Microsoft Windows Server System

Guide sur le renforcement de la sécurité d'Exchange Server 2003

Valide jusqu'au :	2 août 2004
Version du produit :	Exchange Server 2003
Révisé par :	Équipe de développement Exchange
Informations récentes :	www.microsoft.com/exchange/library
Auteurs :	Michael Grimm, Michael Nelte

Guide sur le renforcement de la sécurité d'Exchange Server 2003

Auteurs : Michael Grimm, Michael Nelte

Date de publication : février 2004
S'applique à : Exchange Server 2003

Copyright

Remerciements

Éditeur du projet : Brendon Bennett

Rédacteurs ayant offert leur contribution : John Speare, Christopher Budd (CISSP), Janine de Nysschen, Joey Masterson

Réviseurs techniques : Andrew Moss, Alexander MacLeod, Jason Urban, Eric Rosenberg, Giuseppe Di Silvestre

Conception graphique : Kristie Smith, Paul Carew

Production : Joe Orzech, Sean Pohtilla

Introduction

Ce guide est destiné à vous apporter des informations essentielles sur la manière de renforcer votre environnement Microsoft® Exchange Server 2003. En plus des recommandations de configuration pratiques et concrètes, ce guide comprend des stratégies destinées à combattre le courrier indésirable, les virus et les autres menaces externes qui pèsent sur votre système de messagerie Exchange 2003. Si la plupart des administrateurs de serveur peuvent tirer parti de la lecture de ce guide, celui-ci s'adresse en particulier aux administrateurs responsables d'une messagerie Exchange aussi bien au niveau de la boîte aux lettres que de l'architecture.

Ce guide peut être consulté en conjonction avec le *Guide de la sécurité Windows Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21638. Plus particulièrement, un grand nombre des procédures contenues dans ce guide sont directement liées aux recommandations en matière de sécurité présentées dans le *Guide de la sécurité Windows Server 2003*. Par conséquent, avant de mettre en œuvre les procédures présentées dans ce guide, il est recommandé de commencer par la lecture du *Guide de la sécurité Windows Server 2003*.

Portée de ce guide

Ce guide se concentre explicitement sur les opérations nécessaires à la création et à la maintenance d'un environnement sécurisé Exchange 2003.

Ce guide doit s'utiliser dans le cadre de votre stratégie de sécurité globale pour Exchange 2003 plutôt que comme référence exhaustive destinée à la création et à la maintenance d'un environnement sécurisé.

Ce guide fournit en particulier des réponses détaillées aux questions suivantes :

- Quels sont les conseils disponibles permettant de préparer un environnement Exchange 2003 sécurisé ?
- Quels sont les processus efficaces de gestion des correctifs ?
- Quelles mesures anti-virus puis-je déployer ?
- Comment se protéger contre le courrier électronique commercial non sollicité (courrier indésirable), les attaques de refus de service et l'usurpation d'adresse ?
- Quelles sont les mesures recommandées pour renforcer mon infrastructure Microsoft Windows Server™ 2003 ?
- Quelles sont les mesures recommandées pour renforcer mes serveurs frontaux et mes serveurs principaux ?
- Comment organiser la structure de mon service d'annuaire Microsoft Active Directory® pour prendre en charge le déploiement des modèles de sécurité de stratégie de groupes Exchange ?

Avant de commencer

Avant de passer en revue les recommandations en matière de configuration et les stratégies de sécurité présentées dans ce guide, nous vous invitons à vous familiariser avec les ressources suivantes :

Microsoft Operations Framework (MOF)

MOF est un ensemble de méthodes, de principes et de modèles conseillés qui vous apportent une méthodologie d'exploitation. Pour plus d'informations, consultez le site Web MOF à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21640.

Programme Strategic Technology Protection Program (STPP)

L'objectif du programme STPP est d'intégrer les produits, les services et la prise en charge Microsoft qui se concentrent sur la sécurité. Pour plus d'informations, consultez le site Web du programme STPP à l'adresse suivante : http://www.microsoft.com/france/securite/services/stpp.asp.

Confidentialité et sécurité Microsoft

Ce site Web est la source de référence qui centralise l'ensemble des informations en matière de sécurité et de confidentialité à Microsoft. Pour plus d'informations, consultez le site Web sur la confidentialité et la sécurité Microsoft à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21633.

Ressources de sécurité pour Exchange Server 2003

Ce site Web répertorie les ressources spécifiques à Exchange permettant de sécuriser votre environnement. Pour plus d'informations, consultez le site Web sur les ressources de sécurité pour Exchange Server 2003 à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21660.

Sécurisation de votre environnement de messagerie

La messagerie est un service d'une importance stratégique pour la majorité des organisations. Il est donc essentiel de fournir à vos clients des services de messagerie stables et fiables.

Les attaques malveillantes, sous la forme d'un virus, d'un ver ou d'un refus de service constituent un domaine à risque pour le fonctionnement quotidien de votre installation d'Exchange 2003. De même, le courrier électronique commercial non sollicité (courrier indésirable) est désormais suffisamment gênant et élaboré pour représenter une menace pour le fonctionnement des messageries.

Pour vous protéger contre ces intrusions, cette section vous présente les informations suivantes :

- conseils pour la sécurisation du client ;
- processus de gestion des correctifs Exchange 2003 ;
- mesures anti-virus ;
- protection contre le courrier indésirable, notamment les nouvelles fonctionnalités de Microsoft Office Outlook® 2003 et Exchange 2003 qui peuvent aider dans ce domaine ;
- protection contre les attaques de refus de service ;
- protection contre l'usurpation d'adresse.

Sécurisation du client

Comme Exchange 2003 est une application client-serveur distribuée, il est important de tenir compte du client au fur et à mesure de l'élaboration d'un plan de sécurité destiné à votre environnement de messagerie. Les points à prendre en compte concernent en particulier les domaines suivants :

- Dans le cadre de votre stratégie de la gestion des risques, vous devez examiner quels clients sont strictement nécessaires, puis limiter les fonctionnalités Exchange à ces clients. Par exemple, Exchange 2003 ne configure pas tous les services clients lors de l'installation. Pour exécuter des clients POP3 ou IMAP4 dans votre organisation, vous devez d'abord activer ces services dans votre environnement Exchange 2003.
- Assurez-vous que votre plan de gestion des correctifs s'étend au-delà du système d'exploitation sur le bureau du client. Utilisez des versions à jour et corrigées du logiciel client et vérifiez régulièrement les mises à jour de sécurité du client.
- Les utilisateurs jouent un rôle important dans le maintien de la sécurité du client. Vous devez donc sensibiliser vos utilisateurs aux virus de messagerie, les virus canulars, les chaînes de courrier et le courrier indésirable afin de mettre en place des procédures que vos utilisateurs pourront suivre lorsqu'ils rencontrent ce type de courrier.

Gestion des correctifs Exchange 2003

Pour optimiser la sécurité d'Exchange, il est important de vous tenir au courant des derniers correctifs. Vous devez en particulier veiller à ce qu'Exchange 2003 ainsi que le système d'exploitation soient à jour. Si le système d'exploitation est vulnérable, Exchange l'est également.

Microsoft fournit deux utilitaires pour vous permettre de rester au courant des correctifs, des correctifs à chaud et des service packs Microsoft Windows® : Microsoft Network Security Hotfix Checker (Hfnetchk) et Microsoft Baseline Security Analyzer (MBSA). Hfnetchk est un outil qui répertorie les correctifs ayant été appliqués à un ordinateur ; MBSA identifie les erreurs courantes en matière de configuration de la sécurité. Hfnetchk est disponible via l'interface de ligne de commande de MBSA. Ces deux utilitaires sont disponibles en téléchargement sur le site Web Microsoft Baseline Security Analyzer à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=17809.

Assurez-vous également d'être notifié des nouveaux correctifs qui s'appliquent à votre organisation. Pour recevoir ces notifications automatiquement, abonnez-vous aux bulletins de sécurité Microsoft à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21723.

Pour plus d'informations sur les processus de gestion des correctifs Windows Server 2003, consultez le *Guide de la sécurité Windows Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21638.

Mesures anti-virus

Les virus transmis par messages électroniques sont une des menaces les plus importantes qui pèsent sur votre organisation. Les virus de messagerie peuvent attaquer des systèmes informatiques individuels ou l'ensemble de votre environnement de messagerie. Vous devez donc veiller à disposer d'une protection adéquate contre les virus dans votre environnement Exchange 2003.

Les mécanismes les plus efficaces dans la lutte contre les virus consistent à installer des logiciels anti-virus et à s'assurer que les fichiers de signature anti-virus sont à jour. C'est dans cette optique qu'il faut envisager la protection contre les virus au niveau du pare-feu, de la passerelle SMTP (Simple Mail Transfer Protocol), sur chaque serveur Exchange et chaque ordinateur client. Le but d'installer des logiciels anti-virus à chaque destination de la chaîne de livraison des messages est de fournir une protection aussi large que possible pour chaque message. Par exemple, le moteur anti-virus au niveau de la passerelle SMTP utilise un analyseur MIME (Multipurpose Internet Mail Extensions) différent de celui qui est installé sur le serveur Exchange, lui-même différent de l'analyseur utilisé par Outlook ou Outlook Express. Dans le cadre d'une analyse MIME, cela signifie que le fait de disposer d'un analyseur anti-virus (qui utilise l'analyseur MIME natif) à chaque destination optimise la détection des virus possibles. Vous devez en outre envisager l'exécution de logiciels anti-virus provenant de différents fournisseurs dans l'ensemble de votre entreprise.

Une méthode utilisée couramment par les développeurs de virus pour transporter les virus consiste à inclure ces derniers dans une pièce jointe. Dans les cas les plus évidents, un virus peut être distribué en joignant un programme exécutable (.exe) à un message électronique. Dans certains cas, les virus peuvent être distribués en étant incorporé à une macro qui apparaît aux utilisateurs sous la forme d'un document beaucoup plus bénin (par exemple un fichier Word ou Excel). Afin d'offrir une protection contre certains virus, Outlook et Outlook Web Access fournissent les fonctionnalités suivantes de blocage des pièces jointes :

Fonctionnalités de blocage des pièces jointes dans Outlook

Outlook 2002 et les versions ultérieures comprennent une fonctionnalité de blocage des pièces jointes ; cette fonctionnalité (activée par défaut) bloque les types de fichiers les plus courants, comme .exe, .bat et .vbs. Les anciennes versions d'Outlook nécessitent la Mise à jour de sécurité de messagerie Outlook disponible sur le site Web Microsoft Office Online à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24348. Pour des informations sur la configuration des fonctionnalités de blocage des pièces jointes dans Outlook à l'aide d'une stratégie de groupe, consultez le Kit de ressources Microsoft Office 2003 à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24349.

Fonctionnalités de blocage des pièces jointes dans Outlook Web Access

Dans Exchange 2000 Service Pack 2 (SP2), Outlook Web Access introduit la possibilité de bloquer des pièces jointes en fonction du type de fichier et du type MIME. Dans Outlook Web Access pour Exchange 2000 et Microsoft Office® Outlook Web Access 2003, le blocage des pièces jointes est activé par défaut. Grâce à cette configuration par défaut, les utilisateurs peuvent envoyer n'importe quel type de pièces jointes sans recevoir des types de fichiers dangereux tels que des fichiers .exe, .bat et .vbs.

> **Remarque** Dans leurs configurations par défaut, Outlook 2003 et Outlook Web Access 2003 bloquent les mêmes types de pièces jointes.

Dans Outlook Web Access, vous pouvez configurer deux niveaux de blocage des pièces jointes. Ces niveaux correspondent aux différents niveaux de risque posés par les types de fichiers et les types MIME. Outlook Web Access n'autorise pas le téléchargement, quel que soit leur format, des fichiers de niveau 1 ou de types MIME (spécifiés par les attributs **Level1FileTypes** et **Level1MIMETypes** respectivement). Les fichiers de type MIME et de niveau 2 sont moins critiques ; les utilisateurs ne sont pas autorisés à les ouvrir dans Internet Explorer, mais ils peuvent cliquer avec le bouton droit sur le fichier, l'enregistrer sur le disque et l'ouvrir.

Si vous voulez afficher ou modifier des types de fichiers ou des types MIME bloqués dans Outlook Web Access, exécutez la procédure suivante.

> **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 utiles.

Pour afficher ou changer des types de fichiers ou des types MIME bloqués dans Outlook Web Access

1. Démarrez l'Éditeur du Registre (regedit).
2. Accédez à la clé de Registre suivante :
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeWeb\OWA.
3. La valeur **Level1FileTypes** affiche des pièces jointes bloquées ; la valeur **Level1MIMETypes** affiche des types MIME bloqués.

Protection contre le courrier électronique commercial non sollicité (courrier indésirable)

Le courrier électronique commercial non sollicité (courrier indésirable) pose un problème majeur à de nombreuses organisations. Le courrier indésirable s'avère coûteux à bien des égards, qu'il s'agisse aussi bien du temps que l'utilisateur perd à le trier et à le supprimer que le gaspillage de la bande passante et de l'espace de stockage.

Pour le minimiser, vous devez le combattre sur plusieurs fronts. Aussi, pour vous aider à protéger votre environnement Exchange 2003 contre le courrier indésirable, cette section va :

- aborder les méthodes permettant de sensibiliser vos utilisateurs au courrier indésirable ;
- présenter les fonctionnalités sur la protection contre le courrier indésirable dans Outlook 2003 et Outlook Web Access 2003 ;
- expliquer l'infrastructure SCL (Spam Confidence Level) ;
- vous montrer comment restreindre les listes de distribution Exchange 2003 ;
- expliquer les différents types de filtrage applicables dans Exchange 2003.

Sensibilisation des utilisateurs au courrier indésirable

La première mesure dans la lutte contre le courrier indésirable consiste à sensibiliser vos utilisateurs sur la manière de le traiter. En fait, vos utilisateurs représentent probablement la défense la plus importante contre ce type de courrier. Ce courrier résulte le plus souvent de stratégies d'ingénierie visant les utilisateurs et il est important de sensibiliser ces derniers sur la manière de l'éviter. Par exemple, vos utilisateurs peuvent recevoir du courrier indésirable contenant un avertissement de ce type :

Si vous souhaitez ne plus appartenir à cette liste de distribution, veuillez répondre à ce message en indiquant le mot « Supprimer » dans la ligne d'objet.

Même s'il s'agit là d'un outil légitime utilisé par certaines entreprises dignes de confiance, il représente souvent un moyen de vérifier la validité d'une adresse électronique afin de pouvoir la réutiliser (il est possible qu'elle soit vendue à d'autres expéditeurs de courrier indésirable). Pour plus d'informations sur les moyens disponibles aux utilisateurs pour lutter contre le courrier indésirable, consultez le site Web (en anglais) sur les notions de base dans le domaine de la sécurité et de la confidentialité Microsoft à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24701.

