes de routage en affectant les coûts (dépense correspondante pour le chemin de routage basée sur la disponibilité du réseau, le trafic réseau et les besoins administratifs) aux connecteurs de groupe de routage utilisés par ces groupes. Lorsqu'un utilisateur sur un serveur dans un groupe de routage envoie des messages à un utilisateur sur un serveur dans un autre groupe de routage, Exchange utilise ces coûts (partie des informations sur l'état des liaisons conservées par Exchange) pour déterminer le chemin de routage le plus efficace. Exchange utilise toujours le chemin de routage offrant le coût le plus faible, sauf si un connecteur ou un serveur n'est pas disponible sur celui-ci. Chaque groupe de routage dispose d'un *maître de groupe de routage* qui met à jour et coordonne les informations relatives aux coûts avec tous les autres serveurs du groupe de routage, afin que chacun d'eux connaisse les différents coûts associés à chaque connecteur et l'état de ces derniers. Pour plus d'informations sur les maîtres de groupe de routage, consultez la section « Désignation d'un maître de groupe de routage » plus loin dans ce chapitre.

Connexion des groupes de routage

Lorsque vous créez un groupe de routage, vous désignez un groupe de serveurs qui peuvent communiquer directement entre eux. Vous devez connecter les groupes de routage afin que les serveurs dans les différents groupes puissent communiquer entre eux.

Il est possible de connecter des groupes de routage à l'aide d'un connecteur SMTP ou X.400. Toutefois, il n'est pas recommandé d'utiliser ces types de connecteurs en général. Il est préférable d'utiliser un connecteur de groupe de routage, spécifiquement conçu à cet effet.

> **Remarque** Si vous devez utiliser un connecteur SMTP ou X.400 entre des groupes de routage, n'ajoutez pas d'espace d'adressage sur ce connecteur. Vous devez désigner uniquement un groupe de routage connecté ; sinon, le routage ne fonctionnera pas correctement.

Les connecteurs de groupe de routage représentent des chemins de routage unidirectionnels pour les messages sortants. Ainsi, les messages voyagent en sortie vers le groupe de routage connecté. Pour permettre à deux groupes de routage de communiquer entre eux, un connecteur de groupe de routage doit exister dans chaque groupe de routage pour transmettre les messages à l'autre groupe. Lorsque vous créez un connecteur vers un groupe de routage, Exchange affiche un message pour vous demander si vous souhaitez créer un connecteur de groupe de routage dans le groupe de routage distant pour vous permettre d'envoyer des messages depuis le groupe de routage distant vers le groupe de routage dans lequel vous créez le premier connecteur.

Avant de créer et de configurer un connecteur de groupe de routage, vous devez vous poser les questions suivantes :

- **À quel groupe de routage ce connecteur remet-il les messages ?** Ces informations sont essentielles. L'identification du groupe de routage auquel le connecteur remet les messages établit la relation entre les groupes de routage émetteurs et récepteurs et les autres éléments de votre topologie. Vous devez savoir comment les groupes de routage émetteurs et récepteurs s'intègrent à votre topologie, afin de pouvoir déterminer un coût pour le connecteur correspondant.
- **Quel coût doit être affecté à ce connecteur ?** Le coût représente la variable utilisée par Exchange pour déterminer le chemin de routage le plus efficace des messages. Exchange considère le chemin de routage le moins cher comme étant le plus efficace. Exchange utilise un chemin de routage plus cher uniquement si un serveur ou un connecteur n'est pas disponible sur le chemin le moins cher. Vous devez affecter les coûts les plus faibles aux chemins de routage qui offrent la plus grande largeur de bande réseau disponible.
- **Quels serveurs dans le groupe de routage peuvent agir en tant que serveurs têtes de pont ?** Seuls les serveurs têtes de pont désignés peuvent envoyer des messages par l'intermédiaire du connecteur vers le groupe de routage connecté. La configuration par défaut est recommandée car elle permet à l'un des serveurs du groupe de routage local d'envoyer des messages à l'aide de ce connecteur. Utilisez cette option par défaut lorsque tous les serveurs dans le groupe de routage peuvent se connecter directement au serveur tête de pont distant et partager la même charge de messagerie. La connexion directe au serveur tête de pont distant augmente l'efficacité du flux des messages.

  Vous pouvez toutefois obtenir une meilleure connectivité réseau directe entre des serveurs spécifiques dans le groupe de routage local et le serveur tête de pont distant désigné. Supposons par exemple que le serveur A utilise une connexion directe de 56 kilobits par seconde (Kbits/s) vers un serveur tête de pont distant, et que le serveur B et le serveur C disposent chacun d'une connexion directe de 10 mégabits par seconde (Mbits/s) vers le même serveur tête de pont distant. Dans ce cas, vous devez désigner les serveurs qui offrent la meilleure connectivité réseau directe (le serveur B et le serveur C) en tant que serveurs têtes de pont et ajouter ces serveurs spécifiques à une liste des serveurs têtes de pont autorisés.

  Vous pouvez configurer tous les serveurs dans le groupe de routage pour qu'ils fonctionnent comme serveurs têtes de pont des deux façons suivantes :

  - Sélectionnez l'option par défaut **Tous les serveurs locaux peuvent envoyer des messages via ce conn**. Lorsque vous sélectionnez cette option, le connecteur est toujours marqué comme en service ou disponible même si tous les serveurs têtes de pont ne sont plus disponibles. Cette option offre l'avantage de générer moins d'informations sur l'état des liaisons car ce connecteur n'est jamais marqué comme non disponible.
  - Sélectionnez **Les serveurs suivants peuvent envoyer des messages via ce connecteur** et ajoutez manuellement chaque serveur dans le groupe de routage comme serveur tête de pont. Lorsque vous configurez vos serveurs têtes de pont de cette manière, si tous les serveurs têtes de pont ne sont plus disponibles, le connecteur du groupe de routage est marqué comme non disponible. Cependant, l'utilisation de cette option peut augmenter la taille de votre table d'état des liaisons car le nom de domaine complet de chaque serveur virtuel tête de pont est ensuite écrit dans cette table. Pour plus d'informations sur l'état des liaisons, consultez le chapitre 15, « Concepts avancés sur l'état des liaisons ».

  Pour plus d'informations sur l'évaluation des avantages offerts par l'utilisation de plusieurs serveurs têtes de pont à la place de serveurs têtes de pont désignés, consultez le tableau 5.3 plus haut dans ce chapitre.
- **Les utilisateurs doivent-ils pouvoir accéder aux dossiers publics qui ne sont pas disponibles localement à l'aide de ce connecteur ?** Par défaut, les redirections de dossiers publics sont activées sur les connecteurs qui relient les groupes de routage. Toutefois, le trafic réseau augmente lorsque les utilisateurs accèdent à un dossier public dans un groupe de routage distant. Si vos groupes de routage sont connectés par des liaisons réseau lentes ou si votre réseau ne peut pas gérer le trafic supplémentaire, désactivez les redirections de dossiers publics.

- **À quels serveurs têtes de pont distants ce connecteur peut-il envoyer des messages ?** Les serveurs têtes de pont distants représentent les serveurs qui, dans le groupe de routage connecté, reçoivent tous les messages destinés à ce dernier. Les serveurs têtes de pont distants reçoivent également les informations sur l'état des liaisons des serveurs têtes de pont du connecteur.

Après avoir étudié ces questions, vous pouvez définir vos options de configuration sous l'onglet **Général** de la boîte de dialogue **Propriétés de Connecteur de groupe de routage**. Pour répondre à la dernière question dans la liste ci-dessus, spécifiez les serveurs têtes de pont distants sous l'onglet **Serveur tête de pont distant**.

Pour configurer les options d'un connecteur de groupe de routage

1. Dans le Gestionnaire système Exchange, développez le groupe de routage, cliquez avec le bouton droit sur **Connecteurs**, pointez sur **Nouveau**, puis cliquez sur **Connecteur de groupe de routage**.
2. Sous l'onglet **Général** (Figure 5.5), sélectionnez les options suivantes :
   - Le nom du connecteur de groupe de routage correspond souvent aux noms des deux groupes de routage reliés par celui-ci. Par exemple, le nom ParisÀSeattle définit un connecteur qui connecte le groupe de routage Paris au groupe de routage Seattle.
   - Dans l'option **Connecte ce groupe de routage avec**, sélectionnez les groupes de routage auxquels vous souhaitez vous connecter.
   - Dans l'option **Coût**, affectez un coût au connecteur.
   - Si vous souhaitez que tous les serveurs dans le groupe de routage local fonctionnent en tant que serveurs têtes de pont, sélectionnez l'option **Tous les serveurs locaux peuvent envoyer des messages via ce conn**.

     Important N'oubliez pas que lorsque vous sélectionnez cette option, le connecteur est toujours considéré comme disponible même si tous les serveurs têtes de pont ne sont plus disponibles. Si vous voulez que votre connecteur soit marqué comme non disponible si tous les serveurs têtes de pont ne sont plus disponibles, ajoutez manuellement chaque serveur dans le groupe de routage comme serveur tête de pont, à l'aide de l'option **Les serveurs suivants peuvent envoyer des messages via ce connecteur** décrite plus loin.
   - Pour spécifier quels serveurs du groupe de routage local peuvent fonctionner en tant que serveurs têtes de pont pour ce connecteur, sélectionnez **Les serveurs suivants peuvent envoyer des messages via ce connecteur,** puis cliquez sur **Ajouter** pour ajouter les serveurs appropriés à la liste.
   - Pour empêcher les utilisateurs d'accéder aux dossiers publics qui ne sont pas disponibles localement à l'aide de ce connecteur, activez la case à cocher **Ne pas autoriser les redirections de dossiers publics**.

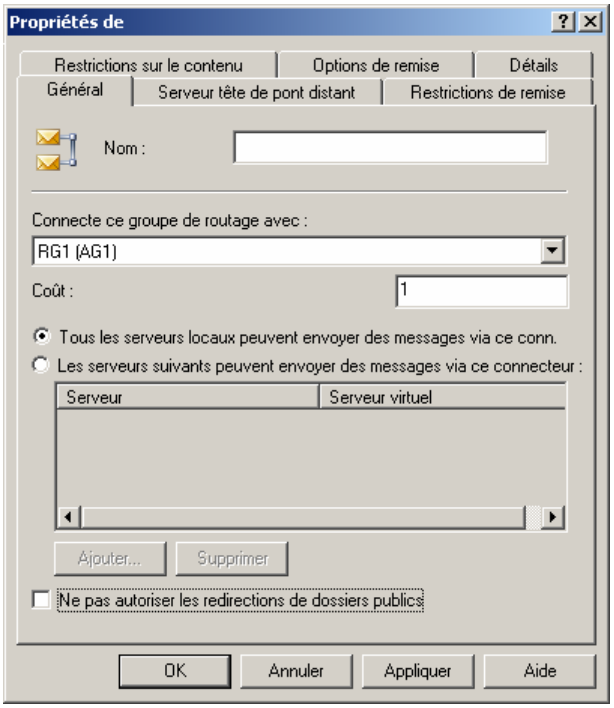


Figure 5.5 Onglet Général de la boîte de dialogue Propriétés de Connecteur de groupe de routage

Pour spécifier un serveur tête de pont distant pour un connecteur de groupe de routage

1. Dans la boîte de dialogue **Propriétés de Connecteur de groupe de routage**, sous l'onglet **Serveur tête de pont distant** (figure 5.6), cliquez sur **Ajouter**, puis sélectionnez le serveur tête de pont distant dans la liste des serveurs du groupe de routage auquel vous vous connectez.

   Remarque Vous devez spécifier un serveur tête de pont distant. Pour améliorer la redondance, il est recommandé de spécifier plusieurs serveurs têtes de pont distants si cela est possible.

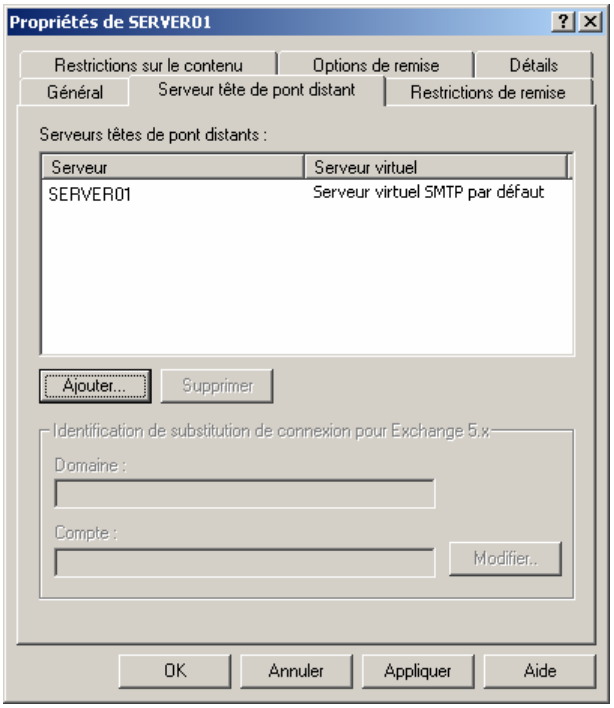


Figure 5.6 Onglet Serveur tête de pont distant de la boîte de dialogue Propriétés de Connecteur de groupe de routage

2. Si vous créez un connecteur de groupe de routage entre les groupes de routage qui incluent des serveurs Exchange 5.5, dans la zone **Identification de substitution de connexion pour Exchange 5.x**, cliquez sur **Modifier**, puis entrez les informations d'identification du compte de services Exchange 5.5 auquel vous vous connectez.
3. Cliquez sur **Appliquer** pour créer le connecteur.
4. Lorsqu'un message apparaît qui vous demande si vous souhaitez créer un connecteur de groupe de routage dans le groupe de routage distant, cliquez sur **Oui**.

Après avoir cliqué sur **Oui**, Exchange crée un connecteur de groupe de routage dans le groupe de routage distant. Le nouveau connecteur du groupe de routage permet au groupe de routage distant d'envoyer des messages au groupe de routage local. Lors de la création du connecteur du groupe de routage, Exchange effectue les opérations suivantes :

- Exchange désigne les serveurs têtes de pont pour le connecteur du groupe de routage distant comme serveurs recensés sous l'onglet **Serveur tête de pont distant** du connecteur du groupe de routage local.

  Remarque Lorsqu'Exchange désigne les serveurs de cette manière, seuls les serveurs recensés sous l'onglet **Serveur tête de pont distant** deviennent des serveurs têtes de pont pour le nouveau connecteur. Si vous préférez que tous les serveurs dans le groupe de routage distant (et non pas uniquement ceux qui sont recensés) fonctionnent comme serveurs têtes de pont pour le nouveau connecteur, vous devez sélectionner manuellement l'option **Tous les serveurs locaux peuvent envoyer des messages via ce conn.** sous l'onglet **Général** du nouveau connecteur ou ajouter individuellement chaque serveur comme serveur tête de pont.

- Exchange désigne les serveurs têtes de pont distants pour le connecteur du groupe de routage distant comme les serveurs recensés en tant que serveurs têtes de pont sous l'onglet **Général** du groupe de routage local.

Description des restrictions et de la portée du connecteur

Si vous devez contrôler l'accès à des connecteurs spécifiques, soit par groupe, soit par zone géographique spécifique, vous avez deux possibilités :

- **Utiliser la portée du connecteur pour limiter son utilisation**. Par définition, seuls les utilisateurs d'un groupe de routage spécifique peuvent utiliser le connecteur de ce groupe de routage. Cependant, vous pouvez également désigner une portée de groupe de routage pour un autre type de connecteur, comme un connecteur SMTP, afin que seuls les utilisateurs d'un groupe de routage particulier puissent utiliser le connecteur SMTP. Utilisez un connecteur SMTP avec une portée de groupe de routage pour garantir que les utilisateurs présents à emplacement spécifique puissent toujours utiliser ce connecteur SMTP.
- **Créer une restriction sur le connecteur**. Vous pouvez limiter l'accès à tous les types de connecteurs en utilisant l'onglet **Restrictions de remise** des propriétés du connecteur. Vous pouvez désigner un groupe de distribution qui possède des droits explicites d'utilisation de ce connecteur ou vous pouvez désigner un groupe de distribution dont les droits d'accès au connecteur ont été explicitement refusés.

Utilisation de la portée du connecteur pour restreindre l'utilisation

Pour comprendre l'incidence de la topologie de votre routage et de la portée du connecteur sur le flux des messages, considérez une entreprise appelée Contoso, S.A. (contoso.com) localisée exclusivement aux États-Unis et possédant deux sièges, l'un dans le Colorado et l'autre dans le Maine (Figure 5.7). Tous les serveurs sont connectés par un réseau à grande vitesse mais un connecteur de fax et un connecteur SMTP existent dans chaque site. Si les connecteurs de fax possèdent une portée sur le plan de l'organisation, les utilisateurs au Colorado peuvent utiliser le connecteur du fax dans le Maine et risquent de supporter des coûts longue distance. En outre, l'administrateur Contoso souhaite que tous les utilisateurs du Maine utilisent le connecteur SMTP vers Internet situé sur le site du Maine et que tous les utilisateurs du Colorado utilisent les connecteurs de fax et SMTP locaux. Dans ce cas, en dépit de la connectivité réseau élevée entre tous les serveurs, il est logique d'utiliser les groupes de routage et de limiter les portées du connecteur au groupe de routage approprié.

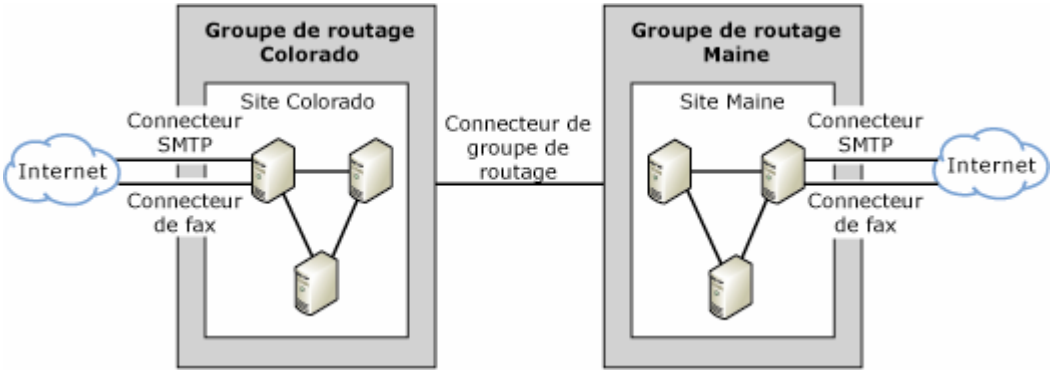


Figure 5.7 Topologie de Contoso.com

Dans cette topologie, chaque site possède les connecteurs suivants :

- Un connecteur SMTP vers Internet avec une portée de groupe de routage.
- Un connecteur de fax avec une portée de groupe de routage.

- Un connecteur de groupe de routage qui permet à tout serveur du groupe de routage d'envoyer des message par ce connecteur et qui désigne les trois serveurs du site distant comme serveurs têtes de pont distants. Comme tous les serveurs de chaque site partagent la même connectivité réseau, il est logique de tous les désigner comme serveurs têtes de pont afin que les serveurs puissent communiquer de point à point.

Utilisation des limites de remise pour restreindre l'utilisation

Vous pouvez limiter l'utilisation de votre connecteur à un groupe particulier d'utilisateurs. L'avantage de faire appel aux limites de remise pour restreindre l'utilisation est que cette option évite d'avoir à créer un groupe de routage. L'inconvénient de cette restriction est que pour chaque message envoyé par l'intermédiaire de ce connecteur, le groupe de distribution doit être élargi à ses destinataires individuels pour appliquer la restriction. Cet élargissement se révèle coûteux sur le plan des performances. Par conséquent, il est recommandé d'utiliser l'onglet **Restrictions de remise** sur un connecteur dans les cas où le groupe de distribution est de petite taille ou lorsque vous êtes certain que l'impact sur les performances est acceptable pour vos utilisateurs.

> **Important** Sachez que restreindre les remises nécessite beaucoup de ressources processus et peut affecter les performances des serveurs.

Une clé du Registre sur le serveur tête de pont basé sur Exchange 2003 (source du connecteur en cours de vérification) contrôle les fonctionnalités vérifiant la restriction. Si vous devez configurer un connecteur pour qu'il limite les expéditeurs de données vers la liaison désignée, vous devez ajouter manuellement la valeur de Registre chargée de vérifier la restriction.

Pour activer les clés de Registre pour les restrictions de remise

> **Avertissement** Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données importantes.

1. Démarrez l'Éditeur du Registre. À une invite de commandes, tapez **Regedt32.exe**.
2. Accédez à et sélectionnez la clé suivante dans le Registre :

   HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/RESvc/Parameters/
3. Dans le menu **Edition**, cliquez sur **Ajouter une valeur**, puis ajoutez la valeur de Registre suivante :

   ```
   Value Name: CheckConnectorRestrictions
   Data Type: REG_DWORD
   Date: 1
   Radix: Decimal
   ```
4. Quittez l'Éditeur du Registre : Dans le menu **Registre**, cliquez sur **Quitter**.
5. Après activation du paramètre de la clé du Registre, redémarrez les services suivants sur votre serveur Exchange :
   - Microsoft Exchange - Piles MTA (MSExchangeMTA)
   - Microsoft Exchange - Moteur de routage (RESvc)
   - Protocole SMTP (SMTPSVC)

Après activation de la clé du Registre et le redémarrage des services ci-dessus, vous pouvez définir des restrictions de remise sur les propriétés du connecteur à l'aide de l'onglet **Restrictions de remise** (Figure 5.8).

Remarque Vous pouvez également désigner des utilisateurs spécifiques ou des groupes de distribution fondés sur une requête sous l'onglet **Restrictions de remise**. Cette approche n'est pas recommandée car chaque utilisateur est ajouté sous la forme d'une entrée dans la table d'état des liaisons dont la taille peut devenir très importante. Une table volumineuse d'état des liaisons peut avoir une incidence sur le réseau et les performances car elle doit être répliquée sur tous les autres serveurs de l'organisation.

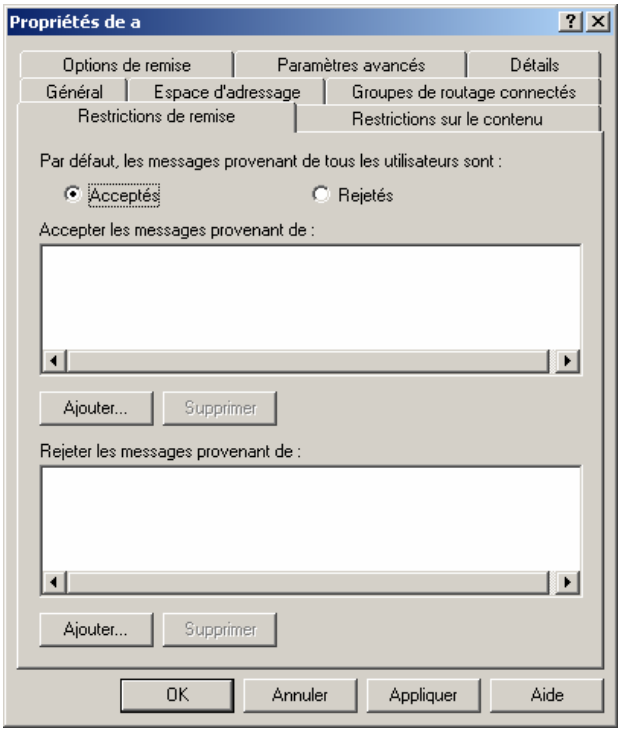


Figure 5.8 Onglet Restrictions de remise de la boîte de dialogue Propriétés du connecteur SMTP

Désignation d'un maître de groupe de routage

Lorsque vous créez un groupe de routage, le premier serveur dans ce groupe est affecté au rôle de maître de groupe de routage. Le maître de groupe de routage maintient les informations actuelles sur l'état des liaisons pour son groupe de routage et propage celui-ci aux autres serveurs dans le groupe de routage. Le maître de groupe de routage surveille la configuration de routage qui est écrite dans Active Directory pour son groupe de routage uniquement. Les serveurs membres peuvent communiquer des informations sur la disponibilité des serveurs et sur l'état du connecteur au maître de groupe de routage. Par exemple, si un serveur membre essaie de contacter un autre serveur dans groupe de routage différent par l'intermédiaire d'un connecteur et que cette liaison n'est pas disponible, le serveur membre notifie immédiatement le maître du groupe de routage. Par ailleurs, lorsqu'un serveur autre que le maître reçoit de nouvelles informations sur l'état des liaisons, il les transfère immédiatement au maître de groupe de routage, de sorte que les autres serveurs puissent recevoir les informations relatives aux modifications du routage.

Lorsque vous désignez un maître de groupe de routage, veillez à ce que le serveur choisi possède un accès approprié au contrôleur de domaine car c'est à ce niveau qu'il lit les informations de configuration stockées dans Active Directory. En outre, lorsqu'une modification se produit dans la configuration de son groupe de routage, le Gestionnaire système Exchange écrit ces informations directement dans Active Directory, puis le

contrôleur de domaine notifie le maître de groupe de routage de cette modification. Le maître de groupe de routage propage ensuite ces informations à tous les serveurs membres.

Au sein d'un groupe de routage, le maître et les autres serveurs Exchange communiquent les informations sur l'état des liaisons par l'intermédiaire du port TCP/IP 691. Toutefois, la communication des informations sur l'état des liaisons entre les groupes de routage est différente. Si le maître du groupe de routage n'est pas un serveur tête de pont pour le groupe de routage, le maître envoie les informations sur l'état des liaisons au serveur tête de pont du groupe par l'intermédiaire du port TCP/IP 691. Le serveur tête de pont transmet ensuite ces informations (sur le port TCP/IP 25 à l'aide de SMTP et du verbe X-LINK2STATE) vers les serveurs tête de pont des autres groupes de routage.

> **Remarque** Pour plus d'informations sur les informations des liaisons et leur mise à jour, consultez le chapitre 15, « Concepts avancés sur l'état des liaisons ».

Si vous ne souhaitez pas que le premier serveur installé dans le groupe de routage soit le maître du groupe de routage (configuration par défaut), vous pouvez spécifier un autre maître du groupe de routage à l'aide de la procédure décrite ci-après.

> **Remarque** Ne changez pas le maître de groupe de routage fréquemment. Lorsque vous désignez un nouveau maître de groupe de routage, tous les serveurs membres doivent se reconnecter et cette modification nécessite la réplication de la table d'état des liaisons dans l'ensemble de l'organisation, ce qui augmente le trafic réseau.

Pour spécifier un autre serveur maître du groupe de routage

- Dans le Gestionnaire système Exchange, développez le groupe de routage, cliquez sur **Membres**, cliquez avec le bouton droit sur un serveur Exchange que vous souhaitez désigner comme maître, puis sélectionnez **Définir comme maître**.

  Important Il n'existe aucun basculement automatique des maîtres de groupe de routage. Si un maître de groupe de routage ne fonctionne pas, vous devez configurer manuellement un nouveau maître de groupe de routage dans le Gestionnaire système Exchange. Lorsqu'un maître de groupe de routage tombe en panne, les autres serveurs dans le groupe utilisent les dernières informations connues sur l'état des liens jusqu'à ce qu'un maître de groupe de routage devienne disponible ou qu'un autre maître soit désigné. Pour plus d'informations sur l'échec d'un maître de groupe de routage, consultez l'article 261827 (en anglais) de la Base de connaissances Microsoft, « XCON : Consequences of an Unavailable Routing Group Master Server » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=261827).

Configuration de routage avancée

Cette section présente des rubriques relatives à la configuration de routage avancée. Elle explique les points suivants :

- **Utilisation des connecteurs pour l'équilibrage de la charge et le basculement** Configurations possibles pour permettre l'équilibrage de la charge et le basculement entre des connecteurs.
- **Configuration de l'état des liaisons avancée** Scénarios spécifiques pour la désactivation ou la suppression des informations de l'état des liaisons.

Utilisation des connecteurs pour l'équilibrage de la charge et le basculement

Le routage utilise les coûts associés aux connecteurs de groupe de routage afin de déterminer une remise optimale des messages en interne. Le routage utilise également les coûts associés aux connecteurs SMTP et X.400 afin de déterminer la méthode optimale de remise des messages externes. Il est important de comprendre que le routage sélectionne toujours le connecteur le plus proche de l'espace d'adressage, puis le coût le moins

élevé. Vous pouvez utiliser également des connecteurs pour équilibrer la charge des messages ou pour configurer des connecteurs pour le basculement.

L'inconvénient de l'utilisation des connecteurs pour l'équilibrage de la charge ou le basculement est que les deux configurations augmentent la taille de la table d'état des liaisons et répliqué dans l'organisation Exchange. N'oubliez pas que plus la table d'état des liaisons est volumineuse, plus grandes sont les exigences en matière de performance du système.

Configuration des connecteurs pour l'équilibrage de la charge

Si vous voulez configurer un connecteur pour équilibrer la charge des requêtes entre deux ou plusieurs serveurs têtes de pont, créez un connecteur unique avec l'espace d'adressage souhaité, par exemple, * pour un connecteur SMTP, puis désignez deux serveurs Exchange et serveurs virtuels SMTP différents comme serveurs têtes de pont. Le routage choisit le serveur tête de pont de manière aléatoire et équilibre la charge efficacement des requêtes envoyées par l'intermédiaire de ce connecteur. Cependant, si un message parvient à un de ces serveurs têtes de pont et que ce serveur n'est plus disponible, le routage ne choisit pas automatiquement l'autre chemin de routage. Les messages sont simplement mis en files d'attente jusqu'à ce que le serveur soit disponible. Il n'y a pas de reroutage entre les serveurs têtes de pont une fois qu'un message parvient au serveur tête de pont approprié.

L'état des liaisons contient uniquement un état du connecteur et un connecteur est toujours considéré comme disponible si un serveur tête de pont est disponible. Si un serveur tête de pont n'est plus disponible, le routage considère toujours ce connecteur comme un chemin valide et choisit de manière aléatoire entre les serveurs têtes de pont disponibles.

Configuration des connecteurs pour le basculement

Si vous souhaitez configurer des connecteurs pour qu'ils basculent automatiquement, vous pouvez créer deux connecteurs séparés sur des serveurs têtes de pont différents, chacun affecté d'un coût différent. C'est le serveur tête de pont local qui détermine l'état des liaisons pour un connecteur. Si le serveur tête de pont sur le connecteur préféré offrant le coût le moins élevé n'est pas disponible, ce connecteur est considéré comme indisponible et le routage choisit automatiquement le deuxième connecteur. Lorsque le serveur tête de pont hébergeant le connecteur offrant le coût moins élevé est disponible, les serveurs Exchange l'utilisent à nouveau.

Si vous utilisez deux connecteurs offrant le même coût, les serveurs Exchange choisissent de manière aléatoire quel serveur tête de pont et quel connecteur utiliser. Si ce serveur tête de pont n'est plus disponible, les serveurs basculent vers le deuxième connecteur. Toutefois, dès que le premier serveur tête de pont est disponible, les serveurs n'exécutent pas de restauration vers ce serveur car le chemin de routage possède le même coût que le serveur déjà utilisé.

Suppression du trafic d'état des liaisons pour les connecteurs

Exchange 2003 supprime le trafic d'état des liaisons si les connexions oscillent ou en l'absence d'un chemin de routage alternatif vers un groupe de routage de nœud feuille. Ces améliorations réduisent la quantité de trafic générée par l'état des liaisons. De plus, si vous utilisez l'option par défaut **Tous les serveurs locaux peuvent envoyer des messages via ce conn.** pour un connecteur de groupe de routage, l'état de ce connecteur est toujours marqué comme en service. L'utilisation de cette option permet de supprimer efficacement le trafic d'état des liaisons généré par des modifications apportées à l'état de ce connecteur. Cependant, cette option n'est pas possible pour les connecteurs SMTP ou X.400.

Dans les environnements dont la bande passante est très faible et la latence élevée, certaines entreprises choisissent de supprimer le trafic d'état des liaisons entre les groupes de routage. Vous pouvez supprimer le trafic d'état des liaisons sur des serveurs individuels pour tous les connecteurs en modifiant une valeur de clé du Registre. Lorsque vous supprimez le trafic d'état des liaisons sur un serveur, celui-ci ignore les modifications d'état des liaisons sur les connecteurs dont il est un serveur tête de pont. Les informations d'état des liaisons destinées à des connecteurs sur d'autres serveurs sont toujours mises à jour, et les informations d'état des liaisons d'organisation sont toujours propagées entre les serveurs de l'organisation ; cependant, le serveur dont le trafic d'état des liaisons est supprimé n'envoie pas d'informations concernant ses connecteurs. Le tableau 5.4 répertorie les avantages et les inconvénients liés à la suppression du trafic d'état des liaisons.

La suppression du trafic d'état des liaisons sur un serveur est soumise aux conditions suivantes :

- Vous disposez d'un connecteur dont le statut n'est pas important pour le reste des autres serveurs de l'organisation Exchange (par exemple, un connecteur utilisé exclusivement par un groupe de routage ou un petit nombre de serveurs chargés d'envoyer des messages sur Internet).
- Si vous rencontrez des problèmes réseau qui font osciller un connecteur entre l'état disponible et indisponible. Gardez à l'esprit que, dans Exchange 2003, une connexion oscillante correspond à un connecteur qui change d'état deux fois (en service et hors service) en l'espace d'un intervalle d'état des liaisons (10 minutes par défaut). Si un connecteur est marqué comme non disponible après l'intervalle d'état des liaisons, puis est disponible après un laps de temps, le trafic d'état des liaisons est généré. Également, si votre organisation Exchange contient des serveurs Exchange 2000, ces serveurs ne disposent pas des améliorations d'état des liaisons fournies par Exchange 2003, ils génèrent donc du trafic pour les liaisons oscillantes.

Tableau 5.4 Avantages et inconvénients liés à la suppression du trafic d'état des liaisons

Avantages	Inconvénients
La suppression du trafic d'état des liaisons est relativement simple à configurer et peut s'appliquer aux serveurs individuels pour des conditions isolées.	Vous ne pouvez pas créer des chemins redondants ou des connecteurs alternatifs sur un serveur où le trafic d'état des liaisons est supprimé. Les modifications de l'état des liaisons sur le connecteur principal ne sont jamais détectées ; par conséquent, les messages ne sont pas redirigés vers un autre connecteur car le routage part du principe que le connecteur principal est disponible.
La suppression du trafic d'état des liaisons sur un serveur peut réduire le trafic réseau causé par des modifications fréquentes. Une réduction du trafic réseau est très avantageuse dans les situations où la bande passante est très limitée. L'avantage réel qu'offre la réduction du trafic dépend de la taille de l'organisation Exchange et de la fréquence des modifications de l'état des liaisons répliquées.	La suppression du trafic d'état des liaisons sur un serveur unique n'élimine pas complètement le trafic d'état des liaisons entre les groupes de routage.

Pour supprimer les informations sur l'état des liaisons sur un serveur

Il est important de comprendre que la modification de cette clé du Registre n'empêche pas la propagation de la table d'état des liaisons entre les serveurs. Celle-ci ne supprime que le trafic d'état des liaisons causé par une modification de l'état du connecteur.

> **Avertissement** Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données importantes.

1. Démarrez l'Éditeur du Registre. À une invite de commandes, tapez **Regedt32.exe**.
2. Accédez à et cliquez avec le bouton droit sur la clé suivante dans le Registre :

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RESvc\Parameters
3. Dans le menu **Edition**, cliquez sur **Ajouter une valeur**, puis ajoutez la valeur de Registre suivante :

   ```
   Value Name: SuppressStateChanges
   Data Type: REG_DWORD
   Data: 1
   Radix: Decimal
   ```
4. Quittez l'Éditeur du Registre : Dans le menu **Registre**, cliquez sur **Quitter**.
5. Redémarrez les services suivants :
   - Microsoft Exchange - Moteur de routage (RESvc)
   - Service SMTP (SMTPSVC)
   - Microsoft Exchange - Piles MTA (MSExchangeMTA)

Scénarios de déploiement pour la connectivité Internet

Maintenant que vous avez configuré le flux des courriers internes, vous souhaitez sans doute vous informer sur la manière de vous connecter à Internet pour permettre à vos utilisateurs d'envoyer et de recevoir des messages Internet. Le chapitre 6 présente des scénarios de déploiement personnalisés et courants pour la connectivité Internet.

Les scénarios de déploiement courants décrivent des configurations standard utilisées par des entreprises pour se connecter à Internet au nombre desquelles figurent l'utilisation de Microsoft® Exchange dans sa configuration par défaut, l'utilisation d'un serveur à double hébergement, d'un serveur tête de pont Exchange derrière un pare-feu et l'utilisation d'un serveur de relais Microsoft Windows®.

Les scénarios de déploiement personnalisés incluent des topologies qui répondent à des besoins particuliers comme l'utilisation d'un fournisseur de services réseau, la configuration de la collaboration de messageries entre forêts et le partage de domaines de messagerie SMTP (Simple Mail Transfer Protocol) ou la prise en charge de deux domaines de messagerie SMTP. Exchange Server 2003 introduit un nouvel outil, Address Rewrite, qui permet de réécrire les adresses de messagerie sortantes depuis la filiale d'une entreprise. Par conséquent, lors d'une fusion ou d'un rachat, tous les utilisateurs affichent la même adresse de messagerie.

Quel que soit le scénario qui convient le mieux à votre organisation, tenez compte des conseils suivants lors de l'élaboration de votre propre implémentation :

- Si votre organisation contient plusieurs serveurs, vous devez inclure les serveurs têtes de pont de passerelle lors de la planification de votre déploiement.
- Les pare-feu offrent la plus grande sécurité en matière de connectivité Internet.
- Les connecteurs SMTP offrent une méthode évolutive et pratique de routage des messages Internet sortants.
- Dans sa configuration par défaut, le serveur virtuel SMTP par défaut convient à la plupart des scénarios.
- Si vous utilisez plusieurs serveurs virtuels SMTP sur un seul serveur Exchange, configurez-les soigneusement. Par défaut, plusieurs serveurs virtuels ne peuvent pas communiquer entre eux. Pour assurer un flux des messages correct, vous devez les configurer de façon appropriée pour permettre le routages des messages entre les serveurs. De plus, chaque serveur virtuel SMTP doit être configuré avec une adresse IP (Internet Protocol) et une combinaison de ports uniques. Généralement, tous les serveurs virtuels SMTP nécessitent le port 25, vous devez donc leur attribuer des adresses IP uniques.

  > **Remarque** Certaines entreprises configurent plusieurs serveurs virtuels sur un serveur tête de pont où une carte d'interface réseau (NIC) accepte les messages Internet entrants et une autre carte se charge du routage des messages Internet sortants. Pour plus d'informations sur cette configuration, consultez la section « Utilisation d'un serveur Exchange à double hébergement comme passerelle Internet » plus loin dans ce chapitre.

Procédures du chapitre 6

Le tableau 6.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 6.1 Procédures du chapitre 6 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Démarrer l'Assistant Messagerie Internet	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Configurer un serveur Windows Server™ 2003 comme serveur de relais ou hôte actif	Membre du groupe Administrateurs local.
Permettre la réécriture d'adresses à l'aide de l'outil exarcfg	Membre du groupe Administrateurs local.
Créer un contact dans les services d'annuaire Microsoft Active Directory®	Membre du groupe Administrateurs local.
Afficher le paramètre qui détermine si Exchange fait autorité	Membre du groupe d'administrateurs locaux et membre d'un groupe auquel le Rôle Administrateurs Exchange Affichage seul a été appliqué au niveau de l'organisation.
Modifier la stratégie de destinataire par défaut	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Créer une stratégie de destinataire de priorité supérieure avec le domaine de messagerie partagée	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Modifier une stratégie de destinataire existante pour le domaine SMTP que vous voulez partager	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Créer une nouvelle stratégie de destinataire pour un domaine de messagerie SMTP qui ne figure pas dans une stratégie de destinataire	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Créer un connecteur SMTP pour router les messages vers un hôte spécifique	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Partager tous les espaces d'adressage dans votre organisation Exchange	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Créer le compte qui servira à l'authentification entre forêts	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Configurer un connecteur et exiger une authentification pour l'authentification entre forêts	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Restreindre l'accès par adresse IP sur le serveur tête de pont récepteur	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Configurer un serveur virtuel SMTP afin de résoudre les adresses de messagerie anonymes	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Procédure	Autorisations ou rôles requis
Permettre à un serveur Exchange d'accepter les propriétés de message étendues envoyées de façon anonyme	Membre du groupe Administrateurs local.
Permettre à un serveur virtuel SMTP d'accepter les propriétés de message étendues envoyées de façon anonyme	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Scénarios de déploiement courants

Cette section présente des scénarios de déploiement courants pour la connectivité Internet. Les scénarios sont présentés par ordre de complexité en commençant par la configuration la plus simple (un serveur Exchange unique dans sa configuration par défaut). Le tableau 6.2 résume chacun de ces scénarios courants.

Tableau 6.2 Résumés des scénarios de déploiement courants pour la connectivité Internet

Topologie	Idéale pour	Avantages	Considérations
Serveur Exchange unique dans sa configuration par défaut	Petite entreprise avec un nombre restreint d'utilisateurs	L'utilisation de la configuration par défaut ne nécessite aucune configuration supplémentaire après l'installation d'Exchange.	Cette topologie n'offre pas la meilleure protection que permet un pare-feu. Votre serveur Exchange est exposé sur Internet.
Serveur Exchange à hébergement double	Petite entreprise avec un nombre restreint d'utilisateurs	Offre une configuration sécurisée derrière un pare-feu.	Cette topologie doit s'utiliser en association à un pare-feu. Sinon, votre serveur Exchange est toujours exposé sur Internet. Envisagez d'utiliser les stratégies de sécurité du protocole Internet (IPSec) pour filtrer les ports sur la carte d'interface réseau Internet.
Utilisation d'un serveur tête de pont Exchange derrière un pare-feu	Toutes les entreprises, quelles que soit leur taille	L'utilisation d'un serveur tête de pont dédié pour les messages Internet isole le trafic Internet. Un pare-feu protège votre intranet.	Normalement, un serveur tête de pont est déployé dans les grandes entreprises. Comme le serveur n'héberge pas de boîtes aux lettres, il risque d'être sous utilisé dans les petites

Topologie	Idéale pour	Avantages	Considérations
			entreprises.
Utilisation d'un serveur tête de pont Exchange pour envoyer des messages à un serveur de relais sur un réseau de périmètre	Moyennes et grandes entreprises avec des environnements multiserveurs	Offre les mêmes avantages qu'un serveur tête de pont Exchange derrière un pare-feu, mais joute une couche supplémentaire en matière de sécurité en isolant votre serveur SMTP d'Internet. Un serveur de relais SMTP, plutôt qu'un serveur Exchange chargé de la gestion des messages Internet, est dans un réseau isolé. Vos informations utilisateur sont sécurisées sur votre serveur Exchange derrière un pare-feu.	Cette topologie demande davantage de configuration et d'installation que les scénarios répertoriés ci-dessus.

Remarque Pour les petites entreprises qui veulent une solution réseau complète qui fournit un programme d'installation unifié pour la messagerie, la planification de groupe, le fax et la base de données ainsi qu'une connectivité Internet partagée pour un environnement comptant jusqu'à cinquante ordinateurs, Microsoft Windows Small Business Server 2003 représente sans doute une solution appropriée. Pour plus d'informations sur Small Business Server, consultez le site Web de Small Business Server (http://go.microsoft.com/fwlink/?LinkId=23456).

Utilisation d'un serveur Exchange unique dans sa configuration par défaut

Ce scénario décrit la remise des messages Internet par Exchange dans sa configuration par défaut.

Configuration de base

Dans ce scénario, vous devez disposer des éléments suivants :

- Une connexion permanente à Internet.
- Un serveur DNS (Domain Name System) qui peut résoudre des noms de domaine externes et un serveur DNS sur Internet avec un enregistrement de serveur de messagerie (MX) qui pointe vers votre serveur Exchange.
- Une stratégie de destinataire configurée ave le domaine de messagerie SMTP pour lequel vous souhaitez que le serveur Exchange reçoive des messages.

Messages Internet entrants

Lorsque vous utilisez un serveur Exchange unique dans sa configuration par défaut, les messages Internet entrants transitent vers le serveur Exchange de la manière suivante :

1. Le serveur SMTP distant interroge le DNS pour la résolution de l'enregistrement MX de votre domaine de messagerie et pour obtenir l'adresse IP de votre serveur Exchange.
2. Le serveur SMTP distant se connecte ensuite à votre serveur Exchange sur le port 25, le port accepté par votre serveur virtuel SMTP par défaut.
3. Votre serveur SMTP par défaut vérifie que le domaine sur les messages entrants correspond à un domaine SMTP dans ses stratégies de destinataire.
4. Votre serveur SMTP par défaut accepte ensuite le message et le remet au destinataire.

Messages Internet sortants

Lorsque vous utilisez un serveur Exchange unique dans sa configuration par défaut, les messages Internet sortants quittent le serveur de la manière suivante :

Un utilisateur interne envoie un message à un utilisateur externe comme destinataire.

5. À partir de ses informations de stratégie de destinataire, le serveur virtuel SMTP par défaut détermine que le message est destiné à un domaine distant.
6. Comme l'utilisateur interne est authentifié, le serveur virtuel SMTP par défaut accepte le message pour une remise sortante. N'oubliez pas que, par défaut, le serveur virtuel SMTP autorise le relais des messages uniquement pour des utilisateurs authentifiés.
7. Le serveur virtuel SMTP par défaut interroge le DNS pour résoudre l'enregistrement MX du serveur de messagerie distant vers l'adresse IP de ce serveur.
8. Le serveur virtuel SMTP par défaut se connecte au serveur SMTP distant sur le port 25 et commence la remise.

Utilisation d'un serveur Exchange à double hébergement comme passerelle Internet

Ce scénario décrit la prise en charge d'une configuration d'un serveur Exchange à double hébergement qui sert de serveur de passerelle pour l'organisation Exchange. Ce serveur peut traiter des messages individuellement ou peut fonctionner comme serveur tête de pont pour d'autres serveurs dans l'organisation. Pour des raisons de sécurité, vous devez utiliser cette configuration derrière un pare-feu.

Configuration de base

La configuration de base se compose d'une passerelle de messagerie configurée avec deux interfaces réseau ; cette passerelle fonctionne comme le point de connexion unique entre votre intranet et Internet.

Les listes suivantes fournissent les configurations générales requises pour les deux serveurs virtuels et le connecteur SMTP :

> **Remarque** Si vous configurez deux serveurs virtuels sur un serveur Exchange unique, vérifiez que vous utilisez une combinaison unique d'adresses et de ports IP. Ne configurez aucun des serveurs virtuels pour qu'ils utilisent la valeur par défaut de toutes les adresses IP disponibles.

Serveur virtuel 1

- Configurez le serveur virtuel 1 comme le serveur tête de pont pour le connecteur SMTP.
- Configurez le serveur virtuel 1 pour qu'il utilise les serveurs DNS externes par l'intermédiaire de la liste de serveurs DNS externes.
- Liez le serveur virtuel 1 à une adresse IP intranet sur le port 25.
- Entrez le domaine de l'entreprise local (par exemple, contoso.com).

Serveur virtuel 2

- Configurez le serveur virtuel 2 pour qu'il ne relaie pas de messages (configuration par défaut). Pour plus d'informations sur les restrictions de relais par défaut, consultez la section « Vérification des restrictions de relais par défaut sur votre serveur virtuel SMTP entrant » au chapitre 7.
- Configurez le serveur virtuel 2 pour autoriser l'accès anonyme (configuration par défaut). Pour plus d'informations sur l'autorisation de l'accès anonyme, consultez la section « Autorisation d'accès anonyme sur le serveur virtuel sortant » au chapitre 7.
- Liez le serveur virtuel 2 à une adresse IP Internet sur le port 25.
- Sélectionnez le domaine de l'entreprise local (par exemple, contoso.com).

Connecteur SMTP

- Configurez le connecteur SMTP pour utiliser le DNS afin de router vers chaque espace d'adressage sur le connecteur.
- Hébergez le connecteur SMTP dans le serveur virtuel 1 en le définissant comme le serveur tête de pont.
- Créez un espace d'adressage * (astérisque) ou un équivalent.
- Utilisez deux cartes d'interface réseau (NIC) — une carte externe et une carte interne.
- Vérifiez qu'il n'existe aucune configuration de routage IP entre les deux réseaux sur votre serveur. (Il s'agit de la configuration par défaut.)

  Pour plus d'informations sur la configuration d'un connecteur SMTP, consultez la section « Configuration d'un connecteur SMTP » au chapitre 7.

Messages Internet entrants

Les messages circulent dans une organisation Exchange de la manière suivante :

1. Les messages provenant d'Internet utilisent l'adresse IP Internet pour envoyer des messages aux destinataires du domaine local.
2. Le serveur virtuel 2 surveille les messages destinés à cette adresse IP Internet et reçoit tous les messages Internet entrants. Comme le serveur virtuel 2 n'est pas configuré pour relayer les messages, celui-ci rejette les messages qui ne sont pas dirigés vers le domaine de l'entreprise (par exemple, contoso.com).
3. Lorsque le serveur virtuel 2 reçoit un message d'Internet destiné à un hôte à l'intérieur du domaine local, il contacte le service d'annuaire Microsoft Active Directory® par l'intermédiaire de la carte d'interface réseau interne pour déterminer la destination du message. Par conséquent, les messages reçus par le serveur virtuel 2 sont envoyés directement vers l'hôte interne ou vers un autre serveur tête de pont pour une remise à un autre groupe de routage.

   Remarque Bien que le serveur virtuel 2 surveille les messages entrants d'une adresse IP externe, celui-ci utilise l'adresse IP appropriée pour le routage des messages basée sur les entrées du tableau de routage. Le serveur virtuel 2 utilise uniquement les services DNS internes pour la résolution de noms. Le serveur virtuel 2 n'est pas configuré avec une liste externe de serveurs DNS, il ne résout donc pas les adresses

externes. Il rejette tous les messages avec des adresses vers un domaine différent de celui de l'entreprise (dans ce cas, contoso.com).

Messages Internet sortants

Les messages sortent d'une organisation Exchange de la manière suivante :

1. Un utilisateur envoie un message à un destinataire externe.
2. Comme ce message est sortant, il utilise le connecteur SMTP hébergé sur le serveur virtuel 1.
3. Lorsque le serveur virtuel 1 reçoit un message destiné à un domaine distant, il utilise la liste des serveurs DNS externes pour rechercher l'adresse IP du destinataire du message, puis il utilise la carte d'interface réseau externe pour remettre les messages externes. (Généralement, les adresses IP Internet externes ne sont pas disponibles sur un serveur DNS interne.)

   Important Bien que le serveur virtuel 1 soit configuré pour surveiller l'adresse IP intranet, celui-ci utilise la carte d'interface réseau Internet pour les messages externes.

La figure 6.1 illustre le flux des messages transmis par l'intermédiaire d'un serveur à double hébergement.

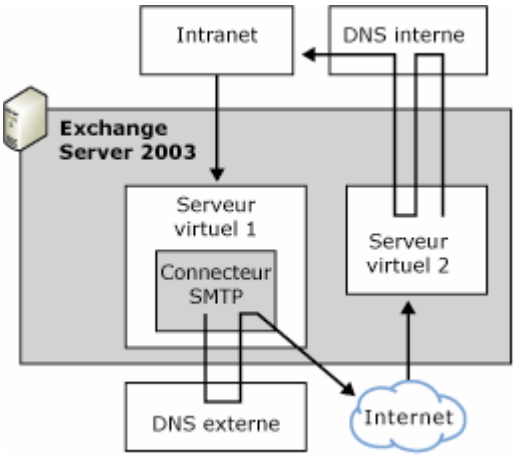


Figure 6.1 Flux des messages Internet transmis par l'intermédiaire d'un serveur de passerelle Exchange à double hébergement

Utilisation de l'Assistant Messagerie Internet pour configurer un serveur Exchange à double hébergement

Vous pouvez utiliser l'Assistant Messagerie Internet pour configurer un serveur Exchange à double hébergement. L'assistant vous guide tout au long de la configuration nécessaire et crée automatiquement un connecteur sur votre serveur virtuel SMTP sortant.

Utilisez la procédure suivante pour la configuration de l'envoi et de la réception de messages Internet sur un serveur Exchange à double hébergement possédant deux serveurs virtuels SMTP. À l'issue de l'Assistant Messagerie Internet, le serveur Exchange enverra et acceptera tous les messages Internet en fonction de la configuration que vous aurez définie dans l'assistant.

Remarque Vous ne pouvez pas utiliser l'Assistant Messagerie Internet si vous avez déjà configuré un connecteur SMTP ou créé un serveur virtuel SMTP supplémentaire sur votre serveur Exchange. Vous devez rétablir la configuration par défaut avant d'exécuter l'Assistant Messagerie Internet.

Pour démarrer l'Assistant Messagerie Internet

1. Dans le Gestionnaire système Exchange, cliquez avec le bouton droit sur votre organisation Exchange, puis cliquez sur **Assistant Messagerie Internet**.

   Remarque Pour exécuter l'Assistant Messagerie Internet, vous devez utiliser la version du Gestionnaire système Exchange livrée avec Exchange Server 2003.

2. Suivez les instructions de l'Assistant pour effectuer les tâches de configuration nécessaires à la remise des messages Internet.

L'Assistant crée un serveur virtuel SMTP supplémentaire sur votre serveur Exchange. Il configure la remise des messages Internet de la manière suivante :

- Pour configurer l'envoi des messages Internet sur un serveur, l'Assistant vous guide tout au long du processus d'affectation de l'adresse IP intranet au serveur virtuel SMTP par défaut sur lequel il crée le connecteur SMTP pour l'envoi des messages sortants. Affectez l'adresse IP intranet à ce serveur virtuel de sorte que seuls les utilisateurs internes connectés à votre intranet puissent envoyer des messages.
- Pour configurer la réception des messages Internet sur un serveur, l'Assistant vous guide tout au long du processus d'affectation d'une adresse IP Internet au serveur virtuel SMTP Internet. L'affectation d'une adresse IP Internet à ce serveur virtuel permet aux serveurs externes de se connecter à ce dernier pour l'envoi des messages Internet vers votre entreprise. De plus, vous devez posséder un enregistrement MX sur votre serveur DNS Internet qui fait référence à ce serveur.

L'Assistant Messagerie Internet effectue également les vérifications nécessaires sur votre serveur virtuel SMTP Internet pour s'assurer qu'il est correctement configuré. Il procède aux vérifications suivantes :

- Votre serveur virtuel SMTP Internet accepte les connexions anonymes.
- Votre serveur SMTP Internet n'autorise le relais des messages.

Pour plus d'informations sur l'Assistant Messagerie Internet, consultez la section « Utilisation de l'Assistant Messagerie Internet pour configurer la remise des messages Internet » au chapitre 7.

Considérations sur la sécurité

Afin d'accroître la sécurité d'une configuration de serveur de passerelle à double hébergement, prenez en compte les recommandations suivantes :

- Utilisez les stratégies de sécurité du protocole Internet (IPSec) pour filtrer les ports sur la carte d'interface réseau Internet. Pour plus d'informations sur les stratégies IPSec, consultez la documentation en ligne de Microsoft Windows 2000 ou Windows Server 2003.
- Limitez strictement les utilisateurs autorisés à se connecter au serveur. Vous pouvez simplement laisser le serveur en cours d'exécution sans clavier, souris ou écran et utiliser les Services Terminal Server pour gérer le serveur. Puis, vous autorisez l'accès au service Terminal server uniquement aux administrateurs.

L'utilisation d'un serveur Exchange à double hébergement comme serveur de passerelle dans cette configuration permet à une entreprise de limiter son exposition en minimisant les points d'entrée depuis Internet vers son intranet. Empêcher le serveur virtuel sur Internet de relayer les messages vers d'autres hôtes Internet vous permet de garantir que le serveur virtuel ne route que les messages adressés à des destinataires internes valides. Comme le serveur virtuel 1 utilise une liste externe de serveurs DNS pour router uniquement les messages Internet sortants (pas les messages internes), les problèmes liés au serveur DNS externe n'ont pas d'incidence sur le trafic des messages internes. En séparant les processus chargés de vos messages Internet entrants, des messages entrants et des messages Internet sortants, les points de défaillance de ces processus restent distincts, ce qui simplifie leur gestion.

Utilisation d'un serveur tête de pont derrière un pare-feu

Généralement, si votre organisation contient plusieurs serveurs Exchange, vous devez faire appel à un serveur tête de pont pour fournir la connectivité Internet à un groupe de routage ou à une organisation Exchange.

La figure 6.2 illustre cette topologie.

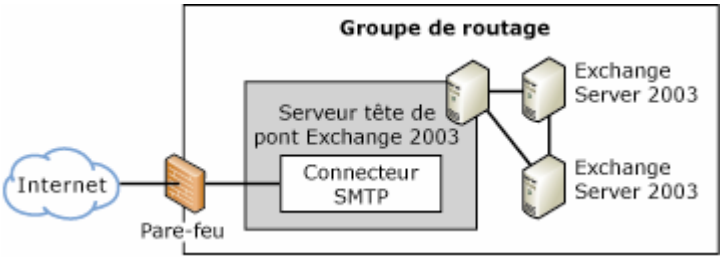


Figure 6.2 Apport de la connectivité Internet à un groupe de routage

Si vous utilisez un serveur tête de pont, il n'est pas nécessaire que chaque serveur Exchange dispose de la connectivité Internet. Cette configuration améliore la sécurité car seul le serveur tête de pont est exposé à Internet.

> **Important** Comme les serveurs de passerelle ont le plus souvent des besoins différents en matière de sécurité que les serveurs internes, vous devez examiner attentivement les risques en matière de sécurité sur vos serveurs de passerelle.

Configuration de base

La configuration de base comporte un serveur tête de pont Exchange connecté à Internet et qui possède la configuration DNS appropriée. Un connecteur SMTP est installé sur le serveur tête de pont et permet la remise des messages sortants sur Internet. De plus, afin de protéger le réseau interne, un pare-feu filtre le trafic Internet entrant et route les messages à partir des adresses IP internes et externes.

Les listes suivantes fournissent la configuration générale requise pour les serveurs DNS, le serveur tête de pont Exchange, les serveurs membres Exchange et le pare-feu :

Serveurs DNS

Exchange s'appuie sur les serveurs DNS existants dans son organisation. En particulier, Exchange utilise le DNS interne pour router les messages internes et s'appuie sur le serveur DNS interne pour transmettre et résoudre les adresses externes par l'intermédiaire d'un serveur DNS externe. Pour configurer ainsi le DNS, vérifiez que les conditions suivantes sont présentes :

- Pour que le serveur tête de pont soit identifié comme le serveur de messagerie du domaine, le serveur DNS externe de l'organisation doit contenir un enregistrement MX pour ce serveur tête de pont. Cette configuration DNS permet aux messages entrants d'être redirigés vers le serveur tête de pont.
- Le serveur DNS interne de l'organisation doit posséder un redirecteur vers son serveur DNS externe.
- Le serveur Exchange doit pointer vers le serveur DNS principal.

Pour plus d'informations sur cette configuration du DNS, consultez les sections « Vérification de la configuration du service DNS pour les messages entrants » et « Configuration du service DNS pour les messages sortants » au chapitre 4.

Serveur tête de pont Exchange

- Le serveur tête de pont Exchange possède une connexion Internet par l'intermédiaire du pare-feu sur le port 25.
- Le serveur virtuel SMTP par défaut est configuré pour l'envoi et la réception de messages Internet avec les paramètres par défaut suivants :
  - Adresse IP de port 25, port SMTP standard.
  - Configuré pour autoriser l'accès anonyme. Vous devez autoriser l'accès anonyme vers votre serveur virtuel SMTP sur votre serveur Exchange tête de pont car les serveurs SMTP Internet qui envoient des messages vers ce domaine ne s'attendront pas à s'authentifier.
  - Configuré sans le relais des messages.
- Le connecteur SMTP hébergé par le serveur virtuel SMTP est configuré avec un espace d'adressage * (astérisque) pour forcer tous les messages sortants à utiliser le serveur tête de pont.

Serveurs membres Exchange

- Ces serveurs ne disposent pas d'une connexion directe à Internet.
- Ces serveurs utilisent les paramètres par défaut sur le serveur virtuel SMTP.

Pare-feu

Le pare-feu est configuré selon les instructions de votre organisation et les spécifications du fournisseur.

Remarque Une description complète sur la configuration des pare-feu sort du cadre de ce guide. Il existe de nombreuses méthodes permettant de configurer un pare-feu pour qu'il fonctionne avec un serveur de relais SMTP. Vous pouvez autoriser soit le pare-feu, soit le serveur de relais SMTP à effectuer des traductions d'adresse réseau entre les adresses internes et externes. Dans le cadre de ce guide, le flux des messages via le pare-feu est traité comme s'il était transparent.

Messages Internet entrants

Les messages circulent dans une organisation Exchange de la manière suivante :

1. Le serveur SMTP distant interroge le DNS pour la résolution de l'enregistrement MX de votre domaine de messagerie et pour obtenir l'adresse IP de votre serveur Exchange.
2. Le serveur SMTP distant se connecte par l'intermédiaire du pare-feu au serveur virtuel SMTP sur le port 25.
3. Le serveur virtuel SMTP accepte le message entrant puis route le message vers le serveur Exchange qui héberge la boîte aux lettres de l'utilisateur ou vers un serveur tête de pont chargé de remettre le message à un autre groupe de routage.

Messages Internet sortants

Les messages sortent d'une organisation Exchange de la manière suivante :

1. Un utilisateur interne envoie un message à un destinataire dans un domaine externe.
2. Le serveur Exchange de l'utilisateur interne envoie des messages au connecteur SMTP sur le serveur tête de pont.

   Comme le connecteur est configuré avec un espace d'adressage * (qui désigne tous les domaines externes), chaque serveur Exchange dans le groupe de routage envoie des messages externes par l'intermédiaire du connecteur SMTP sur le serveur tête de pont.
3. Le connecteur SMTP utilise le DNS pour résoudre l'adresse IP du serveur de messagerie du destinataire et pour router les messages directement vers le serveur SMTP du destinataire.

Utilisation d'un serveur de relais SMTP Windows dans un réseau de périmètre

De nombreuses organisations utilisent un serveur Windows 2000 ou Windows Server 2003 SMTP dans un réseau de périmètre comme serveur de relais de messagerie pour des messages entrants et sortants Internet. Dans cette configuration, votre organisation Exchange se trouve dans un domaine interne derrière le pare-feu et le serveur SMTP se trouve dans un domaine séparé dans un réseau de périmètre. Les serveurs têtes de pont Exchange internes routent les messages sortants par l'intermédiaire d'un connecteur vers le serveur de relais SMTP chargé de la résolution DNS et de la remise des messages. De la même manière, vous pouvez configurer le serveur de relais SMTP pour qu'il accepte les messages Internet entrants et les route en interne.

La figure 6.3 illustre cette topologie.

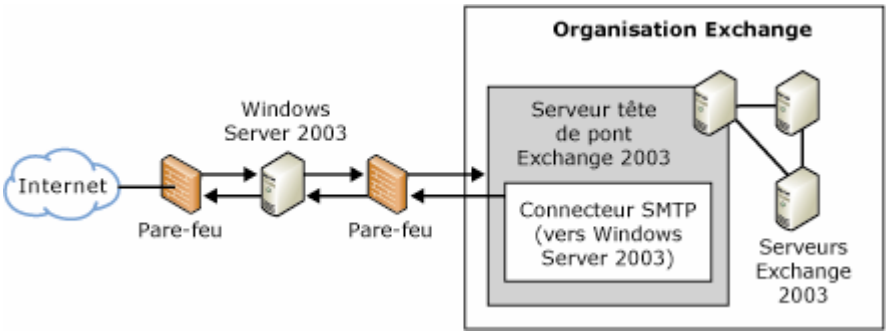


Figure 6.3 Serveur de relais Windows Server 2003 dans un réseau de périmètre

Les avantages offerts par l'utilisation d'un serveur de relais SMTP dans un réseau de périmètre incluent :

- **Exposition limitée à Internet**. Le réseau interne protège vos serveurs Exchange qui contiennent vos informations utilisateur et d'autres données de configuration.
- **Sécurité supplémentaire**. Vous pouvez installer un logiciel anti-virus pour analyser les messages entrants avant qu'ils ne pénètrent votre réseau interne.

Configuration de base

La configuration de base se compose des éléments suivants :

Serveur de relais SMTP Windows Server 2003

Le serveur de relais SMTP est configuré avec un domaine public par défaut. Il est également configuré pour relayer des messages destinés uniquement aux domaines de messagerie SMTP à l'intérieur de l'organisation Exchange — il ne relaie pas de messages vers d'autres domaines. Pour une description détaillée sur la manière de configurer le serveur de relais SMTP, consultez « Pour configurer un serveur Windows Server 2003 comme serveur de relais ou hôte actif » plus loin dans cette section.

Serveur DNS

- Votre serveur DNS externe est configuré avec un enregistrement MX qui pointe vers l'adresse IP du domaine de votre serveur de relais SMTP.
- Tous les serveurs Exchange pointent vers votre serveur DNS interne.

Serveur tête de pont Exchange

Le serveur tête de pont Exchange est connecté à Internet par l'intermédiaire du pare-feu sur le port 25.

Serveur virtuel SMTP

Le serveur virtuel SMTP est configuré pour l'envoi et la réception des messages Internet avec les paramètres par défaut suivants :

- Adresse IP de port 25 (port SMTP standard).
- Autorisation de l'accès anonyme. Vous devez autoriser l'accès anonyme vers votre serveur virtuel SMTP sur votre serveur Exchange tête de pont car les serveurs SMTP Internet qui envoient des messages vers ce domaine ne s'attendront pas à s'authentifier.
- Configuré sans relais de messages.

Connecteur SMTP

- Le serveur virtuel SMTP héberge le connecteur.
- Le connecteur est configuré avec un espace d'adressage * (astérisque) pour forcer tous les messages sortants à utiliser le serveur tête de pont Exchange.
- Le connecteur est configuré pour utiliser le serveur de relais SMTP comme hôte actif pour le relais de messages.
- Tous les autres paramètres conservent leurs valeurs par défaut.

Autres serveurs membres Exchange

- Ces serveurs ne disposent pas d'une connexion directe à Internet.
- Tous ces serveurs utilisent le serveur virtuel SMTP par défaut avec ses paramètres par défaut.

Pare-feu

Le pare-feu est configuré selon les instructions de votre organisation et les spécifications du fournisseur.

Remarque Une description complète sur la configuration des pare-feu sort du cadre de ce guide. Il existe de nombreuses méthodes permettant de configurer un pare-feu pour qu'il fonctionne avec un serveur de relais SMTP. Vous pouvez autoriser soit le pare-feu, soit le serveur de relais SMTP à effectuer des traductions d'adresse réseau (entre les adresses internes et externes). Dans le cadre de ce guide, le flux des messages via le pare-feu est traité comme s'il était transparent.

Pour configurer un serveur Windows Server 2003 comme serveur de relais ou hôte actif

1. Vérifiez que SMTP est installé sur le serveur Windows Server 2003. Pour vérifier que SMTP est installé :
   a. Dans le Panneau de configuration, double-cliquez sur **Ajout/Suppression de programmes**, puis cliquez sur **Ajouter/Supprimer des composants Windows**.
   b. Sous **Composants**, sélectionnez **Services IIS**, puis cliquez sur **Détails**.
   c. Sous **Sous-composants des Services Internet (IIS),** vérifiez que vous avez activé la case à cocher **Service SMTP**. Si la case à cocher n'est pas activée, activez-la, cliquez sur **OK**, puis terminez les instructions d'installation.
2. Dans le Gestionnaire des services Internet, ajoutez le domaine de messagerie SMTP pour lequel vous souhaitez un relais du serveur Windows. Pour ajouter le domaine SMTP :
   a. Cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Outils d'administration**, puis cliquez sur **Gestionnaire des services Internet**.
   b. Développez le serveur souhaité, puis le serveur virtuel SMTP par défaut. Par défaut, le serveur virtuel SMTP par défaut possède un domaine local avec le nom complet de domaine pour le serveur.
   c. Pour créer le domaine de messagerie SMTP entrant, cliquez avec le bouton droit sur **Domaines**, pointez sur **Nouveau**, puis cliquez sur **Domaine**.
   d. Dans **Assistant Nouveau domaine SMTP**, cliquez sur **Distant** comme type de domaine, puis sur **Suivant**.

e. Dans **Nom**, tapez le nom de domaine de votre domaine de messagerie SMTP pour votre organisation Exchange.

f. Cliquez sur **Terminer**.

3. Configurez le domaine de messagerie SMTP que vous venez de créer pour le relais :

a. Dans le Gestionnaire des services Internet, cliquez avec le bouton droit sur le domaine de messagerie SMTP, puis cliquez sur **Propriétés**.

b. Cliquez sur **Autoriser le courrier entrant à être relayé vers ce domaine**.

c. Cliquez sur **Transférer tout le courrier vers l'hôte actif**, puis tapez l'adresse IP entre crochets ([ ]) ou le nom de domaine complet du serveur Exchange chargé de la réception des messages pour le domaine. Par exemple, pour entrer une adresse IP, tapez [123.123.123.123].

d. Cliquez sur OK.

4. Spécifiez les hôtes pour lesquels vous souhaitez un relais ouvert vers tous les domaines :

a. Dans le Gestionnaire des services Internet, cliquez avec le bouton droit sur le **Serveur virtuel par défaut**, puis cliquez sur **Propriétés**.

b. Sous l'onglet Accès, cliquez sur Relais.

c. Cliquez sur Uniquement la liste ci-dessous, sur Ajoutez, puis ajoutez les hôtes que vous souhaitez voir utilisé par le serveur SMTP pour envoyer des messages.

d. Sous Ordinateur unique, spécifiez l'adresse IP du serveur tête de pont Exchange que vous voulez relayer à l'aide de ce serveur SMTP. Cliquez sur Recherche DNS pour recherche l'adresse IP du serveur spécifique.

Pour plus d'informations sur la configuration d'un serveur Windows comme serveur de relais ou hôte actif, consultez l'article 293800 (en anglais) de la Base de connaissances Microsoft, « XCON : How to Set Up Windows 2000 as a SMTP Relay Server or Smart Host » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=293800).

Messages Internet entrants

Lorsque vous utilisez un serveur de relais dans un réseau de périmètre, les messages Internet entrants transitent vers l'organisation Exchange de la manière suivante :

1. Les messages Internet entrants transitent vers le port 25 sur le pare-feu
2. Les messages sont ensuite envoyés au port 25 du serveur de relais SMTP dans le réseau de périmètre.
3. Ce serveur renvoie les messages par l'intermédiaire du pare-feu vers le serveur tête de pont Exchange.
4. Le serveur tête de pont Exchange utilise le routage interne et SMTP pour remettre des messages vers le serveur Exchange qui héberge la boîte aux lettres de l'utilisateur.

Messages Internet sortants

Lorsque vous utilisez un serveur de relais dans un réseau de périmètre, les messages Internet sortants transitent hors de l'organisation Exchange de la manière suivante :

1. Un utilisateur interne envoie un message à un utilisateur distant.
2. Le serveur Exchange sur lequel réside la boîte aux lettres de l'utilisateur transmet les messages au connecteur SMTP sur le serveur tête de pont Exchange.

3. Le connecteur SMTP relaie les messages par l'intermédiaire du pare-feu vers le serveur de relais SMTP dans le réseau de périmètre.
4. Le serveur de relais SMTP utilise le DNS pour rechercher l'enregistrement XM et l'adresse IP du serveur SMTP de l'utilisateur distant.
5. Le serveur de relais SMTP renvoie les messages par l'intermédiaire du port 25 du serveur SMTP de l'utilisateur distant.

Scénarios de déploiement personnalisés

Cette section présente deux scénarios de déploiement personnalisés ainsi que des présentations des configurations générales requises pour chacune d'entre elles.

- **Utilisation d'un fournisseur de services réseau pour envoyer et recevoir des messages.** Ce scénario explique comment configurer votre serveur Exchange pour utiliser une connexion à distance pour la remise des messages Internet.
- **Prise en charge de deux domaines SMTP et partage d'un domaine SMTP**. Ce scénario traite des problèmes qui se rencontrent habituellement lors d'une fusion ou d'un rachat. Durant les premières étapes d'un rachat, vous aurez peut-être besoin de prendre en charge deux domaines de messagerie SMTP existants ; lors des étapes finales, il est courant de partager un domaine de messagerie SMTP unique entre deux systèmes de messagerie. Cette section explique comment configurer Exchange dans ces deux cas. Elle explique également comment utiliser un nouvel outil, appelé Address Rewrite, pour réécrire les adresses de messagerie sortantes pour les utilisateurs du système de messagerie d'une filiale.

Utilisation d'un fournisseur de services réseau pour l'envoi et la réception de messages

Si votre serveur Exchange utilise une connexion distante pour l'envoi et la récupération des messages Internet, vous devez disposer d'un compte distant vers votre fournisseur de services réseau. Vous devez également configurer le service Routage et accès distant (RRAS) de Windows 2000 ou de Windows Server 2003 pour numéroter et authentifier auprès du fournisseur de services réseau à la demande. Pour plus d'informations sur la configuration de ce service, consultez l'aide de Microsoft Windows 2000 ou Windows Server 2003.

Si vous souhaitez utiliser le serveur SMTP d'un fournisseur de services réseau comme hôte actif (également appelé serveur de relais) pour remettre des messages électroniques sortants, vous pouvez vérifier les adresses des messages sortants lors de leur envoi. Il est possible d'envoyer les messages à la demande ou vous pouvez configurer une planification de remise spécifique. Pour configurer ces paramètres, utilisez l'onglet **Options de remise** des propriétés du connecteur SMTP.

Pour récupérer des messages électroniques de l'hôte actif, sous l'onglet **Paramètres avancés** des propriétés du connecteur SMTP, cliquez sur **Demander ETRN/TURN lors de l'envoi de messages**. Comme indiqué précédemment, ETRN est une commande ESMTP envoyée par un serveur SMTP pour demander à autre serveur d'envoyer les messages qu'il possède. TURN est une commande SMTP qui permet au client et au serveur d'inverser leurs rôles et d'envoyer des messages dans la direction opposée sans avoir à établir une nouvelle connexion. Cette possibilité d'inverser les rôles lors d'une session SMTP est utile car elle vous permet d'envoyer des messages puis d'émettre la commande TURN pour recevoir des messages sans avoir à rétablir une nouvelle connexion. Il est possible de spécifier des heures supplémentaires à des fins de récupération uniquement.

