frank CARIUS
ingrid MANTKE

MICROSOFT EXCHANGE SERVER 2003

GRUNDLAGEN UND KONZEPTE FÜR DIE EINFÜHRUNG UND DEN BETRIEB ALS KOMMUNIKATIONS-PLATTFORM

3., aktualisierte Auflage

HANSER

Carius/Mantke

Microsoft **Exchange Server 2003**

Grundlagen und Konzepte
für die Einführung und den Betrieb
als Kommunikationsplattform

3., aktualisierte Auflage

Frank Carius
Ingrid Mantke

Microsoft
Exchange Server 2003

Grundlagen und Konzepte
für die Einführung und den Betrieb
als Kommunikationsplattform

3., aktualisierte Auflage

HANSER

Die Autoren:

Dipl.-Ing. Frank Carius, Paderborn
Ingrid Mantke, Gütersloh

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Lektorat: Fernando Schneider
Herstellung: Monika Kraus
Umschlagdesign: Marc Müller-Bremer, Rebranding, München
Umschlaggestaltung: MCP · Susanne Kraus GbR, Holzkirchen
Datenbelichtung, Druck und Bindung: Kösel, Krugzell
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702
Printed in Germany

ISBN-10: 3-446-40612-3
ISBN-13: 978-3-446-40612-4

www.hanser.de/computer

Inhalt

Teil I

Teil I

Der erste Teil des Buches enthält
die neuen Funktionen von
Exchange 2003 inkl. Service Pack 2
sowie wichtige Grundlagen.

1

Einführung

1 Einführung

1.1 Ausgangslage und Zielsetzung

Seít dem Start der Webseite www.msexchangefaq.de zeigen die hohen Zugriffszahlen, dass trotz aller Dokumentationen und Assistenten ein hoher Bedarf an Fachinformationen zu Microsoft Exchange besteht. Das Release von Microsoft Exchange 2003 ist ein willkommener Anlass, ein Buch hierzu diesem Produkt in deutscher Sprache zu schreiben, das über die eigentliche Produktbeschreibung hinausgeht. Dieses Werk reiht sich ein in die Serie der anderen Computerfachbücher des Hanser Verlags zu Windows 2000 und Windows 2003, dem Internet Information Server und anderen Microsoft-Server wie z.B. dem SQL-Server, dem ISA-Server oder dem Small Business Server.

Neu: Service Pack 2

Ein Buch kann besser auf einen Leser zugeschnitten werden als eine Webseite. Mangels Hyperlinks und anderer Gestaltungsmerkmale mussten die Inhalte daher komplett neu aufbereitet werden. Auf der anderen Seite ist ein Buch eine große neue Herausforderung für uns, und wir hoffen, auch mit der dritten Auflage Ihre und unsere Erwartungen zu erfüllen. In ihr werden die Neuerungen des Exchange Service Pack 2 berücksichtigt, die im Betrieb von Bedeutung sind. Ebenso haben wir einige Korrekturen sowie weitere Aktualisierungen vorgenommen.

Erfahrungswerte

Dieses Buch ist die Summe der Erfahrungen und Ergebnis Franks jahrelanger Arbeit in den Microsoft Newsgroups als MVP und seiner Webseite www.msexchangefaq.de sowie unserer eigenen Erfahrungen mit Exchange. Mit ein wenig Genugtuung stellen wir fest, dass an einem ganz normalen Werktag bis zu 5.000 Benutzer die Web-Informationen abrufen — mit steigender Tendenz. Unser Anliegen war es, beide Welten zu verbinden: die Aktualität und Problemorientierung einer Webseite mit der klaren statischen Struktur eines Buches. Auf einer Webseite können Sie gezielt etwas suchen aber auch wild umherspringen. Das Buch dagegen erfordert eine klare, strukturierte Linie und erlaubt Ihnen die Einarbeitung in das Thema, ohne am Computer zu sitzen.

Die zahlreichen Besucher der Webseite werden beim Lesen die eine oder andere Parallele zum Buch erkennen. Dies ist nicht immer zu vermeiden, zumal auch das Thema übereinstimmt. Aber es gibt auch sehr viel Neues und Interessantes zu lesen, selbst wenn Sie die „MS Exchange FAQ“ auswendig kennen würden.

Hauptmerkmal

Die Besonderheit dieses Buches ist die Verzahnung von Konzepten und einer praktischen Anleitung anhand von Beispielen gestützt auf den Erfahrungen aus der Praxis. Der Schwerpunkt ist weniger eine Vorstellung aller Funktionen von Exchange 2003 mit entsprechenden Bildern, sondern die Fokussierung auf die Bereiche, die von der Mehrzahl der Exchange-Administratoren im Betrieb benutzt werden. Bei den Konzepten haben wir uns die Freiheit erlaubt, von der geraden Linie einer Exchange-Installation etwas abzuweichen, um aus unserer Sicht wichtige Zusatzinformationen zu beschreiben.

1.2 Zielgruppe

Wer es lesen sollte

Dieses Buch soll all jene unterstützen, die mit der Aufgabe betreut sind, einen Exchange-Server in ihrem Unternehmen zu planen, zu implementieren und zu administrieren. Es spricht also alle an, vom Exchange-Neuling über den erfahrenen Administrator bis hin zum IT-Spezialisten.

Ein Teil des Buches widmet sich der Installation einer Musterumgebung, die aber nicht so detailliert ausgeführt ist, dass sie einer Anleitung für Dummies gerecht wird. Sie begleitet die Kapitel für die Planung, die Installation und den Betrieb von Exchange 2003, bietet eine Checkliste für die Dokumentation und beschreibt eine sinnvolle Vorgehensweise der Installation. Das Buch stellt keinen Ersatz für das Administratorhandbuch von Microsoft oder die Microsoft TechNet als Nachschlagewerk für Probleme dar. Es baut vielmehr auf unseren Erfahrungen aus der Praxis und den Fragen der Newsgroup auf und soll all die Themen ausführlicher behandeln, die in offiziellen Dokumentationen zu kurz kommen.

Die Versuchung war groß, einige komplexe, aber wichtige Sachverhalte zu beschreiben und dadurch viele Leser abzuschrecken. Es ist durchaus ein Unterschied, ob eine Firma mit wenigen Standorten Exchange 2003 installiert bzw. migriert oder ob große Firmen mit mehreren tausend Postfächern eine kleine Änderung durchführen. Trotzdem hoffen wir, dass jeder Leser hier nützliche Informationen findet und das Buch damit eine möglichst breite Zielgruppe anspricht. Großkonzerne mit Tausenden von Benutzern und Hunderten Servern in verschiedenen Ländern dieser Welt werden nicht allein anhand dieses Buches eine Migration oder Installation starten, aber vielleicht kann es auch Ihnen mit der einen oder anderen Anregung dienen.

Das Ziel des Buches ist die theoretische und praktische Hilfestellung bei der Exchange-Installation sowie deren Vorbereitung und Erweiterung. Es kann Sie nicht zu einem Spezialisten für Exchange machen und auch keine Schulung ersetzen, aber Ihnen persönliche Erfolgserlebnisse bescheren und den Einstieg in die faszinierende Welt von Microsoft Exchange erleichtern.

Für die Beispielinstallation sind bestimmte Annahmen gemacht worden, die sich in den letzten Jahren unserer praktischen Tätigkeit als sinnvoll oder notwendig herausgestellt haben.

1.3 Struktur und Aufbau

Inhalt des Buches

Dieses Buch ist in fünf Teile untergliedert, die ihrerseits aus mehreren Kapiteln bestehen. Bei dem Entwurf der Gliederung war es nicht immer einfach, bestimmte Texte so einzuordnen, dass sie auch für Sie als Leser leicht zu finden sind. Schließlich sind die Themen sehr stark miteinander verzahnt.

- Teil 1

Grundlagen

Der erste Teil, den Sie gerade lesen, beschreibt neben den Informationen zum Buch die neuen Funktionen von Exchange 2003 sowie des Service Pack 2. Auf eine komplette Auflistung aller Exchange 2003-Funktionen wird hier verzichtet; diese können Sie bei Microsoft im Internet nachlesen. Grundlagen wie E-Mail, Internet-Mail, Exchange-Lizenzierung und -Versionen werden hier kurz erläutert.

- Teil 2

Konzepte

Dieser Teil ist ganz den Konzepten gewidmet, die für uns die Basis einer E-Mail-Infrastruktur darstellen. Wer sofort mit einer Installation von Exchange anfangen möchte, kann zu Teil 3 springen. Die Kapitel in Teil 2 widmen sich den logischen Bausteinen einer Exchange-Installation. Alle Konzepte sind so geschrieben, dass sie Ihnen einen Einblick in die Planung einer Exchange-Installation bieten und das Verständnis für den Betrieb vermitteln.

- Teil 3

How to

Hier werden Sie ganz praktisch durch die Installation einer beispielhaften Exchange-Umgebung geführt. Die Installation ist nicht als Schritt-für-Schritt-Anleitung für Anfänger zu verstehen, sondern führt wie ein roter Faden durch die einzelnen Phasen der Installation – von Windows 2003 Service Pack 1 mit Active Directory, dem Exchange-Server selber bis hin zu der Internet-Anbindung und den Client-Zugriffsmöglichkeiten. Diesen Teil haben wir in der dritten Auflage um das Update bzw. die Installation von Service Pack 2 und seinen Funktionen erweitert. Das Buch bringt Sie dazu, entsprechende Parameter festzulegen und zu dokumentieren, indem es kurz deren Bedeutung wiederholt. Für einige Dinge sollten Sie vorab die Konzepte der vorangegangenen Kapitel gelesen haben. Sie können die Installation parallel durchführen oder angepasst auf Ihr Umfeld modifizieren.

Für diese Installation haben wir einige Randbedingungen und Voraussetzungen festgelegt, die später beschrieben sind.

- Teil 4

  Enterprise

  Dieser Teil widmet sich den weiterführenden Konzepten und Umsetzungen, die über die „Ein Server“-Installation hinausgehen. Teil 4 unterscheidet sich von den Teilen 2 und 3 dadurch, dass die einzelnen Themen konzeptionell erläutert werden, ohne eine Installationsanleitung zu allen Inhalten, nicht jedes Unternehmen setzt diese Funktionen ein. Zudem haben Sie in der Regel die Wahl zwischen vielen verschiedenen Produkten. Anhand konkreter Beispiele erfahren Sie etwas über die Einbindung weiterer Standorte und Server sowie die Verbindung zu anderen Systemen. Das Kapitel zur Migration schließlich soll einen Einblick in die verschiedenen Möglichkeiten geben; sein Schwerpunkt liegt auf der Beschreibung der einzelnen Migrationsarten, damit Sie selbst die Variante finden, die in Ihrem Umfeld die vermutlich beste Migration verspricht. Eine detaillierte Beschreibung würde ein ganzes Buch füllen und hier zu weit führen. Mit Service Pack 1 ist dieses Kapitel um den Punkt „Konsolidierung von Standorten“ erweitert worden.

- Teil 5

  Dokumentvorlagen

  Dieser Teil ist ganz der Dokumentation gewidmet. Hier finden Sie Vorlagen und Checklisten, die exemplarisch zeigen, wie Sie wichtige Informationen festhalten können. Es ist ein Wink mit dem Zaunpfahl, da dies meistens vernachlässigt wird und im Notfall unersetzlich ist. Im Anhang finden Sie darüber hinaus Anlagen, Verzeichnisse und Dokumentationsvorlagen sowie eine Auflistung der CD-Inhalte.

Administration und Betrieb

Alle Bereiche der Administration sind durch die Kapitel 7 bis 11 abgedeckt und werden durch die Videodateien auf der CD komplettiert. Vieles davon finden Sie auch in den Konzepten und Grundlagen. Die Administration einiger Exchange-Objekte kann ebenso aus Outlook heraus erfolgen wie die Pflege der Verteiler, das Anlegen Öffentlicher Ordner-Strukturen sowie die Vergabe von Stellvertreterberechtigungen und Einstellung von Regeln. Die tägliche Administration der Benutzerobjekte, die in der Version 5.5 noch über ein eigenständiges Administratorprogramm abgewickelt wurde, ist seit der Version 2000 im Active Directory enthalten. Viele dieser Aufgaben lassen sich mit einem Administrationsprogramm von Drittherstellern oder mit eigenen Entwicklungen komfortabel umsetzen.

1.4 Weitere Funktionen

Was fehlt?

Einige Funktionen von Exchange 2003 werden im „normalen“ Betrieb nicht verwendet und würden auch den Inhalt des Buches sprengen. Trotzdem stellt

sich dann die Frage: „Was fehlt?“ Eine Auflistung der wichtigen und nicht enthaltenen Funktionen finden Sie in dem Kapitel „Exchange 2003 im Überblick“.

1.5 Die Beispielinstallation im Buch

Anforderungen für die Installation

In einigen Kapiteln dieses Buches werden anhand einer Exchange 2003-Installation mit Service Pack 2 die einzelnen Komponenten und Funktionen erklärt. Die Installationsbeschreibung folgt dem oben erwähnten roten Faden, schwingt jedoch immer wieder nach links und rechts aus, um Randinformationen zu liefern und etwas mehr als das unbedingt Notwendige zu erklären. Der Schwerpunkt aller Texte liegt in der Erklärung, warum bestimmte Konfigurationen und Einstellungen so und nicht anders angenommen wurden und wie Sie diese für Ihre Umgebung anpassen sollten. Sie finden Hintergrundinformationen, so dass Sie daraus lernen und selbst entscheiden können, welche Einstellungen in Ihrem Unternehmen erforderlich sind. Erwarten Sie aber keine Installationsanweisung, die Ihnen jeden Bildschirm und jeden zu drückenden Knopf erklärt.

Die Installation erfolgt in mehreren Stufen, für die Sie entsprechende Ressourcen bereitstellen müssen.

Tabelle 1.1 Voraussetzungen für die Installation

Kapitel	Tätigkeiten	Ressourcen	Hinweis
Kapitel 7	Installation des ersten Servers	Server-Hardware Windows 2003 Server-CD Windows 2003 (Service Pack 1) Hersteller-CD mit Treibern MS Hotfixe	Sie benötigen einen Server, der für die Installation in einem Testumfeld installiert werden kann. Für den Test muss es kein High-End-Server sein, aber wenn Sie auch später die komplette Konfiguration mit RAID, Bandlaufwerk und anderen Komponenten nutzen wollen, dann ist dies der optimale Platz.
Kapitel 8	Installation des ersten Exchange-Servers, Update Service Pack 2 Installation ExBPA	Exchange 2003-CD Download Exchange 2003 Service Pack 2 ExBPA	Prüfen Sie, welche Version (Standard oder Enterprise) für Ihr Unternehmen benötigt wird. Bei späteren Installationen sollten weitere Service Packs und Hotfixes berücksichtigt werden. Setzen Sie ExBPA zur Überprüfung ein.

Kapitel	Tätigkeiten	Ressourcen	Hinweis
Kapitel 9	Anbindung der Clients	Client-PCs Windows 2000/XP-CD Outlook/Office 2003-CD	Ein zweiter und eventuell dritter PC im Netzwerk dient zur Installation und für erste Tests der Client-Anbindung und Exchange 2003-Features.

Begleitende Bildschirmvideos finden Sie auf der CD. Zur Niederschrift der definierten Daten steht ein vorbereitetes Formular am Ende des Buches und auf der Begleit-CD zur Verfügung.

1.5.1 Organisatorische Voraussetzungen

Die beispielhafte Installationsbeschreibung basiert, wie schon erwähnt, auf einigen Annahmen, die von Ihrem individuellen Umfeld abweichen können. Daher ist es sinnvoll, die Installationsschritte mit einem Testsystem durchzuspielen, ehe Sie diese dann für Ihre Produktionsumgebung anpassen. Komplexe Systeme und spezifische Umgebungen werden erst einmal außer Acht gelassen, die Grundlagen können dadurch einfacher erworben und vertieft werden.

Eine Firma

Ausgangssituation für die Installation

Wir gehen zuerst von einem Unternehmen aus, Firma genannt, und nicht von einem Firmenverbund mit einer Holding, Töchtern und Beteiligungen. Diese Einschränkung ist notwendig, um die Installation nicht mit allzu viel „Wenn und Aber“ durchzuführen. Glücklicherweise entspricht dies sehr vielen Szenarien in Deutschland, wo es sehr viele kleine und mittlere Unternehmen gibt, die mit diesem Ansatz problemlos starten können.

Ein Standort

Die zweite Einschränkung für die erste Stufe ist die Limitierung auf einen Standort. Damit werden alle Besonderheiten einer verteilten Installation und einer Replikation des Active Directory über Weitverkehrsverbindungen zunächst ausgeschlossen. Die Erweiterung um weitere Standorte wird im Anschluss an diese Basiskonfiguration erklärt.

Eine Domäne

Als ebenfalls notwendige und sinnvolle Vereinfachung sehen wir die Beschränkung auf eine Domäne im Active Directory. Aus unserer praktischen Erfahrung heraus empfehlen wir die Minimierung der Anzahl an Domänen. Das Active Directory bietet Möglichkeiten, mehrere Standorte in einer Domäne zusammenzufassen und die Replikation effektiv zu steuern.

Dieser Ansatz kann auch für größere Unternehmen ein praktikabler Ansatz sein, denn so gestalten sich Planung und Installation recht einfach. Die Erweiterung um zusätzliche Domänen wird dann in einem Folgekapitel beschrieben.

Ein Server

Wir installieren zunächst einen einzigen Exchange 2003-Server. In den meisten kleinen Firmen ist dieses System zugleich auch der Domänencontroller. Erst ab einer bestimmten Größe lohnt es sich, drei und mehr Server zu betreiben, so dass eine Trennung der Funktionen erfolgen kann. Solange Sie nur drei oder weniger Server haben, ist die Redundanz durch mehrere Domänencontroller wichtiger als die Trennung der Funktionen. Der Einsatz von Exchange auf einem Mitgliedsserver ist einfacher als die Kombination mit einem Domänencontroller.

Eine Maildomäne

Exchange kann Empfänger mit unterschiedlichen Maildomänen verwalten. Um das Setup übersichtlich zu gestalten, gehen wir zunächst von einer Maildomäne der Firma aus, für die Exchange verantwortlich ist. Es gibt keine weiteren Mailserver mehr, an die Nachrichten weitergeleitet werden müssen. Diese Einschränkung wird in einem Folgekapitel wieder aufgehoben.

Externer DNS beim Provider

Weiterhin setzen wir voraus, dass ein Internet Service Provider (ISP) den DNS-Server betreibt und dafür sorgt, dass Nachrichten an die Maildomäne der Firma über das Mail-Relay des Providers bzw. direkt an den Exchange-Server zugestellt werden. Damit kann intern ein eigener DNS-Server vereinfacht installiert und eingesetzt werden. Dies ist häufig der Regelfall. Nur Unternehmen mit eigener Festverbindung, Firewall und entsprechendem Know-how betreiben den DNS-Server für das Internet selbst.

Internet-Anbindung

Unter den verschiedenen Varianten von Internet-Anbindungen haben wir die Anbindung als Beispiel gewählt, die zu akzeptablen Kosten eine gewisse Sicherheit und Stabilität bietet. Exchange kommuniziert dabei mit dem Internet über einen dedizierten Router, der die Verbindung herstellt und die Adressen mittels NAT umsetzt. Dieses Verfahren deckt damit die ISDN-Wählleitungen, den DSL-Volumentarif sowie die Flatrate mit dynamischen IP-Adressen als mögliche Verbindungsarten ab. Der Versand erfolgt per SMTP über den Smarthost des Providers. Zum Empfang werden verschiedene Verfahren aufgezeigt. Zusätzlich wird eine Standleitung mit Firewall erläutert.

Diese Einschränkungen sind notwendig, damit Sie ein installiertes Grundsystem bekommen, das alle wichtigen Funktionen erfüllt. Individuelle schrittweise Anpassungen sind ausgehend von einem lauffähigen System einfacher möglich als die Beschreibung aller möglichen Kombinationen von Beginn an..

Ergebnis

Nach Durcharbeitung dieser Kapitel sollten Sie einen funktionstüchtigen Exchange-Server vor sich haben, mit dem Sie weitere Erfahrungen und Tests durchführen können. Basierend auf dieser Grundlage werden in den Folgekapiteln die möglichen Erweiterungen mit Connectoren, weiteren Standorten und Servern, aber auch zusätzliche Domänen oder vertraute Domänen beschrieben.

Migration?