Fonctionnalités de protection contre le courrier indésirable dans Outlook 2003 et Outlook Web Access 2003

Outlook 2003 et Outlook Web Access 2003 incluent des fonctionnalités permettant de protéger vos utilisateurs contre le courrier indésirable. Ces fonctionnalités sont les suivantes :

Listes d'interdiction et listes de sécurité tenues à jour par l'utilisateur

Les listes d'interdiction et les listes de sécurité utilisées par Outlook 2003 et Outlook Web Access sont stockées dans la boîte aux lettres de l'utilisateur. Comme ces deux programmes client utilisent la même liste, les utilisateurs n'ont pas besoin de tenir deux versions à jour.

Blocage de contenu externe

Exchange 2003 et Outlook Web Access 2003 compliquent la tâche des expéditeurs de messages électroniques indésirables contenant des balises permettant de récupérer des adresses de messagerie. Un message entrant dont le contenu peut être utilisé comme balise, que ce message contienne réellement une balise ou non, entraîne l'affichage par Outlook et Outlook Web Access d'un message d'avertissement. Si les utilisateurs savent que ce message est légitime, ils peuvent cliquer sur le message d'avertissement pour télécharger le contenu. Dans le cas contraire, les utilisateurs peuvent le supprimer sans déclencher les balises qui avertissent un expéditeur de courrier indésirable.

Pour plus d'informations sur le blocage de contenu externe dans Outlook 2003 et Outlook Web Access 2003, consultez « Fonctionnalités client » dans le manuel *Nouveautés dans Exchange Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24402.

Gestion améliorée du courrier indésirable

Grâce à Outlook 2003, les utilisateurs peuvent créer des règles qui recherchent dans les messages électroniques des expressions spécifiques et déplacer automatiquement les messages contenant ces expressions de la Boîte de réception vers un dossier spécifié (comme les dossiers Éléments supprimés ou de courrier indésirable). De plus, les utilisateurs peuvent décider de supprimer de façon permanente le courrier électronique qu'il soupçonne d'être indésirable au lieu de le déplacer vers un dossier spécifié.

Filtre du courrier indésirable

Outlook 2003 comprend un filtre de courrier indésirable qui recherche les attributs de courrier indésirable courants. (Ces attributs sont mis à jour conjointement avec les mises à jour Office.) Pour chaque attribut suspect, Outlook incrémente la valeur d'un compteur – plus le nombre attribué à un message donné est élevé, plus ce dernier est susceptible de représenter du courrier indésirable. Pour définir le niveau de

protection souhaité contre le courrier indésirable, utilisez la boîte de dialogue **Options du courrier indésirable** (dans Outlook 2003, dans le menu **Action**, pointez sur **Courrier indésirable**, puis cliquez sur **Options du courrier indésirable**). Lorsque vos utilisateurs commencent à utiliser ces fonctionnalités de courrier indésirable ou s'ils modifient les options à tout moment, ils doivent vérifier périodiquement les messages qui ont été supprimés de la Boîte de réception pour s'assurer que des messages valides n'ont pas été déplacés. Des mises à jour de ces fonctionnalités dans Outlook 2003 seront répertoriées sur le site Web Microsoft Office Online, sous **Office Update** à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24393.

Infrastructure SCL (Spam Confidence Level)

Exchange 2003 et Outlook 2003 fournissent une infrastructure qui prend en charge une solution de bout en bout permettant de lutter contre le courrier indésirable. Cette infrastructure inclut en particulier des fonctionnalités natives dans Exchange 2003 et Outlook 2003 qui permettent aux fournisseurs de logiciels d'incorporer des filtres de détection contre le courrier indésirable le long du chemin du message. Ces filtres évaluent les messages et déterminent dans quelle mesure un message donné est susceptible d'être indésirable. Un nombre compris entre **0** et **9** est attribué ; ce nombre correspond au contrôle d'accès SCL (Spam Confidence Level). Il s'agit essentiellement d'une valeur normalisée assignée à un message qui indique, en fonction des caractéristiques d'un message (contenu, en-tête du message etc.), dans quelle mesure ce message est indésirable. Un contrôle d'accès **0** indique qu'il est très improbable que le message soit du courrier indésirable. Le contrôle d'accès **9** indique qu'il est fort probable que le message soit du courrier indésirable. Le contrôle d'accès SCL est stocké comme attribut du message.

L'administrateur configure Exchange pour que les messages contenant des contrôles d'accès SCL soient traités d'une manière qui convienne à l'environnement. Par exemple, un serveur de passerelle peut rejeter tout le courrier indésirable dont le contrôle d'accès SCL est supérieur ou égal à **7** et transmettre tous les messages inférieurs à **7** vers le serveur de la boîte aux lettres Exchange. L'administrateur de la boîte aux lettres peut ensuite décider que tous les messages supérieurs ou égaux à **5** sont transférés directement vers le dossier de courrier indésirable de l'utilisateur pendant que tous les messages inférieurs ou égaux à **4** sont transférés vers la Boîte de réception. Enfin, il est possible que l'utilisateur dispose d'un paramètre de boîte aux lettres qui traite tout le courrier dans le dossier de courrier indésirable comme courrier indésirable et supprime celui-ci. L'administrateur Exchange peut également configurer une stratégie de destinataires de boîte aux lettres qui abaisse la période de rétention (selon l'âge ou la taille) dans le dossier de courrier indésirable.

L'infrastructure SCL tient également compte des listes de destinataires, des listes d'interdiction et des listes fiables de l'utilisateur ainsi que des listes de filtrage Exchange. Pour plus d'informations sur SCL, consultez le site Web consacré au filtre du courrier indésirable sur MSDN® à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24395.

Remarque La prochaine version du filtre de messages intelligent Exchange sera également un composant essentiel dans la lutte contre le courrier indésirable. Le filtre de messages intelligent Exchange est un filtre compatible SCL qui fournit un filtrage avancé des messages côté serveur et conçu spécifiquement pour lutter contre le courrier indésirable. Pour plus d'informations, consultez le site Web sur le filtre de messages intelligent Exchange à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=21607.

Listes de distribution restreintes

Parmi les autres formes de dissuasion contre le courrier indésirable figurent les listes de distribution restreintes auxquelles vous pouvez faire appel dans votre organisation Exchange. Une liste de distribution restreinte n'autorise que les utilisateurs authentifiés à envoyer des messages. Cette caractéristique est particulièrement importante car si des expéditeurs de courrier indésirable connaissent l'alias d'une liste de distribution, il leur est possible d'atteindre un grand nombre de vos employés à l'aide d'un message électronique. La restriction des listes de distribution est particulièrement efficace pour des listes importantes qui contiennent un grand nombre de listes de distribution imbriquées.

Remarque Sachez que de nombreux expéditeurs de courrier indésirable utilisent les attaques par dictionnaire (attaques utilisant des logiciels qui ouvrent une connexion au serveur de messagerie visé, puis envoient des millions d'adresses de messagerie de façon aléatoire) comme mécanisme permettant d'atteindre des destinataires. Les listes de distribution sont souvent représentées par un alias qui correspond à un mot usuel du dictionnaire.

Pour définir une liste de distribution restreinte

1. Dans **Utilisateurs et ordinateurs Active Directory**, ouvrez la page des propriétés de la liste de distribution.
2. Cliquez sur l'onglet **Exchange – Général**, puis activez la case à cocher **Provenant des utilisateurs authentifiés uniquement**.

Filtrage Exchange 2003

Exchange 2003 inclut un ensemble de fonctionnalités qui permettent à l'administrateur de créer des listes d'expéditeurs, des listes de destinataires et des listes de filtrage des connexions destinées à bloquer le courrier indésirable à l'extérieur de l'organisation, ce qui réduit les coûts en rejetant les messages à la première occasion. Exchange Server 2003 prend en charge les filtres suivants :

- **Filtrage des connexions** Filtre les messages entrants en comparant leur adresse IP à une liste d'interdiction fournie par un service de liste d'interdiction en temps réel. Vous pouvez également entrer votre propre jeu d'adresses IP interdites/acceptées à un niveau global.
- **Filtrage des expéditeurs** Par défaut, les connexions SMTP créées par les expéditeurs de cette liste sont rompues.
- **Filtrage des destinataires** Vous permet de définir des restrictions globales sur du courrier adressé à des destinataires spécifiques.

Pour plus d'informations sur l'application des filtres, consultez le manuel *Nouveautés dans Exchange Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24402.

Protection contre les attaques de refus de service

Il est généralement difficile de se protéger contre les attaques de refus de service. Cependant, Exchange 2003 inclut des paramètres qui peuvent vous aider à vous protéger contre ces attaques.

Les paramètres de limite des messages configurés sur le serveur virtuel SMTP vous permettent de spécifier un nombre maximal de destinataires par message, une taille de message maximale, un nombre maximal de messages par connexion, etc. Ces limites peuvent contribuer à la prévention des attaques de refus de service provenant du transport du courrier.

Un autre type d'attaque de refus de service consiste à envoyer un grand nombre de messages électroniques vers un serveur particulier jusqu'à ce que l'espace disque soit insuffisant. Pour minimiser cette possibilité, vous pouvez définir des limites de stockage sur des boîtes aux lettres et des dossiers publics. Par défaut, Exchange 2003 n'accepte pas les messages d'une taille supérieure à 10 Mo. De plus, vous devez configurer les serveurs virtuels SMTP sur le serveur de passerelle avec accès Internet pour bloquer les messages d'une taille supérieure à 10 Mo. La taille de message maximale acceptée par un serveur virtuel STMP intervient plus tôt dans le traitement des messages que la limite définie par Exchange.

Remarque Comme il est probable que les besoins en réplication nécessitent le transfert de messages de taille importante, il ne faut pas configurer les serveurs virtuels SMTP internes (sans accès à Internet) pour interdire les messages supérieurs à 10 Mo.

De plus, dans une installation Windows Server 2003, Exchange 2003 utilise les pools d'applications IIS (Internet Information Services) pour atténuer les attaques de refus de service.

Pour obtenir des informations sur l'administration de ces divers paramètres, consultez le *Guide d'administration d'Exchange Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=21769.

Protection contre l'usurpation d'adresse

Une technique utilisée couramment par les expéditeurs de courrier indésirable consiste à configurer la ligne **De** d'un message électronique afin de masquer l'identité de l'expéditeur. Même si SMTP ne nécessite pas de vérifier l'identité d'un expéditeur, Exchange 2003 fournit les fonctionnalités suivantes permettant de minimiser l'usurpation d'adresse :

Paramètres d'authentification par défaut

Par défaut, Exchange 2003 ne résout pas l'adresse de messagerie d'un expéditeur à moins que celui-ci n'utilise un programme client comme Outlook ou Outlook Web Access pour authentifier par rapport à un serveur Exchange. Lorsque Exchange reçoit un message d'un client authentifié, il vérifie que l'expéditeur appartient à la liste d'adresses globale, et si tel est le cas, résout le nom complet de l'utilisateur (dans la ligne **De**) du message. Si le message d'origine a été soumis sans authentification, Exchange 2003 marque le message comme non authentifié à son point d'origine et transfère ces informations d'un serveur à l'autre. Dans ce cas, l'adresse de l'expéditeur n'est pas associée à un nom complet GAL (Global Address List) (par exemple **Alfred Wallace**) ; en fait, elle est affichée au destinataire au format SMTP (par exemple **alfred@contoso.com**). Il est nécessaire de sensibiliser vos utilisateurs afin qu'ils se méfient des messages qui prétendent provenir d'autres utilisateurs de votre organisation mais ne sont pas associés à un nom complet GAL.

Cependant, Exchange 2000 ne résout pas les messages soumis de manière anonyme. Par conséquent, si vous effectuez une mise à niveau depuis Exchange 2000, il est recommandé de mettre à niveau les serveurs de passerelle vers Exchange 2003 avant de mettre à niveau le serveur de boîte aux lettres et les autres serveurs Exchange. Pour empêcher vos serveurs Exchange 2000 de résoudre du courrier anonyme, vous pouvez également exécuter la procédure suivante.

Pour empêcher Exchange 2000 de résoudre des messages électroniques anonymes

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 utiles.

1. Démarrez l'Éditeur du Registre (regedit).
2. Accédez à ou créez la clé suivante dans le Registre (où un ***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

5. Pour déterminer cette valeur, ajoutez les valeurs pour 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 définir ce comportement soit en supprimant la clé, soit en définissant la valeur à l'aide de la formule suivante : 2+16+32=50).
6. Quittez l'Éditeur du Registre.
7. 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 votre organisation comporte un grand nombre de serveurs, tout le courrier interne en provenance d'autres serveurs Exchange 2000 est également affecté. Par conséquent, étant donné qu'Exchange 2000 fait appel à SMTP pour acheminer le courrier interne entre les serveurs, il vous faudra peut-être créer un nouveau serveur virtuel SMTP ou sans doute appliquer ce paramètre uniquement sur un serveur tête de pont SMTP entrant.

Paramètres d'authentification entre forêts

Si votre organisation contient plusieurs forêts, vous pouvez configurer les approbations entre les forêts de façon à ce que les serveurs tête de pont SMTP exigent une authentification.

> **Remarque** Les applications de flux de travail peuvent envoyer du courrier de manière anonyme ; aussi, avant de configurer l'authentification dans votre organisation, assurez-vous d'évaluer les besoins de vos applications de flux de travail.

Pour plus d'informations sur la configuration de l'authentification entre forêts, consultez « Fonctionnalités de transport et de flux de messages » dans le manuel *Nouveautés dans Exchange Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24402.

Paramètres pour l'accès anonyme

Même si Exchange 2003 fournit la possibilité aux utilisateurs côté client de reconnaître le courrier falsifié, vous devez désactiver l'accès SMTP anonyme sur tous les serveurs Exchange internes. La désactivation de l'accès anonyme vous permet de garantir que seuls les utilisateurs authentifiés peuvent envoyer des messages dans votre organisation. De plus, exiger l'authentification force les programmes clients comme Outlook Express et Outlook qui utilisent RPC sur HTTP à authentifier avant d'envoyer du courrier.

Recherches DNS inversées

Si vous recevez des messages directement d'autres domaines sur Internet, vous pouvez configurer votre serveur virtuel SMTP pour effectuer une recherche DNS (Domain Name System) inversée sur les messages électroniques entrants. Cette opération s'assure que l'adresse IP (Internet Protocol) et le nom de domaine complet du serveur de messagerie de l'expéditeur correspondent au nom de domaine répertorié dans le message. Cependant, tenez compte des limitations suivantes affectant les recherches DNS inversées :

- L'adresse IP de l'expéditeur peut ne pas figurer dans le résultat de la recherche DNS inversée ou le serveur d'envoi peut disposer de plusieurs noms pour la même adresse IP qui ne sont pas tous disponibles dans le résultat de la recherche DNS.
- Les recherches DNS inversées entraînent une surcharge sur le serveur Exchange.
- Les recherches DNS inversées exigent que le serveur Exchange puisse contacter les zones de recherche inversée pour le domaine d'envoi.
- Effectuer des recherches DNS inversées sur chaque message peut entraîner une baisse importante des performances en raison du surcroît de latence.

  > **Remarque** Pour plus d'informations sur la recherche DNS inversée, consultez l'article 319356 de la Base de connaissances Microsoft, intitulé « HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000 Server » (http://go.microsoft.com/fwlink/?linkid=3052&kbid=319356).