Si vous voulez envoyer des messages électroniques directement aux domaines distants sans utiliser le serveur de messagerie du fournisseur de services réseau comme hôte actif, vous pouvez configurer le connecteur SMTP pour qu'il utilise le DNS pour l'envoi de messages. Cependant, vous pouvez toujours récupérer des messages depuis votre fournisseur de services réseau. Pour récupérer des messages de votre fournisseur de

services réseau, sélectionnez **Demander ETRN/TURN à partir d'un autre serveur** dans l'onglet **Paramètres avancés** des propriétés du connecteur SMTP. Si vous configurez le connecteur SMTP de cette manière, vous devez configurer un calendrier de récupération.

Prise en charge de deux domaines de messagerie SMTP et partage d'un domaine de messagerie SMTP avec un autre système

Des situations particulières (fusions et rachats en particulier) nécessitent la prise en charge de deux espaces de noms et le partage d'un espace de noms avec un autre système. Pour expliquer ce genre de situation, prenons comme exemple la fusion des deux entreprises suivantes : Contoso, S.A. et Fourth Coffee. Contoso (contoso.com) rachète Fourth Coffee (fourthcoffee.com). Le processus de consolidation des espaces de noms est le suivant :

1. Contoso configure son organisation Exchange pour qu'elle accepte des messages pour le domaine non local de fourthcoffee.com. Pour plus d'informations sur l'acceptation de messages pour plusieurs domaines, consultez la section « Prise en charge de deux domaines de messagerie SMTP » plus loin dans ce chapitre.
2. Les deux systèmes partagent ensuite le domaine de messagerie SMTP contoso.com.
3. Enfin, les utilisateurs sont migrés vers une organisation Exchange unique, l'ancienne organisation ou l'ancien système sont supprimés.

Prise en charge de deux domaines de messagerie SMTP

La prise en charge de deux domaines de messagerie SMTP est un processus courant lors de la phase initiale d'une fusion ou d'un rachat. Pour illustrer la manière dont une organisation Exchange peut prendre en charge deux domaines de messagerie SMTP, considérez le même scénario de fusion concernant Contoso et Fourth Coffee. Lors des premières étapes de la fusion, Contoso continue d'utiliser son domaine de messagerie SMTP contoso.com. Cependant, pour permettre aux employés de Fourth Coffee de recevoir des messages électroniques avec leurs adresses d'origine, Contoso doit également accepter les messages pour le domaine de messagerie non local de fourthcoffee.com. La figure 6.4 illustre la prise en charge des deux domaines fourthcoffee.com et contoso.com.

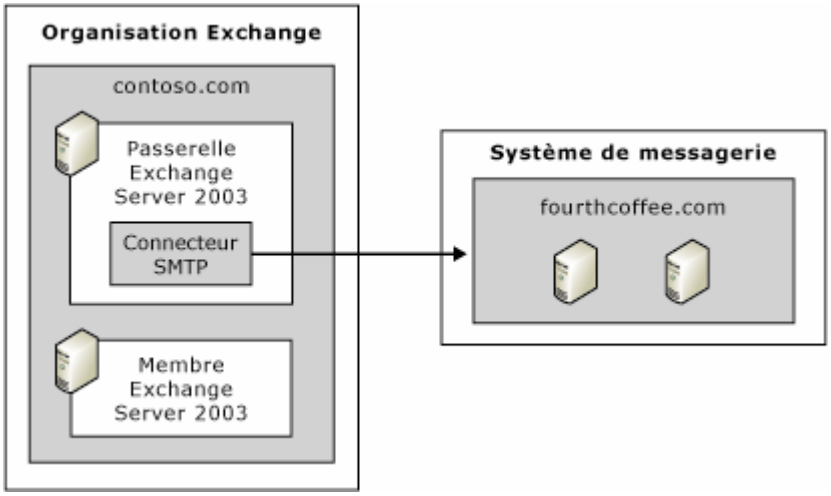


Figure 6.4 Prise en charge de deux domaines de messagerie SMTP

Pour accepter des messages pour le domaine non local de l'entreprise rachetée récemment, Fourth Coffee, un administrateur à Contoso crée un connecteur SMTP vers fourthcoffee.com. Ce connecteur est configuré avec un espace d'adressage du domaine SMTP utilisé par Fourth Coffee (fourthcoffee.com) et configuré pour relayer des messages vers ce domaine. Pour ce faire, l'administrateur ouvre les propriétés du connecteur SMTP, clique sur l'onglet **Espace d'adressage**, puis active la case à cocher **Autoriser les messages à être relayés vers ces domaines**.

> **Important** Vous devez configurer ce connecteur sur chaque serveur tête de pont qui accepte les messages Internet entrants pour le domaine fourthcoffee.com.

De plus, pour le domaine de messagerie (fourthcoffee.com) pour lequel l'administrateur veut accepter des messages, celui-ci vérifie la présence d'un enregistrement MX sur le serveur DNS Internet. Cet enregistrement MX doit pointer vers l'adresse IP du serveur de passerelle qui accepte les messages entrants. Pour plus d'informations sur le service DNS, consultez « DNS » au chapitre 3.

Utilisation d'Address Rewrite comme solution intermédiaire

Dans Exchange 2003, vous pouvez utiliser un nouvel outil appelé Address Rewrite comme étape intermédiaire dans un scénario de fusion ou de rachat. Cet outil réécrit les adresses de messagerie sur les messages sortants envoyés à Exchange et destinés aux adresses Internet ou externes (Address Rewrite est similaire à la fonctionnalité d'Exchange 5.5, ReRouteViaStore). Dans un rachat ou une fusion, vous pouvez réécrire tous les messages Internet sortants avec un seul domaine de messagerie SMTP du parent et continuer la prise en charge des domaines SMTP de l'entreprise parent et de l'entreprise rachetée jusqu'à ce que vous soyez en mesure de faire migrer tous les utilisateurs vers votre système Exchange.

Pour reprendre l'exemple du rachat de Fourth Coffee par Contoso, supposons qu'en guise de solution intermédiaire dans ce rachat, vous souhaitez que tous les utilisateurs de Fourth Coffee se mettent à utiliser le domaine de messagerie SMTP de contoso.com. Comme ces utilisateurs n'ont pas encore migré vers votre système Exchange, vous pouvez utiliser Address Rewrite pour réécrire tous les messages sortants envoyés par des utilisateurs sur le système Fourth Coffee avec l'adresse de messagerie contoso.com. Cependant, vous voulez également continuer à accepter des messages électroniques envoyés aux utilisateurs avec l'ancienne adresse de messagerie fourthcoffee.com.

Pour réécrire les adresses sortantes et continuer la prise en charge des deux domaines SMTP, effectuez les opérations suivantes :

1. Utilisez Address Rewrite pour réécrire toutes les adresses de messagerie sortantes émises par les utilisateurs Fourth Coffee.
2. Créez des contacts dans Active Directory pour tous les utilisateurs sur le système de messagerie Fourth Coffee avec une adresse cible fourthcoffee.com et une adresse SMTP principale contoso.com.
3. Créez un connecteur SMTP avec un espace d'adressage fourthcoffee.com.

Étape 1 : Utiliser Address Rewrite pour réécrire les adresses de messagerie

Après avoir configuré le système de messagerie utilisé par l'entreprise Fourth Coffee pour router les messages Internet sortants à l'aide du service SMTP par l'intermédiaire de votre serveur Exchange, vous devez ensuite activer Address Rewrite sur les serveurs virtuels SMTP dans votre organisation Exchange chargés d'accepter les messages du système de messagerie de la filiale. Dans cet exemple, vous activez la réécriture d'adresses sur tous les serveurs virtuels SMTP qui acceptent des messages de la filiale Fourth Coffee.

Les conditions suivantes doivent être présentes pour garantir le fonctionnement correct de l'outil Address Rewrite :

- Le message correspond à du courrier SMTP soumis en externe et envoyé au serveur tête de pont Exchange.
- Les messages électroniques sont destinés à Internet.

Les messages internes ou les messages envoyés à partir d'autres serveurs Exchange dans votre organisation au serveur tête de pont où la réécriture d'adresses est activée ignore celle-ci. Il y a une exception ; les messages soumis à l'aide d'Outlook Express ou tout autre client SMTP font l'objet d'une réécriture d'adresses sur ce serveur tête de pont.

N'oubliez pas que le but de cet outil est de réécrire des adresses uniquement pour les messages provenant de la filiale (messages SMTP soumis en externe) et adressés aux serveurs de messagerie de votre entreprise puis destinés à Internet.

Vous pouvez télécharger l'outil Address Rewrite (exarcfg) à partir du site Web Microsoft (http://go.microsoft.com/fwlink/?LinkId=25097). Une fois l'outil téléchargé, utilisez la procédure suivante pour activer la réécriture d'adresses sur les serveurs virtuels SMTP appropriés.

> **Important** La réécriture d'adresses doit être activée sur les serveurs virtuels SMTP têtes de pont qui reçoivent des messages du système de messagerie de la filiale. La réécriture d'adresses n'aura pas lieu si le message est d'abord soumis à un serveur virtuel SMTP sans réécriture d'adresses activée.

Pour permettre la réécriture d'adresses à l'aide de l'outil exarcfg

1. Téléchargez exarcfg dans le répertoire de votre choix.
2. Ouvrez une invite de commandes.
3. Accédez au répertoire dans lequel vous avez installé exarcfg.
4. Tapez la commande suivante :

   `exarcfg –e -s` *`server`* `–v:` *`SMTP virtual server instance number`*

   Où

   serveur est le nom de domaine complet du serveur Exchange sur lequel vous voulez activer la réécriture d'adresses et

   numéro de l'instance de serveur virtuel SMTP est le numéro correspondant à l'instance du serveur virtuel SMTP. Si vous ne définissez pas l'option –v, la commande prend l'instance du premier serveur virtuel comme valeur par défaut qui correspond le plus souvent au serveur virtuel SMTP par défaut.

Étape 2: Créer des contacts dans Active Directory pour les utilisateurs de Fourth Coffee

Dans Utilisateurs et ordinateurs Active Directory, vous devez créer un contact pour chaque utilisateur sur le système de messagerie Fourth Coffee. Chaque contact doit posséder une adresse cible fourthcoffee.com et une adresse SMTP principale contoso.com.

L'adresse cible apparaît dans l'onglet **Exchange – Général** des propriétés d'un contact. Vous définissez l'adresse SMTP principale sous l'onglet **Adresse de messagerie** des propriétés d'un contact. Vous pouvez utiliser un processus automatique pour ajouter ces contacts dans Active Directory ou vous pouvez effectuer ces opérations manuellement.

La procédure suivante montre comment créer manuellement un contact dans Active Directory en utilisant l'adresse cible du système de messagerie non Microsoft, Fourth Coffee dans cet exemple, et une adresse SMTP principale utilisée par votre organisation Exchange, Contoso dans cet exemple.

Pour créer un contact dans Active Directory

1. Ouvrez Active Directory.
2. Accédez au dossier dans lequel vous souhaitez créer vos contacts, cliquez avec le bouton droit sur ce dossier, pointez sur **Nouveau**, puis cliquez sur **Contact**.
3. Dans la page Nouvel objet, remplissez les informations de noms, puis cliquez sur **Suivant**.
4. Dans la page suivante, vérifiez que la case à cocher **Créer une adresse de messagerie Exchange** est activée.
5. Dans **Adresse de messagerie**, cliquez sur **Modifier**.
6. Dans **Nouvelle adresse de messagerie**, sélectionnez le type d'adresse de messagerie pour l'adresse cible. Dans cet exemple, sélectionnez **Adresse SMTP**, puis cliquez sur **OK**.
7. Dans **Propriétés de l'adresse Internet**, tapez l'adresse de messagerie utilisée par l'entreprise rachetée récemment. Dans cet exemple, tapez <*utilisateur*>@fourthcoffee.com, puis cliquez sur **OK**.
8. Terminez la procédure de l'Assistant pour créer un contact avec l'adresse cible correcte.
9. Cliquez avec le bouton droit sur le contact, puis cliquez sur **Propriétés**.
10. Cliquez sur l'onglet **Adresses de messagerie** et sélectionnez l'adresse SMTP de l'entreprise parent, dans ce cas, utilisateur1@contoso.com. Cliquez sur **Définir comme principale** (Figure 6.5).

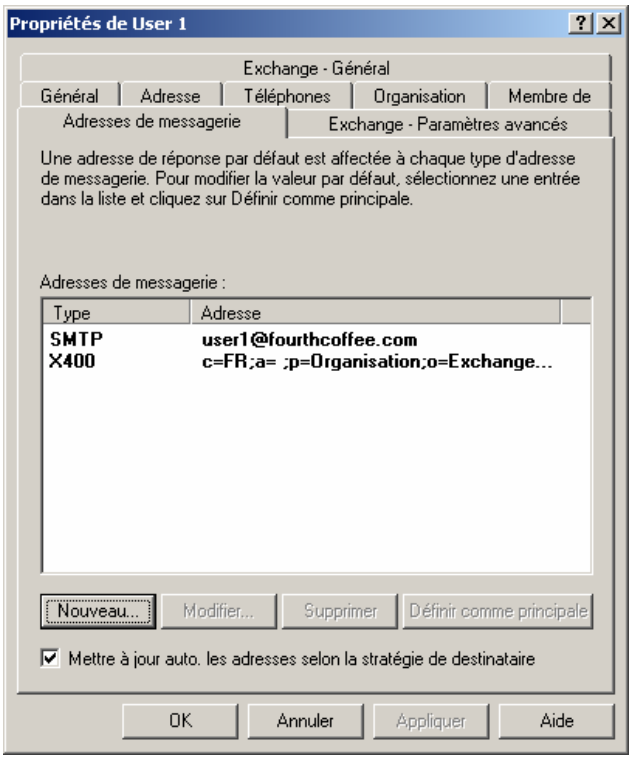


Figure 6.5 Onglet Adresses de messagerie dans la boîte de dialogue Propriétés de l'utilisateur

Étape 3 : Créer un connecteur SMTP avec un espace d'adressage fourthcoffee.com

Pour accepter des messages pour les utilisateurs de l'entreprise Fourth Coffee, un administrateur de Contoso crée un connecteur SMTP vers fourthcoffee.com et spécifie chaque serveur virtuel SMTP qui accepte les

messages Internet entrants comme serveur tête de pont local pour le connecteur. Ce connecteur est configuré avec un espace d'adressage du domaine SMTP utilisé par Fourth Coffee (fourthcoffee.com), il est configuré pour relayer les messages vers ce domaine. Pour ce faire, l'administrateur ouvre les propriétés du connecteur SMTP, clique sur l'onglet **Espace d'adressage**, puis active la case à cocher **Autoriser les messages à être relayés vers ces domaines**.

> **Remarque** Pour des raisons de performance, il est recommandé de ne pas utiliser le même serveur virtuel SMTP pour la réception des messages de la filiale ainsi que l'acceptation des messages Internet entrants. Vous devez désigner des serveurs virtuels SMTP séparés sur des serveurs Exchange distincts pour chaque fonction.

La figure 6.6 illustre la topologie utilisée par Contoso et Fourth Coffee. Remarquez qu'un serveur Exchange accepte les messages sortants de Fourth Coffee et qu'un serveur séparé route les messages entrants vers les utilisateurs Fourth Coffee. Le serveur virtuel SMTP qui accepte les messages de Fourth Coffee peut également fonctionner comme serveur de passerelle sortant, mais cela n'est pas obligatoire. Ce serveur virtuel SMTP peut soit router les messages Internet reçus des utilisateurs Fourth Coffee directement vers Internet, soit router ces messages vers le serveur de passerelle approprié.

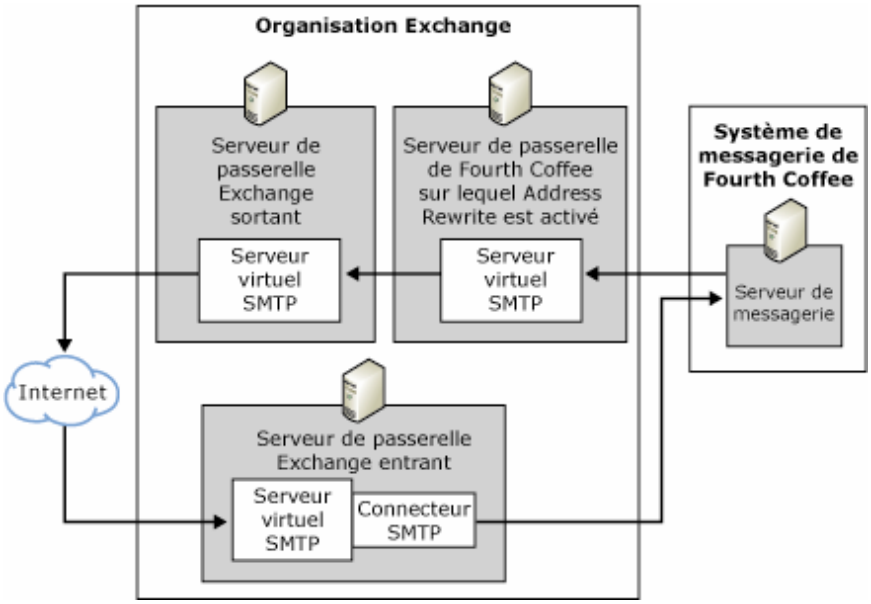


Figure 6.6 Topologie avec la réécriture d'adresses activée

Partage d'un domaine de messagerie SMTP avec un autre système

Partager un domaine de messagerie SMTP entre une organisation Exchange 2003 et un autre système de messagerie ou une autre organisation Exchange 2003 est une opération courante lors des étapes finales d'une fusion ou d'un rachat. Pour poursuivre le scénario précédent, supposez que Contoso se trouve dans les étapes finales de la consolidation de son système avec les systèmes de l'entreprise rachetés récemment, Fourth Coffee. Les boîtes de réception dans les organisations Exchange 2003 (qui contient tous les employés de Contoso) et dans l'autre système (qui contient tous les employés de Fourth Coffee) utilisent désormais le même domaine SMTP contoso.com dans leurs adresses. Dans le meilleur des cas, la meilleure façon de partager un domaine de messagerie SMTP est de permettre à Exchange d'accepter les messages entrants depuis Internet, de localiser un destinataire correspondant dans l'organisation Exchange, puis de transmettre les messages aux utilisateurs sur l'autre système de messagerie. La figure 6.7 illustre un domaine partagé avec un autre système.

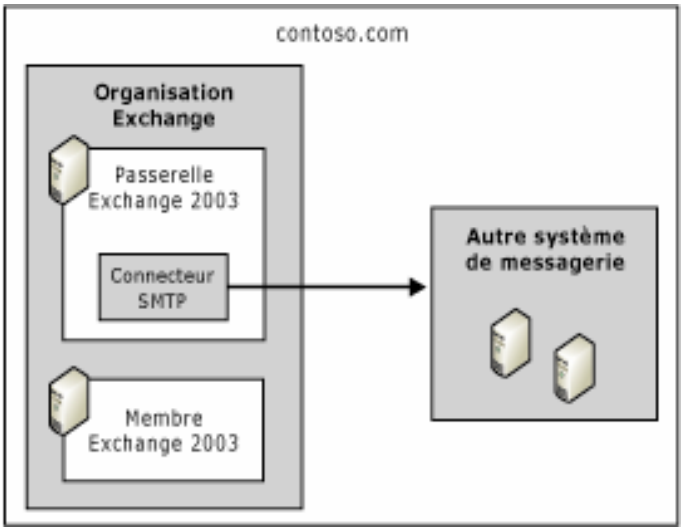


Figure 6.7 Partage d'un domaine SMTP

Si Exchange fonctionne comme premier serveur de messagerie, vous disposez de deux méthodes pour configurer Exchange afin de partager l'espace d'adressage SMTP.

Méthode 1 : Partage des espaces de noms sélectionnés

Dans la Méthode 1, les systèmes de messagerie partagent uniquement les espaces d'adressage SMTP sélectionnés — Exchange fait autorité sur les autres systèmes. Il s'agit là de la méthode préférée en raison de sa flexibilité. Également, vous devez faire appel à cette méthode ou utiliser l'outil Address Rewrite décrit précédemment, si l'une des conditions suivantes se rencontre dans votre environnement :

- Vous créez des contacts dans Active Directory pour l'envoi des messages aux destinataires externes.
- Les adresses SMTP cibles de ces destinataires externes correspondent aux domaines SMTP configurés dans les stratégies de destinataire Exchange 2003. Par exemple, si l'adresse @contoso.com est configurée sur l'une de vos stratégies de destinataire, et si vous souhaitez créer des contacts avec une adresse cible @contoso.com, vous devez utiliser cette méthode pour partager le domaine de messagerie SMTP @contoso.com.

Méthode 2: Partager l'ensemble des espaces d'adressage

Bien que la Méthode 2 soit moins souple, elle est plus simple à configurer dans les petits environnements. Cependant, vous pouvez faire appel à cette méthode si Active Directory contient des contacts pour les destinataires externes sur l'autre système de messagerie. Pour plus d'informations sur l'utilisation des contacts dans un domaine SMTP partagé, consultez l'article 319759 (en anglais) de la Base de connaissances Microsoft, « XADM : How to Configure Exchange 2000 Server to Forward Messages to a Foreign Messaging System That Shares the Same SMTP Domain Name Space » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=319759).

Méthode 1 : Partage des espaces de noms sélectionnés

La Méthode 1 offre une grande souplesse car elle vous permet de créer des contacts dans Active Directory et de faire migrer plus facilement des utilisateurs vers un système unique. Cette méthode utilise deux principes de base :

- **La création d'un connecteur SMTP avec un espace d'adressage du domaine distant, fourthcoffe.com.** Le connecteur permet le relais des messages vers ce domaine. Le fait d'autoriser des relais vers le domaine distant permet à Exchange d'accepter des messages entrants pour ce domaine.

Important Vous devez configurer ce connecteur sur chaque serveur tête de pont qui accepte les messages Internet entrants pour le domaine fourthcoffee.com.

- **Exchange ne fait pas autorité sur le domaine.** Si Exchange ne fait pas autorité sur un domaine, il part du principe que toutes les adresses du domaine existent dans son organisation. Par conséquent, si la résolution des messages ne peut pas avoir lieu localement, Exchange ne cherche jamais à envoyer des messages par l'intermédiaire d'un connecteur externe. En configurant Exchange pour qu'il ne fasse pas autorité pour le domaine, si l'utilisateur ne peut pas être trouvé localement, Exchange route le message vers le système distant par l'intermédiaire du connecteur.

  Remarque Dans ce cas, comme le domaine de messagerie SMTP ne fait pas autorité, il n'est pas important qu'Exchange accepte des messages entrants pour des domaines sur lesquels il fait autorité. La configuration du connecteur garantit que l'organisation Exchange accepte les messages pour ce domaine — en effet, le connecteur est configuré avec un espace d'adressage SMTP du domaine distant et permet le relais des messages vers ce domaine. Exchange accepte uniquement les messages entrants pour le domaine SMTP partagé car le connecteur vers le système de messagerie distant permet aux messages d'être relayés vers cet espace d'adressage. Comme Exchange ne fait pas autorité pour le domaine de messagerie partagé, si vous supprimez le connecteur, Exchange arrête d'accepter les messages entrants pour ce domaine SMTP. Par conséquent, si vous supprimez le connecteur, n'oubliez pas de modifier la stratégie de destinataire et de donner autorité à Exchange pour ce domaine de messagerie SMTP.

L'utilisation de la Méthode 1 s'articule autour de trois étapes principales (chaque étape est approfondie dans les sections suivantes) :

1. Déterminer si Exchange fait autorité sur le domaine de messagerie SMTP que vous voulez partager.
2. Configurer la stratégie de destinataire pour le domaine de messagerie SMTP que vous voulez partager La manière dont vous procédez dépend de la présence ou non du domaine de messagerie SMTP sur la stratégie de destinataire par défaut, d'une autre stratégie de destinataire ou, si celle-ci n'existe pas encore, d'une stratégie de destinataire.
3. Créer un connecteur SMTP pour router les messages vers l'autre système de messagerie ou l'hôte.

Étape 1 : Déterminer si Exchange fait autorité sur le domaine de messagerie SMTP que vous voulez partager

Avant de configurer votre stratégie de destinataire pour le domaine de messagerie SMTP que vous voulez partager, vous devez déterminer si Exchange fait autorité sur le domaine.

N'oubliez pas que, selon si Exchange 2003 fait autorité ou non, celui-ci traite les messages électroniques différemment pour des adresses SMTP particulières. Comme Exchange ne transmet pas les messages qu'il ne peut pas résoudre localement pour un domaine faisant autorité, vous devez vous assurer qu'Exchange ne fait pas autorité sur le domaine de messagerie SMTP que vous souhaitez partager.

Pour afficher le paramètre qui détermine si Exchange fait autorité

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Destinataires**, puis cliquez sur **Stratégies de destinataire**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur une stratégie de destinataire, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Adresses de messagerie (Stratégie)**, sélectionnez une adresse SMTP, puis cliquez sur **Modifier**. Une boîte de dialogue similaire à la figure 6.8 s'affiche.

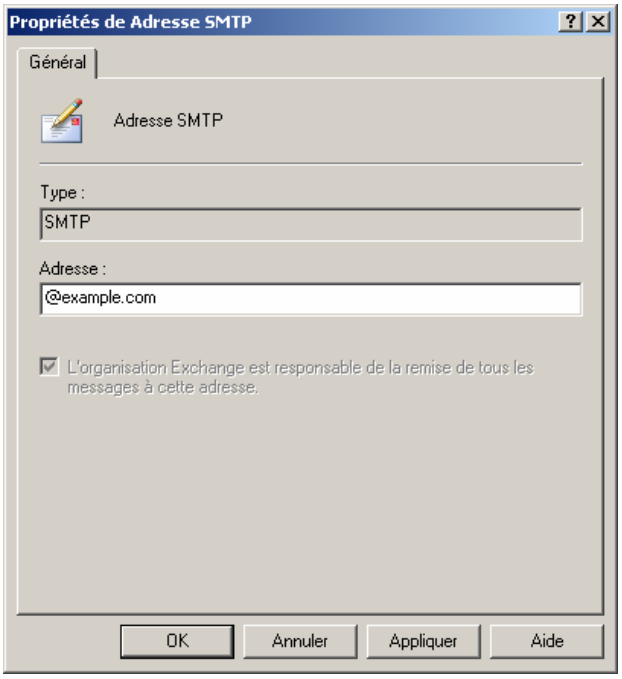


Figure 6.8 Boîte de dialogue Propriétés de Adresse SMTP pour un domaine qui fait autorité

5. Si la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse** est activée, Exchange fait autorité pour l'adresse. Si cette case à cocher est désactivée, Exchange ne fait pas autorité pour l'adresse.

   Pour plus d'informations sur les domaines SMTP qui font ou ne font pas autorité dans Exchange, consultez l'article 315591 (en anglais) de la Base de connaissances Microsoft, « XCON : Authoritative and Non-Authoritative Domains in Exchange 2000 » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=315591).

Étape 2 : Configurer la stratégie de destinataire pour le domaine de messagerie SMTP que vous voulez partager

Lorsque vous configurez la stratégie de destinataire pour le domaine de messagerie SMTP que vous voulez partager, trois scénarios possibles s'offrent à vous :

Scénario 1 Le domaine de messagerie SMTP que vous voulez partager figure dans la stratégie de destinataire par défaut.

Scénario 2 Le domaine de messagerie SMTP que vous voulez partager figure dans une autre stratégie de destinataire.

Scénario 3 Le domaine de messagerie SMTP que vous voulez partager ne figure pas dans une stratégie de destinataire.

Scénario 1 : Configuration d'un domaine SMTP partagé qui figure dans la stratégie de destinataire par défaut

Vous ne pouvez pas définir Exchange comme ne faisant pas autorité sur l'espace d'adressage SMTP principal de la stratégie de destinataire par défaut. Pour empêcher Exchange de faire autorité sur ce domaine, vous devez modifier la stratégie de destinataire par défaut en ajoutant un nouvel espace d'adressage principal réservé à usage interne. Cette adresse peut ressembler à @localhost ce qui signifie qu'elle est réservée au flux des messages internes dans votre organisation Exchange. Après avoir ajouté le nouvel espace d'adressage, vous devez configurer l'espace d'adressage partagé pour qu'il ne fasse pas autorité.

Pour configurer Exchange afin de partager un domaine de messagerie qui existe en tant qu'espace d'adressage principal sur la stratégie de destinataire par défaut, vous devez effectuer les opérations suivantes :

1. Sur la stratégie de destinataire par défaut, ajoutez un nouvel espace d'adressage principal sur lequel Exchange fait autorité, puis configurez l'espace d'adressage partagé pour qu'il ne fasse pas autorité.
2. Créez une deuxième stratégie de destinataire qui possède le même filtre de recherche comme stratégie de destinataire par défaut. Puis, attribuez à la deuxième stratégie de destinataire une priorité supérieure à la stratégie de destinataire par défaut afin que l'adresse de retour ou de réponse soit affichée comme l'espace d'adressage partagé.

   Cette étape est nécessaire car Exchange utilise l'espace d'adressage principal comme l'adresse de réponse affichée sur les messages sortants. Comme vous souhaitez que les messages sortants affichent le nom d'espace partagé sur la ligne Répondre, vous devez créer une autre stratégie de destinataire qui ne fait pas non plus autorité et qui possède une priorité plus élevée ; par conséquent, Exchange utilise cet espace d'adressage sur l'adresse de retour des messages sortants. Étant donné que la nouvelle stratégie de destinataire n'est pas la stratégie par défaut, vous pouvez configurer cet espace d'adressage pour qu'il ne fasse pas autorité.

Pour créer un nouvel espace d'adressage principal sur la stratégie de destinataire par défaut et configurer l'espace d'adressage partagé pour qu'il ne fasse pas autorité, effectuez la procédure suivante.

Pour modifier la stratégie de destinataire par défaut

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Destinataires**, puis cliquez sur **Stratégies de destinataire**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur votre stratégie de destinataire par défaut, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Adresses de messagerie (Stratégie)**, puis sur **Nouvelle**.
5. Dans **Nouvelle adresse de messagerie**, cliquez sur **Adresse SMTP**, puis sur **OK**.
6. Dans **Propriétés de Adresse SMTP**, dans la zone **Adresse**, tapez **@localhost** ou un autre espace d'adressage pour lequel l'organisation Exchange peut faire autorité. Vous pouvez utiliser **@localhost** ou votre domaine Active Directory si celui-ci est différent de votre domaine Internet. Cet espace d'adressage est réservé à l'usage interne.
7. Vérifiez que la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse** est activée, puis cliquez sur **OK**.
8. Sur l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur la nouvelle adresse SMTP que vous venez de créer, puis cliquez sur **Définir comme principale**.
9. Cliquez sur l'espace d'adressage SMTP que vous souhaitez partager (par exemple, contoso.com), puis cliquez sur **Modifier**.
10. Pour configurer Exchange afin qu'il ne fasse pas autorité pour cette adresse SMTP, désactivez la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse**, puis cliquez sur **Appliquer**.
11. Un message s'affiche et vous demande si vous souhaitez mettre à jour toutes les adresses de messagerie de destinataire correspondantes. Cliquez sur **Oui**.
12. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur **OK**.

Modifier ainsi la stratégie de destinataire par défaut force Exchange à utiliser la nouvelle adresse principale comme adresse de retour ou de réponse dans les messages électroniques sortants. Dans l'exemple ci-dessus, tous les utilisateurs de cette stratégie possèdent désormais une adresse de messagerie de retour qui correspond au nouvel espace d'adressage principal de @localhost. Comme vous souhaitez que vos utilisateurs possèdent

l'adresse de retour du domaine de messagerie partagé (dans ce cas, contoso.com), vous devez créer une nouvelle stratégie de destinataire possédant une stratégie de priorité supérieure et qui contient l'espace d'adressage contoso.com. Exchange utilise la stratégie de destinataire à priorité supérieure sur l'adresse de retour. De plus, étant donné que cette nouvelle stratégie de destinataire n'est pas la stratégie par défaut, vous pouvez la configurer pour qu'elle ne fasse pas autorité. (N'oubliez pas que cet espace d'adressage ne doit pas faire autorité pour être routé par Exchange par l'intermédiaire du connecteur vers le système externe.)

Pour créer une stratégie de destinataire de priorité supérieure de sorte que les messages sortants affichent l'adresse de retour (réponse) correcte, effectuez la procédure suivante.

Pour créer une stratégie de destinataire de priorité supérieure avec le domaine de messagerie partagée

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Destinataires**, cliquez avec le bouton droit sur **Stratégies de destinataire**, pointez sur **Nouveau**, puis cliquez sur **Stratégie de destinataire**.
3. Dans **Nouvelle stratégie**, activez la case à cocher **Adresses de messagerie**, puis cliquez sur **OK**.
4. Sous l'onglet **Général**, dans la zone **Nom**, tapez un nom approprié tel que « Adresses utilisateurs ».
5. Sous **Règles de filtrage**, cliquez sur **Modifier**.
6. Dans **Rechercher des destinataires Exchange**, activez ou désactivez les cases à cocher appropriées pour spécifier tous les utilisateurs applicables. Si vous souhaitez appliquer la stratégie à tous les utilisateurs, cliquez sur **OK**.
7. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur le domaine de messagerie SMTP que vous souhaitez partager, puis sur **Définir comme principale** (le domaine @local reste comme proxy secondaire), puis cliquez sur **Appliquer**.
8. Un message s'affiche et vous demande si vous souhaitez mettre à jour toutes les adresses de messagerie de destinataire correspondantes. Cliquez sur **Oui**.
9. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur **OK**.

Scénario 2 : Le domaine SMTP que vous voulez partager figure dans une autre stratégie de destinataire

Si le domaine SMTP que vous souhaitez partager ne figure pas dans la stratégie de destinataire par défaut, vous pouvez configurer l'espace d'adressage pour qu'il ne fasse pas autorité.

Pour modifier une stratégie de destinataire existante pour le domaine SMTP que vous voulez partager

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Destinataires**, puis cliquez sur **Stratégies de destinataire**.
3. Dans le volet d'informations, cliquez avec le bouton droit sur la stratégie de destinataire qui possède l'espace d'adressage SMTP que vous souhaitez partager, puis cliquez sur **Propriétés**.
4. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur l'espace d'adressage SMTP, puis sur **Définir comme principale**.
5. Cliquez sur l'espace d'adressage SMTP que vous souhaitez partager, puis cliquez sur **Modifier**.
6. Pour configurer Exchange afin qu'il ne fasse pas autorité sur cette adresse SMTP, désactivez la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse**, puis cliquez sur **Appliquer**.
7. Un message s'affiche et vous demande si vous souhaitez mettre à jour toutes les adresses de messagerie de destinataire correspondantes. Cliquez sur **Oui**.
8. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur **OK**.

Scénario 3 : Le domaine SMTP que vous voulez partager ne figure pas dans une stratégie de destinataire

Si le domaine SMTP que vous souhaitez partager ne figure pas dans une stratégie de destinataire, vous pouvez créer une nouvelle stratégie de destinataire avec l'espace d'adressage et la configurer pour qu'elle ne fasse pas autorité.

Pour créer une nouvelle stratégie de destinataire pour un domaine de messagerie SMTP qui ne figure pas dans une stratégie de destinataire

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Destinataires**, cliquez avec le bouton droit sur **Stratégies de destinataire**, pointez sur **Nouveau**, puis cliquez sur **Stratégie de destinataire**.
3. Dans **Nouvelle stratégie**, activez la case à cocher **Adresses de messagerie**, puis cliquez sur **OK**.
4. Sous l'onglet **Général**, dans la zone **Nom**, tapez un nom pour votre nouvelle stratégie.
5. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur l'espace d'adressage SMTP, puis sur **Nouvelle**.
6. Dans **Nouvelle adresse de messagerie**, cliquez sur **Adresse SMTP**, puis sur **OK**.
7. Dans **Propriétés Adresse SMTP**, dans la zone **Adresse**, tapez l'espace d'adressage SMTP que vous souhaitez partager.
8. Pour configurer Exchange afin qu'il ne fasse pas autorité pour cette adresse SMTP, désactivez la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse**.
9. Dans **Propriétés Adresse SMTP**, cliquez sur **OK**.
10. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur **OK**.

Étape 3 : Créer un connecteur SMTP pour router les messages vers l'autre système de messagerie

Maintenant qu'Exchange 2003 est configuré pour ne pas faire autorité pour le domaine SMTP partagé, si Exchange 2003 ne trouve pas d'adresse correspondante dans Active Directory, il cherche à localiser un chemin externe vers ce domaine. Pour trouver ce chemin, Exchange commence par rechercher un connecteur puis vérifie le service DNS (Domain Name System). À moins que l'enregistrement de serveur de messagerie (MX) pour ce domaine ne pointe déjà vers le serveur sur lequel réside l'autre système de messagerie (dans la plupart des cas, l'enregistrement MX pointe vers le serveur Exchange 2003 lui-même), vous devez créer un connecteur SMTP pour router les messages vers un hôte spécifique.

> **Important** Vous devez configurer ce connecteur sur chaque serveur tête de pont qui accepte les messages Internet entrants pour le domaine fourthcoffee.com.

Pour créer un connecteur SMTP pour router les messages vers un hôte spécifique

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Connecteurs**, pointez sur **Nouveau**, puis cliquez sur **Connecteur SMTP**.
3. Sous l'onglet **Général**, tapez un nom approprié, puis cliquez sur **Transférer tous les courriers via ce connecteur aux hôtes actifs suivants**. Tapez entre crochets ([ ]) le nom de domaine complet ou l'adresse IP du serveur vers lequel les messages électroniques de l'espace d'adressage SMTP doivent être routés.

4. Cliquez sur **Ajouter** pour configurer vos serveurs têtes de pont, puis sélectionnez vos serveurs de passerelle Exchange qui acceptent les messages Internet pour ce domaine.
5. Cliquez sur l'onglet **Espace d'adressage**, **Ajouter**, **SMTP**, puis sur **OK**.
6. Dans **Domaine de messagerie**, tapez l'espace d'adressage SMTP sans le symbole arobase (@), par exemple, **fourthcoffee.com**, puis cliquez sur **OK**.

   Avertissement Il est important d'entrer le domaine de messagerie SMTP spécifique. N'entrez pas ***** (astérisque) sur le connecteur SMTP. Définir ***** entraîne l'acceptation par Exchange des messages destinés à tous les domaines externes qui sont ensuite relayés en externe. Cette configuration autorise le relais ouvert pour n'importe qui sur Internet et n'est pas du tout sécurisée.
7. Comme Exchange 2003 doit également recevoir des messages pour ce domaine, sous l'onglet **Espace d'adressage**, cliquez sur **Autoriser les messages à être relayés vers ces domaines**, puis sur **OK**. Ce paramètre permet à tous les serveurs virtuels SMTP répertoriés sous **Serveurs têtes de pont locaux** d'accepter des messages pour ce domaine.

Après avoir configuré ces paramètres, si Exchange 2003 ne peut pas localiser une adresse locale correspondante dans ce domaine SMTP, Exchange transmet les messages vers l'hôte qui possède l'espace d'adressage correspondant comme cela est spécifié sur le connecteur SMTP.

Méthode 2: Partage de l'ensemble des espaces d'adressage

Cette méthode concerne le partage de tous les espaces d'adressage ou des domaines de messagerie SMTP. Même si cette configuration est d'une implémentation aisée, elle se révèle moins souple que la Méthode 1. Dans cette configuration, Exchange 2003 fait autorité pour tous les espaces d'adressage. Votre répertoire ne peut pas contenir de contacts dont l'adresse cible correspond à un domaine sur lequel Exchange 2003 fait autorité.

Pour partager tous les espaces d'adressage dans votre organisation Exchange

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, **< *Nom serveur* >**, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur votre serveur virtuel SMTP, puis cliquez sur **Propriétés**.
4. Dans les **Propriétés** du serveur virtuel SMTP, cliquez sur l'onglet **Messages**.
5. Dans la zone **Transférer tous les messages dont les destinataires n'ont pas été résolus vers l'hôte**, tapez l'adresse IP entre crochets ([ ]) ou le nom de domaine complet du serveur qui reçoit les messages non résolus, puis cliquez sur **OK**.
6. Répétez cette procédure pour le serveur virtuel SMTP par défaut sur tous les serveurs Exchange 2003, sauf pour les serveurs virtuels fonctionnant comme passerelle entrante pour l'autre système. Il est recommandé qu'aucune boîte aux lettres ne réside sur ce serveur.

N'oubliez pas que ce paramètre affecte uniquement les domaines qui font autorité. Par conséquent, dans un domaine qui fait autorité, tous les messages envoyés à une adresse non résolue sont transmis au serveur spécifié sur le serveur virtuel SMTP. Les domaines ne faisant pas autorité dans Exchange 2003 ne sont pas affectés par ce paramètre. Les messages envoyés vers une adresse non résolue dans un domaine ne faisant pas autorité sont routés vers un connecteur SMTP correspondant, si celui-ci est présent. En l'absence de tout connecteur SMTP correspondant, le message est envoyé au serveur spécifié dans l'enregistrement MX trouvé dans le DNS.

Prise en charge de systèmes de messagerie supplémentaires

Comme le décrivent les scénarios précédents, l'autre système de messagerie qui reçoit les messages transmis par Exchange peut effectuer les mêmes tâches qu'Exchange et transmettre les messages à un système de messagerie tiers. Pour éviter le bouclage des messages, il est essentiel que le dernier système de messagerie (vers lequel les courriers sont transmis) fasse autorité pour le domaine. En d'autres termes, le système de messagerie doit rechercher un destinataire correspondant ; si le système chargé de recevoir les messages en dernier ne trouve pas de destinataire correspondant, il génère un rapport de non-remise pour le message. Le bouclage des messages se produit lorsque le système receveur recherche une correspondance dans ses destinataires puis retourne les messages vers le système d'origine lorsqu'une correspondance est trouvée.

Si Exchange est le dernier système de cette configuration, il retourne, par défaut, un rapport de non-remise pour les messages non résolus. Cependant, il est préférable de créer des destinataires personnalisés dans Active Directory pour tous les destinataires qui résident dans un système de messagerie différent. Ces destinataires doivent disposer d'adresses cibles similaires à *@sousdomaine*.contoso.com, où *sousdomaine* indique les informations d'adresse supplémentaires afin de distinguer l'espace d'adressage du nom d'espace standard @example.com ; par exemple, @ventes.contoso.com.

Configuration de la collaboration des messageries SMTP entre forêts

Exchange 2003 empêche l'usurpation de noms, ou la falsification d'identités, en exigeant une authentification avant de convertir le nom de l'expéditeur en nom complet dans la liste d'adresses globale. Par conséquent, dans une organisation qui compte deux forêts, un utilisateur qui envoie des messages d'une forêt à l'autre n'est pas authentifié. En outre, le nom de l'utilisateur n'est pas converti en nom affiché dans la liste d'adresses globale, même si cet utilisateur existe en tant que contact dans la forêt de destination.

Pour permettre la collaboration de messageries entre forêts dans Exchange 2003, des étapes supplémentaires de la configuration sont requises pour convertir les contacts situés hors de votre organisation en noms complets figurant dans l'annuaire Active Directory. Deux options s'offrent à vous pour activer la résolution de ces contacts :

- **Option 1 (recommandée)** Utilisez l'authentification pour que les utilisateurs qui envoient des messages d'une forêt à l'autre soient authentifiés et que leurs noms soient associés à des noms complets dans la liste d'adresses globale.
- **Option 2** Limitez l'accès au serveur virtuel SMTP utilisé pour la collaboration entre forêts, puis configurez Exchange afin de résoudre les messages électroniques anonymes. Cette configuration est prise en charge, mais elle n'est pas recommandée. Par défaut, dans cette configuration, les propriétés des messages Exch50, qui correspondent aux propriétés étendues d'un message, ne sont pas conservées en cas d'envoi des messages entre les forêts.

Pour comprendre les avantages liés à la configuration d'une collaboration de messageries entre forêts, examinez les scénarios suivants en matière d'envoi de messages anonymes et d'envoi de messages authentifiés entre forêts.

Scénario : Envoi de messages anonymes

Les adresses de messagerie ne sont pas résolues si l'envoi est anonyme. Par conséquent, lorsqu'un utilisateur anonyme envoie du courrier en tentant d'usurper (falsifier) l'identité d'un utilisateur interne, l'adresse de retour n'est pas convertie en nom complet de la liste d'adresses globale.

Par exemple, Julie Akers est une utilisatrice interne légitime au sein de l'entreprise Contoso, S.A. Son nom complet dans la liste d'adresses globale est **Julie Akers** et son adresse de messagerie est julie@contoso.com.

Pour pouvoir envoyer des messages, Julie doit être authentifiée. Dans la mesure où cette authentification est effectuée, les destinataires appropriés des messages de Julie peuvent voir que l'expéditeur est Julie Akers. En outre, les propriétés affichées pour Julie Akers sont celles de l'entrée correspondante dans la liste d'adresses globale. Cependant, si Pierre Lopez tente d'usurper l'adresse de Julie en utilisant **julie@contoso.com** dans la ligne **De**, et s'il envoie ensuite le courrier au serveur Exchange 2003 de la société Contoso, l'adresse de messagerie ne sera pas convertie en nom complet de Julie, car Pierre ne s'est pas authentifié. Par conséquent, quand ce message électronique s'affiche dans Microsoft Office Outlook®, l'adresse de l'expéditeur indique **julie@contoso.com** et non pas Julie Akers, comme ce serait le cas avec le courrier authentifié provenant de Julie.

Scénario : Remise des messages entre forêts

Prenez l'exemple d'une société qui utilise deux forêts : la forêt Adatum et la forêt Fabrikam. Ces forêts possèdent chacune un domaine unique, adatum.com et fabrikam.com, respectivement. Pour autoriser une collaboration de messageries entre forêts, tous les utilisateurs de la forêt Adatum sont représentés en tant que contacts de l'annuaire Active Directory de la forêt Fabrikam. De même, tous les utilisateurs de la forêt Fabrikam sont représentés en tant que contacts de l'annuaire Active Directory de la forêt Adatum.

Si un utilisateur de la forêt Adatum envoie du courrier à la forêt Fabrikam via une connexion anonyme, l'adresse de l'expéditeur n'est pas résolue, en dépit du fait que cet expéditeur existe en tant que contact dans l'annuaire Active Directory et dans la liste d'adresses globale Outlook. En effet, un utilisateur de la forêt Adatum n'est pas un utilisateur authentifié dans la forêt Fabrikam.

Par exemple, Pierre Lopez est un utilisateur de messagerie dans la forêt Adatum, son adresse de messagerie est pierre@adatum.com et son nom complet dans la liste d'adresses globale Outlook est Pierre Lopez. Bernard Guyot est un utilisateur de messagerie dans la forêt Fabrikam, son adresse de messagerie est bernard@fabrikam.com et son nom complet dans la liste d'adresses globale Outlook est Bernard Guyot. Comme Bernard figure en tant que contact Active Directory dans la forêt Adatum, Pierre peut voir l'adresse électronique de celui-ci et la mettre en correspondance avec le nom complet Bernard Guyot dans la liste d'adresses globale d'Outlook. Quand Bernard reçoit du courrier de Pierre, l'adresse de Pierre n'est pas traduite ; au lieu du nom complet de Pierre tel qu'il figure dans la liste d'adresses globale, Bernard voit l'adresse non résolue pierre@adatum.com. Ceci s'explique par le fait que Pierre a envoyé le courrier en tant qu'utilisateur anonyme. Bien que Pierre soit authentifié au moment où il envoie du courrier, la connexion entre les deux forêts n'est pas authentifiée.

Si vous voulez avoir la garantie que les expéditeurs d'une forêt peuvent envoyer du courrier aux destinataires situés dans d'autres forêts, et si vous voulez être certain que les adresses de messagerie sont converties en noms complets de la liste d'adresses globale, vous devez activer la collaboration de messageries entre forêts. Les sections suivantes décrivent les deux options possibles pour configurer la collaboration de messageries entre deux forêts.

Activation de l'authentification entre forêts

Pour activer l'authentification SMTP entre forêts, vous devez créer des connecteurs dans chaque forêt qui utilisent un compte authentifié de l'autre forêt. Dès lors, tout courrier envoyé d'une forêt à l'autre par un utilisateur authentifié est converti en nom complet approprié figurant dans la liste d'adresses globale. Cette section explique comment activer l'authentification entre forêts.

À l'aide de l'exemple des forêts Adatum et Fabrikam (consultez « Scénario : Remise des messages entre forêts » plus haut dans ce chapitre), effectuez les opérations suivantes pour configurer l'authentification entre forêts :

1. Créez dans la forêt Fabrikam un compte qui dispose des autorisations Envoyer en tant que. (Un contact correspondant existe dans la forêt Fabrikam pour tous les utilisateurs de la forêt Adatum ; par conséquent,

ce compte permet aux utilisateurs Adatum d'envoyer des messages authentifiés.) Configurez ces autorisations sur tous les serveurs Exchange qui accepteront des messages entrants en provenance d'Adatum.

2. Sur un serveur Exchange de la forêt Adatum, créez un connecteur qui exige une authentification en utilisant ce compte pour envoyer des messages sortants.

Pour configurer l'authentification entre les forêts Fabrikam et Adatum, répétez ces étapes en créant cette fois le compte dans Adatum et le connecteur dans Fabrikam.

Étape 1 : Création dans la forêt de destination d'un compte d'utilisateur disposant des autorisations Envoyer en tant que

Avant de configurer votre connecteur dans la forêt de connexion, vous devez créer dans la forêt de destination (la forêt à laquelle vous vous connectez) un compte disposant des autorisations Envoyer en tant que. Configurez ces autorisations sur tous les serveurs de la forêt de destination qui accepteront des connexions entrantes de la forêt de connexion. Les procédures suivantes vous expliquent comment configurer un compte dans la forêt Fabrikam et un connecteur dans la forêt Adatum, ce qui permettra aux utilisateurs de la forêt Adatum d'envoyer du courrier à la forêt Fabrikam avec des adresses de messagerie résolues.

Pour créer un compte qui servira à l'authentification entre forêts

1. Dans la forêt de destination (ici, la forêt Fabrikam), créez un compte d'utilisateur dans Utilisateurs et ordinateurs Active Directory. Ce compte doit être actif, mais ne requiert pas les autorisations suivantes : ouverture d'une session locale et ouverture de session via Terminal Server.
2. Sur chaque serveur Exchange qui acceptera des connexions entrantes de la forêt de connexion, configurez des autorisations Envoyer en tant que pour ce compte :

   Remarque Créez soigneusement votre stratégie de mot de passe. Si vous prévoyez une date d'expiration pour le mot de passe, veillez à ce qu'une stratégie soit mise en place pour que le mot de passe puisse être modifié avant cette date. Si le mot de passe de ce compte expire, l'authentification entre forêts échoue.

3. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
4. Dans l'arborescence de la console, développez **Serveurs**, cliquez avec le bouton droit sur un serveur Exchange qui accepte les connexions entrantes de la forêt de connexion, puis cliquez sur **Propriétés**.
5. Dans Propriétés <***Nom du serveur***>, sous l'onglet **Sécurité**, cliquez sur **Ajouter**.
6. Dans **Sélectionnez les utilisateurs, les ordinateurs ou les groupes**, ajoutez le compte que vous venez de créer, puis cliquez sur **OK**.
7. Sous l'onglet **Sécurité**, sous **Noms d'utilisateurs ou de groupes**, sélectionnez le compte.
8. Sous **Autorisations pour le connecteur**, en regard d'**Envoyer en tant que**, activez la case à cocher **Autoriser** (Figure 6.9).

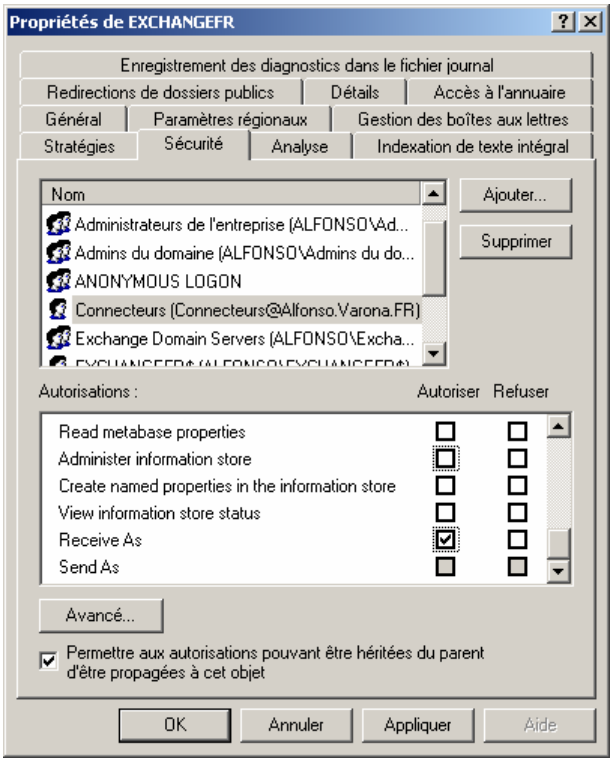


Figure 6.9 Activation de l'autorisation Envoyer en tant que pour un connecteur

Étape 2: Création d'un connecteur dans la forêt de connexion

Une fois que vous avez créé le compte avec les autorisations appropriées dans la forêt de destination, créez un connecteur dans la forêt de connexion et exigez l'authentification à l'aide du compte que vous venez de créer. Dans la procédure suivante, supposez que vous créez sur un serveur Exchange de la forêt Adatum un connecteur qui établit une connexion avec la forêt Fabrikam.

Pour configurer un connecteur et exiger une authentification pour l'authentification entre forêts

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Connecteurs**, pointez sur **Nouveau**, puis cliquez sur **Connecteur SMTP**.
3. Sous l'onglet **Général**, dans la zone **Nom**, tapez un nom pour le connecteur.
4. Cliquez sur **Transférer tous les courriers via ce connecteur aux hôtes actifs suivants**, puis tapez le nom de domaine complet ou l'adresse IP du serveur tête de pont de réception.
5. Cliquez sur **Ajouter** pour sélectionner un serveur tête de pont local et un serveur virtuel SMTP pour héberger le connecteur (Figure 6.10).

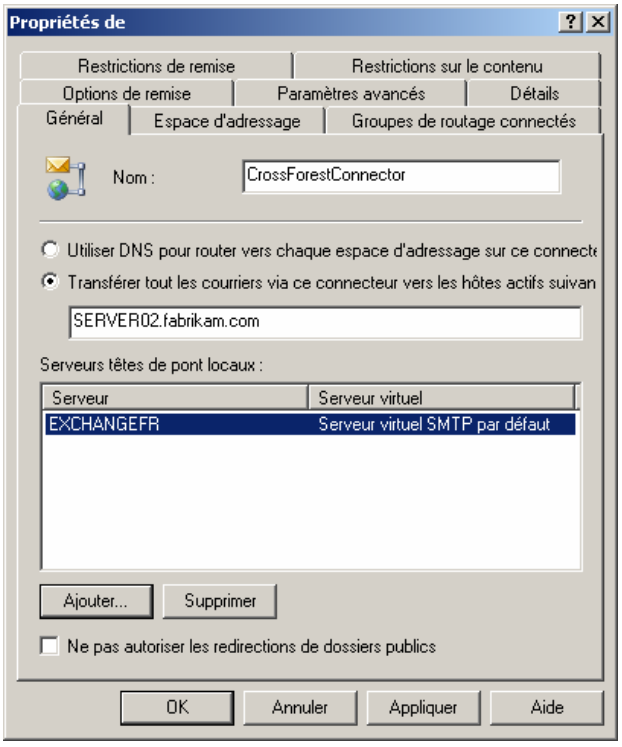


Figure 6.10 Onglet Général de la boîte de dialogue Propriétés d'un serveur virtuel SMTP

6. Sous l'onglet **Espace d'adressage**, cliquez sur **Ajouter**, sélectionnez **SMTP**, puis cliquez sur **OK**.
7. Dans **Propriétés de l'espace d'adressage Internet**, tapez le domaine de la forêt à laquelle vous voulez vous connecter, puis cliquez sur **OK**. Dans cet exemple, comme le connecteur envoie à partir de la forêt Adatum vers la forêt Fabrikam, l'espace d'adressage correspond au domaine de la forêt, fabrikam.com (figure 6.11).

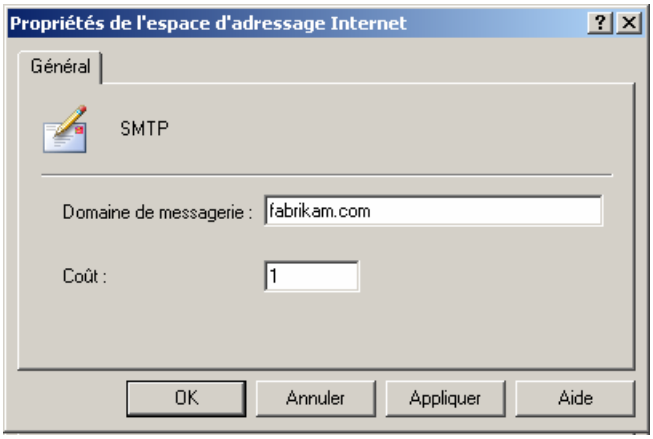


Figure 6.11 Boîte de dialogue Propriétés de l'espace d'adressage Internet

Exchange utilisera désormais ce connecteur pour router l'ensemble du courrier destiné à fabrikam.com (la forêt Fabrikam).

8. Sous l'onglet **Paramètres avancés**, cliquez sur **Sécurité sortante**.
9. Cliquez sur **Authentification intégrée Windows** (figure 6.12).

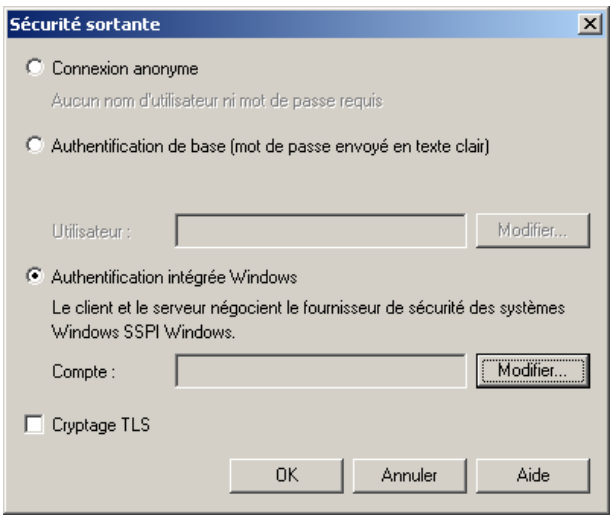


Figure 6.12 Bouton Authentification intégrée Windows de la boîte de dialogue Sécurité sortante

10. Cliquez sur **Modifier**.
11. Dans **Informations d'identification de connexion sortante**, dans les zones **Compte**, **Mot de passe** et **Confirmer le mot de passe**, spécifiez un compte et un mot de passe dans la forêt de destination (ici, Fabrikam), compte qui doit disposer d'autorisations Envoyer en tant que et être authentifié Fabrikam (Figure 6.13). Utilisez le format suivant pour le nom du compte : *domaine\nom d'utilisateur*, où :
    - *domaine* est un domaine de la forêt de destination et
    - *nom d'utilisateur* représente un compte de la forêt de destination possédant des permissions Envoyer comme sur tous les serveurs Exchange de cette forêt qui accepteront du courrier émanant de ce connecteur.

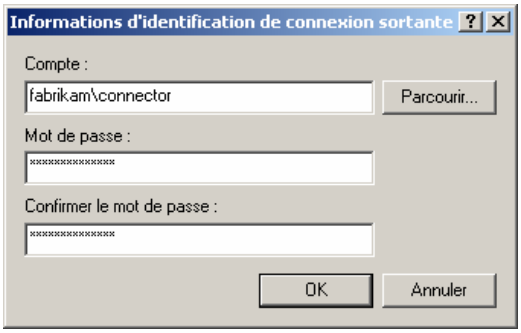


Figure 6.13 Boîte de dialogue Informations d'identification de connexion sortante

12. Cliquez sur **OK**.

Activation de la collaboration entre forêts par résolution du courrier anonyme

Il existe une autre façon de configurer Exchange afin de convertir les contacts situés à l'extérieur de votre organisation en noms complets de l'annuaire Active Directory. Pour ce faire, il suffit de configurer Exchange de sorte qu'il résolve le courrier électronique anonyme. Supposez que votre société utilise deux forêts, la forêt Adatum et la forêt Fabrikam.

Important Si vous configurez des serveurs Exchange en vue de résoudre les envois de courrier anonyme, vous autorisez les utilisateurs malintentionnés à envoyer des messages comportant une adresse de retour falsifiée. Les destinataires ne sont pas en mesure de différencier les messages authentiques des messages falsifiés. Pour réduire ce risque, veillez à limiter l'accès au serveur virtuel SMTP aux adresses IP de vos serveurs Exchange.

Pour convertir les contacts des utilisateurs Adatum en noms complets de la forêt Fabrikam, procédez comme suit. Chacune de ces étapes est décrite en détail dans les sections suivantes :

1. Créez un connecteur dans la forêt Adatum qui se connecte à la forêt Fabrikam.
2. Sur le serveur tête de pont de réception de la forêt Fabrikam, limitez l'accès au serveur virtuel SMTP en fonction de l'adresse IP. En procédant ainsi, vous êtes assuré que seuls les serveurs de la forêt Adatum peuvent envoyer du courrier à ce serveur.
3. Sur le serveur virtuel SMTP hébergeant le connecteur, activez le paramètre Résoudre la messagerie anonyme.
4. Modifiez une clé du Registre pour garantir la persistance des propriétés de message étendues (Exch50) entre les forêts. Dans le cas contraire, vous risquez de perdre des informations de message importantes.

Une fois que vous avez effectué les étapes ci-dessus, tous les utilisateurs qui envoient du courrier de la forêt Adatum à la forêt Fabrikam verront leurs adresses converties en noms complets de la liste d'adresses globale Fabrikam. Dans un environnement de production, répétez simplement ce processus pour configurer la résolution des contacts Fabrikam de la forêt Adatum.

Étape 1: Création d'un connecteur dans la forêt de connexion

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, cliquez avec le bouton droit sur **Connecteurs**, pointez sur **Nouveau**, puis cliquez sur **Connecteur SMTP**.
3. Sous l'onglet **Général**, dans la zone **Nom**, tapez un nom pour le connecteur.
4. Cliquez sur **Transférer tous les courriers via ce connecteur aux hôtes actifs suivants**, puis tapez le nom de domaine complet ou l'adresse IP du serveur tête de pont de réception.
5. Cliquez sur **Ajouter** pour sélectionner un serveur tête de pont local et un serveur virtuel SMTP pour héberger le connecteur (Figure 6.14).

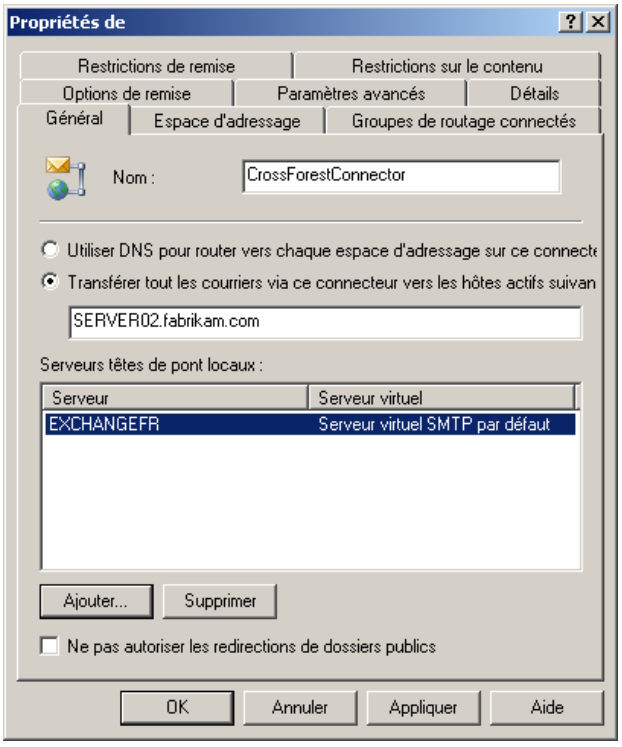


Figure 6.14 Onglet Général de la boîte de dialogue Propriétés d'un serveur virtuel SMTP

6. Sous l'onglet **Espace d'adressage**, cliquez sur **Ajouter**, sélectionnez **SMTP**, puis cliquez sur **OK**.

7. Dans **Propriétés de l'espace d'adressage Internet**, tapez le domaine de la forêt à laquelle vous voulez vous connecter, puis cliquez sur **OK**. Dans cet exemple, comme le connecteur envoie à partir de la forêt Adatum vers la forêt Fabrikam, l'espace d'adressage correspond au domaine de la forêt, fabrikam.com (figure 6.15).

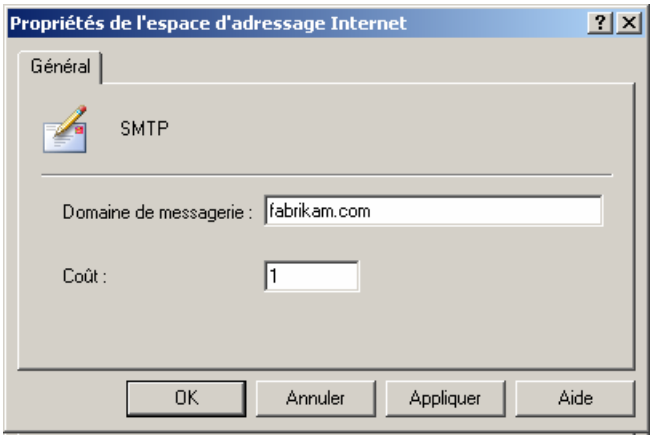


Figure 6.15 Boîte de dialogue Propriétés de l'espace d'adressage Internet

Exchange utilisera désormais ce connecteur pour router l'ensemble du courrier destiné à fabrikam.com (la forêt Fabrikam).

Étape 2 : Limitation des adresses IP sur le serveur tête de pont de réception

Une fois que vous avez créé le connecteur dans la forêt Adatum (la forêt de connexion), vous devez limiter l'accès au serveur tête de pont de réception. Pour ce faire, autorisez uniquement les adresses IP des serveurs de connexion de la forêt Adatum à envoyer du courrier au serveur tête de pont de réception de la forêt Fabrikam.

Pour restreindre l'accès par adresse IP sur le serveur tête de pont de réception

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez le nœud **Serveurs**, **< *Nom serveur tête de pont* >**, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP souhaité, puis cliquez sur **Propriétés**.
4. Sous l'onglet **Accès**, cliquez sur **Connexion**.
5. Dans **Connexion**, cliquez sur **Uniquement la liste ci-dessous** afin de limiter l'accès à une liste spécifique d'adresses IP.
6. Cliquez sur **Ajouter**, puis effectuez l'une des étapes suivantes :
   - Cliquez sur **Ordinateur unique**, puis dans la zone **Adresse IP**, tapez l'adresse IP qui correspond au serveur Exchange de connexion dans la forêt Adatum (la forêt de connexion). Répétez cette étape pour chaque ordinateur de la forêt Adatum.
   - Cliquez sur **Groupe d'ordinateurs**, puis dans les zones **Adresse de sous-réseau** et **Masque de sous-réseau**, tapez l'adresse de sous-réseau et le masque de sous-réseau du groupe d'ordinateurs hébergeant les connecteurs à la forêt Fabrikam.

Étape 3 : Résolution du courrier anonyme sur le serveur virtuel SMTP

Une fois que vous avez limité l'accès au serveur tête de pont de réception, vous devez configurer le serveur virtuel SMTP situé sur ce serveur tête de pont afin de résoudre les adresses de messagerie anonymes.

Pour configurer un serveur virtuel SMTP afin de résoudre les adresses de messagerie anonymes

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez le nœud **Serveurs**, **< *Nom serveur tête de pont* >**, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP souhaité, puis cliquez sur **Propriétés**.
4. Sous l'onglet **Accès**, cliquez sur **Authentification**.
5. Dans **Authentification**, assurez-vous que la case à cocher **Accès anonyme** est activée, puis activez la case à cocher **Résoudre la messagerie anonyme**.

Étape 4 : Activation de la clé de Registre pour conserver les propriétés des messages entre forêts

Comme indiqué précédemment, lorsque des messages sont envoyés de façon anonyme entre des forêts, leurs propriétés étendues ne sont pas transmises. Lorsque des sociétés isolées implémentent un scénario entre forêts,

les propriétés des messages doivent être transmises, car il est possible de perdre les informations relatives aux messages. Par exemple, la propriété Exchange étendue SCL indique le taux de contrôle d'accès de courrier non sollicité généré par des solutions tierces. Cette propriété n'est pas transmise lorsque le courrier est envoyé de façon anonyme. Par conséquent, si une solution de blocage du courrier indésirable est déployée dans la forêt Adatum et si un message reçu dans cette forêt est destiné au destinataire de la forêt Fabrikam, la solution de blocage du courrier indésirable marque la propriété SCL sur le message. Cependant, lorsque le message est remis à la forêt Fabrikam, la propriété étendue qui contient le taux de contrôle d'accès du courrier indésirable disparaît.

Pour configurer Exchange de sorte qu'il accepte les propriétés de message étendues, vous pouvez activer une clé de Registre sur le serveur tête de pont de réception ou sur le serveur virtuel SMTP qui réside sur ce serveur tête de pont. L'activation de la clé de Registre sur le serveur Exchange permet de configurer tous les serveurs virtuels SMTP hébergés sur ce dernier, afin qu'ils acceptent les propriétés étendues.

Configuration du serveur Exchange pour obliger l'acceptation des propriétés de message étendues lors des connexions anonymes

Utilisez la procédure suivante pour configurer le serveur Exchange afin de l'obliger à accepter les propriétés étendues lors des connexions anonymes. Si votre serveur Exchange fonctionne uniquement en tant que serveur tête de pont pour les communications entre forêts, vous pouvez configurer ce paramètre au niveau du serveur. Si vous disposez d'autres serveurs virtuels SMTP sur ce serveur Exchange, songez à définir cette clé de Registre uniquement sur le serveur virtuel SMTP.

> **Remarque** Si vous activez cette clé de Registre sur un serveur Exchange, le paramètre s'applique à l'ensemble des serveurs virtuels SMTP hébergés sur ce serveur Exchange. Pour configurer un seul serveur virtuel SMTP à l'aide de ce paramètre, activez la clé de Registre uniquement sur le serveur virtuel SMTP concerné.

> **Avertissement** Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données importantes.

Pour permettre à un serveur Exchange d'accepter les propriétés de message étendues envoyées de façon anonyme

1. Démarrez l'Éditeur du Registre. cliquez sur **Démarrer**, sur **Exécuter**, puis tapez **regedit**.
2. Dans l'arborescence de la console, accédez à la clé de Registre suivante : **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SMTPSVC\XEXCH50**
3. Cliquez avec le bouton droit sur **XEXCH50**, pointez sur **Nouveau**, puis cliquez sur **Valeur DWORD**.
4. Dans le volet d'informations, tapez **Exch50AuthCheckEnabled** pour indiquer le nom de la valeur. Par défaut, la valeur est **0**, indiquant que les propriétés XEXCH50 sont transmises lors de l'envoi anonyme du courrier.

Configuration d'un serveur virtuel SMTP pour obliger l'acceptation des propriétés de message étendues envoyées de façon anonyme

Utilisez la procédure suivante pour configurer le serveur virtuel SMTP situé sur le serveur Exchange, afin de l'obliger à accepter des propriétés étendues.

Pour permettre à un serveur virtuel SMTP d'accepter les propriétés de message étendues envoyées de façon anonyme

1. Démarrez l'Éditeur du Registre. cliquez sur **Démarrer**, sur **Exécuter**, puis tapez **regedit**.
2. Dans l'arborescence de la console, accédez à la clé de Registre suivante : **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SMTPSVC\XEXCH50**
3. Cliquez avec le bouton droit sur **XEXCH50**, pointez sur **Nouveau**, puis cliquez sur **Clé**.
4. Tapez le numéro d'instance du serveur virtuel SMTP en tant que valeur de la clé. Par exemple, la valeur **1** correspond à l'instance du serveur virtuel SMTP par défaut, alors que la valeur **2** correspond au second serveur virtuel SMTP créé sur un serveur.
5. Cliquez avec le bouton droit sur la clé que vous venez de créer, pointez sur **Nouveau**, puis cliquez sur **Valeur DWORD**.
6. Dans le volet d'informations, tapez **Exch50AuthCheckEnabled** pour indiquer le nom de la valeur. Par défaut, la valeur est **0**, indiquant que les propriétés XEXCH50 sont transmises lors de l'envoi anonyme du courrier.

Connexion à Internet

Maintenant que vous avez configuré les messages internes et que vous avez pris connaissance de divers scénarios de connectivité Internet, vous êtes en mesure de connecter votre organisation Exchange à Internet. Ce chapitre contient des informations de procédure sur la manière de configurer votre organisation Microsoft® Exchange Server 2003 pour l'envoi et la réception de messages Internet. En particulier, vous apprendrez à :

- **Vérifier que SMTP est installé correctement** Vérifiez que le service SMTP (Simple Mail Transfer Protocol) fonctionne correctement sur votre serveur Exchange avant de vous connecter à Internet.
- **Utiliser un Assistant pour configurer la remise des messages Internet** L'Assistant Messagerie Internet est principalement destiné aux petites et moyennes entreprises dont l'environnement est moins complexe que celui des grandes entreprises ou des environnements étendus.
- **Configurer manuellement la remise des messages Internet** Dans un environnement étendu ou celui d'une grande entreprise, vous devrez peut-être configurer la remise des messages Internet manuellement, conformément aux stratégies de votre organisation. Lors de la configuration manuelle des messages Internet, vous devez effectuer un ensemble de tâches distinctes associées à la configuration d'Exchange pour l'envoi et la réception des messages Internet.