Wenn Sie die Daten aus einem bestehenden Exchange 5.5-Mailsystem übernehmen wollen, dann sollten Sie zuerst das Kapitel zur Migration lesen. Die erforderlichen Vorarbeiten sind abhängig vom gewählten Migrationsweg. Die frische Installation eines Exchange 2003-Servers ist zu empfehlen, wenn kein parallel zu betreibendes Exchange 5.5-System vorhanden ist. Sie sollten trotzdem erst in einem Testumfeld die Neuinstallation mit Exchange 2003 üben, um das System entsprechend kennen zu lernen.

1.6 Schreibweisen

Wir möchten den Lesern ein handliches Nachschlagewerk bieten und haben daher der Übersichtlichkeit halber bewusst auf Symbole verzichtet. Stattdessen haben wir uns für eine geringe Anzahl von unterschiedlichen Schreibweisen entschieden, die wir nachfolgend erläutern werden. Am Seitenrand finden Sie ebenfalls kurze Notizen, die auf den Inhalt des Absatzes oder auf wichtige Stichworte hinweisen ebenso wie die Überschriften zu Tabellen und Grafiken.

Formatierungen

Im Buch werden folgende Schreibweisen verwendet, um den Text lesbar und übersichtlich zu gestalten:

- SCHALTFLÄCHEN UND MENÜPUNKTE

  Dialogfelder, Schaltflächen und Menüpunkte und -optionen werden wie bei ÖFFNEN in Kapitälchen gesetzt.

- *Hervorhebungen*

  Hervorgehobene Informationen, selbst gewählte Namen sowie Wörter im Text, denen eine besondere Bedeutung zukommen soll, werden *kursiv* dargestellt. Dies gilt auch für Kommentare.

- Befehle und Befehlszeilen

  Die im laufenden Text genannten Befehle werden in nichtproportionaler Schrift gesetzt, beispielsweise `netdiag`, `winroute`, ebenso wie Beispielcodes. Befehlszeilen werden zusätzlich grau hinterlegt und stehen in einer eigenen Zeile.

```
eseutil /mh priv.edb
```

- Sonderzeichen

  Spitze Klammern stehen für Platzhalter wie bei http://<server name>/Exchange und verweisen auf die Eingabe des Server-Namens. Ordnernamen erkennen Sie an den Anführungsstrichen („Exchsrvr“). Pfadnamen werden mit \ dargestellt (C:\Winnt, \\servername), wie in der Systemsyntax. Tastatureingaben wie [Strg] sind in eckigen Klammern dargestellt, ein + verbindet mehrere Tasten.

- Groß- und Kleinschreibung

  Dateinamen wie priv.edb werden kleingeschrieben, Abkürzungen (E2K) in Großbuchstaben.

Begrifflichkeiten

- Kurznamen

  Zur einfacheren Lesbarkeit werden viele Produkte mit ihrem „Kurznamen“ bezeichnet, also statt Microsoft Exchange 2003-Server einfach nur Exchange, dies gilt auch für Outlook, Windows usw. Nur bei Bedarf ist die Version mit angegeben.

- Abkürzungen

  Viele spezifische Begriffe werden häufig abgekürzt. Im Anhang finden Sie eine Übersicht der im Buch eingesetzten Begriffe.

Englisch versus Deutsch

- Englische Begriffe

  Einige deutsche Begriffe in Exchange und Windows sind für den einen oder anderen gewöhnungsbedürftig und verwirren eher. Daher finden Sie dort, wo es zweckmäßig ist, auch die englischen Begriffe, deren Abkürzung verwendet wird. Gerade für das Troubleshooting benötigen Sie die englischen Begriffe, da nicht alle TechNet-Artikel und Dokumentationen in Deutsch erhältlich sind.

- Glossar

  Bewusst wurde auf ein spezielles Glossar verzichtet. Viele der verwendeten Begriffe gehören zum Standard im IT-Bereich und erklären sich häufig anhand des kompletten Namens. Zudem finden Sie viele sehr gute Internet-Seiten mit einem IT-Lexikon sowie die Zuordnung deutscher und englischer Fachbegriffe wie z.B. von Siemens unter

http://www.networks.siemens.de/solutionprovider/_online_lexikon.
Microsoft stellt zudem ein Exchange-Glossar zur Verfügung.

1.7 Die Webseite zum Buch

Zu diesem Buch gibt es eine Webseite mit vielen nützlichen Inhalten, erweitert um überarbeitete und neue White Paper, der aktuellen Version von Power Controls 3.0 sowie weiteren Informationen. Neben ergänzenden Hinweisen, Dokumenten und Druckvorlagen finden Sie hier auch interessante Software (Trial/Freeware). Ganz besonderes Highlight: Einige der Bilder des Buches finden Sie als Originaldatei, so dass Sie diese selbst farbig ausdrucken können. Die Formulare zur Dokumentation finden Sie ebenso als Word-Datei auf der Webseite wie einige AVI-Videos mit den Bildschirmmitschnitten der meisten Tätigkeiten. Für Ihre ersten Gehversuche mit SSL finden Sie Musterzertifikate zum Import.

1.8 Literaturhinweise und Referenzen

Die folgenden Informationen liefern sehr gute Inhalte für Ihre Arbeit mit Exchange 2003. Sie enthalten viele hilfreiche und aktuelle Details:

- Microsoft Windows 2003-Server-Online-Dokumentation für detaillierte Informationen über Management Utilities und deren Einsatz.
- Microsoft Exchange 2003-Server-Online-Dokumentation für detaillierte Informationen über die Exchange-Administration und den Betrieb.
- Das Microsoft Resource Kit für Windows und Exchange enthält weiterführende Informationen in Bezug auf die Technologie und deren Anwendung.
- Microsoft Exchange 2003-Server White Papers, die vom Microsoft Product Support Service (PSS) herausgegeben wurden und im Internet sowie auf der Microsoft TechNet-CD zu finden sind.
- Des Weiteren möchten wir auf die Buchreihe zu Windows 2000/2003 im Carl Hanser Verlag verweisen.
- Microsoft Exchange Team Blog unter http://blogs.technet.com/exchange/ enthält viele wichtige und aktuelle Informationen.
- Und zuallerletzt noch Franks Internetseite www.msexchangefaq.de, die laufend von ihm aktualisiert wird. Aktualisierungen zum Buch und der Links finden Sie dort unter http://www.msexchangefaq.de/buch.

1.9 Danksagung

Die Zeit, in der das Buch entstanden ist, war manchmal sehr turbulent und hektisch, und ohne die Unterstützung der Familie, Kollegen und Freunde hätte sich der Termin der Veröffentlichung sicher um einige Wochen verschoben.

Wir möchten allen Personen danken, die uns bei der Realisierung dieses Buches unterstützt haben. Dazu zählen:

- Unsere Familien und alle Freunde, die es manchmal nicht einfach mit uns hatten.
- Unsere Kollegen und Kunden, mit denen wir manchmal auch bis Mitternacht und länger vor den Servern verweilt haben.
- Uwe Ulbrich, Geschäftsführer von Net at Work, für das Verständnis, dass das Buch einen Teil von Franks Schaffenskraft gebunden hat.

Weiterer Dank gilt dem Carl Hanser Verlag und dort insbesondere Herrn Fernando Schneider und Frau Monika Kraus, die uns als Erstlingsautoren unterstützend zur Seite gestanden haben, sowie Frau Sandra Gottmann als Korrektorin.

Nicht unerwähnt bleiben dürfen all die Kunden, durch die wir in den letzten Jahren mit der Umsetzung von Exchange-Strukturen beschäftigt waren. Ohne ihre Fragen, Probleme und die Lösungen wäre dieses Buch um einiges theoretischer ausgefallen.

Besonders die Fragen zur Internet-Anbindung über POP3 und andere täglichen Probleme werden sehr oft von vielen Personen in den Newsgroups angesprochen und häufig beantwortet. Auch diese Fragen und die Überlegungen anderer Mitwirkender haben uns geholfen, Exchange als System und die Einsatzmöglichkeiten mehr und mehr zu erkennen. Wir danken Ihnen und hoffen, in diesem Buch einen Teil davon verständlich zur Verfügung zu stellen.

Auch wenn das Grundwerk bereits vorlag, erfordert eine weitere Auflage doch eine komplette Überarbeitung sowie eine Erweiterung um das Exchange Service Pack 2, Hotfixe und wichtige Informationen. Der IT-Bereich ist sehr lebendig und lebt von Erfahrungswerten, Feedback und neuen Informationen, die in Service Packs und Updates einfließen.

Besonders die sehr positiven Rückmeldungen zu den bisherigen Ausgaben und die guten Verkaufszahlen haben uns gezeigt, dass diese Art von Konzeptbuch genau Ihren Anforderungen entspricht. Die dritte Ausgabe enthält also alles, was sich in der Zwischenzeit geändert hat und wir hoffen, dass diese Ausgabe weiterhin hilfreich für Sie sein wird.

Im Mai 2006 Frank Carius & Ingrid Mantke

2

Exchange 2003 im Überblick

2 Exchange 2003 im Überblick

In diesem Kapitel erfahren Sie nicht nur die Neuerungen von Exchange 2003 und dem Service Pack 1. Sie können sich auch mit den Informationen um das Thema E-Mail und Internet vertraut machen. Den meisten ist dies seit Jahren geläufig. Der Einsatz eines Exchange-Servers setzt jedoch einige zusätzliche Bausteine zum Verständnis voraus, die hier vermittelt bzw. aufgefrischt werden.

2.1 E-Mail – was ist das?

Viele Anwender nutzen Outlook nur, um Mails zu senden und zu empfangen. Aber ist das wirklich alles, was Sie und Ihre Firma von Exchange erwarten können? Wo überall kommen Mail und Exchange zum Einsatz? Tauchen Sie ein in die faszinierende Welt der Nachrichten, und erlernen Sie die schematische Funktion. Das Wissen benötigen Sie in den späteren Kapiteln zum effektiven Arbeiten.

2.1.1 Das Mailprogramm

Outlook ist eines von vielen Programmen, mit denen ein Anwender elektronische Nachrichten liest und schreibt. Diese Komponente wird oft auch als „User Agent“ (UA), Frontend oder „Graphic User Interface“ (GUI) bezeichnet. Die weiteren Funktionen werden dabei häufig außer Acht gelassen.

Mail-Clients in den unterschiedlichsten Ausführungen

Neben Outlook gibt es noch eine unüberschaubare Anzahl an Programmen, die sich dem Versand und Empfang von Nachrichten widmen. Hierzu zählen Produkte wie Outlook Express, Eudora, Pegasus Mail, Pine, K-Mail und andere. Oftmals finden Sie für das Mailprogramm auch den Begriff „User Agent“ (UA) in diversen Publikationen, häufig einfach nur „Client“. Alle haben drei Grundfunktionen gemeinsam:

2.1.1.1 Übertragen und anzeigen

Aufgabe des Mailprogramms ist das Abholen und die Anzeige von neuen Nachrichten sowie die Übermittlung von Nachrichten, die ein Anwender sendet. Wenn Sie Outlook oder einen anderen Client auf dem Einzelplatz zu Hause betreiben, dann erfolgt der Versand in der Regel per SMTP an den Mailserver des Providers, und die neuen Nachrichten werden mit dem Protokoll POP3 oder IMAP4 abgeholt und lokal in einer Datei gespeichert.

Beim Einsatz in einer Firma steht der Mailserver im eigenen Haus. Der Client übergibt die Nachrichten an den Server zur weiteren Verarbeitung. Dieser hält alle Nachrichten für den Benutzer zur Ansicht in seinem Speicher zur Verfügung und stellt weitere Dienste je nach Mailprogramm bereit. Zwar könnte der Prozess zwischen Server und Client auch per SMTP/POP3 erfolgen, jedoch würde dies im Falle von Exchange mit Outlook das leistungsstarke System um viele Funktionen berauben.

2.1.1.2 Adressbuch

Zentrale Adressen

Eine weitere Komponente ist das Adressbuch, in dem der Anwender seine Kontakte speichern kann. Einige Systeme erlauben neben den privaten Kontakten auch die Nutzung einer zentral gepflegten Datenbank. Diese wird in der Regel mit dem Protokoll LDAP abgefragt. In Verbindung mit Exchange 2003 übernimmt der Server die Aufgabe der Adressabfrage und stellt dem Anwender ein „Globales Adressbuch“ aller Mitarbeiter bereit.

2.1.1.3 Ablage und Speicher

Alle gesendeten und empfangenen Nachrichten werden in einer Datenbank oder Verzeichnisstruktur abgelegt, damit auch nach Monaten oder Jahren der Zugriff darauf möglich ist. Viele Programme nutzen dazu lokale Dateien. Wird Outlook in einem Unternehmen in Verbindung mit einem Exchange-Server benutzt, dann liegen all diese Informationen zentral auf dem Server (EDB-Dateien) und werden dort gesichert. Bei Bedarf können sie gemeinsam genutzt werden und sind über verschiedene Wege erreichbar.

EDB versus PST

Ohne Anbindung an einen Exchange-Server muss der Outlook-Client die Informationen in einer PST-Datei ablegen. Diese liegt meistens auf der lokalen Festplatte, kann nicht gemeinsam genutzt werden, wird nicht gesichert und erlaubt auch keinen Zugriff von unterwegs per Browser, WAP, Pocket PC oder Notebook.

Alternativ ist eine reine Browser-Ansicht (z.B. GMX, WEB.DE), ohne Übermittlung der Nachrichten auf den lokalen Computer, möglich. Die Daten werden jedoch nach einiger Zeit von den Providern gelöscht, oder die Mailbox läuft voll.

2.1.2 Der Mailserver

Im vorherigen Kapitel ist der Begriff Mailserver schon gefallen. Outlook kann zwar Nachrichten senden und abholen, aber keine Nachrichten empfangen. Der kleine Unterschied ist wichtig, denn nur ein Mailserver kann

von anderen Servern angesprochen werden und Nachrichten annehmen. Ein Client kann Nachrichten nur von einem Server abholen.

Der zentrale Knoten eines Nachrichtensystems ist ein Server, der die für die Anwender bestimmten Nachrichten annimmt und diese in das Postfach des Anwenders zustellt sowie die gesendeten E-Mails des Benutzers annimmt und an den Empfänger übermittelt. Es ist also ein Unterschied, ob eine Software selbst als Server dient und Verbindungen annimmt oder bei einem anderen System nur Daten abholt. Die Funktionalität eines Servers erfordert in der Regel eine 24x7-Verfügbarkeit und zuverlässige Arbeitsweise, er ist in der Regel immer empfangsbereit und nimmt die Nachrichten stellvertretend für den Anwender an. Der Anwender selbst kann dann von diesem System seine Nachrichten abholen oder nur lesen und ausgehende Nachrichten dort zum Versand ablegen. Der Mailserver kümmert sich auch um den Versand an weitere Mailserver, wenn das Postfach des Empfängers nicht auf dem gleichen Server liegt. Die Übertragung von allen Nachrichten übernimmt der Message Transfer Agent (MTA).

Privatpersonen nutzen in der Regel einen Mailserver des Internet-Providers. So sind die Mailserver von GMX, WEB.DE, 1und1 Beispiele für solche Server, teilweise basierend auf Exchange.

Vorteil eigener Mailserver

Warum nun ein eigener Mailserver? Die Daten im Firmennetzwerk können intern mit hoher Geschwindigkeit und entsprechend sicher ausgetauscht werden. Für das Unternehmen bedeutet dies die Unabhängigkeit vom Internet und vom Provider. Weiterer Vorteil ist die interne Verwaltung und Konfiguration, da die Benutzer angelegt und modifiziert werden müssen und das Einrichten von Regeln erforderlich ist. Auch die Anlage von Verteilern und die zentrale Nutzung von Virenscanner und Anti-Spam-Software sprechen dafür. Ein weiterer wichtiger Aspekt ist die interne Datensicherung.

Allerdings stellen der Aufbau, die Installation und die Anbindung eines eigenen Mailservers in der Firma einen höheren Schwierigkeitsgrad dar als die Anbindung einiger Outlook-Clients an ein POP3-Postfach des Internet-Providers. Im Gegensatz zum Outlook-Client erwartet der Mailserver, dass ihm die Nachrichten aus dem Internet zugestellt werden. Die wenigsten Mailserver können per POP3 die Postfächer bei einem Provider abfragen. Die Anbindung eines Mailservers erfolgt in der Regel per SMTP und bedeutet entsprechendes Know-how und eigene Infrastrukturen. Dazu später mehr.

2.1.3 Kommunikationswege

Die vorgestellten Komponenten, also Server und Clients, treten miteinander in Kontakt, das heißt, sie kommunizieren in einer bestimmten Art. Das folgende Bild zeigt, welche Verbindungen zwischen den einzelnen Komponen-

ten eines Messaging-Systems bestehen. Dies erleichtert die Fehlersuche und das Verständnis für manche zuerst kompliziert erscheinenden Prozesse.

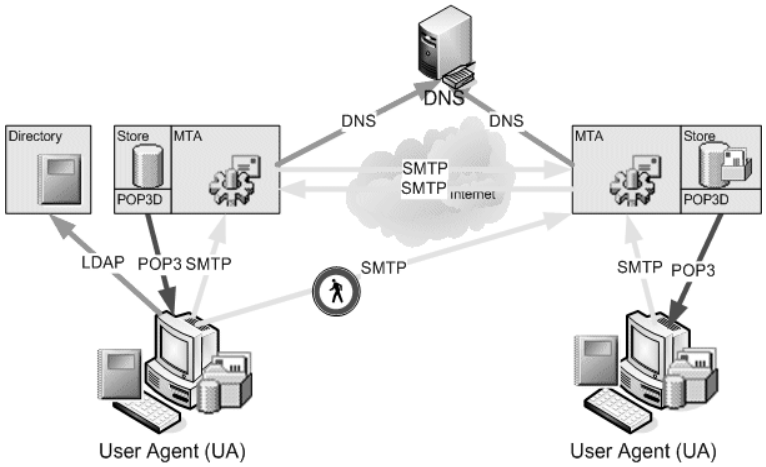


Abbildung 2.1 Kommunikationswege

Tür zu für Spam, Viren und Würmer

Achtung, ein Weg in diesem Diagramm sollte niemals erlaubt sein: Ein Client sollte niemals direkt Nachrichten an externe Systeme ins Internet versenden können. Nur der Versand über den eigenen Mailserver sichert eine Nachvollziehbarkeit und optionalen Virenschutz. Eine solche Lücke würde Tor und Tür für Würmer, Viren und den unautorisierten Versand von Informationen öffnen. Der Empfänger blockiert oft schon mit Hilfe eines Spam-Filters, aber viel wichtiger ist, dass diese Funktion aktiv in Ihrem Netzwerk verhindert wird. Viele Viren und Würmer senden mittlerweile selbst Nachrichten per SMTP. Blockieren Sie als Firma auf jeden Fall diesen Weg ins Internet mit Ausnahme des Mailservers! Und dieser sollte entsprechend kontrolliert werden, um rechtzeitig bei Erscheinen von unerwünschtem Mailtransfer einen Schaden für das Unternehmen auszuschließen.

Am Beispiel einer Nachricht vom Absender (User01) zum Empfänger (User02) können Sie die Funktionen verfolgen:

1. Benutzer erstellt Nachricht

   Beispiel Nachrichtenverlauf

   Der User01 erstellt eine E-Mail in seinem Clientprogramm. Er greift dazu optional auf das lokale Adressbuch zu, um den Empfänger auszuwählen. Bei einem serverbasierten System kann auch eine Datenbank bzw. ein globales Adressbuch genutzt werden. Die Abfrage erfolgt bei Outlook automatisch, andere Mailprogramme nutzen in der Regel die LDAP-Schnittstelle. Auch Windows 2003 bietet per LDAP die Funktion an.

2. Benutzer sendet Mail

   SMTP-Autorisierung

   Nach dem Verfassen der Nachricht schickt User01 diese mit der Aktion SENDEN auf den Weg. Der Mailclient überträgt die E-Mail an einen Mailserver. Die meisten Unternehmen betreiben einen Mailserver im in-

ternen LAN, Privatpersonen nutzen den Server des Providers. Wesentlich ist dabei die Autorisierung des Absenders, die beim Einsatz von Outlook mit Exchange automatisch erfolgt. Der Privatanwender muss die Berechtigung explizit über das SMTP-Protokoll mitteilen. Eine Autorisierung sollte immer vorgezogen werden, da sonst die Gefahr besteht, dass andere Prozesse (auch Viren) Nachrichten versenden und die Spur des Übeltäters sich nicht zurückverfolgen lässt bis auf die IP-Adresse des Absenders.