Renforcement des serveurs Exchange 2003

Cette section explique comment renforcer des serveurs Exchange 2003 en fonction de leur rôle dans votre organisation. Cette section est divisée en trois sous-sections principales.

- **Renforcement de l'infrastructure Windows** Cette section décrit les étapes préliminaires à suivre afin de renforcer vos serveurs Exchange.
- **Renforcement des serveurs principaux** Cette section décrit les étapes à suivre pour renforcer le serveur de boîte aux lettres Exchange, notamment la manière de désactiver les services superflus, de restreindre l'accès aux répertoires locaux ainsi que d'autres configurations.
- **Renforcement des serveurs frontaux** Cette section fournit les étapes à suivre pour renforcer un serveur frontal Exchange. Cette section décrit également les rôles des serveurs frontaux et apporte des recommandations plus précises en matière de configuration et en conformité à ces rôles. De plus, cette section comprend des informations sur URLScan – un outil qui s'exécute sur IIS et vous permet de définir précisément quelles demandes HTTP peuvent s'exécuter en fonction de l'ordinateur.

Cette section, ainsi que la suite de ce guide, a été rédigée en partant du principe que vous avez pris connaissance du *Guide de la sécurité Windows Server 2003* et que vous avez appliqué les recommandations destinées à renforcer votre domaine, vos contrôleurs de domaine et les serveurs membres. Dans certains cas, les recommandations concernant la configuration d'Exchange 2003 dans cette section dépendent des recommandations figurant dans le *Guide de la sécurité Windows Server 2003*. Ces exigences sont définies quand cela est nécessaire.

De plus, l'ensemble des recommandations présentées dans cette section proviennent des configurations des modèles de sécurité de stratégie de groupes Exchange inclus dans ce guide (pour plus d'informations sur ces modèles, consultez la section « Déploiement des modèles de sécurité de stratégie de groupes Exchange » plus loin dans ce guide). Cette section explique en particulier les paramètres des modèles de sécurité, si vous souhaitez configurer vos serveurs manuellement.

Vous pouvez également importer les modèles fournis des deux manières suivantes :

- Vous pouvez importer un modèle de sécurité vers un ordinateur local. Pour ce faire, ouvrez le composant logiciel enfichable MMC de stratégie de sécurité, cliquez avec le bouton droit sur **Paramètres de sécurité**, puis cliquez sur **Importer une stratégie**. Accédez au modèle approprié de sécurité de stratégie de groupes Exchange, puis double-cliquez dessus.
- Vous pouvez reprendre point par point la structure d'organisation Active Directory (telle qu'elle est recommandée par le *Guide de la sécurité Windows Server 2003* et ce guide), puis utiliser l'Éditeur d'objets de stratégie de groupe pour importer les stratégies dans les unités d'organisation appropriées (pour plus d'informations sur cette méthode, consultez la section « Déploiement des modèles de sécurité de stratégie de groupes Exchange » plus loin dans ce guide).

  Important Dans la mesure où la section « Déploiement des modèles de sécurité de stratégie de groupes Exchange » a été rédigée en partant du principe que vous savez comment renforcer des serveurs Exchange 2003, il est important de commencer par la lecture de la section « Renforcement des serveurs Exchange 2003 ».

Comme pour tout déploiement de logiciels, veillez à effectuer un test approfondi de toutes les configurations recommandées dans un environnement de test avant de déployer dans un environnement de production.

Remarque Exécuter des applications personnalisées ou des plug-ins Exchange ou Outlook tiers peut nécessiter davantage de test et de configuration.

Renforcement de l'infrastructure Windows

Comme indiqué précédemment, ce guide part du principe que vous appliquez les configurations recommandées dans le *Guide de la sécurité Windows Server 2003*. Avant de renforcer votre environnement Exchange, vous devez effectuer les deux étapes suivantes.

1. Déployez le domaine, le contrôleur de domaine et les modèles de stratégie de base des serveurs membres dans l'ensemble de votre forêt. Pour des informations sur le déploiement de ces modèles, consultez les chapitres 2, 3 et 4 du *Guide de la sécurité Windows Server 2003* (http://go.microsoft.com/fwlink/?LinkId=21638).

   Remarque Les serveurs Exchange sont considérés comme des serveurs membres ; par conséquent, veillez à appliquer la stratégie de base des serveurs membres à chaque serveur Exchange.

2. Déployez le modèle de stratégie de base des contrôleurs de domaine Exchange (Exchange 2003 DC Incremental.inf) dans tous les contrôleurs de domaine de votre organisation. Le fichier Exchange 2003 DC Incremental.inf est une stratégie de sécurité qui permet à Exchange de fonctionner dans un environnement sécurisé. La section suivante explique cette stratégie en détail, notamment les étapes de déploiement spécifiques.

Stratégie de base des contrôleurs de domaine Exchange

La stratégie de base des contrôleurs de domaine Exchange modifie les contrôleurs de domaine dans votre forêt afin qu'ils puissent prendre en charge les opérations Exchange. Cette stratégie coexiste avec la stratégie de base des contrôleurs de domaine recommandée dans le chapitre 4, « Renforcement des contrôleurs de domaine », du *Guide de la sécurité Windows Server 2003*.

Le modèle de stratégie de base des contrôleurs de domaine Exchange (**Exchange 2003 DC Incremental.inf**) est inclus avec ce guide. Vous devez importer ce modèle dans un objet de stratégie de groupe de l'unité d'organisation des contrôleurs de domaine dans Utilisateurs et ordinateurs Active Directory et faire précéder la stratégie de base des contrôleurs de domaine fournie par Windows Server 2003.

Remarque Les étapes des stratégies sous l'onglet **Stratégie de groupe** déterminent l'ordre dans lequel ces stratégies sont appliquées ; par conséquent, il est important de placer la stratégie de base des contrôleurs de domaine Exchange au-dessus de la stratégie de base des contrôleurs de domaine Windows Server 2003.

Le tableau 1 répertorie les différences entre la stratégie de base des contrôleurs de domaine Windows Server 2003 et la stratégie de base des contrôleurs de domaine Exchange 2003. L'explication de ces différences figure dans le tableau ci-dessous.

Tableau 1 Différences entre les stratégies de base des contrôleurs de domaine dans Windows Server 2003 et Exchange 2003

Option	Base des contrôleurs de domaine Windows Server 2003	Stratégie de base des contrôleurs de domaine Exchange 2003
Restrictions supplémentaires pour les connexions anonymes	Pas d'accès sans connexion anonyme explicite	Aucune. Dépend des autorisations par défaut, car les versions d'Outlook antérieures à Outlook 2003 nécessitent des connexions anonymes
Arrêt immédiat de votre système en cas d'impossibilité d'enregistrer	Activé	Désactivé

Option	Base des contrôleurs de domaine Windows Server 2003	Stratégie de base des contrôleurs de domaine Exchange 2003
les audits de sécurité		
Audit des événements de connexion aux comptes	Succès et échec	Échec
Audit des événements d'ouverture de session	Succès et échec	Échec

Restrictions supplémentaires pour les connexions anonymes

Le paramètre de restriction anonyme dans Exchange 2003 est différent du paramètre de Windows Server 2003 car les clients Outlook 2000 et Outlook 2002 contactent le serveur de catalogue global de manière anonyme pour obtenir des informations. Grâce aux paramètres définis dans le *Guide de la sécurité Windows Server 2003* qui restreignent les requêtes anonymes au serveur de catalogue global, les utilisateurs Outlook 2000 et Outlook 2002 ne peuvent pas envoyer de courrier interne et doivent utiliser des adresses externes. Cependant, comme Outlook 2003 authentifie à l'aide du serveur de catalogue global, il n'est pas nécessaire d'assouplir ce paramètre de sécurité dans un environnement Outlook 2003 pur.

> **Remarque** Pour plus d'informations concernant cette question, consultez l'article 309622 de la Base de connaissances Microsoft, intitulé « XADM: Clients Cannot Browse the Global Address List After You Apply the Q299687 Windows 2000 Security Hotfix », à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=3052&kbid=309622.

Arrêt immédiat de votre système en cas d'impossibilité d'enregistrer les événements de sécurité

Ce paramètre est désactivé car les journaux peuvent se remplir rapidement en cas d'échecs d'ouverture de session comme le fait d'entrer un mot de passe incorrect.

Audit des événements de connexion aux comptes et audit des événements d'ouverture de session

Les paramètres d'audit des événements d'ouverture de session et des événements de connexion aux comptes sont modifiés du fait du grand nombre d'événements d'ouverture de session réussis générés par Exchange lors d'un fonctionnement normal. Si l'audit des succès est activé pour les événements d'ouverture de session, le journal de sécurité se remplit rapidement ; par conséquent, la stratégie de base des contrôleurs de domaine Exchange n'enregistre que des événements d'échec.

Le déploiement du modèle de stratégie de base des contrôleurs de domaine Exchange est particulièrement efficace si vous importez le fichier Exchange 2003 DC Incremental.inf dans l'unité d'organisation des contrôleurs de domaine à l'aide de la page des propriétés de la stratégie de groupe.

Pour créer l'objet de stratégie de groupe des contrôleurs de domaine et importer le modèle de stratégie de base des contrôleurs de domaine Exchange

1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur **Contrôleurs de domaine**, puis cliquez sur **Propriétés**.
2. Sous l'onglet **Stratégie de groupe**, cliquez sur **Nouveau** pour ajouter un nouvel objet de stratégie de groupe.
3. Tapez **Stratégie des contrôleurs de domaine Exchange**, puis appuyez sur ENTRÉE.
4. Cliquez sur **Modifier**. L'**Éditeur d'objets de stratégie de groupe** s'ouvre.
5. Dans l'**Éditeur d'objets de stratégie de groupe**, sous **Configuration ordinateur**, développez **Paramètres Windows**, cliquez avec le bouton droit sur **Paramètres de sécurité**, puis cliquez sur **Importer une stratégie**.

   > **Remarque** Si **Importer une stratégie** n'apparaît pas dans le menu, fermez l'**Éditeur d'objets de stratégie de groupe** et répétez les étapes 4 et 5.
6. Dans **Importer la stratégie à partir de**, accédez au répertoire où vous avez enregistré les modèles de sécurité de stratégie de groupes Exchange, puis double-cliquez sur **Exchange 2003 DC Incremental.inf**.

7. Fermez l'**Éditeur d'objets de stratégie de groupe**, puis cliquez sur **OK**.
8. Dans **Propriétés des contrôleurs de domaine**, sélectionnez **Stratégie des contrôleurs de domaine Exchange**, cliquez sur **Monter** jusqu'à ce que **Stratégie des contrôleurs de domaine Exchange** soit en haut de la liste, cliquez sur **Appliquer**, puis sur **OK**.
9. Une fois la stratégie importée, vous devez attendre la réplication vers d'autres contrôleurs de domaine ou utiliser les composants logiciels enfichables MMC des sites et service Active Directory pour forcer les réplications. La réplication garantit que tous les contrôleurs de domaine sont mis à jour avec la stratégie.

   Remarque Même si la réplication applique la stratégie, vous devez redémarrer les serveurs pour que les stratégies prennent effet.
10. Dans le Journal des événements, pour vérifier que la stratégie a été correctement téléchargée, recherchez l'événement d'informations d'application suivant : **SceCli 1704**. Puis, vérifiez que le serveur peut communiquer avec les autres contrôleurs de domaine du domaine.
11. Redémarrez chaque contrôleur de domaine individuellement pour garantir leur redémarrage correct et la prise d'effet des stratégies.

Renforcement des serveurs principaux

Après le renforcement du domaine, des contrôleurs de domaine et de tous les serveurs membres (en conformité avec le *Guide de la sécurité Windows Server 2003*), et au terme du déploiement de la stratégie de base des contrôleurs de domaine Exchange, vous êtes en mesure de renforcer vos serveurs Exchange 2003.

Le renforcement des serveurs principaux concerne quatre domaines de configuration généraux :

Renforcement des services
De nombreux services ne sont pas utilisés, mais sont activés par défaut et doivent être désactivés.

Renforcement des listes de contrôle d'accès aux fichiers (ACL)
Il est possible de renforcer certains répertoires davantage que ne le permet l'installation par défaut.

Changement des droits des privilèges
Pour autoriser les utilisateurs d'Outlook Web Access à se connecter, vous devez apporter un changement aux privilèges utilisateur.

Activation des services supplémentaires (facultatif)
Activent les services supplémentaires nécessaires pour votre organisation.

L'application du modèle de sécurité Exchange 2003 Backend.inf à vos serveurs principaux est le moyen le plus efficace pour mettre en œuvre le renforcement des configurations décrites dans cette section.

Pour obtenir des informations sur le déploiement des modèles de sécurité de stratégie de groupes Exchange, consultez « Déploiement des modèles de sécurité de stratégie de groupes Exchange » plus loin dans ce guide.

Important Avant de renforcer les serveurs principaux Exchange 2003, vous devez supprimer les banques de dossiers publics de l'ensemble des ordinateurs Exchange locaux qui ne sont pas utilisés comme points d'accès pour les dossiers publics. Supprimer les banques de dossiers publics avant de renforcer l'infrastructure Exchange permet de répliquer les suppressions devant avoir lieu. Pour des informations sur la suppression de la banque de dossiers publics, consultez « Démontage de la banque de boîtes aux lettres et suppression de la banque de dossiers publics » plus loin dans ce guide.

Services

Le tableau 2 répertorie les paramètres de base recommandés que vous devez utiliser lorsque vous commencez le renforcement des services pour un serveur principal Exchange (le fichier Exchange 2003 Backend.inf configure ces paramètres automatiquement). Tous les protocoles de récupération de courrier basés sur Internet sont désactivés. Cela permet de mettre en œuvre une configuration de démarrage renforcée qui nécessite que vous activiez chaque service en fonction des besoins.