Procédures du chapitre 7

Le tableau 7.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 7.1 Procédures du chapitre 7 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Vérifier que SMTP est installé correctement	Membre du groupe Administrateurs local.
Démarrer l'Assistant Messagerie Internet	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Vérifier que vos stratégies de destinataire ne contiennent pas d'adresses qui correspondent au nom de domaine complet	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Vérifier que vos utilisateurs peuvent recevoir des messages d'autres domaines SMTP	Membre du groupe Administrateurs local.
Configurer les adresses de messagerie SMTP nécessaires pour vos utilisateurs	Membre du groupe d'administrateurs locaux et membre d'un groupe auquel le Rôle Administrateurs Exchange a été appliqué au niveau de l'organisation.
Configurer le port entrant et les adresses IP sur votre serveur virtuel SMTP	Membre du groupe d'administrateurs locaux et membre d'un groupe auquel le Rôle Administrateurs Exchange a été appliqué au niveau du groupe d'administration.
Vérifiez que votre serveur virtuel SMTP autorise l'accès anonyme	Membre du groupe d'administrateurs locaux et membre d'un groupe auquel le Rôle Administrateurs

Procédure	Autorisations ou rôles requis
	Exchange Affichage seul permettant d'afficher la configuration ou le Rôle Administrateurs Exchange permettant de modifier celle-ci, a été appliqué au niveau du groupe d'administration.
Vérifier les restrictions de relais sur un serveur virtuel SMTP	Membre du groupe d'administrateurs locaux et membre d'un groupe auquel le Rôle Administrateurs Exchange Affichage seul permettant d'afficher la configuration ou le Rôle Administrateurs Exchange a été appliqué au niveau du groupe d'administration.
Vérifier que votre port sortant est défini pour utiliser le port 25	Membre du groupe d'administrateurs locaux et membre d'un groupe auquel le Rôle Administrateurs Exchange Affichage seul permettant d'afficher la configuration ou le Rôle Administrateurs Exchange permettant de modifier celle-ci, a été appliqué au niveau du groupe d'administration.
Autoriser l'accès anonyme sur votre serveur virtuel SMTP sortant	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Créer un connecteur SMTP	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Spécifier un espace d'adressage pour le connecteur	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Configurer les contrôles d'accès et les méthodes d'authentification	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Spécifier les limites des messages	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Veiller à ce que votre serveur Exchange n'utilise pas le format RTF exclusivement	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Définir les limites des messages sortants sur votre serveur virtuel SMTP	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Activer les clés de Registre pour les restrictions de remise	Membre du groupe Administrateurs local.
Définir les restrictions de remise sur le connecteur SMTP	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Définir un calendrier de connecteur	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Définir les restrictions de contenu sur un connecteur	Membre du groupe Administrateurs local et membre

Procédure	Autorisations ou rôles requis
SMTP	d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Définir la gestion des messages non remis	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Vérification de l'installation correcte de SMTP

Pour garantir un flux correct des messages, le service SMTP doit être installé correctement sur le serveur Exchange avec toutes les commandes nécessaires. Si vous rencontrez des problèmes de messagerie, vous devez d'abord vérifier les fonctionnalités de base de votre installation SMTP.

Lorsqu'un serveur Exchange utilise le service SMTP pour communiquer, il doit avoir accès au port 25. Lorsque le service SMTP est configuré correctement, Exchange fournit des verbes SMTP étendus afin de garantir une communication correcte. Ces verbes sont contrôlés dans la métabase des services IIS (Internet Information Services) et dans les récepteurs d'événements Exchange.

Pour déterminer si les verbes Exchange étendus corrects sont chargés, effectuez un test Telnet. Pour ce faire, exécutez la commande Telnet sur le port 25 de l'adresse IP de votre serveur Exchange. Par exemple, tapez le texte suivant à l'invite de commandes :

telnet <*adresse IP serveur*> 25

où *adresse IP serveur* correspond à l'adresse IP de votre serveur Exchange et **25** indique une connexion au port TCP 25. L'exemple suivant illustre une commande Telnet permettant se connecter au port 25 sur un serveur avec l'adresse IP 172.16.0.1 :

```
telnet 172.16.0.1 25
```

Ensuite, tapez **ehlo <*nom serveur*>**, où *nom serveur* correspond au nom de domaine complet de votre serveur Exchange. Votre serveur Exchange répond ensuite en indiquant une liste des verbes SMTP et ESMTP qu'il prend en charge.

L'exemple 1 répertorie les verbes que vous recevrez si le service SMTP est chargé correctement. Si le service SMTP n'est pas configuré correctement, seuls les verbes répertoriés dans l'exemple 2 sont affichés.

Exemple 1 Verbes étendus SMTP (si les récepteurs d'événements Exchange sont chargés proprement)

```
ehlo example.com
250-mail1.example.com Hello [172.16.0.1]
250-TURN
250-ATRN
250-SIZE 5242880
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
```

```
250-VRFY
250-X-EXPS GSSAPI NTLM   *
250-AUTH GSSAPI NTLM
240-X-EXPS=LOGIN  *
250-X-LINK2STATE  *
250-XEXCH50   *
250 OK
```

* Ces verbes étendus doivent être affichés.

Lorsque le service SMTP Exchange n'est pas chargé correctement ou si la métabase IIS est endommagée, les verbes Exchange étendus n'apparaissent pas dans la réponse du serveur. L'exemple 2 répertorie les verbes que vous recevrez si SMTP Exchange n'est pas chargé correctement.

> **Remarque** Les verbes répertoriés dans l'exemple 2 sont les mêmes verbes qui s'affichent si vous n'avez jamais installé Exchange.

Exemple 2 Verbes étendus SMTP (si les récepteurs d'événements Exchange 2003 ne sont pas chargés)

```
ehlo example.com
250-mail1.example.com Hello [172.16.0.1]
250-TURN
250-ATRN
250-SIZE 5242880
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250-AUTH GSSAPI NTLM
250 OK
```

Si vous recevez uniquement les verbes SMTP répertoriés dans l'exemple 2, le service SMTP pour Microsoft Windows® 2000 Server ou Windows Server 2003™ est installé, mais le service SMTP dans Exchange n'est pas chargé correctement. Notez que tous les verbes commençant par « X » (« X » = eXtended) sont manquants.

D'autres listes incomplètes peuvent indiquer également qu'Exchange n'est pas correctement chargé ou que la métabase IIS est peut-être endommagée. Ce problème peut se produire pour plusieurs des raisons suivantes :

- Réinstallation d'Exchange 2003
- Réinstallation de Windows 2000 Server ou Windows Server 2003
- Suppression ou désactivation du service IIS
- Analyse anti-virus du fichier %systemroot%\system32\inetsrv\metabase.bin
- Arrêt inattendu du processus IIsadmin.exe (arrêts non forcés)
- Modification non prise en charge de la métabase
- Endommagement du disque ou autres défaillances matérielles

Si la métabase IIS est endommagée, vous devez charger le service SMTP Exchange correctement.

Pour charger le service SMTP Exchange correctement

Avertissement Si vous utilisez cette procédure, les personnalisations apportées aux services IIS seront perdues. Cette perte potentielle inclut la personnalisation apportée à Microsoft Office Outlook® Web Access ou à d'autres services IIS.

1. Désinstallez le service IIS.
2. Supprimez le fichier metabase.bin.
3. Redémarrez le serveur.
4. Réinstallez le service IIS.
5. Si vous exécutez Exchange sur un serveur Windows 2000, appliquez une nouvelle fois le Service Pack Windows 2000 le plus récent.
6. Réinstallez Exchange. La réinstallation d'Exchange remplace les fichiers manquants et n'affecte pas les paramètres sur le serveur Exchange.
7. Appliquez à nouveau les service packs Exchange et d'autres programmes de mises à jour liés à Exchange (par exemple, les mises à jour Exchange disponibles à partir du site Web Microsoft à l'adresse suivante : http://www.microsoft.com/exchange).

   Remarque Abonnez-vous au service de notification de sécurité Microsoft pour recevoir des notifications automatiquement sur les mises à jour Exchange liées à la sécurité. Vous pouvez vous inscrire à ce service à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=12322.

Utilisation de l'Assistant Messagerie Internet pour configurer la remise des messages Internet

Exchange 2003 met en œuvre une nouvelle version de l'Assistant Messagerie Internet pour vous aider à configurer la connectivité de messagerie Internet dans Exchange Server 2003 ou Exchange 2000 Server. L'Assistant Messagerie Internet vous permet de configurer un serveur Exchange pour envoyer et/ou recevoir des messages Internet. En outre, grâce à cet assistant, vous n'avez pas besoin de configurer le connecteur SMTP et le serveur virtuel SMTP manuellement. L'Assistant Messagerie Internet crée automatiquement le connecteur SMTP nécessaire aux messages Internet sortants et configure la prise en charge des messages entrants sur votre serveur virtuel SMTP.

Remarque Vous ne pouvez pas exécuter l'Assistant Messagerie Internet si vous avez déjà installé les connecteurs SMTP, modifié l'adresse IP ou le numéro de port de votre serveur SMTP par défaut ou créé des serveurs virtuels SMTP supplémentaires sur votre serveur Exchange, sauf si vous rétablissez la configuration de votre serveur par défaut.

Important L'Assistant Messagerie Internet s'adresse surtout aux petites et moyennes entreprises dont l'environnement est moins complexe que celui des grandes entreprises. Si votre environnement de messagerie est complexe ou s'il concerne une grande entreprise, vous devez configurer Exchange manuellement pour la remise des messages Internet. Pour plus d'informations sur la configuration manuelle, consultez la section « Configuration manuelle de votre serveur Exchange pour la remise de messages Internet » plus loin dans ce chapitre.

Conditions préalables pour la remise des messages Internet

Même si l'Assistant Messagerie Internet configure votre serveur virtuel SMTP et votre connecteur SMTP pour une remise des messages Internet, vous devez effectuer les tâches répertoriées dans le tableau 7.2 avant d'exécuter l'Assistant.

Tableau 7.2 Conditions préalables à l'exécution de l'Assistant Messagerie Internet

Étape	Tâche	Remarques
1	Vérifier que le service SMTP est installé correctement sur votre serveur Exchange.	Pour plus d'informations sur la vérification de l'installation correcte de SMTP, consultez « Vérification de l'installation correcte de SMTP » plus haut dans ce chapitre.
2	Vérifier que le serveur DNS est correctement configuré.	Pour envoyer des messages Internet, le serveur DNS utilisé par votre serveur Exchange doit être en mesure de résoudre les adresses externes. Pour recevoir des messages Internet, vous devez avoir un enregistrement de ressource de serveur de messagerie (MX) qui pointe vers l'adresse IP du serveur virtuel SMTP qui reçoit les messages Internet entrants. De plus, votre serveur de messagerie doit être accessible depuis Internet pour que d'autres serveurs DNS puissent résoudre l'enregistrement MX. Pour plus d'informations sur la vérification de la configuration correcte du service DNS, consultez la section « Configuration du service DNS pour les messages sortants » au chapitre 4.

Exécution de l'assistant

L'Assistant Messagerie Internet vous permet de configurer Exchange pour envoyer et/ou recevoir des messages Internet. N'oubliez pas que si votre environnement de messagerie est étendu ou complexe, vous ne pouvez pas utiliser l'Assistant Messagerie Internet. À la place, vous devez configurer Exchange manuellement pour une remise des messages Internet.

Pour utiliser l'Assistant Messagerie Internet

1. Dans le Gestionnaire système Exchange, cliquez avec le bouton droit sur votre organisation Exchange, puis cliquez sur **Assistant Messagerie Internet**.

   Remarque Pour exécuter l'Assistant Messagerie Internet, vous devez utiliser la version du Gestionnaire système Exchange livrée avec Exchange Server 2003.

2. Suivez les instructions de l'Assistant pour effectuer les tâches de configuration (voir les tableaux 7.3 et 7.4) nécessaires à la configuration de la remise des messages Internet.

   Tableau 7.3 Configuration de l'envoi des messages à l'aide de l'Assistant Messagerie Internet

Tâche	Remarques

Tâche	Remarques
Dans votre organisation, sélectionner un serveur Exchange pour l'envoi des messages Internet.	Vous ne pouvez pas exécuter l'Assistant sur un serveur sur lequel vous avez déjà configuré les connecteurs SMTP ou créé des serveurs virtuels SMTP supplémentaires. L'Assistant vous permet uniquement de désigner des serveurs Exchange 2000 ou ultérieurs.
Désigner un serveur tête de pont.	Ce serveur sert de serveur Exchange et de serveur virtuel SMTP. L'Assistant crée un connecteur SMTP sur le serveur virtuel SMTP et le serveur Exchange sélectionnés. Le serveur tête de pont sortant gère tous les messages envoyés par l'intermédiaire de ce connecteur.
Configurer l'envoi des messages Internet sur un connecteur SMTP.	L'Assistant Messagerie Internet vous guide tout au long du processus de configuration de votre connecteur SMTP. Les options à votre disposition incluent les caractéristiques suivantes : • Vous pouvez autoriser la remise des messages Internet vers tous les domaines externes ou vers certains domaines spécifiques uniquement. • Vous pouvez préciser si le connecteur SMTP utilise DNS pour l'envoi des messages et la résolution des noms de domaines externes, ou s'il fait appel à un hôte intelligent capable d'assumer ces fonctions.
Vérifier que votre serveur virtuel SMTP n'est pas ouvert pour le relais des messages.	Quand il est ouvert, le relais permet aux utilisateurs externes d'employer votre serveur pour envoyer du courrier commercial non sollicité, également connu sous le nom de courrier indésirable, ce qui peut pousser les utilisateurs autorisés à bloquer les messages au niveau du serveur Exchange. Si vous empêchez votre serveur de relayer des messages, seuls les utilisateurs authentifiés pourront envoyer des messages vers Internet à l'aide de votre serveur.

Tableau 7.4 Configuration de la réception des messages à l'aide de l'Assistant Messagerie Internet

Tâche	Remarques
Dans votre organisation, sélectionner un serveur Exchange pour la réception des messages Internet.	Vous ne pouvez pas exécuter l'Assistant sur un serveur sur lequel vous avez déjà configuré les connecteurs SMTP ou créé des serveurs virtuels SMTP supplémentaires. L'Assistant vous permet uniquement de désigner des serveurs Exchange 2000 ou ultérieurs.
Configurer la réception des messages Internet sur le serveur SMTP.	Pour recevoir des messages Internet entrants, le serveur ne doit disposer que d'un serveur virtuel SMTP avec une adresse IP par défaut **Non assignée** et un port TCP 25 assigné. Si plusieurs serveurs virtuels SMTP sont installés sur le serveur Exchange, ou si l'adresse IP ou l'affectation de port est différente des paramètres par défaut, l'Assistant ne continue pas. Vous devez dans ce cas rétablir la configuration par défaut du serveur Exchange et exécuter de nouveau l'Assistant, ou utiliser le Gestionnaire système Exchange pour configurer Exchange manuellement.
Vérifier que votre serveur virtuel SMTP autorise l'accès anonyme.	Les autres serveurs sur Internet s'attendent à pouvoir se connecter de manière anonyme à votre serveur virtuel SMTP. Ainsi, vous devez autoriser l'accès anonyme à votre serveur virtuel SMTP. Si l'accès anonyme n'est pas configuré, l'Assistant vous guide tout au long de la procédure d'activation de ce service.

Tâche	Remarques
Configurer vos stratégies de destinataire avec les domaines SMTP à partir desquels vous souhaitez recevoir des messages entrants.	Les domaines SMTP desquels vous souhaitez recevoir des messages Internet sont configurés dans les **Stratégies de destinataire**, dans le Gestionnaire système Exchange. À chaque domaine SMTP duquel seront acceptés des messages Internet doit correspondre une stratégie de destinataire, et Exchange doit faire autorité pour ce domaine ou disposer d'un connecteur pour ce domaine vers lequel le relais des messages est autorisé. Utilisez cette stratégie si votre stratégie de destinataire par défaut contient le domaine de messagerie approprié pour votre organisation. L'Assistant ne permet pas de créer d'autres stratégies de destinataire si vous en avez déjà créé dans le Gestionnaire système Exchange. Dans ce cas, l'ajout ou la modification de stratégies du destinataire doit s'effectuer directement dans le Gestionnaire système Exchange. Pour plus d'informations sur la configuration manuelle de vos stratégies de destinataire, consultez la section « Configuration des stratégies de destinataire » plus loin dans ce chapitre. N'oubliez pas que vos serveurs DNS doivent être en mesure de résoudre tous les noms de domaine soit localement, soit en utilisant des redirecteurs configurés dans le service DNS. Si votre serveur DNS n'est pas en mesure de résoudre de noms de domaine, Exchange ne peut par traiter les messages.

Configuration d'un serveur à double hébergement à l'aide de l'Assistant

Si vous utilisez l'Assistant Messagerie Internet pour configurer la remise des messages Internet sur un serveur à double hébergement (serveur configuré avec deux ou plusieurs adresses réseau, généralement équipé de deux cartes d'interface réseau), l'Assistant effectue les étapes de la configuration décrites dans les tableaux 7.3 et 7.4.

L'Assistant crée également un serveur SMTP supplémentaire sur le serveur Exchange. Il active la remise des messages Internet sur le serveur virtuel SMTP de la manière suivante :

- Pour configurer l'envoi des messages Internet sur un serveur, l'Assistant vous guide tout au long du processus d'affectation de l'adresse IP intranet au serveur virtuel SMTP par défaut sur lequel il crée le connecteur SMTP pour l'envoi des messages sortants. Affectez l'adresse IP intranet à ce serveur virtuel de sorte que seuls les utilisateurs internes connectés à votre intranet puissent envoyer des messages.
- Pour configurer la réception des messages Internet sur un serveur, l'Assistant vous guide tout au long du processus d'affectation d'une adresse IP Internet au serveur virtuel SMTP Internet. L'affectation d'une adresse IP Internet à ce serveur virtuel permet aux serveurs externes de se connecter à ce dernier pour l'envoi des messages Internet. Vous devez disposer par ailleurs d'un enregistrement MX sur un serveur DNS Internet qui fait référence à votre serveur et à l'adresse IP du serveur virtuel SMTP Internet.

  Important Pour renforcer la sécurité sur un serveur à double hébergement, les stratégies de sécurité du protocole Internet (IPSec) vous permettent d'appliquer des filtres sur les ports de la carte d'interface réseau Internet (NIC) afin de contrôler de manière absolue les utilisateurs habilités à ouvrir une session sur ce serveur. Pour plus d'informations sur la sécurité IPSec, consultez la documentation Windows.

Configuration manuelle de votre serveur Exchange pour la remise de messages Internet

Si votre environnement de messagerie est étendu ou complexe, l'Assistant Messagerie Internet ne vous permet pas de configurer Exchange pour l'envoi et la réception des messages Internet. À la place, vous devez configurer Exchange manuellement pour une remise des messages Internet. Les sections suivantes expliquent :

- la configuration de la réception des messages Internet sur votre serveur Exchange ;
- la configuration de l'envoi des messages Internet sur votre serveur Exchange ;
- la configuration des paramètres avancés.

Configuration de la réception des messages Internet sur votre serveur Exchange

Cette section explique comment configurer votre serveur Exchange pour recevoir des messages Internet. En particulier, vous apprendrez à :

- configurer des stratégies de destinataire ;
- configurer les paramètres du serveur virtuel SMTP entrants.

Utilisez la liste de vérification du tableau 7.5 afin d'effectuer toutes les étapes de la configuration.

Tableau 7.5 Étapes de configuration de votre serveur Exchange pour la réception des messages Internet

Étape	Tâche	Remarques
1	Vérifier que le service SMTP est installé correctement sur votre serveur Exchange.	Consultez la section « Vérification de l'installation correcte de SMTP », plus haut dans ce chapitre.
2	Vérifier que vous disposez d'un enregistrement MX sur un serveur DNS Internet qui fait référence à votre serveur et à l'adresse IP du serveur virtuel SMTP Internet qui accepte les messages Internet entrants.	Consultez la section « Configuration du service DNS pour les messages sortants » au chapitre 4.
3	Vérifier que votre serveur de messagerie est accessible depuis Internet.	Pour permettre aux serveurs DNS externes de résoudre l'enregistrement MX de votre serveur de messagerie et de contacter ce dernier, votre serveur de messagerie doit être accessible depuis Internet. Consultez la section « Configuration du service DNS pour les messages sortants » au chapitre 4.
4	Vérifier qu'aucune stratégie de destinataire ne correspond au nom de domaine complet d'un serveur Exchange	Consultez la section « Configuration des stratégies de

Étape	Tâche	Remarques
		destinataire » plus loin dans ce chapitre.
5	Vérifier que chaque domaine pour lequel vous voulez recevoir des messages Internet entrants figure dans une stratégie de destinataire et qu'Exchange fait autorité pour ce domaine, ou, s'il ne fait pas autorité, Exchange possède un connecteur configuré pour le domaine et autorise le relais des messages vers celui-ci.	Consultez la section « Configuration des stratégies de destinataire » plus loin dans ce chapitre.
6	Vérifier que votre serveur virtuel SMTP entrant utilise le port 25 et est assigné aux adresses IP correctes.	D'autres serveurs SMTP attendent de se connecter à votre serveur virtuel SMTP sur le port 25. Consultez la section « Configuration du port entrant et de l'adresse IP sur votre serveur virtuel SMTP » plus loin dans ce chapitre.
7	Vérifier que votre serveur virtuel SMTP entrant autorise l'accès anonyme.	D'autres serveurs SMTP attendent de se connecter de manière anonyme à votre serveur virtuel SMTP. Consultez la section « Vérification de l'autorisation d'accès anonyme par votre serveur virtuel SMTP entrant », plus loin dans ce chapitre.
8	Vérifier que les restrictions de relais par défaut sont configurées sur votre serveur virtuel SMTP entrant.	Les restrictions par défaut sur un serveur virtuel SMTP empêchent le relais ouvert. Quand il est ouvert, le relais permet aux utilisateurs externes d'employer votre serveur pour envoyer du courrier indésirable, ce qui peut pousser les serveurs autorisés à bloquer les messages au niveau de votre serveur Exchange.

Configuration des stratégies de destinataire

Exchange utilise les stratégies de destinataire pour déterminer les messages qu'il peut accepter et router en interne vers les boîtes aux lettres de votre organisation. Les stratégies de destinataire qui ne sont pas configurées correctement peuvent perturber le flux des messages pour certains ou tous les destinataires dans votre système de messagerie. Pour vérifier la configuration de vos stratégies de destinataire :

- Vérifiez que les stratégies de destinataire n'incluent pas une adresse SMTP qui correspond au nom de domaine complet d'un serveur Exchange dans votre organisation. Par exemple, si @serveurexchange.example.com est répertorié comme adresse SMTP et comme nom de domaine sur une stratégie de destinataire, cela empêche le routage des messages vers d'autres serveurs dans le groupe de routage.

- Vérifiez que le domaine dont vous souhaitez recevoir les messages SMTP est recensé dans la stratégie de destinataire par défaut ou dans une autre stratégie. Ces informations permettent de vous assurer que vos utilisateurs peuvent recevoir des messages d'autres domaines SMTP.
- Vérifiez que les adresses de messagerie SMTP nécessaires sont configurées en vue de la réception des messages électroniques pour les autres domaines. Si vous ne recevez aucun message électronique pour l'ensemble de vos domaines SMTP, vous devrez peut-être configurer des adresses SMTP supplémentaires pour vos destinataires. Par exemple, certains de vos utilisateurs reçoivent peut-être des messages électroniques adressés à contoso.com mais vous souhaitez qu'ils reçoivent également des messages adressés à fourthcoffee.com.

Vérification de l'absence dans les stratégies de destinataire d'adresses SMTP qui correspondent au nom de domaine complet d'un serveur Exchange

Pour vérifier que vos stratégies de destinataire sont configurées correctement et correspondent à votre domaine de messagerie (par exemple, @example.com) plutôt qu'au nom de domaine complet de votre serveur Exchange (par exemple, @exchange.example.com), effectuez la procédure suivante.

Pour vérifier que vos stratégies de destinataire ne contiennent pas d'adresses qui correspondent au nom de domaine complet

1. Dans l'arborescence de la console, développez **Destinataires**, puis cliquez sur **Stratégies de destinataire**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur une stratégie de destinataire configurée sur le serveur, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Adresses de messagerie (Stratégie)** de cette stratégie, affichez les adresses SMTP qui sont configurées par cette stratégie et veillez à ce qu'aucune des adresses SMTP ne corresponde au nom de domaine complet des serveurs Exchange dans votre organisation (figure 7.1).

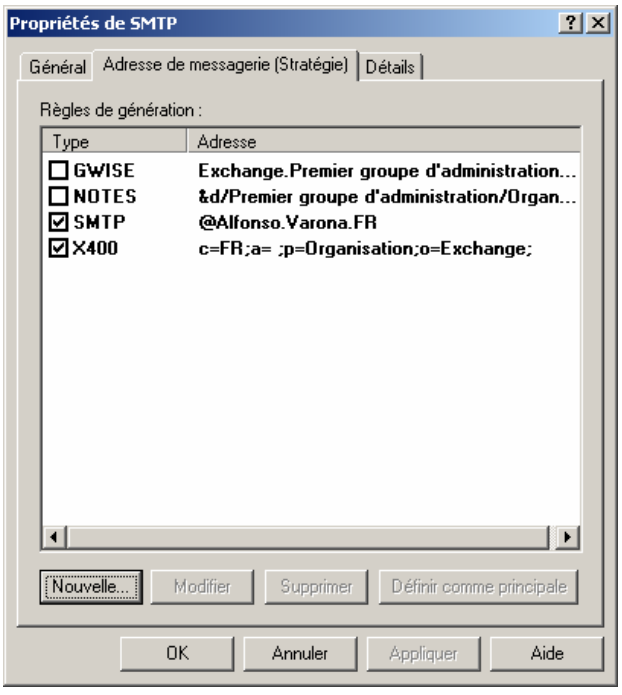


Figure 7.1 Adresses SMTP sur une stratégie de destinataire

4. Répétez les étapes 2 et 3 de cette procédure pour chaque stratégie de destinataire configurée sur ce serveur.

Pour plus d'informations sur les raisons expliquant la non-correspondance entre les stratégies de destinataire et le nom de domaine complet des serveurs Exchange, consultez l'article 288175 (en anglais) de la Base de connaissances Microsoft, « XCON : Recipient Policy Cannot Match the FQDN of Any Server in the Organization, 5.4.8 NDRs » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=288175). Bien que cet article ait été écrit pour Exchange 2000, les principes s'appliquent également à Exchange 2003.

Vérification de la réception des messages d'autres domaines SMTP par les destinataires

Pour recevoir des messages électroniques d'autres domaines SMTP, votre stratégie de destinataire doit spécifier correctement le domaine pour lequel vous souhaitez recevoir des messages.

> **Important** Par défaut, le nom de domaine SMTP dans la stratégie de destinataire par défaut est le nom du domaine qui héberge le service d'annuaire Microsoft Active Directory®. Ce nom de domaine SMTP par défaut ne correspond pas toujours au même nom que vous souhaitez utiliser pour les messages SMTP.

Par exemple, si votre organisation est une grande entreprise distribuée, vous pouvez utiliser une adresse SMTP unique pour créer des adresses de messagerie distinctes pour les destinataires de chaque division. Par exemple, les utilisateurs des différentes divisions de l'entreprise Jouet Mania peuvent avoir des adresses telles que `untel@administration.jouetmania.com` et `untel@marketing.jouetmania.com`.

Effectuez la procédure suivante pour confirmer que les destinataires dans votre organisation sont en mesure de recevoir des messages d'autres domaines SMTP.

Pour vérifier que vos utilisateurs peuvent recevoir des messages d'autres domaines SMTP

1. Dans le Gestionnaire système Exchange, dans l'arborescence de la console, développez **Destinataires**, puis cliquez sur **Stratégies de destinataire**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur une stratégie de destinataire configurée sur ce serveur, puis cliquez sur **Propriétés**.
3. Dans l'onglet **Adresses de messagerie (Stratégie)** de cette stratégie, affichez les adresses SMTP qui sont configurées par cette stratégie, puis veillez à ce que le domaine pour lequel vous souhaitez recevoir des messages SMTP est répertorié en tant qu'adresse. Vérifiez que la case à cocher en regard de l'adresse est activée.
4. Double-cliquez sur l'adresse SMTP souhaitée, puis dans **Propriétés de Adresse SMTP**, vérifiez que la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse** est activée (Figure 7.2).

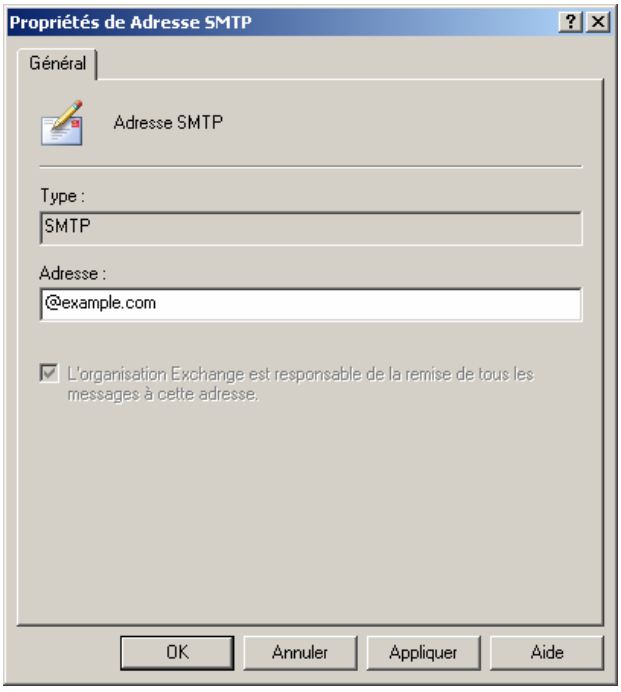


Figure 7.2 Boîte de dialogue Propriétés de Adresse SMTP

Remarque Si vous disposez de plusieurs stratégies de destinataire configurées sur un serveur, l'adresse électronique SMTP que vous tentez de vérifier figure peut-être dans une autre stratégie de destinataire.

5. Si vous avez plusieurs stratégies de destinataire configurées sur un serveur, répétez les étapes 3 à 5 de cette procédure pour chaque stratégie de destinataire.

Configuration des adresses de messagerie SMTP pour vos utilisateurs

La procédure suivante vous permet de vérifier que l'adresse de messagerie de chaque utilisateur est correctement configurée dans une stratégie de destinataire. N'oubliez pas qu' Exchange accepte uniquement les messages pour des adresses configurées correctement dans une stratégie de destinataire. Ces adresses sont stockées dans Active Directory et dans la métabase IIS où le catégoriseur de messages vérifie les informations de configuration et d'adresse.

Pour configurer les adresses de messagerie SMTP nécessaires pour vos utilisateurs

1. Dans le Gestionnaire système Exchange, dans l'arborescence de la console, développez **Destinataires**, puis cliquez sur **Stratégies de destinataire**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur la stratégie de destinataire à modifier, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Adresses de messagerie (Stratégie)**, cliquez sur **Nouvelle**.
4. Dans **Nouvelle adresse de messagerie**, cliquez sur **Adresse SMTP**, puis sur **OK**.
5. Dans **Propriétés de Adresse SMTP**, dans la zone **Adresse**, tapez les informations requises par le type d'adresse que vous avez sélectionné. Par exemple, pour router les messages vers Example Corporation, tapez **@example.com** (Figure 7.3).

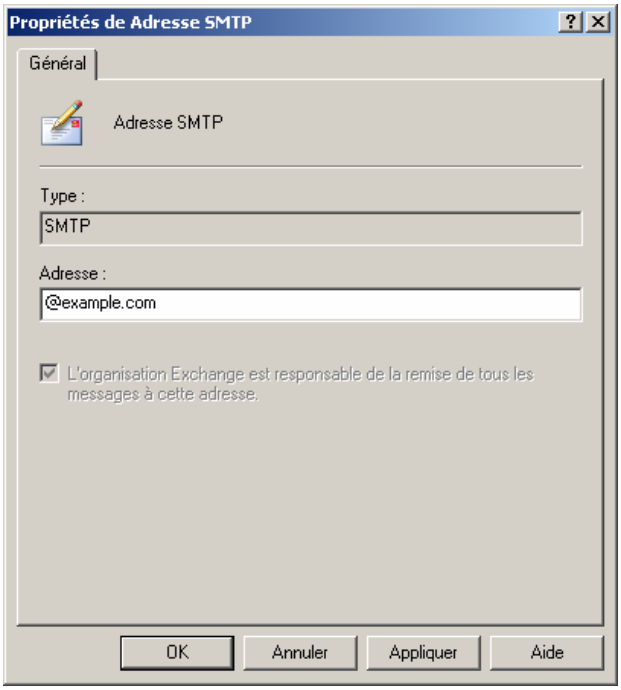


Figure 7.3 Boîte de dialogue Propriétés de Adresse SMTP

6. Vérifiez que la case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse** est activée, puis cliquez sur **OK**.

   Remarque La case à cocher **L'organisation Exchange est responsable de la remise de tous les messages à cette adresse** détermine si Exchange fait autorité ou non pour le domaine sélectionné. Si Exchange fait autorité pour un domaine, il accepte tous les messages de ce domaine ; si Exchange ne localise pas de destinataire valide dans Active Directory, celui-ci retourne un rapport de non-remise pour le message.

7. Pour garantir un suivi des informations relatives à la stratégie de destinataire que vous avez modifiée, dans les propriétés de stratégie de destinataire, cliquez sur l'onglet **Détails**. Sous **Remarque administrative**, tapez les informations relatives à l'adresse que vous avez ajoutée à la stratégie de destinataire.

8. Sous l'onglet **Adresses de messagerie (Stratégie)**, sous **Règles de génération**, sélectionnez l'adresse que vous avez ajoutée, puis cliquez sur **Appliquer**.

   Important Lorsque vous cliquez sur **Appliquer**, Exchange peut vous demander de mettre à jour toutes les adresses de messagerie de destinataire correspondantes pour appliquer les modifications que vous avez apportées. Si vous cliquez sur **Oui**, les modifications apportées à la stratégie de destinataire sont appliquées aux destinataires définis pour la stratégie du cycle suivant du service de mise à jour de destinataire. Les adresses de messagerie configurées précédemment pour ces destinataires sont rétrogradées à des adresses secondaires.

Si vous souhaitez que cette adresse de messagerie ne s'applique qu'à un sous-ensemble d'utilisateurs, créez une nouvelle stratégie de destinataire avec un filtre qui sélectionne le sous-ensemble de destinataires spécifié. Si le filtre est trop complexe ou que seul un petit nombre d'utilisateurs nécessite l'adresse supplémentaire, vous pouvez concevoir un filtre qui crée des adresses de messagerie qui s'appliquent uniquement à des destinataires individuels.

Attention Tous les domaines de messagerie SMTP pour lesquels Exchange accepte des messages doivent posséder une stratégie de destinataire configurée ; toutefois, il n'est pas nécessaire que cette stratégie de destinataire s'applique à chaque utilisateur. Vous pouvez ajouter des nouvelles adresses de messagerie SMTP, mais il est impératif que ces adresses de messagerie SMTP ne correspondent pas

aux noms de domaine complets dans votre organisation. Si une adresse de messagerie SMTP correspond au nom de domaine complet d'un serveur, le flux des messages distants et locaux s'arrêtera.

Pour plus d'informations sur la configuration des stratégies de destinataire, consultez l'article 260973 (en anglais) de la Base de connaissances Microsoft, « XCON : Setting Up SMTP Domains for Inbound and Relay E-Mail in Exchange 2000 Server and Exchange Server 2003 » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=260973). Bien que cet article ait été écrit pour Exchange 2000, les principes s'appliquent également à Exchange 2003.

Pour plus d'informations sur la résolution des problèmes avec les adresses proxy SMTP, consultez l'article 140933 (en anglais) de la Base de connaissances Microsoft, « XFOR: SMTP Proxy Address Generated Incorrectly » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=140933). Bien que cet article ait été écrit pour Exchange 2000, les principes s'appliquent également à Exchange 2003.

Configuration des paramètres entrants sur les serveurs virtuels SMTP

Pour configurer la réception des messages Internet sur votre serveur virtuel SMTP, vous devez effectuer les tâches suivantes :

- Configurer le port entrant en tant que port 25 et spécifier l'adresse IP.
- Vérifier que votre serveur virtuel SMTP entrant autorise l'accès anonyme.
- Pour des raisons de sécurité, vérifiez les restrictions de relais sur votre serveur virtuel entrant. Par défaut, les paramètres de relais autorisent uniquement les utilisateurs autorisés à relayer des messages.

  Important Vous devez vérifier que les paramètres de votre serveur virtuel SMTP sont corrects. Vous devez également connaître les conséquences liées aux choix de configurations spécifiques lors de la résolution des problèmes concernant le flux des messages liés à SMTP.

Configuration du port entrant et de l'adresse IP sur votre serveur virtuel SMTP

Le port entrant est le port où le serveur virtuel SMTP est à l'écoute des communications entrantes ; l'adresse IP est l'adresse vers laquelle sont envoyées les demandes entrantes. Par défaut, le serveur virtuel SMTP par défaut utilise le port 25 et toutes les adresses IP disponibles pour écouter les demandes entrantes.

Pour configurer le port entrant et les adresses IP sur votre serveur virtuel SMTP

1. Cliquez avec le bouton droit sur **Serveur virtuel SMTP par défaut**, puis cliquez sur **Propriétés**.
2. Dans **Propriétés de Serveur virtuel SMTP par défaut**, cliquez sur l'onglet **Général** (Figure 7.4).

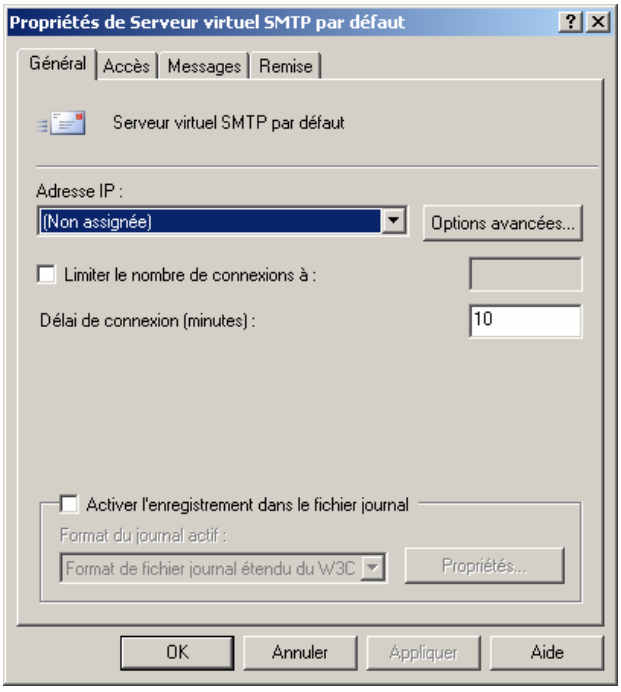


Figure 7.4 Onglet Général de la boîte de dialogue Propriétés de Serveur virtuel SMTP par défaut

3. Sous **Serveur virtuel SMTP par défaut**, vérifiez les paramètres suivants :
4. **Adresse IP** Le paramètre par défaut est **(Non assignée)**. Vous ne devez pas modifier ce paramètre sauf si vous souhaitez configurer plusieurs serveurs virtuels SMTP. (Il s'agit de l'adresse IP utilisée pour les connexions entrantes.)
5. Si vous avez plusieurs cartes d'interface réseau (NIC) ou plusieurs adresses IP assignées à une seule carte d'interface réseau pour l'écoute de ce serveur virtuel SMTP, et que vous voulez sélectionner des adresses IP individuelles, cliquez sur **Options avancées**, puis spécifiez des ports différents du port par défaut.

> **Remarque** Utilisez les **Options avancées** avec discernement. D'autres serveurs (sur Internet par exemple) s'attendent à communiquer avec votre serveur sur le port TCP 25 par défaut.

Vérification de l'autorisation d'accès anonyme par votre serveur virtuel SMTP entrant

Comme vous le savez, les autres serveurs SMTP sur Internet s'attendent à pouvoir se connecter de manière anonyme à votre serveur virtuel SMTP. N'oubliez pas que si vous n'autorisez pas l'accès anonyme sur vos serveurs de passerelle qui acceptent les messages Internet, les autres serveurs SMTP sur Internet ne peuvent pas envoyer de messages à votre organisation.

Pour vérifier que votre serveur virtuel SMTP autorise l'accès anonyme

1. Cliquez avec le bouton droit sur votre serveur virtuel SMTP, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Accès**, puis sur **Authentification**.
3. Dans **Authentification**, vérifiez que la case à cocher **Accès anonyme** est activée (Figure 7.5).

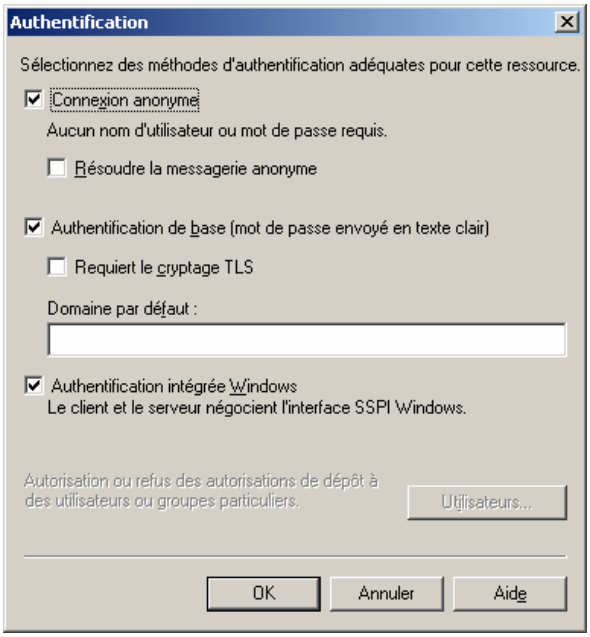


Figure 7.5 Boîte de dialogue Authentification

Vérification des restrictions de relais par défaut sur votre serveur virtuel SMTP entrant

Par défaut, le serveur virtuel SMTP par défaut n'autorise que les utilisateurs authentifiés à relayer des messages électroniques. Ce paramètre est préférable car il empêche les utilisateurs non autorisés d'utiliser le serveur Exchange pour l'envoi de messages électroniques vers les domaines externes. La configuration de relais la plus sécurisée exige l'authentification de tous les utilisateurs qui se connectent depuis Internet et tentent le relais des messages.

Comme indiqué précédemment, les serveurs têtes de pont connectés à Internet et qui acceptent les messages Internet doivent généralement accepter des connexions anonymes ; cependant, par défaut, ces serveurs têtes de pont n'autorisent pas les relais anonymes. Il est fortement déconseillé d'autoriser le relais anonyme. Si vous l'autorisez, les autres utilisateurs peuvent utiliser votre serveur pour envoyer du courrier indésirable. Cette activité peut entraîner ultérieurement l'interdiction de votre serveur par d'autres serveurs Internet.

Pour vérifier les restrictions de relais sur un serveur virtuel SMTP

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Développez **Serveurs**, ***<nom de serveur>***, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur **Serveur virtuel SMTP par défaut**, puis cliquez sur **Propriétés**.
4. Dans **Propriétés de Serveur virtuel SMTP par défaut**, cliquez sur l'onglet **Accès** (Figure 7.6).

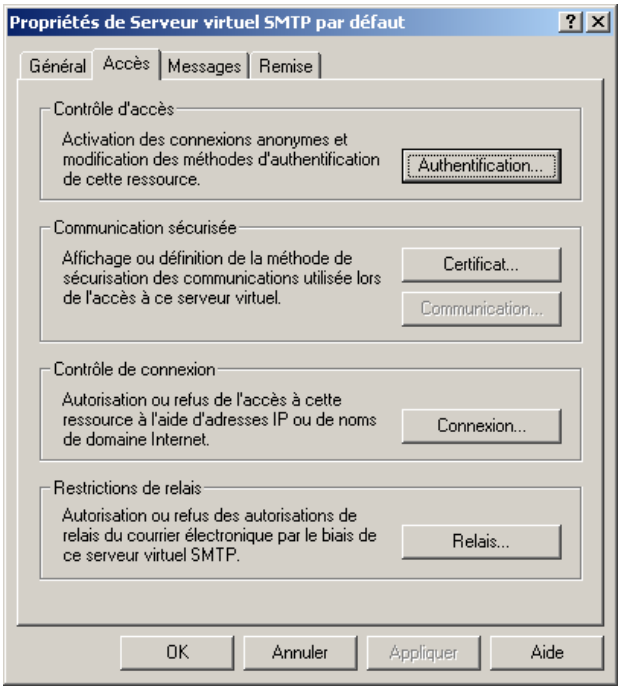


Figure 7.6 Onglet Accès de la boîte de dialogue Propriétés de Serveur virtuel SMTP par défaut

5. Sous **Restrictions de relais**, cliquez sur **Relais** pour vérifier les restrictions de relais. La boîte de dialogue **Restrictions de relais** apparaît (Figure 7.7).

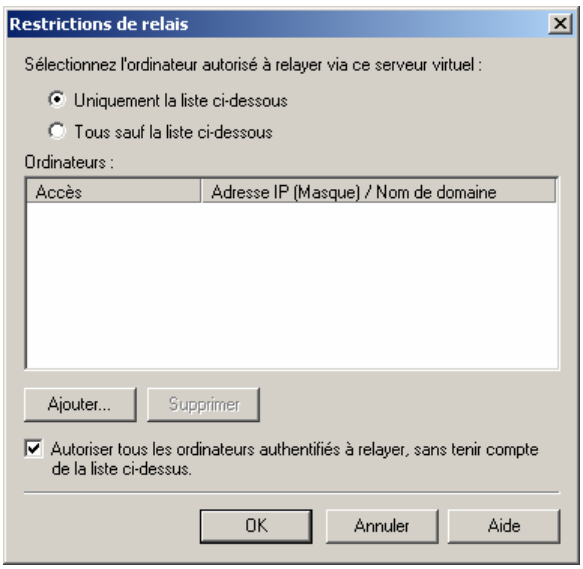


Figure 7.7 Restrictions de relais par défaut dans la boîte de dialogue Restrictions de relais

6. Dans **Restrictions de relais**, vérifiez les paramètres suivants :

   - Vérifiez que l'option **Uniquement la liste ci-dessous** est sélectionnée. Pour afficher uniquement les hôtes que vous voulez autoriser à relayer des messages, cliquez sur **Ajouter**, puis suivez les instructions. Si vous cliquez sur **Tous sauf la liste ci-dessous**, votre serveur peut se révéler être une source de courrier commercial non sollicité sur Internet.
   - Vérifiez que la case à cocher **Autoriser tous les ordinateurs authentifiés à relayer, sans tenir compte de la liste ci-dessus** est activée. Ce paramètre vous permet de refuser l'accès à tous les

utilisateurs qui ne s'authentifient pas. Tous les utilisateurs POP (Post Office Protocol) et IMAP (Internet Message Access Protocol) distants qui accèdent à ce serveur s'authentifient pour envoyer des messages. Si aucun de vos utilisateurs n'accède à ce serveur par l'intermédiaire du protocole IMAP ou POP, vous pouvez désactiver cette case à cocher pour bloquer la fonction de relais et augmenter ainsi la sécurité.

Configuration de l'envoi des messages Internet sur votre serveur Exchange

Cette section explique comment configurer votre serveur Exchange pour l'envoi des messages Internet. En particulier, vous apprendrez à :

- configurer les paramètres sortants sur des serveurs virtuels SMTP ;
- configurer un hôte actif sur un serveur virtuel SMTP ;
- configurer un connecteur SMTP.

Utilisez la liste de vérification du tableau 7.6 afin d'effectuer toutes les étapes de la configuration nécessaires pour configurer votre serveur Exchange pour envoyer des messages Internet. Chaque étape est expliquée en détail dans les sections suivantes ou plus haut dans ce document.

Tableau 7.6 Étapes de configuration de votre serveur Exchange pour l'envoi des messages Internet

Étape	Tâche	Remarques
1	Vérifier que SMTP est chargé correctement sur votre serveur Exchange.	Consultez la section « Vérification de l'installation correcte de SMTP », plus haut dans ce chapitre.
2	Vérifier que votre serveur DNS est en mesure de résoudre les noms (Internet) externes	Consultez la section « Configuration du service DNS pour les messages sortants » au chapitre 4.
3	Vérifier que le port sortant de votre serveur virtuel SMTP est défini sur 25.	Les autres serveurs SMTP sur Internet s'attendent à ce que votre serveur virtuel SMTP se connecte à eux sur le port 25. Consultez la section « Vérification du paramétrage du port TCP sortant sur 25 » plus loin dans ce chapitre.
4	Vérifier que votre serveur virtuel SMTP sortant autorise l'accès anonyme.	Les autres serveurs SMTP sur Internet ne s'attendent pas à ce que votre serveur SMTP s'authentifie. Consultez la section « Autorisation d'accès anonyme sur le serveur virtuel sortant », plus loin dans ce chapitre.
5	Si vous devez configurer un hôte actif sur votre serveur virtuel SMTP, vérifiez que celui-ci est configuré correctement.	Il est recommandé de configurer les hôtes actifs sur un connecteur SMTP plutôt que sur le serveur virtuel lui-même. Si vous devez configurer un hôte actif sur le

Étape	Tâche	Remarques
		serveur virtuel SMTP, vérifiez que celui-ci répond aux critères définis dans la section « Configuration d'un hôte actif sur un serveur virtuel SMTP », plus loin dans ce chapitre.
6	Créer un connecteur SMTP sur votre serveur virtuel SMTP sortant avec un espace d'adressage * (astérisque) pour router les messages Internet.	Lorsque vous créez un connecteur SMTP avec un espace d'adressage *, Exchange route tous les messages Internet par l'intermédiaire de ce connecteur. Consultez la section « Configuration d'un connecteur SMTP », plus loin dans ce chapitre.

Configuration des paramètres des messages sortants sur les serveurs virtuels SMTP

Les paramètres de messages sortants sur un serveur virtuel SMTP contrôlent les ports et les adresses IP par lesquels les messages sortants sont envoyés. Les connecteurs configurés sur les serveurs têtes de pont qui routent les messages vers Internet utilisent ces paramètres. Vous pouvez configurer la plupart de ces paramètres sous l'onglet **Remise** dans les propriétés du serveur virtuel SMTP.

Pour configurer votre serveur virtuel SMTP pour la remise des messages sortants, vous devez :

- vérifier que le port sortant est défini sur le port 25 (paramètre par défaut) ;
- autoriser l'accès anonyme pour votre connexion sortante (paramètre par défaut) ;
- définir des serveurs DNS externes pour une utilisation par SMTP, si nécessaire ; vous pouvez configurer le serveur virtuel SMTP pour qu'il utilise un serveur DNS externe ; cependant, il est plus simple et plus courant de s'appuyer sur les serveurs DNS internes pour transmettre les requêtes DNS aux serveurs DNS externes configurés.

Vérification du paramétrage du port TCP sortant sur 25

Pour configurer le port sortant utilisé par votre serveur pour la remise des messages Internet, utilisez l'onglet **Remise** dans les propriétés du serveur virtuel SMTP. Si vous utilisez les mêmes serveurs de passerelle pour l'envoi et la réception de messages Internet, les ports entrants et sortants doivent être définis sur le port 25.

Pour vérifier que votre port sortant est défini pour utiliser le port 25

1. Cliquez avec le bouton droit sur **Serveur virtuel SMTP par défaut**, puis cliquez sur **Propriétés**.
2. Dans **Propriétés de Serveur virtuel SMTP par défaut**, cliquez sur l'onglet **Remise**. Sous cet onglet, vous pouvez spécifier les paramètres de messages sortants tels que les horloges de nouvelle tentative, les limites de connexion et de sécurité sortantes ainsi que d'autres paramètres avancés (Figure 7.8).

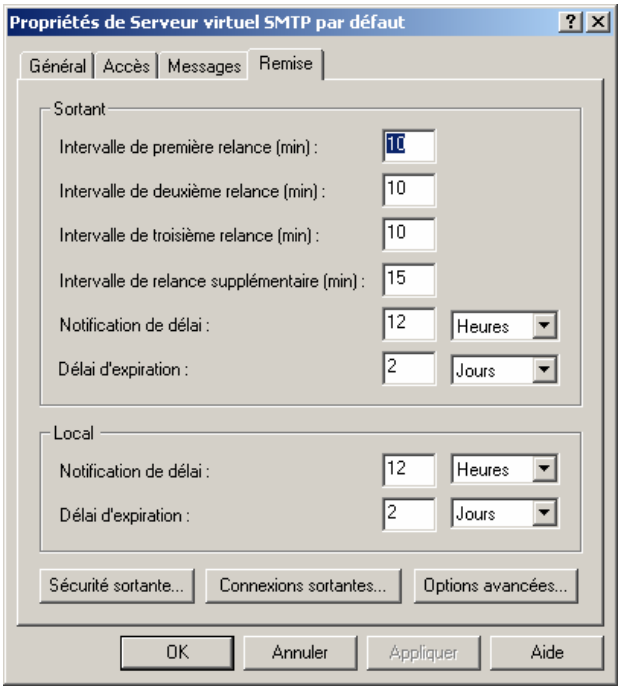


Figure 7.8 Onglet Remise de Propriétés d'un serveur virtuel SMTP par défaut

3. Dans l'onglet **Remise**, cliquez sur **Connexions sortantes** pour définir le port TCP utilisé par le serveur pour se connecter aux serveurs distants. La boîte de dialogue **Connexions sortantes** apparaît (Figure 7.9).

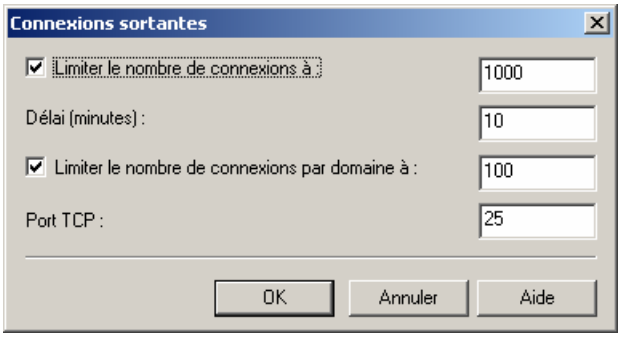


Figure 7.9 Boîte de dialogue Connexions sortantes

4. Dans **Connexions sortantes**, vérifiez que le **Port TCP** est défini sur **25**. Les serveurs distants sur Internet s'attendent à utiliser votre serveur sur le port TCP 25. Il n'est pas recommandé d'attribuer une autre valeur que 25 au **Port TCP**.

Autorisation d'accès anonyme sur le serveur virtuel sortant

Pour votre serveur virtuel SMTP sortant, vous devez autoriser l'accès anonyme (sauf si vous vous connectez directement à un hôte actif). Les serveurs distants sur Internet ne s'attendent pas à ce que votre serveur s'authentifie.

> **Remarque** Généralement, la configuration d'un hôte actif fonctionne mieux sur un connecteur. La configuration d'un hôte actif sur un serveur virtuel SMTP n'est pas la méthode préférée.

Pour autoriser l'accès anonyme sur votre serveur virtuel SMTP sortant

1. Cliquez avec le bouton droit sur ***<votre serveur virtuel SMTP sortant>***, puis cliquez sur **Propriétés**.

2. Cliquez sur l'onglet **Remise**.
3. Cliquez sur **Sécurité sortante** pour sélectionner le type d'authentification utilisé par le serveur avec les serveurs distants.
4. Dans **Sécurité sortante**, cliquez sur **Accès anonyme** (Figure 7.10).

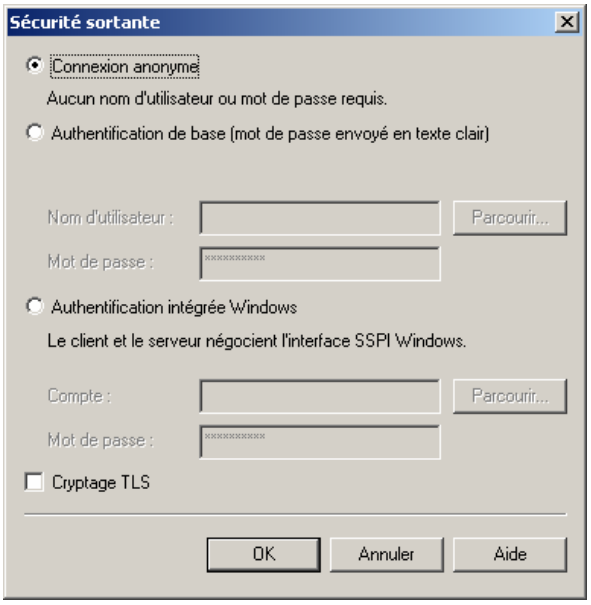


Figure 7.10 Boîte de dialogue Sécurité sortante

> **Remarque** Si vous vous connectez à un hôte actif (configuré en cliquant sur **Options avancées** sous l'onglet **Remise**), celui-ci peut exiger votre authentification. Pour déterminer si l'authentification est nécessaire, contactez le propriétaire de l'hôte actif ou votre fournisseur de services Internet.

Configuration d'un hôte actif sur un serveur virtuel SMTP

Des problèmes peuvent se produire si vous définissez l'hôte actif au niveau du serveur virtuel plutôt qu'au niveau du connecteur SMTP. Lorsque vous configurez l'hôte actif au niveau du serveur virtuel, prenez en compte les restrictions suivantes :

> **Remarque** Les paramètres d'hôte actif suivants figurent dans la boîte de dialogue **Remise avancée**. Pour accéder à cette boîte de dialogue, dans **Propriétés de <*votre serveur virtuel SMTP sortant*>**, sous l'onglet **Remise**, cliquez sur **Options avancées**.

- Si votre organisation Exchange contient plusieurs ordinateurs exécutant Exchange, vous ne devez pas entrer de données dans la zone **Hôte actif**. Le flux des messages entre les serveurs peut ne pas fonctionner.
- Si une adresse IP est répertoriée dans la zone **Hôte actif**, elle doit figurer entre crochets, par exemple, [10.0.0.1].
- Si une adresse IP est répertoriée dans la zone **Hôte actif**, vérifiez que celle-ci ne correspond pas à l'adresse IP de ce serveur Exchange.
- Si un nom est répertorié dans la zone **Hôte actif**, celui-ci doit correspondre à un nom de domaine complet. Par exemple, « Nom de serveur » ne représente pas un nom de domaine complet, contrairement à nomdeserveur.contoso.com.
- Si un nom est répertorié dans la zone **Hôte actif**, celui-ci ne doit pas correspondre au nom de domaine complet de ce serveur.

- Si vous ne disposez pas d'un hôte actif dans votre réseau, contactez votre fournisseur de services Internet (ISP) pour connaître l'adresse IP ou le nom de domaine complet à utiliser.
- Si vous entrez un hôte actif, activez la case à cocher **Essayer la remise directe avant l'envoi à l'hôte actif**. L'activation de cette case à cocher peut réduire la file d'attente sur ce serveur.
- L'utilisation de plusieurs hôtes actifs et l'équilibrage de la charge des requêtes entre ces hôtes exigent une configuration spécifique.

Configuration d'un connecteur SMTP

Les connecteurs SMTP offrent un moyen efficace de router les messages Internet. Cette section explique comment créer et configurer un connecteur SMTP pour l'envoi des messages Internet.

Création d'un connecteur SMTP

Pour créer un connecteur SMTP, procédez de la manière suivante :

Pour créer un connecteur SMTP

1. Dans le Gestionnaire système Exchange, cliquez avec le bouton droit sur **Connecteurs**, pointez sur **Nouveau**, puis cliquez sur **Connecteur SMTP**.
2. Dans **Propriétés**, sous l'onglet **Général**, dans la zone **Nom**, tapez un nom pour le connecteur (Figure 7.11).

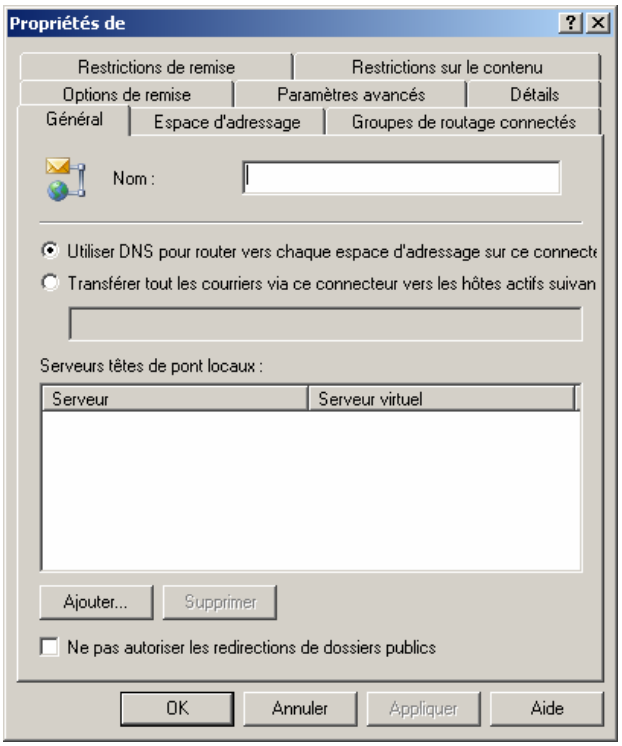


Figure 7.11 Propriétés du connecteur SMTP

3. Activez l'une des cases à cocher suivantes :
   - Si vous souhaitez que ce connecteur fasse appel à des noms DNS pour router des messages directement vers le serveur distant, sélectionnez **Utiliser DNS pour router vers chaque espace d'adressage sur ce connecteur**. En activant cette option, le connecteur utilise le serveur DNS

configuré pour le routage des messages électroniques. Si vous activez cette case à cocher, vérifiez les informations suivantes :

- Vérifiez que vous pouvez utiliser Nslookup pour résoudre correctement les noms sur Internet. Pour plus d'informations sur la topologie de routage, consultez le chapitre 5 « Configuration de votre topologie de routage ».

- Si vous voulez router des messages vers un hôte actif chargé de la résolution de noms DNS et de la remise des messages, activez la case à cocher **Transférer tous les courriers via ce connecteur aux hôtes actifs suivants**. Cette option s'utilise souvent si vous routez des messages vers un serveur SMTP Windows ou un autre serveur dans votre réseau de périmètre. Si vous activez cette case à cocher, vérifiez les informations suivantes :

  - Si vous répertoriez une adresse IP pour l'hôte actif, insérez-la entre crochets, par exemple,`[10.0.0.1]`.
  - Si vous spécifiez une adresse IP pour l'hôte actif, celle-ci ne doit pas correspondre à l'adresse IP de ce serveur.
  - Si vous spécifiez un nom pour l'hôte actif, le nom doit être un nom de domaine complet. Par exemple, “`Server Name`” ne représente pas un nom de domaine complet, contrairement à `servername.contoso.com`.
  - Si un nom est spécifié, celui-ci ne doit pas correspondre au nom de domaine complet de ce serveur.
  - Si vous ne disposez pas d'un hôte actif dans votre réseau, contactez votre fournisseur de services Internet (ISP) pour connaître l'adresse IP ou le nom de domaine complet à utiliser.

4. Sous **Serveurs têtes de pont locaux**, cliquez sur **Ajouter** pour définir au moins un serveur tête de pont et un serveur virtuel SMTP. Pour envoyer des messages sortants, le connecteur utilise le port de sortie configuré sur le serveur virtuel SMTP.

Configuration d’un espace d’adressage

L'espace d'adressage d'un connecteur définit le domaine ou une plage de domaines vers lequel un connecteur envoie des messages. Vous pouvez spécifier quels groupes d'adressage seront gérés par un connecteur spécifique. Si vous utilisez plusieurs connecteurs SMTP pour router des messages Internet, au moins un connecteur doit posséder un espace d'adressage * (astérisque). L'astérisque représente tous les domaines externes.

Pour spécifier un espace d'adressage pour le connecteur

1. Dans les **Propriétés** du connecteur SMTP, cliquez sur l'onglet **Espace d'adressage**.
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un espace d'adressage** apparaît (Figure 7.12).

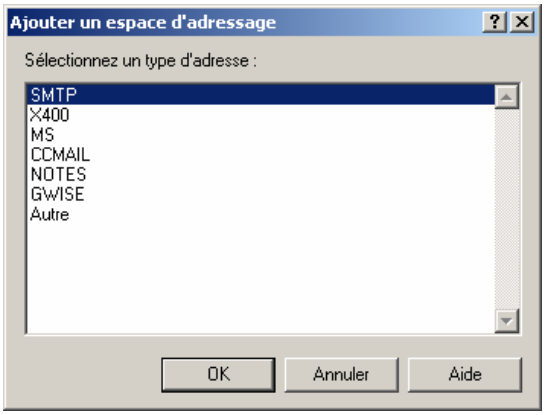


Figure 7.12 Boîte de dialogue Ajouter un espace d'adressage

3. Sous **Sélectionnez un type d'adresse**, cliquez sur **SMTP**, puis sur **OK**. La boîte de dialogue **Propriétés de l'espace d'adressage Internet** apparaît (Figure 7.13).

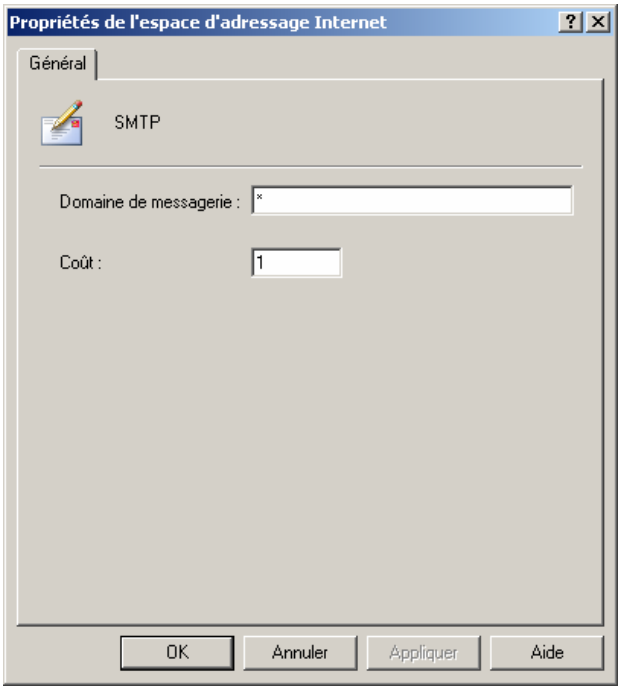


Figure 7.13 Boîte de dialogue Propriétés de l'espace d'adressage Internet

> **Important** Dans **Propriétés de l'espace d'adressage Internet**, dans la zone **Domaine de messagerie**, la valeur par défaut est *****. ***** représente toutes les adresses. Au moins un connecteur dans votre organisation doit avoir cet espace d'adressage afin de garantir que tous les domaines externes sont routés vers Internet.

4. Dans **Propriétés de l'espace d'adressage Internet**, dans la zone **Domaine de messagerie**, tapez le domaine de messagerie du connecteur. Dans la zone **Coût**, attribuez un coût approprié pour ce connecteur. Par exemple, si vous voulez que l'ensemble des utilisateurs utilise toujours ce connecteur et n'utilise qu'un connecteur de sauvegarde si ce connecteur n'est plus disponible, attribuez à ce connecteur un coût de **1** et un coût supérieur au deuxième connecteur. N'oubliez pas qu'Exchange choisit toujours le chemin de routage le moins onéreux, si celui-ci est disponible.

Important Ne listez pas vos domaines entrants sur l'espace d'adressage SMTP d'un connecteur. Vos domaines entrants sont recensés dans vos stratégies de destinataire. (Pour plus d'informations sur les stratégies de destinataire, consultez la section « Configuration des stratégies de destinataire », plus haut dans ce chapitre.) Si certains ou l'ensemble de vos domaines entrants sont répertoriés, vous recevrez peut-être un rapport de non-remise qui indique un bouclage des messages (ces rapports de non-remise peuvent avoir le code de diagnostic 5.3.5). En spécifiant les domaines sous l'onglet **Espace d'adressage**, vous pouvez configurer ces domaines comme des domaines routables.

5. Cliquez sur **OK** pour revenir à l'onglet **Espace d'adressage**.
6. Sous **Portée du connecteur**, sélectionnez l'une des options suivantes en fonction de la topologie de votre routage :
   - Sélectionnez **Organisation entière** si vous voulez que les utilisateurs dans les groupes de routage puissent envoyer des messages Internet par l'intermédiaire de ce connecteur. Une fois cette option sélectionnée, tous les serveurs Exchange dans l'organisation peuvent router des messages vers Internet par l'intermédiaire de ce connecteur.
   - Sélectionnez **Groupe de routage** pour limiter l'envoi de messages par l'intermédiaire de ce connecteur aux utilisateurs appartenant au groupe de routage de ce serveur tête de pont.

     Remarque Pour plus d'informations sur l'attribution des coûts et la limitation d'étendue, consultez la section « Description des restrictions et de la portée du connecteur » au chapitre 5.
7. Pour relayer les messages par l'intermédiaire de votre système vers les domaines spécifiés, activez la case à cocher **Autoriser les messages à être relayés vers ces domaines**.

   Remarque N'activez pas cette case à cocher si vous créez un connecteur avec un espace d'adressage *.
8. Cliquez sur **OK**.

Configuration des paramètres avancés

Cette section explique la configuration de certains paramètres avancés qui contrôlent la remise des messages Internet. Même si ces paramètres ne jouent pas un rôle essentiel dans le flux des messages, ils peuvent vous aider à paramétrer les performances, à contrôler l'accès à vos serveurs virtuels SMTP, et de nombreux autres domaines.

En particulier, vous apprendrez à :

- configurer des paramètres entrants avancés ;
- configurer des paramètres sortants avancés ;
- configurer des paramètres avancés sur le connecteur SMTP ;
- configurer la notification des rapports de remise.

Configuration des paramètres entrants avancés

Cette section vous montre comment configurer les paramètres avancés pour des messages entrants. En particulier, vous apprendrez à :

- configurer des contrôles d'accès et d'autres paramètres de sécurité ;
- configurer des filtres de messages ;
- définir des limites pour les messages entrants.

Configuration des contrôles d'accès et des paramètres de sécurité

Pour des serveurs virtuels SMTP, vous pouvez spécifier les types de connexions acceptées ou refusées et exiger l'authentification des utilisateurs avant la remise des messages. Si vous prenez en charge les clients POP ou IMAP qui se connectent depuis Internet, les méthodes d'authentification sont pratiques. Cependant, sur un serveur virtuel SMTP qui fonctionne comme passerelle Internet, vous ne pouvez pas exiger d'authentification si vous souhaitez recevoir des messages de la part d'utilisateurs sur Internet.

Pour configurer les contrôles d'accès et les méthodes d'authentification

1. Cliquez avec le bouton droit sur **Serveur virtuel SMTP par défaut**, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Accès**, puis, sous **Contrôle d'accès**, cliquez sur **Authentification** pour spécifier les méthodes d'authentification des utilisateurs avant l'envoi des messages vers ce serveur. La boîte de dialogue **Authentification** apparaît (Figure 7.14).

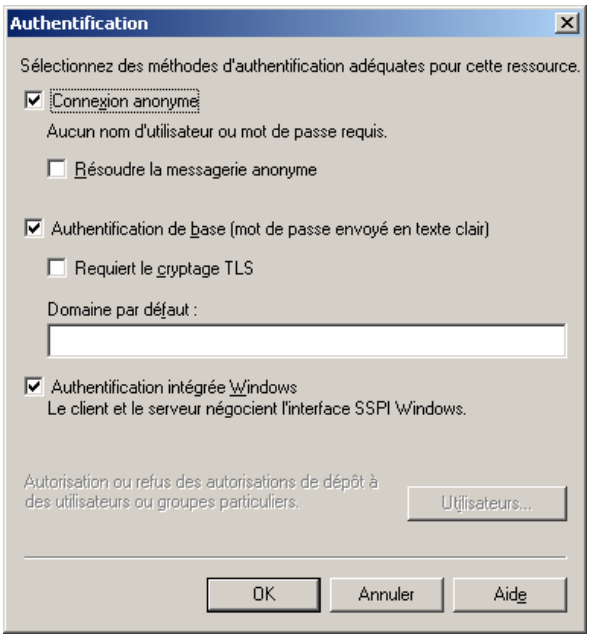


Figure 7.14 Boîte de dialogue Authentification

3. Dans **Authentification**, les cases à cocher suivantes sont disponibles :

   - **Accès anonyme** Généralement, vous activez cette case à cocher pour des serveurs connectés directement à Internet. Si vous activez cette case à cocher, d'autres serveurs sur Internet ne s'authentifient pas auprès de ce serveur avant l'envoi des messages. Pour une sécurité accrue, désactivez l'accès anonyme sur vos serveurs virtuels SMTP internes qui n'acceptent pas les messages Internet entrants. Pour des raisons de sécurité similaires, vous pouvez également désactiver l'accès anonyme sur des serveurs virtuels SMTP dédiés et utilisés pour les utilisateurs IMAP et POP.

     Remarque Si la case à cocher **Accès anonyme** n'est pas sélectionnée sur vos serveurs de passerelle Internet, vous risquez de ne pas recevoir de messages entrants provenant d'Internet. Cependant, pour les serveurs virtuels SMTP internes ou les serveurs SMTP utilisés exclusivement par des utilisateurs IMAP et POP, vous pouvez désactiver cette case à cocher car ces derniers doivent s'authentifier.

   - **Authentification de base** Utilisez cette case à cocher pour les clients de messagerie (tels que Microsoft Outlook) qui utilisent les services POP3 (Post Office Protocol version 3) ou IMAP4

(Internet Message Access Protocol version 4rev1) pour se connecter au serveur. Pour envoyer des messages électroniques, ces clients s'authentifient auprès du serveur.

Important Si vous activez la case à cocher **Authentification de base (mot de passe envoyé en texte clair)**, les noms d'utilisateur et les mots de passe sont envoyés sur le réseau en texte clair. Ces informations peuvent être facilement interceptées sur Internet. Si vous utilisez une authentification de base, vous pouvez envisager la mise en œuvre du service TLS (Transport Layer Security) pour accroître la sécurité.