3. MTA sendet Mail

Mail Transfer Agent

Der Mailserver nimmt die Nachricht an, speichert diese und leitet sie anschließend an den Server des Empfängers weiter. Um das Zielsystem herauszufinden, bedient er sich des DNS-Servers. Mit der Information über die Empfängerdomäne und dem MX-Eintrag in der DNS-Zone erhält der Server die IP-Adressen der Zielservers. Die SMTP-Verbindung wird dann vom Mailserver zum Server des Empfängers aufgebaut, und die Nachricht von User01 wird übermittelt.

4. MTA empfängt Nachrichten

Relay/Proxy als Sicherheit

Der Zielserver nimmt die Nachricht an und legt sie in das Postfach von User02 ab. Liegt das Postfach auf einem anderen Server innerhalb des Zielsystems, wird die Nachricht intern zum richtigen Server übermittelt. Vielfach wird dem eigentlichen Postfachserver ein Relay vorgeschaltet. Damit wird eine Trennung der Serverfunktion erreicht, die eine höhere Sicherheit mit sich bringt. Auf dem Relay-Server können zusätzliche Funktionen wie Virenscanner und Spam-Filter implementiert werden.

5. User02 holt Nachrichten ab

Die Nachricht befindet sich nun in dem Postfach von User02 und kann mit einem Mail-Client gelesen werden. Bei der Anwendung von Outlook mit Exchange erhält der Empfänger sogar aktiv eine Mitteilung über neue Nachrichten. Andere Mailclients prüfen den Server in regelmäßigen Abständen auf neue Nachrichten. Während Outlook die E-Mail sofort anzeigt, müssen andere Clients diese erst vom Server laden, um sie anzuzeigen.

Mit diesem schlichten Verfahren funktioniert der Mailversand im Internet schon viele Jahre sehr problemlos. Auf Basis von SMTP mit POP3 und IMAP4 gibt es sehr viele Mailserver und Clients, die ohne Einschränkungen miteinander kommunizieren. Jedoch stellt dies zugleich auch den kleinsten gemeinsamen Nenner dar.

2.1.4 Internet-Technologie im Firmennetzwerk

Die Vorteile von Exchange können verdeutlicht werden, wenn die Grenzen der klassischen Mailanwendung im Internet bekannt sind. So werden Sie

schnell erkennen, dass Internetlösungen, die auf dem Einzelplatz ausreichen, sich nur bedingt für den Einsatz in Firmen eignen.

Keine Benachrichtigung – teures „Pollen“

Performance-Killer

Für eine Benachrichtigung beim Eintreffen von neuen Nachrichten gibt es keine allgemein gültige Norm. Der Empfänger muss regelmäßig sein Postfach prüfen; das Zeitintervall beträgt häufig zehn Minuten. Viele Anwender assoziieren dieses Verhalten mit einer schlechten Performance des Servers und setzen das Intervall auf geringere Werte. Die Belastung des Servers wächst dadurch enorm. Bei einem Intervall von einer Minute und bei 120 Benutzern müssen schon zwei Anmeldungen pro Sekunde vom Server verarbeitet werden. Hinzu kommt das komplette POP3-Protokoll (mehrere Pakete) und eventuell die Anfrage des Mailservers an einen Anmeldeserver (Domänencontroller, Radius etc.).

Keine Regeln

Abwesenheits-assistent

Bei der alltäglichen Nutzung von Mailclients sind Regeln unverzichtbar. Diese automatisieren die Verarbeitung von Nachrichten und funktionieren meist nur auf dem Client selbst. Für serverbasierte Regeln gibt es keine Standardisierung. Ein weiteres Plus in der Kombination Outlook mit Exchange ist die Einrichtung von Regeln, die auch nach der Abmeldung des Clients aktiv sind. So kann der Anwender automatisch bei Abwesenheit die Nachrichten anhand von Filtern weiterleiten oder beantworten lassen. Mit Outlook 2003 und Exchange 2003 werden sogar die Filterlisten gegen unerwünschte Nachrichten (Spam) auf den Server geladen und dort abgearbeitet.

Keine Stellvertreter

Zugriff der Sekretärin

In einer Firma ist oft die Notwendigkeit gegeben, auf das Postfach eines Kollegen zuzugreifen. Dieser Wunsch besteht im Rahmen der normalen Tätigkeit in Teams oder des Sekretariats. Bei der Umsetzung auf Basis POP3/IMAP bedeutet dies eine Sicherheitslücke, da das Kennwort des anderen Benutzers eingegeben werden muss. Bei einer fehlerhaften Konfiguration holt der Client sogar die Nachrichten des zu vertretenden Benutzers ab und speichert diese lokal. Eine echte Stellvertreterfunktion ist damit nicht realisierbar.

Bedingte Speicherung auf dem Server

Beim Einsatz von POP3 werden die Nachrichten immer heruntergeladen und auf der ungesicherten lokalen Festplatte abgelegt. Dies widerspricht dem Wunsch einer servergestützten Ablage mit all den Vorteilen innerhalb eines Unternehmens. Welche Nachteile entstehen nun dadurch? Wird die PST-Datei von Outlook oder das Archiv einer anderen Anwendung auf einem Dateiserver gespeichert, dann erkennt die Datensicherung diese Datei immer

als Ganzes. Die kleinste Änderung in einer PST-Datei bewirkt die komplette Sicherung dieser „neuen“ Datei und wirkt sich somit ungünstig für das Volumen und den Zeitraum der Sicherung aus.

Mehr Sicherheit durch serverbasierte Daten

Erst das Nachfolgeprotokoll IMAP4 ermöglicht es, die Ordner vom Server zu lesen, ohne die Nachrichten explizit abzurufen und die Daten auf dem Arbeitsplatz zu halten. Aber selbst hier zeigt die Erfahrung, dass nicht alle IMAP4-Server und -Clients den vollen Befehlssatz unterstützen. Die servergestützte Ablage von Informationen ist auch in anderer Hinsicht wünschenswert. Solange die Daten auf dem eigenen PC liegen, ist auch kein Zugriff von anderen Systemen per Webbrowser, Mobiltelefon und anderen Clients möglich.

Kein Standard für besondere Ordner

Definition unterschiedlicher Objekte oder universeller Zugriff auf Informationen fehlt

POP3 und IMAP kennen genau genommen nur Ordner mit Information, also keine Unterscheidung zwischen Mail, Adresseinträgen oder anderen Objekten. Mit Outlook verwenden Anwender wie selbstverständlich die Ordner Kontakte, Kalender und Aufgaben. Andere Produkte können dies natürlich ebenfalls nutzen, mangels einheitlicher Implementierung ist die Zusammenarbeit aber nur mit identischen Produkten möglich. Microsoft Outlook ist aufgrund der großen Verbreitung aber schon fast wie ein Standard anzusehen, so dass diese Zusatzfunktionen Sinn machen. Ohne Outlook müssten parallel zum Nachrichtensystem weitere Dienste installiert werden, was meistens auch weitere Kosten beinhaltet.

Keine gemeinsame Nutzung

Arbeiten unter einer Mailadresse

Viele Informationen sind nicht nur für das Postfach eines Anwenders gedacht, sondern es betrifft eine Gruppe von Usern, die zusammen an dem Thema arbeiten. Ein Beispiel dafür ist der Support in einem Unternehmen. Die E-Mail „support@firma.de“ wird gemeinschaftlich genutzt, die Mitarbeiter im Support besitzen die benötigten Rechte und nutzen zusätzliche Funktionen zur Steuerung der Zusammenarbeit, z.B. Kennzeichnungen und Kategorisierungen. Diese gemeinsamen Bereiche, die mit Exchange schon zur standardisierten Bürokommunikation zählen, sind mit POP3 oder IMAP4 nicht abzubilden. In gewisser Hinsicht ist eine ähnliche Funktion über Newsgroups mit dem Protokoll NNTP realisierbar.

So einfach und günstig der Einsatz eines einfachen POP3-Servers im Unternehmen erscheint, so viele Argumente gibt es, die den Einsatz eines leistungsfähigeren Systems befürworten.

Um dem Vorwurf vorzubeugen, dass die Argumentation gegen Unix gerichtet ist, sollten Sie wissen, dass Windows 2003 ebenfalls einen einfachen SMTP/POP3-Dienst enthält. Ebenso gibt es sehr viele kostenfreie Mail- und News-Server wie Mercury, Hamster und andere für Windows- und auch die

Unix-Welt bietet durchaus leistungsfähigere Nachrichtensysteme an, die dann jedoch nicht mehr dem „offenen Standard“ POP3/IMAP4 folgen.

2.1.5 Mehrwert von Exchange und Outlook

Weil die Nutzung von POP3 und IMAP4 nicht die Bedürfnisse der internen Kommunikation im Unternehmen abdecken kann, gibt es leistungsfähige Systeme wie Microsoft Exchange, Lotus Notes, Novell GroupWise und andere. Alle unterstützen natürlich ebenfalls POP3 und IMAP4, aber erst in Verbindung mit einem leistungsfähigen Client sind wichtige Zusatzfunktionen zugänglich.

Synergie oder Zusammenführen von Leistungsfähigkeit

Microsoft Exchange gibt es nun schon sehr viele Jahre, und es hat in vielen kleinen und großen Umgebungen bewiesen, dass es sehr gut skalierbar ist und alle Anforderungen an eine moderne Kommunikationsinfrastruktur erfüllt. Nur was macht Exchange aus, dass sich so viele Firmen für dieses Produkt entscheiden?

Seit dem Sommer 2003 gibt es die aktuellste Version „Microsoft Exchange-Server 2003“, sie ist die Weiterentwicklung von Exchange 2000, das seit Oktober 2000 auf dem Markt ist. Mit der Einführung des Active Directory haben sich grundlegende Dinge geändert, daher sind die früheren Produkte der Exchange-Produktlinie nicht mehr direkt vergleichbar.

Nicht nur ein Mailserver!

Microsoft Exchange als Mailserver zu bezeichnen ist eine starke Untertreibung dessen, was Exchange zu leisten imstande ist. Natürlich kann Exchange wie jeder andere Mailserver Nachrichten senden und empfangen, aber dies ist nur ein Bruchteil der Funktionalität. Exchange ist der zentrale Server für die Ablage von Nachrichten, Terminen, Kontakten und jeder anderen Art unstrukturierter Informationen, die in einem Unternehmen heute anfallen. Outlook mit der benutzerfreundlichen Oberfläche organisiert diese Informationen für eine volle Ausnutzung der Systemkomponenten.

Speicherplatz und Cache Mode

Geringe Bandbreite

Exchange legt alle Informationen in einer Datenbank (*.edb) auf dem Server ab; die Sicherung kann im laufenden Betrieb erfolgen. Damit ist die Grundlage für einen 24x7-Stunden-Betrieb gelegt. Transaktionsprotokolle und Prüfsummen sichern die Integrität der Daten. Der neue Client greift nicht nur auf diese Daten zu, sondern nutzt die *Cache Mode*, um die Übertragung verlustfrei bei Unterbrechung weiterzuführen sowie eine verbesserte Komprimierung. Mit der optimierten Netzwerkverbindung in der Kombination von 2003 Server und 2003 Client kann die Belastung auf den Exchange-Server reduziert werden, und es bieten sich erweiterte Möglichkeiten der Anbindung (RPC over HTTP).

Mobile und wechselnde Benutzer

Zugriff von überall mit Outlook Web Access

Viele Firmen wechseln zum neuen OWA-Client, der mit Exchange 2003 kaum noch von Outlook zu unterscheiden ist und auch in der Funktionalität mit dem großen Bruder fast gleichzieht. Das optimierte GUI unterstützt neuerdings auch verschlüsselte und signierte Nachrichten, beinhaltet eine Rechtschreibprüfung, den schon lange vermissten Regelassistenten, und unterdrückt Links zu externen Webinhalten. Dabei übergibt der OWA-Client z.B. bei der Rechtschreibprüfung die Anforderungen an den Server, der das Ergebnis im XML-Format zurück übermittelt. Dies eröffnet nun auch die Konsolidierung von Servern auf einen Standort, um die Vorteile des neuen OWA voll ausschöpfen zu können.

Der Zugriff über Handhelds ist mit dem integrierten Mobile Access Server erleichtert worden.

Robustes Nachrichtenrouting

Direkte Wege

Mehrere verbundene Server tauschen untereinander Statusmeldungen aus, welche Verbindungen verfügbar sind und welche aktuell nicht funktionieren. So werden Nachrichten bei Bedarf über alternative Leitwege zugestellt. Der Outlook-Benutzer muss sich nicht um den Kommunikationsweg kümmern, Verzögerungen ermitteln oder eine verspätete Zustellung befürchten.

Mit der Erkenntnis, dass das System nicht nur Nachrichten überträgt, können Sie ermessen, welche Funktionen zukünftig in Ihrem Unternehmen genutzt werden können. Die Erweiterung der Funktionen spielt bei der Dimensionierung der Server eine große Rolle und muss berücksichtigt werden. Es relativiert den Preis im Vergleich zu vielen „günstigeren“ Produkten.

2.1.6 Die Bedeutung von E-Mail im Unternehmen

In den heutigen Unternehmen ist E-Mail als Kommunikationsmedium nicht mehr wegzudenken. Die Entwicklung von Brief und Telefon hin zu den schnellen und zeitunabhängigen E-Mails hat auch ihre Spuren im Unternehmen hinterlassen. Jeder Mitarbeiter im Unternehmen braucht praktisch einen E-Mail-Zugang, um auf essenzielle Unternehmensinformationen zugreifen, mit Kollegen zusammenarbeiten und Kunden adäquat bedienen zu können.

Exchange wird zum unternehmenskritischen System

E-Mail als unternehmenskritische Anwendung steuert Geschäftsprozesse.

Wer kann es sich heute noch leisten, E-Mail-Nachrichten nicht zu erhalten, zu senden oder gar zu verlieren? Mitarbeiter, die schneller und besser informiert sind, können effektiver Entscheidungen treffen und sind jederzeit für den Kunden erreichbar. Daher muss auch Exchange eine hohe Verfügbarkeit gewährleisten, weil unternehmenskritische Prozesse davon abhängen. Unter-

nehmenskritisch bedeutet, dass es zum Stillstand oder zum Ausfall von Anwendungen, Netzwerken, Systemen oder Maschinen kommen kann, für die es weder eine Ausweichmöglichkeit oder einen kurzfristigen Ersatz gibt. Bezogen auf die Auswirkungen und Kundenbedürfnisse wird dies deutlich, wenn Sie abschätzen, wie teuer zum Beispiel ein Produktionsstillstand, verursacht durch den Ausfall des E-Mail-Systems, sein kann. Selbst wenn keine geschäftskritischen Daten verarbeitet werden, sind teils Prozesse betroffen, die extrem unternehmenskritisch eingestuft werden, weil Systemfehler das Geschäft zum Erliegen bringen können.

Datenverlust und Sicherheitslücken sind zu vermeiden

Datensicherung und Schutzmechanismen

Ein großer Teil der Geschäfte wird per E-Mail abgewickelt, und es werden sicherheitsrelevante und geschäftskritische Daten übermittelt. So kann der Verlust der Daten oder deren Manipulation erhebliche Folgen für das Unternehmen haben, deren Haftungsfrage meist nicht geklärt ist. Hier sehen sich die Unternehmen konfrontiert mit Viren, unaufgefordert zugesandten Nachrichten (Spam), Angriffen auf den Mailserver sowie dem Verlust von Produktivität und Verschwendung von Ressourcen. Bei dem Relay-Versand von anstößigen Mails ist sogar mit rechtlichen Konsequenzen zu rechnen, die auch bei Nichteinhaltung von Aufbewahrungsfristen für beispielsweise versendete Rechnungen zu berücksichtigen sind. Auch der Verlust oder die Veruntreuung von vertraulichen Informationen ohne entsprechende Nachvollziehbarkeit sind ein Risiko. Bei der Auswahl des E-Mail-Systems ist der optimale Schutz und die Sicherung der Daten zu beherzigen, da sonst ein ganzes Unternehmen in seinem Betrieb erheblich beeinträchtigt werden kann.

Anforderungen wachsen

Zukunftssicher

Die Anwender stellen immer mehr Bedürfnisse an ein E-Mail-System. Zusätzlich zum E-Mail-Dienst nutzen sie den Kalender und die Terminplanung, gemeinsame Adressbücher und Öffentliche Ordner und erwarten die Synchronisationsfähigkeit in einer Netzwerkumgebung. Zudem erfordert die veränderte Arbeitsform den mobilen Zugriff auf alle Daten, um auch dem Außendienstmitarbeiter gerecht zu werden. Für Ihr Unternehmen ist es auch bedeutsam, die Skalierung des E-Mail-Systems zu betrachten, um die permanente Zunahme von Nachrichten, aber auch Benutzern abzudecken.

Schnelle Reaktionszeit

Totalausfällen vorbeugen

Studien zu der Problematik zeigen, dass ein Drittel aller Administratoren sich ernsthaft Gedanken über den Verlust ihres Arbeitsplatzes macht, wenn das E-Mail-System für einen Tag ausfällt. Bei längeren Unterbrechungen ist von der Unternehmensseite häufig mit dieser Konsequenz zu rechnen. Sie sollten sich daher rechtzeitig die Frage stellen, wie unternehmenskritisch der Einsatz

von E-Mail in Ihrem Unternehmen ist. Es ist für Sie von Vorteil, ein System schnell und mit wenig Aufwand wiederherzustellen und eine hohe Verfügbarkeit, beispielsweise durch Redundanz, zu gewährleisten.

Exchange auslagern

Hosting oder Outsourcing

Einige Unternehmen stellen die Entscheidung für den eigenen Exchange-Server in Frage. Auf der einen Seite ist die IT-Umgebung zu klein, um sich mit so komplexen Themen auseinander zu setzen, andererseits möchten sie jedoch die Vorteile von Exchange 2003 nutzen. Hier stehen zwei Möglichkeiten zur Verfügung: das Auslagern der Betreuung an Experten oder der Betrieb des Exchange-Services bei einem externen Dienstleister. Zur Entscheidungsfindung ist es einfacher, zu prüfen, wie die interne Kommunikationsumgebung aussieht, sprich, um welche Art von Unternehmen es sich handelt. Klein- und mittelständische Unternehmen, die ihren Fokus auf das Kerngeschäft, also Produktion, legen und auch standortübergreifend arbeiten, sollten die Möglichkeit eines internen Servers mit externer Betreuung erwägen. Für Dienstleistungsunternehmen, die hauptsächlich mit kleinen Filialen arbeiten und deren Mitarbeiter im Außendienst tätig sind, könnte der externe Betrieb mit einer eigenen Administrationsoberfläche eine optimale Lösung sein. Hier spielen natürlich auch die Service Level Agreements (SLA) eine große Rolle, die mit externen Anbietern abgeschlossen werden. Was sind nun die Nachteile dieser Lösungen? Beim Outsourcing mit eigenem Server ist man extrem auf die Betreuung und Administration angewiesen, was teilweise dazu führt, dass Probleme nicht sofort gelöst und manchmal nicht erkannt werden. Der Vorteil beim Hosting ist eine optimale Infrastruktur, die Service und Support der Server mit einschließt. Hier sollte ein Anbieter gewählt werden, der auch ein entsprechendes Tool für die einfache Administration, zum Beispiel das Anlegen und Löschen von Benutzern, erleichtert. Nachteil des Hostings ist die Netzanbindung, die wiederum vom Provider abhängig ist. Im Gegensatz zum eigenen Server bieten beide Möglichkeiten den Vorteil, dass im Unternehmen kein Exchange-Wissen aufgebaut werden muss.

2.2 Voraussetzungen für Exchange 2003

Die Installation von Exchange Server 2003 bedingt einige technische Voraussetzungen, die die Infrastruktur und Serverversionen einbeziehen.

Exchange 2003 benötigt zwingend ein Active Directory

Auf Basis AD

Sie müssen vorab ein Windows 2000 oder 2003 Active Directory-System (AD) installieren. Ohne die dazugehörige Netzwerkinfrastruktur (TCP/IP,

DNS, Globaler Katalog etc.) ist Exchange 2003 nicht installierbar. Das AD muss entsprechend vorbereitet werden, um alle Informationen für Exchange bereitzustellen. Idealerweise wird der Mailserver auf einem Windows 2003-AD installiert, um in den Genuss aller der damit verbundenen Vorteile wie Schattenkopien (VSS), IIS6 und dem verbesserten Active Directory zu kommen.