Tableau 2 Paramètres de service configurés par Exchange 2003 Backend.inf

Nom du service	Mode de démarrage	Raison
Microsoft Exchange IMAP4	Désactivé	Serveur non configuré pour IMAP4
Banque d'informations Microsoft Exchange	Automatique	Nécessaire pour accéder aux banques de dossiers publics et de boîtes aux lettres
Microsoft Exchange POP3	Désactivé	Serveur non configuré pour POP3
Microsoft Search	Désactivé	Pas nécessaire pour les fonctionnalités principales
Événement Microsoft Exchange	Désactivé	Nécessaire uniquement en raison de la compatibilité ascendante avec Exchange 5.5
Service de réplication de sites Microsoft Exchange	Désactivé	Nécessaire uniquement en raison de la compatibilité ascendante avec Exchange 5.5
Gestion de Microsoft Exchange	Automatique	Nécessaire au fonctionnement du suivi des messages
Infrastructure de gestion Windows	Automatique	Nécessaire pour la gestion de Microsoft Exchange
Piles MTA Microsoft Exchange	Automatique	Nécessaire uniquement pour la compatibilité ascendante, les déplacements de boîte aux lettres ou si l'ordinateur est équipé de connecteurs X.400
Surveillance du système Microsoft Exchange	Automatique	Nécessaire pour la maintenance d'Exchange et d'autres tâches
Moteur de routage Microsoft Exchange	Automatique	Nécessaire pour coordonner le transfert des messages entre des serveurs Exchange
Agent de stratégie IPSEC	Automatique	Nécessaire pour mettre en œuvre une stratégie IPSec sur serveur
Détecteur d'appel RPC	Automatique	Nécessaire pour communiquer avec les contrôleurs de domaine et les clients
Service d'administration IIS	Automatique	Requis par le moteur de routage d'Exchange et SMTP
Fournisseur de la prise en charge de la sécurité NTLM	Automatique	La surveillance du système dépend de ce service
Protocole SMTP (Simple Mail Transfer Protocol)	Automatique	Requis pour le transport Exchange
Service de publication sur le World Wide Web	Automatique	Requis pour la communication avec les serveurs exécutant Outlook Web Access et Outlook Mobile Access
HTTP SSL	Manuel	Démarre automatiquement lorsqu'il est nécessaire pour le service de publication sur le World Wide Web
NNTP (Network News Transfer Protocol)	Désactivé	Nécessaire uniquement pour les fonctionnalités de groupes de discussion et d'installation

Remarque Pour que le service de surveillance du système Exchange démarre, les services Windows suivants doivent être en cours d'exécution :

- Journal des événements
- Fournisseur de la prise en charge de la sécurité NTLM
- RPC
- Détecteur d'appel RPC
- Serveur
- Station de travail

Services clés désactivés

Comme indiqué précédemment, tous les services superflus pour un serveur Exchange principal sont désactivés. Dans certains cas, en fonction des fonctionnalités nécessaires, vous devrez peut-être réactiver certains services. Pour assurer la cohérence entre vos serveurs, utilisez les stratégies de sécurité incluses avec ce guide ou créez vos propres stratégies pour les appliquer au niveau de l'unité d'organisation.

La liste suivante décrit certains des services désactivés :

Événement Microsoft Exchange
: Introduit dans Exchange Server 5.5, le service Événement Microsoft Exchange (MSExchangeES) prend en charge des scripts côté serveur déclenchés par des événements dossiers soit dans des dossiers publics, soit dans des boîtes aux lettres individuelles. MSExchangeES est fourni dans Exchange 2003 pour des raisons d'ingénierie ascendante avec les scripts d'événements Exchange 5.5. Cependant, les nouvelles applications développées spécifiquement pour Exchange 2003 doivent utiliser des événements de banque natifs plutôt que MSExchangeES. Pour plus d'informations sur ces nouvelles applications, consultez le Kit de développement (SDK) de Microsoft Exchange 2003 disponible sur MSDN à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21641.

Microsoft Search
: Pour optimiser les fonctionnalités lors de la recherche de documents résidant dans une banque, le service Microsoft Search (MSSEARCH) crée et gère des index pour des champs clés courants. Un index permet aux utilisateurs d'Outlook de rechercher des documents plus rapidement. Grâce à l'indexation de texte intégral, l'index est créé avant la recherche client, ce qui permet des recherches plus rapides. Les pièces jointes peuvent être également incluses dans l'indexation de texte intégral. Les services de banque d'informations Microsoft Exchange et MSSEARCH doivent être en cours d'exécution pour que l'index soit créé, mis à jour ou supprimé.

Service de réplication de sites Microsoft Exchange
: Si un serveur Exchange 2003 appartient à un site Exchange 5.5 existant, le service de réplication de sites Microsoft Exchange (MSExchangeSRS) est responsable de la réplication des informations de configuration et de site Exchange 5.*x* vers la partition d'appellation de configuration Active Directory.

Microsoft Exchange POP3
: Le service Microsoft Exchange POP3 (POP3Svc) est chargé de fournir un accès POP3 aux boîtes aux lettres. Par défaut, ce service est désactivé sur les nouvelles installations d'Exchange Server 2003.

Microsoft Exchange IMAP4
: Le service Microsoft Exchange IMAP4 (IMAP4) est chargé de fournir un accès IMAP4 aux boîtes aux lettres et aux dossiers publics. Par défaut, ce service est désactivé sur les nouvelles installations d'Exchange Server 2003.

Protocole NNTP (Network News Transfer Protocol)
: Le service NNTP (NntpSvc) est chargé de fournir un accès NNTP aux groupes de discussion maintenus dans les dossiers publics. Par défaut, ce service est désactivé sur les nouvelles installations d'Exchange Server 2003.

Listes de contrôle d'accès aux fichiers

Le tableau 3 répertorie les paramètres recommandés d'autorisation de liste de contrôle d'accès aux fichiers (le fichier Exchange 2003 Backend.inf configure ces paramètres automatiquement).

Tableau 3 Paramètres de liste de contrôle d'accès aux fichiers configurés par Exchange 2003 Backend.inf

Répertoire	Ancienne liste de contrôle d'accès aux fichiers	Nouvelle liste de contrôle d'accès aux fichiers	Appliqué aux sous-répertoires ?
%systremdrive%\Inetpub\mailroot	Tout le monde : • Accès complet	Administrateurs de domaine : • Accès complet Système local : • Accès complet	Oui
%systremdrive%\Inetpub\nntpfile\	Tout le monde : • Accès complet	Administrateurs de domaine : • Accès complet Système local : • Accès complet	Oui
%systremdrive%\Inetpub\nntpfile\ racine	Tout le monde : • Accès complet	Tout le monde : • Accès complet	Oui
..\exchsrver\	Administrateurs : • Accès complet Utilisateurs authentifiés : • Lecture • Lecture et exécution • Affichage du contenu Opérateurs de serveur : • Modification • Lecture et exécution • Affichage du contenu • Lecture • Écriture	Administrateurs : • Accès complet Opérateurs de serveur : • Modification • Lecture et exécution • Affichage du contenu • Lecture • Écriture	Tous – sauf **OMA** et **exchweb**

Remarque Les paramètres définis sur le répertoire **nntpfile** et sous-répertoires ne sont pas obligatoires sauf si NNTP est configuré pour s'exécuter sur le serveur. Cependant, le paramètre est défini dans le modèle de sécurité Exchange 2003 Backend.inf car il augmente les restrictions sur le système de fichiers. Il est également prêt à l'emploi si vous envisagez d'activer NNTP ultérieurement.

Droits des privilèges

Après avoir appliqué les stratégies de sécurité Windows Server 2003, il ne vous reste plus qu'à configurer un droit de privilège pour activer Outlook Web Access. L'interface utilisateur pour l'administration des dossiers publics et Outlook Web Access nécessite l'activation de la connexion réseau **Invités**. La stratégie de sécurité Windows Server 2003 définit la valeur « Refuser l'ouverture des sessions réseau » pour refuser l'**OUVERTURE DE SESSION ANONYME** et le groupe **Invités**. La façon la plus efficace de configurer cette valeur est d'appliquer une stratégie de groupe qui refuse uniquement l'**OUVERTURE DE SESSION ANONYME**.

Si vous déployez les modèles de sécurité de stratégie de groupes Exchange 2003, le fichier Exchange 2003 Backend.inf définit cette valeur correctement.

Si vous ne déployez pas les modèles de sécurité de stratégie de groupes Exchange 2003, vous pouvez modifier la stratégie de sécurité Windows Server 2003 existante.

Pour activer le groupe Invités dans la stratégie de sécurité de base Windows Server 2003

1. Dans Utilisateurs et ordinateurs Active Directory, cliquez avec le bouton droit sur l'unité d'organisation qui contient les serveurs Exchange et la stratégie de sécurité de base Windows Server 2003, puis cliquez sur **Propriétés**.
2. Dans **Propriétés de l'<*unité d'*organisation>**, sous l'onglet **Stratégie de groupe**, sélectionnez la stratégie de sécurité de base Windows Server 2003, puis cliquez sur **Modifier**. L'**Éditeur d'objets de stratégie de groupe** s'ouvre.
3. Dans l'**Éditeur d'objets de stratégie de groupe**, sous **Configuration ordinateur**, développez l'entrée **Paramètres Windows**, puis l'entrée **Paramètres de sécurité**. Développez l'entrée **Stratégies locales**, puis cliquez sur **Attribution de droits aux utilisateurs**.
4. Dans le volet d'informations, double-cliquez sur la stratégie **Refuser l'accès à cet ordinateur à partir du réseau**.
5. Dans **Propriétés de Refuser l'accès à cet ordinateur à partir du réseau**, sélectionnez **Invités**, puis cliquez sur **Supprimer**.
6. Cliquez sur **Appliquer**, puis sur **OK**.

   Remarque Si vous préférez créer votre propre stratégie de groupe, vous devez ajouter la valeur suivante sous la section [Droits des privilèges] :

   ```
   SeDenyNetworkLogonRight = *S-1-5-7
   ```

   Cet argument bloque uniquement l'OUVERTURE DE SESSION ANONYME.

Activation des services Exchange supplémentaires

Si vous avez effectué correctement les procédures jusqu'à ce point, vous avez renforcé vos serveurs principaux Exchange. Même si votre client MAPI, client HTTP (Outlook Web Access) et SMTP fonctionnent désormais avec votre serveur principal, vos clients POP3 et IMAP4 ne sont pas en mesure de récupérer le courrier. Si votre déploiement frontal et principal inclut ces protocoles, vous devez également activer les services POP3 et IMAP4 appropriés sur le serveur principal Exchange. S'il s'agit d'un serveur NNTP, vous devez également activer le service NNTP. La méthode la plus simple pour activer ces services consiste à importer les modèles de sécurité spécifiques au protocole d'Exchange 2003 correspondants vers les serveurs principaux qui nécessitent un accès client supplémentaire.

Par exemple, si votre organisation fournit un accès POP3 aux boîtes aux lettres, après avoir appliqué les modèles de sécurité Exchange 2003 (ou les configurations recommandées) au serveur POP3 frontal, vous devez appliquer le modèle de sécurité Exchange 2003 POP3 au serveur principal.

Cette section traite des services que vous devez activer pour prendre en charge NNTP. Tous les autres protocoles sont présentés dans la section « Renforcement des serveurs frontaux » plus loin dans ce guide.

Stratégie de serveur NNTP Exchange 2003

Le tableau 4 répertorie les services qui doivent être activés pour prendre en charge NNTP (le fichier Exchange 2003 NNTP.inf configure ces paramètres automatiquement). Cette stratégie de sécurité s'applique uniquement à un serveur principal Exchange car NNTP n'est pas déployé de la même manière que HTTP, POP3 et IMAP4 où un gestionnaire de protocole frontal transmet les demandes à la banque de données principales. Dans ce contexte, NNTP est un protocole « principal » uniquement ; par conséquent, pour ce qui concerne les serveurs frontaux, vous ne devez pas activer NNTP conformément aux paramètres du tableau 4.

Tableau 4 Services configurés pour activer NNTP

Nom du service	Mode de démarrage	Raison
NNTP (Network News Transfer Protocol)	Automatique	Serveur utilisé pour NNTP
Service d'administration IIS	Automatique	Nécessaire pour exécuter le service de publication sur le World Wide Web, les services SMTP, POP3, IMAP4 ou NNTP

Renforcement des serveurs frontaux

Le renforcement de vos serveurs frontaux Exchange s'apparente au renforcement du serveur principal. Vous disposez en outre de l'étape facultative (mais recommandée) permettant de configurer et d'exécuter URLScan sur vos serveurs frontaux HTTP.

Le renforcement des serveurs frontaux concerne six domaines de configuration généraux :

Renforcement des services
De nombreux services ne sont pas utilisés, mais sont activés par défaut et doivent être désactivés si la fonctionnalité correspondante n'est pas nécessaire.

Renforcement des listes de contrôle d'accès aux fichiers (ACL)
La configuration des listes de contrôle d'accès aux fichiers pour les serveurs frontaux est identique à celle des serveurs principaux.

Activation des services supplémentaires (facultatif)
Activent les services supplémentaires frontaux nécessaires pour votre organisation.

Exécution d'URLScan (facultatif, mais recommandé)
Même si l'exécution d'URLScan n'est pas nécessaire au fonctionnement des services, celle-ci est fortement recommandée comme mécanisme permettant d'optimiser le renforcement de vos serveurs HTTP frontaux.

Démontage de la banque de boîte aux lettres et suppression de la banque de dossiers publics (facultatif, mais recommandé)
Pour les serveurs frontaux qui ne sont pas des serveurs frontaux SMTP, vous pouvez démonter et supprimer ces banques.

> **Remarque** Si vous envisagez de supprimer la banque de dossiers publics, vous devez la supprimer avant d'appliquer les stratégies de sécurité Exchange pour que les modifications soient répliquées vers les autres serveurs Exchange.

L'application du modèle de sécurité Exchange 2003 Frontend.inf (inclus avec ce guide) à vos serveurs frontaux est le moyen le plus efficace pour mettre en œuvre le renforcement des configurations décrites dans cette section. De plus, après avoir appliqué le modèle Exchange 2003 Frontend.inf, vous pouvez utiliser les modèles de sécurité spécifiques au protocole pour activer les services appropriés.

Pour obtenir des informations sur le déploiement des modèles de sécurité de stratégie de groupes Exchange, consultez « Déploiement des modèles de sécurité de stratégie de groupes Exchange » plus loin dans ce guide.

Avant de commencer

Avant de commencer le renforcement des serveurs frontaux dans votre organisation, tenez compte des points suivants :

- Exchange 2003 comprend les applications suivantes :
  - Outlook Web Access
  - Outlook Mobile Access
  - Exchange Server ActiveSync®

Ces applications permettent à vos utilisateurs d'accéder aux informations Exchange depuis leurs ordinateurs personnels ou leurs périphériques mobiles. Toutes ces applications utilisent une combinaison des protocoles WebDav et HTTP (Hypertext Transfer Protocol). Par défaut, les applications Outlook Web Access et Exchange Server ActiveSync sont activées. Outlook Mobile Access est également installé par défaut, mais le service est désactivé sur les nouvelles installations d'Exchange 2003.

- Les clients POP3 et IMAP4 peuvent également utiliser des serveurs frontaux pour accéder aux boîtes aux lettres. Dans ces cas, ils utilisent également un serveur frontal comme passerelle SMTP.
- L'utilisation d'un serveur de pare-feu tel qu'ISA (Internet Security and Acceleration) Server 2000 afin de réguler l'accès pour le trafic des protocoles HTTP, RPC sur HTTP, POP3 et IMAP4 est un élément essentiel permettant de renforcer la sécurité d'un système de messagerie. Pour des informations sur le déploiement d'ISA 2000 avec Exchange 2003, consultez l'article technique « *Using ISA Server 2000 with Exchange Server 2003* », à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=23232.
- Il est recommandé d'isoler votre serveur ISA dans un réseau de périmètre (également appelé DMZ ou zone démilitarisée, et sous-réseau filtré) pour n'autoriser que les ports essentiels dans votre organisation. Le serveur frontal Exchange peut ensuite communiquer librement avec tous les services Windows et les services Exchange sur IPSec. Pour une liste des ports utilisables par Exchange 2003, consultez l'Annexe C, « Ports utilisés dans Exchange 2003 » plus loin dans ce guide.
- L'outil IIS Lockdown (IISlockd.exe) est nécessaire uniquement pour Windows 2000 Server. Dans Windows Server 2003, IIS Lockdown est un composant central de IIS (Internet Information Services). Si vous exécutez Exchange 2003 sur un serveur exécutant Windows 2000, consultez l'article technique « *Security Operations Guide for Exchange 2000 Server* », à l'adresse http://go.microsoft.com/fwlink/?linkid=11906, pour obtenir des informations sur l'utilisation de l'outil IIS Lockdown.
- Il est recommandé d'utiliser SSL/TLS et l'authentification par cookies pour Outlook Web Access. Le service TLS (Transport Layer Security) assure la confidentialité en cryptant le trafic des messages entre le client et Exchange 2003. L'authentification par cookies améliore la sécurité en établissant un délai d'expiration pour les connexions inactives sans domaine et en forçant l'utilisateur à s'authentifier de nouveau après une période d'inactivité. Pour plus d'informations sur l'authentification par cookies, consultez le *Guide d'administration d'Exchange Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=21769.