- **Requiert le cryptage TLS** Utilisez cette case à cocher si vous disposez d'un certificat numérique, une pratique courante dans un environnement haute sécurité. Si vous activez cette case à cocher, dans la zone **Domaine par défaut** correspondante, vous devez taper le nom de domaine Windows 2000 ou Windows Server 2003 auprès duquel l'utilisateur doit s'authentifier s'il ou elle ne spécifie pas de domaine. Pour plus d'informations sur le cryptage TLS, consultez la documentation en ligne d'Exchange.
- **Authentification intégrée Windows** Cette case à cocher est utilisée uniquement par les comptes d'utilisateur Windows. À l'aide du protocole NTLM, les mots de passe et les noms d'utilisateur sont cryptés et transmis ensuite au serveur virtuel SMTP à des fins d'authentification.

  Remarque Par défaut, les cases à cocher **Accès anonyme**, **Authentification de base** et **Authentification intégrée Windows** sont activées. Si vous utilisez un seul serveur virtuel par défaut, il est recommandé d'utiliser les paramètres par défaut ; les utilisateurs peuvent ainsi s'authentifier à l'aide des méthodes les plus courantes.

4. Dans **Propriétés de <*Serveur virtuel SMTP*>**, sous l'onglet **Accès**, **Communications sécurisées**, cliquez sur **Certificat** pour configurer un certificat (utilisé pour le cryptage TLS) qui crypte les messages au cours de leur transfert d'un serveur à l'autre. Pour plus d'informations sur le cryptage TLS, consultez la documentation en ligne d'Exchange.
5. Dans l'onglet **Accès**, sous **Contrôle de connexion**, cliquez sur **Connexion** pour autoriser ou interdire l'accès au serveur basé sur l'adresse IP. Si vous utilisez plusieurs serveurs virtuels SMTP et que vous voulez refuser l'accès à des hôtes spécifiques, vous devez effectuer les opérations suivantes pour chaque serveur virtuel :
   a. Dans **Connexion**, cliquez sur **Tous sauf la liste ci-dessous** pour des serveurs connectés directement à Internet.
   b. Pour répertorier uniquement les hôtes desquels vous ne voulez pas recevoir de messages, cliquez sur **Ajouter**, puis suivez les instructions dans la boîte de dialogue **Ordinateur**. Vous pouvez inclure les serveurs que vous considérez comme la source de courrier indésirable.
   c. Cliquez sur **OK** deux fois pour appliquer les paramètres.

Définition des limites des messages

Sous l'onglet **Messages** des propriétés du serveur virtuel, vous pouvez configurer le nombre par défaut de destinataires par message. Réduire ce nombre peut atténuer les effets du courrier indésirable en empêchant la remise d'un message unique vers un grand nombre d'utilisateurs. Vous pouvez également réduire la taille maximale des messages et la longueur de chaque session.

Remarque Si votre organisation utilise de grandes listes de distribution qui arrivent via SMTP d'utilisateurs Internet, la réduction du nombre de destinataires par message peut affecter vos utilisateurs. Cependant, les destinataires MAPI (comme les utilisateurs d'Outlook) ne sont pas concernés par la réduction.

Pour spécifier les limites des messages

1. Cliquez avec le bouton droit sur le serveur virtuel SMTP que vous souhaitez configurer, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Messages** pour spécifier les limites de message pour ce serveur (Figure 7.15).

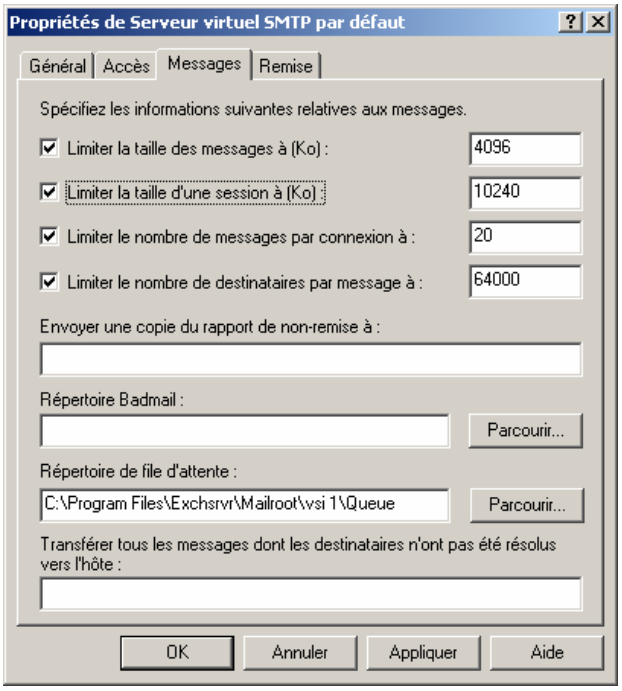


Figure 7.15 Onglet Messages de la boîte de dialogue Propriétés de Serveur virtuel SMTP par défaut

3. Sous **Spécifiez les informations suivantes relatives aux messages**, activez la case à cocher **Limiter la taille des messages à (Ko)** pour limiter la taille maximale de messages. Pour empêcher des utilisateurs d'envoyer des documents volumineux, tapez une petite valeur dans la zone correspondante. Si vous ne définissez pas de limite pour la taille maximale des messages, les performances peuvent s'en ressentir. Il est recommandé de définir une limite égale à la taille maximale de messages appropriée à votre organisation.

   Remarque La taille des documents augmente environ de 33 pour cent lorsqu'ils sont envoyés à l'extérieur du groupe de routage ou de l'organisation. Par exemple, si vous voulez envoyer des documents jusqu'à 3 Mo, définissez la taille maximale des messages à 4,096 Ko.

4. Activez la case à cocher **Limiter la taille d'une session à (Ko)** et tapez une valeur supérieure à la taille maximale de messages.
5. Activez la case à cocher **Limiter le nombre de messages par connexion à** pour configurer le système pour qu'il prévoie l'arrêt de la connexion une fois parvenu au nombre spécifié de messages. Ce paramètre par défaut optimise le flux des messages dans la plupart des topologies de messagerie. Cependant, l'activation de cette case à cocher peut entraîner une légère dégradation des performances si votre système reçoit de nombreux messages d'une source unique.
6. Activez la case à cocher **Limiter le nombre de destinataires par message à** pour qu'Exchange retourne un rapport de non-remise aux expéditeurs dont les messages dépassent le nombre maximal de destinataires. L'activation de cette case à cocher vous permet d'empêcher les utilisateurs d'envoyer un message électronique à un trop grand nombre de destinataires.

Configuration des paramètres sortants avancés

Cette section vous montre comment configurer les paramètres avancés pour contrôler les messages sortants. Vous apprendrez en particulier comment configurer les formats des messages électroniques Internet, les limites des messages sortants et les paramètres de connecteur avancés.

Configuration des formats des messages électroniques Internet

Pour chaque domaine répertorié dans **Formats des messages Internet**, vous pouvez configurer le mode d'envoi des messages électroniques Internet. En règle générale, il ne faut pas envoyer de messages exclusivement au format RTF car de nombreux serveurs de messagerie non Microsoft ne peuvent pas lire les messages au format RTF ; les utilisateurs reçoivent à la place un message électronique vide avec un fichier winmail.dat en pièce jointe. Pour éviter ce problème, vérifiez que votre paramètre de message global n'utilise pas exclusivement le format RTF Exchange.

Pour veiller à ce que votre serveur Exchange n'utilise pas le format RTF exclusivement

1. Dans le Gestionnaire système Exchange, développez l'entrée **Paramètres globaux**, puis cliquez sur **Formats des messages Internet**.
2. Dans le volet droit, cliquez avec le bouton droit sur le nom souhaité, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Paramètres avancés**.
4. Sous **Format RTF Exchange**, vérifiez que l'une des options **Jamais** ou **Définir à l'aide des paramètres utilisateur individuels** est sélectionnée (Figure 7.16).

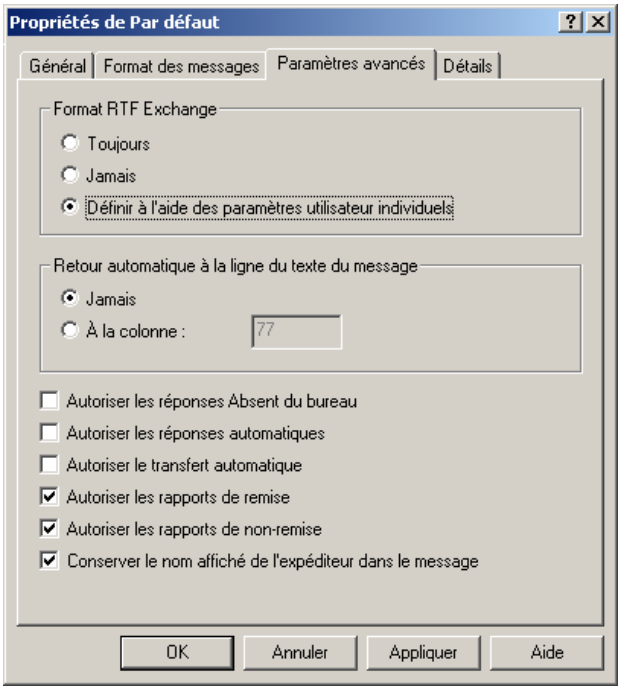


Figure 7.16 Onglet Paramètres avancés pour Formats des messages Internet

> **Remarque** L'activation de **Toujours** peut empêcher les utilisateurs sur des serveurs non Microsoft de lire vos messages électroniques. Ils peuvent recevoir un message électronique avec un fichier winmail.dat en pièce jointe.

Configuration des limites des messages sortants

Sur votre serveur virtuel SMTP chargé de la remise des messages sortants, vous pouvez configurer les limites de connexions et les paramètres de délai que le serveur utilise avec des serveurs distants. Configurez ces limites pour éviter la surcharge de votre serveur.

Pour définir les limites des messages sortants sur votre serveur virtuel SMTP

1. Cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, < ***Nom serveur*** >, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur **<*votre serveur virtuel SMTP sortant*>**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Remise**.
5. Sous **Sortante**, vous pouvez modifier l'heure en minute pour la première, deuxième, troisième tentative et les tentatives ultérieures en entrant les valeurs appropriées pour votre organisation (Figure 7.17). Ces paramètres sortants contrôlent la remise des messages pour les messages envoyés à l'extérieur de l'organisation.

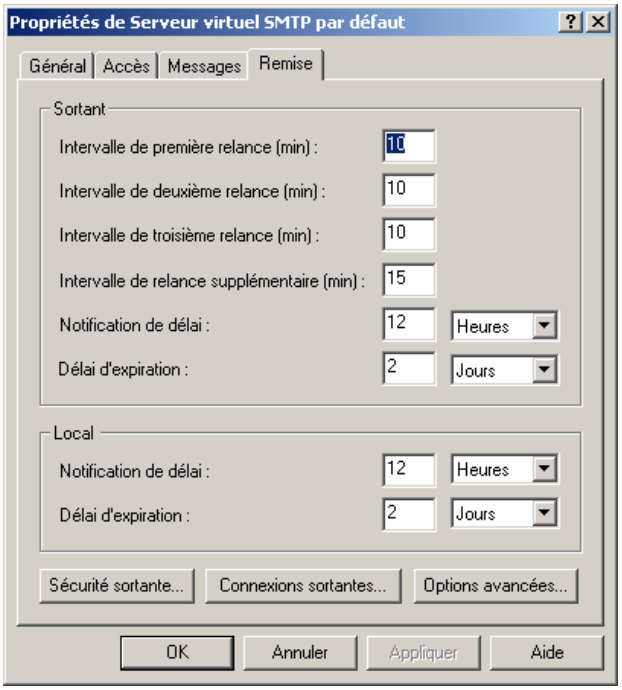


Figure 7.17 Paramètres sortants sous l'onglet Remise

> **Remarque** Le choix d'une valeur trop basse pour un intervalle entre deux tentatives peut nuire aux performances en particulier si votre connexion Internet ou l'hôte actif spécifié n'est pas disponible.

6. Sous **Local**, définissez la **Notification de délai** et le **Délai d'expiration** pour la remise locale des messages en entrant les valeurs dans les zones correspondantes, puis en sélectionnant l'heure dans **Minutes**, **Heures** ou **Jours**. Il est recommandé d'utiliser les paramètres par défaut. Ces paramètres locaux s'appliquent aux messages envoyés vers la banque de boîte aux lettres locale ou dans Microsoft Exchange MTA.

> **Remarque** Les systèmes sur Internet peuvent avoir des valeurs différentes pour la notification de délai et le délai d'expiration. Les valeurs entrées pour ces paramètres concernent les messages en file d'attente sur ce serveur.

7. Cliquez sur **Connexions sortantes** pour configurer des limites de connexion et des valeurs de délai que le serveur utilise avec les serveurs distants. La boîte de dialogue **Connexions sortantes** apparaît (Figure 7.18).

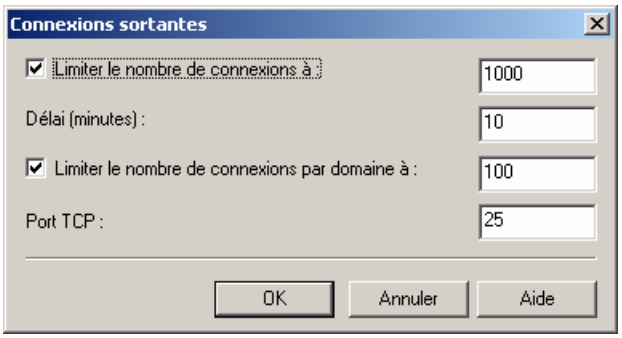


Figure 7.18 Boîte de dialogue Connexions sortantes

8. En fonction de votre matériel, vous pouvez activer la case à cocher **Limiter le nombre de connexions à** pour limiter les connexions aux autres serveurs et réduire le trafic. Vous pouvez également activer la case à cocher **Limiter le nombre de connexions par domaine à**. Après avoir activé les cases à cocher, entrez les valeurs appropriées pour votre organisation.
9. En fonction de la qualité de votre connexion et de votre bande passante, vous pouvez modifier la valeur **Délai (minutes)**.

> **Remarque** La réduction du nombre de connexions sortantes et l'augmentation du délai d'attente peuvent entraîner un délai d'attente des réponses des serveurs distants sur toutes vos connexions sortantes. Avec ces paramètres, les messages électroniques restent en file d'attente durant des périodes plus longues (ce qui peut retarder la livraison des messages), en revanche le trafic réseau est le plus faible possible.

Configuration des paramètres avancés sur le connecteur SMTP

Le connecteur SMTP offre plusieurs options de configuration auxquelles vous pouvez faire appel pour affiner les spécifications de vos messages électroniques routés par l'intermédiaire de ce serveur. Hormis la taille limite des messages, les paramètres sur le connecteur SMTP prennent le pas sur les paramètres du serveur virtuel SMTP. Dans ce cas, la taille limite la plus basse est appliquée.

Dans cette section, vous allez apprendre comment accomplir les tâches suivantes :

- définir des restrictions de remise ;
- définir un calendrier de connecteur pour la connexion à un fournisseur de services réseau ;
- définir les restrictions de contenu sur un connecteur SMTP ;
- configurer la gestion des rapports de non-remise.

Définition de restrictions de remise

Le paramètre par défaut permet à tous les utilisateurs de votre organisation d'utiliser ce connecteur. Dans la plupart des situations, ce paramètre suffit car il permet généralement à vos utilisateurs d'envoyer des messages Internet. Si vous souhaitez définir des restrictions plus strictes, utilisez les procédures suivantes pour définir des restrictions de remise.

Utilisez l'onglet **Remise** pour restreindre l'utilisation de votre connecteur. Cependant, pour activer ces restrictions, vous devez également modifier certains paramètres de clé de Registre.

> **Important** Sachez que restreindre les remises nécessite beaucoup de ressources processus et peut affecter les performances des serveurs.

Une clé du Registre sur le serveur tête de pont basé sur Exchange 2003 (source du connecteur en cours de vérification) contrôle les fonctionnalités vérifiant la restriction. Si vous devez configurer un connecteur pour qu'il limite les expéditeurs de données vers la liaison désignée, vous devez ajouter manuellement la valeur de Registre chargée de vérifier la restriction.

Pour activer les clés de Registre pour les restrictions de remise

> **Avertissement** Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données importantes.

1. Démarrez l'Éditeur du Registre. À une invite de commandes, tapez **Regedit.exe**.
2. Accédez à et sélectionnez la clé suivante dans le Registre :

   HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/RESvc/Parameters/
3. Dans le menu **Edition**, cliquez sur **Ajouter une valeur**, puis ajoutez la valeur de Registre suivante :

   ```
   Value Name: CheckConnectorRestrictions
   Data Type: REG_DWORD
   Date: 1
   Radix: Decimal
   ```
4. Quittez l'Éditeur du Registre : Dans le menu **Registre**, cliquez sur **Quitter**.
5. Après activation du paramètre de la clé du Registre, vous devez redémarrer les services suivants sur votre serveur Exchange :
   - Microsoft Exchange - Piles MTA (MSExchangeMTA)
   - Microsoft Exchange - Moteur de routage (RESvc)
   - Protocole SMTP (SMTPSVC)

Après avoir activé la clé du Registre et redémarré les services, vous pouvez définir des restrictions de remise sur le connecteur SMTP.

Pour définir les restrictions de remise sur le connecteur SMTP

1. Dans le Gestionnaire système Exchange, développez **Connecteurs** en effectuant l'une des opérations suivantes :
   - Si les groupes de routage ou les groupes d'administration ne sont pas affichés, développez votre organisation Exchange, puis **Connecteurs**.
   - Si seuls les groupes de routage sont affichés, développez **Groupes de routage**, <***Nom de groupe de routage***>, puis **Connecteurs**.
   - Si seuls les groupes d'administration sont affichés, développez **Groupes d'administration**, <***Nom de groupe d'administration***>, puis **Connecteurs**.
   - Si les groupes d'administration et les groupes de routage sont affichés, développez **Groupes d'administration**, <***Nom de groupe d'administration***>, **Groupes de routage**, <***Nom de groupe de routage***>, puis **Connecteurs**.
2. Cliquez avec le bouton droit sur **<*votre connecteur SMTP*>**, puis cliquez sur **Propriétés**.

3. Cliquez sur l'onglet **Restrictions de remise** (Figure 7.19).

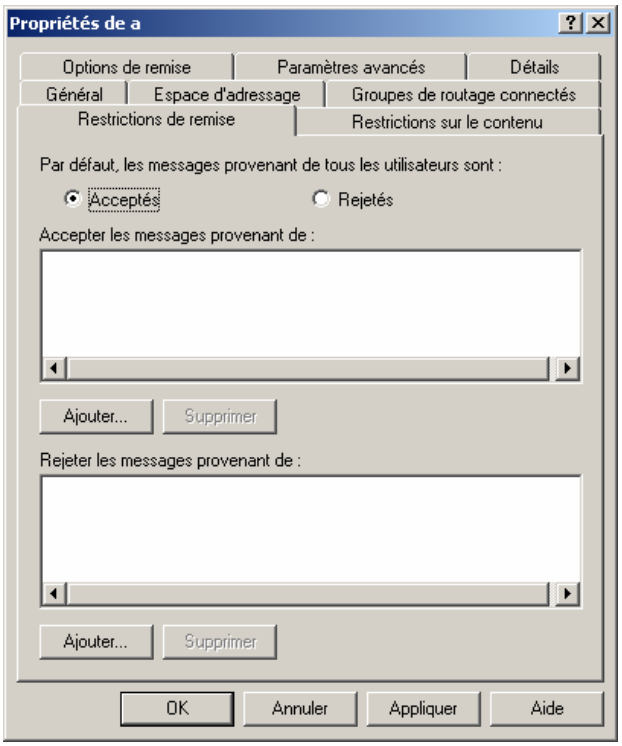


Figure 7.19 Onglet Restrictions de remise de la boîte de dialogue Propriétés du connecteur SMTP

4. Pour accepter des messages de tous les utilisateurs mais rejeter des utilisateurs spécifiés :
   a. Sous Par défaut, les messages provenant de tous les utilisateurs sont, vérifiez que Acceptés est sélectionné.
   b. Sous **Rejeter les messages provenant de**, cliquez sur **Ajouter**, puis, dans **Sélectionnez un destinataire**, tapez le nom de chaque utilisateur ou groupe que vous voulez empêcher d'utiliser le connecteur.
5. Pour rejeter des messages de tous les utilisateurs sauf des utilisateurs spécifiés :
   a. Sous Par défaut, les messages provenant de tous les utilisateurs sont, cliquez sur Refusés.
   b. Sous Accepter les messages provenant de, cliquez sur Ajouter, puis, dans Sélectionnez un destinataire, tapez le nom de chaque utilisateur que vous voulez autoriser à utiliser le connecteur.

Définition d'un calendrier de connecteur pour la connexion à un fournisseur de services réseau

Si vous utilisez un connecteur SMTP pour vous connecter à un fournisseur de services réseau et pour télécharger vos messages Internet, vous souhaitez peut-être planifier des heures spécifiques pour que le connecteur contacte le serveur du fournisseur de services réseau. Vous pouvez également spécifier qu'un connecteur conserve des messages électroniques jusqu'à leur remise déclenchée par un serveur distant.

Pour définir un calendrier de connecteur

1. Dans le Gestionnaire système Exchange, développez **Connecteurs** en effectuant l'une des opérations suivantes :

- Si les groupes de routage ou les groupes d'administration ne sont pas affichés, développez votre organisation Exchange, puis **Connecteurs**.
- Si seuls les groupes de routage sont affichés, développez **Groupes de routage**, <***Nom de groupe de routage***>, puis **Connecteurs**.
- Si seuls les groupes d'administration sont affichés, développez **Groupes d'administration**, <***Nom de groupe d'administration***>, puis **Connecteurs**.
- Si les groupes d'administration et les groupes de routage sont affichés, développez **Groupes d'administration**, <***Nom de groupe d'administration***>, **Groupes de routage**, <***Nom de groupe de routage***>, puis **Connecteurs**.

2. Cliquez avec le bouton droit sur **<*votre connecteur SMTP*>**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Options de remise** (Figure 7.20).

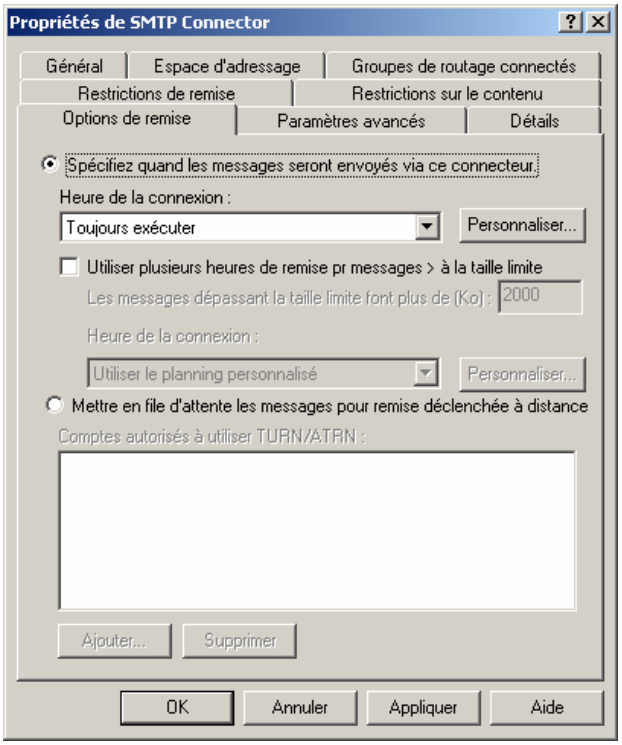


Figure 7.20 Onglet Options de remise de la boîte de dialogue Propriétés du connecteur SMTP

4. Pour définir une heure d'exécution du connecteur, cliquez sur **Spécifiez quand les messages seront envoyés via ce connecteur**.
5. Dans la liste **Heure de la connexion**, sélectionnez une heure ou cliquez sur **Personnaliser** pour créer une planification personnalisée.
6. Pour planifier une heure différente pour la remise par le connecteur des messages de taille limite, activez la case à cocher **Utiliser plusieurs heures de remise pr messages > à la taille limite**. Si vous activez cette case à cocher, les options suivantes s'affichent :
   - **Les messages dépassant la taille limite font plus de (Ko)** Dans cette zone, tapez un nombre du seuil qui définit les messages de taille limite.
   - **Heure de la connexion** Dans cette liste, sélectionnez une heure ou cliquez sur **Personnaliser** pour créer une planification personnalisée.

7. Pour conserver des messages électroniques jusqu'à leur remise déclenchée par un serveur distant, cliquez sur **Mettre en file d'attente les messages pour remise déclenchée à distance**, puis cliquez sur **Ajouter** pour ajouter des comptes autorisés qui peuvent déclencher une remise à distance.

Définition de restrictions sur le contenu

Vous pouvez restreindre le type de messages remis par l'intermédiaire d'un connecteur. Par exemple, si vous avez des besoins particuliers sur le plan commercial ou administratif, vous pouvez restreindre le type de message uniquement aux messages à priorité élevée par l'intermédiaire d'un connecteur particulier.

Pour définir les restrictions de contenu sur un connecteur SMTP

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, accédez à **Connecteurs** en effectuant l'une des opérations suivantes :
   - Sous l'organisation Exchange, développez **Connecteurs**.
   - Si les groupes de routage ne sont pas définis, développez **Groupes d'administration**, <***Nom de groupe d'administration***>, puis **Connecteurs**.
   - Si les groupes de routage sont définis, développez **Groupes d'administration**, <***Nom de groupe d'administration***>, **Groupes de routage**, <***Nom de groupe de routage***>, puis **Connecteurs**.
3. Cliquez avec le bouton droit sur **<*votre connecteur SMTP*>**, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Restrictions sur le contenu** (Figure 7.21).

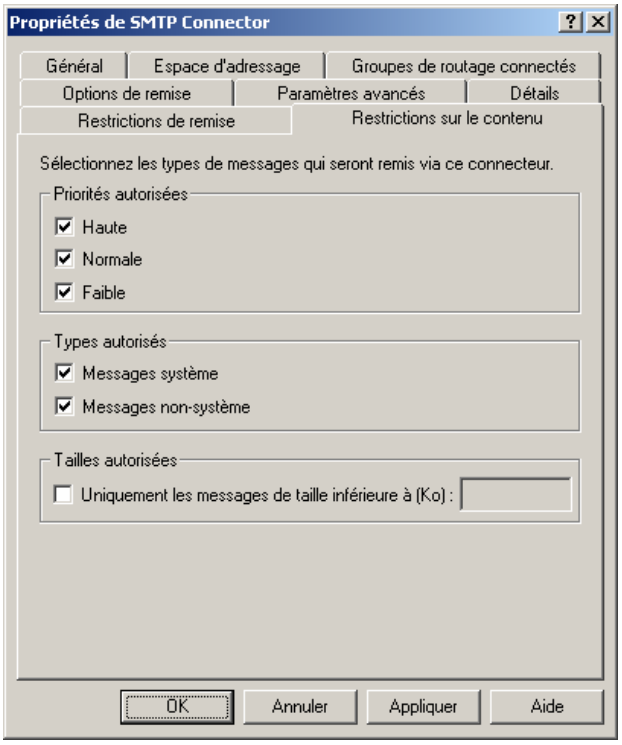


Figure 7.21 Onglet Restrictions de contenu de la boîte de dialogue Propriétés du connecteur SMTP

5. Sous **Priorités autorisées**, sélectionnez chaque type de messages à priorité que vous souhaitez envoyer par l'intermédiaire du connecteur.

6. Sous **Types autorisés**, sélectionnez chaque type de messages (système ou non système) que vous souhaitez envoyer par l'intermédiaire du connecteur.
7. Sous **Tailles autorisées**, si vous souhaitez définir une restriction de taille, activez la case à cocher **Uniquement les messages de taille inférieure à (Ko)**, puis tapez une limite de taille.

Configuration de la notification des rapports de remise

Suivez la procédure suivante pour contrôler la gestion des messages non remis sur un serveur virtuel spécifique. Vous pouvez toujours faire appel au compte administrateur pour la gestion de l'ensemble des rapports de non remise pour une organisation. Si vous partagez un espace de noms avec un autre système de messagerie, et que vous voulez accepter des messages pour ces utilisateurs et transmettre ces messages vers l'autre système en le désignant comme hôte actif, il est utile de définir la gestion des messages non remis sur un serveur virtuel.

Pour définir la gestion des messages non remis

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, < ***Nom serveur*** >, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP souhaité, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Messages** (figure 7.22).

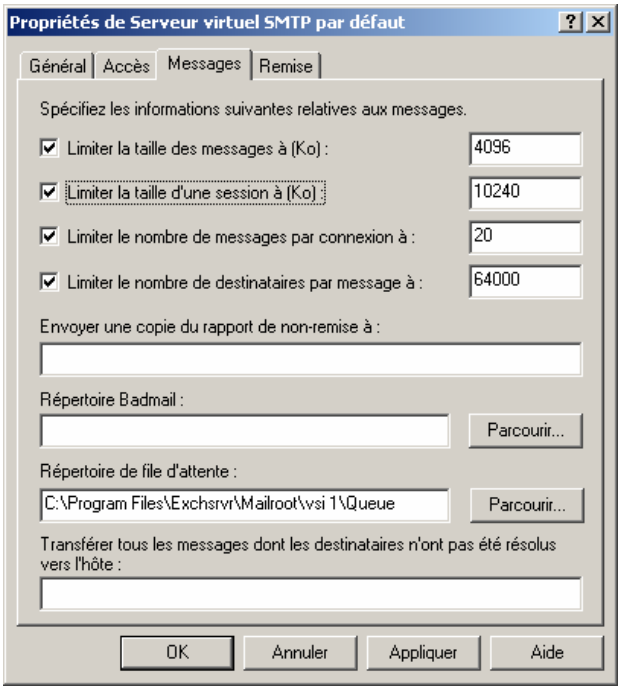


Figure 7.22 Onglet Messages de la boîte de dialogue Propriétés de Serveur virtuel SMTP par défaut

5. Dans la zone **Envoyer une copie du rapport de non-remise à**, tapez l'adresse SMTP de l'administrateur Exchange à qui vous voulez remettre des copies des rapports de non-remise. Vous pouvez utiliser les rapports de non remise pour vous aider à diagnostiquer les problèmes des utilisateurs. Pour plus d'informations sur l'analyse des rapports de non remise, consultez le chapitre 13, « Résolution des problèmes de rapports de non-remise ».

Remarque Les rapports de non-remise se produisent souvent lorsque que les utilisateurs tapent des adresses de messagerie incorrectes. Vous pouvez envisager de désactiver cette fonctionnalité tant que vous ne rencontrez pas de problème et que vous n'avez pas besoin d'analyser ces rapports.

6. Dans la zone **répertoire Badmail**, vous pouvez modifier l'emplacement des messages déroutés et non remis. Il est recommandé d'utiliser l'emplacement par défaut. L'emplacement par défaut est \Exchsrvr\Mailroot\vsi *n° d'instance de serveur virtuel*\badmail.

   Attention Le fait de déplacer le répertoire Badmail vers un disque distinct du répertoire de file d'attente peut nuire aux performances et compliquer le suivi des messages incorrects.

7. Dans la zone **Transférer tous les messages dont les destinataires n'ont pas été résolus vers l'hôte**, vous pouvez définir un hôte différent vers lequel sont transmis les messages non remis. Cette opération est utile si vous partagez un espace de noms avec un autre système de messagerie — en particulier s'il existe des destinataires de messages avec votre nom de domaine qui n'appartiennent pas à l'organisation Exchange. Par exemple, *utilisateur.exchange*@contoso.com réside dans l'organisation Exchange et *utilisateur.unix*@contoso.com réside en dehors de l'organisation Exchange. Dans cet exemple, les utilisateurs à l'adresse *utilisateur.exchange*@contoso.com peuvent envoyer des messages aux utilisateurs à l'adresse *utilisateur.unix*@contoso.com, et Exchange transmet le message à l'hôte différent spécifié.

Troisième partie Sécurisation du transport

Les attaques réseau n'ont jamais été plus courantes et cette tendance est appelée à continuer. Par conséquent, après avoir configuré le flux des messages dans votre organisation Exchange, il est essentiel de prendre des mesures destinées à sécuriser ce flux. Les messages routés depuis et vers des serveurs Microsoft® Exchange et d'autres systèmes externes peuvent également voyager sur votre réseau local et sur Internet. Pour empêcher les utilisateurs Internet malveillants d'intercepter les messages de votre organisation et d'attaquer vos serveurs, il est important de sécuriser vos connexions Internet. Les trois types de connectivité Internet sont les suivants :

- Utilisation de connecteurs sur Internet pour permettre la connectivité des messages électroniques entre votre organisation et les autres systèmes externes.
- L'utilisation de connecteurs pour connecter les groupes de routage Exchange dans votre organisation à Internet.
- L'autorisation des clients Exchange d'utiliser les protocoles de messagerie Internet ou Microsoft Office Outlook® Web Access pour accéder aux boîtes aux lettres Exchange dans votre organisation.

Généralement, chacun de ces types de connectivité nécessite un niveau de sécurité différent. Les chapitres de la troisième partie traitent des différentes méthodes permettant de sécuriser votre organisation Exchange :

Chapitre 8 « Sécurisation de votre infrastructure »
: Ce chapitre se penche sur les méthodes dont vous disposez pour protéger votre infrastructure en désactivant les services superflus dans le service IIS (Internet Information Services) et en utilisant des pare-feu et des réseaux privés virtuels.

Chapitre 9 « Sécurisation de votre serveur Exchange »
: Ce chapitre traite des méthodes recommandées en matière de sécurité générale vous permettant de protéger vos serveurs Exchange.

Chapitrer 10 « Configuration du filtrage et contrôle du courrier indésirable »
: Ce chapitre explique comment contrôler les messages commerciaux non sollicités, également connu sous le nom de courrier indésirable, à l'aide de filtrage au niveau des connexions, des expéditeurs et des destinataires Exchange.

Remarque Pour plus d'informations sur la sécurisation d'Exchange, consultez le *Guide sur le renforcement de la sécurité d'Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=3052&kbid=25210).

Sécurisation de votre infrastructure

Ce chapitre décrit des composants d'infrastructure essentiels dont l'implémentation permet d'offrir une plus grande sécurité. Les points suivants sont abordés :

- Sécurisation de l'infrastructure des services Internet (IIS) dans le but de protéger efficacement les services relatifs à Internet.
- Importance des pare-feu dans la protection des serveurs face à l'accès Internet direct.
- Utilisation de réseaux privés virtuels pour accéder de manière sécurisée à des ressources réseau privées.

Sécurisation des services Internet (IIS)

Comme indiqué dans « Services IIS (Internet Information Services) » dans le chapitre 3, les services Internet (IIS) offrent une infrastructure aux services relatifs à Internet, par exemple les protocoles HTTP, SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol) et NNTP (Network News Transfer Protocol). Par conséquent, il est essentiel de s'assurer que les services Internet (IIS) sont sécurisés. La méthode de sécurisation des services Internet (IIS) diffère selon la version de Microsoft® Windows® exécutée sur votre serveur Exchange. Windows 2000 Server fournit l'Assistant IIS Lockdown, alors que Windows Server 2003™ fournit l'outil URLScan. Utilisez l'outil approprié pour votre version de Windows afin de sécuriser les services Internet (IIS).

Utilisation de l'Assistant IIS Lockdown sur Windows 2000 Server

Sur Windows 2000, l'Assistant IIS Lockdown fourni pour IIS 5.0 désactive les services Internet (IIS) non nécessaires, ce qui permet de réduire l'exposition aux attaques dont ces services peuvent faire l'objet. En guise de défense contre les intrus, l'Assistant IIS Lockdown intègre l'outil URLScan ainsi que des modèles personnalisés pour les serveurs Exchange. L'Assistant IIS Lockdown est conçu principalement pour sécuriser les serveurs et les serveurs frontaux Microsoft Office Outlook® Web Access ; cependant, il permet également de vérifier la configuration de la sécurité sur un serveur Exchange.

Pour une sécurité optimale, exécutez l'Assistant IIS Lockdown sur chaque contrôleur de domaine et serveur Exchange de votre organisation. Vous pouvez télécharger l'Assistant IIS Lockdown à partir du Centre de téléchargement Microsoft (http://go.microsoft.com/fwlink/?LinkId=12281).

Pour plus d'informations sur l'Assistant IIS Lockdown, consultez l'article 309508 de la Base de connaissances Microsoft, « XCCC : Configurations des outils IIS Lockdown et URLscan dans un environnement Exchange » (http://support.microsoft.com/default.aspx?scid=kb;fr;309508).

Certains problèmes peuvent se poser lors de l'exécution à deux reprises de l'Assistant IIS Lockdown. Pour plus d'informations sur l'exécution à deux reprises de l'Assistant IIS Lockdown, consultez l'article 317052 de la Base de connaissances Microsoft, « COMMENT FAIRE : Annuler des modifications effectuées par l'Assistant IIS Lockdown » (http://support.microsoft.com/default.aspx?scid=kb;fr;317052).

Exécution de l'outil URLScan sur Windows Server 2003

L'Assistant IIS Lockdown n'est pas disponible pour Windows Server 2003 ; toutefois, vous pouvez exécuter l'outil URLScan afin de sécuriser les services Internet (IIS) sur Windows Server 2003. URLScan version 2.5 est un outil de sécurité qui restreint les types de demandes HTTP traitées par les services Internet (IIS). En bloquant des demandes HTTP spécifiques, l'outil de sécurité URLScan contribue à empêcher les demandes potentiellement dangereuses d'atteindre votre serveur Exchange.

Pour plus d'informations sur l'outil URLScan, consultez l'article 823175 (en anglais) de la Base de connaissances Microsoft, « Fine-Tuning and Known Issues When You Use the Urlscan Utility in an Exchange 2003 Environment » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=823175).

Utilisation de pare-feu

Un pare-feu empêche tout accès non autorisé aux données situées sur des serveurs placés derrière ce pare-feu. Que votre organisation dispose d'un réseau déjà existant ou qu'elle en bâtisse un nouveau, la planification d'un pare-feu est une phase extrêmement importante.

Grâce à des logiciels tels que Microsoft ISA (Internet Security and Acceleration) Server, vous pouvez router l'ensemble du trafic Internet via une connexion unique. Bien que cela nécessite davantage de planification et de configuration qu'une simple connexion Internet directe, il en résulte une sécurité accrue pour les serveurs de votre organisation.

Vous pouvez utiliser un pare-feu pour autoriser uniquement le trafic Internet essentiel via les ports de votre choix. Par exemple, vous pouvez configurer votre réseau pour autoriser uniquement le trafic SMTP (port 25) via votre pare-feu, ce qui empêche toute connexion sur les autres ports.

Pour permettre à Exchange de fonctionner correctement dans un environnement basé sur un pare-feu, en particulier à l'égard des clients distants, certaines exigences doivent être respectées afin de conserver une connectivité Internet. Par exemple, les pare-feu peuvent filtrer certains ports TCP ou les bloquer entièrement. Par conséquent, pour permettre aux clients distants et aux serveurs de communiquer à travers un pare-feu, vous ne pouvez pas modifier ni bloquer les affectations de port associées aux divers protocoles pris en charge par Exchange. Pour plus d'informations sur les ports nécessaires au bon fonctionnement d'Exchange, consultez « Ports couramment utilisés par Exchange » dans l'annexe A, ainsi que l'article 278339 de la Base de connaissances Microsoft, « XGEN : Ports TCP/UDP utilisés par Exchange 2000 Server » (http://support.microsoft.com/default.aspx?scid=kb;fr;278339). Bien que cet article soit destiné à Exchange 2000 Server, les informations qu'il contient s'appliquent également à Exchange 2003.

Si vous avez besoin d'un simple serveur SMTP dans le réseau de périmètre d'un pare-feu, il suffit bien souvent de disposer d'un service SMTP s'exécutant sur un ordinateur Windows 2000 ou Windows Server 2003. Exchange 2003 Enterprise Server, la fonctionnalité NAT (Network Address Translation) de Windows 2000 ou de Windows Server 2003, Microsoft ISA Server ou toute solution permettant d'isoler le réseau local d'Internet sont autant de moyens d'accroître la sécurité.

Si vous n'implémentez pas de connexion Internet protégée par pare-feu, vous devez tenir compte des risques posés en matière de sécurité. Tous les serveurs Exchange présents sur un réseau et qui disposent d'une connexion directe à Internet sont exposés.

Utilisation de réseaux privés virtuels

Le service RRAS (Routing and Remote Access Service) de Windows 2000 et Windows Server 2003 est une plate-forme ouverte, extensible, pour le routage et l'interconnexion de réseaux. Le service RRAS permet

d'accéder à distance via Internet à des organisations situées dans des environnements basés sur des réseaux locaux (LAN) ou étendus (WAN) en utilisant des connexions de réseau privé virtuel (VPN, *Virtual Private Network*). Les connexions VPN sont des liens sécurisés et authentifiés entre des réseaux privés ou publics, par exemple Internet.

Le service RAS (Remote Access Service) et les outils RRAS de Windows 2000 et Windows Server 2003 offrent des options qui permettent aux utilisateurs distants d'effectuer un accès distant via Internet. Pour fonctionner correctement, ces services d'accès doivent disposer des éléments suivants :

- une méthode de connexion à distance nommée protocole PPTP (Point-to-Point Tunneling Protocol) ;
- une connexion Internet pour créer un réseau privé virtuel.

Le protocole PPTP est conçu pour prendre en charge les réseaux VPN. Grâce aux connexions Internet par liaison DSL (Digital Subscriber Line) et modem câble, les réseaux VPN sont moins coûteux à mettre en place et à prendre en charge que les réseaux étendus (WAN) classiques. Un réseau VPN permet de s'affranchir des coûts liés aux communications téléphoniques longue distance. Par ailleurs, il offre d'autres avantages tels que la sécurisation des connexions, l'authentification mutuelle et le filtrage de paquets.

Une fois qu'un serveur PPTP a authentifié un client distant, la connexion VPN est établie. La session PPTP peut être représentée comme un tunnel à travers lequel circulent les paquets réseau. Avant d'être envoyés, ces paquets sont préalablement cryptés. Ils circulent ensuite à travers le tunnel et sont décryptés lors de leur réception. Par exemple, une organisation peut autoriser des clients distants à se connecter à un réseau d'entreprise via Internet à l'aide d'une connexion VPN. Bien qu'il ne soit pas nécessaire d'utiliser une connexion haut débit pour un réseau VPN, une connexion VPN haut débit peut s'avérer très utile aux utilisateurs d'un réseau VPN. Grâce à une connexion VPN haut débit, les utilisateurs peuvent recourir à Internet pour se connecter à un réseau d'entreprise et l'utiliser comme s'ils y étaient directement connectés.

Sécurisation de votre serveur Exchange

Ce chapitre décrit les différentes manières de sécuriser votre serveur Microsoft® Exchange. Vous pouvez contribuer à protéger vos serveurs en effectuant les tâches ci-dessous. Chacune d'entre elles est décrite en détail dans les sections suivantes :

- **Désactiver le relais ouvert sur tous les serveurs virtuels SMTP**. Les restrictions de relais par défaut empêchent les utilisateurs non autorisés d'accéder à votre serveur Exchange pour envoyer du courrier vers des emplacements externes. Si votre serveur permet le relais ouvert, des utilisateurs non autorisés peuvent s'en servir pour envoyer du courrier indésirable. Par conséquent, votre serveur risque d'être identifié par d'autres organisations comme étant une source de relais ouvert, ce qui l'empêcherait d'envoyer des messages valables.
- **Empêcher l'accès anonyme aux serveurs virtuels SMTP internes et aux serveurs virtuels SMTP dédiés pour les clients IMAP et POP**. Dans la mesure où tous les serveurs Exchange de votre organisation s'authentifient entre eux pour envoyer du courrier, vous n'avez pas besoin de permettre l'accès anonyme à vos serveurs virtuels SMTP (Simple Mail Transfer Protocol) internes. En outre, tous les clients POP (Post Office Protocol) et IMAP (Internet Message Access Protocol) s'authentifient auprès de votre serveur virtuel SMTP ; par conséquent, l'accès anonyme n'est pas nécessaire sur un serveur utilisé exclusivement par des clients POP et IMAP. En désactivant l'accès anonyme à ces serveurs, vous bloquez l'accès aux utilisateurs non autorisés.
- **Restreindre les dépôts et les relais sur les serveurs virtuels SMTP internes**. Dans Microsoft Exchange Server 2003, vous pouvez restreindre davantage l'accès aux serveurs virtuels SMTP en utilisant des principes de sécurité via la liste de contrôle d'accès discrétionnaire standard (DACL, *Discretionary Access Control List*) de Microsoft Windows® 2000 Server ou Windows Server™ 2003. Cela vous permet d'accorder des autorisations explicites aux utilisateurs et groupes habilités à utiliser un serveur virtuel SMTP.

Procédures du chapitre 9

Le tableau 9.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 9.1 Procédures du chapitre 9 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Définir des restrictions pour un utilisateur	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Définir des restrictions pour un groupe de distribution	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Restreindre les dépôts sur un serveur SMTP en fonction d'un groupe de sécurité	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Restreindre les relais en fonction d'un groupe de	Membre du groupe Administrateurs local et membre

Procédure	Autorisations ou rôles requis
sécurité	d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Désactivation du relais ouvert sur tous les serveurs virtuels SMTP

Comme indiqué dans « Restrictions de relais », dans le chapitre 2, il est primordial que vous refusiez l'accès anonyme ou le relais ouvert sur vos serveurs virtuels SMTP. Le relais permet à un utilisateur de se servir de votre serveur Exchange pour envoyer du courrier vers un domaine externe.

Dans sa configuration par défaut, Exchange autorise uniquement les utilisateurs authentifiés à relayer du courrier ; en d'autres termes, seuls les utilisateurs authentifiés peuvent se servir d'Exchange pour envoyer du courrier vers un domaine externe. Si vous modifiez les paramètres de relais par défaut pour autoriser les utilisateurs non authentifiés à relayer du courrier, ou si vous autorisez le relais ouvert vers un domaine via un connecteur, les utilisateurs non autorisés pourront se servir de votre serveur Exchange pour envoyer du courrier indésirable. Par conséquent, votre serveur risque de figurer sur une liste d'interdiction, ce qui l'empêcherait d'envoyer du courrier valable vers des serveurs distants. Pour empêcher les utilisateurs non autorisés de se servir de votre serveur Exchange pour relayer du courrier, utilisez toujours les restrictions de relais par défaut.

> **Remarque** Relais et courrier indésirable sont souvent confondus. Le contrôle du relais ne bloque pas le courrier indésirable. Pour plus d'informations sur le contrôle du courrier indésirable, consultez le chapitre 10, « Configuration du filtrage et contrôle du courrier indésirable ».

Pour plus d'informations sur le contrôle du relais, consultez l'article 304897 de la Base de connaissances Microsoft, « XIMS : Les serveurs Microsoft SMTP peuvent sembler accepter et relayer les messages électroniques dans les tests tiers » (http://support.microsoft.com/default.aspx?scid=kb;fr;304897).

Blocage de l'accès anonyme aux serveurs virtuels SMTP internes et aux serveurs virtuels SMTP dédiés pour les clients IMAP et POP

Pour accroître la sécurité, vous pouvez empêcher les utilisateurs IMAP et POP distants d'accéder de manière anonyme aux serveurs virtuels SMTP internes ainsi qu'aux serveurs virtuels SMTP dédiés à l'acceptation de courrier entrant. Lors de l'envoi de courrier interne, les serveurs Exchange s'authentifient automatiquement ; par conséquent, le blocage de l'accès anonyme à vos serveurs internes n'interrompt pas le flux des messages. En outre, une couche supplémentaire de sécurité est ajoutée à votre serveur virtuel SMTP interne.

De même, les clients IMAP et POP s'authentifient avant d'envoyer du courrier aux serveurs virtuels SMTP. Par conséquent, si vous utilisez des serveurs virtuels SMTP dédiés pour vos clients IMAP et POP, vous pouvez configurer ces serveurs pour autoriser uniquement l'accès authentifié. Pour empêcher l'accès anonyme, sous l'onglet **Accès** des propriétés du serveur virtuel SMTP, cliquez sur **Authentification**, puis désactivez la case à cocher **Accès anonyme**. Pour obtenir des instructions détaillées sur le blocage de l'accès anonyme, consultez « Configuration des contrôles d'accès et des paramètres de sécurité » dans le chapitre 7.

Important Ne désactivez pas l'accès anonyme aux serveurs virtuels SMTP têtes de pont pour Internet. En effet, les serveurs virtuels SMTP qui acceptent du courrier provenant d'Internet doivent autoriser l'accès anonyme.

Restriction des dépôts destinés aux utilisateurs et aux listes de distribution

Dans Exchange 2003, vous pouvez déterminer qui peut envoyer des messages électroniques à un utilisateur individuel ou à une liste de distribution. La restriction des dépôts destinés à une liste de distribution empêche les expéditeurs non approuvés, par exemple des utilisateurs Internet non autorisés, d'envoyer du courrier à une liste de distribution à usage interne uniquement. Par exemple, une liste de distribution **Tous les employés** ne doit être accessible à aucune personne externe à l'entreprise (par usurpation ou tout autre moyen).

Remarque Les listes de distribution restreintes et les restrictions de dépôt pour les utilisateurs fonctionnent uniquement sur les serveurs têtes de pont ou sur les serveurs de passerelle SMTP exécutant Exchange Server 2003.

Songez à définir des restrictions pour les listes de distribution internes appartenant aux employés à plein temps, ainsi que pour les autres groupes internes. En procédant ainsi, vous protégez ces listes de distribution contre la réception de courrier indésirable et vous empêchez les utilisateurs anonymes d'effectuer des envois vers ces listes de distribution.

Utilisez les procédures ci-dessous pour définir des restrictions de dépôt pour les utilisateurs et les listes de distribution, respectivement.

Pour définir des restrictions pour un utilisateur

1. Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Utilisateurs et ordinateurs Active Directory**.
2. Développez le conteneur de votre unité d'organisation, puis cliquez sur **Utilisateurs** ou sur le conteneur dans lequel réside l'utilisateur.
3. Dans le volet d'informations, cliquez avec le bouton droit sur l'utilisateur pour lequel vous souhaitez restreindre les dépôts, puis cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Exchange - Général**, puis sur **Restrictions de remise**.
5. Sous **Restrictions au niveau du message**, sous **Accepter les messages**, sélectionnez l'une des options suivantes :
   - Cliquez sur **Provenant des utilisateurs authentifiés uniquement** pour autoriser uniquement les utilisateurs authentifiés à envoyer des messages à l'utilisateur sélectionné. Le choix de l'option **Provenant des utilisateurs authentifiés uniquement** affecte la manière dont les autres options sont mises en œuvre.
   - Cliquez sur **Provenant de tout utilisateur** pour permettre à tout utilisateur authentifié d'envoyer des messages à l'utilisateur sélectionné.
   - Cliquez sur **Uniquement de** pour spécifier un ensemble d'utilisateurs ou de groupes authentifiés qui pourront envoyer des messages à l'utilisateur sélectionné. Cliquez sur **Ajouter** pour spécifier les utilisateurs ou groupes autorisés à envoyer des messages à l'utilisateur sélectionné.
   - Cliquez sur **Provenant de tout utilisateur sauf** pour autoriser tous les utilisateurs authentifiés, à l'exception d'un ensemble bien précis, à envoyer des messages à l'utilisateur sélectionné. Cliquez sur **Ajouter** pour spécifier la liste des utilisateurs ou des groupes qui ne sont pas autorisés à envoyer des messages à l'utilisateur sélectionné.

6. Laissez désactivée l'option **Provenant des utilisateurs authentifiés uniquement**. Si cette case à cocher reste désactivée, les options suivantes sont mises en œuvre comme suit :

   - Cliquez sur **Provenant de tout utilisateur** pour permettre à tous les utilisateurs d'envoyer des messages à l'utilisateur sélectionné. Cela inclut les utilisateurs anonymes sur Internet.
   - Cliquez sur **Uniquement de** pour spécifier un ensemble précis d'utilisateurs ou de groupes qui pourront envoyer des messages à l'utilisateur sélectionné. Cliquez sur **Ajouter** pour spécifier les utilisateurs ou groupes autorisés à envoyer des messages à l'utilisateur sélectionné.
   - Cliquez sur **Provenant de tout utilisateur sauf** pour autoriser tous les utilisateurs, à l'exception d'un ensemble d'utilisateurs ou de groupes bien précis, à envoyer des messages à l'utilisateur sélectionné. Cliquez sur **Ajouter** pour spécifier la liste des utilisateurs ou des groupes qui ne sont pas autorisés à envoyer des messages à l'utilisateur sélectionné. Ces utilisateurs ou groupes peuvent être authentifiés ou anonymes.

Pour définir des restrictions pour une liste de distribution

1. Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Utilisateurs et ordinateurs Active Directory**.
2. Développez le conteneur de votre unité d'organisation, puis cliquez sur **Utilisateurs** ou sur le conteneur dans lequel réside la liste de distribution.
3. Dans le volet d'informations, cliquez avec le bouton droit sur la liste de distribution pour laquelle vous souhaitez restreindre les dépôts, puis cliquez sur **Propriétés**.
4. Dans **<*Liste de distribution*> - Propriétés**, cliquez sur l'onglet **Exchange - Général**.
5. Sous **Restrictions au niveau du message**, sous **Accepter les messages**, sélectionnez l'une des options suivantes :

   - Activez la case à cocher **Provenant des utilisateurs authentifiés uniquement** pour autoriser uniquement les utilisateurs authentifiés à envoyer des messages à la liste de distribution sélectionnée. Si vous activez cette case à cocher, les options suivantes sont mises en œuvre comme suit :
   - Cliquez sur **Provenant de tout utilisateur** pour permettre à tous les utilisateurs authentifiés d'envoyer des messages à la liste de distribution sélectionnée.
   - Cliquez sur **Uniquement de** pour spécifier un ensemble précis d'utilisateurs ou de groupes authentifiés qui pourront envoyer des messages à la liste de distribution sélectionnée. Cliquez sur **Ajouter** pour spécifier les utilisateurs ou groupes autorisés à envoyer des messages à la liste de distribution sélectionnée.
   - Cliquez sur **Provenant de tout utilisateur sauf** pour autoriser tous les utilisateurs authentifiés, à l'exception d'un ensemble bien précis, à envoyer des messages à la liste de distribution sélectionnée. Cliquez sur **Ajouter** pour spécifier la liste des utilisateurs ou des groupes qui ne sont pas autorisés à envoyer des messages à la liste de distribution sélectionnée.

6. Laissez désactivée l'option **Provenant des utilisateurs authentifiés uniquement**. Si cette case à cocher reste désactivée, les options suivantes sont mises en œuvre comme suit :

   - Cliquez sur **Provenant de tout utilisateur** pour permettre à tous les utilisateurs d'envoyer des messages à la liste de distribution sélectionnée. Cela inclut les utilisateurs anonymes sur Internet.
   - Cliquez sur **Uniquement de** pour spécifier un ensemble précis d'utilisateurs ou de groupes qui pourront envoyer des messages à la liste de distribution sélectionnée. Cliquez sur **Ajouter** pour spécifier les utilisateurs ou groupes autorisés à envoyer des messages à la liste de distribution sélectionnée.
   - Cliquez sur **Provenant de tout utilisateur sauf** pour autoriser tous les utilisateurs, à l'exception d'un ensemble d'utilisateurs ou de groupes bien précis, à envoyer des messages à la liste de distribution

sélectionnée. Cliquez sur **Ajouter** pour spécifier la liste des utilisateurs ou des groupes qui ne sont pas autorisés à envoyer des messages à la liste de distribution sélectionnée. Ces utilisateurs ou groupes peuvent être authentifiés ou anonymes.

Restriction des autorisations de dépôt et de relais pour un serveur virtuel SMTP interne

Exchange Server 2003 permet de restreindre à un nombre limité d'utilisateurs ou de groupes, les autorisations de dépôt et de relais pour un serveur virtuel SMTP, grâce à la liste de contrôle d'accès discrétionnaire standard (DACL, *Discretionary Access Control List*) de Windows 2000 Server ou Windows Server 2003. Vous pouvez ainsi spécifier les groupes d'utilisateurs qui peuvent déposer ou relayer du courrier via un serveur virtuel.

Restriction des dépôts sur un serveur virtuel SMTP

La restriction des dépôts sur un serveur virtuel SMTP est d'une grande utilité si vous souhaitez autoriser des utilisateurs bien précis à envoyer des messages Internet vers des serveurs virtuels spécifiques. Vous pouvez uniquement accorder à ces utilisateurs ou groupes l'accès nécessaire pour déposer du courrier sur les serveurs virtuels SMTP.

Remarque Évitez de restreindre les dépôts sur les serveurs virtuels SMTP qui acceptent des messages Internet.

Pour restreindre les dépôts sur un serveur SMTP en fonction d'un groupe de sécurité

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, le serveur qui vous intéresse, puis **Protocoles** et **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP dont vous souhaitez restreindre les dépôts, puis cliquez sur **Propriétés**.
4. Dans l'onglet **Général** de **Propriétés de <*Serveur virtuel SMTP*>**, cliquez sur l'onglet **Accès**, puis sur **Authentification**.
5. Dans **Authentification**, désactivez la case à cocher **Accès anonyme**, puis cliquez sur **Utilisateurs** pour indiquer un sous-ensemble d'utilisateurs auquel vous souhaitez accorder des autorisations de dépôt sur ce serveur virtuel SMTP.
6. Dans **Autorisations pour Dépôt et relais**, sélectionnez le groupe ou l'utilisateur à retirer, puis cliquez sur **Supprimer**.
7. Pour ajouter un groupe ou un utilisateur, cliquez sur **Ajouter**, puis sélectionnez le groupe ou l'utilisateur auquel vous souhaitez accorder des autorisations. Sélectionnez l'une des options suivantes :
   - Sur Windows Server 2003, dans **Sélectionnez les utilisateurs, les ordinateurs ou les groupes**, sous **Entrez le nom de l'objet à sélectionner**, tapez le nom de l'utilisateur ou du groupe. Pour rechercher l'utilisateur ou le groupe, cliquez sur **Avancé**, recherchez l'utilisateur ou le groupe, puis cliquez sur **Vérifier les noms** pour valider votre entrée.

     Conseil Cliquez sur le lien **exemples** afin d'afficher les formats pris en charge.

- Sur Windows 2000 Server, dans **Sélectionnez les utilisateurs, les ordinateurs ou les groupes**, sélectionnez le groupe ou l'utilisateur auquel vous souhaitez accorder des autorisations de dépôt, puis cliquez sur **Ajouter**.

8. Cliquez sur **OK** pour revenir à la boîte de dialogue **Autorisations pour Dépôt et relais**.
9. Sous **Noms d'utilisateurs ou de groupes**, sélectionnez le groupe que vous venez d'ajouter.
10. Sous **Autorisations pour <*groupe sélectionné*>**, en regard d'**Autorisation de dépôt**, cliquez si nécessaire sur **Autoriser** pour autoriser l'utilisateur ou le groupe sélectionné à déposer du courrier via ce serveur virtuel SMTP.
11. Cliquez sur **OK**.

Restreindre les relais sur un serveur virtuel SMTP

La restriction des relais sur les serveurs virtuels est d'une grande utilité si vous souhaitez autoriser un groupe d'utilisateurs à relayer des messages vers Internet, tout en refusant des privilèges de relais à un autre groupe.

Pour restreindre les relais en fonction d'un groupe de sécurité

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, le serveur qui vous intéresse, puis **Protocoles** et **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP auquel vous voulez appliquer les restrictions de relais, puis cliquez sur **Propriétés**.
4. Dans l'onglet **Général** de **Propriétés de <*Serveur virtuel SMTP*>**, cliquez sur l'onglet **Accès**, puis sur **Relais**.
5. Dans **Restrictions de relais**, désactivez la case à cocher **Autoriser tous les ordinateurs authentifiés à relayer, sans tenir compte de la liste ci-dessus**, puis cliquez sur **Utilisateurs** pour définir un sous-ensemble d'utilisateurs auquel vous souhaitez attribuer des autorisations de relais sur ce serveur virtuel SMTP.
6. Dans **Autorisations pour Dépôt et relais**, sélectionnez le groupe ou l'utilisateur à retirer, puis cliquez sur **Supprimer**.
7. Pour ajouter un groupe ou un utilisateur, cliquez sur **Ajouter**, puis sélectionnez le groupe ou l'utilisateur auquel vous souhaitez accorder des autorisations. Sélectionnez l'une des options suivantes :

   - Sur Windows Server 2003, dans **Sélectionnez les utilisateurs, les ordinateurs ou les groupes**, sous **Entrez le nom de l'objet à sélectionner**, tapez le nom de l'utilisateur ou du groupe. Pour rechercher l'utilisateur ou le groupe, cliquez sur **Avancé**, recherchez l'utilisateur ou le groupe, puis cliquez sur **Vérifier les noms** pour valider votre entrée.

     Conseil Cliquez sur le lien **exemples** afin d'afficher les formats pris en charge.

   - Sur Windows 2000 Server, dans **Sélectionnez les utilisateurs, les ordinateurs ou les groupes**, sélectionnez le groupe ou l'utilisateur auquel vous souhaitez accorder des autorisations de dépôt, puis cliquez sur **Ajouter**.

8. Cliquez sur **OK** pour revenir à la boîte de dialogue **Autorisations pour Dépôt et relais**.
9. Sous **Noms d'utilisateurs ou de groupes**, sélectionnez le groupe que vous venez d'ajouter.

10. Sous **Autorisations pour <*groupe sélectionné*>**, en regard d'**Autorisation de dépôt**, activez si nécessaire la case à cocher située sous **Autoriser** afin d'autoriser l'utilisateur ou le groupe sélectionné à déposer du courrier via ce serveur virtuel SMTP.
11. En regard d'**Autorisation de relais**, activez la case à cocher située sous **Autoriser** ou sous **Refuser**, selon que vous souhaitez autoriser ou empêcher le relais de l'objet sélectionné via ce serveur virtuel.

    Remarque Pour pouvoir activer les autorisations de relais, vous devez avoir activé au préalable les autorisations de dépôt.

12. Cliquez sur **OK**.

Configuration du filtrage et contrôle du courrier indésirable

Le contrôle du courrier indésirable est un véritable défi, mais les conseils ci-dessous vous permettront d'atténuer ce fléau :

- **Utilisez les fonctionnalités de filtrage d'Exchange 2003**. Microsoft® Exchange Server 2003 permet de filtrer les connexions, les destinataires et les expéditeurs afin de réduire le volume de courrier indésirable reçu par les utilisateurs de votre organisation.
- **Incitez les utilisateurs à ne pas répondre au courrier indésirable ni à le transférer**. Recommandez aux utilisateurs de ne pas cliquer sur les liens de type « supprimer » contenus dans le courrier indésirable, car ces liens servent souvent à vérifier les adresses.

Dans Exchange Server 2003, vous pouvez configurer et activer le filtrage sur vos serveurs virtuels SMTP afin de restreindre l'accès à ces derniers. La configuration du filtrage s'effectue dans le Gestionnaire système Exchange sous les paramètres globaux des propriétés de remise des messages. Bien que vous puissiez configurer le filtrage au niveau global, vous devez l'activer sur chacun des serveurs virtuels individuels.

Grâce au filtrage, vous pouvez bloquer de plusieurs façons les messages électroniques entrants envoyés vers votre serveur virtuel SMTP :

- Le **filtrage des connexions** permet de bloquer les messages envoyés à votre organisation en fonction de l'adresse IP (Internet Protocol) du serveur SMTP de connexion. Vous pouvez configurer des listes d'autorisations globales pour les adresses IP dont vous souhaitez toujours accepter les messages, ainsi que des listes de refus globales pour les adresses IP dont vous souhaitez systématiquement rejeter les messages. Vous pouvez également vous abonner auprès d'un fournisseur tiers de liste d'interdiction afin de vérifier si l'adresse IP de connexion ne figure pas sur la liste des adresses IP bloquées.

  Remarque Si vous souhaitez empêcher une adresse IP particulière d'envoyer du courrier vers vos serveurs virtuels SMTP, vous pouvez ajouter cette adresse IP en cliquant sur le bouton **Connexion** situé sous l'onglet **Accès** des propriétés de votre serveur virtuel SMTP. Vous devez configurer ces restrictions sur vos serveurs virtuels SMTP de passerelle.

- Le **filtrage de destinataire** vous permet de bloquer les messages envoyés à un destinataire spécifique de votre organisation.
- Le **filtrage des expéditeurs** vous permet de bloquer les messages envoyés par un expéditeur spécifique. Si votre organisation reçoit fréquemment du courrier indésirable provenant des mêmes expéditeurs, vous pouvez empêcher ces derniers de continuer à envoyer du courrier à votre organisation.

Procédures du chapitre 10

Le tableau 10.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 10.1 Procédures du chapitre 10 et autorisations correspondantes

Procédure	Autorisations ou rôles requis

Procédure	Autorisations ou rôles requis
Créer une liste d'autorisations globale	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Créer une liste de refus globale	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Créer un filtre de connexion	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Spécifier une exception relative à une règle de connexion	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Appliquer un filtre de connexion à un serveur virtuel SMTP	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Créer un filtre destinataire	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.
Appliquer un filtre destinataire à un serveur virtuel SMTP	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
S'assurer que le serveur Exchange 2003 est configuré pour ne pas résoudre la messagerie anonyme	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Configurer Exchange 2000 pour ne pas résoudre les adresses de messagerie ayant une origine externe	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Filtrage des connexions

Exchange 2003 prend en charge le filtrage des connexions en fonction de listes d'interdiction. Le filtrage des connexions tire parti des services externes qui répertorient les sources connues de courrier indésirable, des listes de comptes d'utilisateur d'accès à distance et des serveurs ouverts pour un relais (en fonction des adresses IP). Le filtrage des connexions complète les produits tiers de filtrage de contenu. Cette fonctionnalité vous permet de comparer une adresse IP entrante à la liste d'un fournisseur de liste d'interdiction pour déterminer si elle appartient à l'une des catégories que vous souhaitez filtrer. Par ailleurs, vous pouvez utiliser plusieurs filtres de connexion et déterminer un ordre de priorité pour chaque filtre à appliquer.

Grâce au filtrage des connexions, vous pouvez également effectuer les tâches suivantes :

- **Configurer des listes d'autorisations et de refus globales.** Une liste d'autorisations globale regroupe les adresses IP dont vous acceptez systématiquement le courrier. Une liste de refus globale regroupe les adresses IP dont vous refusez systématiquement le courrier. Vous pouvez utiliser des listes d'autorisations et de refus globales avec ou sans l'aide d'un fournisseur de service de liste d'interdiction.
- **Configurer une adresse de destinataire échappant à toutes les règles de filtrage des connexions**. Tout courrier envoyé à l'adresse en question est automatiquement accepté même si l'expéditeur figure sur une liste d'interdiction.

Définition des règles de filtrage des connexions

Lorsque vous créez une règle de filtrage des connexions, le protocole SMTP l'utilise pour effectuer une recherche DNS dans une liste fournie par un service de liste d'interdiction tiers. Le filtre de connexion compare chaque adresse IP entrante au contenu de la liste d'interdiction tierce. Le fournisseur de liste d'interdiction émet l'une des deux réponses suivantes :

- **hôte introuvable** Indique que l'adresse IP ne figure pas dans sa liste d'interdiction.
- **127.0.0.*x*** Code d'état de réponse indiquant qu'une adresse IP correspondante a été trouvée dans la liste des contrevenants. La valeur *x* peut varier en fonction du fournisseur de liste d'interdiction.

Si l'adresse IP entrante existe dans la liste d'interdiction, le protocole SMTP renvoie une erreur de type 5.*x*.*x* en réponse à la commande RCPT TO (cette dernière est la commande SMTP que le serveur de connexion émet pour identifier le destinataire attendu).

Il est possible de personnaliser la réponse renvoyée à l'expéditeur. En outre, dans la mesure où les fournisseurs de listes d'interdiction disposent généralement de catégories de contrevenants différentes, vous pouvez indiquer les correspondances à refuser. Voici les trois types de contrevenants traités par la plupart des fournisseurs de listes d'interdiction :

- **Sources de courrier indésirable** Ces listes sont établies à partir des adresses sources correspondant aux messages publicitaires non sollicités reçus.
- **Serveurs de relais ouvert connus** Ces listes sont établies à partir de l'identification des serveurs SMTP de relais ouvert présents sur Internet. L'existence d'un serveur de relais ouvert résulte généralement d'une erreur de configuration de la part de l'administrateur système.
- **Utilisateurs d'accès à distance** Ces listes sont créées à partir de listes déjà établies par les fournisseurs de services Internet et qui comportent des adresses IP d'accès à distance, ou à partir d'adresses liées à une probable connexion à distance.

Identification des adresses IP interdites

Quand un message électronique est envoyé à votre organisation alors que vous avez défini un filtre de connexion, Exchange contacte le fournisseur de liste d'interdiction. Le fournisseur vérifie l'existence d'un enregistrement A (hôte) auprès de son serveur DNS. Exchange soumet la requête d'information dans un format spécifique. Par exemple, si l'adresse de connexion est 192.168.5.1 alors que l'organisation du fournisseur de liste d'interdiction est contoso.org, Exchange soumet la requête dans le format suivant :

```
<reverse IP address of the connecting server>.<dns name for the block list organization> IN A 127. 0.0.x
```

soit, dans ce cas :

```
1.5.168.192..contoso.org
```

Si cette adresse IP figure dans la liste d'interdiction du fournisseur, celui-ci renvoie un code d'état 127.0.0.*x* indiquant l'adresse IP incriminée et le type d'infraction. Tous les fournisseurs de listes d'interdiction retournent un code de réponse au format 127.0.0.*x*, où *x* désigne le type d'infraction. La valeur *x* varie en fonction du fournisseur de liste d'interdiction.

Description des codes de réponse émanant des fournisseurs de listes d'interdiction

Nous avons vu précédemment que le fournisseur de liste d'interdiction renvoie systématiquement le code d'état 127.0.0.*x* s'il trouve une correspondance. Le code d'état est soit un code de retour explicite, soit un masque de bits (code de retour multifonction). Si votre fournisseur de liste d'interdiction retourne une valeur, vous pouvez la filtrer. Cependant, si votre fournisseur de liste d'interdiction retourne un masque de bits, vous devez être familiarisé avec ce type de valeur de retour pour indiquer correctement les adresses à filtrer.

Un masque de bits est une méthode qui permet de s'assurer qu'un bit précis est défini pour une entrée. Un masque de bits se distingue d'un masque classique dans la mesure où il recherche une valeur de bit spécifique, contrairement à un masque de sous-réseau, qui recherche une plage de valeurs. Prenons l'exemple suivant.

Pour chaque correspondance trouvée dans sa liste d'interdiction, un fournisseur renvoie l'un des codes d'état répertoriés dans le tableau 10.2.

Tableau 10.2 Exemples de codes d'état d'une liste d'interdiction

Catégorie	Code d'état retourné
Source de courrier indésirable connue	127.0.0.3
Compte d'utilisateur d'accès à distance	127.0.0.2
Serveur de relais connu	127.0.0.4

Toutefois, si une adresse IP figure dans deux listes, le fournisseur de liste d'interdiction ajoute les valeurs du dernier octet. Par conséquent, si une adresse IP figure sur la liste des serveurs de relais connus ainsi que sur la liste des sources de courrier indésirable connues, le fournisseur de liste d'interdiction renvoie le code d'état 127.0.0.7, où 7 correspond à la somme des valeurs des derniers octets de retour pour les codes d'état des sources de courrier indésirable connues et des serveurs de relais connus.

Pour définir un filtre ne s'appliquant qu'aux sources connues de courrier publicitaire non sollicité, entrez 0.0.0.3 comme valeur de masque de bits ; la liste d'interdiction filtre alors les valeurs possibles, dans le cas présent, 127.0.0.3, 127.0.0.5, 127.0.0.7 et 127.0.0.9.

Le tableau 10.3 répertorie les valeurs de masque de bits associées à chaque exemple de code d'état.

Tableau 10.3 Exemples de codes d'état d'une liste d'interdiction et valeurs de masque de bits correspondantes

Catégorie	Code d'état retourné	Valeur de masque de bits
Source de courrier indésirable connue	127.0.0.3	0.0.0.3
Compte d'utilisateur d'accès à distance	127.0.0.2	0.0.0.2
Serveur de relais connu	127.0.0.4	0.0.0.4
Serveur de relais connu et compte d'utilisateur d'accès à distance	127.0.0.6	0.0.0.6

Dans la dernière catégorie du tableau 10.3 (« Serveur de relais connu et compte d'utilisateur d'accès à distance »), le masque de bits 0.0.0.6 ne retourne une adresse IP correspondante que si celle-ci figure à la fois dans la liste serveur de relais et dans la liste compte d'utilisateur d'accès à distance. Il ne retourne pas de correspondance si l'adresse IP figure uniquement dans l'une des deux listes. Un masque de bits ne permet pas de rechercher une seule correspondance dans plusieurs listes.

> **Remarque** Un masque de bits effectue une vérification par rapport à une seule valeur. Si vous définissez une valeur de masque de bits qui est retournée lorsqu'une adresse IP apparaît dans deux listes, le masque ne mettra en correspondance que les adresses IP figurant à la fois dans l'une et l'autre liste. Si vous voulez rechercher une adresse IP dans l'une ou l'autre liste, entrez les codes d'état de ces paramètres.

Spécification d'exceptions aux règles de filtrage des connexions

Il est possible d'autoriser la remise de messages à des destinataires particuliers, même si leur adresse figure dans une liste d'interdiction. Cette exception s'avère utile si vous souhaitez que des organisations fiables puissent contacter le compte administrateur pour communiquer avec vos administrateurs. Par exemple, imaginez qu'une société fiable possède un serveur configuré par inadvertance pour autoriser le relais ouvert ; dans ce cas, les messages électroniques envoyés par cette société à vos utilisateurs sont bloqués. Pourtant, si vous configurez un filtrage des connexions autorisant la remise de messages au compte administrateur de votre organisation, l'administrateur de la société interdite peut envoyer un message électronique à votre compte administrateur pour signaler le blocage ou en demander les raisons.