Exchange 2003

Member-Server oder Domänen-controller?

Exchange 2003 kann auf einem Mitgliedsserver (Member-Server) oder einen Domänencontroller (DC) installiert werden. Die Installation auf einem Mitgliedsserver ist bei entsprechender Netzwerkgröße vorzuziehen. Wird Exchange auf einem Domänencontroller installiert, so bedingt dies einige Einschränkungen in der Sicherheit. Beispielsweise ist in dem Fall der Exchange-Administrator gleichzeitig auch Domänen-Administrator mit entsprechend weit reichenden Berechtigungen. Der Zugriff per Netscape-Browser und anderer Dienste funktioniert nur, wenn die Anwender auch das Recht der lokalen Anmeldung haben; bei einem Domänencontroller eher bedenklich. Zudem nimmt die Komplexität des Servers zu, was sich negativ auf die Stabilität auswirken kann. Trotzdem gibt es auch stabile Small Business-Umgebungen, bei denen alles auf einem Server installiert wird.

Feste Serverrolle

Nachdem Sie Exchange auf dem Server installiert haben, dürfen Sie jedoch auf keinen Fall die Rolle des Servers ändern. Das Wechseln der Serverrolle eines Exchange Servers von Member Server nach Domaincontroller oder umgekehrt kann zu Verlusten einiger Exchange Funktionen führen und wird von Microsoft nicht unterstützt. Sie sollten daher die Installation im voraus gut planen und sich für eine Serverrolle entscheiden.

Windows 2000 Server und Windows Server 2003

Windows 200x Server

Exchange 2003 kann auf Windows 2000-Server und Windows Server 2003 installiert werden. Und auch nur dort, denn die Installation auf ein Workstation-System oder auf Windows NT4 ist nicht möglich. Verwechseln Sie Exchange nicht mit dem veralteten „Microsoft Exchange Client“, der aus Windows NT4 und Windows 95 noch bekannt ist. Allerdings werden erst auf Windows 2003 einige erweiterte Funktionen von Exchange 2003 wie „RPC over HTTP“ und die Sicherheit des IIS6 nutzbar. Berücksichtigen Sie dabei die Anforderungen des aktuellen Service Packs.

Über 2 GB Hauptspeicher

Aufgrund der Schnelllebigkeit der technischen Neuerung im IT-Bereich macht es Sinn, die aktuellsten Systeme einzusetzen. Dies bedeutet auch, dass mehr Hauptspeicher entsprechende Serverversionen erfordern. Über 1 GB Hauptspeicher sollte mindestens beim *Windows 2000 Advanced Server* oder

Windows Server 2003 eingesetzt werden, um die */3GB-Option* nutzen zu können. Über 4 GB wird die Unterstützung von PAE (Physical Address Extension) notwendig, um Anwendungen wie Exchange entsprechenden Speicher bereitzustellen. Diese Funktionen sind ebenfalls erst ab Windows 2000 Advanced Server oder Windows Enterprise Server 2003 verfügbar.

Kombination Windows und Exchange-Editionen

Enterprise versus Standard - Datacenter versus Web Edition

Sie haben die Wahl, ob Sie *Windows Server 2003 Standard Edition* mit Exchange Enterprise installieren oder auf einem Windows 2003 Enterprise Server die Exchange Standard Edition. Bis auf die *Windows 2003 Server Web Edition* sind alle Kombinationen möglich, allerdings machen einige davon wenig Sinn. Beim Einsatz eines Windows Advanced Servers mit 6 Gigabyte Arbeitsspeicher ist es unsinnig, einen Exchange Standard-Server zu installieren. Die eine Speichergruppe nutzt kaum mehr als 1 GB Hauptspeicher.

Hochverfügbarkeit

Cluster

Wenn Sie Exchange „clustern“ wollen, dann ist als Basis nicht nur *Windows Advanced Server* oder *Windows Datacenter Server* einzusetzen, sondern auch *Exchange 2003 Enterprise*. Nur diese Kombination in Verbindung mit der passenden Hardware erlaubt die Konfiguration als Cluster. In der 2003-Verbindung sind sogar bis zu 8-Knoten-Cluster-Systeme möglich, deren Verfügbarkeit bei fast 100 % liegt.

Praktische Konstellation

Best Practice

Zusammenfassend ist zu vermerken, dass in mittelständischen und kleinen Unternehmen, deren Server nicht mehr als 2 GB Hauptspeicher haben und die 16 GB-Grenze der Datenbank nicht überschreiten, die Kombination von einem Windows 2000/2003 Standard-Server mit Exchange 2003 Standard ausreichend ist. Erst wenn eine Maildatenbank mit mehr als 16 Gigabyte zu erwarten ist, muss der Exchange 2003 Enterprise Server eingesetzt werden. Der Einsatz von X.400-Connectoren wird heute durch SMTP-basierte Routinggruppen abgelöst. Größere Unternehmen bedienen sich meist anderen Zusammensetzungen.

2.3 Die verschiedenen Exchange-Versionen

Neben den Unterschieden zwischen *Exchange Server 2003 Standard* und *Exchange Server 2003 Enterprise* ist im Hinblick auf die Auswahl der Server auch ein Vergleich mit den früheren Exchange-Versionen angebracht. Folgende Tabelle zeigt die wichtigsten Unterschiede:

Tabelle 2.1 Exchange-Versionen im Überblick

Funktion	Exchange 5.5	Exchange 2000	Exchange 2003 Service Pack 2
Betriebssystem	NT4 und W2K nicht W2K3	➔ nur W2K	W2K ab SP4 und W2K3
RPC	☑ IPX ☑ IP ☑ NetBeui	☑ IPX ☑ IP ☑ NetBeui	☑ IPX ☑ IP ☑ NetBeui
RPC over HTTP ab Outlook 2003	☐ Nein	☐ Nein	☑ nur ab W2K3 und WinXP SP2
OWA	☑ ASP-Seiten IIS3/IIS4/IIS5	☑ (1) WebDav Nur IIS5 auf W2K	☑ WebDav IIS5/IIS6
WAP/ActiveSync	➔ MIS-Server (39 $)	➔ MIS-Server (39 $)	☑ Ja OMA integriert
POP3/IMAP4/NNTP	☑ eigener Connector	☑ eigener Dienst bzw. erweitert W2K NNTP-Dienst	☑ eigener Dienst bzw. erweitert W2K NNTP-Dienst
SMTP	☑ eigener Connector	☑ erweitert W2K SMTP-Dienst	☑ erweitert W2K/W2K3 SMTP-Dienst
Spamschutz	☐ Nein	☐ Nein	☑ Ja, IMF
M:-Laufwerk	☐ Nein	☑ Ja, abschaltbar Q305145	➔ per Default deaktiviert
Collaboration	☐ Nein	☑ Ja, enthält Instant Messaging	☐ Nein. Eigenes Produkt „Office Live Communication Server“
Chat-Dienste	☑ Ja	☑ Ja	☐ Nein
Key Management	☑ (3)	☑ Eingeschränkt	☐ Nein
X.400-Connector	➔ Nur Enterprise	➔ Nur Enterprise	➔ Nur Enterprise
MSMail-Connector	☑ Ja	☑ Ja	☐ Nein
cc-Mail-Connector	☑ Ja	☑ Ja	☐ Nein
Notes Connector	☑ Ja	☑ Ja	☑ Ja
GroupWise Connector	☑ Ja	☑ Ja	☑ Ja

Funktion	Exchange 5.5	Exchange 2000	Exchange 2003 Service Pack 2
Cluster-tauglich	Enterprise: 2 Node Active/Passiv	Enterprise: 4 Node Active/Active	Enterprise: 8 Node Active/Active
Hauptspeicher	1 GB effektiv nutzbar, > mit „W2K Advanced/ W2K3 Ent. und */3GB-Option*	2 GB nutzbar, 3 GB mit W2K Advanced Server	2 GB nutzbar, 3 GB mit W2K Advanced Server, oder W3K und /3GB Option
Datenbanken	*Standard und Enterprise:* 1 Postfächer 1 Öff. Ordner	*Standard*: 1 Speichergruppe 1 Postfächer 1 Öff. Ordner *Enterprise*: Bis zu 4 Speichergruppen mit bis zu je 5 Datenbanken	*Standard*:: 1 Speichergruppe 1 Postfächer 1 Öff. Ordner *Enterprise*: Bis zu 4 Speichergruppen mit bis zu je 5 Datenbanken
Datenbankgrenzen	Standard 16GB Enterprise 2TB	Standard 16GB Enterprise 2TB	Standard 75GB Enterprise 8TB (1)
SAN Support	☑ Ja	☑ Ja	☑ Ja
NAS Support	☐ Nein	☐ Nein	☐ Nein
Virenscan	MAPI, AVAPI 1.0, ESE	MAPI, AVAPI 2.5, ESE	MAPI, AVAPI 2.5, ESE
Frontend/Backend HTTP/POP3/IMAP	☐ Nein Nur OWA (HTTP) kann abgetrennt werden.	☑ Ja Nur mit E2K Enterprise Server als Frontend	☑ Ja Auch Exchange Server Standard!
Sonstige Funktionen			Mailbox Recovery Center, Internet Connection Wizard, und vieles mehr

(1) maximale Sicherheitsgrenze liegt bereits bei 8000 GB, nicht bei 8192 GB.

Die Liste ist bei weitem nicht komplett. Weitere Details finden Sie im Internet:

- Funktionen von Exchange 2003 unter Windows 2000 und 2003
  http://www.microsoft.com/exchange/evaluation/features/win_compare.asp
- Vergleich der Exchange-Versionen 5.5, 2000, 2003
  http://www.microsoft.com/exchange/evaluation/features/ex_compare.asp

2.4 Standard oder Enterprise?

Standard versus Enterprise Edition

Exchange 2003 gibt es in zwei Versionen, die beide bis auf wenige Feinheiten identisch in den Funktionen sind und auch problemlos nebeneinander im gleichen Netzwerk installiert werden können. Trotzdem stellt sich die Frage: Welche Version sollten Sie in Ihrem Unternehmen einsetzen? Ein Vergleich der technischen Unterschiede in aller Kürze:

Standard Edition

75 GB Limit

Die wesentliche Einschränkung dieser Version ist die Begrenzung auf nur einen Postfachspeicher und einen Speicher für Öffentliche Ordner. Service Pack 2 hebt die maximal Speichergrenze von 16 GB bis zu 75 GB an und ist somit für die meisten Installationen ausreichend. Weiterhin fehlt der X.400-Connector und die Unterstützung für Microsoft Cluster Server.. Im Gegensatz zur vorhergehenden Version ist auch ein Exchange 2003 Standard-Server in der Lage, als *Front-End-Server* zu agieren. Praktisch stellt das zu konfigurierende 75 GB-Limit für viele Unternehmen keine ernst zu nehmende Begrenzung mehr dar.

Enterprise Edition

20 Datenbanken pro Server

Die *Enterprise Edition* unterstützt im Gegensatz zur *Standard Edition* bis zu vier Speichergruppen mit möglichen fünf Datenbanken und stellt den X.400-Connector zur Verfügung. Zusätzlich umfasst die Enterprise Edition das Clustering, d.h., bis zu acht Systeme bilden einen Verbund, und beim Ausfall eines Servers übernehmen die anderen Systeme die Funktion.

Update-Möglichkeiten

Update-Analyse

Wenn Sie bereits eine 120-Tage-Testversion Exchange 2003 als produktives System einsetzen, so sollten Sie vor dem Update prüfen, welche Exchange-Edition im Einsatz ist. Die Evaluierungsversion der Exchange Enterprise Edition kann nicht auf Exchange 2003 Standard aktualisiert werden. Für eine Evaluierung sollten Sie daher immer mit der Standardversion starten. Wenn die Funktionen nicht ausreichen, ist ein Update auf eine Enterprise-Version (Testversion und Vollversion) einfach durch Überinstallieren möglich.

Auch ein Exchange 2000 Enterprise-Server kann nicht auf einen Exchange 2003 Standard-Server hochgerüstet werden, um zum Beispiel einen Exchange 2003 *Front-End-Server* zu betreiben. Alternativ kann parallel ein Standard-Server installiert werden. Grundsätzlich gilt: Update von Standard auf Enterprise ist möglich, der entgegengesetzte Fall nicht.

Ein Update auf Service Pack 1 ist unabhängig von der Edition. Hier gibt es nur eine Update-Datei, die für Standard und Enterprise verfügbar ist.

Tabelle 2.2 Standard versus Enterprise

Merkmal	Standard Edition	Enterprise Edition
Anzahl möglicher Speichergruppen	1 Speichergruppe	4 Speichergruppen
Anzahl Datenbanken pro Speichergruppe	1 Datenbank für Mailboxen. 1 Datenbank für öffentlichen Ordner	5 Datenbanken (aber maximal 1 Datenbank für öffentlicher Ordner pro Server)
Datenbankgröße	Je maximal 75 GB	Je Maximal 8000 GB (8TB), Hardwareabhängig
Windows Clustering	☐ Nein	☑ Ja
X.400-Connector	☐ Nein	☑ Ja

2.5 Exchange und das Betriebssystem

Verbindung Exchange mit Windows-System

Exchange 2003 ist nicht nur vom Betriebssystem (OS) abhängig, auf dem es installiert wird. Es gibt eine starke Verbindung mit der Version des Active Directory. Die Zusammenhänge werden in einer Gegenüberstellung der Exchange-Versionen und der damit verbundenen Betriebssystemplattform am ehesten verständlich. In der Tabelle wurden die aktuellsten Versionen mit Service Pack (SP) berücksichtigt.

Sicherheitsupdates auch für Exchange!

Aufgrund der engen Verbindung von Exchange mit Windows beeinflussen einige Windows-Updates auch das Exchange-System. Bitte prüfen Sie unbedingt, inwieweit sich vor allem ein Sicherheitsupdate auf die Funktionalität von Exchange auswirkt. Sicherheitspatches, Service Packs und andere Updates für Ihren Microsoft Windows Server finden Sie direkt auf http://windowsupdate.microsoft.com/. Das System wird geprüft und alle erforderlichen Updates werden Ihnen angezeigt.

2.5.1 Abhängigkeit des Servers

Für alle Installationen gilt:

- Exchange 5.5 benötigt eine Domäne. Dies kann eine NT4-Domäne oder Windows 2000/2003-Domäne (Active Directory) sein.

- Exchange 2000 und 2003 benötigen IMMER ein Active Directory, dies kann auf dem gleichen oder einem anderen Rechner laufen.
- Exchange 2000 und Exchange 5.5 können beide nicht auf Windows 2003 installiert werden.

Tabelle 2.3 Abhängigkeiten Exchange und Windows-Server

Alle Angaben ohne Gewähr	Exchange 5.5 SP4 Standard/ Enterprise	Exchange 2000 SP3 Standard/ Enterprise	Exchange 2003 SP2 Standard/ Enterprise
Desktop-Systeme			
NT4 Professional W2K Professional W2K Home Windows XP Windows 95 Windows 98 Windows ME	☐ Nein Kein Server	☐ Nein Kein Server	☐ Nein Kein Server
Windows NT 4.0			
NT4 Standalone	☐ Nein keine Domäne	☐ Nein kein Active Directory	☐ Nein kein Active Directory
NT4 Member Server	☑ Ja	☐ Nein kein Active Directory	☐ Nein kein Active Directory
NT4 PDC/BDC	☑ Ja	☐ Nein kein Active Directory	☐ Nein kein Active Directory
Windows 2000 Service Pack 4			
Arbeitsgruppe	☐ Nein keine Domäne	☐ Nein kein Active Directory	☐ Nein kein Active Directory
Standard-Server	☑ Ja	☑ Ja (5)	☑ Ja (3) eingeschränkt
Advanced Server/ Datacenter Server	☑ Ja	☑ Ja (4)	☑ Ja (3) eingeschränkt
Domänen-controller	☑ Ja (1) LDAP-Konflikt lösen	☑ Ja (5)	☑ Ja (3) eingeschränkt
Windows 2003 (Service Pack 1)			
Windows 2003 Standard/ Enterprise/ Datacenter Server	☐ Nein	☐ Nein (2) IIS6-inkompatibel Nicht unterstützt	☑ Ja

Alle Angaben ohne Gewähr	Exchange 5.5 SP4 Standard/ Enterprise	Exchange 2000 SP3 Standard/ Enterprise	Exchange 2003 SP2 Standard/ Enterprise
Windows 2003 Web Edition	☐ Nein	☐ Nein (2) IIS6-inkompatibel Nicht unterstützt	☐ Nein

1. Der LDAP-Port von Exchange 5.5 muss von 398 TCP z.B. auf 390 umgelegt werden, damit kein Konflikt mit der LDAP-Funktion des Domänencontrollers auftritt.
2. Beachten Sie, dass Exchange 2000 NICHT auf Windows 2003 installiert werden kann, begründet durch die hochgeschraubten Sicherheitseinstellungen des IIS6.
3. Die Exchange 2003 Enterprise Edition ist erforderlich bei einer Cluster-Installation (siehe Hochverfügbarkeit mit Cluster-Systemen), beim Einsatz von mehreren Datenbanken in einer Speichergruppe, bei Überschreitung des 16 GB-Limits sowie bei der Nutzung von Hardware mit mehr als 4 GB Hauptspeicher.
4. Exchange 2000 Enterprise Edition kann auf Windows 2000 Standard-Server installiert werden, um das 16 GB-Limit zu umgehen. Allerdings werden weder Cluster oder große Speicherausbauten unterstützt.
5. Exchange 2000 und 2003 müssen zwingend Mitglied in einem Active Directory sein.

Test mit *Virtual Server*

Die hier mit ☑ gelisteten Kombinationen sind offiziell möglich und werden von Microsoft unterstützt. Andere Kombinationen funktionieren entweder nicht oder werden nicht unterstützt. Für Testzwecke können Sie wunderbar Windows und Exchange auf einem „virtuellen Server“ installieren, wie Sie unter anderem von VMWare oder Microsoft bereitgestellt werden.

2.5.2 Abhängigkeiten vom Active Directory

Seit der Einführung von Exchange 2000 arbeitet das E-Mail-System nicht mehr mit einer eigenen Verzeichnisdatenbank (DIR.EDB), sondern mit dem AD, das zwangsläufig erforderlich ist. Exchange 5.5 kann in einer Active Directory-Domäne installiert werden, nutzt jedoch nicht die Active Directory-Datenbank. Eine weitere Voraussetzung ist die Service Pack-Version; Exchange 2000 SP1 kann zum Beispiel nicht in einer Windows 2003-Domäne genutzt werden.

Alle Angaben ohne Gewähr	Exchange 5.5 SP3 Std/Ent	Exchange 2000 SP3 Std/Ent	Exchange 2003 SP1 Std/Ent
Windows NT4 Domain	☑ Ja	☐ Nein Kein Active Directory vorhanden	☐ Nein Kein Active Directory vorhanden
Windows 2000 SP4 Active Directory	☑ Ja Nicht genutzt (1)	☑ OK auf Windows 2000 Server	☑ Ja (2) mit Einschränkungen
Windows 2003 SP1 Active Directory	☑ Ja Nicht genutzt (1)	☑ OK	☑ OK

Tabelle 2.4 Exchange und Windows-Domänen-Nutzung

1. Active Directory simuliert eine NT4-Domäne und ist für Exchange 5.x mit einer eigenen Benutzerdatenbank ausreichend. Eine Kopplung der Verzeichnisse ist mittels ADC möglich.
2. Nicht alle Funktionen sind verfügbar, beispielsweise fehlen „RPC over HTTP“, das Objekt INetOrgPerson und die abfragebasierten Verteilerlisten (QBDL).

2.6 Lizenzierung

Lizenztechnische Komponenten

Nach der Klärung der technischen Bedingungen muss auch die lizenzrechtliche Betrachtung erfolgen. Die Lizenzthematik ist sehr umfangreich und wird in eigenen Schulungen vermittelt. Trotzdem lässt sich das Thema recht einfach klären: Exchange wie auch Windows und die Clients müssen korrekt lizenziert sein. Eine ausführliche Übersicht der aktuellen Exchange-Lizenzierung finden Sie auch auf den Microsoft-Seiten unter http://www.microsoft.com/exchange/howtobuy.