Services

Comme pour le renforcement de vos serveurs principaux, il est important de désactiver tous les services frontaux superflus. Vous pourrez activer ces services ultérieurement en fonction de vos besoins.

Cette section part du principe que vous avez effectué les tâches suivantes :

- Vous avez déjà utilisé le Gestionnaire système Exchange pour désigner le serveur comme serveur frontal Exchange.
- Vous avez déjà configuré le serveur comme passerelle SMTP ou serveur tête de pont.

  Important Le fait de désigner un ordinateur comme serveur frontal reconfigure les piles de protocole pour activer les déploiements frontaux et principaux. Si vous avez déployé le modèle de sécurité Exchange 2003 Frontend.inf avant de désigner le serveur comme serveur frontal, vous devez démarrer manuellement le service Surveillance du système Microsoft (et ses dépendances), utiliser le Gestionnaire système Exchange pour désigner le serveur comme serveur frontal, puis redémarrer l'ordinateur.

Le tableau 5 répertorie les paramètres de base recommandés que vous devez utiliser lorsque vous commencer le renforcement des services pour un serveur frontal Exchange (le fichier Exchange 2003 Frontend.inf configure ces paramètres automatiquement).

Tableau 5 Paramètres de service configurés par Exchange 2003 Frontend.inf

Nom du service	Mode de démarrage	Raison
Microsoft Exchange IMAP4	Désactivé	Serveur non configuré pour IMAP4
Banque d'informations Microsoft Exchange	Désactivé	Pas nécessaire en raison de l'absence de banque de dossiers publics ou de banque de boîte aux lettres
Microsoft Exchange POP3	Désactivé	Serveur non configuré pour POP3
Microsoft Search	Désactivé	Aucune banque de messages à rechercher
Événement Microsoft Exchange	Désactivé	Nécessaire uniquement en raison de la compatibilité ascendante avec Exchange 5.5
Service de réplication de sites Microsoft Exchange	Désactivé	Nécessaire uniquement en raison de la compatibilité ascendante avec Exchange 5.5
Gestion de Microsoft Exchange	Désactivé	Nécessaire uniquement pour le suivi de messages
Infrastructure de gestion Windows	Automatique	Nécessaire pour la gestion de Microsoft Exchange
Piles MTA Microsoft Exchange	Désactivé	Nécessaire uniquement pour la compatibilité ascendante ou si l'ordinateur est équipé de connecteurs X.400
Surveillance du système Microsoft Exchange	Désactivé	Nécessaire uniquement en cas d'exécution de la maintenance d'Exchange et d'autres tâches sur ce serveur
Moteur de routage Microsoft Exchange	Automatique	Nécessaire pour coordonner le transfert des messages entre des serveurs Exchange
Agent de stratégie IPSEC	Automatique	Nécessaire pour mettre en œuvre une stratégie IPSec sur serveur
Détecteur d'appel RPC	Automatique	Nécessaire pour communiquer avec les contrôleurs de domaine et les clients
Service d'administration IIS	Désactivé	Nécessaire pour exécuter le service de publication sur le World Wide Web, les services SMTP, POP3, IMAP4 ou NNTP
Fournisseur de la prise en charge de la sécurité NTLM	Automatique	La surveillance du système dépend de ce service
Protocole SMTP (Simple Mail Transfer Protocol)	Désactivé	Requis pour le transport Exchange
Service de publication sur le World Wide Web	Désactivé	Requis pour la communication avec les serveurs exécutant Outlook Web Access et Outlook Mobile Access
HTTP SSL	Manuel	Démarre automatiquement lorsqu'il est nécessaire pour le service de publication sur le World Wide Web
NNTP (Network News Transfer Protocol)	Désactivé	Nécessaire uniquement pour les fonctionnalités de groupes de discussion et d'installation

Services clés désactivés

Comme pour la configuration principale, vous devrez peut-être réactiver certains services pour fournir les fonctionnalités dont vous avez besoin. La liste suivante décrit certains des services désactivés :

Microsoft Exchange POP3, Microsoft Exchange IMAP4
Si vous ne disposez pas des clients POP3 ou IMAP4, vous pouvez vérifier que ces services sont désactivés par stratégie de groupe. Cependant, avant de désactiver ces services, assurez-vous qu'il n'y a aucun programme personnalisé en cours d'exécution dans votre environnement qui nécessite ces services.

Protocole SMTP (Simple Mail Transfer Protocol)
Lorsqu'un serveur frontal fonctionne comme serveur HTTP, POP3 ou IMAP4, il ne nécessite pas obligatoirement SMTP. Cependant, si vous configurez votre serveur frontal pour qu'il reçoive du courrier SMTP (soit comme serveur de passerelle, soit comme serveur d'envoi SMTP pour les clients IMAP4 ou POP3), vous devez activer le service SMTP (SMTPSVC). Pour les analyseurs anti-virus, les services de Banque d'informations Microsoft Exchange (MSExchangeIS) et de Surveillance du système Microsoft Exchange (MSExchangeSA) sont également requis.

Surveillance du système Microsoft Exchange
Sur un serveur frontal, la Surveillance du système est nécessaire seulement si vous souhaitez apporter des modifications à la configuration du serveur. Plus particulièrement, pour apporter des modifications à un serveur qui utilise la stratégie de sécurité frontale Exchange 2003 (y compris le fait de désigner le serveur comme serveur frontal), vous devez d'abord démarrer de manière temporaire le service Surveillance du système Microsoft Exchange (MSExchangeSA) et les services associés.

Banque d'informations Microsoft Exchange
Comme ce serveur ne reçoit aucun courrier, le service de Banque d'informations Microsoft Exchange (MSExchangeIS) n'est pas nécessaire. Cependant, si le serveur est configuré comme serveur de passerelle SMTP (sans dossier public ou boîte aux lettres utilisateur), MSExchangeIS est nécessaire pour l'analyse anti-virus et l'acheminement fiable du courrier des dossiers publics.

Gestion de Microsoft Exchange
Le service Gestion de Microsoft Exchange (MSExchangeMGMT) vous permet de définir, grâce à l'interface utilisateur, quel contrôleur de domaine ou serveur de catalogue global Exchange 2003 utilise pour accéder à Active Directory. Ce service est également nécessaire pour le suivi de messages. Vous pouvez désactiver ce service sans affecter la fonctionnalité principale d'Exchange. Cependant, lors de l'audit de vos fonctionnalités Exchange, vous aurez peut-être besoin des fonctions de suivi des messages. Comme le serveur frontal est utilisé pour accéder au courrier plutôt que pour l'acheminer, vous n'aurez peut-être pas besoin d'exécuter MSExchangeMGMT sur vos serveurs frontaux.

Listes de contrôle d'accès aux fichiers

Les paramètres de liste de contrôle d'accès aux fichiers pour les serveurs frontaux sont identiques à ceux des serveurs principaux. Pour des informations sur ces paramètres, consultez « Listes de contrôle d'accès aux fichiers » dans la section « Renforcement des serveurs principaux ».

Remarque Le modèle de sécurité Exchange 2003 Frontend.inf configure ces paramètres automatiquement.

Activation des services Exchange supplémentaires

Si vous avez effectué correctement les procédures jusqu'à ce point, vous avez renforcé vos serveurs frontaux Exchange. Cependant, pour tirer parti des fonctionnalités et des services Exchange 2003, vous devez activer la prise en charge des protocoles pour chaque type de client. Cette section explique quels services vous devez activer pour prendre en charge les protocoles clients.

Important Pour assurer le fonctionnement de POP3 et IMAP4, vous devez configurer ces deux protocoles sur les serveurs frontaux et principaux.

Chacune des sous-sections suivantes correspond à un modèle de sécurité spécifique inclus dans les modèles de sécurité de stratégie de groupes Exchange. L'installation de ces modèles est la méthode la plus efficace pour activer un protocole.

Stratégie de serveur HTTP Exchange 2003

La stratégie de sécurité HTTP Exchange 2003 active le service HTTP sur les serveurs frontaux.

> **Remarque** Si vous avez suivi les recommandations dans cette section ou si vous déployez les modèles de sécurité de stratégie de groupes Exchange 2003 inclus dans ce guide, il n'est pas nécessaire d'activer cette stratégie sur le serveur principal ; les modèles et les recommandations en matière de sécurité dans cette section supposent un accès HTTP pour le serveur principal.

Le tableau 6 répertorie les services qui doivent être activés pour prendre en charge HTTP (le fichier Exchange 2003 HTTP.inf configure ces paramètres automatiquement).

Tableau 6 Services configurés pour activer HTTP

Nom du service	Mode de démarrage	Raison
Service de publication sur le World Wide Web	Automatique	Serveur utilisé pour HTTP
HTTP SSL	Manuel	Démarre automatiquement lorsqu'il est nécessaire pour le service de publication sur le World Wide Web
Service d'administration IIS	Automatique	Nécessaire pour exécuter le service de publication sur le World Wide Web, les services SMTP, POP3, IMAP4 ou NNTP

Stratégie de serveur POP3 Exchange 2003

La stratégie de sécurité POP3 Exchange 2003 active le service POP3. Si vous faites appel au service POP3, vous devez appliquer cette stratégie sur le serveur principal également.

Le tableau 7 répertorie les services qui doivent être activés pour prendre en charge POP3 (le fichier Exchange 2003 POP3.inf configure ces paramètres automatiquement).

Tableau 7 Services configurés pour activer POP3

Nom du service	Mode de démarrage	Raison
Microsoft Exchange POP3	Automatique	Serveur utilisé pour POP3
Service d'administration IIS	Automatique	Nécessaire pour exécuter le service de publication sur le World Wide Web, les services SMTP, POP3, IMAP4 ou NNTP

Stratégie de serveur IMAP4 Exchange 2003

La stratégie de sécurité IMAP4 Exchange 2003 active le service IMAP4. Si vous faites appel au service IMAP4, vous devez appliquer cette stratégie sur le serveur principal également.

Le tableau 8 répertorie les services qui doivent être activés pour prendre en charge IMAP4 (le fichier Exchange 2003 IMAP4.inf configure ces paramètres automatiquement).

Tableau 8 Services configurés pour activer IMAP4

Nom du service	Mode de démarrage	Raison
Microsoft Exchange IMAP4	Automatique	Serveur utilisé pour IMAP4
Service d'administration IIS	Automatique	Nécessaire pour exécuter le service de publication sur le World Wide Web, les services SMTP, POP3, IMAP4 ou NNTP

Stratégie de serveur SMTP Exchange 2003

La stratégie de sécurité SMTP Exchange 2003 active le service SMTP.

> **Remarque** Si vous avez suivi les recommandations dans cette section ou si vous déployez les modèles de sécurité de stratégie de groupes Exchange 2003 inclus dans ce guide, il n'est pas nécessaire d'activer cette stratégie sur le serveur principal ; les modèles et les recommandations en matière de sécurité dans cette section supposent un accès SMTP pour le serveur principal.

Le tableau 9 répertorie les services qui doivent être activés pour prendre en charge SMTP (le fichier Exchange 2003 SMTP.inf configure ces paramètres automatiquement). Ces paramètres sont également les paramètres par défaut après une installation Exchange 2003 standard.

Tableau 9 Services configurés pour activer SMTP

Nom du service	Mode de démarrage	Raison
Protocole SMTP (Simple Mail Transport Protocol)	Automatique	Serveur utilisé pour SMTP
Service d'administration IIS	Automatique	Nécessaire pour exécuter le service de publication sur le World Wide Web, les services SMTP, POP3, IMAP4 ou NNTP
Banque d'informations Microsoft Exchange	Automatique	Utilisé par les analyseurs anti-virus, SMTP
Surveillance du système Microsoft Exchange	Automatique	Nécessaire pour la maintenance d'Exchange et d'autres tâches
Gestion de Microsoft Exchange	Automatique	Nécessaire au fonctionnement du suivi des messages
Piles MTA Microsoft Exchange	Activé	Utilisé pour la gestion des erreurs de certains messages

URLScan

URLScan.exe analyse toutes les demandes HTTP entrantes vers un serveur IIS et n'autorise que celles qui se conforment à un ensemble de règles spécifiques. De cette manière, le serveur ne répond qu'à des requêtes valides, ce qui améliore sensiblement la sécurité. URLScan vous permet de filtrer des requêtes basées sur la longueur, le jeu de caractères, le contenu et d'autres facteurs. Pour plus d'informations sur URLScan ainsi que des instructions d'installation et de téléchargement, consultez le site Web sur l'outil de sécurité URLScan à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=24490.

Configuration de URLScan d'Exchange 2003

URLScan est configuré manuellement en modifiant un fichier de texte de configuration appelé urlscan.ini. Une fois URLScan installé, ce fichier est situé dans le dossier suivant : **<*WinDir*>\System32\Inetsrv\Urlscan**.

Les tableaux 10 et 11 répertorient les valeurs nécessaires utilisées par chaque application HTTP Exchange. Pour toutes les applications HTTP que vous exécutez sur un serveur donné, créez un fichier de configuration URLScan qui inclut le sur-ensemble des valeurs de configuration.

> **Remarque** Si vous rencontrez des problèmes avec Outlook Web Access ou Outlook Mobile Access lorsque l'outil URLScan est activé, examinez le fichier URLScan.log situé dans le dossier **<WinDir>\System32\Inetsrv\UrlScan** pour obtenir la liste des demandes rejetées.

Verbes autorisés

Le tableau 10 répertorie les verbes nécessaires pour chaque fonctionnalité basée sur le Web sur un serveur donné. Les administrateurs peuvent personnaliser le fichier URLScan.ini pour autoriser uniquement les verbes nécessaires à la prise en charge du rôle de ce serveur. Si plusieurs fonctionnalités basées sur le Web sont nécessaires sur un serveur unique, l'administrateur doit regrouper les exigences en matière de « verbes autorisés ».