Activation du filtrage des connexions

Activez le filtrage des connexions en procédant comme suit :

1. Créez le filtre de connexion dans la boîte de dialogue **Propriétés de Remise des messages**, sous l'onglet **Filtrage des connexions**.
2. Appliquez le filtre au niveau du serveur virtuel SMTP.

Chaque étape est décrite en détail dans les sections ci-après.

Étape 1 : configuration du filtrage des connexions

Configurez le filtrage des connexions en procédant comme suit :

- Créez des listes d'autorisations et de refus globales.
- Créez des règles de filtrage des connexions.
- Créez des exceptions aux règles de filtrage des connexions.

Création de listes d'autorisations et de refus globales

Le filtrage des connexions permet de créer des listes d'autorisations et de refus globales. À l'aide de ces listes, vous pourrez ensuite accepter ou refuser systématiquement du courrier émanant d'adresses IP particulières, que vous fassiez appel ou non à un fournisseur de service de liste d'interdiction. Toute adresse IP figurant dans la liste d'autorisations globale est acceptée automatiquement, sans qu'il soit tenu compte des règles de filtrage. De même, toute adresse IP figurant dans la liste de refus globale est systématiquement refusée.

Les entrées de la liste d'autorisations globale ont la priorité sur celles de la liste de refus globale. Exchange examine la liste d'autorisations globale avant la liste de refus globale ; par conséquent, pour refuser les

connexions d'un sous-réseau et d'un masque spécifiques tout en acceptant les connexions d'une adresse IP unique présente dans cette plage, vous devez :

- entrer dans la liste d'autorisations globale l'adresse IP dont vous souhaitez accepter les connexions ;
- entrer dans la liste de refus globale le sous-réseau et le masque de la plage d'adresses IP dont vous souhaitez refuser les connexions.

Lorsque l'adresse IP que vous avez ajoutée à la liste d'autorisations globale tente de se connecter à votre serveur Exchange, celui-ci examine au préalable la liste d'autorisations globale. Dans la mesure où Exchange trouve une adresse IP correspondante, il arrête la vérification liée au filtrage des connexions et accepte la connexion.

Pour créer une liste d'autorisations globale

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, double-cliquez sur **Paramètres globaux**, cliquez avec le bouton droit sur **Remise des messages**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Filtrage des connexions**.
4. Cliquez sur **Accepter**. La boîte de dialogue **Liste des autorisations** s'affiche (figure 10.1).

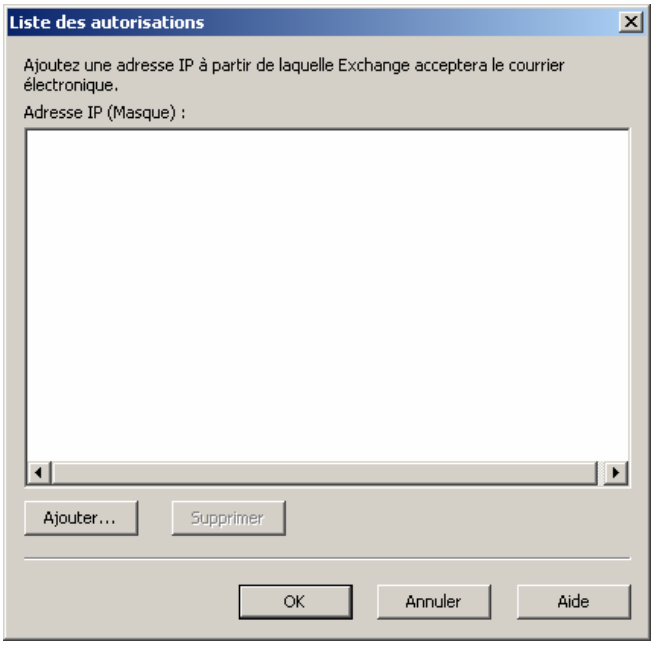


Figure 10.1 Boîte de dialogue Liste des autorisations

5. Cliquez sur **Ajouter**.
6. Dans **Adresse IP (Masque)**, sélectionnez l'une des options suivantes :
   - Cliquez sur **Adresse IP unique** pour ajouter une seule adresse IP à la liste d'autorisations globale pour cette règle de filtrage de connexion.
   - Cliquez sur **Groupe d'adresses IP** pour ajouter une adresse et un masque de sous-réseau à la liste d'autorisations globale.
7. Cliquez sur **OK**.

Pour créer une liste de refus globale

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, double-cliquez sur **Paramètres globaux**, cliquez avec le bouton droit sur **Remise des messages**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Filtrage des connexions**.
4. Cliquez sur **Refuser**. La boîte de dialogue **Liste des refus** s'affiche (figure 10.2).

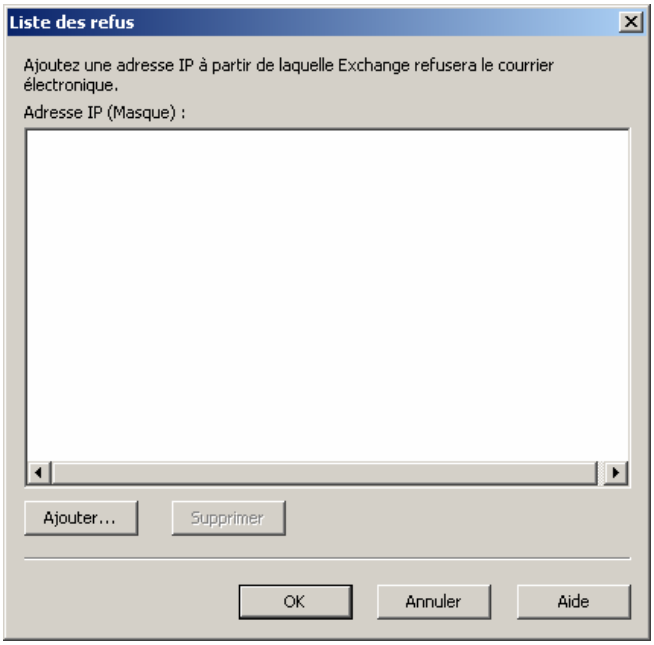


Figure 10.2 Boîte de dialogue Liste des refus

5. Cliquez sur **Ajouter**.
6. Dans **Adresse IP (Masque)**, sélectionnez l'une des options suivantes :
   - Cliquez sur **Adresse IP unique** pour ajouter une seule adresse IP à la liste de refus globale pour cette règle de filtrage de connexion.
   - Cliquez sur **Groupe d'adresses IP** pour ajouter une adresse et un masque de sous-réseau à la liste de refus globale.
7. Cliquez sur **OK**.

Création d'une règle de filtrage des connexions

Utilisez la procédure suivante pour créer une règle de filtrage de connexion ainsi que pour configurer les exceptions correspondantes.

Pour créer un filtre de connexion

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, double-cliquez sur **Paramètres globaux**, cliquez avec le bouton droit sur **Remise des messages**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Filtrage des connexions** (figure 10.3).

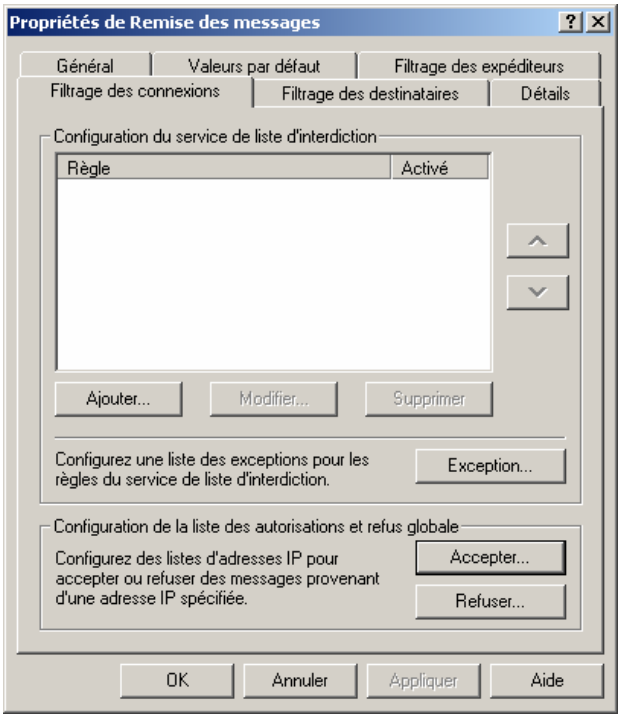


Figure 10.3 Onglet Filtrage des connexions de la boîte de dialogue Propriétés de Remise des messages

4. Pour créer une règle de filtrage de connexion, cliquez sur **Ajouter**. La boîte de dialogue **Règle de filtrage des connexions** s'affiche (figure 10.4).

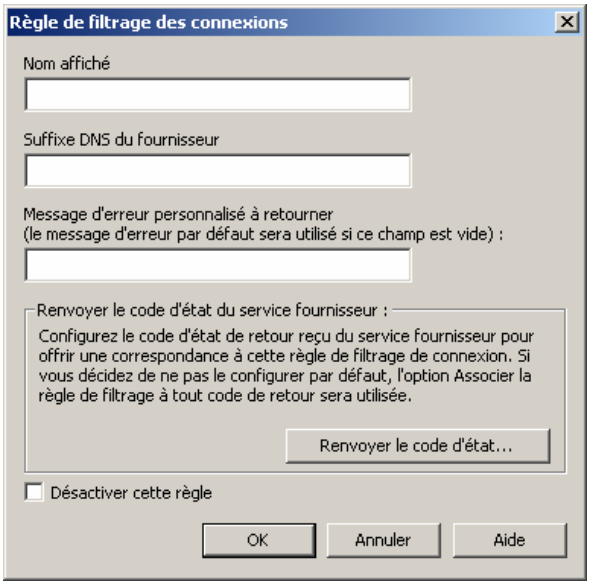


Figure 10.4 Boîte de dialogue Règle de filtrage des connexions

5. Dans la zone **Nom affiché**, tapez le nom souhaité pour le filtre de connexion.
6. Dans la zone **Suffixe DNS du fournisseur**, tapez le suffixe DNS que le fournisseur ajoute à l'adresse IP.
7. Dans la zone **Message d'erreur personnalisé à retourner (le message d'erreur par défaut sera utilisé si ce champ est vide)**, vous pouvez, si vous le souhaitez, taper le message d'erreur personnalisé à retourner à l'expéditeur. Laissez cette zone vide pour que le message d'erreur par défaut soit utilisé :

<*Adresse IP*> a été bloqué par <*Nom de la règle de filtrage de connexion*>

Vous pouvez utiliser les variables suivantes pour générer un message personnalisé :

- %0 – adresse IP de connexion
- %1 – nom de la règle de filtrage de connexion
- %2 - nom du fournisseur de liste d'interdiction

Par exemple, si vous souhaitez que le message personnalisé indique :

L'adresse IP <*adresse IP*> a été refusée par le fournisseur de liste d'interdiction <*nom du fournisseur de liste d'interdiction*>.

Rédigez le message d'erreur sous la forme :

L'adresse IP %0 a été refusée par le fournisseur de liste d'interdiction %2.

Exchange remplace **%0** par l'adresse IP de connexion et **%2** par le fournisseur de liste d'interdiction.

> **Remarque** Si vous souhaitez inclure un signe de pourcentage (%) dans votre message d'erreur, vous devez taper %%.

8. Pour configurer les codes d'état de retour reçus de la part du fournisseur de liste d'interdiction et qui doivent correspondre au filtre de connexion, cliquez sur **Renvoyer le code d'état**. La boîte de dialogue **Renvoyer le code d'état** s'affiche (figure 10.5).

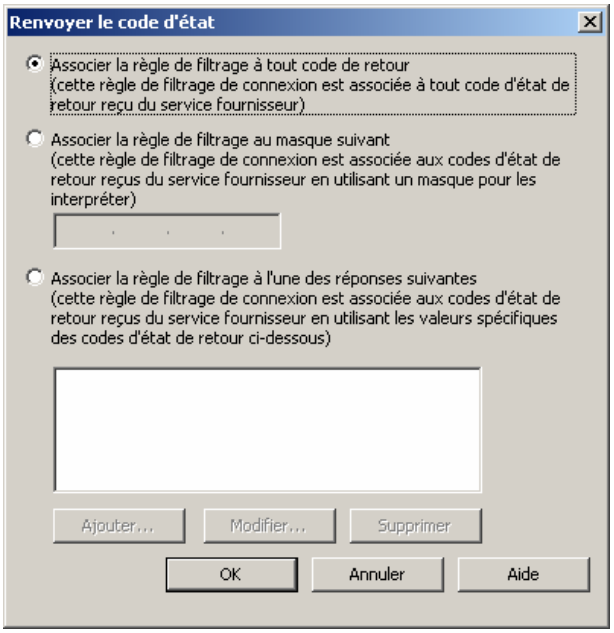


Figure 10.5 Boîte de dialogue Renvoyer le code d'état

9. Sélectionnez l'une des options suivantes :

   - Cliquez sur **Associer la règle de filtrage à tout code de retour (cette règle de filtrage de connexion est associée à tout code d'état de retour reçu du service fournisseur)** pour définir la valeur par défaut à associer à tous les codes de retour.
   - Cliquez sur **Associer la règle de filtrage au masque suivant (cette règle de filtrage de connexion est associée aux codes d'état de retour reçus du service fournisseur en utilisant un masque pour les interpréter)**, puis tapez le masque à filtrer par rapport aux masques employés par vos fournisseurs.

Remarque Un masque de bits effectue une vérification par rapport à une seule valeur. Si vous définissez une valeur de masque de bits qui est retournée lorsqu'une adresse IP apparaît dans deux listes, le masque ne mettra en correspondance que les adresses IP figurant à la fois dans l'une et l'autre liste. Si vous voulez rechercher une adresse IP dans l'une ou l'autre liste, entrez les codes d'état de ces paramètres.

- Cliquez sur **Associer la règle de filtrage à l'une des réponses suivantes (cette règle de filtrage de connexion est associée aux codes d'état de retour reçus du service fournisseur en utilisant les valeurs spécifiques des codes d'état de retour ci-dessous)**. Cliquez sur **Ajouter**, puis, dans **Renvoyer le code d'état**, tapez le code d'état à associer. Pour chaque code d'état supplémentaire, cliquez sur **Ajouter**, tapez le code, puis cliquez sur **OK**.

10. Cliquez sur **OK**.

Vous avez la possibilité de créer des exceptions à la règle de filtrage de connexion. En l'occurrence, il est possible d'autoriser la remise de messages à des destinataires particuliers (par exemple l'administrateur), même si leur adresse IP de connexion figure dans une liste d'interdiction.

Pour spécifier une exception à une règle de connexion

1. Dans la boîte de dialogue **Propriétés de Remise des messages**, sous l'onglet **Filtrage des connexions**, cliquez sur **Exception**. La boîte de dialogue **Paramètres de configuration du service de liste d'interdiction** s'affiche (figure 10.6).

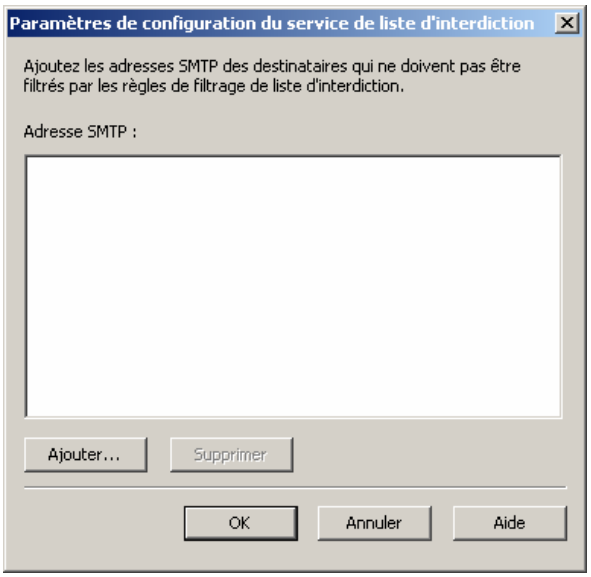


Figure 10.6 Boîte de dialogue Paramètres de configuration du service de liste d'interdiction

2. Cliquez sur **Ajouter**.
3. Dans la zone **Ajouter un destinataire**, tapez l'adresse SMTP du destinataire dont vous souhaitez accepter tous les messages, même si l'adresse IP de connexion figure dans une liste d'interdiction.
4. Cliquez sur **OK** à deux reprises.

Étape 2 : application du filtre de connexion aux serveurs virtuels SMTP appropriés

Après avoir créé le filtre de connexion et les exceptions correspondantes, vous devez appliquer ce filtre aux serveurs virtuels SMTP adéquats. En règle générale, vous devez effectuer cette opération sur les serveurs

virtuels SMTP présents sur les serveurs de passerelle qui acceptent les messages électroniques en provenance d'Internet. La procédure ci-dessous vous permet d'appliquer un filtre de connexion à un serveur virtuel SMTP.

Pour appliquer un filtre de connexion à un serveur virtuel SMTP

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, le serveur qui vous intéresse, puis **Protocoles** et **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP auquel le filtre doit être appliqué, puis cliquez sur **Propriétés**.
4. Dans **Propriétés de <*Serveur virtuel SMTP*>**, sous l'onglet **Général**, cliquez sur **Avancé**.
5. Dans la boîte de dialogue **Fonctionnalités avancées**, sélectionnez l'adresse IP à laquelle appliquer le filtre, puis cliquez sur **Modifier**.
6. Dans **Identification**, activez la case à cocher **Appliquer le filtre de connexion** afin de mettre en œuvre le filtre défini précédemment (figure 10.7).

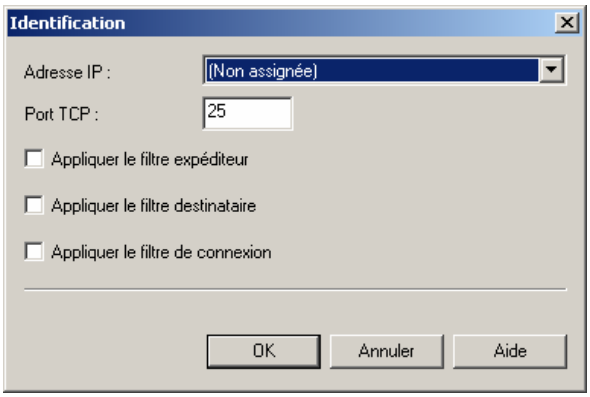


Figure 10.7 Boîte de dialogue Identification

7. Si vous possédez plusieurs serveurs virtuels, répétez les étapes 3 à 6 pour chaque serveur auquel le filtre doit être appliqué.

Filtrage des destinataires

Grâce au filtrage des destinataires, vous pouvez filtrer les messages envoyés aux destinataires qui n'existent pas dans votre organisation ou ajouter des adresses de destinataires spécifiques souvent ciblées par les expéditeurs de courrier indésirable.

Activation du filtrage des destinataires

Activez le filtrage des destinataires en procédant comme suit :

1. Créez le filtre destinataire dans la boîte de dialogue **Propriétés de Remise des messages**, sous l'onglet **Filtrage des destinataires**.
2. Appliquez le filtre au niveau du serveur virtuel SMTP.

Chaque étape est décrite en détail dans les sections ci-après.

Étape 1 : création d'un filtre destinataire

Créez un filtre destinataire en procédant comme suit :

Pour créer un filtre destinataire

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, double-cliquez sur **Paramètres globaux**, cliquez avec le bouton droit sur **Remise des messages**, puis cliquez sur **Propriétés**.
3. Dans **Propriétés de Remise des messages**, cliquez sur l'onglet **Filtrage des destinataires** (figure 10.8).

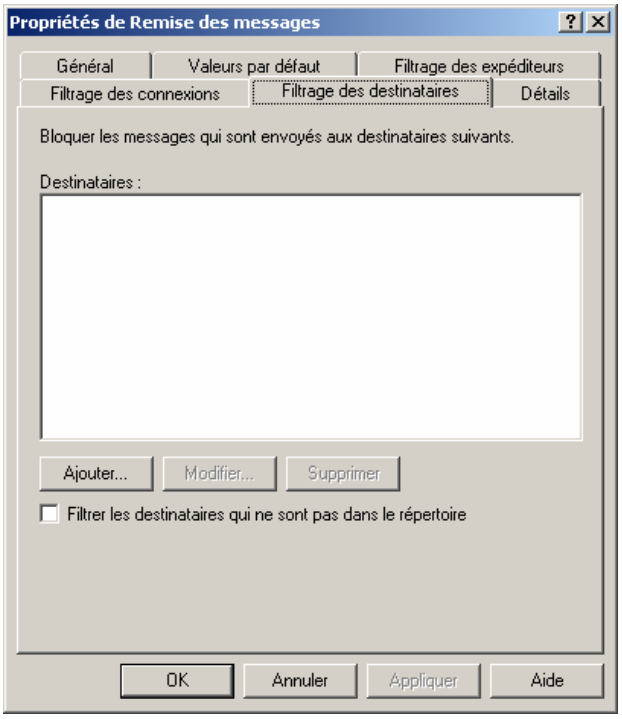


Figure 10.8 Onglet Filtrage des destinataires de la boîte de dialogue Propriétés de Remise des messages

4. Pour ajouter l'adresse d'un destinataire précis, cliquez sur **Ajouter**, puis, dans **Ajouter un destinataire**, entrez l'adresse du destinataire et cliquez sur **OK**. L'adresse du destinataire doit répondre aux critères suivants :
   - L'adresse du destinataire doit contenir le signe @.
   - Les noms complets doivent être placés entre guillemets et suivis immédiatement du signe @. Assurez-vous qu'aucun espace ne figure entre les guillemets et le signe @. Par exemple, si vous souhaitez filtrer le courrier d'un destinataire dont le nom complet est Pierre Lopez dans le domaine contoso.com, vous devez taper :

     "Pierre Lopez"@contoso.com
   - Utilisez un astérisque (*) pour englober tous les membres d'un domaine ou entrez simplement @domaine. Par exemple, pour filtrer le courrier envoyé à tous les utilisateurs dont le suffixe de domaine est contoso.com, tapez au choix :

     ***@contoso.com**

     @contoso.com

5. Pour filtrer le courrier envoyé aux utilisateurs qui ne figurent pas dans le service d'annuaire Microsoft Active Directory®, activez la case à cocher **Filtrer les destinataires qui ne sont pas dans le répertoire**.

   Remarque L'activation de la case à cocher **Filtrer les destinataires qui ne sont pas dans le répertoire** peut permettre à des expéditeurs malintentionnés de découvrir des adresses électroniques valides dans votre organisation Exchange.

Étape 2 : application du filtre destinataire aux serveurs virtuels SMTP appropriés

Après avoir créé le filtre destinataire, vous devez l'appliquer aux serveurs virtuels SMTP adéquats. En règle générale, vous devez effectuer cette opération sur les serveurs virtuels SMTP présents sur les serveurs de passerelle qui acceptent les messages électroniques en provenance d'Internet. La procédure ci-dessous vous permet d'appliquer un filtre destinataire à un serveur virtuel SMTP.

Pour appliquer un filtre destinataire à un serveur virtuel SMTP

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez **Serveurs**, le serveur qui vous intéresse, puis **Protocoles** et **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP auquel le filtre doit être appliqué, puis cliquez sur **Propriétés**.
4. Dans **Propriétés de <*Serveur virtuel SMTP*>**, sous l'onglet **Général**, cliquez sur **Avancé**.
5. Dans la boîte de dialogue **Fonctionnalités avancées**, sélectionnez l'adresse IP à laquelle appliquer le filtre, puis cliquez sur **Modifier**.
6. Dans **Identification**, activez la case à cocher **Appliquer le filtre destinataire** afin de mettre en œuvre le filtre défini précédemment (figure 10.9).

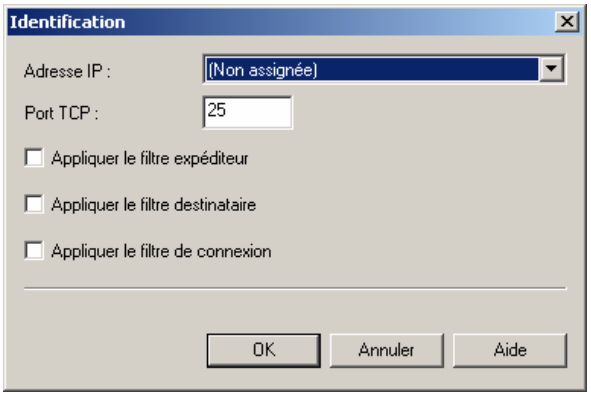


Figure 10.9 Boîte de dialogue Identification

7. Si vous possédez plusieurs serveurs virtuels, répétez les étapes 3 à 6 pour chaque serveur auquel le filtre doit être appliqué.

Filtrage des expéditeurs

Il fonctionne de la même manière dans Exchange Server 2003 et Exchange 2000 Server ; il vous permet de filtrer les messages envoyés par un expéditeur spécifique. Vous pouvez bloquer les messages envoyés par les utilisateurs d'un domaine ou par un expéditeur spécifique.

Activation du filtrage des expéditeurs

Activez le filtrage des expéditeurs en procédant comme suit :

1. Créez le filtre expéditeur à partir des paramètres globaux, dans la boîte de dialogue **Propriétés de Remise des messages**, sous l'onglet **Filtrage des expéditeurs**.
2. Appliquez le filtre au niveau du serveur virtuel SMTP.

Description de l'application des filtres activés et des restrictions IP

Exchange 2003 prend en charge les filtres et restrictions IP suivants :

- filtrage des connexions ;
- filtrage des destinataires ;
- filtrage des expéditeurs ;
- restrictions IP en fonction d'un serveur virtuel.

Bien que configurés dans la boîte de dialogue **Propriétés de Remise des messages**, le filtrage des connexions, le filtrage des destinataires et le filtrage des expéditeurs doivent être activés sur chaque serveur virtuel SMTP. En revanche, les restrictions IP sont configurées sur chaque serveur virtuel SMTP.

Cette section décrit l'ordre dans lequel les filtres et restrictions IP, une fois configurés et activés, sont contrôlés lors d'une session SMTP.

1. Un client SMTP tente de se connecter au serveur virtuel SMTP.
2. L'adresse IP du client qui se connecte est comparée aux restrictions IP du serveur virtuel SMTP (configurées via le bouton **Connexion** situé sous l'onglet **Accès** de la boîte de dialogue **Propriétés** du serveur virtuel SMTP) :
   - Si l'adresse IP de connexion figure dans la liste des adresses IP restreintes, la connexion est immédiatement abandonnée.
   - Si l'adresse IP de connexion ne figure pas dans la liste des adresses IP restreintes, la connexion est acceptée.
3. Le client SMTP émet une commande EHLO ou HELO.
4. Le client SMTP émet une commande MAIL FROM: similaire à celle-ci :

   MAIL FROM: pierre@contoso.com
5. L'adresse IP du client SMTP est alors recherchée dans la liste d'autorisations globale (configurée via l'onglet **Filtrage des connexions** de la boîte de dialogue **Propriétés de Remise des messages** du Gestionnaire système Exchange).
   - Si l'adresse IP de connexion figure dans la liste d'autorisations globale, Exchange ne consulte pas la liste de refus globale. L'étape 6 du traitement est ignorée pour être remplacée par l'étape 7.

- Si l'adresse IP de connexion ne figure pas dans la liste d'autorisations globale, les étapes 6 et 7 sont exécutées.

6. L'adresse IP du client SMTP est recherchée dans la liste de refus globale (configurée via l'onglet **Filtrage des connexions** de la boîte de dialogue **Propriétés de Remise des messages** du Gestionnaire système Exchange).
   - Si l'adresse IP du client SMTP figure dans la liste de refus globale, la connexion est abandonnée.
   - Si l'adresse IP du client SMTP ne figure pas dans la liste de refus globale, la session se poursuit.
7. Le filtrage des expéditeurs consiste à vérifier dans la liste des expéditeurs bloqués, l'existence de l'expéditeur indiqué dans la commande MAIL FROM (cette liste est configurée via l'onglet **Filtrage des expéditeurs** de la boîte de dialogue **Propriétés de la remise des messages** du Gestionnaire système Exchange).
   - Si l'expéditeur figure dans la liste des expéditeurs bloqués, l'un des deux scénarios suivants se produit, selon la configuration du filtrage des expéditeurs :

     - Si le filtrage des expéditeurs prévoit l'arrêt de la connexion, celle-ci est abandonnée.

     - Si le filtrage des expéditeurs prévoit l'acceptation des messages sans notification à l'expéditeur, la session se poursuit ; cependant, le courrier est envoyé vers le répertoire Badmail sans être remis au destinataire indiqué.
   - Si l'expéditeur ne figure pas dans la liste de filtrage des expéditeurs, le serveur virtuel SMTP émet une réponse similaire à celle-ci :

     250 2.1.0 pierre@contoso.com…Expéditeur OK
8. Le serveur SMTP de connexion émet une commande RCPT TO similaire à celle-ci :

   RCPT TO: julie@example.com
9. Les règles de filtrage des connexions vérifient l'existence de l'adresse IP de connexion dans les listes transmises par les fournisseurs de listes d'interdiction.
   - Si l'adresse IP du client SMTP figure dans la liste des autorisations, les règles de filtrage des connexions ne sont pas prises en compte. La poursuite du traitement s'effectue à l'étape 10.
   - Le filtrage des connexions vérifie chaque liste d'interdiction du fournisseur de service en fonction de l'ordre configuré. Si le filtrage des connexions trouve une correspondance dans la liste d'interdiction d'un fournisseur, le serveur virtuel SMTP retourne un code d'erreur, puis envoie le message d'erreur personnalisé qui a été configuré pour la règle de filtrage des connexions. Une fois qu'une correspondance est trouvée, la vérification des listes d'interdiction des fournisseurs s'arrête.
   - Si l'adresse IP du client SMTP ne figure pas dans la liste d'interdiction d'un fournisseur de service, la session se poursuit.
10. Le filtrage des connexions vérifie si le destinataire attendu figure dans la liste des exceptions.
    - Si le destinataire figure sur cette liste, la communication est acceptée et aucun autre contrôle n'est appliqué à la commande RCPT TO. Les étapes 11 et 12 du traitement sont ignorées pour être remplacées par l'étape 13.
    - Si le destinataire ne figure pas dans la liste des exceptions, il est recherché dans d'autres filtres.
11. S'il ne figure pas dans la liste des exceptions configurée dans le filtrage des connexions, le destinataire est recherché parmi les destinataires bloqués configurés dans le filtrage des destinataires.
    - Si le destinataire est un destinataire refusé, le serveur virtuel SMTP retourne une erreur indiquant que le destinataire n'est pas valide.
    - Si le destinataire n'est pas un destinataire refusé, la session continue.

12. Si le destinataire n'est pas un destinataire refusé, il fait l'objet d'une recherche dans Active Directory.
    - Si le destinataire n'est pas un destinataire valide dans Active Directory, le serveur virtuel SMTP retourne une erreur indiquant que le destinataire n'est pas valide.
    - Si le destinataire est un destinataire valide répertorié dans Active Directory, la session continue.
13. Les étapes 10 à 12 sont appliquées pour chaque destinataire supplémentaire spécifié dans une commande RCPT TO.
14. Le serveur qui se connecte émet une commande DATA similaire à celle-ci :

    DATA

    À : Julie Akers

    De : pierre@contoso.com<Pierre Lopez>

    Objet : Message électronique
15. Le filtrage des expéditeurs s'assure ensuite que l'adresse **De** ne correspond pas à un expéditeur bloqué.
    - Si l'expéditeur spécifié dans la commande DATA est un expéditeur bloqué, l'un des scénarios suivants se produit :

      - Si la configuration du filtrage des expéditeurs prévoit l'abandon de la connexion, le serveur virtuel SMTP renvoie une erreur 5.1.0 indiquant que l'expéditeur est refusé, puis abandonne la communication.

      - Si le filtrage des expéditeurs prévoit l'acceptation des messages sans notification à l'expéditeur, la session se poursuit ; cependant, le courrier est envoyé vers le répertoire Badmail sans être remis au destinataire indiqué.
    - Si l'expéditeur spécifié dans la commande DATA n'est pas un expéditeur bloqué, le message est accepté et placé en file d'attente pour être remis.

Identification du courrier falsifié

Vous pouvez apprendre à vos utilisateurs à reconnaître du courrier falsifié. Contrairement à Exchange 2000, la configuration par défaut d'Exchange 2003 empêche la résolution des messages électroniques anonymes à l'aide des noms complets. Par conséquent, lorsque du courrier est envoyé depuis une adresse falsifiée, Exchange 2003 ne résout pas l'adresse de messagerie de l'expéditeur à l'aide du nom complet dans la liste d'adresses globale.

Pour comprendre comment Exchange 2003 empêche l'usurpation d'adresse, prenons l'exemple d'un utilisateur interne nommé Pierre Lopez. Celui-ci envoie du courrier en interne à partir du domaine example.com. Le message électronique affiche l'adresse d'expédition sous la forme **Pierre Lopez**, ce qui correspond au nom complet configuré dans Active Directory pour pierre@example.com (en effet, lorsque Pierre Lopez envoie du courrier, il représente un utilisateur authentifié). Exchange vérifie ensuite si Pierre Lopez dispose des autorisations « Envoyer en tant que » dans ses informations d'identification, puis il résout l'adresse de messagerie en utilisant le nom complet correspondant dans Active Directory. L'usurpation d'adresse se produit lorsqu'un utilisateur non autorisé falsifie l'adresse de Pierre pour envoyer du courrier à un autre utilisateur du même domaine.

Exchange 2003 ne résout pas les adresses de messagerie ayant une origine externe. Par conséquent, lorsqu'un utilisateur anonyme tente d'envoyer du courrier en usurpant l'adresse de Pierre, Exchange ne résout pas l'adresse d'expédition en nom complet sur la ligne **De**. À la place, **pierre@example.com** s'affiche sur la ligne **De** du courrier électronique. Si vos utilisateurs comprennent cette différence, ils pourront au moins identifier le courrier falsifié.

Toutefois, par défaut, les serveurs Exchange 2000 résolvent effectivement le courrier électronique anonyme. Si votre organisation comporte des serveurs Exchange 2000 et si ces derniers résolvent un message électronique anonyme qu'ils envoient ensuite vers un serveur Exchange 2003, l'adresse du message sera convertie en nom complet figurant dans la liste d'adresses globale. Pour y remédier, configurez vos serveurs Exchange 2000 de sorte qu'ils ne résolvent pas le courrier anonyme.

Pour s'assurer que le serveur Exchange 2003 est configuré pour ne pas résoudre le courrier anonyme

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez le nœud **Serveurs**, **< *Nom serveur tête de pont* >**, **Protocoles**, puis **SMTP**.
3. Cliquez avec le bouton droit sur le serveur virtuel SMTP souhaité, puis cliquez sur **Propriétés**.
4. Sous l'onglet **Accès**, cliquez sur **Authentification**.
5. Dans **Authentification**, sous la case à cocher **Accès anonyme**, assurez-vous que la case à cocher **Résoudre la messagerie anonyme** est désactivée.

   Remarque N'oubliez pas que si le serveur est un serveur virtuel SMTP interne, vous pouvez également désactiver la case à cocher **Accès anonyme**. Pour plus d'informations sur l'accès anonyme à un serveur virtuel SMTP interne, consultez « Blocage de l'accès anonyme aux serveurs virtuels SMTP internes et aux serveurs virtuels SMTP dédiés pour les clients IMAP et POP » dans le chapitre 9.

Pour configurer Exchange 2000 afin de ne pas résoudre les adresses de messagerie ayant une origine externe

Avertissement Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données importantes.

1. Démarrez l'Éditeur du Registre. Cliquez sur **Démarrer**, sur **Exécuter**, tapez **regedt32**, puis cliquez sur **OK**.
2. Recherchez ou créez la clé suivante dans le Registre (où *1* correspond au numéro du serveur virtuel SMTP) :

   HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/MsExchangeTransport/Parameters/1

   Remarque Vous devrez peut-être créer la clé **Parameters** et la clé **1**.
3. Dans le menu **Edition**, cliquez sur **Ajouter une valeur**, puis ajoutez la valeur de Registre suivante :

   ```
   Value name: ResolveP2
   Data type: REG_DWORD
   ```
4. À l'aide des indicateurs suivants, déterminez la valeur à utiliser :

   ```
   Field                Value
   -----------          -----
   FROM:                2
   TO: and CC:          16
   REPLY TO:            32
   ```

   Pour déterminer cette valeur, ajoutez les valeurs de tous les éléments à résoudre. Par exemple, pour résoudre tous les champs à l'exception de l'expéditeur, tapez **48** (16+32=48). Pour résoudre uniquement les destinataires, tapez seulement **16**. Par défaut, Exchange 2000 résout tous les champs (vous pouvez

spécifier ce comportement soit en supprimant la clé, soit en définissant la valeur à l'aide de la formule suivante : 2+16+32=50).

5. Quittez l'Éditeur du Registre.
6. Redémarrez le serveur virtuel SMTP.

Soyez prudent lorsque vous sélectionnez les serveurs sur lesquels vous souhaitez activer ce paramètre. Si vous modifiez le comportement sur le serveur virtuel SMTP par défaut et si votre organisation comporte un grand nombre de serveurs, tout le courrier interne en provenance d'autres serveurs Exchange 2000 sera également affecté. Par conséquent, dans la mesure où Exchange 2000 utilise le protocole SMTP pour router le courrier interne entre les serveurs, vous devrez peut-être créer un serveur virtuel SMTP, voire appliquer ce paramètre uniquement à un serveur SMTP tête de pont entrant.

Quatrième partie Résolution des problèmes

La quatrième partie se concentre sur les techniques relatives à la résolution des problèmes ; vous pouvez utiliser ces informations pour identifier et résoudre les problèmes de transport. Elle présente également certains scénarios classiques pouvant être à l'origine des problèmes de flux des messages, ainsi que les solutions envisageables.

Chapitre 11 « Résolution des problèmes de routage »
: Ce chapitre fournit des informations sur l'utilisation de l'outil WinRoute pour résoudre les problèmes de routage dans un environnement de messagerie basé sur Microsoft® Exchange 2000 Server et Exchange Server 2003.

Chapitre 12 « Résolution des problèmes de flux des messages et SMTP »
: Ce chapitre décrit de nombreux problèmes courants liés au flux des messages. En outre, il fournit des informations sur l'utilisation de plusieurs outils et explique comment configurer l'enregistrement des diagnostics.

Chapitre 13 « Résolution des problèmes de rapports de non-remise »
: Ce chapitre fournit les stratégies et outils à utiliser lorsque vous tentez de résoudre des problèmes liés aux rapports de non-remise. Les rapports de non-remise représentent un type de notification d'état de remise.

Résolution des problèmes de routage

Ce chapitre décrit certaines situations usuelles qui peuvent perturber le routage dans votre organisation Microsoft® Exchange. Les thèmes abordés sont les suivants :

Utilisation de WinRoute
Cette section décrit l'importance de l'outil WinRoute pour la résolution des problèmes de routage.

Problèmes courants relatifs à l'état des liaisons
Cette section décrit les problèmes engendrés par les déconnexions entre groupes de routage, les conflits entre maîtres de groupe de routage, les suppressions de groupes de routage, les connecteurs non signalés comme étant disponibles et les connexions oscillantes. Par ailleurs, cette section explique également comment résoudre les problèmes cités précédemment.

Propagation de l'état des liaisons rompues
Cette section décrit les problèmes qui surviennent lorsque vous remplacez le serveur tête de pont Exchange Server 5.5 d'un groupe de routage par un serveur tête de pont Exchange 2000 Server ou Exchange Server 2003, et que vous restaurez ultérieurement le serveur tête de pont à la version Exchange Server 5.5.

Procédures du chapitre 11

Le tableau 11.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 11.1 Procédures du chapitre 11 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Désactiver les modifications de l'état des liaisons	Membre du groupe Administrateurs local.

Utilisation de WinRoute

WinRoute est un outil Exchange 2003 qui permet de déterminer les informations connues du maître de routage, notamment la topologie du routage et l'état des liaisons. Cet outil doit constituer la première étape de la résolution des problèmes de routage dans un environnement de messagerie Exchange 2000 et Exchange 2003. L'outil se connecte au port d'état des liaisons (port TCP 691) sur un serveur Exchange 2000 ou Exchange 2003, puis extrait les informations sur l'état des liaisons pour une organisation. Les informations se composent d'une série de GUID que WinRoute associe à des objets du service d'annuaire Microsoft Active Directory®, des connecteurs et des serveurs têtes de pont. Ces informations sont ensuite présentées par WinRoute dans un format lisible.

> **Remarque** L'outil WinRoute et la documentation de l'utilisateur (en anglais) sont disponibles sur le site Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=25097). Il est recommandé de télécharger et d'utiliser cet outil sur tous les serveurs Exchange 2000 et Exchange 2003 de votre organisation. De préférence, utilisez cet outil à la place de l'outil WinRoute livré avec Exchange 2000.

Problèmes courants relatifs à l'état des liaisons

Dans un groupe de routage, Exchange utilise le port TCP 691 pour communiquer les mises à jour d'informations relatives à l'état des liaisons et au routage entre le maître et les membres du groupe de routage. Entre deux groupes de routage, deux serveurs têtes de pont de groupe de routage utilisent le verbe X-LINK2STATE pour échanger des informations sur l'état des liaisons en comparant le condensé, une signature numérique cryptée dans le paquet Orginfo, qui contient les informations sur l'état des liaisons des deux serveurs têtes de pont du groupe de routage. Toute incohérence entre ces condensés entraîne l'échange d'informations sur l'état des liaisons entre les deux serveurs via le port SMTP 25.

Le maître du groupe de routage coordonne les modifications de l'état des liaisons reçues par les serveurs de son groupe de routage ; il extrait ensuite les mises à jour à partir d'Active Directory. Si le maître du groupe de routage n'est plus disponible, tous les serveurs du groupe de routage continuent de fonctionner en se basant sur les informations communes reçues au moment de la perte du contact avec le maître du groupe de routage.

Lorsque le maître du groupe de routage est à nouveau disponible, il reconstruit ses informations sur l'état des liaisons, en commençant par tous les serveurs et connecteurs signalés comme étant non disponibles. Au fil de sa recherche des serveurs non disponibles, le maître du groupe de routage met à jour les membres du groupe de routage.

Cette section traite des problèmes relatifs à l'état des liaisons et décrit la solution recommandée :

- Déconnexion entre le membre et le maître du groupe de routage
- Conflits entre les maîtres de groupe de routage
- Problèmes causés par la suppression de groupes de routage
- Connecteurs non signalés comme étant « hors service »
- Connexions oscillantes

Déconnexion entre un membre et le maître du groupe de routage

Lorsqu'un membre du groupe de routage ne parvient pas à se connecter au maître du groupe de routage, WinRoute signale le problème par une croix (X) rouge en regard du membre du groupe de routage (voir figure 11.1).

Figure 11.1 Déconnexion entre des membres et le maître du groupe de routage

Résolvez le problème en procédant comme suit :

- Assurez-vous que le service du moteur de routage Microsoft Exchange (RESvc) a démarré et qu'il se trouve dans un état stable sur tous les serveurs concernés du groupe de routage. Si le service du moteur de routage n'est pas dans un état stable, les membres du groupe de routage risquent de ne pas pouvoir se connecter au maître du groupe de routage. Recherchez au préalable toute cause principale d'instabilité des services.
- Assurez-vous que le port 691 n'est pas bloqué par un pare-feu. Pour ce faire, démarrez une session telnet sur le port 691 des serveurs affectés et du nœud maître. Vous devez voir s'afficher une bannière du moteur de routage Microsoft qui indique un état actif.
- À partir d'une ligne de commande, tapez :

  ```
  netstat –a –n
  ```

  Le résultat doit montrer que tous les membres du groupe de routage, y compris le maître, sont connectés au port 691 sur le nœud maître, comme l'illustrent les informations ci-après :

  ```
  TCP    127.0.0.1:691          127.0.0.1:691          ESTABLISHED
  ```

- Recherchez dans le journal Applications de l'Observateur d'événements les événements indiquant un échec de l'authentification à l'aide du compte d'ordinateur (*domaine*\n*om du serveur*). Analysez les événements de transport suivants :
  - L'ID d'événement 961 est enregistré lorsqu'un serveur membre ne parvient pas à s'authentifier auprès de son maître de groupe de routage.
  - L'ID d'événement 962 est enregistré une fois qu'un nœud client n'est pas parvenu à s'authentifier auprès du service de routage (RESvc).
  - L'ID d'événement 996 est enregistré lorsque le nœud de routage d'un client parvient à s'authentifier auprès du service du moteur de routage.
  - L'ID d'événement 995 est enregistré lorsque le membre d'un groupe de routage parvient à s'authentifier auprès de son maître de groupe de routage.
- Assurez-vous que les serveurs affectés peuvent générer un nom principal de service (SPN) lors du processus d'authentification ; à cet effet, vérifiez la valeur ncacn_ip_tcp dans l'attribut d'adresse réseau de

ces serveurs. Pour ce faire, utilisez un outil d'accès à l'annuaire, par exemple LDP (ldp.exe) ou ADSI Edit (adsiEdit.msc).

Les membres d'un groupe de routage doivent s'authentifier mutuellement auprès du maître du groupe de routage auquel ils doivent se connecter. Pour y parvenir, ils utilisent la valeur ncacn_ip_tcp contenue dans l'attribut d'adresse réseau du serveur Exchange afin de générer le nom principal de service du nœud maître en appelant **DsClientMakeSpnForTargetServer**. Les membres du groupe de routage peuvent alors s'authentifier via Kerberos. Assurez-vous que cette valeur correspond à un nom de domaine complet et non à un nom NetBIOS ou une adresse IP (Internet Protocol). Redémarrez le service du moteur de routage Exchange.

- Assurez-vous que le mot de passe du compte d'ordinateur de domaine n'est pas arrivé à expiration.
- Assurez-vous que le nom de domaine complet du serveur virtuel correspond au nom de domaine complet contenu dans le serveur DNS.
- Si le groupe de routage appartient à plusieurs domaines, assurez-vous que la cause du problème n'est pas liée à une erreur de configuration DNS pour un domaine enfant ou racine.
- Passez en revue les applications ou objets de stratégie de groupe non-Microsoft qui restreignent les autorisations ou la sécurité.
- Configurez un autre serveur du groupe de routage en tant que maître du groupe de routage. Cette approche constitue une solution provisoire. La réaffectation du rôle assumé par le maître du groupe de routage peut permettre de contourner le problème en attendant qu'il soit définitivement résolu.

Conflits entre les maîtres de groupe de routage

Le premier serveur installé dans le groupe de routage est automatiquement désigné en tant que nœud maître ou maître du groupe de routage. Au fur et à mesure que des serveurs supplémentaires sont installés, vous pouvez désigner un autre serveur en tant que maître du groupe de routage.

Quel que soit le moment, il ne doit exister qu'un seul serveur identifié par lui-même et les autres serveurs comme étant le maître. Cette configuration est mise en œuvre par un algorithme selon lequel (*N*/2) + 1 serveurs du groupe de routage doivent accepter et reconnaître le maître. *N* représente le nombre de serveurs du groupe de routage. Par conséquent, les nœuds membres envoient au maître les données ATTACH relatives à l'état des liaisons.

Parfois, plusieurs serveurs considèrent à tort un autre serveur comme le maître du groupe de routage. Par exemple, si un maître du groupe de routage est déplacé ou supprimé sans qu'un autre nœud maître soit choisi, il arrive que **msExchRoutingMasterDN** (attribut contenu dans Active Directory et qui désigne le maître du groupe de routage) pointe vers un serveur supprimé dans la mesure où cet attribut n'est pas lié.

En outre, cette situation peut également se produire lorsqu'un ancien maître du groupe de routage refuse de céder son rôle de maître, ou lorsqu'un nœud non autorisé continue d'envoyer des données ATTACH sur l'état des liaisons vers un ancien maître du groupe de routage. Dans Exchange 2003, si **msExchRoutingMasterDN** pointe vers un objet supprimé, le nœud maître cède puis arrête son rôle de maître.

Résolvez le problème en procédant comme suit :

- Assurez-vous que la propagation de l'état des liaisons s'effectue correctement dans le groupe de routage sur le port 691. Assurez-vous également que la communication n'est pas bloquée par un pare-feu ou un filtre SMTP.
- Assurez-vous qu'aucun service Exchange n'est arrêté.
- Vérifiez les latences au niveau de la réplication Active Directory en utilisant le moniteur de réplication Active Directory (Replmon.exe) disponible dans le Kit de Ressources techniques de Windows.
- Recherchez l'existence de problèmes et latences sur le réseau.

- Vérifiez si des maîtres de groupe de routage ont été supprimés ou si des serveurs ont cessé d'exister. Si tel est le cas, l'événement de transport 958 est enregistré dans le journal Applications de l'Observateur d'événements afin d'indiquer qu'un maître du groupe de routage a cessé d'exister. Vérifiez ces informations en utilisant un outil d'accès à l'annuaire, par exemple LDP (ldp.exe) ou ADSI Edit (adsiEdit.msc).

Problèmes causés par la suppression de groupes de routage

Lorsque des groupes de routage sont supprimés à la suite de l'éviction de serveurs ou pour d'autres raisons, WinRoute affiche parfois le message « object_not_found_in_DS » (figure 11.2).

Les serveurs Exchange gèrent la table d'état des liaisons qui continue de faire référence aux objets ; cependant, ces derniers ne figurent plus dans Active Directory lorsque le service du moteur de routage initialise puis parcourt Active Directory à leur recherche.

Le service de routage Exchange ne peut pas supprimer automatiquement les groupes de routage et leurs membres (c'est-à-dire les serveurs et les connecteurs) de la table d'état des liaisons. En fait, le service de routage traite les groupes de routage supprimés de la même façon que les groupes de routage fonctionnels déjà existants. Très rarement, il arrive que les groupes de routage supprimés provoquent des dysfonctionnements en matière de routage et de boucles de courrier. Les groupes de routage supprimés peuvent sérieusement affecter les topologies dans lesquelles un site Exchange 5.5 se joint à une organisation Exchange 2003.

En outre, les objets relatifs aux groupes de routage supprimés peuvent faire augmenter de manière significative la taille de la table d'état des liaisons, ce qui se traduit par un accroissement du trafic réseau lié à l'échange des informations sur l'état des liaisons.

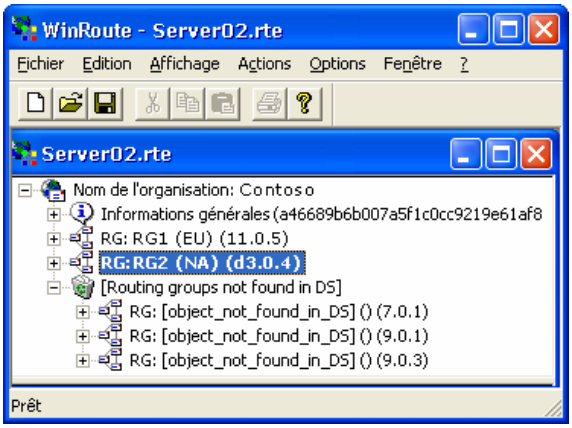


Figure 11.2 Groupe de routage supprimé dans WinRoute

Pour résoudre ce problème, assurez-vous que le compte utilisé pour afficher les informations de routage sur le serveur dispose des autorisations appropriées. Si possible, connectez-vous à WinRoute à l'aide du compte système et utilisez la commande interactive AT. L'absence d'autorisations de lecture appropriées peut entraîner l'affichage de messages d'erreur du type object_not_found_in_DS dans WinRoute.

Utilisez l'une des méthodes ci-après pour purger les données relatives aux groupes de routage supprimés dans les informations sur l'état des liaisons :

- Arrêtez simultanément tous les serveurs de l'organisation afin d'actualiser les informations du cache du routage, puis purgez les connecteurs et les groupes de routage supprimés.
- Arrêtez simultanément tous les services liés à Exchange et à l'Infrastructure de gestion Windows (WMI, *Windows Management Instrumentation*) sur tous les serveurs Exchange de l'organisation.

Connecteurs non signalés comme étant « hors service »

Il arrive que l'état des liaisons d'un connecteur indique « en service » alors qu'il est en réalité non disponible ou « hors service ». Voici les situations dans lesquelles le service de routage ne signale pas que l'état des liaisons d'un connecteur est hors service :

- Les connecteurs utilisent un service DNS pour effectuer un routage vers un domaine de l'espace d'adressage (connecteurs SMTP utilisant le service DNS par exemple).
- Les connecteurs sont de type Exchange 5.5 ou EDK (Exchange Development Kit) ; ils n'utilisent pas le routage des informations sur l'état des liaisons.
- Les connecteurs du groupe de routage sont utilisés avec les serveurs têtes de pont locaux d'un serveur tête de pont local. Pour désigner un serveur en tant que serveur tête de pont local, cliquez sur **Tous les serveurs locaux peuvent envoyer des messages via ce conn.** lors de la création d'un groupe de routage.
- Les connecteurs du groupe de routage sont utilisés avec un serveur Exchange 5.5 désigné en tant que serveur tête de pont.

Voici d'autres situations particulières :

- Le relais du courrier ne parvient pas à empêcher les boucles de l'Agent de transfert des messages dans un groupe de routage.
- Les connecteurs sont configurés à l'aide d'un hôte actif qui vient juste d'être modifié.

Pour permettre au service de routage de signaler le connecteur comme étant hors service, tous les serveurs têtes de pont sources doivent être mis hors service et indiquer l'état VS_CONN_NOT_AVAILABLE ou VS_CONN_NOT_STARTED. Vous pouvez vérifier les informations d'état à l'aide de WinRoute.

Connexions oscillantes

Les connecteurs situés sur un réseau non fiable et signalés comme étant « en service » puis « hors service » de manière répétée, provoquent de très nombreuses mises à jour de l'état des liaisons entre les serveurs. Ces modifications entraînent des opérations lourdes et fréquentes qui consistent à recalculer les itinéraires dans Exchange. Dans l'Observateur d'événements, l'ID d'événement 4005 est enregistré fréquemment et s'affiche aux côtés du texte « réinitialisation des itinéraires ». Si Exchange 2003 détecte de fréquentes modifications de l'état du connecteur, il les atténue en laissant indiqué l'état « en service » dans une seule plage d'interrogation, période durant laquelle un serveur analyse les modifications. Cependant, si ces modifications se produisent à différentes périodes d'interrogation, une connexion oscillante peut tout de même générer du trafic relatif à l'état des liaisons. Par défaut, l'intervalle entre deux interrogations est de 10 minutes pour les serveurs Exchange 2003.

Le service de routage Exchange choisit le chemin d'accès optimal et recherche le serveur suivant vers lequel un message pourra effectuer son prochain saut ; par ailleurs, il place en file d'attente le nom du serveur correspondant au « saut suivant ». Le chemin d'accès optimal est choisi en fonction de variables telles que la charge de traitement, le type de message et les restrictions. Par conséquent, en raison de l'état oscillant d'un connecteur, Exchange doit recalculer fréquemment le chemin d'accès le plus optimal possible, ce qui entraîne l'envoi de requêtes vers Active Directory et une baisse des performances.

Lorsque la file d'attente Exchange détecte un problème de liaison vers le serveur tête de pont d'un connecteur, le service de routage relaie ces informations vers le maître du groupe de routage. Ce dernier supprime les informations pendant 10 minutes au maximum afin d'empêcher toute fluctuation de l'état du connecteur. Si le service de routage signale le connecteur comme étant hors service, cette modification est propagée vers tous les serveurs Exchange de l'organisation, y compris le serveur sur lequel la défaillance s'est produite. Cette

notification se nomme une réinitialisation d'itinéraire. Par ailleurs, il s'agit d'un processus très lourd en terme d'utilisation de la CPU. Le courrier n'est plus placé en file d'attente sur le connecteur ; en outre, le service de routage doit générer de nouveaux chemins d'accès de remise. Le même traitement se produit pour signaler un connecteur comme étant en service.

Une connexion oscillante a lieu dans les situations suivantes :

- Il existe des problèmes réseau qui sont visibles via un suivi du réseau.
- Des réactions se produisent face aux rappels de notification d'état des liaisons émanant de services de protocoles sous-jacents (SMTP et MTA), à la suite d'une interférence provoquée aux niveaux des protocoles X.400 ou SMTP par des applications non-Microsoft. Dans ce scénario, les problèmes ne sont visibles qu'à travers une capture des événements à l'aide d'un moniteur réseau. En outre, vous pouvez utiliser l'outil remonitor.exe disponible auprès des services de support technique Microsoft.

Vous pouvez utiliser le Moniteur réseau (Netmon.exe) ou l'outil remonitor.exe pour identifier et résoudre à la base les problèmes de connexions oscillantes.

Propagation de l'état des liaisons rompues

Les serveurs Exchange 5.5 n'utilisent pas les informations sur l'état des liaisons. En revanche, ils s'appuient sur la table de routage d'adresses de la passerelle pour router les messages. Dans une organisation en mode mixte, Exchange 2000 et les versions ultérieures reconnaissent cette limitation et lisent la configuration des serveurs Exchange 5.5 directement depuis Active Directory. Par conséquent, les serveurs Exchange 2000 et Exchange 2003 ne s'attendent pas à un échange d'informations sur l'état des liaisons avec les serveurs Exchange 5.5.

Lorsqu'un serveur tête de pont Exchange 5.5 appartenant à un groupe de routage Exchange est mis à niveau vers un serveur Exchange 2000 ou Exchange 2003, et qu'il est désigné en tant que serveur tête de pont, il commence à participer à l'échange d'informations sur l'état des liaisons ; par ailleurs, son numéro de version majeur n'est plus zéro. Les serveurs Exchange 2000 et Exchange 2003 utilisent des numéros de version dans les tables d'état des liaisons afin de les comparer entre elles et de s'assurer que les serveurs disposent des informations les plus récentes sur l'état des liaisons. Un numéro de version majeur dont la valeur est égale à zéro désigne un serveur qui ne participe pas à l'échange d'informations sur l'état des liaisons ou qui n'y a jamais participé. Tous les serveurs Exchange 5.5 disposent d'un numéro de version égal à zéro, car ils n'échangent pas d'informations sur l'état des liaisons. Lorsque le serveur est mis à niveau vers un serveur Exchange 2000 ou Exchange 2003, il se met à participer à l'échange d'informations sur l'état des liaisons et incrémente son numéro de version majeur. Par conséquent, les serveurs têtes de pont des autres groupes de routage s'attendent à ce que le serveur qui vient d'être mis à niveau les informe sur les modifications de l'état des liaisons dans son propre groupe de routage.

Un problème se produit si vous désignez à présent un serveur Exchange 5.5 en tant que serveur tête de pont de ce groupe de routage. En effet, les autres serveurs s'attendent à ce que le serveur tête de pont Exchange 5.5, anciennement serveur tête de pont Exchange 2000 ou Exchange 2003, participe à la propagation de l'état des liaisons ; par conséquent, ils attendent que ce serveur leur fournisse des informations mises à jour sur l'état des liaisons. Cependant, dans la mesure où le serveur est redevenu un serveur Exchange 5.5, il ne dispose plus d'une table d'état des liaisons. Par conséquent, ce groupe de routage est à présent isolé et ne participe pas aux mises à jour dynamiques de l'état des liaisons dans l'organisation.

L'isolement d'un groupe de routage s'avère problématique dans une situation comme celle illustrée dans la figure 11.3. Un connecteur Messagerie Internet Exchange 5.5 et un connecteur SMTP Exchange 2003 utilisent tous les deux le même hôte actif pour router le courrier vers Internet. L'hôte actif cesse d'être disponible. Par conséquent, le serveur tête de pont Exchange 2003 indique que l'itinéraire passant par son connecteur SMTP n'est pas disponible. Toutefois, dans la mesure où le serveur tête de pont s'attend à ce que le serveur Exchange

5.5 envoie des informations sur l'état des liaisons concernant ses groupes de routage et ses connecteurs, il suppose que l'itinéraire passant par le connecteur Messagerie Internet est disponible et tente donc de l'utiliser pour remettre des messages. Après un seul échec, le serveur Exchange 2003 détecte une éventuelle boucle et cesse d'effectuer des remises en empruntant cet itinéraire.

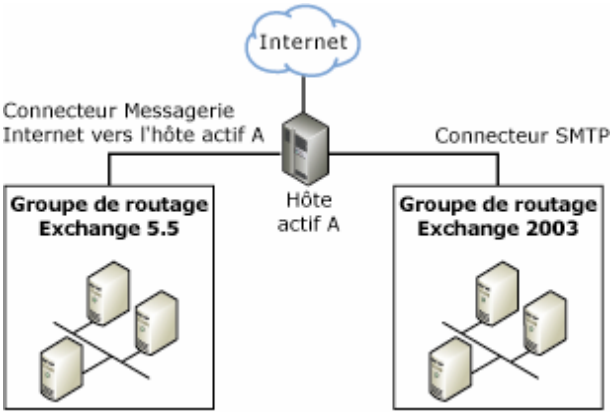


Figure 11.3 Serveurs Exchange 5.5 et Exchange 2003 se connectant à un hôte actif

Pour résoudre ce problème, il existe deux solutions possibles :

- Vous mettez à niveau le serveur tête de pont Exchange 5.5 vers un serveur Exchange 2000 ou Exchange 2003, ou bien vous utilisez un autre serveur Exchange 2000 ou Exchange 2003 pour envoyer à nouveau les informations sur l'état des liaisons pour ce groupe de routage. Chacune de ces options constitue une méthode de résolution simple et conseillée.
- Vous désactivez entièrement l'état des liaisons entre les groupes de routage, puis vous redémarrez tous les serveurs de votre organisation.

Si vous ne pouvez pas désigner de serveur tête de pont Exchange 2000 ou Exchange 2003, désactivez l'état des liaisons. Pour désactiver l'état des liaisons entre des groupes de routage dans votre organisation Exchange, annulez l'inscription de xlsasink.dll sur tous vos serveurs têtes de pont. Ce fichier active les interfaces entre le protocole SMTP et le moteur de routage utilisé pour communiquer les informations sur l'état des liaisons entre les groupes de routage, dans l'ensemble de l'organisation. Lorsque vous annulez l'inscription de xlsasink.dll, vous supprimez la commande qui rend possible la communication de l'état des liaisons entre les groupes de routage. Si les informations sur l'état des liaisons ne peuvent plus être envoyées via le protocole SMTP, le groupe de routage s'isole effectivement du reste de l'organisation (du point de vue de l'état des liaisons).

> **Important** Vous devez soigneusement choisir le moment où vous désactivez l'état des liaisons, car il est important que tous les serveurs disposent d'un numéro de version majeur égal à zéro (0). (Ces informations indiquent des modifications dans un groupe de routage.) Dans une nouvelle installation, vous devez désactiver les informations sur l'état des liaisons immédiatement après avoir installé Exchange. Dans une organisation Exchange existante, travaillez en collaboration avec les services de support technique Microsoft pour vous assurer que vous disposez d'une topologie stable et statique avant de désactiver les informations sur l'état des liaisons.

Pour désactiver les informations sur l'état des liaisons

1. Ouvrez une fenêtre d'invite de commandes et accédez au répertoire ..\Exchsrvr\bin dans le répertoire d'installation de Microsoft Exchange. Par défaut, ce répertoire correspond à *<lettre de lecteur>*:\Program Files\Exchsrvr\bin.
2. Tapez la commande suivante :

   ```
   Regsrv32 –u xlsasink.dll
   ```

3. Redémarrez les services suivants :

- Microsoft Exchange - Moteur de routage (RESvc)
- Service SMTP (SMTPSVC)
- Microsoft Exchange - Piles MTA (MSExchangeMTA)

4. Répétez ce processus sur chaque serveur tête de pont de l'organisation dont vous souhaitez supprimer l'état du connecteur.

Résolution des problèmes de flux des messages et SMTP

Même si vous avez réussi à configurer le protocole SMTP (Simple Mail Transfer Protocol) dans votre organisation Microsoft® Exchange et même si vous avez pris toutes les mesures nécessaires pour le sécuriser, vous pouvez encore rencontrer des problèmes relatifs au flux des messages. Ce chapitre décrit de nombreux problèmes fréquemment rencontrés ainsi que les méthodes permettant de les résoudre.

En particulier, vous apprendrez à :

- utiliser Telnet ;
- utiliser les files d'attente SMTP et X.400 ;
- utiliser le Centre de suivi des messages ;
- utiliser l'Observateur d'événements ;
- configurer l'enregistrement des diagnostics pour le protocole SMTP.

Cependant, avant d'aborder les conseils présentés dans ce chapitre en matière de résolution des problèmes, assurez-vous au préalable qu'Exchange est correctement configuré pour envoyer et recevoir du courrier. Les listes ci-dessous résument brièvement la configuration requise pour assurer un flux correct des messages entrants et sortants.

Pour assurer un flux correct des messages Internet entrants :

- Vos stratégies de destinataire doivent être configurées correctement.
- Le serveur virtuel SMTP qui accepte les messages Internet doit être configuré pour utiliser le port 25 et autoriser les connexions anonymes.
- Un enregistrement de ressource de serveur de messagerie (MX) correspondant à votre domaine doit exister sur un serveur DNS Internet ; en outre, l'enregistrement MX doit pointer vers le domaine Internet ou externe de votre serveur de messagerie.
- Votre serveur de messagerie Internet doit être accessible aux serveurs distants situés sur Internet.

Pour assurer un flux correct des messages Internet sortants :

- Le serveur virtuel SMTP qui envoie les messages Internet doit être configuré pour utiliser le port 25.
- Si vous utilisez des connecteurs SMTP, l'un d'entre eux au moins doit contenir un espace d'adressage composé de *, qui spécifie l'ensemble des domaines externes.
- Votre serveur Exchange doit être capable de résoudre les noms DNS externes. Il existe plusieurs méthodes possibles pour résoudre les noms DNS externes :
    - Utilisez un serveur DNS interne qui transfère le courrier vers un serveur DNS externe.
    - Configurez votre serveur virtuel SMTP de sorte qu'il utilise un serveur DNS externe spécifique.
    - Routez le courrier vers un hôte actif qui effectue la résolution DNS.

Pour plus d'informations sur la manière de configurer Exchange dans le but d'envoyer et de recevoir des messages électroniques, consultez le chapitre 5, « Configuration du service DNS ».

Procédures du chapitre 12

Le tableau 12.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 12.1 Procédures du chapitre 12 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Utiliser telnet pour tester la communication SMTP	Membre du groupe Administrateurs local.
Afficher les propriétés d'une file d'attente	Être membre du groupe Administrateurs local et être membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Afficher les messages d'une file d'attente	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Consulter les compteurs de performance	Membre du groupe Administrateurs local.
Activer le Centre de suivi des messages sur un serveur	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Afficher le journal Applications dans l'Observateur d'événements	Membre du groupe Administrateurs local.
Afficher le journal Système dans l'Observateur d'événements	Membre du groupe Administrateurs local.
Modifier les paramètres d'enregistrement du transport MSExchange	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Activer l'enregistrement dans un fichier journal au niveau du débogage pour le protocole SMTP	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Activation de l'enregistrement au niveau débogage du catégoriseur de messages	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.

Utilisation de Telnet

Telnet est un outil très utile pour résoudre les problèmes relatifs au protocole SMTP et au flux des messages. Par exemple, vous pouvez utiliser telnet pour :

- vous assurer que le protocole SMTP est correctement installé et qu'il dispose de toutes les commandes nécessaires ;
- vous assurer que votre serveur est accessible via Internet ;
- tenter une remise du courrier directement par le port TCP ;
- déterminer si tous les serveurs acceptent les connexions ;
- déterminer si un pare-feu bloque une connexion ;

- vous assurer qu'un utilisateur spécifique peut recevoir du courrier ;
- vous assurer qu'un domaine spécifique peut recevoir du courrier ;
- vous assurer qu'un utilisateur ou un domaine spécifique peut envoyer du courrier vers votre domaine.

Pour utiliser telnet afin de tester la communication SMTP

Remarque La procédure suivante vous indique comment tester l'envoi de courrier par un utilisateur interne vers un utilisateur distant lorsque l'authentification de base est nécessaire pour relayer du courrier hors de votre organisation.

1. Ouvrez une session telnet : à partir de l'invite de commandes, tapez **telnet**, puis appuyez sur ENTRÉE.
2. Tapez **set local_echo** sur un ordinateur qui exécute Microsoft Windows® 2000 Server ou tapez SET LOCALECHO sur un ordinateur qui exécute Windows Server™ 2003 ou Windows XP, puis appuyez sur ENTRÉE. Cette commande vous permet d'afficher les réponses aux commandes.

   Remarque Pour obtenir une liste des commandes telnet disponibles, tapez **set ?**.
3. Tapez **o <*domaine de votre serveur de messagerie*> 25**, puis appuyez sur ENTRÉE.
4. Tapez **EHLO <*domaine de votre serveur de messagerie*>**, puis appuyez sur ENTRÉE.
5. Tapez **AUTH LOGIN**. Le serveur répond en vous invitant à entrer votre nom d'utilisateur de manière cryptée.
6. Entrez votre nom d'utilisateur crypté en base 64. Vous pouvez utiliser l'un des nombreux outils disponibles pour coder votre nom d'utilisateur.
7. Le serveur répond en vous invitant à entrer votre mot de passe crypté en base 64. Entrez votre mot de passe crypté en base 64.
8. Tapez **MAIL FROM:<*expéditeur@domaine.com*>**, puis appuyez sur ENTRÉE. Si l'expéditeur n'est pas autorisé à envoyer du courrier, le serveur SMTP retourne une erreur.
9. Tapez **RCPT TO:<*destinataire@domainedistant.com*>**, puis appuyez sur ENTRÉE. Si le destinataire n'est pas valide ou si le serveur n'accepte pas de courrier provenant de ce domaine, le serveur SMTP retourne une erreur.
10. Tapez **DATA**.
11. Si vous le souhaitez, tapez le texte du message, appuyez sur ENTRÉE, tapez un point (**.**), puis appuyez à nouveau sur ENTRÉE.
12. Si la fonctionnalité du courrier fonctionne correctement, une réponse similaire aux informations ci-dessous s'affiche en indiquant que le courrier est placé en file d'attente de remise :

    ```
    250 2.6.0 <INET-IMC-01UWr81nn9000fbad8@mail1.contoso.com> Queued mail for delivery
    ```

L'exemple suivant montre un test telnet qui consiste à envoyer du courrier depuis le domaine contoso.com vers un domaine distant (l'entrée de l'utilisateur s'affiche en gras) :

```
ehlo fourthcoffee.com
250-mail1.fourthcoffee.com Hello [172.16.0.0]
250-TURN
250-ATRN
250-SIZE 5242880
250-ETRN
250-PIPELINING
250-DSN
```

```
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFY
250-X-EXPS GSSAPI NTLM
250-AUTH GSSAPI NTLM
250-X-LINK2STATE
250-XEXCH50
250 OK
auth login
334 VXNlcm5hbWU6
c2ZpbmVz
334 UGFzc3dvcmQ6
cGFzc3dvcmQ=
235 2.7.0 Authentication successful.
mail from:kim@fourthcoffee.com
250 2.1.0 kim@fourthcoffee.com....Sender OK
rcpt to:ted@contoso.com
250 2.1.5 ted@contoso.com
data
354 Start mail input; end with <CRLF>.<CRLF>
This is a test mail sent on SMTP port 25 to verify test my SMTP server
.
250 2.6.0 <INET-IMC-01UWr81nn9000fbad8@mail1.fourthcoffee.com> Queued mail for
delivery
```

Utilisation des files d'attente SMTP et X.400

Le protocole SMTP utilise les files d'attente SMTP pour remettre du courrier de manière interne et externe. Les serveurs Exchange Server 5.5, les clients MAPI (par exemple Microsoft Office Outlook®) et d'autres connecteurs Messagerie Internet (par exemple Microsoft Exchange - Connecteur pour Lotus Notes et Microsoft Exchange - Connecteur pour Novell GroupWise) utilisent des files d'attente X.400 pour envoyer et recevoir du courrier via Exchange. Les sections suivantes décrivent l'utilisation des files d'attente SMTP et X.400 pour résoudre les problèmes liés au flux des messages.

Description des files d'attente SMTP

Lors de la catégorisation et de la remise des messages, le moteur de files d'attente avancé envoie tous les messages via les files d'attente SMTP d'un serveur virtuel SMTP. Si un problème survient lors de la remise du message à n'importe quel stade du processus, le message reste dans la file d'attente concernée.

Les files d'attente SMTP permettent d'identifier les causes possibles des problèmes associés au flux des messages. Si une file d'attente comporte l'état « Réessayer », vérifiez ses propriétés afin de déterminer l'origine

du problème. Par exemple, si les propriétés de la file d'attente affichent un message du type « Une erreur SMTP s'est produite », consultez les journaux des événements de votre serveur afin d'identifier les erreurs SMTP éventuelles. Si le journal ne contient pas d'événements, augmentez le niveau d'enregistrement du protocole SMTP. Pour plus d'informations sur l'augmentation du niveau d'enregistrement du protocole SMTP, consultez « Utilisation de l'Observateur d'événements » et « Configuration de l'enregistrement des diagnostics pour le protocole SMTP » plus loin dans ce chapitre.

Le tableau 12.2 répertorie les files d'attente SMTP, leur description et les modalités de résolution des problèmes d'accumulation des messages dans chaque file d'attente.