Server

Jeder Server mit dem Betriebssystem Windows erfordert zwingend eine Serverlizenz. Nun benötigen Sie jedoch auch noch so genannte „Client-Zugriffslizenzen“ (CAL), die den Zugriff der PC-Arbeitsplätze auf den Server erlauben. Die Lizenzierung ist für Windows 2000 und Windows 2003 unterschiedlich. Während es bei Windows 2000 die Möglichkeit gegeben hat, eine Zugriffslizenz an den Server (pro Verbindung) zu koppeln oder an das Endgerät zu binden, gibt es mit Windows 2003 und Exchange 2003 ein abweichendes Lizenzmodell, bei dem neben dem Server auch das Endgerät oder die Person lizenziert wird.

Support MS Virtual Server 2005

Das Unternehmen benötigt für den Exchange-Server eine entsprechende Server-Lizenz für das Betriebssystem und den darauf installierten Exchange-

Server. Diese Lizenzen können als Einzelprodukt gekauft werden. Mit Service Pack 2 unterstützt Microsoft auch offiziell den Virtual Server 2005, auch hier gilt: für jeden installierten Exchange Server 2003 benötigen Sie eine Lizenz. Auf jeden Fall sollte eine Prüfung erfolgen, welche Updates oder Paketangebote genutzt werden können. Für kleinere Firmen bietet sich der Small Business Server inklusive Exchange als kostengünstige Variante an.

Arbeitsplatz

Der Arbeitsplatz benötigt eine Lizenz für das eingesetzte Betriebssystem wie Windows XP, Windows 2000, Windows 98. Für den Zugriff auf einen Windows 2003-Server ist für jeden Arbeitsplatz eine Windows Server-CAL notwendig, selbst wenn Sie auf dem Arbeitsplatz Linux oder Macintosh einsetzen.

Exchange-Anwendung (Client)

User Client Access License (User CAL)

Für den Zugriff auf den Exchange 2003-Server haben Sie die Wahl, ob Sie eine CAL pro Person (User-CAL) kaufen oder pro Endgerät (Device-CAL). Auch eine Kombination der CALs ist möglich. So können Sie einer Person die Lizenz zuweisen, von einer beliebigen Anzahl von Endgeräten auf das eigene Postfach zuzugreifen. Umgekehrt können Sie auch für bestimmte Arbeitsplätze in Ihrer Firma eine Lizenz erwerben, damit alle Personen auf diesem System mit Exchange arbeiten können. Auch eine Kombination der Lizenzen ist möglich. Diese CAL ist auch notwendig, wenn ein anderes Programm als Outlook zum Einsatz kommt.

Die Lizenz enthält das Recht, Outlook 2003 für den Zugriff auf den Mail-Server zu nutzen. Sollten Sie jedoch eine Office-Lizenz besitzen, dürften Sie das darin enthaltene Outlook nutzen, aber nicht an einen Exchange-Server anbinden. Dazu ist zusätzlich die Exchange-CAL notwendig.

Beispiel

In einem durchschnittlichen Netzwerk mit einem Mail- und einem Dateiserver sowie zehn Clients bedeutet dies den Erwerb von folgenden Lizenzen. Zusätzlich müssen Sie die entsprechende Server-Edition ordern.

Tabelle 2.5 Lizenzierung der Server und Clients

System	Lizenzen
Windows 2003 Server	1 x Windows 2003 Server-Lizenz
Exchange 2003 Server	1 x Windows 2003 Server-Lizenz 1 x Exchange 2003 Server-Lizenz
12 Mitarbeiter arbeiten auf 10 Arbeitsplatzrechnern und 5 Arbeitsplätze zu Hause (Home-User)	10 x Windows XP 12 x Windows 2003 Server-CAL 12 x Exchange 2003 User-CAL

Sind die Mitarbeiter aber überwiegend Teilzeitkräfte, die sich wenige PCs teilen, dann könnte eine Lizenzierung pro Endgerät wieder günstiger sein.

Die CALs werden nicht explizit irgendwo eingetragen. Der Lizenzverwaltungsdienst aus früheren Windows-Versionen ist bei Windows 2003 Server standardmäßig deaktiviert. Nur beim Small Business Server (SBS) werden die Lizenzen über eine Lizenzdiskette physikalisch eingespielt.

Mit diesem kurzen Einstieg können Sie eine einfache Exchange-Umgebung rechtlich korrekt lizenzieren. Weitere Lizenzierungen sind möglich, würden hier jedoch den Rahmen sprengen, da die Problematik sehr komplex ist. Die Angaben sind jedoch ohne Gewähr, Sie müssen immer die aktuelle Lizenzierung bei Microsoft-Produkten prüfen, da eine Änderung nicht auszuschließen ist.

2.7 Die wichtigsten Neuerungen

Vorteile mit Exchange 2003 und dem Service Pack 2

Nicht nur für den erfahrenen Exchange-Administrator, sondern auch für den Neuling ist es wichtig zu erfahren, welche Änderungen Exchange 2003 mit sich bringt. Die dreijährige Erfahrung mit Exchange 2000 hat viele kleine Verbesserungen mit sich gebracht, die die Handhabung der neuen Version erheblich vereinfacht. Die nachfolgenden Punkte helfen, Exchange 2003 optimal zu nutzen und von den wichtigsten Neuerungen und Verbesserungen zu profitieren. Neben der Beseitigung von bekannten Fehlern durch das Service Pack 2 (SP2) hat dieses noch weitere Neuerungen und Tools mit sich gebracht, auf die speziell hingewiesen werden. Alle Funktionen und Verbesserungen durch Exchange Service Pack 1 sind in SP2 enthalten. Sie können daher direkt das aktuelle Service Pack installieren.

2.7.1 Installationsvoraussetzungen

Exchange 2003 kann sowohl auf Windows 2000 Server als auch Windows Server 2003 installiert werden. Vor der Installation von Exchange 2003 müssen Sie den Windows 2003-Server entsprechend vorbereiten. Die Vorgängerversion Exchange 2000 arbeitet bekanntlich nicht auf Basis von Windows 2003.

NNTP und WWW

Der Internet News-Dienst eröffnet Exchange die Möglichkeit, auch Öffentliche Ordner per NNTP verfügbar zu machen. Den Dienst können Sie später beenden, wenn Ihre Firma Exchange nicht als News-Server nutzen möchte oder den Zugriff auf bestimmte IP-Adressen einschränkt. Auch der WWW-

Dienst muss explizit installiert werden, diese Option ist nicht mehr per Default aktiviert.

SMTP

Exchange 2003 bringt keinen eigenen SMTP-Dienst mit, wie dies bei Exchange 5.5 der Fall war, sondern erweitert den Windows SMTP-Dienst um eigene Befehle. Der SMTP-Dienst muss bei Windows 2003 nachinstalliert werden, da er bei der Standardinstallation nicht enthalten ist.

IIS6 (Internet Information Server)

Der IIS regelt nicht nur den Exchange-Zugriff für Outlook Web Access-Benutzer, sondern wird auch für andere Funktionen von Exchange benötigt. Der Exchange System-Manager benutzt die Dienste des IIS-Servers für die Verwaltung. Beispielsweise werden Einstellungen in Öffentlichen Ordnern per HTTP ausgelesen und gesetzt. Bei der Installation auf einem Windows 2000 Server mit IIS5 ist mit Einschränkungen zu rechnen.

Updates und Sicherheitspatches

System auf Service Pack 2 vorbereiten

Bevor Sie das Service Pack 2 für Exchange installieren, sollten Sie die erforderlichen Windows Updates und Patches prüfen. Microsoft empfiehlt die Installation von Windows Server 2003 Service Pack 1, jedoch muss der Hotfix 898060 zwingend nachinstalliert werden. Small Business Server-Kunden benötigen das SBS SP1, um Exchange 2003 SP2 zu installieren. Zur Aktivierung der Absendererkennung (Sender-ID) benötigen Sie unbedingt einen Windows 2003 Hotfix, den Sie direkt bei Microsoft Product Support Services anfordern müssen. Sie sollten auf jeden Fall alle kritischen Patches auf Ihrem Server installieren. Nach dem Update auf SP2 können ebenfalls noch Patches erforderlich werden, die später veröffentlicht wurden. Jedes Service Pack ist differentiell und enthält alle vorherigen Service Packs. Nutzen Sie einfach die Microsoft Update Webseite oder installieren und konfigurieren Sie den kostenfreien Windows Software Update Service (WSUS).

ASP.NET

Die Installation dieser Komponente ist z.B. für den Betrieb von Mobile Access notwendig. Das eigentliche *.NET-Framework* ist hingegen schon bei der Installation des Betriebssystems Windows 2003 mit installiert.

Weitere Installationsunterstützung

ExDeploy-Tools

Der Installationsassistent ist sehr genau bei der Überprüfung der Voraussetzungen und lässt die Exchange-Installation erst zu, nachdem die Umgebung geprüft und angepasst wurde. Aber das ist noch nicht alles. In einer

vorhandenen Exchange 5.5-Organisation, die migriert werden soll, installiert der Assistent auch den Active Directory Connector (ADC) und erwartet die Einrichtung aller notwendigen Verbindungsvereinbarungen (CA), um mit der Installation fortfahren zu können. „Mal eben schnell“ Exchange installieren und dann einiges später nachholen ist so nicht mehr möglich. Andererseits sind damit häufig gemachte Fehler im Vorhinein nicht mehr möglich, und der Assistent zeigt an, warum das Setup nicht erfolgreich war. Diese Werkzeuge (Bereitstellungstools) finden Sie auf der *Exchange 2003 Server*-CD-ROM im Verzeichnis „\support\exdeploy“, mit der zu startenden Hilfe-Datei können Sie die Funktionen steuern. Da diese Tools jedoch regelmäßig verbessert werden, sollten Sie die aktuelle Version der Bereitstellungs-tools (Exdeploy.exe) aus dem Internet downloaden. Auch enthält Service Pack 2 eine ganze Reihe weiterer Features in den Exdeploy-Tools.

2.7.2 Sicherheit

Per Default deaktiviert

Im Gegensatz zu den Vorgängern hat Microsoft mit der neuen Version die Sicherheit extrem verschärft. Funktionen, die in Exchange 2000 oder 5.5 noch möglich waren, müssen heute explizit frei geschaltet werden. Exchange 2003 ist somit sehr viel restriktiver bei der Berechtigungskonfiguration. Beispielsweise müssen Sie den Zugriff auf die Protokolldateien der Nachrichtenverfolgung (Tracking Log) einrichten, ebenso können Sie keine Basisordner (Top Level Public Folder) ohne die entsprechende Berechtigung anlegen, dazu sind Sie nur noch als Administrator befugt. Mit der standardmäßigen Deaktivierung von POP3 soll verhindert werden, dass Kennwörter im Klartext übertragen und bei Abruf über das Protokoll die Nachrichten im Postfach gelöscht werden. Mit Service Pack 2 ermöglicht ein Plus an Sicherheit, wenn Sie Outlook auf mobilen Geräten nutzen. Beachten Sie, dass einige Zusatzprogramme eine entsprechende Änderung benötigen und dann erst mit den neuen „sicheren“ Einstellungen funktionieren.

2.7.3 Datensicherung und Wiederherstellung

Exchange 2003 kann mit dem Programm NTBACKUP im laufenden Betrieb gesichert werden, da die Installation das Backup-Programm um die Online-Sicherung erweitert. Einzelne Nachrichten bzw. das so genannte „Brick Level Backup“ oder „Single Mailbox Backup“ werden nicht von NTBACKUP unterstützt.

Mit der Anzeige über den Status der Sicherung im *Exchange System-Manager* (ESM) erweitert Microsoft die Überprüfung wichtiger Systeminformationen. Somit wird dem Administrator mitgeteilt, wann das letzte

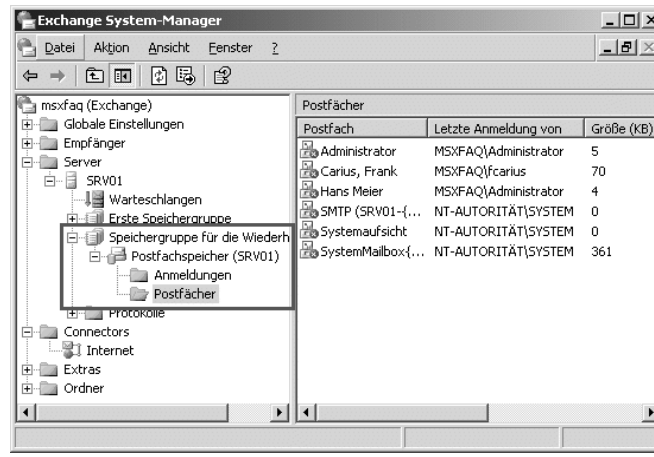
erfolgreiche Backup des Servers stattgefunden hat, und er kann somit auf eine Fehlfunktion reagieren.

Abbildung 2.2 Anzeige der letzten Sicherung

Recovery Storage Group

Die Rücksicherung von Postfächern oder Mails in den vorhergehenden Exchange-Versionen führte immer zum gleichen Problem: Sie benötigen einen separaten Server zur Wiederherstellung. Backup-Programme können die Exchange-Datenbank immer nur als einen monolithischen Block sichern und restaurieren. Dies bedeutet, dass auch die Rückgewinnung eines einzelnen Postfachs oder einer einzigen gelöschten Nachricht einen großen Zeitaufwand bedeutete. Exchange 2003 erlaubt nun die Wiederherstellung von Datenbanken einer Sicherung in eine eigens angelegte Speichergruppe. Durch diese besondere Speichergruppe kann eine alte Datenbank des produktiven Servers wieder hergestellt und die Inhalte können übertragen (ExMerge) werden.

Abbildung 2.3 Recovery Storage Group im Einsatz



Seit Exchange Service Pack 1 ist nun auch die direkte Übertragung der Daten aus der Wiederherstellungsdatenbank in das aktuelle Postfach möglich. Eine Filterung der Daten nach bestimmten Kriterien ist jedoch weiterhin nur mit EXMERGE möglich.

Volume Shadow Copy Services (VSS)

Windows 2003 bringt die Funktion der Schattenkopie (Shadow Copy) mit, die eine schnelle Dateirücksicherung ermöglicht. Dies gilt auch für ganze Festplatten, die mit einem zeitsynchronen Schnappschuss festgehalten werden. Der Zustand des Datenträgers wird anschließend mit einer geeigneten Software gesichert. Die Schattenkopie erlaubt also, alle Daten zu einem festen Zeitpunkt zu kopieren und dann mit einer VSS-tauglichen Sicherungssoftware zu sichern. Mit der Installation von Exchange 2003 wird dieser Windows 2003-Dienst erweitert, damit auch Exchange-Datenbanken korrekt behandelt werden. NTBACKUP unterstützt leider keine Sicherung dieser Schattenkopien, so dass Lösungen von Drittherstellern notwendig sind.

2.7.4 Abfragebasierte Verteiler

Query based Distribution Lists (QBDL)

Eine der Neuerungen, auf die jeder Exchange-Administrator schon sehnsüchtig gewartet hat. Bislang wurden die Exchange-Verteiler im Active Directory als Gruppe manuell gepflegt. Dies bedeutete einen ständigen Pflegeaufwand. Bei der Zuordnung unterschiedlicher Berechtigungen für Verteilergruppen und Sicherheitsgruppen kann es auch schon mal zu falschen Einträgen kommen. In der Kombination Windows 2003 Server und Exchange 2003 Server im *Native Mode* ist eine neue Definition von Verteilern möglich. Und zwar werden dynamische Verteiler auf Basis einer LDAP-Abfrage erstellt und aktualisiert. Wer diesen Verteiler nun auch für Berechtigungen auf OUs oder Öffentliche Ordner nutzen möchte, sieht sich indessen schwer enttäuscht. Es handelt sich hier um eine neue Art von Active Directory-Gruppe, die nicht als Sicherheitsgruppe aktiviert und auch kein Mitglied dieser werden kann. Nutzen Sie dieses Feature zur automatischen Verwaltung von flexiblen Verteilern für den Mailverkehr, und lösen Sie damit regelmäßig ablaufende Skripte oder entsprechende Drittprogramme ab.

2.7.5 Mobile Geräte und ActiveSync

OMA und Direct-Push

E-Mail ist in vielen Unternehmen bereits so wichtig, dass auch mobile Anwender von dem Service Pack 2 profitieren. Mit Exchange 2000 war der Zugriff per WAP oder ActiveSync nur möglich, wenn das Zusatzprodukt „Mobile Information Server“ installiert wurde. Beide Funktionen sind in Exchange 2003 integriert und wurden mit dem Service Pack 2 aktualisiert. Besonders zu erwähnen sind die neuen Funktionen zur sofortigen Übertragung neuer Nachrichten an den Client ohne SMS, Zugriff auf das

globale Adressbuch und die Verwaltungsfunktionen wie z.B. RemoteWipe, Richtlinien für Geräteschutz und zertifikatbasierte Anmeldung. Diese Mobilitätsverbesserungen sind allerdings nur mit aktuellen PDA's nutzbar, die Windows Mobile 5 und das Message Security und Feature Pack (MSFP) installiert haben.

2.7.6 Outlook Web Access

Outlook Web Access (OWA)

Analog zur neuen Oberfläche von Outlook 2003 wurde auch der Outlook Web Access (OWA) umfassend verändert und zeigt sich als komfortable Weboberfläche. Eine gesteigerte Produktivität ist durch die neue Aufteilung und der damit verbundenen Leistung ganz sicher zu erwarten. Hinzugekommen ist der Zugriff auf Aufgaben, die Bearbeitung von verschlüsselten und signierten Nachrichten per S/MIME und eine Rechtschreibprüfung. Hier sind mit SP1 weitere Sprachen hinzugekommen, mit SP2 auch Portugiesisch. OWA ist also sehr viel flexibler geworden und kann umfassend angepasst werden. Auch die Sicherheit wurde erheblich verbessert. Hat ein Anwender nach der Nutzung des Outlook Web-Zugriffs mit Exchange 2000 nicht den Browser beendet, so konnte eine andere Person an diesem PC das Postfach im Internet Explorer ohne Autorisierung öffnen. Outlook Web Access erlaubt mit Exchange 2003 eine formularbasierte Authentifizierung mit Cookies, die bei der Abmeldung eine Wiederaufnahme ohne Kennwort verhindern. Ganz hilfreich und häufig vermisst ist auch die Implementierung von Regeln. Sollten Sie die Anlagensicherheit bei OWA angepasst haben, überschreibt SP2 diese Einstellung und Sie müssen den Registrierungsschlüssel neu definieren.

2.7.7 Zusammenführung von Warteschlangen

Queue Viewer

Mit Exchange 2000 war es für Administratoren relativ aufwändig, alle Warteschlangen eines Servers zu kontrollieren. Die Ansicht der oft umfangreichen Warteschlangen war auf mehrere Ordner in der Protokollstruktur verteilt. Der Exchange 2003 System-Manager erlaubt die zentrale Ansicht der Warteschlangen pro Server und erleichtert so die Fehlersuche. Bei großen Mailaufkommen können Sie über Suchfunktionen eine einzelne Nachricht leichter finden.

2.7.8 Internet Connection Wizard

SMTP Server und RUS

Komplett neu ist der Assistent zur Einrichtung der Internet-Verbindung. Schritt für Schritt wird die Konfiguration erläutert, und der Server erhält die richtigen Einstellungen, um Nachrichten per SMTP zu senden und anzu-

nehmen. Unter anderem richtet der Assistent auch die Empfängerrichtlinien (Recipient Update Service) ein und führt Änderungen am virtuellen SMTP-Server aus. Trotz Assistent können die häufigsten Fehlerursachen nicht vermieden oder korrigiert werden. Dazu zählen die Einrichtung der MXRecords, die Freischaltungen in einer Firewall oder einem Router und der technische Anschluss an das Internet. Hierzu ist das Verständnis der Zusammenhänge, die später erläutert werden, wichtig.

2.7.9 Öffentliche Ordner

Sammelbox für Informationen

Viele Unternehmen nutzen die Öffentlichen Ordner als Informationsdrehscheibe für gemeinsame Nachrichten und die kollektive Zusammenarbeit mit Kalendern, Aufgaben und Ablagen.

Mit Exchange 2003 wurden zusätzliche Funktionen realisiert. Das Senden der *Public Folder*-Hierarchie, die teils über 24 Stunden nach einer Änderung nicht auf anderen Servern sichtbar war, kann beschleunigt werden. Aufgrund einer Berechtigungseinstellung können anonyme Benutzer eine Nachricht an einen Öffentlichen Ordner senden, dies war in Exchange 2000 nicht möglich. Somit können Sie einen Öffentlichen Ordner wieder als „Sammelbox“ auch für Internet-Mails nutzen.