Tableau 10 Verbes requis pour les fonctionnalités basées sur le Web

[AllowVerbs]	OWA : BE/FE	OMA : FE	OMA : BE	Exchange Active Sync : FE	Exchange Active Sync : BE	RPC sur HTTP	Dossiers Web
GET	√	√			√		√
POST	√	√		√	√		
PROPFIND	√		√		√		√
PROPPATCH	√		√		√		
BPROPPATCH	√						
MKCOL	√				√		√
DELETE	√		√		√		√
BDELETE	√						√
BCOPY	√						√
MOVE	√		√		√		
SUBSCRIBE	√						
BMOVE	√				√		
POLL	√						
SEARCH	√		√		√		
HEAD			√				
PUT					√		√
OPTIONS				√	√		√
RPC_OUT_DAT						√	

[AllowVerbs]	OWA : BE/FE	OMA : FE	OMA : BE	Exchange Active Sync : FE	Exchange Active Sync : BE	RPC sur HTTP	Dossiers Web
A							
RPC_IN_DATA						√	
X-MS-ENUMATTS			√		√		
LOCK							√
UNLOCK							√

Limites des demandes

Le tableau 11 répertorie les limites des demandes pour chaque fonctionnalité basée sur le Web sur un serveur donné. Les administrateurs peuvent personnaliser le fichier URLSCNA.ini pour restreindre les limites des demandes basées sur le rôle du serveur. Si plusieurs fonctionnalités basées sur le Web sont nécessaires sur un serveur unique, l'administrateur doit utiliser la valeur la plus élevée des limites des demandes.

Tableau 11 Limites des demandes HTTP, basées sur le type client

[RequestLimits]	OWA : BE/FE	OMA : FE	OMA : BE	EAS : FE	EAS : BE	RPC sur HTTP
MaxAllowedContentLength	1,048,760	16,384	10,485,760	65,536	65,536	1,073,741,824
MaxUrl	16,384	260	16,384	1024	1024	16,384
MaxQueryString	4096	13	4096	4096	4096	4096

Remarque La valeur **MaxAllowedContentLength** pour Outlook Web Access et Outlook Mobile Access (principal) est basée sur une taille de message maximale de 10 Mo (paramètre par défaut d'Exchange 2003). Les administrateurs doivent modifier ce paramètre de façon appropriée, en fonction de la taille de leur messagerie existante.

Refus des extensions

Si RPC sur HTTP n'est pas utilisé sur le serveur, il est possible d'ajouter l'extension DLL aux sections Refus des extensions.

Courrier électronique bloqué

Les caractères suivants dans [DenyUrlSequences] sont bloqués. Cependant, les messages ou dossiers contenant ces séquences ne sont pas bloqués dans Outlook Web Access car les caractères sont normalisés dans la banque d'informations Exchange et n'apparaissent pas explicitement dans l'URL :

- ./
- \

Démontage de la banque de boîtes aux lettres et suppression de la banque de dossiers publics

Étant donné que le rôle d'un serveur frontal est de transmettre les demandes aux serveurs principaux, vous n'aurez peut-être pas besoin de boîte aux lettres ou de dossiers publics Exchange sur les serveurs frontaux. Le serveur Exchange principal gère ces banques. Si le serveur frontal n'est pas un serveur frontal SMTP, vous pouvez démonter et supprimer ces banques.

> **Important** Si vous exécutez SMTP sur le serveur frontal, vous ne devez pas supprimer la banque de dossiers publics. Dans ce cas, SMTP dépend de la banque de dossiers publics pour fournir un acheminement fiable pour des messages électroniques destinés à des dossiers publics principaux.

Pour répliquer les suppressions de dossiers publics vers d'autres serveurs Exchange, vous devez supprimer les banques de dossiers publics avant de renforcer les serveurs.

Pour démonter et supprimer les bases de données de dossiers publics et de boîtes aux lettres

1. Démarrez l'outil d'administration **Services**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur **Fournisseur de la prise en charge de la sécurité NTLM**, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, dans la liste **Type de démarrage**, sélectionnez **Automatique**.
4. Cliquez sur **Appliquer**, sur **Démarrer**, puis sur **OK**.
5. Répétez les étapes 2 à 4 pour le service **Surveillance du système Microsoft Exchange**. Si SMTP s'exécute sur ce serveur, vous devez également démarrer le service de **Banque d'informations Microsoft Exchange**.
6. Démarrez le Gestionnaire système Exchange sur le serveur frontal.
7. Développez **Serveurs**, puis le serveur frontal, puis développez le **Premier groupe de stockage**.
8. Si la banque de boîte aux lettres est montée, cliquez avec le bouton droit sur **Banque de boîtes aux lettres**, puis cliquez sur **Oui** pour démonter la banque de boîte aux lettres.
9. Cliquez avec le bouton droit sur **Banque de boîtes aux lettres**, puis cliquez sur **Propriétés**.
10. Sous l'onglet **Base de données**, activez la case à cocher **Ne pas monter cette banque d'informations au démarrage**, puis cliquez sur **OK**.
11. Si la banque de dossiers publics est montée, cliquez avec le bouton droit sur **Banque de dossiers publics**, cliquez sur **Démonter la banque d'informations**, puis sur **Oui** pour démonter la banque de dossiers publics.
12. Cliquez avec le bouton droit sur **Banque de dossiers publics**, puis cliquez sur **Supprimer**.
13. Cliquez sur **Oui**, sur **OK**, sélectionnez un serveur principal, puis cliquez sur **OK**.
14. Cliquez sur **Oui** pour supprimer la banque de dossiers publics, puis cliquez sur **OK**.
15. Redémarrez le serveur frontal.

> **Remarque** Si vous installez le modèle de sécurité Exchange 2003 Frontend.inf sur cet ordinateur, il n'est pas nécessaire de désactiver à nouveau le fournisseur de la prise en charge de la sécurité NTLM et la Surveillance du système Microsoft Exchange – cette opération se produit automatiquement au redémarrage du serveur.

Déploiement des modèles de sécurité de stratégie de groupes Exchange

Dans Windows Server 2003, vous pouvez définir plusieurs paramètres de sécurité, notamment l'audit, les options de sécurité, les paramètres du Registre, les autorisations de fichier et les services. Le *Guide de la sécurité Windows Server 2003* fournit des recommandations pour la plupart de ces paramètres, ces paramètres

sont les mêmes pour Exchange 2003. Comme indiqué précédemment, les services sont le domaine principal concerné par l'application des paramètres supplémentaires même s'il y a des modifications des autorisations de fichier, et pour les contrôleurs de domaine, des modifications du Registre.

Cette section explique comment organiser votre structure Active Directory pour prendre en charge le déploiement des modèles de sécurité de stratégie de groupes Exchange au niveau de l'unité d'organisation. Les sections précédentes ont fourni des étapes pour l'installation des modèles de sécurité individuelle sur chaque machine locale ou pour la configuration manuelle des paramètres recommandés. Par comparaison, le déploiement des modèles de sécurité de stratégie de groupes Exchange (conformément à la structure d'unité d'organisation recommandée et présentée dans cette section) est plus prévisible et moins sujet à des problèmes de configuration. L'utilisation d'unités d'organisation et d'objets de stratégie de groupe pour déployer les modèles de sécurité vous permet de garantir une configuration identique de tous les serveurs d'une unité d'organisation donnée.

> **Important** Cette section a pour but d'approfondir directement les recommandations en matière d'unité d'organisation spécifique du *Guide de la sécurité Windows Server 2003.* Il est essentiel, cependant, de prendre connaissance de l'ensemble de la section « Renforcement des serveurs Exchange 2003 ».

Structure Active Directory pour la prise en charge des rôles des serveurs Exchange 2003

Le Guide de la sécurité Windows Server 2003 recommande une structure d'unité d'organisation qui vous permet d'adopter facilement les modèles de sécurité fournis avec ce guide. Comme Exchange 2003 est une application d'annuaire, il est facile d'élargir la structure d'unité d'organisation Windows Server 2003 pour incorporer les rôles des nouveaux serveurs définis dans cette section.

- Dans l'unité d'organisation **Serveurs membres**, créez deux nouvelles unités d'organisation intitulées **Serveurs principaux Exchange** et **Serveurs frontaux Exchange**. Si vous disposez de plusieurs serveurs NNTP, vous pouvez créer une unité d'organisation pour eux dans l'unité d'organisation **Serveurs principaux Exchange**.
- Dans l'unité d'organisation **Serveurs frontaux Exchange**, créez des unités d'organisation séparées pour les éléments suivants (selon les besoins des services clients dans votre organisation) :
  - **Serveurs SMTP Exchange 2003**
  - **Serveurs HTTP Exchange 2003**
  - **Serveurs POP3 Exchange 2003**
  - **Serveurs IMAP4 Exchange 2003**

Vous pouvez également combiner des rôles de serveur sous la forme d'une unité d'organisation unique. Par exemple, si votre organisation exécute des services IMAP4 et POP3 sur le même ordinateur, vous pouvez créer une unité d'organisation unique appelée **Serveurs IMAP4 et POP3**. Les stratégies de sécurité contenues dans ce guide sont cumulables ; par conséquent, si vous respectez la séquence des stratégies, vous pouvez appliquer plusieurs stratégies à une unité d'organisation unique.

La figure 1 illustre la structure d'unité d'organisation recommandée pour prendre en charge les nouveaux rôles des serveurs notamment le type de modèle de sécurité et de stratégie de sécurité (fichier .inf) qui correspond à chaque unité d'organisation.

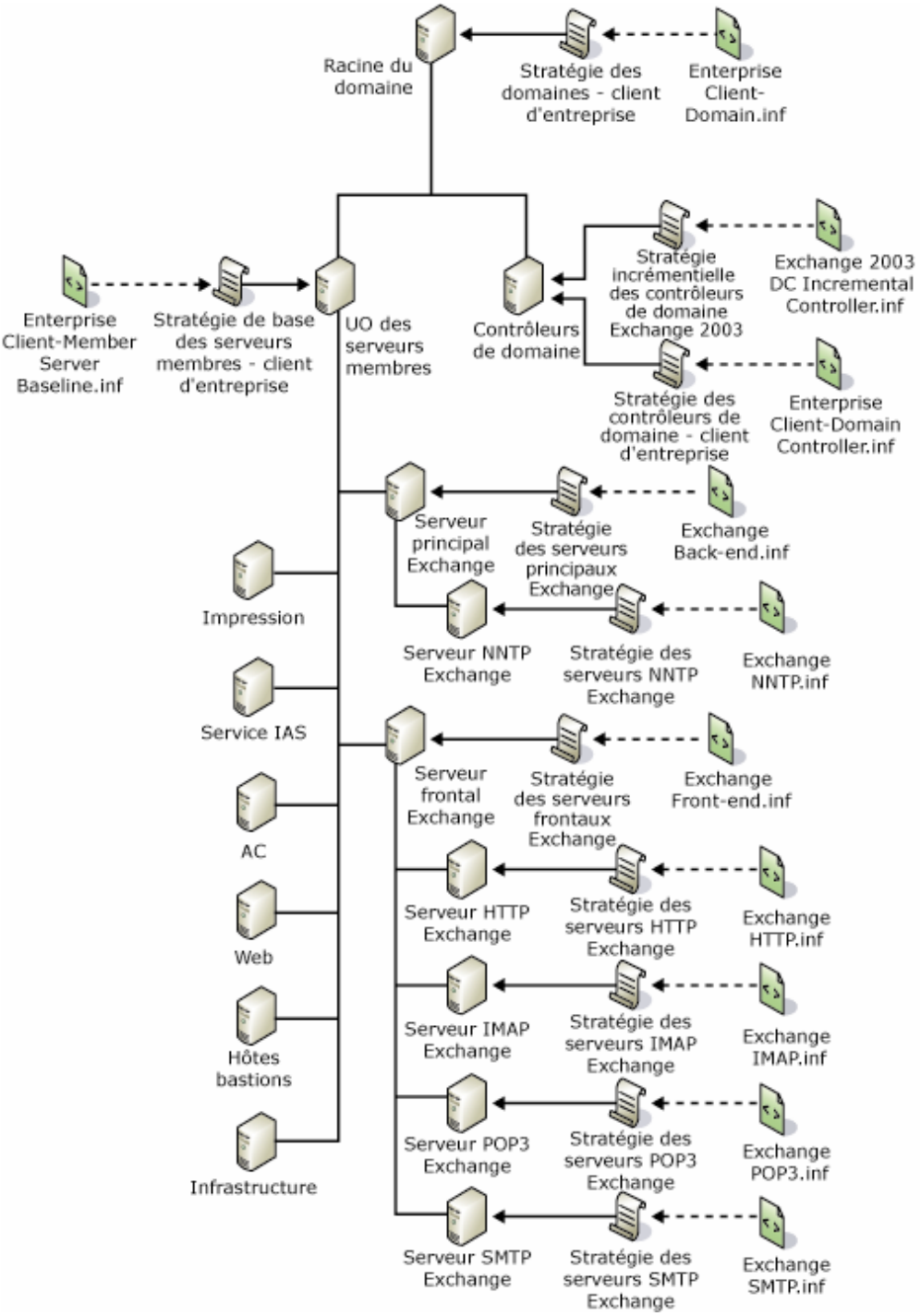

Figure 1 Structure d'unité d'organisation avec des unités d'organisation Exchange 2003 supplémentaires

Remarque La création d'une structure d'unité d'organisation en fonction des recommandations de ce guide est abordée de manière plus détaillée dans le *Guide de la sécurité Windows Server 2003* à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21638.

Comme les serveurs Exchange 2003 résident dans des unités d'organisation situées sous l'unité d'organisations **Serveurs membres**, les serveurs héritent des paramètres définis dans la stratégie de base du serveur membre. Les stratégies Exchange modifient ces paramètres de deux façons :

- Certains des services qui ne sont pas nécessaires pour les fonctionnalités de Windows Server 2003 de base sont nécessaires dans Exchange 2003.
- Exchange 2003 introduit de nombreux services supplémentaires qui ne sont pas tous nécessaires pour permettre aux serveurs Exchange d'assumer leurs rôles particuliers.

Sécurisation des rôles des serveurs dans Exchange 2003

Les modèles de sécurité de stratégie de groupes Exchange sont inclus dans ce guide pour vous aider à sécuriser les rôles des serveurs dans votre environnement Exchange 2003. Pour appliquer les modèles, vous devez les importer dans vos paramètres de stratégie de groupe.

Le tableau 12 décrit la correspondance entre les rôles des serveurs et les modèles de sécurité.

> **Important** Dans le tableau 12, la séquence des modèles de sécurité correspond à l'ordre de leur application et non pas à l'ordre de leur apparition dans le filtrage d'objet de stratégie de groupe. En fait, étant donné que les Stratégies de groupe sont mises en œuvre du haut de la liste vers le bas, l'ordre dans lequel les modèles doivent apparaître dans le filtrage d'objet de stratégie de groupe est exactement inverse.