Tableau 12.2 Descriptions des files d'attente SMTP et modalités de résolution des problèmes associés

File d'attente SMTP	Description	Résolution des problèmes
[nom de domaine local] (Remise locale)	Contient les messages placés en file d'attente sur le serveur Exchange en vue de leur remise locale dans une boîte aux lettres Exchange ou une banque de dossiers publics.	Les messages peuvent s'accumuler dans cette file d'attente si le serveur Exchange n'accepte pas la remise locale des messages. Une remise lente ou sporadique des messages peut signaler une boucle au niveau des messages ou un problème de performance. Cette file d'attente est affectée par la banque d'informations d'Exchange. Augmentez le niveau d'enregistrement des diagnostics pour la banque d'informations Exchange, selon les instructions fournies dans la section « Configuration de l'enregistrement des diagnostics pour le protocole SMTP », plus loin dans ce chapitre.
Messages en attente d'une recherche dans l'annuaire	Contient les messages adressés aux destinataires dont les noms ne sont pas encore résolus au niveau du service d'annuaire Microsoft Active Directory®. Les messages figurent également ici lors de l'extension des listes de distribution.	En général, les messages s'accumulent dans cette file d'attente lorsque le moteur de files d'attente avancé ne peut pas catégoriser le message. Le moteur de files d'attente avancé ne parvient peut-être pas à accéder aux serveurs de catalogue global ni à accéder aux informations relatives aux destinataires, ou les serveurs de catalogue global sont inaccessibles ou fonctionnent lentement. D'autres raisons peuvent également entraîner l'accumulation des messages : • Active Directory n'est pas accessible (en effet, le

File d'attente SMTP	Description	Résolution des problèmes
		catégoriseur utilise Active Directory pour classifier les messages). • Active Directory est peut-être chargé de manière excessive (si de nombreux messages sont placés dans une file d'attente préalable à la catégorisation). • Un problème de conversion se produit. Le catégoriseur gère également la conversion de contenu. • Le catégoriseur de message ne parvient pas à trouver les banques de boîtes aux lettres. • Si le protocole SMTP a été réinstallé ou supprimé, les clés suivantes de la métabase IIS risquent de ne plus être valides : /smtpsvc/DsUseCat et /smtpsvc/vsi#/DsUseCat. Déterminez si le protocole SMTP a été réinstallé ou supprimé. Le catégoriseur affecte cette file d'attente. Augmentez le niveau d'enregistrement des diagnostics pour le catégoriseur, selon les instructions fournies dans la section « Configuration de l'enregistrement des diagnostics pour le protocole SMTP », plus loin dans ce chapitre.
Messages en attente de routage	Conserve les messages tant que le serveur de destination suivant n'est pas déterminé, puis déplace les messages vers leurs files d'attente de liaison respectives.	Les messages s'accumulent dans cette file d'attente si des problèmes existent au niveau du routage Exchange. Le routage des messages peut être sauvegardé. Augmentez le niveau d'enregistrement des diagnostics pour le routage,

File d'attente SMTP	Description	Résolution des problèmes
		selon les instructions fournies dans la section « Configuration de l'enregistrement des diagnostics pour le protocole SMTP », plus loin dans ce chapitre.
Remise distante [*Nom de connecteur*| *Nom de serveur*| *Domaine distant*]	Contient les messages destinés à une remise distante. Le nom de la file d'attente correspond à celui de la destination de remise distante qui peut être un connecteur, un serveur ou un domaine.	Si les messages s'accumulent dans cette file d'attente, vous devez d'abord identifier l'état de cette dernière. Si l'état « Réessayer » est défini pour la file d'attente, vérifiez les propriétés de cette dernière afin de connaître les raisons pour lesquelles cet état a été appliqué. Pour résoudre les problèmes DNS, utilisez Nslookup et Telnet. Si l'hôte est inaccessible, utilisez Telnet pour vérifier si le serveur distant répond.
Destination finale inaccessible actuellement	Le serveur de destination finale des messages n'est pas accessible. Par exemple, Exchange ne peut pas déterminer le chemin d'accès réseau à la destination finale.	Les messages peuvent s'accumuler dans cette file d'attente s'il n'existe aucun itinéraire pour la remise. Par ailleurs, chaque fois qu'un connecteur ou une file d'attente de remise distante n'est pas disponible ou est à l'état « Réessayer » pendant un certain temps, et qu'aucun autre chemin de routage n'existe vers le connecteur ou la destination distante, les nouveaux messages sont placés dans cette file d'attente. Cela permet à un administrateur de corriger le problème ou de définir un itinéraire secondaire. Si vous souhaitez que les nouveaux messages circulent vers leur file d'attente de destination distante pour vous permettre de forcer une connexion et d'obtenir une trace du Moniteur réseau (NetMon), redémarrez le serveur virtuel SMTP.

File d'attente SMTP	Description	Résolution des problèmes
Dépôt préalable	Contient les messages qui ont été reçus et acceptés par le service SMTP. Le traitement de ces messages n'a pas commencé.	Les messages qui s'accumulent constamment peuvent indiquer un problème de performance. Les messages peuvent apparaître dans cette file d'attente par intermittence lors de l'exploitation maximale occasionnelle des performances.
Dépôt de messages DSN suspendu	Contient les notifications d'état de remise, connues également sous le nom de rapports de non-remise, qui sont prêtes à être remises par Exchange. **Remarque** Les opérations suivantes ne sont pas disponibles pour cette file d'attente : • Supprimer tous les messages (pas de rapport de non-remise) • Supprimer tous les messages (rapport de non-remise)	Des messages peuvent s'accumuler dans cette file d'attente, si le service de banque d'informations Microsoft Exchange n'est pas disponible ou en cours d'exécution, ou si des problèmes liés au composant de banque Exchange IMAIL se sont produits. Ce composant est celui qui effectue la conversion des messages. Recherchez dans le journal des événements des erreurs éventuelles liées au service de banque d'informations Microsoft Exchange.
File de nouvel essai des messages qui ont échoué	Contient les messages qui n'ont pas pu être placés en file d'attente de dépôt, avant tout autre traitement bien souvent. Par défaut, les messages de cette file d'attente sont retraités dans les 60 minutes.	Les raisons possibles de l'échec des messages sont les suivantes : • Les messages sont endommagés. • Des récepteurs d'événements ou programmes tiers interfèrent peut-être avec la file d'attente ou le traitement des messages. • Une insuffisance des ressources système peut entraîner une certaine lenteur de réponse du système ou d'autres problèmes de performances. Le redémarrage des services Internet (IIS) peut améliorer temporairement

File d'attente SMTP	Description	Résolution des problèmes
		les problèmes de ressources. Toutefois, il vous appartient d'en déterminer la cause principale.
Messages en file d'attente pour une remise différée	Contient les messages qui sont mis en file d'attente pour être remis ultérieurement, y compris les messages qui ont été envoyés par des versions antérieures de Microsoft Outlook. (Vous pouvez définir cette option sur les ordinateurs clients Outlook). Les versions antérieures d'Outlook dépendent de l'Agent de transfert des messages (MTA) pour la remise des messages. Désormais, cependant, le protocole SMTP gère la remise des messages à la place de l'Agent de transfert des messages. Ainsi, les messages envoyés par des versions antérieures d'Outlook traitent différemment la remise différée. Ces messages restent dans cette file d'attente jusqu'au moment prévu pour leur remise.	Les raisons possibles de l'accumulation de messages sont les suivantes : • Si un message est envoyé vers la boîte aux lettres d'un utilisateur lorsque la boîte aux lettres est déplacée, le message peut être placé dans cette file d'attente. • L'utilisateur ne possède pas encore de boîte aux lettres et ne dispose d'aucun identificateur de sécurité (SID) de compte principal. Pour plus d'informations, consultez l'article 316047 (en anglais) de la Base de connaissances Microsoft, « XADM: Addressing Problems That Are Created When You Enable ADC-Generated Accounts » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=316047). • Le message est peut-être endommagé ou le destinataire non valide. • Pour déterminer si un message est endommagé, vérifiez ses propriétés. Si un message n'est pas accessible, il est peut-être endommagé. Vous pouvez aussi vous assurer que le destinataire est valide.

Affichage des propriétés d'une file d'attente

Lorsque des messages s'accumulent dans une file d'attente, vous pouvez afficher les propriétés de cette dernière afin d'obtenir des informations complémentaires sur les causes possibles de l'accumulation.

Pour afficher les propriétés d'une file d'attente

1. Démarrez le Gestionnaire système Exchange : Cliquez sur **Démarrer**, pointez sur **Tous les programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Développez **Groupes administratifs**, développez <***Nom du groupe administratif***>, développez **Serveurs**, développez le serveur souhaité, puis cliquez sur **Files d'attente**.
3. Dans le volet d'informations, cliquez sur la file d'attente de votre choix. Des informations supplémentaires sur cette file d'attente apparaissent sous **Autres informations sur la file d'attente**, au bas du volet d'informations.

Affichage des messages dans une file d'attente

Si vous rencontrez des problèmes au niveau du flux des messages, il convient de déterminer s'il s'agit de problèmes globaux ou de problèmes liés à des destinataires individuels ou des domaines. L'affichage des messages dans une file d'attente peut vous aider à le déterminer.

Pour afficher les messages d'une file d'attente

1. Dans le volet d'informations, cliquez avec le bouton droit sur la file d'attente à examiner, puis cliquez sur **Énumérer 100 messages** pour afficher les 100 premiers messages. Si des messages se trouvent en file d'attente, les 100 premiers d'entre eux s'affichent dans le volet d'informations.
2. Pour afficher les propriétés d'un message individuel, dans le volet d'informations, cliquez avec le bouton droit sur le message souhaité, puis cliquez sur **Propriétés**. La boîte de dialogue **Propriétés** du message affiche le nom de l'expéditeur, le nom du destinataire, la taille du message, ainsi que d'autres informations relatives à ce dernier.

Consultation des compteurs de performance

Si des messages s'accumulent dans la file d'attente préalable à la catégorisation (nommée « Messages en attente d'une recherche dans l'annuaire » dans l'Afficheur des files d'attente), consultez les compteurs de performance SMTP, en particulier les compteurs relatifs à la longueur des files d'attente du catégoriseur. Activez ces compteurs de performance en procédant comme suit :

Pour consulter les compteurs de performance SMTP

1. Ouvrez le Moniteur système : cliquez sur **Démarrer**, pointez sur **Exécuter**, puis tapez **perfmon**.
2. Dans le Moniteur système, cliquez avec le bouton droit sur le volet d'informations correspondant, puis cliquez sur Ajouter des compteurs.
3. Procédez de l'une des manières suivantes :
   - Pour analyser un ordinateur sur lequel s'exécute la console d'analyse, cliquez sur **Utiliser les compteurs locaux de l'ordinateur**.
   - Pour analyser un ordinateur spécifique, quel que soit l'emplacement où s'exécute la console d'analyse, cliquez sur **Choisir les compteurs sur**, puis spécifiez un nom d'ordinateur (le nom de l'ordinateur local est sélectionné par défaut).

4. Dans **Objet de performance**, cliquez sur **Serveur SMTP**.
5. Procédez de l'une des manières suivantes :
   - Pour analyser tous les compteurs, cliquez sur **Tous les compteurs**.
   - Pour analyser uniquement les compteurs sélectionnés, cliquez sur **Choisir les compteurs dans la liste**, puis sélectionnez les compteurs à analyser.
6. Cliquez sur **Ajouter**.
7. Examinez le compteur Cat. : longueur de la file d'attente du catégoriseur.

Le tableau 12.3 répertorie les compteurs de performance supplémentaires dont vous disposez pour analyser les problèmes de catégorisation.

Tableau 12.3 Compteurs de performance pour l'analyse des problèmes de catégorisation

Compteur de performance	Description
Cat. : recherches d'adresses abouties	Nombre de recherches d'adresses traitées et abouties.
Cat. : recherches d'adresses abouties/s	Nombre de recherches d'adresses traitées et abouties par seconde.
Cat. : recherches d'adresses	Nombre de recherches d'adresses individuelles dans le service Annuaire.
Cat. : recherches d'adresses non abouties	Nombre de recherches d'adresses qui n'ont trouvé aucun objet service Annuaire.
Cat. : recherches d'adresses/s	Nombre de recherches d'adresses distribuées au service Annuaire par seconde.
Cat. : catégorisations terminées	Nombre total de messages déposés auprès du catégoriseur et dont la catégorisation est terminée.
Cat. : catégorisations terminées avec succès	Nombre de catégorisations terminées sans erreur.
Cat. : catégorisations terminées/s	Nombre total de catégorisations terminées par seconde.
Cat. : catégorisations échouées (échec de connexion du service Annuaire)	Nombre de catégorisations échouées en raison d'un échec de connexion du service Annuaire.
Cat. : catégorisations échouées (échec d'ouverture de session du service Annuaire)	Nombre de catégorisations échouées en raison d'un échec d'ouverture de session du service Annuaire.
Cat. : catégorisations échouées (nouvelle tentative impossible)	Nombre de catégorisations échouées en raison d'une erreur machine (nouvelle tentative impossible).
Cat. : catégorisations échouées (mémoire insuffisante)	Nombre de catégorisations échouées en raison d'une insuffisance de mémoire disponible.
Cat. : catégorisations échouées (nouvelle tentative possible)	Nombre de catégorisations échouées (nouvelle tentative possible).
Cat. : catégorisations échouées (nouvelle tentative possible pour le récepteur)	Nombre de catégorisations échouées (nouvelle tentative générique possible).
Cat. : catégorisations en cours	Nombre de catégorisations en cours.
Cat. : échecs de liaisons LDAP	Nombre total d'échecs de liaisons LDAP (Lightweight Directory Access Protocol).

Compteur de performance	Description
Cat. : liaisons LDAP	Nombre total de liaisons LDAP correctement établies.
Cat. : échecs de connexion LDAP	Nombre total d'échecs de connexion aux serveurs LDAP.
Cat. : connexions LDAP	Nombre total de connexions LDAP ouvertes.
Cat. : connexions LDAP ouvertes actuellement	Nombre de connexions LDAP ouvertes actuellement.
Cat. : échecs génériques des recherches LDAP abouties	Nombre de recherches LDAP abouties avec un échec générique.
Cat. : recherches paginées LDAP abouties et incorrectes	Nombre de recherches paginées LDAP abouties et incorrectes.
Cat. : échecs de recherches paginées LDAP	Nombre d'échecs de distribution d'une recherche paginée LDAP asynchrone.
Cat. : recherches paginées LDAP	Nombre de recherches paginées LDAP correctement distribuées.
Cat. : recherches paginées LDAP abouties	Nombre de recherches paginées LDAP traitées et abouties.
Cat. : recherches LDAP abouties et incorrectes	Nombre de recherches LDAP abouties et incorrectes.
Cat. : échecs de recherches LDAP	Nombre d'échecs de distribution d'une recherche LDAP asynchrone.
Cat. : recherches LDAP	Nombre de recherches LDAP correctement distribuées.
Cat. : recherches LDAP abandonnées	Nombre de recherches LDAP abandonnées.
Cat. : recherches LDAP abouties	Nombre de recherches LDAP traitées et abouties.
Cat. : recherches LDAP abouties/s	Nombre de recherches LDAP traitées et abouties par seconde.
Cat. : recherches LDAP en cours d'aboutissement	Nombre de recherches LDAP en cours d'aboutissement asynchrone.
Cat. : recherches LDAP/s	Nombre de recherches LDAP correctement distribuées par seconde.
Cat. : collisions dues à mailmsg dupliqué	Nombre de détections d'une adresse de destinataire dupliquée par mailmsg ou le catégoriseur de message.
Cat. : messages abandonnés	Nombre de messages marqués pour abandon par le catégoriseur.
Cat. : messages bifurqués	Nombre de nouveaux messages créés par le catégoriseur (bifurcation).
Cat. : messages catégorisés	Nombre de messages déposés en file d'attente par le catégoriseur.
Cat. : messages soumis	Nombre total de messages déposés auprès du catégoriseur.

Compteur de performance	Description
Cat. : messages soumis/s	Taux auquel les messages sont déposés auprès du catégoriseur.
Cat. : destinataires après catégorisation	Nombre de destinataires de message déposés en file d'attente après catégorisation.
Cat. : destinataires avant catégorisation	Nombre de destinataires de message déposés auprès du catégoriseur.
Cat. : destinataires en cours de catégorisation	Nombre de destinataires que le catégoriseur de message traite actuellement.
Cat. : destinataires qui ont reçu un rapport de non remise (adresse ambiguë)	Nombre de destinataires dont l'adresse correspond à plusieurs objets service Annuaire.
Cat. : destinataires qui ont reçu un rapport de non remise (boucle de transfert)	Nombre de destinataires qui ont reçu un rapport de non remise du catégoriseur suite à la détection d'une boucle de transfert.
Cat. : destinataires qui ont reçu un rapport de non remise (adresse non conforme)	Nombre de destinataires dont l'adresse détectée par le catégoriseur n'est pas conforme.
Cat. : destinataires qui ont reçu un rapport de non remise (erreurs de destinataire pour le récepteur)	Nombre de destinataires qui ont reçu un rapport de non remise du catégoriseur à cause d'un destinataire générique incorrect.
Cat. : destinataires qui ont reçu un rapport de non remise (non résolus)	Nombre de destinataires non résolus (adresses locales introuvables).
Cat. : destinataires qui ont reçu un rapport de non remise du catégoriseur	Nombre de destinataires qui ont reçu un rapport de non remise du catégoriseur.
Cat. : expéditeurs non résolus	Nombre d'expéditeurs introuvables dans le service Annuaire.
Cat. : expéditeurs dont l'adresse est ambiguë	Nombre d'expéditeurs dont l'adresse correspond à plusieurs objets service Annuaire.
Longueur de la file d'attente du catégoriseur	Nombre de messages dans la file d'attente du catégoriseur.

Utilisation du Centre de suivi des messages

Pour enregistrer des informations relatives aux messages envoyés via votre système de messagerie, vous pouvez utiliser le Centre de suivi des messages dans Exchange. Le Centre de suivi des messages enregistre des informations sur l'expéditeur, le message électronique proprement dit et les destinataires. En particulier, vous pouvez consulter des statistiques telles que l'heure d'envoi ou de réception d'un message, la taille de ce dernier, sa priorité, ainsi que la liste de ses destinataires. Vous pouvez également enregistrer la ligne d'objet des messages électroniques. Le Centre de suivi des messages recherche tous les types de messages, notamment les messages système, les messages des dossiers publics et les messages électroniques.

Vous devez activer le Centre de suivi des messages sur chaque serveur où vous souhaitez effectuer le suivi des messages. Une fois l'activation effectuée, tous les messages routés par un serveur sont ajoutés aux journaux de suivi de messages.

Pour activer le Centre de suivi des messages sur un serveur

1. Dans le Gestionnaire système Exchange, développez **Serveurs**, cliquez avec le bouton droit sur le serveur sur lequel vous voulez activer le suivi des messages, puis cliquez sur **Propriétés**.
2. Sous l'onglet **Général**, activez la case à cocher **Activer le suivi des messages**.
3. Pour enregistrer l'objet d'un message envoyé, reçu ou transféré via le serveur, activez la case à cocher **Activer l'enregistrement et l'affichage de l'objet des messages**.

   Remarque L'activation de l'enregistrement de l'objet entraîne certaines dégradations des performances.
4. Sous **Maintenance des fichiers journaux**, vous pouvez empêcher la suppression des fichiers journaux ou modifier leur délai de garde. Par défaut, les journaux de suivi sont conservés pendant sept jours.

   Remarque Sur les serveurs qui traitent de grandes quantités de courrier, la taille des journaux de suivi augmente rapidement. Assurez-vous que vous disposez de suffisamment d'espace disque pour le stockage des fichiers journaux, ainsi que pour l'utilisation d'autres services ou applications.
5. Cliquez sur **OK** ou sur **Appliquer**. Vous n'avez pas besoin de redémarrer les services pour que la modification prenne effet.

Pour plus d'informations sur l'utilisation du Centre de suivi des messages, consultez l'article 262162 (en anglais) de la Base de connaissances Microsoft, « XADM: Using the Message Tracking Center to Track a Message » (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=262162).

Utilisation de l'Observateur d'événements

Dans l'Observateur d'événements, le journal Applications et le journal Système contiennent tous deux des erreurs, des avertissements et des événements d'information relatifs au fonctionnement d'Exchange, du service SMTP et d'autres applications. Pour vous aider à identifier la cause des problèmes liés au flux des messages, examinez attentivement les données contenues dans le journal Applications et le journal Système.

Affichage du journal Applications

Consultez les erreurs, avertissements et événements d'information du journal Applications en procédant comme suit :

Pour afficher le journal Applications dans l'Observateur d'événements

1. Cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Outils d'administration**, puis cliquez sur **Observateur d'événements**.
2. Dans l'arborescence de la console, cliquez sur **Journal d'application**.
3. Pour trier le journal par ordre alphabétique et trouver facilement l'entrée d'un service Exchange, cliquez dans le volet d'informations sur **Source**.
4. Double-cliquez sur une entrée du journal pour ouvrir la page de propriétés d'un événement.
5. Pour filtrer le journal de sorte qu'il affiche uniquement les entrées correspondant à un certain type d'événement Exchange, dans le menu **Affichage**, cliquez sur **Filtre**.
6. Dans **Propriétés du journal de l'application**, utilisez la liste **Nom de source d'événement** pour sélectionner une source d'événement Exchange. Par exemple :

- **MSExchangeTransport** Événements enregistrés lorsque le protocole SMTP est utilisé pour router les messages.
- **IMAP4Svc** Événements liés au service qui autorise les utilisateurs à accéder aux boîtes aux lettres et dossiers publics via le protocole IMAP4.
- **MSExchangeAL** Événements liés au service qui envoie des messages électroniques à partir de listes d'adresses.
- **MSExchangeIS** Événements liés au service qui autorise l'accès au service de banque d'informations Exchange.
- **MSExchangeMTA** Événements liés au service qui autorise les connecteurs X.400 à utiliser l'Agent de transfert des messages.
- **MSExchangeMU** Événements liés au service de mise à jour de métabase, un composant qui lit les informations contenues dans Active Directory et les transpose dans la métabase IIS locale.
- **MSExchangeSA** Événements enregistrés lorsque Microsoft Exchange utilise Active Directory pour stocker et partager des informations d'annuaire.
- **MSExchangeSRS** Événements enregistrés lorsque le service de réplication de sites (SRS) est utilisé pour répliquer des ordinateurs exécutant Exchange 2003 vers des ordinateurs exécutant Exchange 5.5.
- **POP3Svc** Événements enregistrés lorsque le protocole POP3 (Post Office Protocol version 3) est utilisé pour accéder au courrier électronique.

7. Dans la liste **Catégorie**, sélectionnez un ensemble spécifique d'événements ou, si vous souhaitez afficher tous les événements de la source d'événement considérée, laissez le paramètre par défaut **Toutes**.
8. Cliquez sur **OK**.

Affichage du journal Système

Consultez les erreurs, avertissements et événements d'information du journal Système pour le service SMTP en procédant comme suit :

Pour afficher le journal Système dans l'Observateur d'événements

1. Cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Outils d'administration**, puis cliquez sur **Observateur d'événements**.
2. Dans l'arborescence de la console, cliquez sur **Journal système**.
3. Pour trier le journal par ordre alphabétique et trouver facilement l'entrée d'un service Exchange, cliquez dans le volet d'informations sur **Source**.
4. Double-cliquez sur une entrée du journal pour ouvrir la page de propriétés d'un événement.
5. Pour filtrer le journal de sorte qu'il affiche uniquement les entrées correspondant à un certain type d'événement du service SMTP, dans le menu **Affichage**, cliquez sur **Filtre**.
6. Dans **Propriétés du journal système**, dans la liste **Source de l'événement**, sélectionnez **SMTPSVC**.
7. Dans la liste **Catégorie**, sélectionnez un ensemble spécifique d'événements ou, si vous souhaitez afficher tous les événements du service SMTP, laissez le paramètre par défaut **Toutes**.
8. Cliquez sur **OK**.

Configuration de l'enregistrement des diagnostics pour le protocole SMTP

Pour mieux identifier l'origine d'un problème de transport, vous pouvez afficher les événements relatifs au transport MSExchange. Si vous rencontrez des problèmes au niveau du flux des messages Exchange, augmentez immédiatement les niveaux d'enregistrement relatifs au transport MSExchange. Les niveaux d'enregistrement contrôlent la quantité de données qui peut être enregistrée dans le journal Applications. Plus il y a d'événements enregistrés, plus vous pouvez voir d'événements relatifs au transport dans le journal Applications ; par conséquent, vous avez de plus grandes chances de déterminer l'origine du problème de flux des messages. Le fichier journal SMTP se trouve dans le dossier Exchsrvr\ *Nom_serveur*.log.

Comme indiqué dans « Description des files d'attente SMTP » plus haut dans ce chapitre, les problèmes relatifs à des composants de routage et de transport spécifiques peuvent entraîner l'accumulation de messages dans une file d'attente. Si vous rencontrez des problèmes au niveau d'une file d'attente spécifique, augmentez les niveaux d'enregistrement du composant qui affecte la file d'attente.

Modification des paramètres d'enregistrement

La procédure suivante explique comment modifier l'enregistrement des diagnostics pour le transport MSExchange.

Pour modifier les paramètres d'enregistrement du transport MSExchange

1. cliquez sur **Démarrer**, pointez sur **Programmes**, sur **Microsoft Exchange**, puis cliquez sur **Gestionnaire système**.
2. Dans l'arborescence de la console, développez le nœud **Serveurs**, cliquez avec le bouton droit sur **<*Nom de serveur*>**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Enregistrement des diagnostics**.
4. Sous **Services**, cliquez sur **MSExchangeTransport**.
5. Sous **Catégories**, cliquez sur la catégorie dont vous souhaitez configurer le niveau d'enregistrement :
   - Sélectionnez **Moteur de routage/Service** pour résoudre les problèmes de routage. Augmentez le niveau d'enregistrement de ce composant si les messages s'accumulent dans la file d'attente SMTP **Messages en attente de routage**.
   - Sélectionnez **Catégoriseur** pour corriger les problèmes relatifs à la résolution des adresses dans Active Directory, à l'extension de la liste de distribution et aux autres catégoriseurs. Augmentez le niveau d'enregistrement de ce composant si les messages s'accumulent dans la file d'attente SMTP **Messages en attente d'une recherche dans l'annuaire**.
   - Sélectionnez **Gestionnaire de connexions** pour résoudre les problèmes de connectivité aux niveaux de l'accès à distance et d'un réseau privé virtuel par l'intermédiaire du Gestionnaire de connexions.
   - Sélectionnez **Moteur de files d'attente** pour résoudre les problèmes relatifs au moteur de files d'attente. Augmentez le niveau d'enregistrement de ce composant si vous rencontrez des problèmes de flux des messages alors que les messages ne s'accumulent dans aucune file d'attente.
   - Sélectionnez **Gestionnaire de stockage Exchange** pour résoudre les problèmes liés au Gestionnaire de stockage Exchange. Augmentez le niveau d'enregistrement de ce composant si les messages s'accumulent dans la file d'attente SMTP de remise locale ou dans les files d'attente X.400, ou bien si vous rencontrez des problèmes au niveau de la réception du courrier depuis les serveurs Exchange 5.*x* ou d'autres systèmes de messagerie.

- Sélectionnez **Protocole SMTP** pour résoudre les problèmes généraux relatifs au protocole SMTP. Augmentez le niveau d'enregistrement de ce composant si les messages s'accumulent dans la file d'attente SMTP **Remise distante**, afin de déterminer si les erreurs SMTP sont à l'origine du goulot d'étranglement.
- Sélectionnez **Gestionnaire de stockage NTFS** pour résoudre les problèmes liés au Gestionnaire de stockage NTFS. Augmentez le niveau d'enregistrement de cette catégorie si les messages s'accumulent dans le dossier de file d'attente de votre serveur virtuel SMTP et s'ils sont traités lentement, voire pas du tout.

6. Sous **Niveau d'enregistrement**, cliquez sur **Aucun**, **Minimum**, **Moyen** ou **Maximum**. Cliquez sur **Maximum** si vous souhaitez effectuer un dépannage.

   Attention Si vous augmentez les niveaux d'enregistrement des services Exchange, vous constaterez une dégradation au niveau des performances. Il est recommandé d'augmenter la taille du journal Applications de sorte qu'il contienne toutes les données générées. Si vous ne le faites pas, vous recevrez des rappels fréquents vous informant que le journal Applications est saturé.

Définition de l'enregistrement dans un fichier journal à un niveau de débogage

Si vous rencontrez des problèmes de flux des messages et si vous souhaitez visualiser tous les événements, vous pouvez modifier une clé de Registre afin de définir l'enregistrement au niveau le plus élevé (niveau 7 d'ingénierie de maintenance).

Avertissement Une modification incorrecte du Registre peut entraîner des problèmes graves dont la résolution peut impliquer la réinstallation du système d'exploitation. Les problèmes résultant d'une modification incorrecte du Registre peuvent même ne pas avoir de solution. Avant de modifier le Registre, sauvegardez toutes les données importantes.

Pour définir l'enregistrement dans un ficher journal au niveau du débogage pour le protocole SMTP

1. Démarrez l'Éditeur du Registre. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis tapez **regedit**.
2. Dans l'Éditeur du Registre, recherchez la clé de Registre ci-après, cliquez avec le bouton droit sur cette dernière, puis cliquez sur **Modifier** :

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
   MSExchangeTransport\Diagnostics\SMTP Protocol

3. Attribuez-lui la valeur **7**.

Pour activer l'enregistrement au niveau débogage du catégoriseur de messages

1. Démarrez l'Éditeur du Registre. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis tapez **regedit**.
2. Dans l'Éditeur du Registre, accédez à la valeur de clé de Registre suivante, cliquez dessus avec le bouton droit, puis cliquez sur **Modifier** :

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
   MSExchangeTransport\Diagnostics\Categorizer

3. Attribuez-lui la valeur **7**.

Résolution des problèmes de rapports de non-remise

Les rapports de non-remise constituent un type de notification d'état de remise. Ils sont générés chaque fois qu'un message ne peut pas être remis. Si un serveur détecte la raison de l'échec de la remise, il associe la raison à un code d'état et un message d'erreur correspondant est rédigé.

La liste ci-après indique les informations de base à prendre en considération pour résoudre les problèmes de rapports de non-remise dans Microsoft® Exchange Server 2003. Recueillez ces informations au début de la procédure :

- Quels sont les types de clients utilisés (par exemple, Microsoft Outlook® 2000, Outlook 2002 ou Microsoft Office Outlook 2003) ?
- Un ou plusieurs utilisateurs reçoivent-ils des rapports de non-remise lorsqu'ils envoient un message à un destinataire déterminé ou à tous les destinataires ?
- Les messages des autres utilisateurs parviennent-ils correctement au même destinataire sur le même serveur ?
- Le problème est-il rencontré par des utilisateurs sur un serveur déterminé ou par des utilisateurs sur plusieurs serveurs ?
- Ce problème se produit-il sur un site déterminé ou sur plusieurs sites ?
- Pouvez-vous reproduire ce problème sur demande ou apparaît-il de façon aléatoire ?
- Si les rapports de non-remise sont aléatoires, à quelle fréquence se produisent-ils ?
- Quel type de destinataire est touché par ce problème ? Où réside physiquement le destinataire ?
- Comment le destinataire a-t-il été entré dans le champ **À** du message (par exemple, a-t-il été sélectionné dans le carnet d'adresses global, sélectionné dans un carnet d'adresses personnel ou entré au clavier) ?

  Remarque La création d'un utilisateur test constitue toujours une aide utile pour la résolution des problèmes de rapports de non-remise. Pensez à tester les plages horaires au cours desquelles les rapports de non-remise sont apparus et à collecter des informations d'ordre général sur le problème. Prenez en considération les modifications de variables ayant une incidence sur le problème. Il est important que vous limitiez le plus possible le problème en posant des questions comparables à celles qui figurent dans la liste ci-dessus.

Procédures du chapitre 13

Le tableau 13.1 répertorie les procédures spécifiques qui sont détaillées dans ce chapitre ainsi que les autorisations requises pour les effectuer.

Tableau 13.1 Procédures du chapitre 13 et autorisations correspondantes

Procédure	Autorisations ou rôles requis
Activation de l'enregistrement au niveau débogage du catégoriseur de messages	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'administration.
Activation de regtrace	Membre du groupe Administrateurs local.

Procédure	Autorisations ou rôles requis
Détermination du serveur d'expansion pour un groupe de distribution	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau du groupe d'administration.
Correction des problèmes d'attributs manquants	Membre du groupe Administrateurs local.
Indication d'un serveur de catalogue global.	Membre du groupe Administrateurs local et membre d'un groupe auquel le rôle d'administrateur Exchange a été appliqué au niveau de l'organisation.

Outils de résolution des problèmes de rapports de non-remise

Les outils et les fichiers de diagnostic suivants sont mis à votre disposition pour faciliter la résolution des problèmes de base liés aux rapports de non-remise :

- **Exemplaire du rapport de non-remise.** Veillez à enregistrer le message du rapport.
- **Code de notification d'état de remise dans le rapport de non-remise.** Veillez à enregistrer ce code.
- **Journal des événements Applications**. Paramétrez au niveau 7 l'enregistrement du diagnostic du catégoriseur de messages.
- **Résultats de l'outil LDP.** Les résultats de l'outil LDP (ldp.exe) contribuent à la résolution des problèmes de rapports de non-remise. Cet outil permet d'effectuer des opérations LDAP (Lightweight Directory Access Protocol) dans le service d'annuaire Microsoft Active Directory®. L'outil LDP est intégré aux outils de support de Microsoft Windows® 2000 Server et Windows Server™ 2003.
- **Résultats LDIFDE.** Les résultats de la commande LDIFDE contribuent à la résolution des problèmes de rapports de non-remise. Cet outil de ligne de commande permet de créer, de modifier et de supprimer des objets Active Directory. Il est intégré à Windows 2000 Server et à Windows Server 2003. Pour plus d'informations sur LDIFDE, consultez la documentation en ligne de Windows.
- **Centre de suivi des messages.** Le centre de suivi des messages permet de suivre des messages dans les organisations Exchange 2003 ainsi que dans des déploiements mixtes d'Exchange Server version 5.5, d'Exchange 2000 et d'Exchange Server 2003. Pour plus d'informations sur le centre de suivi des messages, consultez la documentation en ligne d'Exchange Server 2003.
- **Sorties de la métabase.** Vous pouvez obtenir des sorties de la métabase en utilisant l'éditeur de la métabase pour parcourir et modifier les attributs dans la métabase des services Microsoft Internet Information Services (IIS). L'éditeur de la métabase est intégré au Kit de ressources de Microsoft Windows 2000 Server et de Microsoft Windows Server 2003.
- **Compteurs du Moniteur système.** Les compteurs du Moniteur système du catégoriseur de messages sont destinés à faciliter la résolution des problèmes de rapports de non-remise. Les compteurs de performance du catégoriseur de messages sont décrits plus loin dans ce chapitre.
- **Traçage du Moniteur réseau.** Le Moniteur réseau (Netmon.exe) permet de capturer l'ensemble du trafic du réseau local ou de sélectionner le sous-ensemble de trames à capturer. Il est également possible de configurer une capture capable de réagir aux événements sur le réseau. Le Moniteur réseau est intégré à Windows 2000 Server et à Windows Server 2003. Pour plus d'informations sur cet outil, consultez la documentation en ligne de Windows.
- **Outil regtrace** Pour plus d'informations sur cet outil, consultez l'article 238614 (en anglais) de la Base de connaissances Microsoft, « XCON: How to Set Up Regtrace for Exchange 2000 »

(http://support.microsoft.com/?id=238614). Bien que cet article ait été écrit pour Exchange 2000, les mêmes informations s'appliquent à Exchange 2003.

Stratégies et conseils de résolution des problèmes

Cette section comporte des stratégies et des conseils pour résoudre les problèmes de rapports de non-remise. La cause d'un rapport de non-remise peut être déterminée en exécutant la procédure suivante :

1. Utilisez le code de diagnostic pour identifier les causes possibles.
2. Développez l'enregistrement des événements de façon à consigner tous les événements.
3. Collectez les informations à l'aide de regtrace.

Étape 1 : Déterminer les causes possibles d'un rapport de non-remise

Le tableau 13.2 répertorie les principaux codes de diagnostic des rapports de non-remise, les conditions d'erreur correspondantes et les suggestions de résolution des erreurs.

Tableau 13.2 Codes de diagnostic des rapports de non-remise et conditions d'erreur correspondantes

Code de rapport de non-remise	Cause possible	Résolution des problèmes
4.2.2	Dans Exchange 2000, cette notification d'état de remise est générée quand la boîte aux lettres du destinataire dépasse sa capacité de stockage. Sous Windows 2000 et Microsoft Windows Server 2003, ce message est généré quand la capacité de stockage du répertoire de dépôt (répertoire dans lequel sont placés les messages à remettre) dépasse le quota de disque du serveur virtuel SMTP (Simple Mail Transfer Protocol). Le quota de disque du serveur virtuel SMTP correspond à 11 fois la taille maximale d'un message sur le serveur virtuel. En l'absence de taille maximale explicite, le quota de disque est de 22 Mo par défaut. Si l'espace disque est inférieur ou égal à la taille maximale de message ou s'il atteint 20 Mo et qu'aucune	Vérifiez la taille maximale de la boîte aux lettres et du quota de stockage de la file d'attente.

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	taille maximale de message n'est définie, Exchange part du principe que le message entrant va dépasser le quota de disque et émet le rapport de non-remise.	
4.3.1	Une erreur de mémoire insuffisante s'est produite. Un problème de ressource, comme une saturation du disque, peut être à l'origine de ce problème.	Vérifiez que votre serveur Exchange dispose d'une capacité de disque suffisante. Si possible, déplacez vos files d'attente de courrier sur une partition de disque NTFS.
4.3.2	Disponible dans Exchange 2000 Service Pack (SP) 1 et versions ultérieures. Ce rapport de non-remise est généré lorsqu'une file d'attente a été gelée.	Libérez la file d'attente.
4.4.1	L'hôte ne répond pas. Un état passager du réseau peut être à l'origine de cette erreur. Le serveur Exchange réessaye automatiquement d'établir la connexion et de remettre le message. Si la remise échoue après plusieurs tentatives, un rapport de non-remise avec un code d'erreur permanent est généré.	Suivez l'évolution du problème. Il s'agit d'un problème transitoire qui peut se régler de lui-même.
4.4.2	Une connexion a été interrompue entre les serveurs. Un état passager du réseau ou l'indisponibilité des serveurs peut être à l'origine de cette erreur. Le serveur tente de remettre le message pendant une période déterminée, puis génère des rapports d'état supplémentaires.	Suivez l'évolution du problème. Il s'agit d'un problème transitoire qui peut se régler de lui-même.
4.4.6	Le nombre maximal de sauts a été dépassé pour le message. Une situation de boucle entre les serveurs d'envoi et de réception de différentes organisations peut être à l'origine de cette erreur. Les	La propriété du nombre maximal de sauts est définie par serveur virtuel, mais vous pouvez redéfinir manuellement la valeur par défaut (**15**). Vous devez également rechercher les

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	serveurs se renvoient le message jusqu'à ce que le nombre maximal de sauts soit dépassé.	situations pouvant entraîner une boucle entre les serveurs.
4.4.7	Le message dans la file d'attente est arrivé à expiration. Le serveur d'envoi a tenté de relayer ou de remettre le message, mais l'action n'a pas pu être réalisée avant le délai d'expiration du message. Ce message peut également signifier que la limite d'un en-tête de message a été atteinte sur un serveur distant ou qu'un délai de protocole est arrivé à expiration pendant la communication avec le serveur distant.	Ce message indique généralement un problème lié au serveur de réception. Vérifiez la validité de l'adresse du destinataire et déterminez si le serveur de réception est configuré correctement pour recevoir les messages. Il peut s'avérer nécessaire de réduire le nombre de destinataires dans l'en-tête du message destiné à l'hôte à propos duquel vous recevez cette erreur. Si vous renvoyez ce message, il est placé de nouveau dans la file d'attente. Si le serveur de réception est disponible, le message est remis.
4.4.9	Correspond à une erreur temporaire de routage ou à une configuration de routage erronée. Causes possibles : • Premier scénario : Un connecteur SMTP a été configuré à l'aide de DNS (au lieu d'un hôte actif) et un espace d'adressage autre que SMTP (comme une adresse X.400) lui a été ajouté. • Deuxième scénario : Dans un groupe de routage créé par un utilisateur, un destinataire est supposé recevoir du courrier. Un connecteur de groupe de routage utilisant DNS a été employé pour relier le groupe de routage, puis ce groupe (de routage ou d'administration) a été supprimé. Par conséquent,	Le routage détecte ces situations et Exchange renvoie des notifications d'état de remise. • La solution du premier scénario consiste à configurer le connecteur SMTP pour qu'il utilise un hôte actif, au lieu de DNS, afin de résoudre l'espace d'adressage autre que SMTP. • La solution du second scénario consiste à placer tous les utilisateurs du groupe de routage ou d'administration supprimé dans un groupe valide.

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	tout courrier envoyé à ce groupe de routage a été encodé au format MSGWIA.X500 (d'encapsulation pour les adresses autres que SMTP) qui n'est pas pris en charge par DNS.	
5.0.0	**Remarque** Avant Exchange 2000 SP1, les codes suivants apparaissaient sous le code 5.0.0. : • 4.3.2 • 5.4.0 • 5.4.4 • 5.5.0 Échec du catégoriseur dont la cause peut être l'une de celles décrites ci-après : • Il n'existe pas d'itinéraire pour l'espace d'adressage donné. Par exemple, un connecteur SMTP est configuré, mais l'adresse ne correspond pas. • DNS a retourné un hôte faisant autorité qui est introuvable pour le domaine. • Le groupe de routage n'a pas de connecteur défini. Les messages provenant d'un serveur dans un groupe de routage n'ont pas d'itinéraire vers un autre groupe de routage. • Une erreur SMTP s'est produite.	Sur un ou plusieurs connecteurs SMTP, ajoutez la valeur astérisque (*****) en tant qu'espace d'adressage, vérifiez que DNS est opérationnel et que les groupes de routage sont reliés à des connecteurs.
5.1.0	Ce rapport de non-remise a pour origine une défaillance générale liée au catégoriseur (échec associé à une adresse erronée). Une adresse de messagerie ou un autre attribut	Soit l'adresse du destinataire n'est pas configurée correctement soit le catégoriseur n'a pas réussi à convertir correctement le destinataire. La première étape

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	est introuvable dans Active Directory. Des entrées de contact sans définition de l'attribut **targetAddress** peuvent être à l'origine de ce problème. Autre cause possible, le catégoriseur ne réussit pas à déterminer l'attribut **homeMDB** d'un utilisateur. L'attribut **homeMDB** correspond au serveur Exchange sur lequel réside la boîte aux lettres de l'utilisateur. Autre situation courante pouvant engendrer ce rapport de non-remise : vous avez utilisé Outlook pour enregistrer le message en tant que fichier, puis quelqu'un a ouvert le message hors ligne et y a répondu. Comme la propriété du message conserve uniquement l'attribut **legacyExchangeDN** quand Outlook remet le message, la recherche peut échouer.	pour résoudre cette erreur consiste à vérifier l'adresse du destinataire et à renvoyer le message.
5.1.1	Le compte de messagerie n'existe pas dans l'organisation où le message a été envoyé. Ceci peut se produire lorsque des utilisateurs sont transférés à l'intérieur d'un site. Si, par exemple, un utilisateur dont l'adresse Groupe_d'administration_1 devient Groupe_d'administration_2 répond à un ancien message ou ne recrée pas son profil Outlook, l'ancienne adresse LegacyDN du groupe d'administration sera utilisée et ce rapport de non-remise est généré. De la même façon, l'envoi de messages à des entrées obsolètes du carnet d'adresses personnel peut produire cette erreur.	Soit l'adresse du destinataire n'est pas configurée correctement soit le catégoriseur n'a pas réussi à convertir correctement le destinataire. La première étape pour résoudre cette erreur consiste à vérifier l'adresse du destinataire et à renvoyer le message.

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	Si, par ailleurs, vous avez configuré votre contact SMTP avec des caractères SMTP non valides (tels que décrits dans la RFC 821), le catégoriseur rejette la remise avec ce code de diagnostic.	
5.1.3	Ce rapport de non-remise provient d'une erreur de syntaxe dans l'adresse. Ainsi, un contact configuré dans Active Directory avec un attribut **targetAddress**, mais sans adresse, provoque cette erreur.	Soit l'adresse du destinataire n'est pas configurée correctement soit le catégoriseur n'a pas réussi à convertir correctement le destinataire. La première étape pour résoudre cette erreur consiste à vérifier l'adresse du destinataire et à renvoyer le message.
5.1.4	Un message est envoyé à une adresse (proxy) partagée par deux objets. Autre cause possible, le destinataire du message n'existe pas sur le serveur distant.	Vérifiez l'adresse du destinataire et renvoyez le message.
5.1.6	Une cause possible de ce rapport de non-remise est que les attributs de l'annuaire de l'utilisateur comme **homeMDB** (la banque de boîtes aux lettres associée de l'utilisateur) ou **msExchHomeServerName** (le serveur sur lequel réside la boîte aux lettres de l'utilisateur) sont absents ou endommagés.	Vérifiez l'intégrité de l'attribut de l'annuaire de l'utilisateur et réexécutez le service de mise à jour de destinataire pour garantir la validité des attributs requis pour le transport.
5.1.7	L'adresse SMTP de l'expéditeur, soit l'attribut **mail** dans le service d'annuaire, est mal configurée ou manquante. Le catégoriseur ne peut pas remettre le message sans attribut **mail** valide.	Vérifiez la structure de l'annuaire de l'expéditeur et si l'attribut **mail** existe.
5.2.1	Un message local est refusé, car il est trop volumineux. Cette erreur peut aussi	Vérifiez les autorisations d'accès ainsi que la taille du message. Vérifiez si le

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	provenir d'un identificateur de sécurité (SID) de compte principal manquant.	destinataire a un identificateur de sécurité dans Active Directory.
5.2.2	Ce rapport de non-remise est généré quand la boîte aux lettres du destinataire dépasse sa capacité de stockage.	Vérifiez la taille maximale de la boîte aux lettres ou le quota de stockage de la file d'attente.
5.2.3	Le message est trop volumineux et le quota local est dépassé. Par exemple, un utilisateur Exchange distant peut avoir une restriction quant à la taille maximale d'un message entrant.	Renvoyez le message sans les pièces jointes ou redéfinissez la limite côté client ou serveur de façon à autoriser les messages plus volumineux.
5.3.0	Exchange 2003 peut fonctionner sans l'Agent de transfert des messages (MTA). Si le courrier a été envoyé par erreur au MTA, Exchange retourne cette notification d'état de remise à l'expéditeur. Cette condition n'est appliquée que si vous avez désactivé le service MTA et utilisé des paramètres spécifiques du Registre pour désactiver le MTA/StoreDriver. Une configuration par défaut dirige les messages déroutés vers les files d'attente du MTA.	Vérifiez votre topologie de routage. Employez l'outil WinRoute pour garantir la réplication parfaite des itinéraires entre serveurs et groupes de routage.
5.3.3	Ce rapport de non-remise a pu être généré lorsque l'espace disque du serveur Exchange distant a atteint la limite imposée pour le stockage des messages. Cette erreur se produit généralement lorsque le serveur d'envoi envoie un message à l'aide d'une commande ESMTP BDAT. Cette erreur indique également la présence possible d'une erreur SMTP.	Vérifiez que le serveur distant dispose d'une capacité de stockage suffisante pour contenir les messages. Vérifiez le journal SMTP.
5.3.5	Une situation de boucle de courrier est détectée. Ceci signifie que le serveur est	Recherchez les boucles éventuelles dans la configuration des connecteurs

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	configuré pour se renvoyer le courrier. Si plusieurs serveurs virtuels SMTP sont configurés sur votre serveur Exchange, vérifiez qu'ils desservent des ports entrants uniques. Par ailleurs, pour éviter les boucles entre les serveurs virtuels SMTP locaux, assurez-vous que la configuration du port SMTP sortant est valide.	du serveur. S'il existe plusieurs serveurs virtuels, vérifiez qu'aucun n'a la valeur « Non assignée ».
5.4.0	Causes possibles : • Un hôte faisant autorité est introuvable dans DNS. • Une entrée hôte actif n'est pas correcte. • Un nom de domaine complet figure dans le fichier HOSTS (corrigé dans Windows 2000 SP3). • Une erreur DNS s'est produite ou vous avez configuré une adresse ID non valide en tant qu'hôte actif. • Le serveur virtuel SMTP n'a pas de nom de domaine complet ou de recherche de serveur virtuel SMTP valide. • Le domaine SMTP du contact n'est pas converti en espace d'adressage SMTP.	Employez l'outil de résolution DNS (Dnsdiag.exe) ou Nslookup pour vérifier la configuration DNS. Vérifiez que l'adresse IP a bien le format littéral IPv4. Vérifiez que l'entrée DNS correspondant au nom du serveur/de l'ordinateur concerné est valide. Si vous vous fondez sur un nom de domaine complet dans un fichier HOSTS, mettez à jour l'entrée dans le Gestionnaire système Exchange en entrant une adresse IP valide ou un nom correct.
5.4.4	Disponible dans Exchange 2000 SP1 et versions ultérieures. Ce rapport de non-remise est généré s'il n'existe aucun itinéraire pour la remise des messages ou si le catégoriseur n'a pas réussi à déterminer la destination du saut suivant.	Ajoutez ou configurez votre connecteur de groupe de routage entre les groupes de routage.

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	Vous avez défini une topologie de groupe de routage, mais il n'existe aucun connecteur de groupe de routage entre les groupes de routage.	
5.4.6	Une boucle avant a été détectée au niveau du catégoriseur. L'attribut **targetAddress** a pour valeur un utilisateur avec boîte aux lettres. Ce problème courant de configuration d'hébergement se produit lorsque quelqu'un crée un contact dans une unité d'organisation, puis emploie l'outil de configuration pour créer un utilisateur dans une autre unité d'organisation avec la même adresse de messagerie.	Cette situation se produit lorsque le *contact A* a un destinataire suppléant qui pointe vers le *contact B*, qui a lui un destinataire suppléant qui pointe de nouveau vers le *contact A*. Vérifiez le destinataire suppléant du contact. Vérifiez et supprimez l'attribut **targetAddress** des utilisateurs avec boîte aux lettres. Pour l'hébergement, c'est-à-dire l'envoi de messages provenant d'un utilisateur d'une société dans une unité d'organisation à un utilisateur d'une autre société dans une unité d'organisation distincte, vous devez configurer les deux objets associés suivants : Utilisateur : Proxy SMTP : utilisateur@contoso.com Contact : targetAddress: utilisateur@contoso.com; proxy SMTP : contact@fourthcoffee.com, où fourthcoffee.com est le nom de la deuxième société.
5.4.8	Disponible dans Exchange 2000 SP1 et versions ultérieures. Ce message signale une condition de boucle, qui peut se produire parce que l'une des stratégies de destinataire comprend un domaine local correspondant au nom de domaine complet d'un serveur Exchange de l'organisation. Lorsque le catégoriseur traite	Vérifiez vos stratégies de destinataire. Si une stratégie de destinataire contient un nom de domaine complet de serveur Exchange, vous devez retirer cette entrée. Votre stratégie de destinataire ne doit pas contenir le nom de domaine complet de votre serveur, mais uniquement le nom du domaine de messagerie (par exemple,

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	un message destiné à un domaine correspondant au nom de domaine complet d'un serveur Exchange, il retourne ce rapport de non-remise.	contoso.com au lieu de serveur1.contoso.com).
5.5.0	Une erreur générique de protocole ou une erreur SMTP est à l'origine de ce rapport de non-remise. Le serveur SMTP distant répond à un EHLO d'identification du serveur d'envoi par une erreur de niveau 500. Le système d'envoi interrompt ensuite la connexion et remet un rapport de non-remise indiquant que le serveur SMTP distant ne peut pas gérer le protocole. Si, par exemple, un compte de messagerie Microsoft Hotmail® n'est plus actif, une erreur SMTP 550 se produit.	Exécutez le journal SMTP ou une trace Netmon afin de découvrir la raison pour laquelle le serveur SMTP distant rejette la demande du protocole.
5.5.2	Une erreur SMTP générique se produit lorsque des commandes SMTP sont émises hors séquence. Par exemple, un serveur tente d'envoyer une commande AUTH (autorisation) avant de s'identifier à l'aide d'une commande EHLO. Cette erreur peut également se produire lorsque le disque système est saturé.	Exécutez le journal SMTP ou une trace Netmon, puis vérifiez que l'espace disque et la mémoire virtuelle sont suffisants pour permettre l'exécution de SMTP.
5.5.3	Ce rapport de non-remise peut être dû au fait que le message a trop de destinataires.	Le nombre maximal de destinataires est un paramètre configurable. La solution à ce problème consiste à augmenter ce plafond ou à découper le message en plusieurs messages de façon à respecter la limite du serveur. **Remarque** Le nombre maximal par défaut de destinataires d'un message SMTP est **5 000**. Pour modifier cette limite,

Code de rapport de non-remise	Cause possible	Résolution des problèmes
		démarrez le Gestionnaire système Exchange, développez **Paramètres globaux**, cliquez avec le bouton droit sur **Remise du message**, cliquez sur **Propriétés**, puis utilisez l'onglet **Paramètres par défaut**. Ce paramètre peut également varier en fonction de l'utilisateur dans Active Directory.
5.7.1	Causes possibles : • Accès général refusé et accès de l'expéditeur refusé : l'expéditeur du message ne dispose pas des autorisations requises pour mener à bien la remise. • Vous tentez de relayer votre courrier par le biais d'un autre serveur SMTP qui ne vous autorise pas à le faire. • Il est possible que des restrictions de remise soient associées au destinataire. Si, par exemple, une restriction de remise associée à un destinataire autorise la réception de messages provenant uniquement d'une liste de distribution, le courrier provenant de personnes qui n'en sont pas membres est rejeté et cette erreur se produit. • **Nouveauté d'Exchange 2003 :** Un utilisateur anonyme a tenté d'envoyer des messages électroniques à des destinataires ou des listes de distribution acceptant du courrier émanant uniquement	Vérifiez les privilèges et les attributs système du contact, et essayez de renvoyer le message. Par ailleurs, pour résoudre d'autres problèmes éventuels, vérifiez que vous exécutez Exchange 2000 SP1 ou versions ultérieures.

Code de rapport de non-remise	Cause possible	Résolution des problèmes
	d'une session SMTP authentifiée.	

Étape 2: Utiliser les journaux des événements

Si vous ne parvenez toujours pas à déterminer la raison pour laquelle votre message génère des rapports de non-remise, la prochaine étape consiste à étendre l'enregistrement des diagnostics dans le journal des événements. Ensuite, tentez de reproduire le rapport de non-remise, puis examinez le journal des événements Applications. Vous y trouverez peut-être des informations sur la raison pour laquelle le rapport de non-remise a été généré. Le catégoriseur Windows a limité l'enregistrement des événements, mais le catégoriseur Exchange effectue un enregistrement des événements étendu.

Pour identifier les origines des rapports de non-remise, vous devez paramétrer l'enregistrement des diagnostics du catégoriseur de messages au niveau 7 d'ingénierie de maintenance.

Pour activer l'enregistrement au niveau débogage du catégoriseur de messages

1. Démarrez l'Éditeur du Registre. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis tapez **regedit**.
2. Dans l'Éditeur du Registre, accédez à la valeur de clé de Registre suivante, cliquez dessus avec le bouton droit, puis cliquez sur **Modifier** :

   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeTransport\Diagnostics\Categorizer
3. Attribuez-lui la valeur **7**.

Lorsque vous activez l'enregistrement à ce niveau, le message descriptif d'événement suivant est généré dans l'Observateur d'événements pour les messages qui génèrent les rapports de non-remise :

```
Messageid=9000
Facility=Interface
Severity=Informational
SymbolicName=PHATCAT_NDR_REASON
The function of <function name> failed for reason <cause of failure> when
processing recipient <recipient name> of type <recipient type> A delivery status
notification has been generated
```

Étape 3: Utiliser Regtrace

Disponible sur les serveurs Exchange, Regtrace est un outil efficace pour le diagnostic et la résolution des problèmes de rapports de non-remise. Utilisez la procédure suivante pour activer regtrace.

Pour activer regtrace

1. À une invite de commandes, tapez **regtrace**. La fenêtre **Paramètres de traçage** s'ouvre.
2. Sous l'onglet **Traces**, activez toutes les cases à cocher.

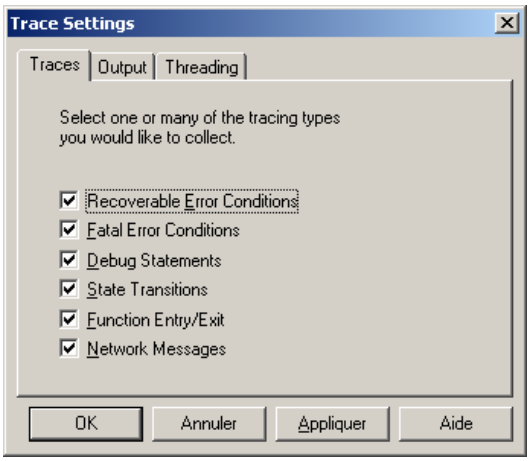


Figure 13.1 Onglet Traces des propriétés Paramètres de traçage

3. Sous l'onglet **Sortie**, vérifiez que l'option **Fichier** est sélectionnée, puis indiquez un chemin d'accès à un emplacement offrant une capacité suffisante pour stocker un fichier très volumineux en sortie.
4. Sous l'onglet **Threads**, vérifiez que l'option **Écrire les traces sur une thread en arrière-plan** n'est pas sélectionnée, puis cliquez sur OK.
5. Dans l'Éditeur du Registre, recherchez la clé de Registre suivante :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MosTrace\CurrentVersion\
   DebugAsyncTrace
   ```

6. Dans le menu **Edition**, cliquez sur **Ajouter une valeur**, puis ajoutez les valeurs de Registre suivantes :

   ```
   Value Name: Modules
   Data Type: REG_SZ
   Value: AQ
            CAT
            DS2MB
            dsevntwrap
            EXSINK
            IMAP4SVC
            REAPI
            RESVC
            Routing
            SMTP
            StoreDev
            TranMsg
            DSACCESS
   ```

7. Ensuite, ajoutez la valeur de la clé de Registre **MaxTraceFileSize** pour définir la taille maximale du fichier de suivi à 20 méga-octets (Mo). Dans le menu **Edition**, cliquez sur **Ajouter une valeur**, puis ajoutez les éléments suivants :

   ```
   Value Name:   MaxTraceFileSize
   Data Type:    REG_DWORD
   Value: 20 (decimal)
   ```

8. Quittez l'Éditeur du Registre.

9. Reproduisez le problème que vous tentez de résoudre. Si, par exemple, le courrier est retourné au motif qu'il n'a pas pu être remis, envoyez des messages à une adresse qui conduira Exchange à retourner le message non remis.
10. Lorsque vous avez reproduit le problème plusieurs fois, arrêtez le traçage. Dans Regtrace, cliquez sur l'onglet **Sortie**, puis sélectionnez **Pas de traçage**.

Fichier de suivi

Le fichier de suivi est disponible à l'emplacement indiqué sous l'onglet **Sortie** de Regtrace. L'emplacement par défaut du fichier est C:\Trace.atf.

Le fichier de suivi est un fichier codé binaire contenant des informations de niveau débogage à propos des composants de transport et de routage faisant l'objet du suivi. Pour cette raison, les Services de support technique de Microsoft demandent aux clients d'envoyer les fichiers de suivi à des fins d'analyse interne. Vous pouvez recourir à un logiciel de compression de fichier pour conditionner les fichiers à envoyer à ces Services par le biais d'un serveur FTP, de MSFE (Microsoft File Exchange) ou de Premier Service Desk. Pour plus d'informations sur l'un ou l'autre de ces modes de remise, consultez un représentant des Services de support technique.

Vérification des attributs Active Directory obligatoires

Lorsque vous résolvez un problème de rapport de non-remise, vérifiez que tous les attributs à extension messagerie requis par le catégoriseur de messages existent pour ce destinataire dans Active Directory. Dans Exchange 2000, plusieurs attributs doivent être corrects pour permettre la catégorisation des messages :

- **homeMDB**
- **homeMTA**
- **legacyExchangeDN**
- **mail**
- **mailNickname**
- **msExchHomeServerName**
- **msExchMailboxGuid**
- **msExchMailboxSecurityDescriptor**
- **proxyAddresses**

Cette liste d'attributs obligatoires n'est valide que si le destinataire est un objet avec boîte aux lettres dans Active Directory (par exemple, un destinataire Exchange 2003). Cependant, si le destinataire est un destinataire Exchange Server 5.5, les seuls attributs indispensables sont :

- **legacyExchangeDN**
- **homeMDB**
- **homeMTA**

Pour les objets à extension messagerie (par exemple, un destinataire personnalisé) et les adresses de remplacement, l'attribut **targetAddress** est obligatoire. En l'absence d'attribut **targetAddress**, la solution de repli est l'attribut **mail**.

Si un message ne présente pas l'un ou l'autre des attributs obligatoires ou s'ils ne sont pas corrects, le message peut rester dans le catégoriseur et aucun événement n'est créé dans l'Observateur d'événements. Si le message fait l'objet d'un suivi, il apparaît dans le catégoriseur de messages ou génère un rapport de non-remise en fonction de l'attribut manquant. Si vous souhaitez vérifier ces attributs pour un utilisateur dans Active Directory, utilisez l'outil LDP ou ADSI Edit. Pour plus d'informations sur l'outil LDP ou ADSI Edit, consultez la documentation en ligne de Windows.

> **Avertissement** Si vous utilisez le composant logiciel enfichable ADSI Edit, l'outil LDP ou tout autre client LDAP version 3, et que vous modifiez de façon incorrecte les attributs des objets Active Directory, des problèmes graves peuvent se produire. Ces problèmes peuvent exiger une réinstallation de l'un ou l'autre des éléments suivants : Windows 2000 Server, Windows Server 2003 ou Exchange Server 2003. Vous risquez de ne pas pouvoir résoudre les problèmes éventuels si vous modifiez de façon incorrecte des attributs d'objets Active Directory. Vous êtes responsable de la modification de ces attributs.

Le tableau 13.3 fournit quelques exemples d'attributs requis par Active Directory.

Tableau 13.3 Attributs Active Directory d'Exchange 2003 à extension messagerie

Attribut Exchange 2003 à extension messagerie	Exemple
homeMDB	CN=Banque de boîtes aux lettres (CONTOSO-MSG-01),CN=Premier groupe de stockage,CN=Banque d'informations,CN=CONTOSO-MSG-01,CN=Serveurs,CN=Premier groupe d'administration,CN=Groupes d'administration,CN=Première organisation,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=contoso,DC=com
homeMTA	CN=MTA Microsoft,CN=CONTOSO-MSG-01,CN=Serveurs,CN=Premier groupe d'administration,CN=Groupes d'administration,CN=Première organisation,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=contoso,DC=com
legacyDN	/o=Première organisation/ou=Premier groupe d'administration/cn=Destinataires/cn=pierre
mail	pierre@contoso.com
mailNickname	pierre
msExchHomeServerName	/o=Première organisation/ou=Premier groupe d'administration/cn=Configuration/cn=Serveurs/cn=CONTOSO-MSG-01
msExchMailboxGuid	0x06 0x4f 0x69 0xcc 0x5e 0xfe 0x79 0x4f 0x8c 0x6e 0x7b 0x67 0x57 0x92 0x51 0xd2
msExchMailboxSecurityDescriptor	Cet attribut est un blob binaire qui n'affiche pas de valeur dans ADSIEdit ni dans LDP.
proxyAddresses	SMTP: serge@contoso.com X400:c=us;a=;p=Première organisation=Exchange;s=Lopez;g=Pierre;

L'exemple suivant illustre un fichier de l'image mémoire provenant de l'outil LDP avec tous les attributs Active Directory d'Exchange 2003 à extension messagerie requis par le catégoriseur :

```
Expanding base 'CN=Ted Bremer,CN=Users,DC=contoso,DC=com'...
Result <0>: (null)
Matched DNs:
Getting 1 entries:
>> Dn: CN=Ted Bremer,CN=Users,DC=contoso,DC=com
1> homeMDB: CN=Mailbox Store (CONTOSO-MSG-01),CN=First Storage
Group,CN=InformationStore,CN=CONTOSO-MSG-01,CN=Servers,CN=First Administrative
Group,CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=contoso,DC=com;
1> memberOf: CN=Sales Team,CN=Users,DC=contoso,DC=com;
1> accountExpires: 9223372036854775807;
1> badPasswordTime: 0;
1> badPwdCount: 0;
1> codePage: 0;
1> cn: Ted Bremer;
1> countryCode: 0;
1> displayName: Ted Bremer;
1> mail: ted@contoso.com;
1> givenName: Ted;
1> instanceType: 4;
1> lastLogoff: 0;
1> lastLogon: 126416003544864704;
1> legacyExchangeDN: /o=First Organization/ou=First Administrative
Group/cn=Recipients/cn=ted;
1> logonCount: 19;
1> distinguishedName: CN=Ted Bremer,CN=Users,DC=contoso,DC=com;
1> objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=contoso,DC=com;
4> objectClass: top; person; organizationalPerson; user;
1> objectGUID: fdd08ce8-be92-4652-96db-f44785ef49e4;
1> objectSid: S-15-C2EF2A3A-4F67EE69-69068D04-64A;
1> primaryGroupID: 513;
2> proxyAddresses: SMTP:ted@contoso.com; X400:c=us;a= ;p=First
Organizati;o=Exchange;s=Bremer;g=Ted;;
1> pwdLastSet: 126415962391597356;
1> name: Ted Bremer;
1> sAMAccountName: ted;
1> sAMAccountType: 805306368;
2> showInAddressBook: CN=Default Global Address List,CN=All Global Address
Lists,CN=Address Lists Container,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=contoso,DC=com; CN=All Users,CN=All
Address Lists,CN=Address Lists Container,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=contoso,DC=com;
1> sn: Bremer;
1> textEncodedORAddress: c=us;a= ;p=First Organizati;o=Exchange;s=Bremer;g=Ted;;
1> userAccountControl: 512;
1> userPrincipalName: ted@contoso.com;
1> uSNChanged: 16820;
1> uSNCreated: 16814;
1> whenChanged: 8/6/2001 11:31:17 Pacific Standard Time Pacific Daylight Time;
1> whenCreated: 8/6/2001 11:30:38 Pacific Standard Time Pacific Daylight Time;
1> homeMTA: CN=Microsoft MTA,CN=CONTOSO-MSG-01,CN=Servers,CN=First Administrative
```

```
Group,CN=Administrative Groups,CN=First Organization,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=contoso,DC=com;
1> msExchMailboxGuid: <ldp: Binary blob>;
1> msExchMailboxSecurityDescriptor: <ldp: Binary blob>;
1> msExchALObjectVersion: 56;
1> msExchHomeServerName: /o=First Organization/ou=First Administrative
Group/cn=Configuration/cn=Servers/cn=CONTOSO-MSG-01;
1> mailNickname: ted;
1> mDBUseDefaults: TRUE;
1> msExchPoliciesIncluded: {E7B464D2-65EF-4B3E-8AF4-8EB84BA7088E},{26491CFC-9E50-
4857-861B-0CB8DF22B5D7};
1> msExchUserAccountControl: 0;
```

Mise à jour d'attributs par le service de mise à jour de destinataire

Le service de mise à jour de destinataire applique trois stratégies système pour les destinataires à extension messagerie, les utilisateurs avec boîtes aux lettres et l'appartenance aux groupes de distribution masquée, qui sont installées par défaut lors de l'installation d'Exchange 2003. Ces trois stratégies ont le même but : mettre à jour quelques attributs d'objets dans Active Directory dans certaines circonstances.

Lorsque des utilisateurs, des contacts ou des groupes de distribution sont créés à l'aide d'outils personnalisés, le service de mise à jour de destinataire tente de corriger les omissions éventuelles dans les cas où un outil ne crée pas tous les attributs nécessaires pour un objet. Si des attributs obligatoires d'un utilisateur, d'un contact ou d'un groupe de distribution manquent, des problèmes peuvent se produire.

Pour un destinataire à extension messagerie, un ensemble minimal d'attributs est requis pour que tous les composants Exchange puissent fonctionner correctement. Par exemple, une entrée à extension messagerie (un utilisateur, un contact, un groupe ou un dossier public) doit avoir au moins ces attributs : **mailNickname**, **legacyExchangeDN** et **displayName**. Sans l'attribut **mailNickname**, un objet n'est pas considéré comme ayant une extension messagerie. Dès lors qu'un objet a un attribut **mailNickname**, les deux autres attributs doivent être définis.

Stratégie de destinataire à extension messagerie

Si le service de mise à jour de destinataire identifie une entrée nouvelle ou modifiée et dotée de l'attribut **mailNickname** mais dépourvue de l'attribut **legacyExchangeDN** ou **displayName**, il tente de créer ces attributs.

L'attribut **displayName** est copié tel quel à partir de l'attribut **mailNickname**. L'attribut **legacyExchangeDN** est traité par un algorithme qui identifie l'organisation et le groupe d'administration de cette entrée, puis crée une valeur au format suivant :

```
/o=MyCompany/ou=MyAdminGroup/cn=Recipients/cn=MailNickname
```

Stratégie d'utilisateur avec boîte aux lettres

Pour un utilisateur avec boîte aux lettres, deux attributs doivent être présents. Le premier est l'attribut **mailNickname** et le deuxième est l'un des suivants :

- **msExchHomeServerName**
- **homeMDB**
- **homeMTA**

Si l'un de ces attributs est présent et que l'utilisateur a un attribut **mailNickname**, l'utilisateur est considéré comme étant un utilisateur avec boîte aux lettres.

Dans ce cas, le service de mise à jour de destinataire tente de compléter quelques-uns des attributs suivants s'ils sont absents :

- **msExchHomeServerName**
- **homeMDB**
- **homeMTA**
- **legacyExchangeDN**
- **displayName**
- **msExchMailboxGuid**

Ces attributs sont complétés dans l'ordre suivant :

1. Si absent, l'attribut **msExchHomeServerName** est créé en fonction de l'attribut présent : **homeMDB** ou **homeMTA**. S'il ne peut pas être créé, le processus s'arrête.
2. Une fois l'attribut **msExchHomeServerName** défini, les attributs **homeMDB** et **homeMTA** sont complétés si l'un d'eux est manquant. Si plusieurs banques de boîtes aux lettres ou Agents de transfert des messages (MTA) figurent sur votre serveur, le service de mise à jour de destinataire sélectionne le premier rencontré au cours d'une recherche Active Directory. Par conséquent, la sélection peut être considérée comme étant un choix aléatoire.
3. Pour créer les attributs **legacyExchangeDN** et **displayName**, le service de mise à jour de destinataire procède de la même façon que pour un destinataire à extension messagerie.
4. Enfin, si l'attribut **msExchMailboxGuid** est absent, le service de mise à jour de destinataire crée cet attribut en générant un identificateur globalement unique (GUID).

Stratégie d'appartenance aux groupes de distribution masquée

Pour la stratégie d'appartenance aux groupes de distribution masquée, le service de mise à jour de destinataire ne s'exécute pas uniquement lorsqu'une entrée est créée (comme un groupe de sécurité ou un groupe de distribution). Ce service s'exécute également lorsque vous modifiez l'état de l'attribut **hideDLMembership**.

Si l'attribut a la valeur TRUE, le service de mise à jour de destinataire ajoute une partie non canonique au descripteur de sécurité, qui empêche quiconque de voir l'attribut « membre » de cette entrée. Ceci s'applique à n'importe quel type de client qui parcourt l'annuaire à l'aide de MAPI ou de LDAP.

Si l'attribut a la valeur FALSE, le service de mise à jour de destinataire supprime le descripteur de sécurité non canonique, qui expose à nouveau l'attribut « membre ».

Pour plus d'informations sur l'appartenance aux groupes masquée, consultez l'article 253827 (en anglais) de la Base de connaissances Microsoft, « XADM: How Exchange Hides Group Membership in Active Directory » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=253827). Bien que cet article ait été écrit pour Exchange 2000, les principes s'appliquent également à Exchange 2003.

Scénarios courants de rapports de non-remise

Cette section décrit les scénarios courants pouvant entraîner la création de rapports de non-remise :

- Problèmes liés à Active Directory

- Remise de messages retardée en raison de problèmes liés au serveur de catalogue global
- Envoi de messages à des destinataires dans des carnets d'adresses personnels ou des listes de contacts
- Envoi de messages à un dossier public

Problèmes liés à Active Directory

Des problèmes avec Active Directory peuvent produire des rapports de non-remise. Les catégories suivantes de rapports de non-remise sont liées à des problèmes relatifs à Active Directory :

- Les destinataires ont été transférés dans Active Directory à l'aide du Connecteur Active Directory.
- Les destinataires ont été transférés dans Active Directory à l'aide de l'outil de déplacement de boîte aux lettres.
- Des attributs manquent.

Les destinataires ont été transférés dans Active Directory à l'aide du Connecteur Active Directory

Si les rapports de non-remise concernent certains de vos utilisateurs et que vous avez déplacé les destinataires à l'aide du Connecteur Active Directory, déterminez les points suivants :

- Le type de destinataire qui génère le rapport de non-remise (par exemple, une boîte aux lettres, un groupe de distribution ou un contact).
- Le mode de transfert du destinataire vers Active Directory. Si le destinataire a été répliqué dans Active Directory par le Connecteur Active Directory, utilisez l'outil ADCDump pour obtenir un fichier de l'image mémoire du Connecteur Active Directory, puis comparez les attributs existant dans les deux annuaires pour le destinataire en question. Le fichier de l'image mémoire du Connecteur Active Directory fait apparaître les attributs manquants entre l'objet Exchange 2003 et l'objet Exchange Server 5.5. Pour obtenir l'outil ADCDump, contactez les Services de support technique de Microsoft.

Si les utilisateurs ont été transférés à l'aide du Connecteur Active Directory, ils doivent exister dans Active Directory, au moins en tant qu'utilisateurs désactivés. La réplication d'utilisateurs dans Active Directory comme contacts (destinataires personnalisés), à partir de l'annuaire Exchange 5.5, génère des rapports de non-remise. Si les destinataires Exchange 5.5 et Microsoft Windows NT® Server version 4.0 ont été répliqués dans Active Directory en tant que contacts, Exchange 2003 n'envoie plus de messages aux destinataires Windows NT Server 4.0 qui sont présentés comme contacts dans Active Directory. Dans ce scénario, le rapport de non-remise suivant est retourné :