Verbessertes Management mit SP2

Das Service Pack 2 vereinfacht die Verwaltung der Öffentlichen Ordner und minimiert dadurch die Belastung aufgrund zahlreicher Replikationsanfragen. Neben dem Stoppen der Replikation, der gezielten Vererbung von Einzelrechten und dem erneuten Senden von Änderungen können Sie mit SP2 das Löschen von Ordnern protokollieren. Auch das Verschieben von Öffentlichen Ordnern wird nun mit einer benutzerfreundlichen Lösung unterstützt, trotzdem ist die Anwendung mit Vorsicht zu empfehlen,

2.7.10 Postfächer wieder verbinden

Mailbox Recovery Center

Seit der Einführung des Active Directory ist die Exchange Mailbox nun ein Attribut eines Benutzers. Wird ein Benutzer im Active Directory gelöscht, so verliert Exchange die Verbindung und kennzeichnet das Postfach in der Speichergruppe mit einem roten X. Häufig ist es erforderlich, das Postfach einem neuen Benutzer zuzuordnen oder Inhalte daraus wieder bereitzustellen. Eine zentrale Übersicht im Exchange System-Manager erleichtert nun das Auffinden und Verbinden solcher verwaisten Postfächer. Die Ansicht erstreckt sich über viele Server mit einer ganzen Anzahl an „Postfachspeichern“, die auszuwählen sind.

2.7.11 Nachrichtenverfolgung und Sicherheit

Message Tracking Center

Wer bislang problemlos den Nachrichtenstatus ausgelesen hat, stößt nun auf eine neue Sicherheitsanforderung, die die Autorisierung der Freigabe `%SERVERNAME%.LOG` einfordert. Der Zugriff für `Jeder` ist nun per Default deaktiviert, nur noch Administratoren haben Zugriff auf die Freigabe. Prüfen Sie, wem diese Rechte zugewiesen werden, und fügen Sie die Benutzer in einer Gruppe zusammen, die die Log-Dateien auswerten darf. Bei Exchange 2000 und früher konnte noch jeder diese Textdateien einsehen.

2.7.12 Spamschutz

RBL oder ORDB

Unerwünschte Nachrichten, so genannter Spam, nehmen täglich zu und verstopfen die Postfächer. Verschiedene Dritthersteller bieten entsprechende Filterprogramme an, die z.B. die IP-Adresse des Absendersystems in einer Datenbank abfragen. Hier sind z.B. Adressen von offenen Relay-Systemen hinterlegt, die von Spam-Versendern gerne missbraucht werden. Der virtuelle SMTP-Server kann die RBL und ORDB nutzen, um diese Werbenachrichten zu reduzieren. Diese Einstellung ersetzt jedoch nicht die Funktionalität eines professionellen Anti-Spam-Programms.

IMF und Sender-ID

Mit der Installation des Service Packs integriert Exchange das Zusatzmodul „Intelligent Message Filter (IMF)“, das eingehende E-Mails analysiert und bewertet. Diese Funktion wurde mit dem letzten Service Pack weiter verbessert, nicht nur um die Identifizierung gefälschter Absenderadressen sondern auch um das Erkennen und Blocken von spoofing Angriffen und „Phishing“ E-Mails. Sie können die Schlüsselwörter selbst definieren, allerdings ohne eine benutzerfreundliche GUI.

2.7.13 Active Directory Connector

ADC und ADC-Tools

Der *Active Directory Connector* ist eine wichtige Komponente speziell bei der Migration von Exchange 5.5-Umgebungen nach Exchange 2003. Dieser Prozess muss während der gesamten Umstellungszeit dafür sorgen, dass die beiden Verzeichnisdienste von Exchange 5.5 und das Active Directory korrekt abgeglichen werden. Dazu ist es notwendig, dass die Voraussetzungen für einen erfolgreichen Abgleich geschaffen und die Verbindungsvereinbarungen korrekt eingerichtet werden.

Hierbei helfen die neuen *ADC-Tools*, die mit der Installation des Active Directory Connectors installiert werden. Das Exchange 2003-Setup prüft diese Vorbedingung und verweigert gegebenenfalls die Arbeit. Auch der ADC wird mit dem SP1 aktualisiert. Dazu müssen Sie manuell aus dem Archiv das Setup im Verzeichnis „ADC“ ausführen.

2.7.14 Exchange Datenbank

16GB-Limit fällt

Für viele kleinere Unternehmen bedeutet die Erhöhung der Größenbeschränkung der Exchange Server 2003 Standard Edition Service Pack 2.eine wahrhaft willkommene Verbesserung. Verweigerte der Exchange Standard Server bislang bei Datenbanken größer 16 GB seinen Dienst, kann die Datenbank seit SP2 bis auf 75 GB wachsen. Jedoch sind auch hier einige Direktiven zu beachten. Der Standardgrenzwert für die Standard Edition nach der Installation von SP2 ist 18 GB, den Sie mittels Registrierungsschlüssel „Database Size Limit in GB“ überschreiben können. Doch auch für die Enterprise Edition bietet sich eine Limitierung der Datenbank an, um beispielsweise ein unbeabsichtigtes Wachstum der Datenbankgröße zu vermeiden oder um vereinbarte SLA’s für die Wiederherstellung zu erreichen.

Berechnung logische Datenbankgröße

Neu ist auch die Berechnung der Datenbankgröße seit SP2, die nun der logischen Größe und nicht mehr der Dateigröße entspricht. Bei 90% Kapazitätserreichung erhalten Sie bereits eine Warnmeldung, bei der ersten Überschreitung wird nur ein Eintrag im Eventlog geschrieben und Sie können die Datenbank reduzieren. Der Serverdienst wird erst 24 Stunden später bei anhaltender Überschreitung beendet. Sie sehen jetzt, wie wichtig eine Überwachung des Eventlog für den Betrieb Ihres Servers ist. Die für die manuelle Konfiguration erforderlichen Registrierungseinstellungen finden Sie in dem Microsoft Exchange Server TechCenter im Bereich Information Store Service Architecture unter folgender URL:
http://www.microsoft.com/technet/prodtechnol/exchange/guides.

2.7.15 Weitere Verbesserungen

RPC over http

Die Erfahrungen mit Exchange 2003 haben gezeigt, dass die Funktion RPC over HTTP(s) an Bedeutung zunimmt. Nicht nur für die Konsolidierung von Standorten sondern auch für das Outsourcing von Exchange als Service spielt dieses Protokoll eine entscheidende Rolle. In den Profileinstellungen von Outlook 2003 können Sie die Verbindung per HTTP oder per HTTPS (SSL-Verschlüsselung) mit dem Server konfigurieren. So können Sie Outlook ohne VPN auch über das Internet betreiben.

MAPI-Zugriff steuern

Microsoft hat mit Service Pack 2 zudem die Möglichkeit geschaffen, das Protokoll MAPI pro Anwender zu deaktivieren oder einzuschränken. Somit können Sie den Zugriff steuern und z.B. nur OWA ermöglichen oder sogar den Einsatz mit Outlook im Cache Modus erzwingen. Mit dem Tool ADSIEDIT können Sie das erforderliche Attribut `ProtocolSettings` bearbeiten, das jedoch nicht bei dem Verschieben von Postfächern sowie bei der Stellvertreterfunktionalität greift.

OAB Optimierung

Die Verwendung des Offline Adressbuches (OAB) im Outlook Cached Mode war häufig nicht zufriedenstellend. In Exchange Sercive Pack 2 wurde die OAB Version 4.0 eingeführt, die Outlook 2003 Service Pack 2 voraussetzt. Neben der enormen Reduzierung der OAB-Größe wurde auch das Verfahren der Indizierung geändert. Sie können den Index lokal am Client erstellen sowie auch Eigenschaften anpassen. Das OAB wird nun nicht mehr so häufig vollständig transferiert sondern es werden kleinere Aktualisierungsdateien abgerufen. OAB 4.0 erfordert den Postfachmodus Unicode im Client-Profil, d.h. Sie müssen eine vorhandene PST oder OST-Datei neu als UNICODE-Version erstellen lassen.

Virtual Server

Mit Service Pack 2 erlaubt Microsoft nun auch offiziell die Exchange 2003 Installation in virtuellen Maschinen mit der Version MS Virtual Server 2005 R2. Dazu sind einige spezifische Konfigurationen erforderlich. Ein Einsatz in anderen virtuellen Serversysteme wird nicht unterstützt.

2.7.16 Neue Tools

Hilfsprogramme

Viele Unternehmen haben ihr E-Mail-System bereits auf Exchange 2000 umgestellt oder sind noch in der Umstellungsphase. Dabei sind viele Probleme erkannt worden, für die Microsoft immer wieder neue Hilfsprogramme zur Erkennung und Beseitigung entwickelt. Mit Exchange 2003 wird ein *Exchange-Deployment-Paket* ausgeliefert, das jede Menge solcher Tools für die Migration und Administration enthält. So ist es mit dem Skript „pfmigrate.wsf“ möglich, die Replikate von Öffentlichen Ordnern per Skript zu verändern, SP2 bietet diese Funktion nun auch im Exchange System Manager an. Dies erspart viel manuelle Arbeit bei der Umstellung einer großen Anzahl öffentlicher Ordner auf einen anderen Server. Das Programm „EXCHDUMP.EXE“ erlaubt die Ausgabe der aktuellen Konfiguration in eine Datei, mit der Support-Firmen sehr schnell einen Überblick über die Installation erhalten. Wie bereits erwähnt enthält es viele hilfreiche Informationen für die Migration und Prüfung der Active Directory-Struktur.

ExBPA

Der *Microsoft Exchange Server Best Practices Analyser Tool*.prüft Ihr System auf Basis neuester Erkenntnisse und zeigt, wie Sie diese anwenden können (Kapitel 8.6).

IMF und ExMerge

Aufgrund des steigenden Spam-Aufkommens können Sie nun den *Microsoft Exchange Intelligent Message Filter* einrichten, der diese Emails direkt am Gateway oder im Postfachspeicher blockiert, SP2 enthält zusätzlich das Sender-ID Verfahren. Auch der Assistent zum Zusammenführen von PST-Dateien und Postfächern (ExMerge) wurde aktualisiert.

Konsolidierung von Standorten im gemischten Modus

Die Bereitstellungstools (ExDeploy) sind ebenfalls seit SP1 verbessert worden. Dazu gehört auch das Programm zur Standortkonsolidierung in einer gemischten Exchange 5.5 und 200x-Umgebung. Somit ist es erstmals möglich, auch im gemischten Exchange-Modus Postfächer, Verteiler und Kontakte von einer Administrativen Gruppe in eine andere zu verschieben. Der Assistent zur Konsolidierung zeigt die detaillierte Vorgehensweise in drei Phasen genau auf. Mit dem Exchange-Profilaktualisierungstool (Exchange Profile Update) können Sie das Outlook-Profil nach der Konsolidierung auf die neue Administrative Gruppe umstellen, ohne die bisherigen Einschränkungen wie etwa den Verlust von Regeln in Kauf nehmen zu müssen.

Einige neue Tools wie SMTPDiag zur Fehleranalyse von SMTP und DNS, Outlook Web Access Web Administration (OWAAdmin) zur Anpassung der OWA-Konfiguration sowie der Auto Accept-Agent zum automatischen Akzeptieren von Besprechungsanfragen finden Sie auf der Exchange-Download-Seite:
http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/tools.mspx.

Neue Onlinehilfe

Das Exchange Service Pack 2 enthält viele Updates und Verbesserungen, die seit der Einführung von Exchange 2003 auf Basis der Erfahrungen und Ihres Feedbacks entwickelt wurden. Einige haben wir bereits genannt, alle weiteren Informationen und Problemlösungen finden Sie unter anderem in den *Exchange Server 2003 SP2 Release Notes* (Download unter der URL http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/sp2rn.mspx). Auch einige Sicherheitslücken wurden geschlossen. Die Programmhilfe wird nun automatisch aktualisiert. Das Exchange Server 2003-Administratorhandbuch finden Sie unter der folgenden URL: http://www.microsoft.com/technet/prodtechnol/exchange/DE/Guides/E2k3AdminGuide.

2.8 Neue Funktionen ohne Berücksichtigung

Was fehlt?

Aufgrund der vielen Neuerungen von Exchange 2003 und dem breiten Einsatzspektrum von einem kleinen Netzwerk bis zu internationalen Organisationen mit tausenden Postfächern ist bei der weiteren Beschreibung von Exchange 2003 eine Auswahl getroffen worden. Die nachfolgenden Themen werden im Buch nicht weiter behandelt.

Im Gegensatz zur Vorgängerversion fehlen nun auch einige Funktionen. Es gibt keinen eigenen *Key Management Service*, Exchange 2003 nutzt stattdessen die PKI des Windows 2003 Servers. Ebenso ist das häufig zu Irritationen führende Laufwerk M: (*Web Storage System*) per Vorgabe nicht

mehr verfügbar. Auch die Konnektoren für MSMail und cc-Mail sind nicht mehr enthalten. Die erweiterten Funktionen zur Zusammenarbeit (Collaboration Services wie Instant Messaging und Conferencing) sind nun als neues Produkt *Microsoft Office Live Communications Server 2003* verfügbar und nicht mehr Teil von Exchange.

Verbundene Standorte über SMTP und X.400

X.400-Connector

Wer in seiner Exchange 5.5-Umgebung bislang SMTP-Connectoren über VPN und X.400-Connectoren eingesetzt hat, kann diese auch weiter mit Exchange 2003 nutzen. Allerdings sind diese Connectoren nur noch zweite Wahl. Stattdessen ist der Einsatz von Routinggruppen-Connectoren zu empfehlen, die im Gegensatz die Leitwege flexibel berechnen und innerhalb einer Gruppe von Exchange-Servern diese Liste austauscht..

Key Management Service

KMS

Exchange 2000 und Exchange 5.5 hatten eine Funktion, die öffentliche und private Schlüssel für Anwender bereitstellte. Dadurch konnten Anwender per S/MIME Nachrichten verschlüsselt austauschen und signieren. Die Funktion des Key Management Servers ist bei Exchange 2003 komplett in der Zertifikatsstelle von Windows 2003 aufgegangen. Die Zertifikatsstelle von Windows 2003 kann auch verlorene Zertifikate erneut ausstellen.

Von Instant Messaging zu Live Communication Server

IM

Mit Exchange 2003 entfällt der Dienst für Instant Messaging. Diese Funktion wurde in den neuen *Office Live Communications Server 2003* integriert. Ein Inplace-Update eines Exchange 2000-Servers auf Exchange 2003 funktioniert erst nach der Deinstallation der Instant Messaging-Komponente. Der Exchange 2000 Instant Messaging-Dienst kann in einer Organisation von allen Benutzern verwendet werden, solange noch ein Exchange 2000-Server dafür bereitsteht. Da das Ende dieses Produkts besiegelt ist, sollten Sie eine Migration zum Office Real-Time Communications Server einplanen.

Clustering

Cluster

Die Hochverfügbarkeit von Exchange mit dem Microsoft Cluster-Service wurde mit Exchange 2003 erneut gesteigert. Neben den Funktionen der Schattenkopien, der Recovery Storage Group und des verbesserten Monitoring ist die Funktion des Clusters eine wesentliche Funktion zur Verfügbarkeit. Die Aufteilung eines Postfachspeichers kann nicht auf mehrere Server erfolgen, da es sich hierbei um eine physische Datei handelt. Es müssen Vorkehrungen getroffen werden, um den Ausfall des Servers selbst aufzufangen. Defekte beim Hauptspeicher, Netzteil oder bei der Betriebssysteminstallation können sonst den Server längere Zeit außer Funktion

setzen. Hierzu eignet sich der Cluster-Server, der mit Exchange 2003 Enterprise die Zusammenschaltung von bis zu acht Servern erlaubt, die alle die Funktion eines ausgefallenen Servers übernehmen können und gemeinsam auf einen Festplattenkäfig mit den Postfachspeichern zugreifen.

Outlook-Programmierung

Outlook Scripting und Workflow

Outlook ist der primäre Client für Exchange 2003, und die neue Version 2003 erweitert nochmals die Möglichkeit einer optimalen Ausnutzung aller Funktionen innerhalb des Postfachs. Der Umfang von Outlook ist nochmals durch eigene Programme und Skripte erweiterbar, um Lösungen wie die Abwicklung von Betriebsabläufen zu schaffen. Die Programmierung mit Outlook ist kein Thema in diesem Buch.

Exchange Management Pack für Microsoft Operation Manager

MOM

Unternehmen, die heute schon mit dem Microsoft Operation Manager ihre Infrastruktur überwachen, werden von dem Management Pack für Exchange 2003 profitieren können. Dieses ergänzt MOM um wichtige Funktionen und die Kenntnis, welche Parameter für Exchange wichtig und zu überwachen sind.

OMA-Anbindungen an Telefonprovider

SMS-Benachrichtigung

Die in Exchange 2003 integrierte Funktion, mit mobilen Geräten über Funktelefone, Internet, WiFi, WAP und weitere Möglichkeiten und Protokolle auf das Postfach zuzugreifen, wird immer mehr genutzt. Dies erlaubt nun auch eine Benachrichtigung des Endgeräts über neu angekommene Mails. Aufgrund mangelnder Erfahrungen mit entsprechenden Telefon-Providern und den Angeboten im Markt kann diese Funktion nicht genauer beschrieben werden. Die SMS-Benachrichtigung beruht auf einer Übertragung der Nachrichten per SMTP an ein SMTP-to-SMS-Service Gateway des Telefonanbieters.

Windows Management Instrumentation-Nutzung

WMI

Exchange 2003 erweitert die WMI-Schnittstelle, um auch per Skript nahezu alle Funktionen auszuführen, die bislang nur über die grafische Oberfläche möglich waren. Dies wurde besonders bei Exchange 2000 bemängelt, da sehr viele Aktionen (User-Liste mit Postfachgröße) nicht automatisiert werden konnten. Der Umgang mit dieser Schnittstelle bleibt den Entwicklern vorbehalten, die in der Produktdokumentation die notwendigen Hinweise finden.

Windows 2003- und IIS6-Verbesserungen

Windows 2003

Veränderungen, die die Weiterentwicklung von Windows 2003 betreffen, werden nur in Beziehung mit Exchange aufgeführt, wenn dies für den Betrieb

relevant ist. Auf die Besonderheiten und Änderungen des IIS6 wird ebenfalls nur so weit eingegangen, wie dies für Exchange 2003 erforderlich ist.

Migration: Active Directory Connector, ExDeploy-Tools, ADC-Wizard

Migration im Detail

Exchange 2003 bringt sehr viele neue Programme und Erweiterungen mit, die dem Administrator bei der Migration seiner Exchange 5.5-Umgebungen nach Exchange 2003 helfen. Hierzu zählt ein Assistent für die Installation des Active Directory Connector und die Einrichtung von Verbindungsvereinbarungen zwischen der „alten" und der „neuen Welt". Viele Werkzeuge aus dem Verzeichnis `\support\ExDeploy` erlauben eine Prüfung der bisherigen Exchange 5.5-Umgebung. Die Migration von Exchange 5.5 ist ein Thema, das mehrere Bücher füllen kann und sehr ähnlich der Migration zu Exchange 2000 ist. Im Kapitel „Migration" wird im Allgemeinen auf die Exchange-Migration eingegangen, auf Details und How-To's wird verzichtet. Auch die davon betroffenen Neuerungen der Service Packs, wie die Standortkonsolidierung, das ADC-Update, die Unterstützung der Novell GroupWise 6.x-Konnektoren und -Migrationstools und weitere Migrationsunterstützungen, werden nicht weiter berücksichtigt.

Multi-Forest-Szenarien

Multi Forest

Exchange 2003 erlaubt den Betrieb mit mehreren Active Directory-Gesamtstrukturen (Forests). Gerade die Windows 2003-Möglichkeit, einem Forest transitiv zu vertrauen, motiviert große Organisationen, die Installation von Exchange in einem Ressource Forest zu betreiben. Solche Szenarien werden nicht vertieft, dazu sind sie einfach zu speziell und selten. Die Anbindung von Benutzern einer Windows NT4-Domäne wird jedoch beschrieben.

DS-Proxy Verhalten

DS-Proxy

Der Einsatz mehrerer Domänen führte häufig zu Problemen bei der Berechtigung von Stellvertretern, Veröffentlichung von Zertifikaten sowie bei der Pflege von Gruppenmitgliedschaften. Exchange Service Pack 2 bringt eine Änderung des DS-Proxy-Verhaltens mit, indem ein fünfstufiger Algorithmus Hilfestellung bei der Wahl eines Globalen Kataloges in der eigenen Domäne bietet. In ungünstigen Situationen spricht der Client einen GC in einem anderen Standort an.