Tableau 12 Rôles des serveurs Exchange 2003 et modèles de sécurité correspondants

Rôle des serveurs	Description	Modèles de sécurité
Serveur principal Exchange 2003	Serveur destiné à l'accès aux dossiers publics et aux boîtes aux lettres ; lors de l'utilisation de POP, IMAP4 ou NNTP, inclure le modèle incrémentiel correspondant	• Modèle de base Windows Server 2003 (client d'entreprise, client hérité, haute sécurité) • Exchange 2003 Backend.inf
Serveur frontal Exchange 2003	Paramètres courants pour tous les serveurs frontaux ; désactive tous les protocoles ; doit appliquer un protocole spécifique pour que fonctionne le serveur	• Modèle de base Windows Server 2003 (client d'entreprise, client hérité, haute sécurité) • Exchange 2003 Frontend.inf
Serveur HTTP Exchange 2003	Serveur frontal dédié pour HTTP ; utilisé par les applications Outlook Web Access, Outlook Mobile Access, Exchange Server ActiveSync et WebDAV	• Modèle de base Windows Server 2003 (client d'entreprise, client hérité, haute sécurité) • Exchange 2003 Frontend.inf • Exchange 2003 HTTP.inf
Serveur POP3 Exchange 2003	Serveur frontal dédié pour POP3 ou ajouté de manière incrémentielle à un serveur principal Exchange 2003	• Modèle de base Windows Server 2003 (client d'entreprise, client hérité, haute sécurité) • Exchange 2003 Frontend.inf • Exchange 2003 POP3.inf
Serveur IMAP4 Exchange 2003	Serveur frontal dédié pour IMAP4 ou ajouté de manière incrémentielle à un serveur principal Exchange 2003	• Modèle de base Windows Server 2003 (client d'entreprise, client hérité, haute sécurité) • Exchange 2003 Frontend.inf • Exchange 2003 IMAP4.inf
Serveur NNTP	Ajouté de manière incrémentielle	• Modèle de base Windows Server 2003

Rôle des serveurs		Modèles de sécurité
Exchange 2003	à un serveur principal Exchange 2003	(client d'entreprise, client hérité, haute sécurité) • Exchange 2003 Backend.inf • Exchange 2003 NNTP.inf
Serveur SMTP Exchange 2003	Serveur de passerelle avec accès Internet dédié pour SMTP ou tête de pont	• Modèle de base Windows Server 2003 (client d'entreprise, client hérité, haute sécurité) • Exchange 2003 Frontend.inf • Exchange 2003 SMTP.inf

Pour les serveurs frontaux, toute combinaison des stratégies HTTP, POP3, IMAP4 et SMTP peut s'appliquer en plus de la stratégie Exchange 2003 Frontend.inf. En fait, comme la stratégie de sécurité Exchange 2003 Frontend.inf désactive tous les protocoles clients Internet, vous devez appliquer l'ensemble de ces stratégies de sécurité de protocole après le déploiement d'Exchange 2003 Frontend.inf. Pour les serveurs principaux, toute combinaison de POP3, IMAP4 et NNTP peut s'appliquer en plus de la stratégie Exchange 2003 Backend.inf.

Importation des modèles de sécurité de stratégie de groupes Exchange

Les modèles de sécurité de stratégie de groupes Exchange sont contenus dans le fichier Ex03SecurityOps.exe (inclus dans ce guide). Vous devez extraire ce fichier avant d'importer les modèles de sécurité.

Ces modèles de sécurité vous permettent d'accroître la sécurité dans votre environnement Exchange 2003. Cependant, lorsque vous importez ces modèles, vous risquez de perdre des fonctionnalités dans votre environnement – ce qui peut entraîner l'échec d'applications critiques. Il est donc essentiel de tester ces modèles de manière approfondie et d'apporter des modifications appropriées avant de les déployer dans un environnement de production. Veillez à inclure des applications personnalisées, des applications tierces et d'autres logiciels qui interagissent avec votre système de messagerie dans votre test. N'oubliez pas non plus de sauvegarder chaque contrôleur et serveur de domaine avant d'appliquer de nouveaux paramètres de sécurité. Assurez-vous que la sauvegarde contient l'état du système, notamment les données du Registre et les bases de données Active Directory.

> **Remarque** La stratégie de base des contrôleurs de domaine et la stratégie de base des serveurs membres (incluse dans le *Guide de la sécurité Windows Server 2003*) définissent le niveau d'authentification LAN Manager dans NTLMv2 seulement. Pour que les clients Outlook communiquent avec les serveurs et les contrôleurs de domaine Exchange, ils doivent être également configurés pour utiliser NTLMv2.

La procédure suivante importe les modèles de sécurité de stratégie de groupes Exchange inclus dans ce guide dans la structure de l'unité d'organisation suggérée précédemment dans ce chapitre.

Pour créer les objets de stratégie de groupe et importer les modèles de sécurité de stratégie de groupes Exchange

1. Dans Utilisateurs et ordinateurs Active Directory, développez **Serveurs membres**, cliquez avec le bouton droit **Serveurs principaux Exchange**, puis cliquez sur **Propriétés**.
2. Sous l'onglet **Stratégie de groupe**, cliquez sur **Nouveau** pour ajouter un nouvel objet de stratégie de groupe (GPO, *Group Policy Object*).
3. Tapez **Stratégie des serveurs principaux Exchange**, puis appuyez sur ENTRÉE.
4. Cliquez sur **Modifier**.

5. Dans l'**Éditeur d'objets de stratégie de groupe**, sous **Configuration ordinateur**, développez **Paramètres Windows**, cliquez avec le bouton droit sur **Paramètres de sécurité**, puis cliquez sur **Importer une stratégie**.
6. **Remarque** Si **Importer une stratégie** n'apparaît pas dans le menu, fermez l'**Éditeur d'objets de stratégie de groupe** et répétez les étapes 4 et 5.
7. Dans **Importer la stratégie à partir de**, accédez à l'emplacement où vous avez enregistré les modèles de sécurité de stratégie de groupes Exchange, puis double-cliquez sur **Exchange 2003 Backend.inf**.
8. Fermez l'**Éditeur d'objets de stratégie de groupe**, puis cliquez sur **OK**.
9. Répétez les étapes 1 à 7 pour l'unité d'organisation des serveurs frontaux Exchange 2003 (à l'aide du modèle Exchange 2003 Frontend.inf) et pour chaque protocole utilisé par votre organisation.
10. Pour forcer la réplication entre vos contrôleurs de domaine afin que tous les contrôleurs de domaine se voient appliquer la stratégie, tapez **gpupdate /force** à l'invite de commande.
11. Si vous n'avez pas déjà déplacé les serveurs de l'unité d'organisation racine **Serveur membre**, déplacez un serveur pour chaque rôle vers l'unité d'organisation appropriée.
12. Sur le serveur, téléchargez la stratégie à l'aide de la commande **secedit /import /overwrite**.
13. Redémarrez chaque serveur pour garantir leur redémarrage correct et la prise d'effet des stratégies.

Utilisation d'un serveur Exchange renforcé

Si vous avez correctement exécuté la procédure de la section précédente, vous avez déplacé vos serveurs Exchange existants dans les unités d'organisation appropriées, ce qui accroît le niveau de sécurité dans votre environnement. Pour optimiser votre sécurité, vous devez déplacer les nouveaux serveurs dans l'unité d'organisation appropriée avant d'installer Exchange.

> **Remarque** Les changements que vous apportez à la configuration sur un serveur frontal renforcé nécessitent que le service Surveillance du système Microsoft Exchange soit en cours d'exécution. Le service Surveillance du système Microsoft Exchange inscrit les modifications de la configuration dans la métabase IIS, ce qui est essentiel pour la plupart des modifications de la configuration apportées au serveur frontal.

Même si votre environnement Exchange renforcé permet aux services Exchange principaux de s'exécuter, celui-ci ne vous autorise pas, par défaut, à installer ou mettre à niveau Exchange. La procédure suivante décrit la manière d'installer ou de mettre à niveau Exchange sur des serveurs renforcés.

> **Remarque** Lors de l'installation d'Exchange 2003 sur un serveur renforcé, vous recevrez des erreurs « Signature numérique non trouvée ». Cette erreur provient de l'augmentation de la sécurité sur le serveur et peut être ignorée.

Pour installer Exchange 2003 sur un serveur renforcé

1. Démarrez l'outil d'administration **Services**.
2. Dans le volet d'informations, cliquez avec le bouton droit sur **Coordinateur de transactions distribuées**, puis cliquez sur **Propriétés**.
3. Sous l'onglet **Général**, dans la liste **Type de démarrage**, sélectionnez **Automatique**.
4. Cliquez sur **Appliquer**.
5. Cliquez sur **Démarrer**.
6. Cliquez sur **OK**.
7. Répétez les étapes 2 à 6 pour les services **Network News Transport Protocol (NNTP)** et **Windows Installer**.

   > **Remarque** Si vous effectuez ces étapes sur un serveur dans l'unité d'organisation frontale d'Exchange 2003, répétez les étapes 2 à 6 pour le service **Infrastructure de gestion Windows**.
8. Installez Exchange 2003

Remarque Lors de l'installation d'Exchange 2003, à la fin du programme d'installation, une boîte de dialogue peut s'afficher pour indiquer une erreur récupérable d'installation car le service Microsoft Search n'a pas démarré. Ce scénario est prévu lors de l'installation d'un serveur renforcé et peut être ignoré.

9. Démarrez l'outil d'administration **Services**.
10. Dans le volet d'informations, cliquez avec le bouton droit sur **Coordinateur de transactions distribuées**, puis cliquez sur **Propriétés**.
11. Sous l'onglet **Général**, dans la liste **Type de démarrage**, sélectionnez **Désactivé**.
12. Cliquez sur **Appliquer**.
13. Cliquez sur **Arrêter**.
14. Cliquez sur **OK**.
15. Répétez les étapes 9 à 14 pour les services **Network News Transport Protocol (NNTP)** et **Windows Installer**.

Remarque Si vous effectuez ces étapes sur un serveur dans l'unité d'organisation frontale d'Exchange 2003, répétez les étapes 9 à 14 pour le service **Infrastructure de gestion Windows**.

Les stratégies incrémentielles pour les serveurs Exchange frontaux et principaux activent NTLMv2. Cette opération permet aux serveurs Exchange de communiquer avec vos contrôleurs de domaine renforcés. Si vous ne placez pas vos serveurs dans l'unité d'organisation appropriée avant d'installer Exchange, les serveurs ne pourront pas contacter de contrôleurs de domaine.

Annexes

Annexe A : Utilisation des autorisations et des rôles administratifs pour contrôler l'accès

Comme pour toutes les applications de votre environnement, lorsque vous définissez les autorisations pour Exchange, vous devez considérer les rôles de vos administrateurs Exchange et leur attribuer uniquement les autorisations nécessaires. Pour simplifier le processus, Exchange 2003 utilise des rôles administratifs. Un rôle administratif est un ensemble d'objets Exchange 2003 destinés à gérer et déléguer des autorisations. Un rôle administratif peut comprendre des stratégies, des groupes de routage, des hiérarchies de dossiers publics et des serveurs.

Par exemple, si votre organisation compte deux équipes d'administrateurs qui gèrent deux ensembles de serveurs Exchange 2003, vous pouvez créer deux groupes d'administration contenant ces deux ensembles de serveurs. En fonction de votre modèle d'administration, vous pouvez développer un plan d'administration qui réponde à vos besoins.

Pour octroyer facilement des autorisations de rôle Exchange aux groupes d'administration (et à l'organisation Exchange), vous pouvez utiliser l'Assistant Délégation d'administration Exchange. Pour utiliser cet assistant, vous devez être connecté comme utilisateur disposant d'un contrôle total sur l'organisation Exchange. Pour démarrer l'Assistant Délégation d'administration Exchange, dans le Gestionnaire système Exchange, cliquez avec le bouton droit sur le groupe d'administration ou l'organisation, puis cliquez sur **Déléguer le contrôle**.

Le tableau A.1 répertorie les rôles administratifs dans Exchange 2003.

Tableau A.1 Rôles administratifs dans Exchange Server 2003

Rôle	Description
Affichage Exchange seul	Accorde des autorisations permettant de lister et de lire les propriétés de tous les objets sous ce conteneur. Sauf si l'administrateur a besoin de modifier des propriétés d'objet, toujours attribuer ce rôle.
Administrateur Exchange	Accorde toutes les autorisations sauf la possibilité de prendre possession, de modifier des autorisations ou d'ouvrir des boîtes aux lettres utilisateur. Si l'administrateur doit ajouter des objets ou modifier des propriétés d'objet sans avoir à déléguer des autorisations sur les objets, attribuer ce rôle.
Administrateur intégral Exchange	Accorde toutes les autorisations à tous les objets situés sous ce conteneur sauf la possibilité d'ouvrir des boîtes aux lettres utilisateur ou d'imiter la boîte aux lettres d'un utilisateur, y compris la possibilité de modifier des autorisations. Attribuer ce rôle uniquement aux administrateurs qui doivent déléguer des autorisations aux objets. L'installation d'Exchange 2003 nécessite les autorisations d'administrateur intégral Exchange. Le premier serveur, quel que soit le domaine (y compris le tout premier de la forêt), nécessite les privilèges d'administration complète Exchange au niveau de l'organisation. Il est possible d'installer dans le même domaine des serveurs supplémentaires dont les comptes possèdent des privilèges d'administration complète au niveau du groupe d'administration.

Dans certains cas, l'Assistant Délégation d'administration Exchange ne fournit pas suffisamment de précision pour octroyer des autorisations de sécurité. Par conséquent, pour des objets individuels dans Exchange, vous pouvez modifier les paramètres sous l'onglet **Sécurité**. Cependant, par défaut, l'onglet **Sécurité** s'affiche uniquement sur les objets suivants :

- Listes d'adresses

- Listes d'adresses globales
- Bases de données (banques de boîtes aux lettres et banques de dossiers publics)
- Hiérarchie de dossiers publics de niveau supérieur

Normalement, il n'est pas nécessaire de modifier les options de sécurité sur les autres objets Exchange ; cependant, il est possible d'afficher l'onglet **Sécurité** sur tous les objets Exchange. La procédure suivante décrit la manière d'afficher l'onglet **Sécurité** sur tous les objets Exchange.

Remarque Modifiez avec prudence les autorisations sur les objets Exchange. Si vous attribuez des autorisations « Refuser », vous ne pourrez peut-être pas afficher certains objets dans le Gestionnaire système Exchange.

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 utiles.

Pour afficher l'onglet Sécurité sur tous les objets Exchange

1. Démarrez l'Éditeur du Registre (regedit).
2. Accédez à la clé suivante : **HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin**
3. Dans le menu **Edition**, cliquez sur **Ajouter une valeur**, puis ajoutez la valeur de Registre suivante :

   Nom de la valeur : **ShowSecurityPage**

   Type de données : **REG_DWORD**

   Valeur : **1**
4. Fermez l'Éditeur du Registre.

Ce changement prend effet immédiatement ; il n'est pas nécessaire de redémarrer le Gestionnaire système Exchange.

Remarque Comme vous modifiez une clé dans HKEY_CURRENT_USER, le changement n'affecte que l'utilisateur qui est connecté à l'ordinateur sur lequel vous travaillez.

Annexe B : Mise à niveau de Microsoft Exchange 2000

Lorsque vous mettez à niveau Exchange 2000 vers Exchange 2003, l'utilitaire ForestPrep et le programme d'installation d'Exchange 2003 configurent la plupart des paramètres « sécurisés par défaut » mis en œuvre avec les nouvelles installations d'Exchange 2003. Cette section explique quels paramètres de sécurité sont configurés automatiquement durant une mise à niveau et lesquels sont configurés manuellement.