```
A configuration error in the e-mail system caused the message to bounce between
two servers or to be forwarded between two recipients. Contact your administrator.
<servername.contoso.com #5.4.6>
```

Pour plus d'informations, consultez l'article 272593 de la Base de connaissances Microsoft, « XCON : Le message génère un rapport de non-remise lorsqu'il est envoyé à un destinataire Windows NT Server 4.0 présenté comme un contact dans Active Directory » (http://support.microsoft.com/default.aspx?scid=kb;fr;272593). Bien que cet article ait été écrit pour Exchange 2000, les principes s'appliquent également à Exchange 2003.

Ce comportement ne se produit pas avec les contacts créés dans Exchange 2003. Il apparaît uniquement avec les utilisateurs Windows NT Server 4.0 répliqués dans Active Directory comme contacts par le biais du Connecteur Active Directory. L'envoi de messages aux contacts Exchange 2003 natifs s'effectue sans difficulté.

Remarque Si les utilisateurs désactivés ne sont pas affichés dans Active Directory et que vous recevez des messages d'erreur MSADC 8277, remplacez le serveur de réplication de l'accord de connexion par le serveur tête de pont dans le site ou le domaine Exchange 2003 vers lequel vous effectuez la réplication. Par ailleurs, pour une interopérabilité complète entre les serveurs Exchange 2003 et les ordinateurs Exchange 5.5, vérifiez que la définition de la réplication ADC est bidirectionnelle.

Les destinataires ont été transférés dans Active Directory à l'aide de l'outil de déplacement de boîte aux lettres

Vérifiez que tous les attributs à extension messagerie sont présents si un destinataire, un groupe de distribution ou un utilisateur existe en tant qu'objet Exchange 2003 natif ou s'il a été déplacé à partir d'Exchange 5.5 à l'aide de l'outil de déplacement de boîte aux lettres. Les étapes suivantes sont destinées à :

- identifier le serveur Exchange sur lequel l'expéditeur réside physiquement, déterminer si le destinataire est un groupe de distribution, rechercher le serveur d'expansion du groupe ;
- déterminer le serveur de catalogue global que le serveur Exchange de l'expéditeur ou le serveur d'expansion du groupe de distribution contacte pour la résolution des noms (pour des instructions détaillées, consultez la procédure décrite plus loin dans cette section) ;
- exécuter l'outil Nltest, disponible dans Windows 2000 et Windows Server 2003, afin de déterminer le serveur de catalogue global contacté par le serveur de l'expéditeur ou par le serveur d'expansion du groupe de distribution. Veillez à exécuter Nltest à partir du serveur Exchange de l'expéditeur ou du serveur d'expansion du groupe de distribution. Si l'expansion du groupe de distribution est configurée sur un serveur quelconque de l'organisation, exécutez Nltest à partir du serveur d'envoi.

Pour déterminer le serveur d'expansion d'un groupe de distribution

1. Dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur le groupe de distribution, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Exchange - Paramètres avancés**, puis regardez la valeur indiquée sous **Serveur d'expansion**.

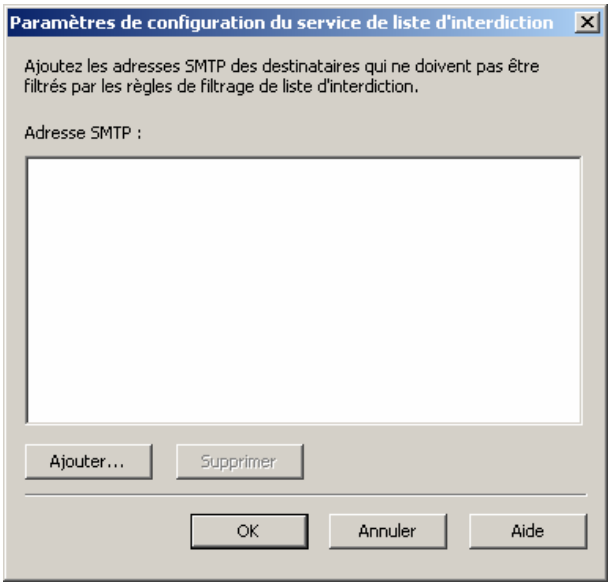


Figure 13.2 Onglet Exchange - Paramètres avancés de la boîte de dialogue Propriétés du groupe de distribution

3. À partir d'une invite de commandes, tapez ceci :

   ```
   NLTEST /DSGETDC:<domain> /GC
   ```

   où *domaine* est le nom de votre domaine

Maintenant que vous savez quel est le catalogue global utilisé, obtenez un fichier de l'image mémoire du groupe de distribution de l'utilisateur destinataire. Pour plus d'informations sur la façon d'obtenir un fichier de l'image mémoire, consultez les articles suivants (en anglais) de la Base de connaissances Microsoft :

- 255253, « XADM: How to Perform a Dump of a Container or Object in Exchange 2000 » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=255253)
- 271201, « XADM: Alternative Methods to Obtain a Dump of an Object » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=271201)

Vous pouvez également utiliser l'outil LDP pour obtenir le fichier de l'image mémoire LDP de l'objet destinataire. Si vous utilisez l'outil LDP, vérifiez que le port 3268 est utilisé lors de la connexion au serveur de catalogue global. Il s'agit du port utilisé par le catégoriseur de messages pour interroger les serveurs de catalogue global pour la résolution du nom.

Remarque Si l'outil LDP tronque les résultats, vous pouvez récupérer les informations du nom unique de base de l'objet (qui sont indispensables pour utiliser la procédure décrite dans l'article 271201, en anglais, de la Base de connaissances) à partir du rapport de non-remise. Chaque rapport contient les informations sur le nom unique de base de l'objet qui n'ont pas pu être remises. Si le format du rapport de non-remise ou si les informations sur le nom unique de base de l'objet sont douteuses, vous pouvez envoyer un nouveau message de test avec une demande d'accusé de réception. Envoyez le message de test au destinataire qui rencontre le problème avec un utilisateur qui n'a de son côté aucune difficulté à lui envoyer des messages.

Des attributs manquent

Pour diverses raisons pouvant aller d'une suppression manuelle jusqu'aux problèmes de synchronisation avec le catalogue global, des attributs peuvent s'avérer manquants pour un objet donné. Cependant, les attributs sont le plus souvent absents, car le service de mise à jour de destinataire ne les a pas correctement consignés ou parce que des problèmes sont survenus au niveau de la réplication ADC.

Pour corriger des problèmes d'attributs manquants

1. Dans le Gestionnaire système Exchange, développez **Destinataires**, puis **Services de mise à jour de destinataire.**
2. Cliquez avec le bouton droit sur le service de mise à jour de destinataire que vous souhaitez corriger, puis cliquez sur **Mettre à jour maintenant** pour mettre à jour les attributs manquants dans l'objet destinataire qui rencontre la difficulté, ou cliquez sur **Reconstruire** pour reconstruire tous les objets destinataires.

Remise de messages retardée en raison de problèmes liés au serveur de catalogue global

Des problèmes liés au catalogue global peuvent entraîner des retards dans la remise des messages. Dans ce cas, des rapports de non-remise sont générés pour signaler le retard à l'expéditeur. Le centre de suivi des messages permet de diagnostiquer ces problèmes. L'exemple suivant illustre des données collectées par le centre de suivi des messages :

```
6/22/2001  3:54 PM Tracked message history on server CONTOSO-MSG-01
6/22/2001  3:54 PM  SMTP Store Driver: Message Submitted from Store
```

```
6/22/2001  3:54 PM  SMTP: Message Submitted to Advanced Queuing
6/22/2001  3:54 PM  SMTP: Started Message Submission to Advanced Queue
6/22/2001  3:54 PM  SMTP: Message Submitted to Categorizer
6/22/2001  4:24 PM  SMTP: Started Outbound Transfer of Message
6/22/2001  4:24 PM   Message transferred out to FOURTHCOFFEE.COM through SMTP
6/22/2001  4:24 PM  SMTP: Message Submitted to Advanced Queuing
6/22/2001  4:24 PM  SMTP: Started Message Submission to Advanced Queue
6/22/2001  4:24 PM  SMTP: Message Submitted to Categorizer
6/22/2001  4:24 PM  SMTP: Started Outbound Transfer of Message
6/22/2001  4:24 PM  Message transferred out to FOURTHCOFFEE.COM through SMTP
6/22/2001  4:24 PM  SMTP Store Driver: Message Delivered Locally to Store
```

Dans cet exemple, vous noterez que le message a été retenu dans le catégoriseur de messages pendant 30 minutes avant le démarrage du transfert sortant, puis a finalement été remis. Dans de telles situations, déterminez le serveur de catalogue global utilisé par Exchange en exécutant l'outil Nltest comme indiqué dans la section « Les destinataires ont été transférés dans Active Directory à l'aide de l'outil de déplacement de boîte aux lettres », plus haut dans ce chapitre. Ensuite, analysez les serveurs de catalogue global impliqués. Voici les causes fréquentes de problèmes liés au catalogue global :

- Serveurs de catalogue global surchargés ou saturés.
- Problèmes de performance avec les serveurs de catalogue global.
- Mémoire insuffisante.
- Espace disque dur réduit.
- Problèmes de réseau temporaires entre Exchange 2000 et les serveurs de catalogue global.
- Un trop grand nombre de serveurs Exchange utilisant le même serveur de catalogue global (le nombre recommandé de processeurs Exchange par processeur de serveurs de catalogue global est de quatre pour un).

  Important Les journaux de suivi des messages peuvent induire en erreur. Par exemple, si le serveur de catalogue global fonctionne correctement et que le message est classé correctement, mais qu'un serveur SMTP distant n'était pas disponible pendant 30 minutes, le journal de suivi des messages se présentera comme notre exemple ci-dessus. Par ailleurs, si le message a dû être remis en local et qu'un ralentissement s'est produit au niveau de la banque d'informations Exchange, le journal de suivi des messages signale un long intervalle entre « Message soumis au catégoriseur de messages » et « Remise du message en local à la banque d'informations ».

Utilisez un journal du Moniteur système provenant d'un serveur de catalogue global lorsque vous tenterez de reproduire le problème. Ceci peut vous aider à diagnostiquer les problèmes. Le recyclage des serveurs de catalogue global peut faciliter leur résolution. Pour résoudre ces problèmes, vous pouvez indiquer un serveur de catalogue global pour chaque serveur Exchange.

Remarque La configuration manuelle de serveurs de catalogue global est uniquement recommandée pour résoudre des problèmes. Lorsque vos serveurs de catalogue global sont configurés manuellement, Exchange ne peut pas détecter si un serveur devient indisponible.

Pour indiquer un serveur de catalogue global

1. Dans le Gestionnaire système Exchange, développez **Serveurs**, cliquez avec le bouton droit sur le serveur Exchange, puis cliquez sur **Propriétés**.
2. Cliquez sur l'onglet **Accès à l'annuaire**.
3. Dans **Afficher**, sélectionnez **Serveurs de catalogue global**.

4. Désactivez la case à cocher **Détection automatique de serveurs**.

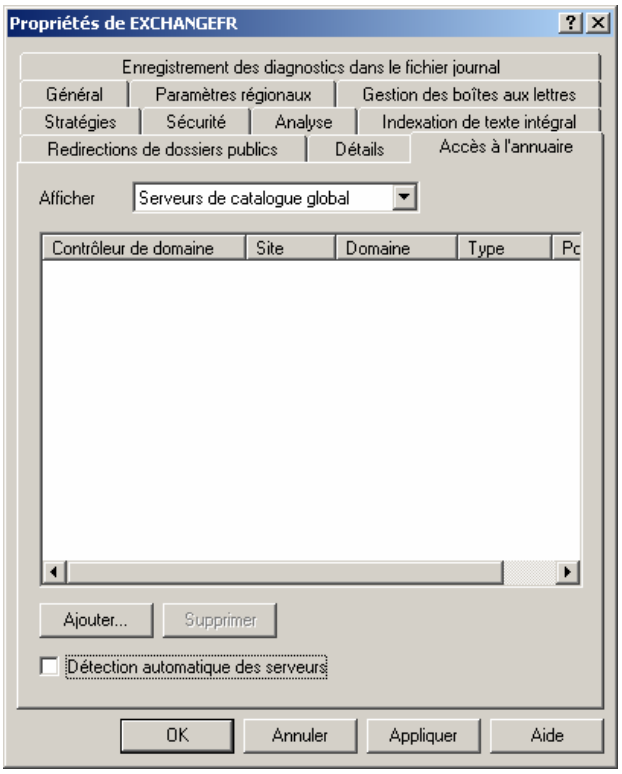


Figure 13.3 Onglet Accès à l'annuaire

5. Cliquez sur **Ajouter**, puis sélectionnez le serveur de catalogue global que vous souhaitez dépanner. Le catalogue global que vous sélectionnez pour le domaine doit exister dans Active Directory, être accessible par le biais du port LDAP 3268, traiter la demande du serveur Exchange en temps voulu et avoir tous les attributs à extension messagerie de l'objet destinataire.

Pour plus d'informations sur DSAccess, consultez l'article 250570 (en anglais) de la Base de connaissances Microsoft, « XCON: Directory Service Server Detection and DSAccess Usage » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=250570).

Rapports de non-remise liés à l'envoi vers un carnet d'adresses personnel et une liste de contacts

Si un utilisateur est déplacé d'un ordinateur Exchange Server 5.5 à l'aide de l'outil de déplacement de boîte aux lettres Exchange 2003 et que la boîte aux lettres déplacée a un carnet d'adresses personnel ou une liste de contacts dans la boîte aux lettres Exchange 5.5, le carnet d'adresses personnel et la liste de contacts deviennent non valides dans une boîte aux lettres Exchange 2003. Les adresses converties dans le carnet d'adresses personnel ou la liste de contacts génèrent un rapport de non-remise comparable au suivant :

```
Your message did not reach some or all of the intended recipients.
Objet : Test
Sent: 8/3/2000 5:24 PM
The following recipient(s) could not be reached:
```

```
CN=\ Network,OU=United States,OU=Distribution Lists,DC=Contoso,DC=com on 8/3/2000
5:24 PM

The e-mail address could not be found. Perhaps the recipient moved to a different
e-mail organization, or there was a mistake in the address. Check the address and
try again.

<CONTOSO-MSG-01.Contoso.com #5.1.0>
```

Comme l'outil de déplacement de boîte aux lettres ne déplace pas les carnets d'adresses personnels ni les listes de contacts, toutes les informations d'adressage dans ces carnets et ces listes deviennent non valides.

Pour résoudre ce problème, vérifiez sur votre client Outlook que la liste d'adresses globale est sélectionnée en tant que source du carnet d'adresses. Idéalement, les utilisateurs qui ont été déplacés à partir d'un serveur Exchange 5.5 doivent supprimer les carnets d'adresses personnels et listes de contacts, puis les recréer.

Envoi de messages à un dossier public

L'envoi d'un message à un dossier public dans Exchange est plus complexe que l'envoi d'un message à une boîte aux lettres. Une boîte aux lettres ne peut exister que sur un seul serveur et appartient par conséquent à une banque de boîtes aux lettres déterminée. Les attributs Active Directory d'une boîte aux lettres pointent vers un serveur spécifique. Par conséquent, une fois l'entrée résolue, Exchange peut utiliser le routage afin de déterminer la banque de boîtes aux lettres à laquelle remettre le message.

Un dossier public dans Active Directory n'a pas de serveur associé. Un dossier public peut exister sur plusieurs serveurs et aucune indication quant aux serveurs contenant des réplicas du dossier n'est conservée dans Active Directory. La banque d'informations Exchange traite ces informations.

Lorsqu'Exchange remet un message à un dossier public, la première tâche qu'il effectue est de remettre le message à une banque d'informations Exchange qui pointe vers l'emplacement des réplicas du dossier public. La banque d'informations Exchange consulte l'entrée ptagReplicaList, qui répertorie les serveurs Exchange avec les réplicas du dossier, puis resoumet le message réacheminé vers une banque d'informations Exchange contenant un réplica du dossier.

Le catégoriseur a pour tâche de résoudre correctement l'adresse d'un message. Dans le cas des dossiers publics, il assure également les fonctions suivantes :

- déterminer la hiérarchie de niveau supérieur à laquelle appartient le dossier ;
- adresser correctement le message à soumettre à une banque située dans cette hiérarchie ;
- une fois la liste des réplicas obtenue, réécrire l'adresse du message destinée à une banque contenant un réplica du dossier public.

Lorsqu'un message est envoyé à un dossier public, le catégoriseur effectue les étapes suivantes pour remettre le message :

1. Rechercher le dossier public initial
2. Rechercher le serveur dans la hiérarchie de niveau supérieur

Étape 1: Rechercher le dossier public initial

Lorsqu'un message électronique est soumis, Exchange convertit l'adresse en une entrée dans Active Directory. Si cette entrée est un dossier public, et non une boîte aux lettres, le catégoriseur tente d'obtenir l'attribut **homeMDB** du dossier public :

```
homeMDB: CN=Public Folders,CN=Folder Hierarchies,CN=First Administrative
Group,CN=Administrative Groups,CN=First
```

```
Organization,CN=MicrosoftExchange,CN=Services,CN=Configuration,DC=contoso-msg-
01,DC=contoso,DC=com;
```

L'attribut **homeMDB** du dossier contient le nom unique de la hiérarchie de niveau supérieur à laquelle appartient le dossier.

Étape 2 : Rechercher le serveur dans la hiérarchie de niveau supérieur

Le catégoriseur parcourt ensuite la hiérarchie de niveau supérieur indiquée par l'attribut **homeMDB** du dossier afin d'obtenir la liste de tous les serveurs contenus dans la hiérarchie de ce dossier. Il ne peut pas déterminer l'emplacement du réplica, mais peut déposer le message dans une banque d'informations Exchange qui possède les informations d'emplacement. Le nom unique de la hiérarchie de niveau supérieur contient une liaison vers tous les serveurs qui se trouvent dans cette hiérarchie.

Pour déterminer la banque ou le serveur de dossiers publics que le catégoriseur doit sélectionner dans la hiérarchie de niveau supérieur, Exchange utilise les critères suivants :

- L'une des banques de dossiers publics existe-t-elle sur le serveur local ? Si c'est le cas, Exchange utilise cette banque.
- L'une des banques de dossiers publics existe-t-elle sur un serveur Exchange dans le groupe de routage local ? Si c'est le cas, Exchange utilise cette banque.
- L'une des banques de dossiers publics existe-t-elle sur un serveur Exchange ? Si c'est le cas, Exchange utilise cette banque. Sinon, Exchange utilise la première banque dans la liste.

Le premier serveur sur la liste figure dans l'attribut **msExchOwningPFTreeBL**. Cet attribut est situé dans l'arborescence de dossiers publics, sous les hiérarchies de dossiers. Le catégoriseur choisit ensuite un serveur dans l'attribut **msExchOwningPFTreeBL** auquel il envoie le message.

L'exemple suivant indique le contenu de l'attribut **msExchOwningPFTreeBL**, tel qu'il a été obtenu à partir de la sortie LDP :

```
msExchOwningPFTreeBL: CN=Public Information Store (PFREP55),CN=First Storage
Group,CN=InformationStore,CN=PFREP55,CN=Servers,CN=FourthCoffee,CN=Administrative
Groups,CN=Lake District,CN=Microsoft Exchange,CN=Services,CN=Configuration,
DC=cumbria,DC=extest,DC=microsoft, DC=com;
CN=Public Folder Store (PFREP57),CN=First Storage Group,CN=InformationStore,
CN=PFREP57,CN=Servers,CN=Coniston,CN=Administrative Groups,CN=Lake
District,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=cumbria,DC=example,DC=microsoft,DC=com;
CN=Public Information Store (PFREP56),CN=First Storage
Group,CN=InformationStore,CN=PFREP56,CN=Servers,CN=Coniston,CN=Administrative
Groups,CN=Lake District,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=cumbria,DC=example,DC=microsoft,DC=com;
```

Référence supplémentaire de rapports de non-remise

Le tableau 13.4 décrit les codes de notification d'état de remise. Ce tableau peut vous aider à interpréter les codes reçus dans les rapports de non-remise.

Tableau 13.4 Codes de notification d'état de remise

Code de notification d'état de remise	Description
X.1.0	Autre état d'adresse
X.1.1	Mauvaise adresse de boîte aux lettres de destination
X.1.2	Mauvaise adresse de système de destination
X.1.3	Erreur de syntaxe dans l'adresse de la boîte aux lettres de destination
X.1.4	Adresse de boîte aux lettres de destination ambiguë
X.1.5	Adresse de boîte aux lettres de destination valide
X.1.6	Boîte aux lettres déplacée
X.1.7	Erreur de syntaxe dans l'adresse de la boîte aux lettres de l'expéditeur
X.1.8	Adresse du système de l'expéditeur erronée
X.2.0	Autre état ou état de boîte aux lettres non défini
X.2.1	Boîte aux lettres désactivée, n'accepte pas de messages
X.2.2	Boîte aux lettres saturée
X.2.3	Longueur de message supérieure à la limite administrative
X.2.4	Problème lié à l'expansion de la liste de distribution
X.3.0	Autre état ou état non défini du système de messagerie
X.3.1	Système de messagerie saturé
X.3.2	Messages réseau refusés par le système
X.3.3	Fonctionnalités sélectionnées non prises en charge par le système
X.3.4	Message trop volumineux pour le système
X.3.5	Mauvaise configuration du système
X.4.0	Autre état ou état non défini du réseau ou du routage
X.4.1	Pas de réponse de l'hôte
X.4.2	Mauvaise connexion
X.4.3	Défaillance du serveur de routage
X.4.4	Routage impossible
X.4.5	Congestion du réseau
X.4.6	Boucle de routage détectée
X.4.7	Délai de remise arrivé à expiration
X.5.0	Autre état ou état de protocole non défini
X.5.1	Commande non valide

Code de notification d'état de remise	Description
X.5.2	Erreur de syntaxe
X.5.3	Trop de destinataires
X.5.4	Arguments de commande non valides
X.5.5	Version de protocole erronée
X.6.0	Autre erreur ou erreur de support non définie
X.6.1	Support non pris en charge
X.6.2	Conversion obligatoire et interdite
X.6.3	Conversion requise mais non prise en charge
X.6.4	Conversion avec perte
X.6.5	Échec de la conversion
X.7.0	Autre état ou état de sécurité non défini
X.7.1	Remise non autorisée, message refusé
X.7.2	Expansion de la liste de distribution interdite
X.7.3	Conversion de sécurité obligatoire mais impossible
X.7.4	Fonctionnalités de sécurité non prises en charge
X.7.5	Échec de la cryptographie
X.7.6	Algorithme de cryptage non pris en charge
X.7.7	Défaillance de l'intégrité du message

Partie 5 Informations internes de transport

La partie 5 décrit les concepts avancés relatifs à l'architecture de transport sous-jacente de Microsoft® Exchange Server 2003 ainsi que les concepts utilisés en matière d'état des liaisons. Vous devez lire la partie 1 de ce guide et bien maîtriser les concepts présentés dans ce guide avant de lire la présente section. La partie 5 comprend les chapitres suivants :

Chapitre 14 « Présentation des composants de transport internes »
: Ce chapitre indique comment les composants de transport internes, comme le moteur de routage, le moteur de files d'attente avancé et le catégoriseur de messages, opèrent conjointement pendant la remise des messages.

Chapitre 15 « Concepts avancés sur l'état des liaisons »
: Ce chapitre examine les détails du paquet de l'état des liaisons et décrit des concepts avancés relatifs à l'état des liaisons.

Présentation des composants de transport internes

Ce chapitre décrit en détail les composants intervenant dans la réception et l'envoi de messages suivant le protocole SMTP (Simple Mail Transfer Protocol). Il indique également comment ces composants opèrent dans un processus courant de flux des messages. Voici les composants fondamentaux intervenant dans le transport de courrier :

Moteur de routage

Le moteur de routage Microsoft® Exchange, un des services Microsoft Exchange par défaut, se charge de déterminer le chemin le plus économique pour la remise des messages. Il fournit ces informations au moteur de files d'attente avancé dans le cadre du processus de remise de messages.

Moteur de files d'attente avancé

Le moteur de files d'attente avancé assure plusieurs aspects de la remise de messages. Plus particulièrement, il extrait les messages de SMTP ou du pilote de banque d'informations Microsoft Exchange, les classe, détermine la destination de chaque message, puis assure l'interface avec les files d'attente auxquelles un message peut être affecté en attendant d'être remis.

Catégoriseur de messages

Le catégoriseur de messages est un composant du moteur de files d'attente avancé, qui envoie les requêtes LDAP (Lightweight Directory Access Protocol) au serveur de catalogue global afin d'effectuer des recherches dans l'annuaire. Ces requêtes extraient les informations suivantes :

- les adresses de messagerie du destinataire ;
- la banque de boîtes aux lettres sur laquelle réside la boîte aux lettres du destinataire ;
- le serveur Exchange hébergeant cette banque de boîtes aux lettres.

La figure 14.1 illustre les composants de transport intervenant dans le flux des messages. Les parties ombrées représentent les composants de transport.

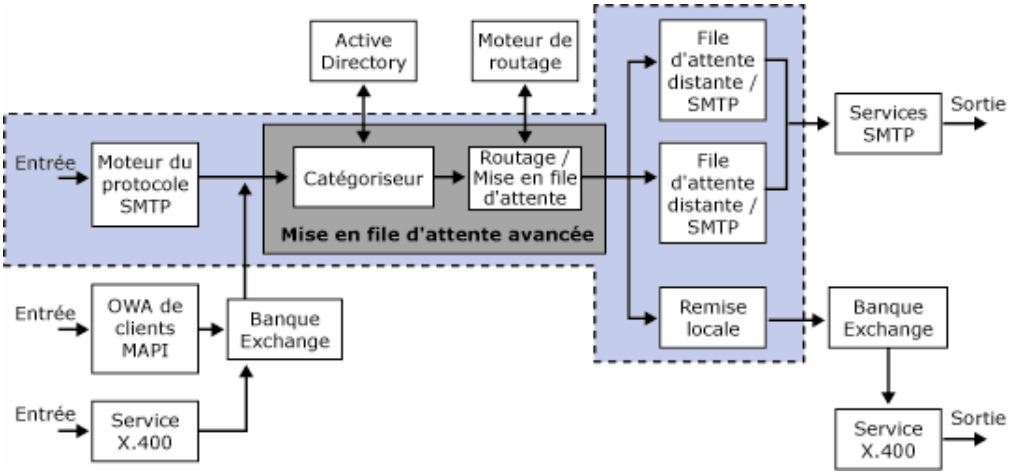


Figure 14.1 Flux des messages à l'intérieur des composants de transport internes

Réception de messages Internet

Exchange s'appuie sur DNS, le protocole SMTP, le catégoriseur de messages, le moteur de files d'attente avancé et le moteur de routage Exchange pour recevoir des messages Internet. Ces composants effectuent les tâches suivantes pour remettre des messages Internet à un utilisateur dans une organisation Exchange :

1. Le serveur SMTP d'envoi utilise DNS pour rechercher l'enregistrement MX (serveur de messagerie) préféré du domaine de destination ou du serveur cible. DNS retourne une liste d'enregistrements (hôtes) A, qui sont convertis en une ou plusieurs adresses IP (Internet Protocol) du serveur.
2. Le serveur SMTP d'envoi établit une connexion au port 25 du serveur SMTP de destination. Le serveur SMTP de destination est le serveur virtuel SMTP situé sur le serveur de passerelle physique configuré pour accepter les messages Internet entrants destinés au domaine auquel ils sont adressés.
3. Dans l'idéal, le serveur SMTP entrant accepte le message entrant uniquement s'il est destiné à un domaine de messagerie SMTP défini dans une stratégie de destinataire (sauf si le serveur autorise les relais, ce qui est fortement déconseillé).
4. Lorsque le message est accepté, le serveur virtuel SMTP crée une enveloppe pour le message (cette structure de message est appelée MAILMSG). MAILMSG contient toutes les propriétés du message, y compris les noms de l'expéditeur et du destinataire.
5. Le *catégoriseur de messages* effectue une requête LDAP dans le serveur de catalogue global pour trouver l'attribut **homeMdb** du destinataire. Le catégoriseur de messages affecte ensuite le nom de domaine complet de ce serveur Exchange à l'objet MAILMSG. L'attribut **homeMdb** est le serveur de boîtes aux lettres associé de l'utilisateur, qui est l'emplacement où résident la banque de boîtes aux lettres et la boîte aux lettres de l'utilisateur.
6. L'un des deux événements suivants se produit :
   - Si la banque de boîtes aux lettres de l'utilisateur est située sur ce serveur Exchange, le catégoriseur de messages balise le message pour une remise locale et le *moteur de files d'attente avancé* transfère le message au pilote de banque d'informations Exchange. Le pilote de banque d'informations Exchange remet ensuite le message à la banque de boîtes aux lettres.
   - Si la banque de boîtes aux lettres de l'utilisateur ne figure pas sur ce serveur Exchange, le catégoriseur de messages transfère le message au moteur de files d'attente avancé. Ce dernier appelle le *moteur de routage Exchange* afin de déterminer la meilleure façon d'envoyer le message au serveur (en fonction du routage de l'état des liaisons) et détermine la prochaine destination, ou saut, sur l'itinéraire vers le serveur associé de l'utilisateur.
7. Enfin, avec les informations de destination provenant du catégoriseur de messages et les informations de routage provenant du moteur de routage, le moteur de files d'attente avancé envoie le message à sa destination finale de l'une des façons suivantes :
   - Si la destination est un domaine local, le message est remis au serveur virtuel SMTP situé sur le serveur Exchange où réside la boîte aux lettres de l'utilisateur. Si la boîte aux lettres de l'utilisateur est dans un groupe de routage distant, il peut s'avérer nécessaire d'envoyer le message par le biais d'autres connecteurs.
   - Si la destination est à l'extérieur de l'organisation Exchange, le message est remis au serveur SMTP de domaines distants dans une file d'attente distante différente. Un message entrant est envoyé à un domaine distant uniquement si l'une des configurations suivantes est appliquée :
     - Le serveur Exchange autorise les relais.
     - L'utilisateur qui envoie le message a l'autorisation de relais.
     - Un autre connecteur autorisant les relais vers ces domaines est configuré.

- Si la destination est un connecteur vers un autre système ou vers une version précédente d'Exchange, le pilote de banque d'informations Exchange soumet le message à l'Agent de transfert des messages.

Envoi de messages Internet

Pour envoyer des messages Internet, Exchange s'appuie sur les mêmes composants sollicités pour la réception : DNS, le protocole SMTP, le catégoriseur de messages, le moteur de files d'attente avancé et le moteur de routage Exchange. Le courrier Internet est envoyé par le biais d'Exchange de la manière suivante :

1. Un utilisateur interne envoie un message à un domaine distant. Le message est soumis au serveur Exchange sur lequel réside la boîte aux lettres de l'utilisateur.
2. Le message est soumis au *moteur de files d'attente avancé* de l'une des deux façons suivantes :
   - Si le message a été envoyé à l'aide d'un client Microsoft Office Outlook® Web Access ou Outlook (MAPI), la banque d'informations Exchange soumet le message au moteur de files d'attente avancé par le biais du pilote de banque d'informations.
   - Si le message a été envoyé à l'aide d'un client POP (Post Office Protocol) ou IMAP (Internet Mail Access Protocol), SMTP le transmet au moteur de files d'attente avancé.
3. Le *catégoriseur de messages* recherche ensuite l'adresse du destinataire dans le serveur de catalogue global afin de trouver l'utilisateur. Si l'adresse du destinataire n'est pas dans une stratégie de destinataire ou s'il n'existe pas de destinataire correspondant avec une adresse proxy (l'adresse du destinataire n'est pas stockée dans Active Directory), le catégoriseur de messages en déduit que le message est destiné à un domaine distant.
4. Le moteur de files d'attente avancé appelle le *moteur de routage Exchange* afin de déterminer la destination suivante, ou saut, sur un itinéraire vers l'espace d'adressage qui correspond le mieux au domaine distant.
5. À l'aide de ces informations, le serveur détermine s'il doit envoyer le message, le router vers l'hôte actif ou utiliser un connecteur SMTP avec l'espace d'adressage distant.
6. Si plusieurs connecteurs ou plusieurs serveurs virtuels gèrent les messages sortants, le moteur de files d'attente avancé détermine le serveur virtuel ou le connecteur avec l'espace d'adressage correspondant le mieux à l'espace d'adressage du domaine distant et aux restrictions définies pour ce connecteur.
7. Le message est routé vers le serveur virtuel SMTP du connecteur sortant ou vers le serveur virtuel SMTP sortant assurant la remise.
8. Le serveur virtuel SMTP situé sur le serveur Exchange assurant la catégorisation utilise ensuite les informations de sa métabase relatives à l'attribut action de routage du domaine distant.
9. Le serveur virtuel SMTP sur le serveur Exchange effectue ensuite l'une des deux tâches suivantes :
   - Utilise DNS pour rechercher l'adresse IP du domaine cible, puis tente de remettre le message.
   - Transmet le message à un hôte actif qui assure la résolution DNS et la remise.

Concepts avancés sur l'état des liaisons

Cette section décrit les concepts avancés qui régissent la façon dont les informations sur l'état des liaisons sont communiquées et propagées dans une organisation Microsoft® Exchange. Elle comprend les sections suivantes :

- Composants de l'état des liaisons
- Description du paquet OrgInfo
- Description des détails du paquet OrgInfo
- Services serveur et nœuds clients
- Mises à jour de routage
- Communications sur la mise à jour de la topologie de routage

Composants de l'état des liaisons

Plusieurs composants jouent un rôle essentiel dans la propagation des informations sur l'état des liaisons. Ces composants sont les suivants :

- paquet OrgInfo qui contient le paquet des informations sur l'état des liaisons pour la topologie Exchange ;
- services serveur et nœuds clients qui utilisent ou échangent des informations sur l'état des liaisons ;
- maître du groupe de routage, un type de service serveur, qui est responsable de la gestion d'informations exactes sur l'état des liaisons pour son groupe de routage et de la distribution de ces informations (le paquet OrgInfo) aux membres de son groupe.

Description du paquet OrgInfo

Le paquet OrgInfo est la table d'état des liaisons qui affiche les détails et l'état de la topologie de routage de l'organisation Exchange. Les maîtres des groupes de routage propagent ces informations dans l'organisation sous la forme du paquet OrgInfo. Le paquet comprend des détails, tels que le nom de l'organisation, les groupes de routage, les connecteurs et les espaces d'adressage. L'outil WinRoute affiche le contenu du paquet OrgInfo sous une forme plus lisible que sa forme brute. Toutefois, pour identifier de façon détaillée les différentes parties de ce paquet, ce chapitre le présente sous la forme de données brutes.

> **Remarque** Vous pouvez télécharger l'outil WinRoute à partir du site Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=25097).

En règle générale, les champs d'informations du paquet sont séparés par des parenthèses de la façon suivante :

(Groupe de routage (Membres du groupe de routage (Connecteurs du groupe de routage (Configuration du connecteur))))

Dans le paquet, les GUID sont référencés pour les différents composants. Certaines informations sont représentées sous la forme de texte ASCII, par exemple :

- parties des adresses de groupe de routage X.400 et X.500 qui sont répertoriées dans chaque section de groupe de routage ;

- noms uniques hérités, legacyExchangeDN, des connecteurs ;
- noms des domaines complets des serveurs virtuels lors de l'affichage des serveurs têtes de pont sources ou distants des connecteurs ;
- pour chaque restriction définie sur un connecteur, nom unique de l'objet restreint (par exemple, si un connecteur refuse l'utilisation à trois utilisateurs, les trois noms uniques de ceux-ci sont répertoriés sous la forme de texte ASCII dans le paquet).

Dans la mesure où les composants ci-dessus sont répertoriés sous la forme de texte ASCII, leur nombre dans une topologie de routage affecte la taille globale du paquet OrgInfo. Par exemple, le fait de refuser l'accès au connecteur à des utilisateurs plutôt qu'à des groupes de distribution ou de spécifier des serveurs têtes de pont sources et de destination lorsque cela n'est pas nécessaire générera un paquet OrgInfo beaucoup plus volumineux. Étant donné que ce paquet est distribué dans l'organisation Exchange et que ces restrictions s'ajoutent à sa taille, l'échange du paquet des informations sur l'état des liaisons entre les serveurs peut avoir des conséquences importantes sur l'utilisation du réseau en fonction de la taille de l'organisation Exchange. Si vous devez limiter l'accès au connecteur, il est préconisé d'utiliser des groupes de distribution plutôt que des utilisateurs et de n'appliquer des serveurs têtes de pont sources et de destination spécifiques que lorsque nécessaire si la taille du paquet OrgInfo est une préoccupation.

Un autre point important relatif à la taille du paquet OrgInfo concerne le groupe de routage qui, une fois créé, reste en mémoire sur chaque serveur Exchange de l'organisation (du moment où les informations y ont été propagées) indéfiniment jusqu'à ce que tous les serveurs Exchange de l'organisation soient arrêtés en même temps. Cela est valable même si le groupe de routage a été supprimé dans le Gestionnaire système Exchange.

Description des détails du paquet OrgInfo

Pour expliquer le contenu d'un paquet OrgInfo, cette section analyse la transmission d'un paquet OrgInfo entre deux serveurs au sein d'un groupe de routage.

L'exemple illustré à la figure 15.1 est tiré d'une organisation Exchange dotée d'un groupe de routage qui contient deux serveurs exécutant tous deux Exchange Server 2003, avec un seul connecteur SMTP qui intègre les restrictions utilisateur. Le paquet OrgInfo transmis sur le réseau contenait les informations suivantes :

```
{00000457}.ORGINFO.a9c421ebe14f06710f6ab596345ac615.(.a2a0f896d197b84999557850ac79
6258.2d07476703630a4d87a651498e2d73b9.a.0.0.f0dcd868912f54479b26d729863bb825.{26}*
.A2A0F896-D197-B849-9955-
7850AC796258.{4b}c=US;a=.;p=Example;o=Exchange;cn=A2A0F896-D197-B849-9955-
7850AC796258;*.{53}/o=Example/ou=First.Administrative.Group/*/A2A0F896-D197-B849-
99557850AC796258.(.2d07476703630a4d87a651498e2d73b9.YES.1.1aae.{10}070100000000010
1..979733932e995742bc2d5ecf93198b4d.YES.1.1aae.{10}0701000000000101.).(.f76005bd57
ad93428518268f28f4f7e6.(.CONFIG.{4}SMTP.{23}_f76005bd57ad93428518268f28f4f7e6_S.{}
.{54}/o=Example/ou=First.Administrative.Group/cn=Configuration/cn=Connections/cn=J
UNK.0.0.0.0.ffffffff.ffffffff.0.1.0.().6.(.{24}CN=tester07,CN=Users,DC=domain,DC=c
om..{24}CN=tester04,CN=Users,DC=domain,DC=com..{24}CN=tester03,CN=Users,DC=domain,
DC=com..{24}CN=tester02,CN=Users,DC=domain,DC=com..{24}CN=tester01,CN=Users,DC=dom
ain,DC=com..{29}CN=Administrator,CN=Users,DC=domain,DC=com.).0.().0.()..ARROWS.(.{
4}SMTP.{1}*.1.).BH.(.2fdb30b62e4ea949a71f91f319535143.CONN_AVAIL.{13}RGR-65-
02.domain.com.).TARGBH.().STATE.UP))))..
```

Figure 15.1 Exemple du contenu d'un paquet OrgInfo

En analysant le paquet illustré à la figure 15.1 dans l'ordre de présentation, « ORGINFO » indique au serveur de réception que le paquet OrgInfo figure dans cette trame. « ORGINFO » est suivi du contenu ci-dessous :

- Hachage MD5, signature cryptée qui représente le numéro de version de la table d'état des liaisons, du paquet OrgInfo actuel. Cette signature est importante, car les serveurs utilisent ces informations pour déterminer s'ils possèdent les mêmes informations sur l'état des liaisons. Comme illustré plus loin, un

hachage différent entre deux serveurs Exchange indique qu'ils ont des informations de routage différentes et qu'ils s'échangeront les paquets OrgInfo pour identifier celui qui possède les informations les plus à jour.

- Le premier ensemble de parenthèses indique que les informations qui y sont contenues se rapportent à un groupe de routage particulier. Cet exemple illustrant un seul groupe de routage, toutes les informations de routage figurent dans cet ensemble de parenthèses :
  - GUID du groupe de routage : a2a0f896d197b84999557850ac796258
  - GUID du maître du groupe de routage : 2d07476703630a4d87a651498e2d73b9
  - Versions majeure, mineure et utilisateur des informations sur l'état des liaisons : a.0.0
  - GUID de ces informations de versions : f0dcd868912f54479b26d729863bb825
- Informations relatives à l'adresse SMTP du groupe de routage : {26}. Les crochets signalent le début des informations. Lorsqu'une organisation a intégralement convergé, chaque groupe de routage héberge ces informations. En d'autres termes, s'il existe deux groupes de routage, les informations ci-dessous sont répertoriées dans la section de chaque groupe du paquet OrgInfo. (Notez que les caractères figurant à l'intérieur de ces crochets et des crochets suivants mentionnés ne sont pas nécessairement identiques entre les implémentations.)
  - Le GUID immédiatement après {26}, A2A0F896-D197-B849-9955-7850AC796258, est celui du groupe de routage particulier.
- {4b} Il s'agit du début des adresses X.400 du groupe de routage. De même que ci-dessus, ces informations sont répertoriées dans la section de chaque groupe du paquet OrgInfo :
  - c=US;a=.;p=Exemple;o=Exchange;cn=A2A0F896-D197-B849-9955-7850AC796258;* indique l'espace d'adressage X.400, la partie « cn » étant le GUID du groupe de routage.
- {53} Il s'agit des informations relatives à l'adresse X.500 du groupe de routage. De même que ci-dessus, ces informations sont répertoriées dans la section de chaque groupe du paquet OrgInfo :
  - /o=Exemple/ou=Premier groupe d'administration/*/A2A0F896-D197-B849-9955-7850AC796258
- En commençant à la parenthèse ouverte suivante, les membres du groupe de routage sont identifiés :
  - GUID d'un serveur membre du groupe de routage : 2d07476703630a4d87a651498e2d73b9
  - Connexion ou non du membre au maître du groupe de routage. « OUI » indique que le serveur est connecté.
  - Les numéros de version du serveur sont répertoriés en dernier.

  Les trois attributs ci-dessus sont alors identifiés pour le second serveur du groupe de routage.
- En commençant à la parenthèse ouverte suivante, les connecteurs sont identifiés :
  - GUID du connecteur unique : a9c421ebe14f06710f6ab596345ac615
- La parenthèse ouverte suivante identifie les informations de configuration du connecteur :
  - Type de connecteur (SMTP) : {4}
  - Adresse du serveur tête de pont source local qui se présente au format suivant : GUID du connecteur lui-même auquel est ajouté « _S » (sans les chevrons) pour indiquer un serveur tête de pont source : {23}_f76005bd57ad93428518268f28f4f7e6_S

    Remarque Il s'agit d'un connecteur SMTP. Toutefois, dans le cas d'un connecteur de groupe de routage auquel est affecté un serveur tête de pont distant ou de destination, le paquet OrgInfo affiche un autre élément {23} suivi encore par le GUID du connecteur lui-même auquel est ajouté « _D ». Dans le cas d'un connecteur SMTP qui spécifie un hôte actif, le paquet OrgInfo affiche le nom de domaine complet de cet hôte actif.

    - Nom unique du connecteur : {54}/o=Exemple/ou=Premier.groupe.d'administration/cn=Configuration/cn=Connexions/cn=INDÉSIRABLE
    - La planification du connecteur est identifiée par le premier « 0 ». (Dans ce cas, elle a la valeur « Toujours ».)
- Les restrictions du connecteur sont ensuite identifiées :
    - L'étendue du connecteur est identifiée par le « 0 » suivant. (Dans ce cas, elle a la valeur « Organisation ».)
    - Configuration ou non de la remise déclenchée. Le troisième « 0 » identifie la remise déclenchée, par exemple TURN/ETRN (dans ce cas, la remise déclenchée n'est pas configurée).
    - Le type de la priorité du message (Haute, Normale, Basse) autorisé par ce connecteur est identifié par le dernier « 0 ».
    - Limites de taille des messages : ffffffff indique qu'il n'existe aucune limite de taille des messages via ce connecteur.
    - Définition ou non d'un seuil pour les messages volumineux : ffffffff indique qu'aucun seuil pour les messages n'a été défini.
    - « 0 1 0 » à la suite des éléments ci-dessus fournit les indications ci-après :
        - Les redirections de dossiers publics sont autorisées.
        - Par défaut, les messages de tous les utilisateurs sont acceptés.
        - Expéditeurs autorisés (qui est vide dans ce cas, car les messages de tous les utilisateurs sont acceptés par défaut selon le paramètre ci-dessus).
    - Le chiffre suivant, « 6 », indique que six entrées figurent dans le champ des expéditeurs refusés. Le nom unique de chaque objet est ensuite répertorié.
    - Les deux derniers « 0 » des paramètres des restrictions du connecteur indiquent qu'aucun objet n'est identifié en tant que liste de distribution autorisée ou refusée.
- ARROWS indique le début des informations d'espace d'adressage du connecteur :
    - {4}SMTP indique que le type de l'espace d'adressage est SMTP.
    - {1}* indique qu'il s'adresse à tous les domaines SMTP.
    - 1 indique un coût de un.
- Commençant par « BH », les serveurs têtes de pont pour le connecteur sont identifiés. Dans cet exemple, un serveur tête de pont est identifié par les éléments suivants :
    - GUID du serveur virtuel SMTP qui est désigné comme serveur tête de pont local : 2fdb30b62e4ea949a71f91f319535143
    - Disponibilité du serveur tête de pont distant : CONN_AVAIL
    - Nom de domaine complet du serveur virtuel qui joue le rôle de serveur tête de pont pour ce connecteur : {13}RGR-65-02.domaine.com
- Nom de domaine complet de tout serveur tête de pont cible spécifié (dans cet exemple, aucun n'a été spécifié) : TARGBH.
- État du connecteur : « ACTIF » signifie que le connecteur est disponible. (« INACTIF », ou non disponible, est la seule autre option possible.)

Services serveur et nœuds de routage

Maintenant que vous connaissez le contenu du paquet OrgInfo, cette section décrit les nœuds de routage, qui sont les composants impliqués dans la propagation de ces informations dans une organisation Exchange. Il peut exister trois types de nœuds de routage sur un serveur Exchange :

- Nœud du service maître
- Nœud du service esclave
- Nœud client

Un seul type de nœud du service peut exister sur un serveur : le nœud du service maître (si le serveur est le maître du groupe de routage) ou le nœud du service esclave (si le serveur est un membre du groupe de routage). Les nœuds clients sont constitués de différents processus, qui utilisent des informations de routage, exécutés sur le serveur. Parmi ces processus figurent SMTP (inetinfo.exe), l'Agent de transfert des messages (emsmta.exe), la banque d'informations (store.exe) et le service Infrastructure de gestion Windows (wmiprvse.exe). Deux DLL implémentent la fonction de routage dans ces composants : resvc.dll pour les nœuds des services et reapi.dll pour les nœuds clients.

La figure 15.2 illustre les nœuds de routage et services serveur.

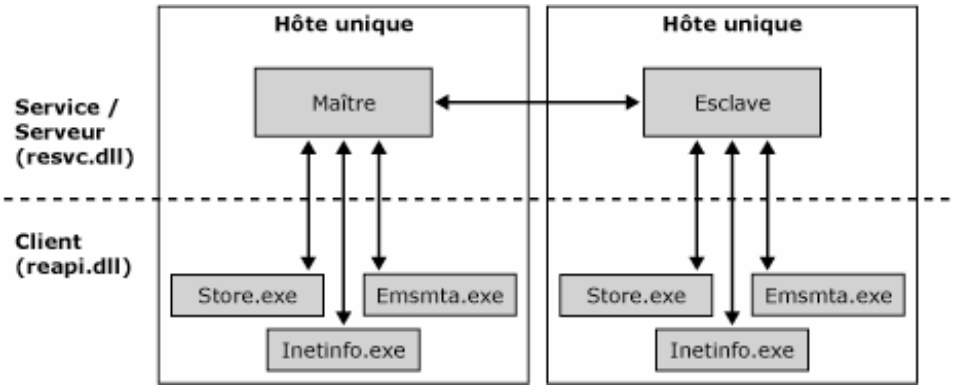


Figure 15.2 Nœuds des services de routage

Les nœuds clients communiquent directement avec leurs services serveur correspondants. Cette communication ne se produit jamais à l'extérieur d'un hôte individuel, par exemple un nœud client communique uniquement avec d'autres composants sur le même serveur. Les nœuds des services maître et esclave à l'intérieur du même groupe de routage communiquent entre eux via le port TCP 691.

Mises à jour de routage

Cette section décrit les types de mises à jour que le maître du groupe de routage reçoit et distribue aux membres de son groupe. Les serveurs et les contrôleurs de domaine Exchange peuvent communiquer au sujet des types d'informations suivants dans le contexte des mises à jour de la topologie du routage et de l'état des liaisons :

- **Majeure** Lorsque des mises à jour de la topologie du routage se produisent, telles que la configuration de connecteur qui comprend l'ajout ou la suppression d'un connecteur, l'ajout ou la suppression d'un espace d'adressage sur un connecteur, ou lorsqu'un nouveau serveur est désigné en tant que maître du groupe de routage.
- **Mineure** Lorsque des informations relatives à la disponibilité d'un connecteur ou serveur virtuel sont modifiées, par exemple lorsque l'état du connecteur passe d'actif à inactif.

- **Utilisateur** Lorsque des services ont été démarrés ou arrêtés sur un serveur Exchange (utilisé dans l'implémentation du nœud 'Status' dans le Gestionnaire système Exchange), qu'un autre serveur a été ajouté au groupe de routage ou qu'un serveur perd sa connectivité avec le maître du groupe de routage.

Mises à jour majeures

Un contrôleur de domaine informe les maîtres des groupes de routage des mises à jour majeures apportées à la topologie de routage relatives à leur groupe de routage en particulier, selon le processus de notification de modification LDAP (Lightweight Directory Access Protocol) standard. Lorsque le maître du groupe de routage démarre, il s'inscrit dans l'annuaire à l'aide de DSAccess pour recevoir les notifications des modifications qui se rapportent à son groupe de routage.

Un maître de groupe de routage n'accepte les mises à jour majeures des informations de routage qui se rapportent à son groupe de routage que du contrôleur de domaine avec lequel il communique. Lorsqu'une mise à jour des informations de routage est envoyée à un groupe de routage par un autre groupe, par exemple, le maître du groupe de routage de réception ignore toujours les informations relatives à son groupe qui figurent dans le paquet OrgInfo. Dans le cas de mises à jour mineure et utilisateur qui se rapportent à son groupe de routage, le maître accepte les modifications de ses nœuds clients locaux ou de tout service esclave (membre du groupe de routage) au sein de son groupe.

Un contrôleur de domaine envoie des notifications au maître du groupe de routage dans les cas suivants :

- Un nouveau connecteur a été ajouté au groupe de routage ou une modification d'attribut a été apportée à un connecteur existant.
- Lorsque des modifications ont été apportées à l'objet groupe de routage lui-même, par exemple, le maître change.

Une fois le processus de notification de modification terminé, le maître de groupe de routage communique la modification de la topologie à tous les serveurs du groupe de routage local et à tout serveur qui joue le rôle de serveur tête de pont distant pour l'un des connecteurs de ce groupe de routage.

Mises à jour mineures

Les mises à jour mineures sont des modifications de l'état des liaisons dans l'environnement, par exemple lorsque l'état du connecteur passe d'actif à inactif. Cette modification de l'état des liaisons peut être détectée par tout nœud client dans l'environnement. Dans Exchange 2000 Server, lorsqu'un nœud client détecte une modification, il la communique à ses nœuds de services serveur à des intervalles de 5 minutes. En règle générale, chaque fois qu'une mise à jour de l'état des liaisons est reçue par un maître ou un nœud de service esclave, le serveur est obligé de placer à nouveau en file d'attente tous les messages et d'informer le maître du groupe de routage de la modification de l'état des liaisons. Dans le cas de connexions peu fiables qui provoquent de fréquentes modifications de l'état (connexions oscillantes), les communications sont excessives et souvent en conflit.

Dans Exchange Server 2003, si aucun autre chemin n'existe pour une liaison dans un groupe de routage nœud feuille, l'état de la liaison est toujours signalé comme disponible. Exchange n'affecte pas l'état non disponible à la liaison si aucun autre chemin n'existe. Exchange place le courrier en file d'attente pour l'envoyer quand la route devient à nouveau disponible. Cette modification améliore les performances en réduisant la propagation des informations sur l'état des liaisons.

Dans le cas des connexions oscillantes, Exchange 2003 affiche la file d'attente de l'état des liaisons ; s'il détecte plusieurs modifications en conflit dans un intervalle donné pour un connecteur, ce dernier est assimilé à une connexion oscillante et l'état de sa liaison reste disponible. Il est préférable de laisser un connecteur oscillant dans un état disponible plutôt que de modifier continuellement l'état de la liaison. Cette approche réduit le trafic relatif à l'état des liaisons répliqué entre serveurs.

Mises à jour utilisateur

Les mises à jour utilisateur sont des modifications minimales, telles que le moment où le maître du groupe de routage a été modifié, où les services ont été démarrés ou arrêtés sur un serveur Exchange, où un autre serveur a été ajouté au groupe de routage ou encore où un serveur membre perd sa connectivité avec le maître du groupe de routage.

Communications sur la mise à jour de la topologie de routage

La façon dont Exchange communique les informations de routage varie selon qu'il traite une mise à jour entre des groupes de routage ou à l'intérieur des groupes de routage. Cette section présente le mode de fonctionnement de processus de mise à jour des communications spécifiques dans plusieurs scénarios de topologie de routage présentés ci-dessous :

- **Mises à jour d'annuaires vers les maîtres des groupes de routage** Un seul serveur Exchange, un seul contrôleur de domaine
- **Mises à jour des maîtres des groupes de routage vers les membres des groupes de routage** Deux serveurs Exchange (même groupe de routage), un contrôleur de domaine
- **Mises à jour entre des groupes de routage** Trois serveurs Exchange (deux dans un groupe de routage, un dans un autre groupe), un contrôleur de domaine

  Remarque Les captures réseau qui illustrent les concepts en pratique sont fournis pour que vous compreniez parfaitement le processus de mise à jour des communications. Toutes les captures ont été réalisées à l'aide de l'outil d'analyse de réseau (Netmon.exe) qui accompagne Microsoft Windows Server™ 2003.

Mises à jour d'annuaires vers les maîtres des groupes de routage

Les maîtres des groupes de routage reçoivent les mises à jour majeures d'un contrôleur de domaine au moyen du processus de notification de modification du service d'annuaire Microsoft Active Directory®. Plus particulièrement, Exchange s'appuie sur son contrôleur de domaine de configuration pour les informations de mise à jour de l'annuaire, qui portent le nom **Config** sous l'onglet **DSAccess** de la boîte de dialogue **Propriétés** d'un serveur dans le Gestionnaire système Exchange.

Le processus de notification de modification commence lorsque le client ou la station de travail où un nouveau connecteur a été ajouté ou toute autre modification de routage a été effectuée à l'aide du Gestionnaire système Exchange contacte le contrôleur de domaine pour lui demander d'ajouter ce nouveau connecteur à Active Directory. Le contrôleur de domaine indique à la station de travail que l'ajout a été effectué. Le contrôleur de domaine avertit alors le serveur Exchange qui est le maître de routage de ce nouveau connecteur et envoie des informations sur ce connecteur par le biais de plusieurs communications. Les captures réseau suivantes illustrent ce processus.

La figure 15.3 illustre un extrait d'une capture réseau qui concerne un contrôleur de domaine Windows 2000 où un nouveau connecteur a été ajouté à un groupe de routage (Exchange 2000). Notez la trame 147 qui affiche « AddRequest ».

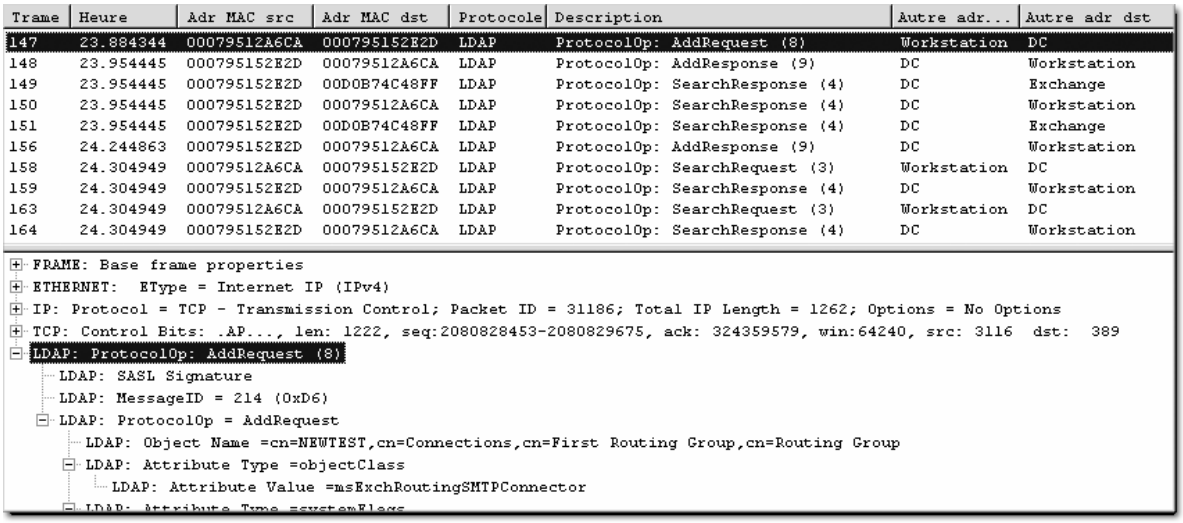


Figure 15.3 Contrôleur de domaine Windows 2000 où un nouveau connecteur a été ajouté à un groupe de routage

La figure 15.3 illustre le client (la station de travail) qui demande au contrôleur de domaine d'ajouter un nouveau connecteur SMTP à l'annuaire. La trame 148 montre le contrôleur de domaine qui indique que cet ajout a été effectué. Immédiatement après dans la trame 149 (figure 15.4), le contrôleur de domaine envoie un message « SearchResponse » au serveur Exchange qui informe Exchange au sujet du nouveau connecteur.

Le contrôleur de domaine exécute automatiquement cette action apparemment non sollicitée, car le serveur Exchange s'est auparavant inscrit pour recevoir les notifications des modifications comme le font tous les serveurs Exchange 2000 et Exchange 2003. Il s'agit là de l'illustration du déroulement du processus de notification de modification. Dans la trame 149, le contrôleur de domaine ne fait qu'informer Exchange du nom et du nom unique du nouveau connecteur.

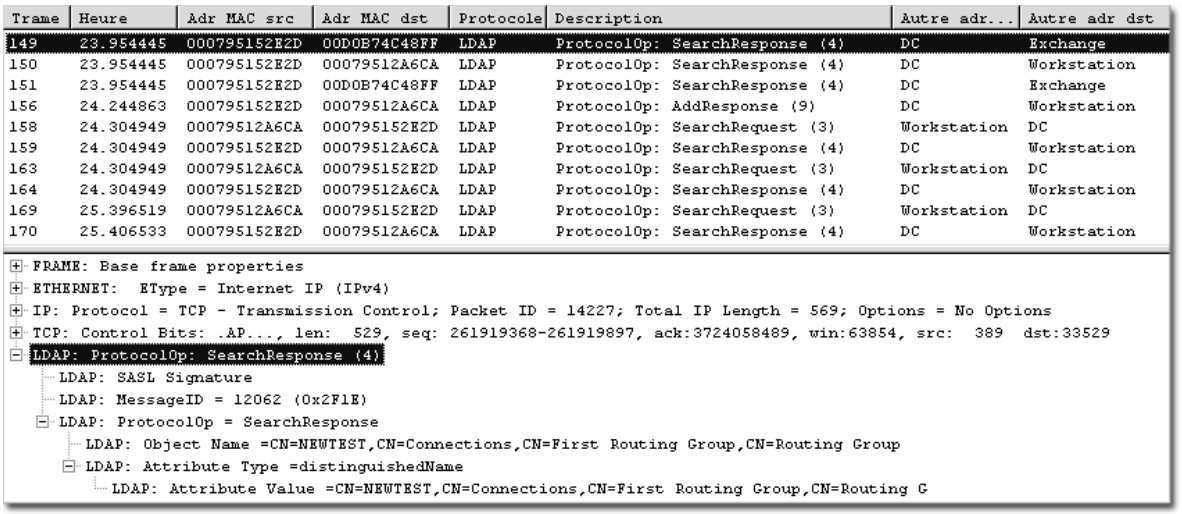
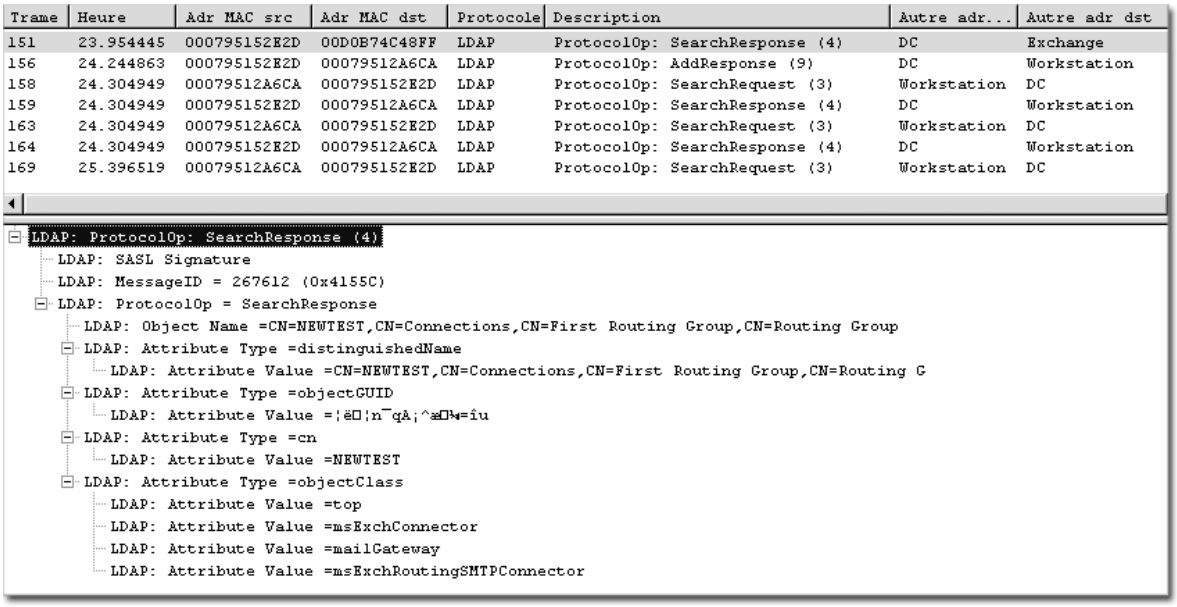


Figure 15.4 Le contrôleur de domaine envoie un message « SearchResponse » au serveur Exchange qui informe Exchange au sujet du nouveau connecteur

Dans les trames 150 et 151, le contrôleur de domaine envoie d'autres informations sur cet ajout à la fois à la station de travail sur laquelle ce connecteur a été ajouté et au serveur Exchange. La figure 15.5 illustre la trame 151 (envoyée à Exchange). Outre le nom de l'objet et le nom **distinguishedname**, les attributs **objectGUID**, **cn** et **objectClass** sont à présent inclus.



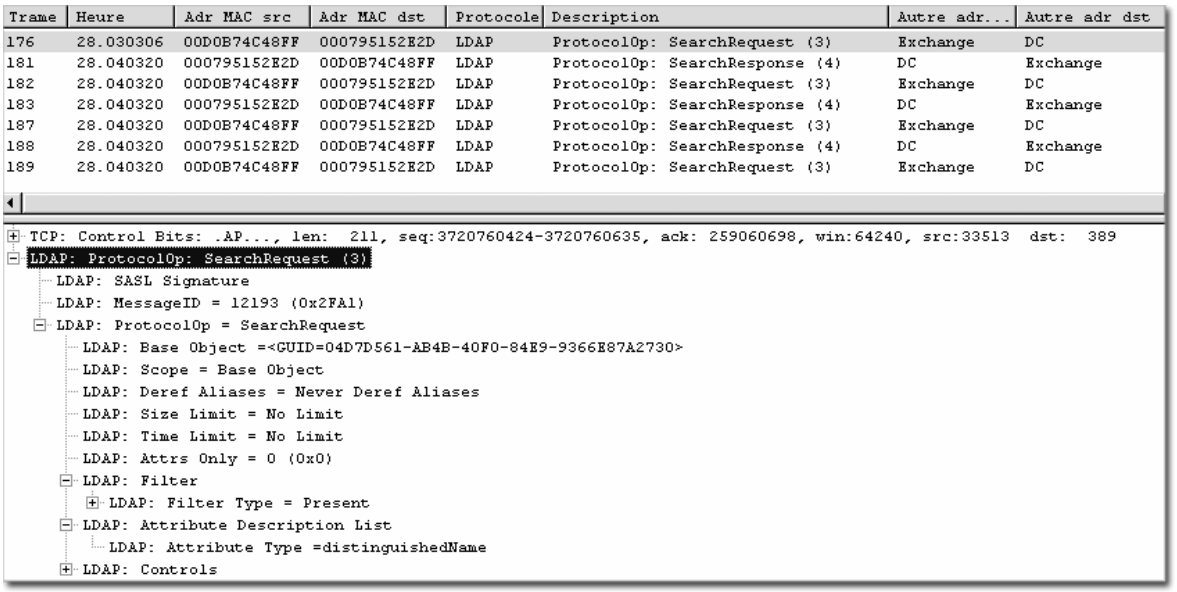
Trame	Heure	Adr MAC src	Adr MAC dst	Protocole	Description	Autre adr...	Autre adr dst
151	23.954445	000795152E2D	00D0B74C48FF	LDAP	ProtocolOp: SearchResponse (4)	DC	Exchange
156	24.244863	000795152E2D	00079512A6CA	LDAP	ProtocolOp: AddResponse (9)	DC	Workstation
158	24.304949	00079512A6CA	000795152E2D	LDAP	ProtocolOp: SearchRequest (3)	Workstation	DC
159	24.304949	000795152E2D	00079512A6CA	LDAP	ProtocolOp: SearchResponse (4)	DC	Workstation
163	24.304949	00079512A6CA	000795152E2D	LDAP	ProtocolOp: SearchRequest (3)	Workstation	DC
164	24.304949	000795152E2D	00079512A6CA	LDAP	ProtocolOp: SearchResponse (4)	DC	Workstation
169	25.396519	00079512A6CA	000795152E2D	LDAP	ProtocolOp: SearchRequest (3)	Workstation	DC

```
LDAP: ProtocolOp: SearchResponse (4)
    LDAP: SASL Signature
    LDAP: MessageID = 267612 (0x4155C)
  LDAP: ProtocolOp = SearchResponse
      LDAP: Object Name =CN=NEWTEST,CN=Connections,CN=First Routing Group,CN=Routing Group
    LDAP: Attribute Type =distinguishedName
        LDAP: Attribute Value =CN=NEWTEST,CN=Connections,CN=First Routing Group,CN=Routing G
    LDAP: Attribute Type =objectGUID
        LDAP: Attribute Value =¦ë□¦n¯qA¡^æ□¼=îu
    LDAP: Attribute Type =cn
        LDAP: Attribute Value =NEWTEST
    LDAP: Attribute Type =objectClass
        LDAP: Attribute Value =top
        LDAP: Attribute Value =msExchConnector
        LDAP: Attribute Value =mailGateway
        LDAP: Attribute Value =msExchRoutingSMTPConnector
```

Figure 15.5 Le contrôleur de domaine envoie d'autres informations sur cet ajout à la fois à la station de travail sur laquelle ce connecteur a été ajouté et au serveur Exchange

Une fois que le contrôleur de domaine a envoyé ces informations, la station de travail lui demande la liste complète des attributs relatifs au nouveau connecteur.

Dans la trame 176 (figure 15.6), Exchange lance des requêtes relatives à son groupe de routage. Le serveur Exchange lance ces actions chaque fois qu'il reçoit une notification de modification. Plus précisément, il commence par demander le nom unique du GUID du groupe de routage.



Trame	Heure	Adr MAC src	Adr MAC dst	Protocole	Description	Autre adr...	Autre adr dst
176	28.030306	00D0B74C48FF	000795152E2D	LDAP	ProtocolOp: SearchRequest (3)	Exchange	DC
181	28.040320	000795152E2D	00D0B74C48FF	LDAP	ProtocolOp: SearchResponse (4)	DC	Exchange
182	28.040320	00D0B74C48FF	000795152E2D	LDAP	ProtocolOp: SearchRequest (3)	Exchange	DC
183	28.040320	000795152E2D	00D0B74C48FF	LDAP	ProtocolOp: SearchResponse (4)	DC	Exchange
187	28.040320	00D0B74C48FF	000795152E2D	LDAP	ProtocolOp: SearchRequest (3)	Exchange	DC
188	28.040320	000795152E2D	00D0B74C48FF	LDAP	ProtocolOp: SearchResponse (4)	DC	Exchange
189	28.040320	00D0B74C48FF	000795152E2D	LDAP	ProtocolOp: SearchRequest (3)	Exchange	DC