Verzeichnisreplikation mit Metadirectory

Metadirectory

Das Active Directory dient in vielen Unternehmen als globales Verzeichnis und wird immer häufiger mit anderen Verzeichnisdiensten synchronisiert. Dies beeinflusst auch Exchange, da über solche Abgleichmechanismen ebenfalls Kontakte und Mailadressen in dem Active Directory gepflegt werden. Auf solche Umfelder wird nicht weiter eingegangen. Weitergehende Informa-

tionen finden Sie z.B. auch auf der Microsoft-Informationsseite im Internet zum Microsoft Identity Integration Server (MIIS).

Softwareverteilung für Outlook und Office-Gruppenrichtlinien

Client-Installation

Der Einsatz von Exchange 2003 zieht auch die Umstellung oder Einführung des Outlook-Clients nach sich. Die Installation, Konfiguration und Wartung von Outlook oder eines anderen Clients im Unternehmen ist sehr zeitaufwändig und bedingt häufig die Phase mit der größten Gewichtung. Das Active Directory erlaubt mittels Gruppenrichtlinien eine sehr weitgehende Steuerung der Installation und des Funktionsumfangs der Clients.

-1018-Fehler und Exchange SP1

„-1018“

Exchange prüft die Integrität der Datenbank über eine blockweise CRC-Prüfsumme bei jedem Festplattenzugriff. Fehler in der Prüfsumme weisen auf Fehler im Speichersubsystem hin und werden im Eventlog als „-1018“-Fehler protokolliert. Ab Exchange 2003 SP1 hat Microsoft das Prüfsummeverfahren derart verbessert, dass so genannte "1-Bit-Fehler" erkannt und korrigiert werden. Allerdings sollten Sie diesen Fehler nicht auf die leichte Schulter nehmen, denn das Problem ist wie beim „echten“ -1018 weiterhin vorhanden und kann sich verschlimmern. Spätestens beim zweiten Bitfehler sind ihre Daten defekt. Unter www.msxfaq.de finden Sie weitere Informationen hierzu.

Keine „In Depth“-Artikel

Exchange-Details

Im Gegensatz zu der Webseite www.msxfaq.de, die teilweise sehr ins Detail geht, soll das Buch eine bestimmte Komplexität nicht überschreiten. Daher werden hier nicht die letzten Bits und Bytes und Tricks zum Tuning beschrieben, sondern der Fokus liegt auf der Exchange 2003-Installation und dem Betrieb. Die meisten Exchange-Server erfüllen die Anforderungen des Unternehmens mit ein wenig Anpassung zur vollsten Zufriedenheit. Die Informationen der Webseite sind für den Betrieb eines Exchange-Servers zwar nützlich zu wissen, aber nicht unerlässlich für die Installation eines normalen Servers.

2.9 Gründe für ein Update auf Exchange 2003

Viele Unternehmen setzen bereits Exchange als E-Mail-System im Unternehmen ein. Es stellt sich nun die Frage, warum ein Update auf Exchange 2003 sinnvoll sein soll. Im Gegensatz zu Exchange 2000 genießt der Anwender einige Vorteile durch das Update, die jedoch weniger die breite Masse betreffen (OMA, RPC over HTTP usw.). Einige Unternehmen

scheuen den Einsatz von Exchange 2003, da eine Umstellung immer mit Kosten verbunden ist und die Zuverlässigkeit neuer Versionen in Frage gestellt wird. Dabei wird häufig die Einsparung im Betrieb missachtet. „Never touch a running System“ heißt die Devise, die vom Einsatz 2003 abhält. Warum wechseln, wenn bislang alles läuft?

Anhand der neuen und verbesserten Funktionen werden hier nun die zehn wichtigsten Gründe aufgezeigt, die ein Update empfehlenswert machen. Erweitern Sie diese mit Fällen aus der eigenen Praxis, um das Update bzw. den Einsatz von Exchange 2003 in Ihrem Hause zu prüfen bzw. dem Management den Vorteil zu verdeutlichen. Eintretende Fälle können der Verlust wichtiger Nachrichten sowie der Abruf von zeitkritischen Informationen per PDA sein.

Infrastruktur und Betriebszuverlässigkeit

Vorteil für Unternehmen

Nutzen Sie die neue Technologie, die Exchange 2003 bietet, und die Möglichkeit, diese in einem gemischten Umfeld mit Windows NT4, Windows 2000, Exchange 5.5 und Exchange 2000 einzusetzen. Exchange 2003 SP2 kann auf einem Windows 2000 Server mit SP4 oder einem Windows Server 2003 (Empfehlung: SP1) installiert werden. Ein harter Umstieg mit den daraus basierenden Konsequenzen entfällt. Die langsame Migration benötigt weniger IT-Ressourcen und ermöglicht einen Roll-Back.

Die neue Wiederherstellungsstrategie macht das System noch sicherer und zuverlässiger. Bei dem Verlust eines Postfachs oder einzelner Outlook-Objekte können diese innerhalb kürzester Zeit wieder präsent sein, ohne Exchange 2003 selbst zu beeinträchtigen. Langwierige Restore-Prozesse sowie das Suchen nach gelöschten Postfächern entfallen.

Arbeitsproduktivität und mobiler Zugriff

Unterwegs

Einer der entscheidenden Gründe für ein Update ist die Arbeitsweise der Clients. Ein schnellerer Mailzugriff und die optimierte Outlook-Oberfläche erleichtern die Arbeit am PC erheblich. Der Zugriff „*RPC over HTTP*“ ermöglicht Außendienstmitarbeitern und anderen Standorten eine problemlose Serveranbindung. Besonders interessant einzustufen ist die Outlook Web Access Performance, die den Installationsaufwand des Clients in Frage stellt, sowie der Zugriff mit dem Handheld über OMA. Service Pack 2 trumpft mit verbessertem mobilen E-Mail-Zugriff via Direct Push-Technologie auf und bietet abgesehen von mehr mobiler Kontrolle und Sicherheit auch eine optimierte Datenkomprimierung

Support-Unterstützung und Migration

Exchange 5.5 Support

Nicht zu verachten ist dabei die Support-Unterstützung für Exchange 5.5 durch Microsoft, die Ende Dezember 2004 ausgelaufen ist. Das geplante

Ende war für 2003 vorgesehen, die Anzahl der noch eingesetzten alten Versionen hat den Hersteller bewogen, noch ein Jahr „Galgenfrist“ für den Upgrade-Prozess anzuhängen. Gerade 25 % hatten damals erst den Umstieg auf 2000 geschafft. Mittlerweile dürfte die Mehrzahl der Exchange Installationen aktualisiert worden sein. Lassen Sie sich also nicht mehr zu viel Zeit, ein Jahr ist schnell um. Wer den Weg der Migration beschreitet, kann sich über die neuen Assistenten freuen, die den bislang erschwerten Prozess um einiges transparenter und einfacher machen.

Erweiterte Sicherheitseinstellungen

OWA Security

Lange Zeit waren Produkte von Microsoft primär auf das schnelle Erreichen einer Funktion ausgelegt, was zu Abstrichen bei der Sicherheit geführt hat. Sehr viele Dinge sind einfach möglich gewesen, und es wurde den Anwendern und Administratoren überlassen, die Systeme abzusichern, was häufig genug nicht erfolgt ist. Mit Windows Server 2003 werden erstmals viele Dinge nicht mehr installiert und werden auch nach der Installation erst funktionieren, wenn die gewünschten Funktionen frei geschaltet wurden. Exchange 2003 verfügt ebenfalls über einige Änderungen, die das System sicherer machen. Die neue Junk-Mail-Funktion reduziert den Anteil der täglich eingehenden Spam-Mails und schützt somit das E-Mail-System, ausführbare Dateien werden von Outlook blockiert. Der Zugriff über Outlook Web Access unterstützt jetzt S/MIME, und bei Inaktivität wird die OWA-Session automatisch beendet. Die Sicherheit wird durch die neuen Verbindungs- und Empfängerfilter noch ergänzt. Die Service Pack-Installation ermöglicht einen besseren Schutz gegen Spam mittels IMF und Sender-ID.

Kosten

Geringere Kosten

Kosten sind immer wieder ein entscheidender Faktor für den Einsatz von Software oder den Verzicht. Neben den Anschaffungskosten erweisen sich die Betriebskosten eines Systems oft als ausschlaggebend für die Entscheidung. Mit Exchange 2003 können nun aus der Historie gewachsene Standorte optimal konsolidiert werden, da die Performance zwischen Client und Server wesentlich erhöht wurde, das heißt geringere Netzwerklast und weniger Administrationsaufwand, die eine Einsparung von Kosten nach sich zieht. Ein weiterer Faktor ist die verbesserte Replikation auf Basis von Windows 2003. Dadurch werden nur noch die erforderlichen Informationen zu anderen Domänencontrollern übermittelt, die Fehleranfälligkeit zum Beispiel beim Ändern von Gruppenmitgliedschaften auf mehreren Servern entfällt. Für den Enterprise-Bereich stellt die 8-Note-Cluster-Unterstützung einen interessanten Aspekt zum Wechseln dar, dies jedoch abhängig auch von der Hardware.

Es gibt verschiedene Methoden, wie man updaten kann, dies ist von der Vorgängerversion abhängig. Weitere Details dazu erfahren Sie im Kapitel „Migration“.

2.10 Know-how und Weiterbildung

Erforderliche Grundlagen

Wie immer im Leben können Sie Ihre Aufgabe umso besser erledigen, je mehr Sie über das „Wie und Warum“ wissen und Erfahrung gesammelt haben. Unglücklicherweise sind dies Dinge, die nicht einfach kopiert oder vervielfältigt werden können. Daher bedeutet gerade die Einführung von Exchange 2003 und dem dazu erforderlichen Active Directory-System für viele Administratoren ein ganz großer Schritt in unbekanntes Gebiet, begleitet von einer entsprechend langen Lernphase und Zeit der Umgewöhnung.

Für die Konzeption, Installation, Konfiguration und den Betrieb von Exchange 2003 ist es notwendig, neben Exchange auch die Grundlagen im Bereich Active Directory zu kennen. Und für die Planung, Installation und den Betrieb von Active Directory sind neben Kenntnissen in Windows 2003 auch die Grundlagen von TCP/IP und DNS notwendig. Sehr viele Probleme einer Exchange-Installation sind gar nicht bei Exchange zu suchen, sondern im Bereich des Active Directory und der Namensauflösung im Netzwerk.

Dieses Buch soll Ihnen als interessiertem Leser zusätzliche Informationen zum Einsatz von Exchange in Ihrem Unternehmen liefern. Es kann aber weder das Handbuch noch die Erfahrung vieler Installationen ersetzen. Die in diesem Buch gemachten Annahmen und Erläuterungen sind das Ergebnis einer jahrelangen Exchange-Praxis und werden anhand einer Beispielinstallation, die vermutlich die Mehrzahl der Installationen abdeckt, erläutert. Durch das Durcharbeiten dieser Installation soll das Verständnis für Exchange 2003 und die Zusammenhänge wachsen und Ihnen die spätere Installation der Produktionsumgebung erleichtern.

Sie sollten Sich trotzdem weitere Informationsquellen erschließen. Bis auf wenige Ausnahmen sind die nachfolgend genannten kostenfrei. Allerdings ist es nicht für jeden Administrator einfach, sich eine Materie von Anfang an anhand von Texten zu erschließen, dann kommen kostenpflichtige Angebote in Frage.

Exchange 2003-Programm-Hilfe

Programm-Hilfe

Microsoft hat in den vergangenen Jahren sehr viel in der zum Exchange-Programm ausgelieferten Hilfe getan. Im Vergleich zu den Vorgängern sind wir teilweise sehr positiv überrascht, wie gut und ausführlich die Exchange-Hilfe mittlerweile ist. Auch für den Exchange-Experten ist die F1-Hilfe der erste Anlaufpunkt, wenn Fragen zu der einen oder anderen Option auftreten.

Diese „Online-Hilfe“ wurde mit SP2 aktualisiert und enthält zusätzliche Themen, die nicht auf der Programm-CD enthalten sind.

Exchange 2003-Produktdokumentation

Dokumentation

Neben der Exchange-Hilfe enthält jede CD auch die komplette Produktdokumentation. Ausgedruckt ergeben diese Dokumente über viele hundert Seiten eine sehr gut geschriebene und verständliche Zusammenfassung. Viele Fragen in den Newsgroups können wirklich schon mit einem Blick in diese wertvolle Dokumentation beantwortet werden, speziell die Ergänzungen sind sehr zu schätzen.

Exchange-Glossar

Glossar

Seit Januar 2004 gibt es nun auch ein auf Exchange zugeschnittenes Glossar in Englisch. Microsoft erläutert hier alle Exchange-spezifischen Begriffe. Sie können das Glossar als Word-Datei (Technische Referenz) herunterladen.

Exchange 2003 White Papers

Zusätzlich gibt es jede Menge „White Papers“ zu Exchange, die meistens in Englisch gehalten sind. Sie können diese bei Microsoft im Internet herunterladen oder auf der Webseite zum Buch finden. Diese Dokumente gehen teils sehr tief in die Technik ein, und wer immer eine Beschreibung zu einem bestimmten Sachverhalt sucht, findet in den White Papers Antworten.

Microsoft Support-Datenbank

Knowledge Base

Auf der Microsoft-Seite können Sie hier auch eine Wissensdatenbank in deutscher und englischer Sprache in Anspruch nehmen. Hier finden Sie eine erweiterte Hilfe mit Suchmöglichkeiten für jedes Microsoft-Produkt. Die Datenbank wird ständig aktualisiert und gilt für den heutigen Administrator als unverzichtbar.

Abbildung 2.4 Microsoft Support-Datenbank

MOC-Kurse

Seminare

Als Startlehrgang empfehlen sich neben diesem Buch auch die offiziellen Microsoft-Kurse. In diesen Seminaren arbeiten Sie mit speziell vorbereiteten Unterlagen in dafür eingerichteten Schulungsräumen und werden von einem zertifizierten Trainer beim Einstieg in Windows und Exchange unterstützt. Oft ist gerade die geführte Schulung der beste Einstand und erspart Ihnen viel Ärger und Verdruss bei der Installation. Sehr häufig bietet sich hier auch die Gelegenheit, im Gespräch mit anderen Teilnehmern oder dem Trainer die persönliche Situation zu besprechen und weitere Ideen zu erhalten.

Vergessen Sie hierbei aber nicht, dass auch die Grundlagen des Active Directory und TCP/IP als auch die Internet-Anbindung zum Beispiel mittels ISA-Server zur Vorbereitung gehören.

Microsoft TechNet

TechNet

Neben dem Internet und Handbüchern ist *TechNet* das unersetzliche Hilfsmittel jedes Administrators. Dazu zählt nicht nur die Packung CDs, die alle Ressource Kits und Updates enthält, sondern primär die ersten beiden CDs, die die *Microsoft Knowledge Base* und jede Menge aktualisierter Produktdokumentationen enthält. Sie ist unverzichtbar, wenn Sie Produkte von Microsoft einsetzen. Der Umgang mit der TechNet erfordert ein wenig Einarbeitung, um die Suchfunktion richtig einzusetzen. Als Ergebnis finden Sie hier die meisten Fehlermeldungen wieder und erhalten die Informationen, wie diese abzustellen sind. Es ist sinnvoll, auf andere nicht häufig benutzte Informationen zu verzichten und dafür die TechNet zu abonnieren, die letztlich eine große Zeitersparnis bei der Fehlerbehebung mitbringt.

Externe Hilfe

Consulting

Natürlich können Sie auch eine Firma beauftragen, Ihnen bei der Planung, Installation und dem Betrieb behilflich zu sein. Es gibt dabei keine Ober- oder Untergrenze, ab wann externe Dienstleistung sinnvoll ist oder nicht. Bei kleineren Firmen erscheint es nicht sinnvoll, einen Mitarbeiter für die Planung und Installation von Exchange ausbilden zu lassen, damit dieser dann einmalig Exchange installiert. Hier ist die Schulung für den Betrieb wichtiger. Bei größeren Firmen werden externe Mitarbeiter sehr gerne eingesetzt, weil diese aufgrund anderer Einsätze eine entsprechende Erfahrung mitbringen und an vergangenen Fehlern und Problemen Alternativen aufzeigen können. Aber externe Berater können Ihnen nur so weit die Arbeit abnehmen und die Qualität verbessern, wie Sie dies zulassen. Da nur Sie die internen Abläufe in Ihrer Firma am besten kennen, ist eine Mischform häufig die beste Wahl.

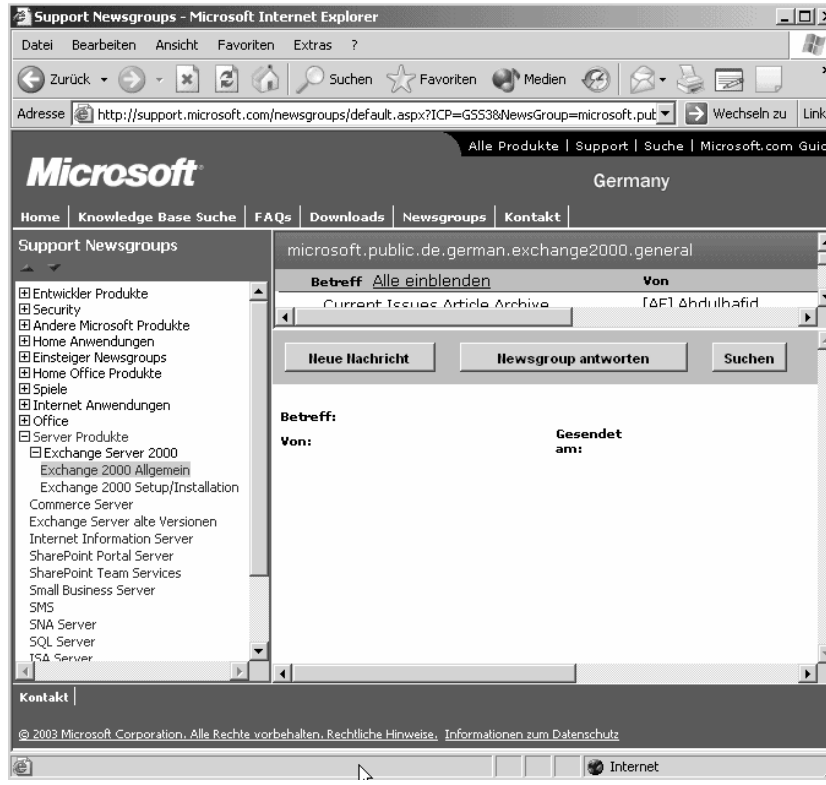
Microsoft Newsgroups

Newsgroups

Neben den kostenfreien Microsoft-Informationen und den kostenpflichtigen Angeboten gibt es einen weiteren Bereich, der nicht verschwiegen werden sollte, das sind die Microsoft Newsgroups.

Schon lange existieren öffentliche Diskussionsforen im Internet, in denen die verschiedensten Themen erörtert werden. So gibt es auch einen News-Server „*msnews.microsoft.com*“ mit Hunderten Foren zu eigentlich allen Produkten aus Seattle. Microsoft bietet auch ein Forum für Exchange an, von der Version 5.x bis 200x in mehreren Sprachen, in denen die Teilnehmer untereinander ihre Probleme und Lösungen austauschen. Über die Suchfunktion von Google in Newsgroups können Sie teils sehr interessante Antworten auch nach Jahren noch nachlesen. Hier diskutieren Praktiker und Administratoren miteinander. Für einige ist daraus ein Hobby geworden, anderen zu helfen und über den Weg ihr Know-how zu zeigen und zu erweitern. Herausragende Personen werden jährlich von Microsoft mit dem MVP-Titel geehrt.

Abbildung 2.5 Deutsche Microsoft-Foren für Exchange



Webseiten

Internet-Seiten

Zudem gibt es eine Fülle von Webseiten in vielen Sprachen, die sich mit Exchange beschäftigen und zusätzliche Artikel, Informationen und Hilfen anbieten. Sehr viele davon sind ebenfalls kostenfrei, teils mit Werbung finanziert oder ebenfalls das Aushängeschild der einen oder anderen Firma, einer Person oder eines Buchautors. An dieser Stelle möchten wir auf Franks eigene Webseite hinweisen, die viele nützliche Informationen enthält und ständig aktualisiert wird. Weitere Links finden Sie im Anhang.