Limites des messages

L'une des attaques de refus de service les plus efficaces se produit lorsqu'un système de messagerie est bombardé de messages de grande taille (plus de 20 Mo). Ce type d'attaque oblige le serveur de messagerie à déplacer d'importants blocs de données, ce qui peut affecter les entrées et sorties d'un ordinateur au point de retarder ou d'interrompre le service de messagerie.

En réponse à ce type d'attaque, Exchange 2003 définit toutes les limites de message à 10 Mo (1024 Ko). Cela inclut les messages envoyés et reçus par l'organisation Exchange. De plus, une taille limite de message de 10 Mo est imposée à tous les messages publiés dans les dossiers publics.

Lors d'une mise à niveau, l'installation d'Exchange ne change pas les limites déjà définies. L'installation d'Exchange impose ces paramètres seulement si la valeur **Aucune limite** est affectée aux limites.

Pour configurer les paramètres permettant d'envoyer ou de recevoir des messages, dans le Gestionnaire système Exchange, utilisez l'onglet **Valeurs par défaut** dans les propriétés **Remise globale du message**.

Pour configurer les paramètres de la taille de message maximale pour les dossiers publics, dans le Gestionnaire système Exchange, utilisez l'onglet **Limites** dans les propriétés **Banque de dossiers publics**.

Exchange 2003 fournit également des limites de messages pour MIME. Ces limites sont également imposées lors de la mise à niveau vers Exchange 2003. Le tableau B.1 décrit ces paramètres.

> **Remarque** Si une limite MIME est atteinte, un rapport de non remise (NDR, *Non-delivery Report*) est renvoyé à l'expéditeur.

Tableau B.1 Limites MIME

Limite	Valeur	Description
Niveaux d'imbrication	30	Nombre de composants MIME imbriqués par message
Composants du corps du message	250	Nombre maximal de composants du corps du message dans un message donné
Taille de l'en-tête de l'ID de message	1877 octets	Taille maximale de l'en-tête de l'ID de message
Taille de l'en-tête du sujet	2000 octets	Taille maximale de l'en-tête du sujet
Taille de l'en-tête MIME	2000 octets chacun	Taille maximale des en-têtes suivants : type de contenu, description du contenu, disposition du contenu, codage du transfert du contenu, identificateur du contenu, base du contenu, emplacement du contenu

Services

L'installation d'Exchange 2003 n'apporte aucune modification à la configuration des services existante. Il est fortement recommandé soit d'appliquer les modèles de stratégie de sécurité de groupes Exchange, soit de configurer les services conformément au rôle du serveur.

Outlook Mobile Access

Le paramètre permettant d'activer les fonctionnalités d'Outlook Mobile Access est défini de façon à s'exécuter sur Exchange 2003 ForestPrep. Par défaut, Exchange 2003 ForestPrep n'active pas Outlook Mobile Access. Cependant, lors d'une mise à niveau, si l'application Outlook Mobile Access est déjà activée, celle-ci n'est pas désactivée par Exchange 2003 ForestPrep.

Lecteur M:

Lors d'une mise à niveau d'Exchange 2000, le programme d'installation d'Exchange 2003 supprime le lecteur M: M:

Authentification de serveur virtuel

Lors d'une mise à niveau d'Exchange 2000, le programme d'installation d'Exchange 2003 renforce certaines instances de serveur virtuel de POP3, IMAP4 et NNTP.

Serveurs virtuels POP3 et IMAP4

Lors de la mise à niveau d'un ordinateur Exchange 2000 configuré comme serveur frontal, le programme d'installation Exchange 2003 désactive l'accès anonyme et active l'authentification de base sur les serveurs virtuels POP3 et IMAP4. Si vous mettez à niveau un serveur principal, les instances de serveur virtuel ne sont pas modifiées.

Serveurs virtuels NNTP

Lors d'une mise à niveau, le programme d'installation d'Exchange 2003 modifie les instances par défaut des serveurs virtuels NNTP. En particulier, l'authentification anonyme est désactivée et l'authentification de base et l'authentification intégrée Windows sont activées. Les serveurs virtuels non définis par défaut (instances de serveur virtuel non créées par le programme d'installation) ne sont pas modifiés lors de la mise à niveau. Si vous créez de nouvelles instances de serveur virtuel NNTP, assurez-vous qu'une authentification appropriée est nécessaire.

Refus d'accès local pour les utilisateurs du domaine

Dans Exchange 2003, les utilisateurs de domaine ne peuvent pas se connecter localement au serveur Exchange. Lors d'une mise à niveau, le programme d'installation d'Exchange configure la stratégie d'ordinateur local pour refuser l'accès local aux utilisateurs du domaine.

Création de dossiers publics de niveau supérieur

Dans Exchange 2003, des membres du groupe Tout le monde et des utilisateurs Anonymes ne peuvent pas créer une hiérarchie de dossiers publics de niveau supérieur. Lors d'une mise à niveau, Exchange 2003 ForestPrep configure ce paramètre de contrôle d'accès.

Configuration de contrôle d'accès

Pour les mises à niveau comme pour les nouvelles installations, le programme d'installation d'Exchange 2003 applique les listes de contrôle d'accès aux répertoires qu'il crée selon les listes de contrôle d'accès explicites définies dans le répertoire Program Files. Si vous ou un autre administrateur modifiez les listes de contrôle d'accès par défaut dans le répertoire Program Files, le programme d'installation d'Exchange 2003 applique cette modification à la plupart des répertoires créés lors de l'installation. En dehors des modifications explicites, les répertoires sont autrement verrouillés. Cependant, quelles que soient les listes de contrôle d'accès explicites présentes dans le répertoire Program Files, le programme d'installation d'Exchange configure le répertoire Mailroot (situé dans \Program Files\Exchsrvr) afin de supprimer l'accès du compte Invité et l'accès anonyme.

Il est fortement recommandé de configurer le contrôle d'accès sur les répertoires Exchange. Pour obtenir des informations sur la configuration de contrôle d'accès sur vos répertoires Exchange, consultez « Renforcement des serveurs principaux » précédemment dans ce guide.

Annexe C : Ports utilisés dans Exchange 2003

Le tableau C.1 répertorie les services Exchange 2003 et leurs ports correspondants. Pour plus d'informations sur la configuration de vos serveurs frontaux et principaux Exchange, ainsi que les ports associés à divers scénarios, consultez l'article technique « *Using Microsoft Exchange 2000 Front-End Servers* », à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=14575. Bien que cet article concerne Exchange 2000, les informations qu'il contient sont également applicables à Exchange 2003.

Tableau C.1 Ports utilisés dans Exchange 2003

Services (dépendances)	Ports entrants	Ports sortants (initialisent les connexions vers)	Remarques
Surveillance du système Microsoft Exchange	135 et autre RPC 6002 pour DsProxy RpcHHTP 6004 pour Dsreferral RpcHTTP		Tous les services Exchange principaux nécessitent le service Surveillance du système Microsoft Exchange. DsProxy et DsReferral pour RpcHTTP sont codés en dur vers 6002 et 6003. Destiné à l'accès RPC sur HTTP Outlook.
Banque d'informations Microsoft Exchange (surveillance du système Microsoft Exchange)	135 et autre RPC 6001 pour Store RpcHTTP	Paquets UDP (User Datagram Protocol) vers les ports aléatoires pour la notification de nouveau courrier	Exécute les bases de données Exchange. La banque pour RPC sur HTTP a été codée en dur vers le port 6001. Destiné à l'accès RPC sur HTTP Outlook.
Piles MTA Microsoft Exchange (surveillance du système Microsoft Exchange)	135 et autre RPC 102 pour X.400 sur TCP	135 et autre RPC 102 pour X.400 sur TCP	Microsoft Exchange - Piles MTA nécessaires pour déplacer des connexions utilisateurs et des connexions héritées vers des serveurs Exchange 5.5. Port 102 ouvert uniquement pour des connexions X.400 actives.
Protocole SMTP (Simple Mail Transfer Protocol) (service d'administration IIS)	25	25	La banque Exchange requiert le service SMTP.
Moteur de routage Microsoft Exchange (service d'administration IIS)	691	691	Service du moteur de routage
Service de publication sur le World Wide Web (service d'administration IIS)	80 et 443	80 sur le serveur frontal	Nécessaire pour l'administration des dossiers publics et Outlook Web Access
Microsoft Exchange POP3 (service d'administration IIS)	110 et 993 (SSL)	110 sur le serveur frontal	Nécessaire pour l'accès POP3
Microsoft Exchange IMAP4	143 et 995 (SSL)	143 sur le serveur frontal	Nécessaire pour l'accès IMAP4

Services (dépendances)	Ports entrants	Ports sortants (initialisent les connexions vers)	Remarques
(service d'administration IIS)			
Protocole NNTP (Network News Transfer Protocol) (service d'administration IIS)	119 et 563 (SSL)		S/O
Service de réplication de sites Microsoft Exchange	379, 135 et autre RPC	135 et autre RPC	Dépend si les serveurs Exchange 5.5 sont dans l'organisation
Connecteur Active Directory	S/O	379, 389 peuvent être configurés	Dépend si les serveurs Exchange 5.5 sont dans l'organisation
Événement Microsoft Exchange (banque d'informations de Microsoft Exchange)			Pas automatique par défaut
Gestion d'Exchange (Infrastructure de gestion Windows)			Ce service n'est pas nécessaire, cependant, Microsoft Operations Manager et d'autres programmes ne fonctionnent pas sans ce service.

Annexe D : Ressources

Pour des informations sur Microsoft Exchange Server, consultez le site Web de Microsoft Exchange Server à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=81. En outre, les ressources suivantes fournissent des informations précieuses concernant les processus et les concepts en matière de sécurité.

> **Remarque** Pour télécharger un fichier auto-extractible des articles techniques et des ouvrages en ligne de l'équipe de développement d'Exchange, visitez le site Web à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=10687.

Manuels consacrés à Exchange Server 2003

Nouveautés dans Exchange Server 2003
(http://go.microsoft.com/fwlink/?linkid=21765)

Guide d'administration d'Exchange Server 2003
(http://go.microsoft.com/fwlink/?linkid=21769)

Articles techniques

Guide de la sécurité Windows Server 2003
(http://go.microsoft.com/fwlink/?LinkId=21638)

Using Microsoft Exchange 2000 Front-end Servers
(http://go.microsoft.com/fwlink/?linkid=4721)

Microsoft Operations Framework (MOF) Service Management Function Library Overview
(http://go.microsoft.com/fwlink/?LinkId=21639)

Using ISA Server 2000 with Exchange Server 2003
(http://go.microsoft.com/fwlink/?linkid=23232)

Security Operations Guide for Exchange 2000 Server
(http://go.microsoft.com/fwlink/?linkid=11906)

Customizing Outlook 2003 to Help Prevent Viruses
(http://go.microsoft.com/fwlink/?LinkId=24545)

Sites Web

Microsoft Operations Framework
(http://go.microsoft.com/fwlink/?LinkId=21640)

Programme de protection technologique stratégique de Microsoft
(http://go.microsoft.com/fwlink/?LinkId=21643)

Confidentialité et sécurité Microsoft
(http://go.microsoft.com/fwlink/?LinkId=21633)

Notions fondamentales sur la confidentialité et sécurité Microsoft
(http://go.microsoft.com/fwlink/?LinkId=24701)

Ressources de sécurité pour Exchange Server 2003
(http://go.microsoft.com/fwlink/?LinkId=21660)

Microsoft Baseline Security Analyzer (MBSA)
(http://go.microsoft.com/fwlink/?linkid=17809)

Filtre du courrier indésirable sur MSDN
(http://go.microsoft.com/fwlink/?LinkId=24395)

Filtre de messages intelligent Microsoft Exchange
(http://go.microsoft.com/fwlink/?linkid=21607)

Outil de sécurité URLScan
(http://go.microsoft.com/fwlink/?LinkId=24490)

Microsoft Office Online
(http://go.microsoft.com/fwlink/?LinkId=24348)

Pour une présentation en détail des Événements système de stockage Web natifs, consultez le Kit de développement (SDK) Microsoft Exchange (en anglais) à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21641.

Bibliothèque de documentation technique d'Exchange Server
http://go.microsoft.com/fwlink/?linkid=21277

Kits de ressources

Kit de ressources Microsoft Exchange 2000 Server
(http://go.microsoft.com/fwlink/?LinkId=6543)

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 Windows 2000
(http://go.microsoft.com/fwlink/?LinkId=6545)

Vous pouvez commander un exemplaire du *Kit de ressources Microsoft Windows 2000* auprès de Microsoft Press à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=6546.

Kit de ressources Microsoft Office 2003 Éditions
(http://go.microsoft.com/fwlink/?LinkId=24546)

Vous pouvez commander un exemplaire du *Kit de ressources Microsoft Office 2003 Éditions* auprès de Microsoft Press à l'adresse suivante : http://go.microsoft.com/fwlink/?linkid=21757.

Articles de la Base de connaissances Microsoft

Les articles de la Base de connaissances Microsoft suivants sont disponibles sur le Web à l'adresse http://go.microsoft.com/fwlink/?linkid=14898 :

319356, « HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000 Server »
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=319356)

309622, « XADM: Clients Cannot Browse the Global Address List After You Apply the Q299687 Windows 2000 Security Hotfix »
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=309622)

313807, « XADM: Enhancing the Security of Exchange 2003 for the Exchange Domain Servers Group »
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=313807)

309677, « XADM: Known Issues and Fine Tuning When You Use the IIS Lockdown Wizard in an Exchange 2000 Environment »
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=309677)

316685, « Active Directory-Integrated Domain Name Is Not Displayed in DNS Snap-in with Event ID 4000 and 4013 Messages » (cet article fournit des informations sur l'activation de l'audit des succès pour les événements d'ouverture de session dans le journal de la sécurité)
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=316685)

259373, « XADM: W3SVC Logs Event ID 101 in the System Event Log »
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=259373)

Accessibilité

Pour plus d'informations sur l'accessibilité pour les personnes atteintes de handicaps, consultez le site Web de Microsoft sur l'accessibilité à l'adresse suivante : http://go.microsoft.com/fwlink/?LinkId=21487.

Cet ouvrage vous a-t-il aidé ? Donnez-nous votre avis. Sur une échelle de 1 (médiocre) à 5 (excellent), quelle note donneriez-vous à cet ouvrage ?

Adressez vos commentaires à exchdocs@microsoft.com.

Pour obtenir les informations les plus récentes concernant Exchange, visitez les sites Web suivants (en anglais) :

- Ensemble des articles techniques et ouvrages de l'équipe de développement de Microsoft Exchange (http://go.microsoft.com/fwlink/?linkid=21277)
- Outils et mises à jour Exchange
  http://go.microsoft.com/fwlink/?linkid=21316
- Fichier auto-extractible contenant tous les articles techniques et ouvrages de l'équipe de développement de Microsoft Exchange
  http://go.microsoft.com/fwlink/?LinkId=10687
- Communauté Exchange Server
  http://go.microsoft.com/fwlink/?linkid=14927