```
TCP: Control Bits: .AP..., len:  211, seq:3720760424-3720760635, ack: 259060698, win:64240, src:33513  dst:  389
LDAP: ProtocolOp: SearchRequest (3)
    LDAP: SASL Signature
    LDAP: MessageID = 12193 (0x2FA1)
  LDAP: ProtocolOp = SearchRequest
      LDAP: Base Object =<GUID=04D7D561-AB4B-40F0-84E9-9366E87A2730>
      LDAP: Scope = Base Object
      LDAP: Deref Aliases = Never Deref Aliases
      LDAP: Size Limit = No Limit
      LDAP: Time Limit = No Limit
      LDAP: Attrs Only = 0 (0x0)
    LDAP: Filter
      LDAP: Filter Type = Present
    LDAP: Attribute Description List
        LDAP: Attribute Type =distinguishedName
    LDAP: Controls
```

Figure 15.6 Exchange lance des requêtes relatives à son groupe de routage

Après avoir reçu le nom unique du GUID du groupe de routage, Exchange demande tous les attributs de tout objet enfant duquel cet objet peut être un parent et qui sont du type d'objet « **msExchconnector** ». Notez l'étendue « Niveau unique » de la recherche par rapport à la recherche « Objet de base ». Cette désignation

indique que la recherche porte sur un objet enfant. La trame 182 (figure 15.7) affiche cette demande de recherche.

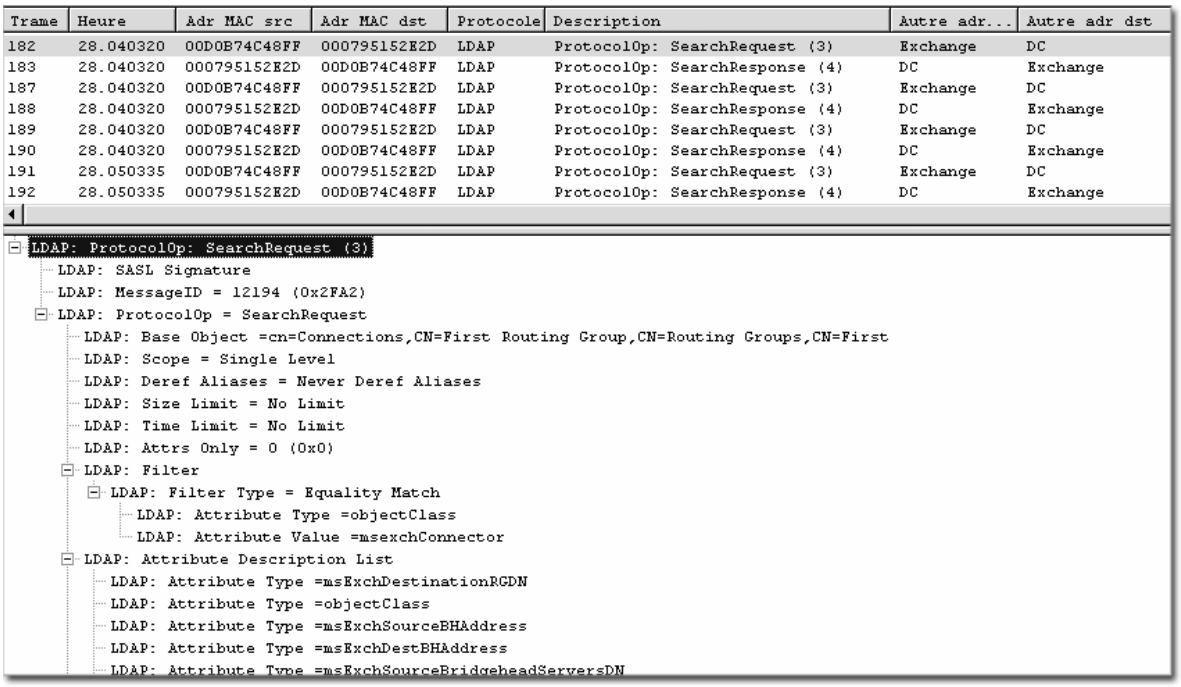


Figure 15.7 Demande de recherche d'un objet enfant

La trame 183 (figure 15.8) présente la réponse partielle du contrôleur de domaine.

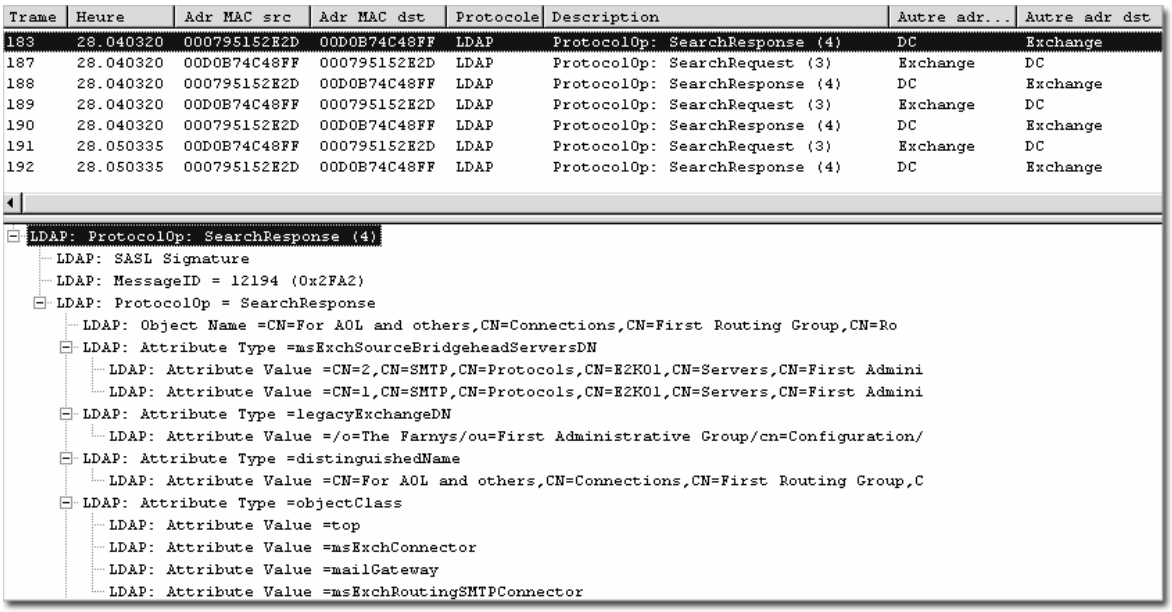


Figure 15.8 Réponse partielle du contrôleur de domaine

Exchange interroge ensuite le contrôleur de domaine et reçoit les éléments suivants :

- Nom de domaine complet et GUID de tout serveur tête de pont associé au connecteur en question.

- Requête de plusieurs attributs du nouveau connecteur. Cette requête est basée sur le GUID du connecteur et retourne le résultat illustré à la figure 15.9.

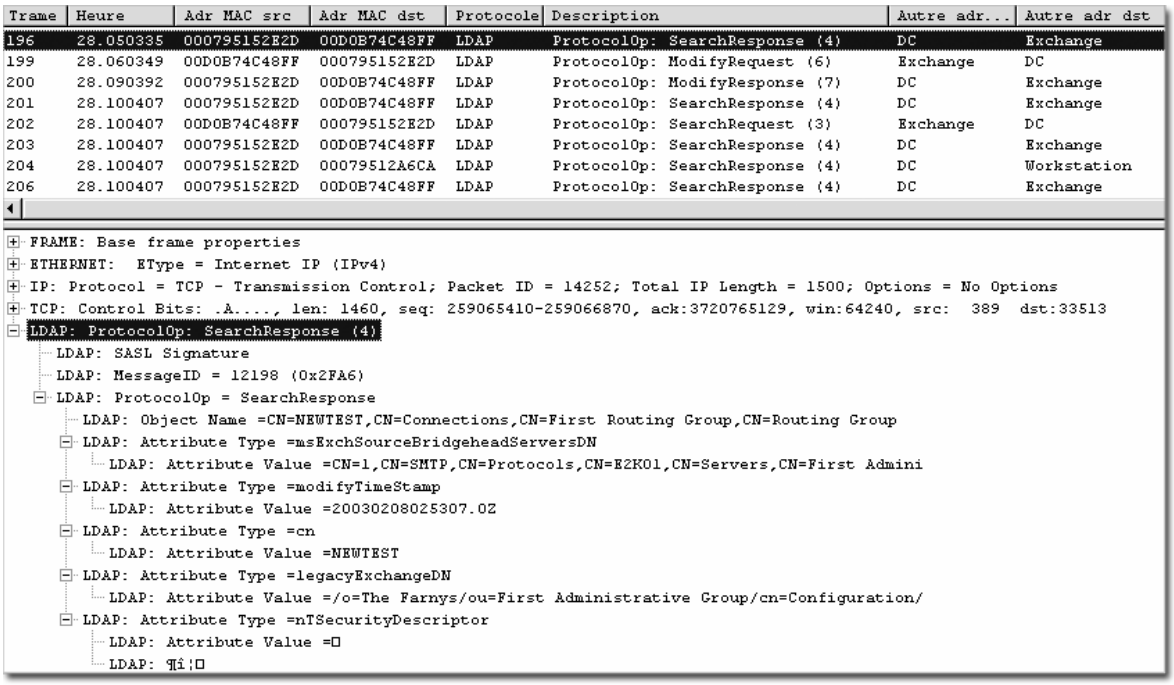


Figure 15.9 Résultat d'une requête d'attributs d'un nouveau connecteur

Comme illustré à la figure 15.10, le serveur Exchange envoie un message « ModifyRequest » qui demande au contrôleur de domaine de remplacer trois attributs de l'objet « GWART hérité » dans le groupe d'administration : **GatewayRoutingTree**, **GWARTLastModified** et **ridServer**.

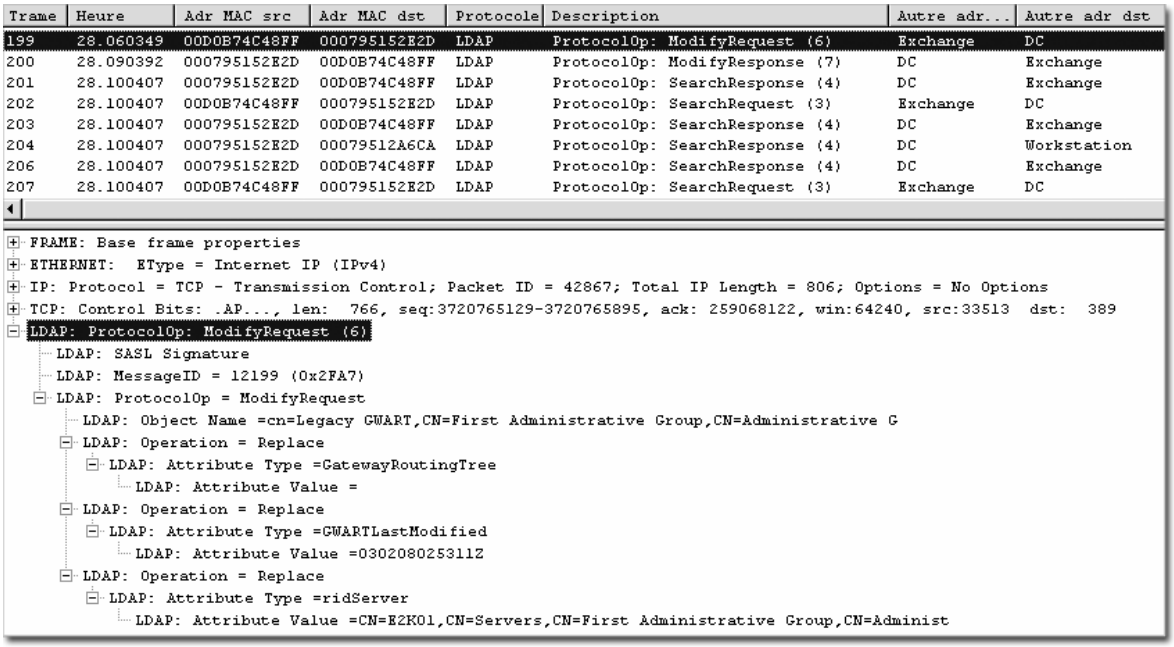


Figure 15.10 Demande du serveur Exchange au contrôleur de domaine de remplacer trois attributs de l'objet « GWART hérité »

Le contrôleur de domaine répond par un message « ModifyResponse » de réussite et le serveur Exchange continue de demander différents objets dans son groupe d'administration.

Tout le processus qui est décrit dans cette section illustre la façon dont les contrôleurs de domaine communiquent les mises à jour majeures de la topologie aux maîtres des groupes de routage. À la suite de cette mise à jour, le maître du groupe de routage doit désormais communiquer les informations à ses serveurs membres. La section suivante décrit la façon dont le maître du groupe de routage communique ces informations aux membres de son groupe de routage.

Mises à jour des maîtres des groupes de routage vers les membres des groupes de routage

Lorsque le maître du groupe de routage est informé d'une mise à jour, il remplace les informations sur l'état des liaisons contenues en mémoire (le paquet OrgInfo) par les nouvelles informations, ce qui entraîne la création d'un hachage MD5 basé sur celles-ci. Il propage ensuite le nouveau paquet OrgInfo vers les nœuds clients sur le même ordinateur et les nœuds des services esclaves ou membres du groupe de routage au sein du groupe. Le maître du groupe de routage communique avec le groupe de routage via le port TCP 691.

La figure 15.11 représente la communication qui se produit sur le port 691 source ou de destination. L'exemple illustre l'ajout d'un nouveau connecteur à un groupe de routage qui contient deux serveurs.

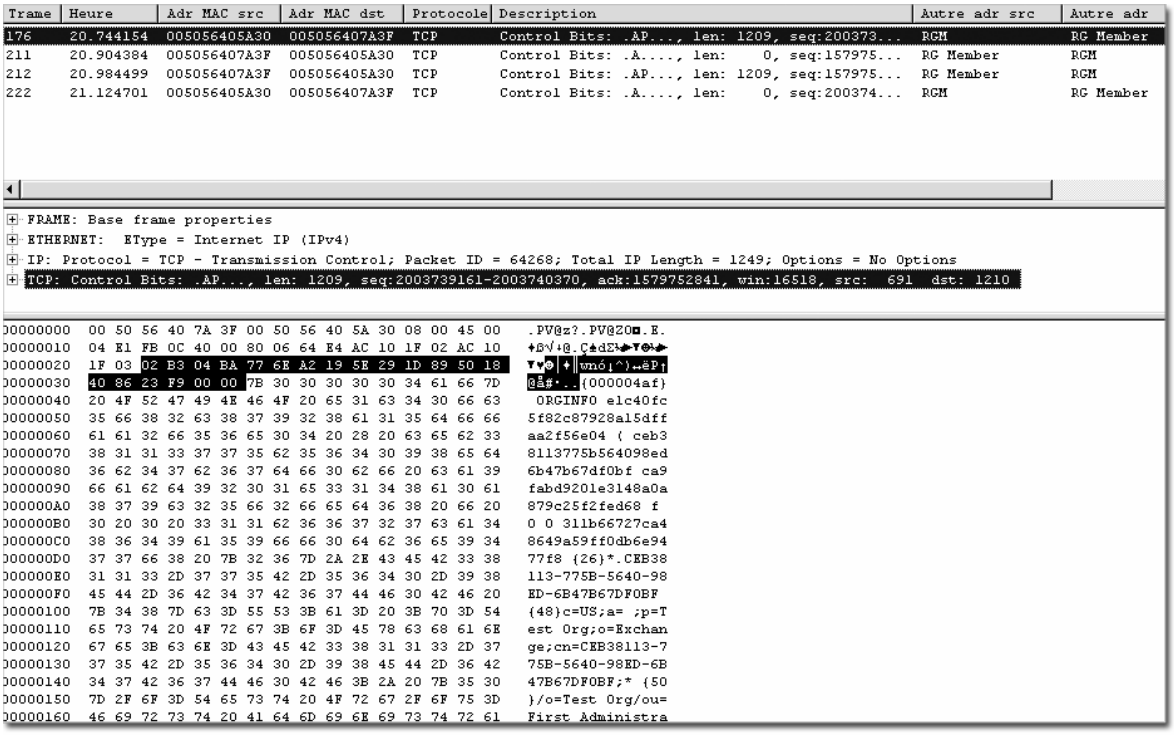


Figure 15.11 Le maître du groupe de routage propage les informations de mise à jour vers les membres du groupe de routage

La trame 175 est le message « SearchResponse » qu'un contrôleur de domaine envoie au maître du groupe de routage qui est inscrit pour recevoir les notifications des modifications. Immédiatement après avoir reçu ces informations, le maître du groupe de routage envoie l'intégralité du paquet OrgInfo au membre du groupe, comme illustré à la trame 176 (figure 15.11). Les caractères qui figurent avant la première parenthèse de ce

paquet représentent le hachage MD5 du paquet OrgInfo, que les serveurs utilisent pour déterminer s'ils disposent des informations les plus à jour.

Comme le hachage MD5 reçu est différent de celui qui figure en mémoire, le membre du groupe de routage traite également le paquet OrgInfo. Après avoir apporté les modifications appropriées à sa table d'état des liaisons en mémoire, le membre envoie une courte réponse au maître du groupe de routage, suivie dans la trame suivante par le paquet OrgInfo qu'il vient de réviser, en faisant désormais également référence au dernier hachage MD5 que le maître a envoyé précédemment. La figure 15.12 illustre la réponse initiale.

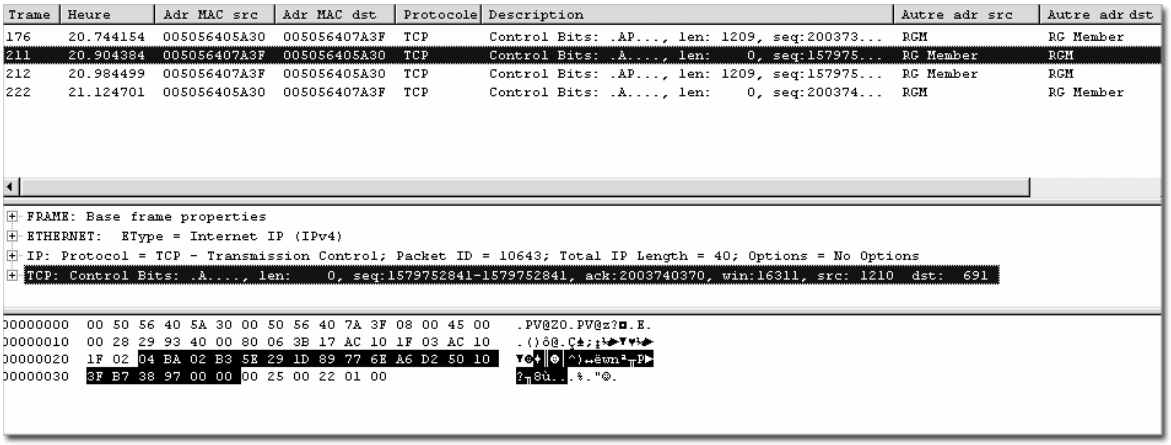


Figure 15.12 Réponse initiale du membre au maître du groupe de routage

La réponse OrgInfo du membre du groupe de routage qui contient le paquet OrgInfo maintenant à jour est ensuite envoyée au maître du groupe de routage (figure 15.13).

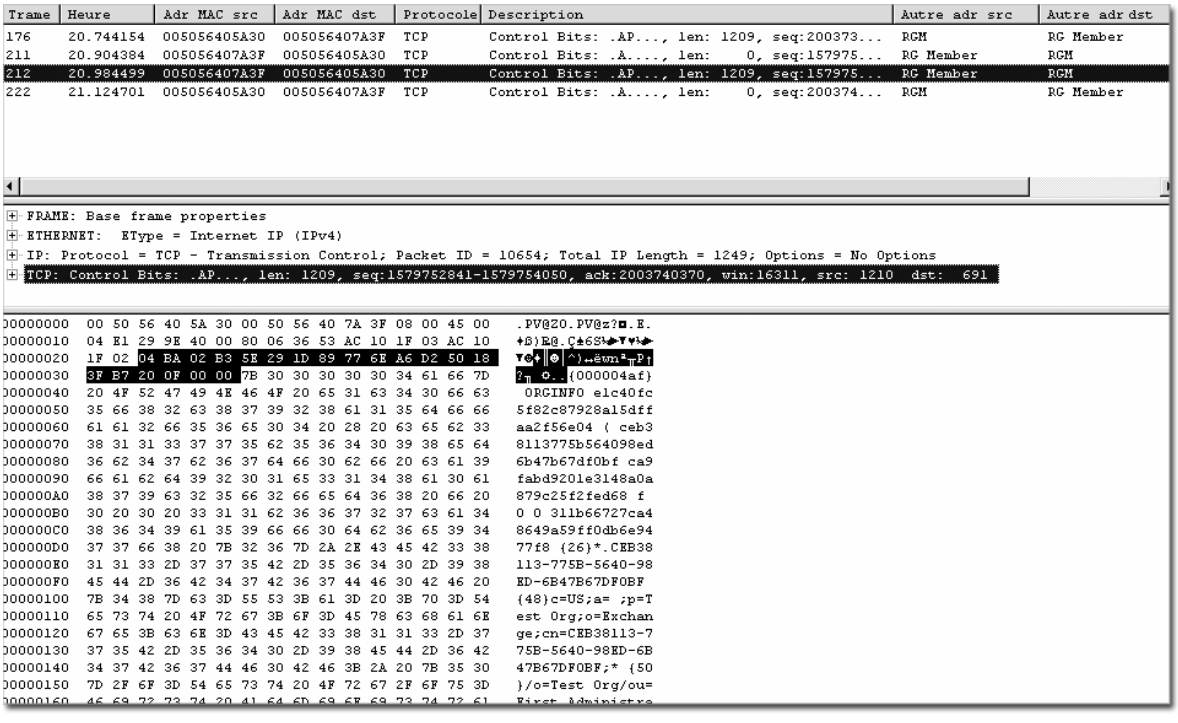


Figure 15.13 Réponse OrgInfo du membre du groupe de routage

Le maître du groupe de routage traite ces informations et envoie un bref accusé de réception au membre.

Ce processus se déroule entre tous les membres et le maître au sein du groupe de routage spécifique. Un autre processus, connu sous le nom d'*interrogation*, permet de garantir que tous les membres du groupe de routage ont reçu les informations les plus à jour du maître.

Interrogation

L'interrogation désigne le processus par lequel un membre de groupe de routage demande au maître du groupe des informations de routage à jour. La figure 15.14 illustre l'interrogation du maître par le membre toutes les 5 minutes. Notez la valeur de temps associée à chaque trame (la capture a été enregistrée avec un filtre sur les communications effectuées uniquement via le port 691 ; par conséquent, les numéros de trame affichés ne reflètent pas les numéros d'origine).

Trame	Heure	Adr MAC src	Adr MAC dst	Protocole	Description	Autre adr src	Autre adr dst
1	220.66...	005056407A3F	005056405A30	TCP	Control Bits: .AP..., len: 24, seq:157975...	RG Member	RGM
2	220.85...	005056405A30	005056407A3F	TCP	Control Bits: .A...., len: 0, seq:200374...	RGM	RG Member
3	521.08...	005056407A3F	005056405A30	TCP	Control Bits: .AP..., len: 24, seq:157975...	RG Member	RGM
4	521.28...	005056405A30	005056407A3F	TCP	Control Bits: .A...., len: 0, seq:200374...	RGM	RG Member
5	821.02...	005056407A3F	005056405A30	TCP	Control Bits: .AP..., len: 24, seq:157975...	RG Member	RGM
6	821.12...	005056405A30	005056407A3F	TCP	Control Bits: .A...., len: 0, seq:200374...	RGM	RG Member
7	1120.9...	005056407A3F	005056405A30	TCP	Control Bits: .AP..., len: 24, seq:157975...	RG Member	RGM
8	1121.1...	005056405A30	005056407A3F	TCP	Control Bits: .A...., len: 0, seq:200374...	RGM	RG Member
9	1420.9...	005056407A3F	005056405A30	TCP	Control Bits: .AP..., len: 24, seq:157975...	RG Member	RGM
10	1421.0...	005056405A30	005056407A3F	TCP	Control Bits: .A...., len: 0, seq:200374...	RGM	RG Member
11	1720.7...	005056407A3F	005056405A30	TCP	Control Bits: .AP..., len: 24, seq:157975...	RG Member	RGM
12	1720.8...	005056405A30	005056407A3F	TCP	Control Bits: .A...., len: 0, seq:200374...	RGM	RG Member

Figure 15.14 Interrogation du maître par le membre du groupe de routage

Chaque échange effectué entre deux trames comprend le texte « Simple_Poll » provenant du membre et une réponse du maître du groupe de routage. La trame 1 illustre la requête (figure 15.15).

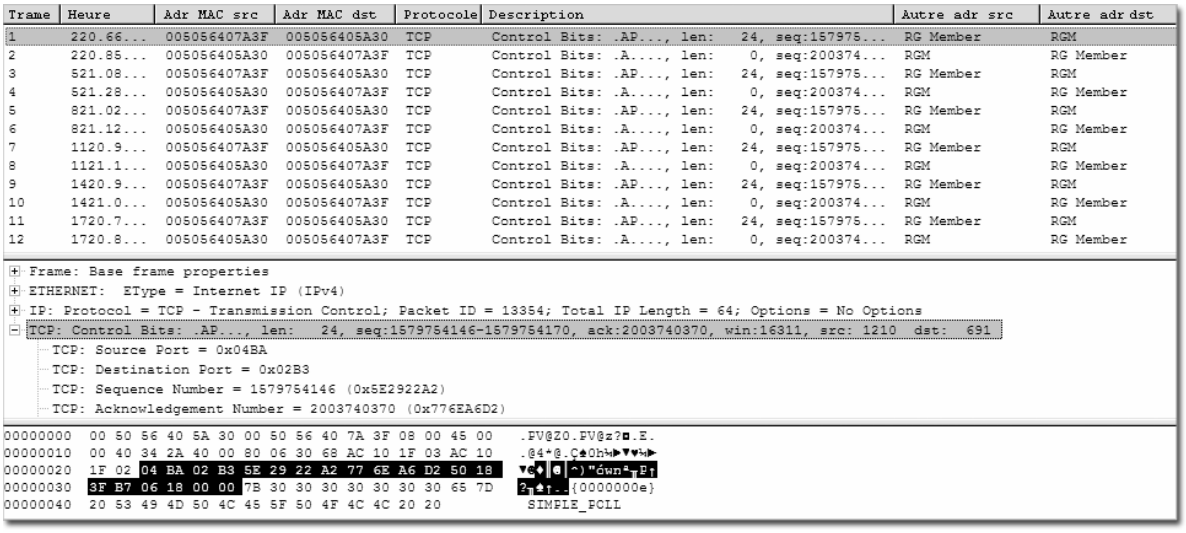


Figure 15.15 Requête du membre adressée au maître du groupe de routage

La trame 2 illustre la réponse (figure 15.16).

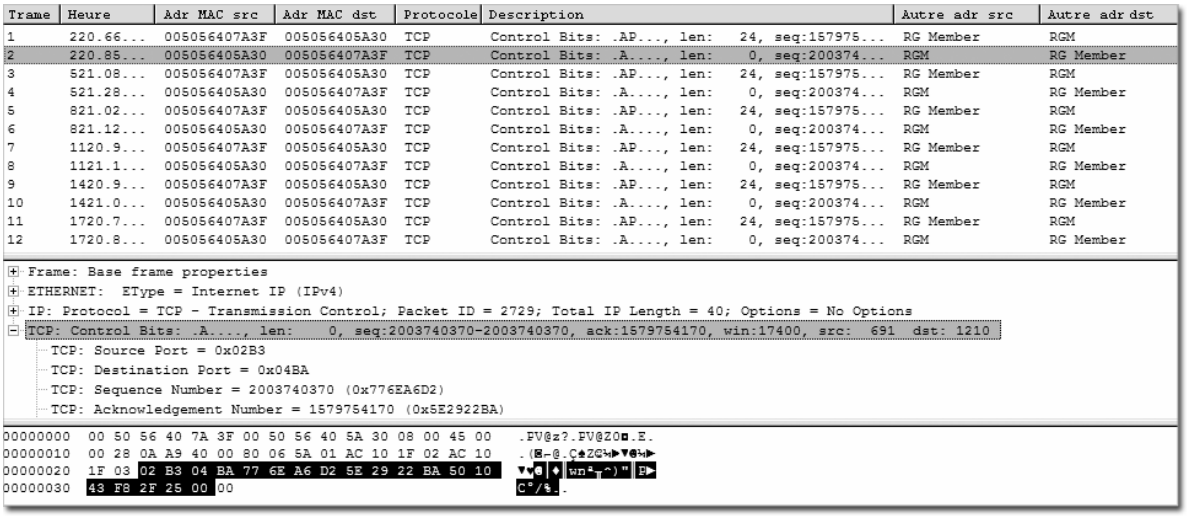


Figure 15.16 Réponse du maître au membre du groupe de routage

Outre la mise à jour du groupe de routage local, le maître doit mettre à jour les autres membres de l'organisation Exchange. Le service SMTP d'Exchange permet d'effectuer les mises à jour entre les groupes de routage.

Communication des mises à jour dans une conversation SMTP

Les communications sur la mise à jour du routage et de l'état des liaisons font partie du service SMTP d'Exchange Server 2003 et d'Exchange 2000. Le service SMTP d'Exchange compare les versions du paquet OrgInfo sur chaque serveur au cours de chaque session SMTP entre deux serveurs. Le fait qu'il s'agisse d'une mise à jour entre des groupes de routage ou à l'intérieur des groupes de routage n'a aucune conséquence sur ce processus. Le processus fonctionne de la manière suivante :

1. Le serveur 1 lance la session TCP et contacte le serveur 2 à l'aide de SMTP. Le serveur 2 envoie une réponse « 220 Ready » (220 Prêt) au serveur 1.
2. Le serveur 1 envoie la commande EHLO.
3. Le serveur 2 répond par « 250 » et une liste de ses commandes ESMTP implémentées.
4. Le serveur 1 répond par « X-EXPS GSS API », ce qui indique qu'il souhaite s'authentifier par le biais de GSS API.
5. Le serveur 2 répond par « 334 GSSAPI supported » (334 GSSAPI non pris en charge).
6. Les trames suivantes concernent l'authentification entre les deux serveurs qui se termine par la réponse du serveur 2 « 235 2.7.0 Authentication successful » (235 2.7.0 Authentification réussie).
7. Les communications sur l'état des liaisons commencent après cette réponse.
8. Le serveur 1 envoie les informations illustrées à la figure 15.17 au serveur 2 :

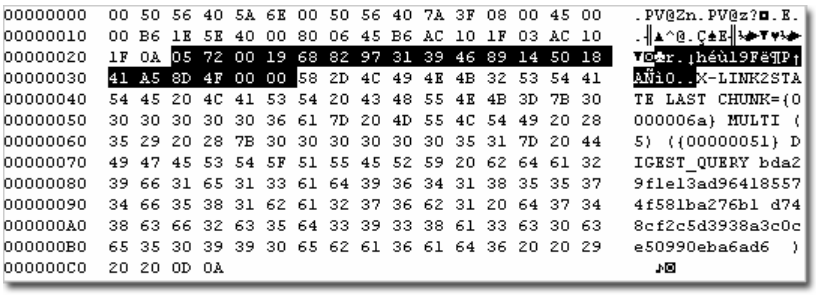


Figure 15.17 Informations envoyées du serveur 1 vers le serveur 2

Les informations suivantes figurent dans celles envoyées à partir du serveur 1 :

- X-LINK2STATE indique que ce paquet contient des informations qui se rapportent à la topologie de routage de l'organisation.
- LAST CHUNK indique qu'il s'agit de la dernière trame des communications sur l'état des liaisons de la session SMTP en cours. Les autres options relatives à cette commande sont :
  - FIRST CHUNK Indique que les informations sur l'état des liaisons à suivre sont réparties sur plusieurs trames, celle-ci étant la première.
  - NEXT CHUNK Indique que les informations sur l'état des liaisons à suivre sont réparties sur plusieurs trames, celle-ci n'étant ni la première ni la dernière.
- DIGEST_QUERY indique que le serveur demande le hachage MD5 du paquet OrgInfo sur le serveur tête de pont distant.
- Le premier GUID à la suite de DIGEST_QUERY est celui du nom de l'organisation Exchange.
- Le second GUID est le hachage MD5 du paquet OrgInfo sur le serveur tête de pont local.

9. Le serveur 2 compare maintenant son hachage MD5 à celui que le serveur 1 a envoyé et l'une des deux actions suivantes se produit :
   - Si les hachages sont identiques, le serveur 2 n'a pas besoin de recevoir tout le paquet OrgInfo du serveur 1. Par conséquent, il envoie une réponse « DONE_RESPONSE » (figure 15.18) et le serveur 1 envoie la commande « MAIL FROM: », puis termine le processus d'envoi du message électronique.

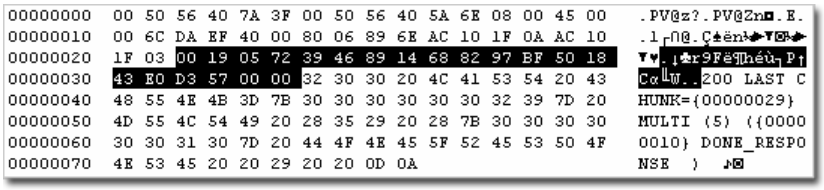


Figure 15.18 Message « Done_Response » envoyé du serveur 2 vers le serveur 1

- Si le hachage du serveur 2 est différent de celui du serveur 1, le serveur 2 envoie tout le paquet OrgInfo vers le serveur 1 lors d'un processus similaire à celui par lequel le serveur 1 a envoyé ses informations vers le serveur 2. La section suivante décrit ce processus dans le contexte des mises à jour entre des groupes de routage.

Mises à jour entre des groupes de routage

Lorsqu'une mise à jour majeure ou mineure a lieu au sein d'un groupe de routage, les serveurs têtes de pont locaux qui sont connectés à d'autres groupes de routage propagent la mise à jour vers leurs groupes de routage associés via SMTP sur le port TCP 25.

Les trames 485 à 487 (figure 15.19) contiennent l'intégralité du paquet OrgInfo transmis du maître au membre du groupe de routage qui est le serveur tête de pont local. La trame 488 illustre l'accusé de réception du serveur tête de pont local.

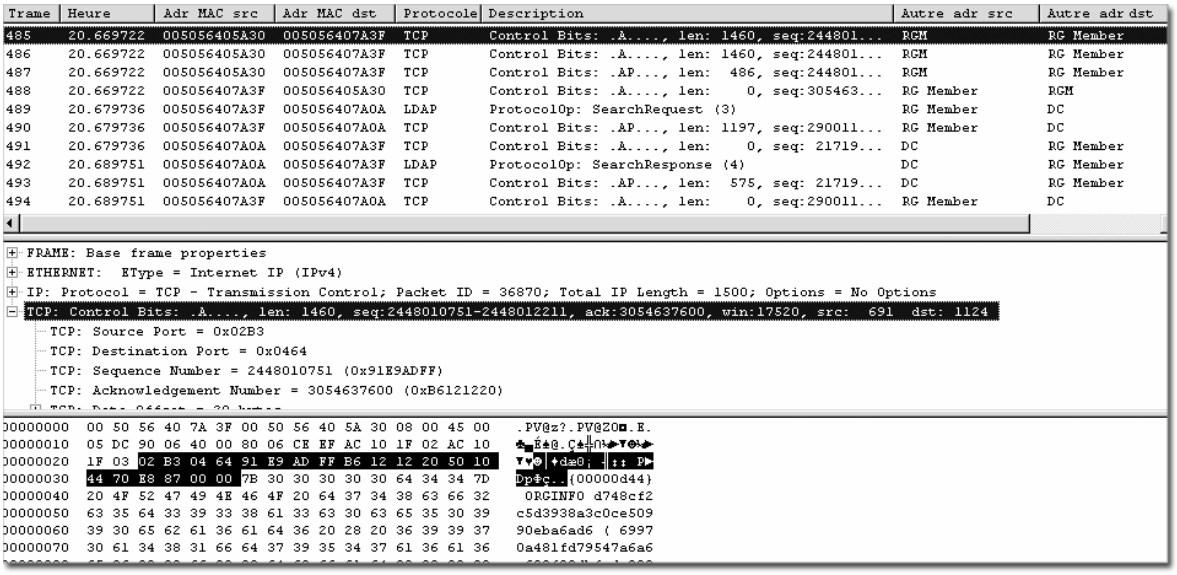


Figure 15.19 Transmission du paquet OrgInfo du maître au membre du groupe de routage qui est le serveur tête de pont local

Dans les trames 489 et 490 (figure 15.20), le serveur tête de pont local demande à Active Directory les attributs de la stratégie de destinataire par défaut, qui est la seule stratégie de destinataire qui existait dans l'exemple d'environnement.

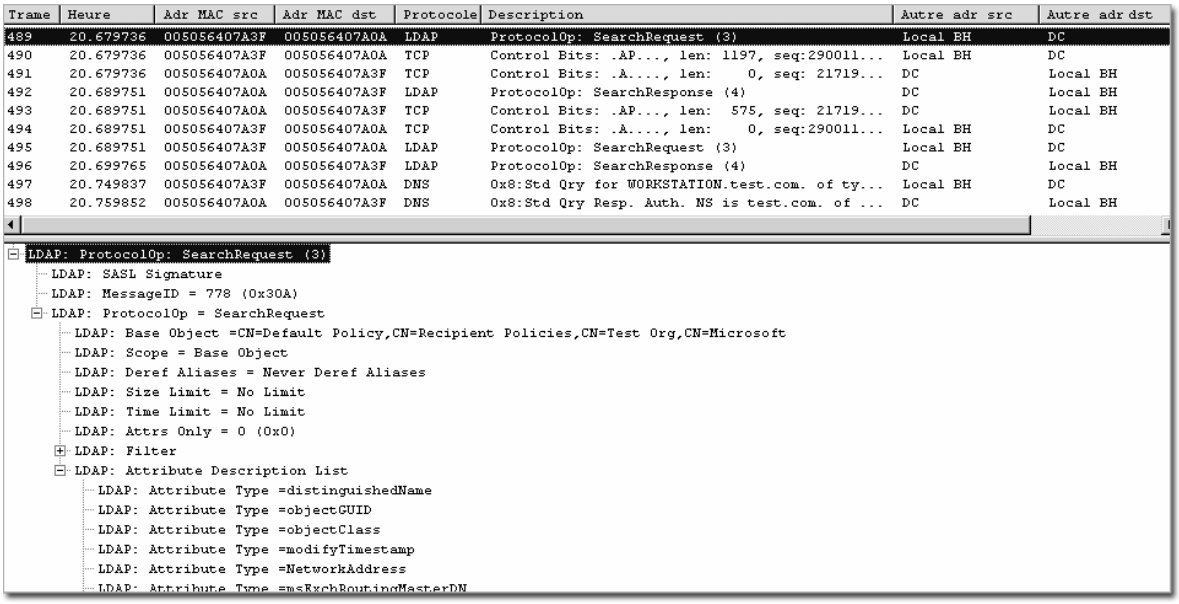
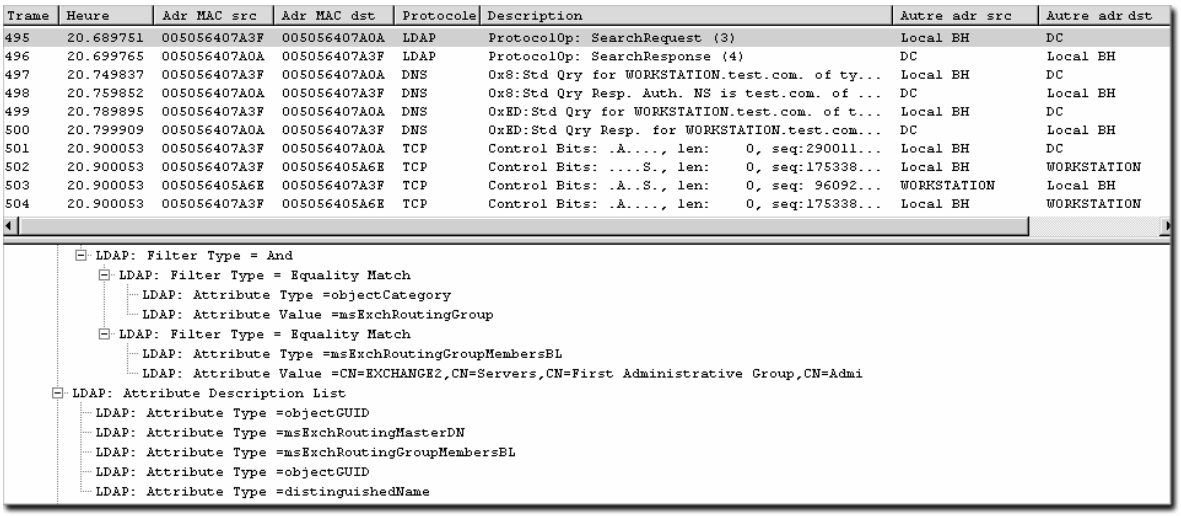


Figure 15.20 Requête du serveur tête de pont local adressée à Active Directory

Après avoir reçu les réponses dans les trames 491 à 494, la trame 495 (figure 15.21) illustre le serveur tête de pont local qui exécute à présent une recherche dans la sous-arborescence du conteneur de configuration pour tout groupe de routage duquel il est serveur tête de pont (notez la ligne « LDAP: Type de filtre »).



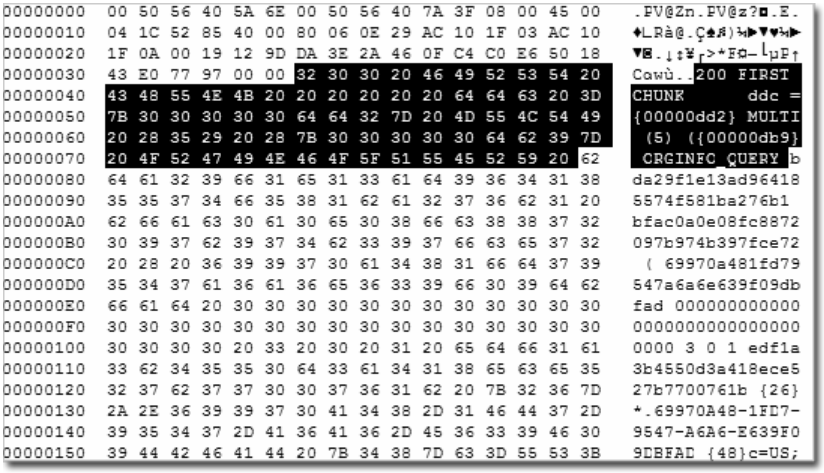
Trame	Heure	Adr MAC src	Adr MAC dst	Protocole	Description	Autre adr src	Autre adr dst
495	20.689751	005056407A3F	005056407A0A	LDAP	Protocol0p: SearchRequest (3)	Local BH	DC
496	20.699765	005056407A0A	005056407A3F	LDAP	Protocol0p: SearchResponse (4)	DC	Local BH
497	20.749837	005056407A3F	005056407A0A	DNS	0x8:Std Qry for WORKSTATION.test.com. of ty...	Local BH	DC
498	20.759852	005056407A0A	005056407A3F	DNS	0x8:Std Qry Resp. Auth. NS is test.com. of ...	DC	Local BH
499	20.789895	005056407A3F	005056407A0A	DNS	0xED:Std Qry for WORKSTATION.test.com. of t...	Local BH	DC
500	20.799909	005056407A0A	005056407A3F	DNS	0xED:Std Qry Resp. for WORKSTATION.test.com...	DC	Local BH
501	20.900053	005056407A3F	005056407A0A	TCP	Control Bits: .A....., len: 0, seq:290011...	Local BH	DC
502	20.900053	005056407A3F	005056405A6E	TCP	Control Bits: ....S., len: 0, seq:175338...	Local BH	WORKSTATION
503	20.900053	005056405A6E	005056407A3F	TCP	Control Bits: .A..S., len: 0, seq: 96092...	WORKSTATION	Local BH
504	20.900053	005056407A3F	005056405A6E	TCP	Control Bits: .A....., len: 0, seq:175338...	Local BH	WORKSTATION

Figure 15.21 Recherche par le serveur tête de pont local des groupes de routage desquels il est serveur tête de pont

Après avoir reçu la réponse, le serveur tête de pont local commence à interroger DNS pour le serveur Exchange dans le groupe de routage distant et configure une session TCP avec ce serveur tête de pont distant.

Le serveur tête de pont local suit la procédure décrite dans la section « Communication des mises à jour dans une conversation SMTP », plus haut dans ce chapitre. Le processus est le suivant :

1. Lorsque les serveurs comparent les hachages MD5, le serveur tête de pont distant réalise qu'il n'a pas le même hachage que le serveur tête de pont local et envoie l'intégralité du paquet OrgInfo à ce dernier. Dans la mesure où cette communication s'effectue à l'aide de SMTP et que les RFC (Request For Comments) SMTP stipulent que toute commande de données SMTP ne peut pas avoir une taille supérieure à 1 Ko, il est probable que le paquet OrgInfo sera réparti en plusieurs trames. Dans ce cas, le service SMTP utilise les différentes commandes CHUNK illustrées à la figure 15.22.



```
00000000  00 50 56 40 5A 6E 00 50 56 40 7A 3F 08 00 45 00   .PV@Zn.PV@z?◘.E.
00000010  04 1C 52 85 40 00 80 06 0E 29 AC 10 1F 03 AC 10   ♦LRà@.Ç♠♯)¼►▼♥¼►
00000020  1F 0A 00 19 12 9D DA 3E 2A 46 0F C4 C0 E6 50 18   ▼◙.↓↕¥┌>*F☼─└µP↑
00000030  43 E0 77 97 00 00 32 30 30 20 46 49 52 53 54 20   Cαwù..200 FIRST
00000040  43 48 55 4E 4B 20 20 20 20 20 20 64 64 63 20 3D   CHUNK      ddc =
00000050  7B 30 30 30 30 30 64 64 32 7D 20 4D 55 4C 54 49   {00000dd2} MULTI
00000060  20 28 35 29 20 28 7B 30 30 30 30 30 64 62 39 7D    (5) ({00000db9}
00000070  20 4F 52 47 49 4E 46 4F 5F 51 55 45 52 59 20 62    ORGINFO_QUERY b
00000080  64 61 32 39 66 31 65 31 33 61 64 39 36 34 31 38   da29f1e13ad96418
00000090  35 35 37 34 66 35 38 31 62 61 32 37 36 62 31 20   5574f581ba276b1
000000A0  62 66 61 63 30 61 30 65 30 38 66 63 38 38 37 32   bfac0a0e08fc8872
000000B0  30 39 37 62 39 37 34 62 33 39 37 66 63 65 37 32   097b974b397fce72
000000C0  20 28 20 36 39 39 37 30 61 34 38 31 66 64 37 39    ( 69970a481fd79
000000D0  35 34 37 61 36 61 36 65 36 33 39 66 30 39 64 62   547a6a6e639f09db
000000E0  66 61 64 20 30 30 30 30 30 30 30 30 30 30 30 30   fad 00000000000
000000F0  30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
00000100  30 30 30 30 20 33 20 30 20 31 20 65 64 66 31 61   0000 3 0 1 edf1a
00000110  33 62 34 35 35 30 64 33 61 34 31 38 65 63 65 35   3b4550d3a418ece5
00000120  32 37 62 37 37 30 30 37 36 31 62 20 7B 32 36 7D   27b7700761b {26}
00000130  2A 2E 36 39 39 37 30 41 34 38 2D 31 46 44 37 2D   *.69970A48-1FD7-
00000140  39 35 34 37 2D 41 36 41 36 2D 45 36 33 39 46 30   9547-A6A6-E639F0
00000150  39 44 42 46 41 44 20 7B 34 38 7D 63 3D 55 53 3B   9DBFAD {48}c=US;
```

Figure 15.22 Utilisation de la commande FIRST_CHUNK

2. Le serveur tête de pont local répond par « X-LINK2STATE MORE » (figure 15.23).

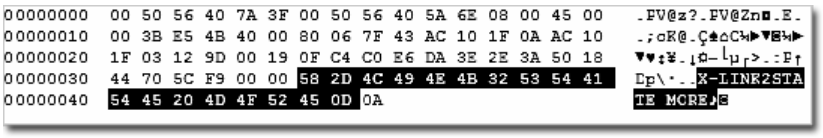


Figure 15.23 Réponse du serveur tête de pont local au serveur tête de pont distant

3. Le serveur tête de pont distant envoie la partie suivante du paquet OrgInfo (figure 15.24). Notez qu'il indique uniquement « CHUNK » :

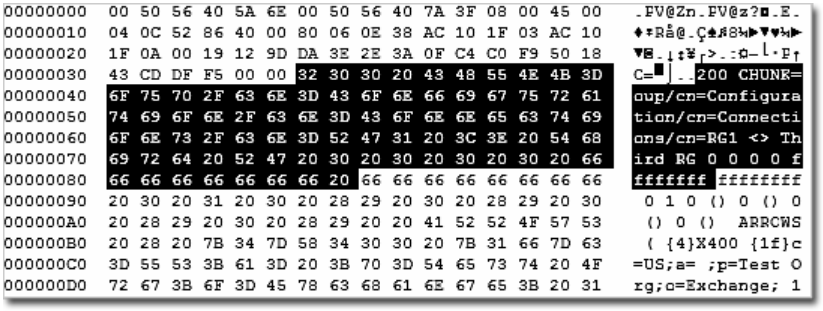


Figure 15.24 Réponse du serveur tête de pont distant au serveur tête de pont local

4. Le serveur tête de pont distant répond à nouveau par « X-LINK2STATE MORE ». Cette communication se poursuit jusqu'à ce que le serveur tête de pont distant envoie la dernière partie du paquet OrgInfo, qu'il signale à l'aide de la commande LAST_CHUNK (figure 15.25).

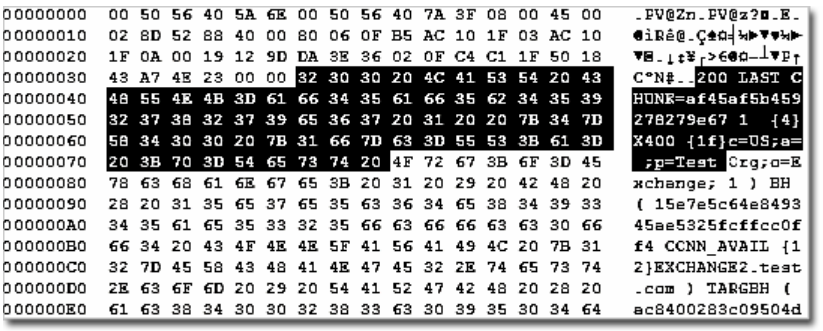


Figure 15.25 Le serveur tête de pont distant signale à l'aide de la commande LAST_CHUNK qu'il envoie la dernière partie du paquet OrgInfo

5. Une fois ce processus de communication terminé, les serveurs têtes de pont distant et local inversent les rôles. Une fois qu'il a reçu la trame LAST_CHUNK du serveur tête de pont distant, le serveur tête de pont local envoie immédiatement une trame FIRST_CHUNK (qui identifie le début de la transmission du paquet OrgInfo) au serveur tête de pont distant.

6. Après avoir effectué le même processus pour l'échange des informations OrgInfo, le serveur tête de pont distant répond par une commande « 200 Done » (200 Terminé) (figure 15.26) lorsqu'il a reçu la commande LAST_CHUNK.

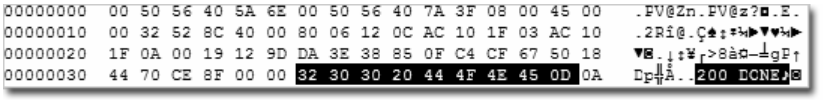


Figure 15.26 Le serveur tête de pont distant indique qu'il a reçu le paquet OrgInfo dans son intégralité

7. Le serveur tête de pont local émet à présent la commande « Quit » et le serveur tête de pont distant en accuse réception en fermant le canal de transmission SMTP.

Annexes

Référence

Cette annexe contient des documents de référence sur les sujets suivants :

- Commandes SMTP (Simple Mail Transfer Protocol)
- Mécanismes de transport SMTP internes
- Récepteurs d'événements SMTP
- Ports couramment utilisés par Microsoft® Exchange

Commandes SMTP

Le tableau A.1 répertorie les commandes SMTP fournies par le service SMTP (SMTPSVC) de Microsoft Windows®.

Tableau A.1 Commandes SMTP

Commande SMTP	Fonction de la commande
HELO	Envoyée par un client pour s'identifier, généralement avec un nom de domaine.
EHLO	Permet au serveur d'identifier sa prise en charge des commandes ESMTP (Extended Simple Mail Transfer Protocol).
MAIL FROM	Identifie l'expéditeur du message ; utilisée sous la forme MAIL FROM:.
RCPT TO	Identifie les destinataires du message ; utilisée sous la forme RCPT TO:.
TURN	Permet au client et au serveur d'inverser les rôles et d'envoyer des messages dans l'autre sens sans avoir à établir une nouvelle connexion.
ATRN	La commande ATRN (Authenticated TURN) prend de façon facultative un ou plusieurs domaines comme paramètre. La commande ATRN doit être rejetée si la session n'a pas été authentifiée.
SIZE	Offre un mécanisme par lequel le serveur SMTP peut indiquer la taille maximale des messages prise en charge. Les serveurs compatibles doivent fournir des extensions de taille pour indiquer la taille maximale des messages acceptable. Les clients ne doivent

Commande SMTP	Fonction de la commande
	pas envoyer de messages dont la taille est supérieure à celle spécifiée par le serveur.
ETRN	Extension de SMTP. ETRN est envoyée par un serveur SMTP pour demander à un autre serveur d'envoyer tous les messages électroniques dont il dispose.
PIPELINING	Permet d'envoyer un flux de commandes sans attendre de réponse après chaque commande.
CHUNKING	Commande ESMTP qui remplace la commande DATA. Pour que l'hôte SMTP n'ait pas à rechercher en permanence la fin des données, cette commande envoie une commande BDAT avec un argument qui contient le nombre total d'octets dans un message. Le serveur de réception compte les octets du message et, lorsque la taille du message est égale à la valeur envoyée par la commande BDAT, il considère qu'il a reçu toutes les données du message.
DATA	Envoyée par un client pour lancer le transfert du contenu du message.
DSN	Commande ESMTP qui active les notifications d'état de remise.
RSET	Annule l'intégralité de la transaction des messages et réinitialise le tampon.
VRFY	Vérifie qu'une boîte aux lettres est disponible pour la remise des messages ; par exemple, `vrfy pierre` vérifie qu'une boîte aux lettres pour Pierre se trouve sur le serveur local. Cette commande est désactivée par défaut dans les implémentations Exchange.
HELP	Retourne une liste de commandes prises en charge par le service SMTP.
QUIT	Met fin à la session.

Le tableau A.2 répertorie les commandes ESMTP qu'Exchange met à la disposition du service SMTP.

Tableau A.2 Commandes ESMTP

Commande ESMTP	Fonction de la commande
X-EXPS GSSAPI	Méthode utilisée par les serveurs Microsoft Exchange

Commande ESMTP	Fonction de la commande
	Server 2003 et Exchange 2000 Server pour s'authentifier.
X-EXPS=LOGIN	Méthode utilisée par les serveurs Exchange 2000 et Exchange 2003 pour s'authentifier.
X-EXCH50	Permet de propager les propriétés des messages lors d'une communication de serveur à serveur.
X-LINK2STATE	Ajoute la prise en charge du routage de l'état des liaisons à Exchange.

Récepteurs d'événements

Vous pouvez utiliser les récepteurs d'événements pour étendre et modifier le comportement du service SMTP de Microsoft Windows 2000 Server et Windows Server™ 2003. Exchange 2003 nécessite le service SMTP de Windows 2000 ou Windows Server 2003 pour fonctionner, car la plupart des fonctionnalités de transport dans Exchange 2003 s'exécutent avec cette architecture. Par conséquent, après avoir réinstallé les services Internet (IIS) ou le service SMTP de Windows 2000 ou Windows Server 2003, vous devez également réinstaller Exchange.

Un événement du service SMTP est l'occurrence d'une activité au sein du service SMTP, par exemple la transmission ou la réception d'une commande SMTP, ou le dépôt d'un message dans le composant de transport du service SMTP. Lorsqu'un événement particulier se produit, le service SMTP utilise un répartiteur d'événements pour en avertir les récepteurs d'événements inscrits. Lorsqu'il avertit les récepteurs d'événements, le service SMTP transmet les informations au récepteur sous la forme de références d'objet COM (Component Object Model).

Les deux catégories générales des événements du service SMTP sont les suivantes :

Événements du protocole
Les événements du protocole se produisent lors de la réception ou de la transmission de commandes SMTP via le réseau. Ces événements surviennent dans les cas suivants :

- Un service SMTP client ou un agent utilisateur de messagerie utilise SMTP pour transmettre des messages à remettre au service local.
- Le service SMTP relaye les messages vers d'autres services SMTP.

Événements de transport
Les événements de transport se produisent lorsque le service SMTP reçoit un message qui passe par le transport principal SMTP. Lors de son passage par le transport, le message est classé (examiné et placé dans une catégorie), puis remis à un emplacement de stockage local ou, si cet emplacement n'est pas local, relayé vers une autre destination.

Les événements de transport et du protocole Windows 2000 et Windows Server 2003 par défaut ne sont accessibles que par l'écriture d'objets COM dans Microsoft Visual C++®. Ces événements sont rapides, ne nécessitent pas de traitement supplémentaire et permettent d'accéder aux propriétés des messages de niveau inférieur ; toutefois, ils sont plus complexes à écrire. Pour les petites tâches qui n'exigent pas de performances élevées, vous pouvez utiliser l'événement CDO_OnArrival, que vous pouvez écrire à l'aide de VBScript (Microsoft Visual Basic® Scripting Edition).

Pour plus d'informations sur l'écriture d'un de ces récepteurs d'événements, téléchargez le Kit de développement Platform SDK (http://go.microsoft.com/fwlink/?LinkId=12059) ou consultez l'article technique

du programme de développement MSDN® *Microsoft SMTP Server Events for Windows 2000* (http://go.microsoft.com/fwlink/?LinkId=12279).

Ports couramment utilisés par Exchange

Le tableau A.3 répertorie les ports couramment utilisés par Exchange. Pour plus d'informations sur les ports qui doivent être ouverts en interne ou en externe, consultez le manuel *Using Microsoft Exchange 2000 Front-End Servers* (en anglais) (http://go.microsoft.com/fwlink/?LinkId=12055).

Tableau A.3 Ports utilisés par Exchange

Protocole	Port	Description
SMTP	TCP: 25	Le service SMTP utilise le port TCP 25.
DNS	TCP/UDP: 53	DNS écoute sur le port 53. Les contrôleurs de domaine l'utilisent.
LSA	TCP: 691	Le service du moteur de routage Microsoft Exchange (RESvc) écoute les informations de routage sur l'état des liaisons sur ce port.
LDAP	TCP/UPD: 389	Le protocole LDAP (Lightweight Directory Access Protocol) utilisé par le service d'annuaire Microsoft Active Directory®, le Connecteur Active Directory et l'annuaire Microsoft Exchange Server 5.5 utilisent ce port.
LDAP/SSL	TCP/UDP: 636	LDAP sur SSL (Secure Sockets Layer) utilise ce port.
LDAP	TCP/UDP: 379	Le service de réplication de sites utilise ce port.
LDAP	TCP/UDP: 390	Il s'agit de l'autre port conseillé pour configurer le protocole LDAP Exchange Server 5.5 lorsqu'Exchange Server 5.5 fonctionne sur un contrôleur de domaine Active Directory.
LDAP	TCP: 3268	Catalogue global. Le catalogue global Active Directory Windows 2000 et Windows Server 2003 (« rôle » d'un contrôleur de domaine) écoute sur le port TCP 3268.
LDAP/SSLPort	TCP: 3269	Catalogue global sur SSL. Les applications qui se connectent au port TCP 3269 d'un serveur de catalogue global peuvent échanger des données cryptées SSL.
IMAP4	TCP: 143	Le protocole IMAP (Internet Message Access Protocol) utilise ce port.
IMAP4/SSL	TCP: 993	IMAP4 sur SSL utilise ce port.

Protocole	Port	Description
POP3	TCP: 110	Le protocole POP3 (Post Office Protocol version 3) utilise ce port.
POP3/SSL	TCP: 995	POP3 sur SSL utilise ce port.
NNTP	TCP: 119	Le protocole NNTP (Network News Transfer Protocol) utilise ce port.
NNTP/SSL	TCP: 563	NNTP sur SSL utilise ce port.
HTTP	TCP: 80	HTTP utilise ce port.
HTTP/SSL	TCP: 443	HTTP sur SSL utilise ce port.

Ressources mentionnées dans ce guide

Exchange Server 2003

Articles de la Base de connaissances Microsoft

- 823175, « Fine-Tuning and Known Issues When You Use the Urlscan Utility in an Exchange 2003 Environment » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=823175)
- 260973, « XCON : Configuration des domaines SMTP pour le courrier entrant et relayé dans Exchange 2000 Server » (http://support.microsoft.com/default.aspx?scid=kb;fr;260973)

Exchange 2000 Server

Articles de la Base de connaissances Microsoft

- 315591, « XCON: Authoritative and Non-Authoritative Domains in Exchange 2000 » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=315591)
- 278339, « XGEN : Ports TCP/UDP utilisés par Exchange 2000 Server » (http://support.microsoft.com/default.aspx?scid=kb;fr;278339)
- 255253, « XADM: How to Perform a Dump of a Container or Object in Exchange 2000 » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=255253)
- 271201, « XADM: Alternative Methods to Obtain a Dump of an Object » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=271201)
- 253827, « How Exchange Hides Group Membership in Active Directory » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=253827)
- 294736, « When to Create SMTP Connectors in Exchange 2000 » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=294736)
- 319759, « How to Configure Exchange to Forward Messages to a Foreign Messaging System That Shares the Same SMTP Domain Name Space » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=319759)
- 288175, « XCON: Recipient Policy Cannot Match the FQDN of Any Server in the Organization, 5.4.8 NDRs » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=288175)
- 304897, « XIMS : Les serveurs Microsoft SMTP peuvent sembler accepter et relayer les messages électroniques dans les tests tiers » (http://support.microsoft.com/default.aspx?scid=kb;fr;304897)
- 316047, « XADM: Addressing Problems That Are Created When You Enable ADC-Generated Accounts » (en anglais) ().

- 262162, « XADM: Using the Message Tracking Center to Track a Message » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=262162)
- 272593, « XCON: Le message génère un rapport de non-remise lorsqu'il est envoyé à un destinataire Windows NT Server 4.0 présenté comme un contact dans Active Directory » (http://support.microsoft.com/default.aspx?scid=kb;fr;272593)
- 250570, « XCON: Directory Service Server Detection and DSAccess Usage » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=250570)
- 316047, « XADM: Addressing Problems That Are Created When You Enable ADC-Generated Accounts » (en anglais) (http://go.microsoft.com/fwlink/?linkid=3052&kbid=316047)
- 296232, « XCCC : Empty Inbox When Using Internet Explorer 5 and Later to Gain Access to OWA » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=296232)

Articles techniques

- « Microsoft Internet Security & Acceleration Server: Configuring and Securing Exchange 2000 Server and Clients » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=10733)

Windows 2000 Server

Articles de la Base de connaissances Microsoft

- 293800, « XCON: How to Set Up Windows 2000 as a SMTP Relay Server or Smart Host » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=293800)
- 298448, « Ressources techniques et informations sur le serveur DNS Windows 2000 et Active Directory » (http://support.microsoft.com/default.aspx?scid=kb;fr;298448)

Registre Windows

Articles de la Base de connaissances Microsoft

- 256986, « Description du Registre de Microsoft Windows » (http://support.microsoft.com/default.aspx?scid=kb;fr;256986)

Assistant IIS Lockdown

Sites Web

- Assistant IIS Lockdown à partir du Centre de téléchargement Microsoft (http://go.microsoft.com/fwlink/?LinkId=12281)

Articles de la Base de connaissances Microsoft

- 309508, « XCCC : Configurations des outils IIS Lockdown et URLscan dans un environnement Exchange » (http://support.microsoft.com/default.aspx?scid=kb;fr;309508)

- 317052, « COMMENT FAIRE : Annuler des modifications effectuées par l'Assistant IIS Lockdown » (http://support.microsoft.com/default.aspx?scid=kb;fr;317052)

Autres sites Web

- Service des bulletins de sécurité et des correctifs à l'adresse (http://www.microsoft.com/technet/security/current.aspx)
- Microsoft Developer Network (MSDN®) (http://msdn.microsoft.com/)
- Outil de résolution DNS à l'adresse (http://go.microsoft.com/fwlink/?LinkId=25097)

Ressources supplémentaires

Outre les ressources citées dans ce guide, les ressources mentionnées ci-après peuvent vous apporter une aide précieuse pour votre mise en œuvre de Microsoft® Exchange Server 2003.

Sites Web

- Bibliothèque technique de Microsoft Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=21277)
- Outils et mises à jour Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=25097)
- Site Web de sécurité Microsoft (http://go.microsoft.com/fwlink/?linkid=21633)
- Site Web de sécurité TechNet (http://go.microsoft.com/fwlink/?LinkID=5936)
- Page d'accueil des Kits de ressources et de déploiement Microsoft Windows (http://go.microsoft.com/fwlink/?LinkId=25196)

Guides d'Exchange Server 2003

- *Exchange Server 2003 Glossary* (http://go.microsoft.com/fwlink/?LinkId=24625)
- Nouveautés dans Exchange Server 2003 (http://go.microsoft.com/fwlink/?linkid=21765)
- *Guide de déploiement de Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=21768)
- *Planification d'un système de messagerie Microsoft Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=21766)
- *Guide d'administration d'Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=21769)
- *Guide de sécurité des messages Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=23216)

- *Guide sur le renforcement de la sécurité d'Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=25210)

Kits de ressources et de déploiement

- *Kit de ressources Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?LinkId=12058)

  Remarque Vous pouvez commander un exemplaire du *Kit de ressources Microsoft Exchange 2000 Server* auprès de Microsoft Press® à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=6544.

- *Kit de Ressources Techniques Microsoft Windows 2000 Server* (http://go.microsoft.com/fwlink/?LinkId=6545)

  Remarque Vous pouvez commander un exemplaire du *Kit de Ressources Techniques Microsoft Windows 2000 Server* auprès de Microsoft Press® à l'adresse suivante : .

- *Outils du Kit de Ressources Techniques Microsoft Windows 2003 Server* (http://go.microsoft.com/fwlink/?LinkId=16721)
- *Kit de déploiement Microsoft Windows 2003 Server* (http://go.microsoft.com/fwlink/?LinkId=25197)

Accessibilité pour les personnes atteintes de handicaps

Microsoft s'engage à rendre l'utilisation de ses produits et services facile pour chacun. Cette annexe fournit des informations sur les fonctionnalités, produits et services qui facilitent l'accès à la famille Microsoft® Windows Server™ 2003, la famille Windows® 2000 Server, Microsoft Exchange Server 2003 et Microsoft Office Outlook Web Access® 2003 pour les personnes présentant une incapacité physique. Elle comprend les rubriques suivantes :

- Accessibilité dans Microsoft Windows
- Ajustement des produits Microsoft aux personnes ayant recours aux fonctionnalités d'accessibilité
- Documentation des produits Microsoft dans d'autres formats
- Services Microsoft pour les personnes sourdes ou malentendantes
- Informations spécifiques à Exchange 2003 et Outlook Web Access 2003
- Autres sources d'information pour les personnes atteintes de handicaps

Remarque Les informations décrites dans cette annexe sont uniquement valables si vous avez acquis vos produits Microsoft aux États-Unis. Si vous avez acheté le produit hors des États-Unis, il doit être accompagné d'une fiche d'information indiquant le numéro de téléphone et l'adresse des services de support technique de Microsoft. Contactez votre revendeur pour savoir si les types de produits et services décrits dans cette annexe sont disponibles dans votre pays. Pour plus d'informations en chinois, anglais, français, italien, japonais, portugais, espagnol (Amérique du Sud) et espagnol (Espagne), consultez le site Web international de Microsoft sur l'accessibilité (http://go.microsoft.com/fwlink/?LinkId=22008).

Accessibilité dans Microsoft Windows

De nombreuses fonctionnalités d'accessibilité ont été intégrées au système d'exploitation Windows, dès l'introduction de Windows 95. Ces fonctionnalités sont utiles pour les personnes ayant des difficultés à utiliser un clavier ou une souris, les personnes aveugles ou malvoyantes, sourdes ou malentendantes. Les fonctionnalités peuvent être installées pendant l'installation.

Pour plus d'informations sur les fonctionnalités d'accessibilité des différents systèmes d'exploitation Windows, consultez le site Web sur l'accessibilité aux produits Microsoft (http://www.microsoft.com/france/accessibilite/default.asp).

Fichiers d'accessibilité à télécharger

Si vous disposez d'un modem ou d'une connexion réseau, vous pouvez télécharger les fichiers d'accessibilité à partir des services réseau suivants :

- Site Web de Microsoft sur l'accessibilité (http://www.microsoft.com/france/accessibilite/default.asp).
- Site Web de Microsoft sur l'aide et le support technique : http://support.microsoft.com/default.aspx?ln=FR. Sélectionnez l'option de recherche par numéro d'article dans la Base de connaissances, tapez **165486** dans la zone de recherche, puis cliquez sur la flèche. La recherche affiche un lien vers l'article de la Base de connaissances intitulé « Personnalisation de Windows

pour les personnes handicapées », qui contient des liens vers les documents relatifs à la personnalisation des différentes versions de Microsoft Windows.

Pour obtenir d'autres articles relatifs à l'accessibilité, sur le site Web d'aide et de support Microsoft, sélectionnez l'option **Rechercher dans KB française**, sélectionnez **Tous les produits Microsoft**, puis dans la zone **Recherche de**, tapez **kbenable** et cliquez sur **Rechercher**.

- Microsoft Internet Server à l'adresse ftp://ftp.microsoft.com/, dans softlib/MSLFILES.
- Service de téléchargement Microsoft (MSDL, *Microsoft Download Service*), que vous pouvez contacter en composant le (425) 936 67 35 aux États-Unis ou le (905) 507 30 22 au Canada. Le service MSDL est accessible directement par modem 24 heures sur 24, 365 jours par an. En dehors des États-Unis et du Canada, contactez votre filiale Microsoft pour plus d'informations.

  Remarque Le service MSDL prend en charge les vitesses de transmission à 1 200, 2 400, 9 600 ou 14 400 bauds sans parité, avec 8 bits de données et 1 bit d'arrêt. Le service de téléchargement Microsoft ne prend pas en charge les connexions à 28,8 Kbits/s, à 56 Kbits/s ou les connexions RNIS.

Ajustement des produits Microsoft aux personnes ayant recours aux fonctionnalités d'accessibilité

Des options et fonctionnalités d'accessibilité sont intégrées dans un grand nombre de produits Microsoft, y compris le système d'exploitation Windows. Ces options et fonctionnalités sont destinées aux personnes ayant des difficultés à utiliser un clavier ou une souris, aux aveugles et aux malvoyants ou aux sourds et aux malentendants.

Guides étape par étape gratuits

Microsoft offre une série de guides étape par étape pour vous aider à apprendre comment ajuster les paramètres et les options d'accessibilité de votre ordinateur. Les guides gratuits fournissent des procédures détaillées sur la façon de régler les options, fonctionnalités et paramètres pour répondre à vos besoins d'accessibilité. Les informations qui indiquent comment utiliser la souris, le clavier ou les deux sont présentées en vis-à-vis pour faciliter l'apprentissage.

Pour accéder aux derniers guides étape par étape, consultez la page de présentation générale des guides étape par étape du site sur l'accessibilité de Microsoft (http://go.microsoft.com/fwlink/?LinkId=14899).

Technologies d'aide informatiques pour Windows

Il existe des technologies d'aide informatiques très variées pour permettre aux personnes souffrant de handicaps d'utiliser leurs ordinateurs plus facilement.

Microsoft fournit un catalogue permettant de rechercher les technologies d'aide informatiques fonctionnant sur les systèmes d'exploitation Windows ; vous pouvez y accéder à partir de la page de présentation des technologies d'aide informatiques (http://www.microsoft.com/france/accessibilite/handicap/technologies/default.asp).

À titre d'exemple, les produits disponibles pour les systèmes d'exploitation MS-DOS®, Windows et Windows NT sont les suivants :

- Programmes qui décrivent les informations affichées à l'écran en braille ou qui fournissent un synthétiseur vocal aux personnes aveugles ou ayant des difficultés à lire.
- Outils matériels et logiciels qui modifient le comportement de la souris et du clavier.
- Programmes permettant aux personnes d'entrer du texte à l'aide de la souris ou de leur voix.
- Logiciels de saisie prédictive qui permettent aux personnes de taper plus vite en effectuant moins de frappes de touches.
- Dispositifs de saisie alternatifs, tels que des systèmes à commande unique ou commandés par la respiration, pour les personnes qui ne peuvent utiliser ni souris, ni clavier.

Mise à niveau d'un produit basé sur les technologies d'aide informatiques

Si vous utilisez une technologie d'aide informatique, contactez votre agent commercial pour vérifier la compatibilité avec les produits installés sur votre ordinateur avant de procéder à une mise à niveau. Celui-ci peut également vous montrer comment définir vos paramètres pour optimiser la compatibilité avec votre version de Windows ou d'autres produits Microsoft.

Documentation Microsoft dans d'autres formats

La documentation de nombreux produits Microsoft est disponible dans plusieurs formats pour la rendre plus accessible. Les documents relatifs à Exchange 2003 sont également disponibles en tant qu'aide sur le CD-ROM inclus avec le produit et sur le site Web Exchange à l'adresse suivante : http://www.microsoft.com/exchange.

Si vous avez des difficultés pour lire ou pour manipuler une documentation imprimée, vous pouvez obtenir un grand nombre de publications Microsoft auprès de Recording for the Blind & Dyslexic, Inc. (RFB&D). Cette société distribue ces documents dans plusieurs formats, notamment sur cassettes audio et sur CD-ROM, aux personnes inscrites auprès de leur service de diffusion. La collection de Recording for the Blind and Dyslexic contient plus de 90 000 titres, dont la documentation sur les produits Microsoft et les ouvrages de Microsoft Press®. Vous pouvez télécharger de nombreux ouvrages Microsoft à partir du site Web consacré à la documentation d'accessibilité aux produits Microsoft (en anglais) (http://go.microsoft.com/fwlink/?LinkId=22007).

Pour plus d'informations, contactez Recording for the Blind and Dyslexic à l'adresse ou aux numéros de téléphone suivants :

Recording for the Blind & Dyslexic
20 Roszel Road
Princeton, NJ 08540
États-Unis
Téléphone si vous appelez des États-Unis : (866) 732 35 85
Téléphone si vous appelez d'un autre pays que les États-Unis et le Canada : (609) 452 48 00
Télécopie : (609) 987-8116
Web : http://www.rfbd.org/

Il est possible que les adresses Web changent et que vous ne puissiez plus vous connecter au site mentionné ici.

Services Microsoft à l'attention des sourds et malentendants

Si vous êtes sourd ou malentendant, l'accès complet aux services clients et produits Microsoft est disponible via tout périphérique de télécommunication compatible avec le service de type téléphone texte (TTY/TDD).

Service client

Contactez Microsoft Sales Information Center via le service TTY/TTD (téléphone texte) en composant le (800) 892 52 34 entre 06 h 30 et 17 h 30 Pacifique (UTC-8, GMT), du lundi au vendredi, en dehors des périodes de vacances.

Assistance technique

Pour obtenir une assistance technique aux États-Unis, contactez les Services de Support Technique de Microsoft par téléphone texte au (800) 892 52 34 entre 06 h 00 et 18 h 00 Pacifique (UTC-8), du lundi au vendredi, en dehors des périodes de vacances. Au Canada, composez le (905) 568 96 41 entre 8 h 00 et 20 h 00 Est (UTC-5), du lundi au vendredi, en dehors des périodes de vacances. Les services du support technique de Microsoft sont soumis aux tarifs, termes et conditions valables au moment de leur utilisation.

Exchange 2003

La section 508 du « Rehabilitation Act » réglemente la façon dont les agences gouvernementales des États-Unis achètent les technologies électroniques et de l'information. Elle exige des fonctionnaires chargés des achats d'acheter uniquement les technologies électroniques et de l'information accessibles aux personnes handicapées. La section 508 stipule que toute technologie électronique et de l'information développée, obtenue, gérée ou utilisée par des agences fédérales doit être accessible aux personnes handicapées, y compris les employés et membres du public, à moins qu'une charge excessive ne soit imposée à l'agence.

Pour consulter Exchange 2003 Voluntary Product Accessibility Template (VPAT), qui décrit les fonctionnalités d'accessibilité répondant aux normes de la section 508, visitez le site Web http://go.microsoft.com/fwlink/?LinkId=22011 (en anglais).

Outlook Web Access

Il est recommandé aux clients ayant besoin de périphériques d'assistance technique pour interagir avec leurs applications logicielles d'utiliser le client Outlook Web Access de base. Par défaut, le client de base s'affiche dans tous les navigateurs à l'exception de Microsoft Internet Explorer 5.01 à 6.*x*. Toutefois, un administrateur Exchange peut offrir aux utilisateurs de Microsoft Internet Explorer 5.01 à 6.*x* la possibilité de choisir le client de base lors de l'ouverture d'une session sur Outlook Web Access. Pour ce faire, l'administrateur doit utiliser le Gestionnaire système Exchange pour activer l'authentification basée sur des formulaires pour Outlook Web Access. Pour plus d'informations sur l'activation de l'authentification basée sur des formulaires, consultez le *Guide d'administration d'Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=21769).

Les administrateurs ont également la possibilité de définir le client de base comme client par défaut pour tous les navigateurs. Pour plus d'informations sur cette approche, consultez l'article 296232 de la Base de connaissances Microsoft, « XCCC: Empty Inbox When Using Internet Explorer 5 and Later to Gain Access to OWA » (en anglais) (http://go.microsoft.com/fwlink/?LinkId=3052&kbid=296232)

Obtention d'informations complémentaires sur l'accessibilité

Le site Web de Microsoft sur l'accessibilité (http://www.microsoft.com/france/accessibilite/default.asp) fournit des informations aux personnes handicapées, ainsi qu'à leurs amis, aux membres de leur famille, aux personnes appartenant à des organisations de proximité, aux formateurs et aux personnes soutenant leur cause.

Il existe un bulletin d'informations mensuel gratuit pour vous permettre de vous tenir informé sur les sujets traitant de l'accessibilité en rapport avec les produits Microsoft. Pour vous abonner, visitez la page d'abonnement à la lettre de l'accessibilité (http://www.microsoft.com/france/accessibilite/lettre/default.asp).

Ce guide vous a-t-il aidé ? Donnez-nous votre avis. Sur une échelle de 1 (médiocre) à 5 (excellent), quelle note donneriez-vous à ce guide ?

Adressez vos commentaire à : exchdocs@microsoft.com.

Pour obtenir les informations les plus récentes concernant Exchange, visitez les pages Web suivantes (en anglais) :

- Ensemble des articles techniques et guides de l'équipe de développement de Microsoft Exchange
  http://go.microsoft.com/fwlink/?linkid=21277
- Outils et mises à jour Exchange
- Communauté Exchange Server
  http://go.microsoft.com/fwlink/?linkid=14927
- Fichier auto-extractible contenant tous les articles techniques et guides de l'équipe de développement de Microsoft Exchange
  http://go.microsoft.com/fwlink/?LinkId=10687