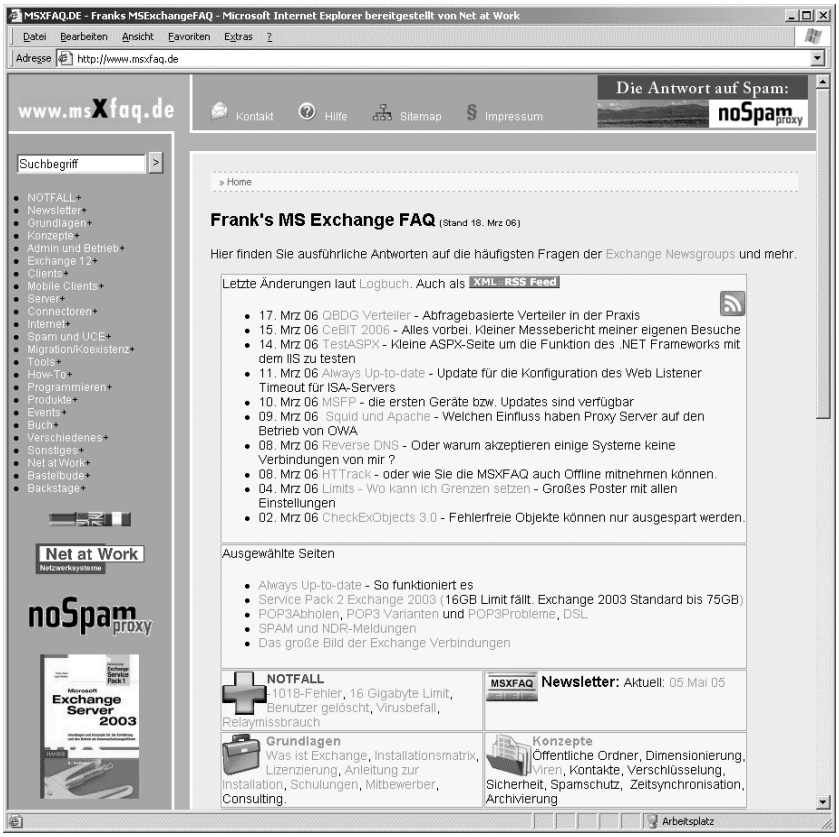


Abbildung 2.6 Microsoft Exchange FAQ-Seite

FAQs

FAQ

Egal, wer Exchange installiert oder einsetzt, es bleibt immer die eine oder andere Frage offen. Sehr häufig sind es die gleichen Fragen, die gestellt und beantwortet werden. So gibt es auch zu Exchange entsprechende „FAQs“ (Frequently asked Questions). Gemeint ist damit eine Auflistung von Fragen und Antworten, die ständig gestellt werden und meist als Textdatei heruntergeladen werden können. Auch diese Quellen sind hilfreich für den Anfang, um die einfachsten Fehler und Probleme zu umgehen.

2.11 Mitbewerber am Markt

Neben Exchange gibt es natürlich andere Produkte, die eine ähnliche Funktionalität aufweisen oder anhand des Namens vermuten lassen. Die Betrachtung einiger Mitbewerber verdeutlicht, wo die Stärken von Exchange liegen und welche Bereiche mit anderen Programmen abgedeckt werden. Jedes Produkt hat seine Daseinsberechtigung am Markt, der Unterschied liegt im Einsatzbereich Ihres Unternehmens.

Zuerst müssen die Funktionen jedes Systems bekannt sein, bevor ein emotionaler Kampf über richtige Mailserver und andere Lösungen ausbricht. Beispielsweise ist der Fokus von Sendmail die Mailserver-Funktionalität, die als Grundlage auch bei Exchange implementiert ist, jedoch erweitert wird zu einer Informationsablage und Drehscheibe im Unternehmen.

Aufgrund der Vielzahl der verschiedenen Systeme ist es sinnvoll, diese zu gruppieren. Im späteren Abschnitt erhalten Sie einen Überblick über die Varianten Groupware-, Internet-Lösungen und andere Systeme, die häufig ein Mix darstellen.

Groupware, Internet und andere Komponenten

MTA

Jedes E-Mail-System muss Nachrichten annehmen und senden können und diese irgendwo zwischenspeichern. Diese Funktion erfüllt heute jedes System und nutzt dabei auch den Standard SMTP. Auch Sendmail und QMAIL zählen hierzu.

Client-Service

Die Anwender müssen nun diese Nachrichten erhalten, um sie zu lesen und mit dem Server zu kommunizieren. Im Internet sind hier Protokolle wir POP3 oder IMAP4 gebräuchlich. Exchange nutzt MAPI/RPC. Sendmail enthält keinen entsprechenden Dienst. Diese Funktion erfüllen andere Programme.

Datenspeicher für Mailboxen

Exchange bietet eine sehr gute Datenbank an, damit alle Nachrichten prinzipiell zentral gespeichert werden. Ohne eine Datenbank im Hintergrund werden die Nachrichten zumeist auf Dateiservern oder lokalen Festplatten gespeichert. Das ist zum Beispiel mit Netscape Mail und vielen anderen POP3-Lösungen der Fall.

Datenspeicher für gemeinsame Daten

Hier ist Exchange mit den Öffentlichen Ordnern und der Stellvertreter-Funktion präsent. Internet-Systeme versuchen dies per NNTP (News) abzubilden oder nutzen andere proprietäre Wege.

Weitere Datentypen

Mails sind nicht alles in einer Unternehmensstruktur, wie wäre es mit Kalenderfunktionen, Aufgaben und Kontakten, die viele tägliche Anforderungen abdecken? Im Grunde sind dies auch nur „Mailelemente“, bei denen der Client die Interpretation der Daten übernimmt. Jedoch hindert die Ablage auf lokalen Festplatten die optimierte gemeinsame Nutzung.

Der Client

Eine ganze Reihe von Mail-Clients für den Arbeitsplatz überflutet den heutigen Markt. Neben Microsoft Outlook und Outlook Express gibt es noch Lotus Notes- und GroupWise-Clients sowie viele mit POP3 und IMAP4 kompatible Programme, die sich stark in Aufbau und Funktionalität unterscheiden. Unverkennbar spielt Outlook in Verbindung mit Exchange seine volle Leistungsfähigkeit sehr gut aus und hat sich damit schon zu einem Standardprogramm für die Kommunikation etabliert.

Sonstige Funktionen

Der Anwender erwartet mehr von seinem E-Mail-System als die reine Grundfunktion. Hier sind Anforderungen wie eine Kalenderabfrage bei Besprechungsplanungen (Frei-/Belegt-Zeiten), Formulare, Regeln und Abwesenheitsassistenten gefragt. So wird der Server aktiv, arbeitet diese Aufgaben ab und stellt einen hohen Nutzwert für den Anwender dar.

Verwaltung

Nicht nur der Anwender möchte die Vorteile eines Systems nutzen, auch dem Administrator obliegt eine leichte Administration durch eine einheitliche Oberfläche. Wichtig ist auch die gute Integration in die bestehende Unternehmensumgebung und der sinnvolle Einsatz des Systems.

Einsatzbereiche

Der IT-Verantwortliche ist hier aufgefordert, die Unterschiede zu kennen und bewusst das richtige Programm für seine spezifischen Anforderungen auszuwählen. Der Einsatz von Exchange als Relay-Server im Provider-Umfeld ist ebenso fraglich wie Sendmail in einer Outlook-Umgebung, die den Bedarf an Regeln, Ansichten sowie formularbasierte Abläufe stellt. Die Auflistung der nachfolgenden Produkte soll keinen Anspruch auf Vollständigkeit und Ausgewogenheit darstellen, sondern der Einschätzung im Hinblick auf Exchange dienen.

2.11.1 Groupware-Systeme

Bei der Vielzahl der Systeme ist es häufig schwierig, den Überblick zu erhalten. Zu den so genannten Groupware-Systemen zählen alle E-Mail-Systeme, die über einen eigenen Client verfügen, der eine sehr leistungsfähige Benutzerführung und Funktionsvielfalt erlaubt. Diese Produkte werden sehr häufig miteinander verglichen, obwohl dies nur beschränkt möglich ist. Die Hauptfunktion bei allen ist der Austausch von Nachrichten, zusätzlich werden weitere Funktionen angeboten.

Exchange

Microsoft

Exchange zählt mit dem Client Outlook mit zu den Groupware-Systemen und hat mittlerweile eine führende Rolle übernommen. Das Programm kommt bei Unternehmen mit fünf bis 500.000 Postfächern in einer Organisation zum Einsatz. Bei Hosting-Providern erhöht sich diese Zahl sogar auf über 1 Mio. Postfächer.

Lotus Notes

IBM

Lotus Notes wird sehr gerne mit Exchange verglichen, obwohl diese beiden Systeme zwar die gleiche Basisfunktion bieten (Mail, Kalender, Aufgaben), aber im Kern komplett unterschiedlich sind. Sowohl die Datenbank als auch die Verbindung von Servern und die komplette Workflow-Funktionalität sind nicht direkt vergleichbar. Jedes Produkt hat seine Stärken, aber ein Vergleich dieser beiden Systeme sollte nur auf Basis eines bestimmten Einsatzzwecks erfolgen.

Sowohl Exchange als auch Notes sind beide sehr leistungsfähige Produkte, die erst durch entsprechende "Anpassungen" ihre wahre Stärke ausspielen können. Ein Exchange-Server mit Outlook ist mit wenig Konfiguration sehr leicht produktiv zu bringen, während der Einsatz von Lotus Notes als E-Mail-System unter den Möglichkeiten bleibt. Der große Unterschied bei den Vorgängerversionen war die Programmierfähigkeit und die daraus in den Köpfen hinterlassene Zuordnung. Während ein Lotus Notes-Server noch vor einigen Jahren erst nach vielen Tagen Entwicklungsleistung als richtig produktiv galt, musste sich Exchange dem Vorwurf stellen, keine geeignete Schnittstelle für die Programmierung bereitzustellen. Das hat sich mit den aktuellen Notes- und Exchange-Versionen relativiert. Exchange 2003 stellt eine gute Plattform für eigene Entwicklungen dar, und die aktuelle Version von Notes ähnelt beim Client vom Prinzip her schon stark Outlook. Eine Stärke von Notes ist die breite Plattformunterstützung, bei der nicht nur Windows, sondern auch Unix, AS400 und andere Server möglich sind. Dies kann ein Vorteil sein, bedingt aber Kompromisse bei der Entwicklung, da die Notes eigene Sprachen genutzt werden muss.

Ein Vergleich beider Systeme ist ohne ein Anforderungsprofil daher nicht seriös möglich. So gibt es Firmen, die wohl wissend über die individuellen Stärken und Schwächen der beiden Produkte zwei Systeme einsetzen. Der Notes Connector von Exchange verbindet beide Welten sehr elegant. Von Microsoft gibt es sogar einen Notes Connector Service für Outlook, damit Sie Outlook auch als Client an einem Notes Server betreiben können. So ist Notes als Serverplattform nutzbar, obwohl auf dem Arbeitsplatz vielleicht lieber mit Outlook gearbeitet wird.

GroupWise

Novell

GroupWise hieß früher WordPerfect Office, ehe Novell das Produkt übernommen und in GroupWise umbenannt hat. Im Laufe der Entwicklung wurde GroupWise mit seinem Client wesentlich leistungsfähiger und unterstützt auch POP3/IMAP4 und SMTP. Heute ist GroupWise ein Messaging-Produkt unter vielen, das mehr Funktionen als eine rein auf Internet-Protokollen basierte Software bietet.

Tobit David

Tobit

Tobit David, gewachsen aus einer Faxserverlösung für NetWare und bis vor einigen Jahren noch sehr Windows-feindlich, versucht vor allem den deutschen Markt der klein- und mittelständischen Unternehmen zu erobern. Mit David wird eine integrierte Lösung für viele Dienste angeboten, die auf eigenständige Add-Ons aufgebaut ist und mit dem eigenen Tobit-Client arbeitet. David integriert von Anfang an neben Nachrichten auch Fax- und Telefonfunktionen auf einem zentralen Server für bis zu 500 Nutzer. Exchange und Notes sind dagegen primär für elektronische Dokumente und deren Einsatz im Unternehmen über viele Standorte hinweg vorgesehen, Fax- und Telefondienste werden über zusätzliche Komponenten ergänzt. Die häufig als David-Vorteil dargestellte Offline-Funktionalität von öffentlichen Informationen wird schon lange von Outlook bereitgestellt, indem Sie einen Ordner als Favoriten ablegen und synchronisieren.

Auch wenn David gerne mit Exchange und Lotus Notes verglichen wird, ist es gesondert zu betrachten. David ist eine ganze Ansammlung von Tools in einer Produktlinie, ein einzelnes Produkt vergleichbar mit anderen Groupware-Systemen hält mit diesen nicht stand.

2.11.2 Internet-Mail-Systeme

Der Vergleich von Groupware-Lösungen mit Internet-Mail-Systemen stellt keine adäquate Basis dar. Grob verallgemeinert bestehen diese Systeme aus einem Mailserver, der SMTP-Nachrichten annimmt und versendet und teils auch per POP3 abholt. Für den Anwender sind diese Server nur per POP3 oder IMAP4 erreichbar, ein Adressbuchzugriff per LDAP ist nur bedingt möglich. Diese Programme gibt es für alle Plattformen, von Windows über Linux bis zu anderen Betriebssystemen. Teilweise wird der Internet-Mail-Service schon auf einem DSL-Router gehandhabt. Die Administration wird häufig als Weboberfläche für den Benutzer ermöglicht. Wichtig ist zu erkennen: Es handelt sich dabei um reine Mailfunktionalität.

Sendmail und QMail

Sendmail, QMail

Die beiden Systeme sind klassische Mailserver und werden sehr häufig eingesetzt, da es sich um kostenfreie Produkte handelt. Die Server bestechen durch eine gute Mailfunktionalität, legen die Nachrichten jedoch in einer offenen Verzeichnisstruktur ab. Um die Nachrichten dort abzuholen, wird ein POP3- oder IMAP4-Service oder -Server wie Exchange benötigt, nur so kann der Anwender die Nachrichten von seinem Mailprogramm aus dem Verzeichnis lesen. Was sich zuerst als kostengünstig erweist, entwickelt sich im Betrieb häufig zu einem unhandlichen System, da meistens die Unix-Kenntnisse fehlen. Auch können diese Programme nicht die Anforderungen der Anwender an serverbasierten Regeln, Formularen, Ansichten, Adressbüchern oder gar gemeinsamen Ordnern abdecken. Hier ist wieder ein Groupware-System gefragt, und im Praxisumfeld sind viele Migrationen von Sendmail zu Exchange zu finden. Eine vielfache Anwendung finden diese Programme in Umgebungen, die große Mengen an Nachrichten umschlagen oder verändern, beispielsweise bei Providern, Universitäten oder auch als Relay zwischen dem Internet und einem Exchange-Server, was also als friedliche Koexistenz zu Exchange betrachtet werden kann.

Webbasierte Systeme

Web-Mail-Systeme

Die Verarbeitung der Nachrichten am Client mit POP3 oder IMAP4 handhabt zwar problemlos die Mails, jedoch werden zusätzliche Erweiterungen mangels Standard nicht unterstützt. Viele Anbieter vermarkten heute eine webunterstützte Umgebung, die mit Outlook vergleichbare Funktionen unterstützt. Der Ansatz hat Charme, da damit die Abhängigkeit von Windows und die Installation zusätzlicher Software auf den Clients entfällt. Ein Browser ist mittlerweile schon fast überall installiert. So ansprechend diese Lösung auf den ersten Blick ist, so scheitert der Anwender doch an den Beschränkungen der Browseroberfläche: Drag & Drop aus anderen Anwendungen ist ebenso wenig nutzbar wie ein einfacher Zugriff aus Dateien zum Anhängen bzw. die Funktion SENDEN AN E-MAIL-EMPFÄNGER. Andere Dienste können nur über Formulare realisiert werden, der Offline-Betrieb ist nicht möglich. Für die Konvertierung von umfangreichen HTMLCodes mit Skripten und Applets ist auch ein leistungsfähiger Arbeitsplatzrechner gefragt, der über die aktuellste Browserversion verfügt. Die für den Heimarbeitsplatz sehr beliebte Variante wird von vielen Providern wie T-Online, HotMail, GMX und WEB.DE angeboten, aber auch Strato und Puretec gewähren einen „Webmail“-Zugriff per Browser auf die Postfächer. Bei den kostenfreien Diensten kann man als Anbieter gleich noch Werbung mit einblenden.

2.11.3 Browserlösungen und Add-Ons

HTTP als Client

Neben den Groupware- und Internet-basierten Lösungen gibt es noch so genannte Zwittersysteme mit dem internen Mailverkehr im Mittelpunkt. Dazu zählen Systeme, die zum Beispiel über eine Weboberfläche per HTTP auf Daten zugreifen, die in SMTP-, POP3- und IMAP4-Systemen gespeichert sind; wie das Programm Infinite WebMail von Captaris. Zumeist sind diese Programme von ambitionierten Entwicklern geschrieben, wodurch ein Support oft entfällt. Neben der Erweiterung bestehender E-Mail-Systeme um ein „Webfrontend“ gibt es auch Systeme, die den HTML-Zugriff als strategischen Client betrachten und somit POP3/IMAP4 nur als Abfallprodukt bzw. Zusatzfunktion nutzen.

Novell/SUSE Openexchange und OpenGroupware

Openexchange, OpenGroupware

Der SUSE Linux Openexchange-Server bietet diese Funktion an. Über einen Webmail-Client wird eine Terminverwaltung, eine zentrale Adressverwaltung, ein Dokumentenmanagement und ein gruppenbasiertes Diskussionsforum ermöglicht, unterstützt durch eine 128-Bit-SSL-Verschlüsselung. Openexchange ist ein Versuch, mit kommerzieller Software im Bereich der Groupware-Lösungen Fuß zu fassen. Um sich mit den Groupware-Lösungen am Markt gleichstellen zu können, müsste diese Lösung noch um Komponenten wie eine Replikation zwischen mehreren Systemen, der Offline-Betrieb und eigene Adressbücher erweitert werden.

Einen ähnlichen Weg, jedoch als echte Open Source, beschreitet das Projekt OpenGroupware, das mit OpenOffice arbeitet und unabhängig von SUN eine Plattform für Groupware auf Unix bietet. Allerdings ist OpenGroupware auf einen Mailserver angewiesen, da es selbst keinen SMTP-Server enthält.

Evolution

Novell/Ximian

Der früher von Ximian entwickelte und nun als Open Source und Novell weiter betreute Client Evolution bietet eine Outlook-Alternative für Linux- und Unix-basierte Systeme. Dabei setzt der Client auf andere Mailserver auf, wie SUSE Linux Openexchange, und ermöglicht eine verbesserte Personalisierbarkeit und Bedienung gegenüber der Vorversion. Interessant ist die Verbindung zu Exchange mittels Connector für Microsoft Exchange, der es Linux-/Unix-basierten Arbeitsstationen mit dem erlaubt, als Client auf Microsoft Exchange-Server per WebDAV zuzugreifen, und per LDAP die globale Adressliste nutzt.

Oracle und andere Datenbanken

Database-Systems

Auch Oracle, bekannt aus dem Datenbankbereich, bietet eine leistungsfähige Lösung auf Basis einer Datenbank an. In der Collaboration Suite können alle

Daten zentral in einer Datenbank abgelegt und Funktionen wie Indizierung, schneller Zugriff und deren Kontrolle genutzt werden. Eine optimale Datensicherung und die Archivierungsoption sind weitere Faktoren.

Übrigens gibt es auch andere kleine Firmen, die für Outlook pfiffige Ideen einbringen. So kann Oaklodge mit einer Software dienen, die für Outlook einen „Storeprovider“ anbietet, damit eine SQL-Datenbank zur Ablage von Dokumenten genutzt werden kann.

Shared PST

Eine ganz andere Variante bieten Produkte, die einfach den Outlook-Client und die PST-Dateien nutzen, um mit Add-Ons eine gemeinsame Nutzung zu erlauben. Besonders für kleine Unternehmen ist es interessant, ein Outlook als Server zu benutzen oder gemeinsame PST-Dateien auf einem Dateiserver zu nutzen. Diese Art von Programmen bietet Quester (*Outlookfolders*) und SDMD (*PublicOutlook*). Die „NetFolders“-Funktion von Microsoft in früheren Outlook-Versionen wurde wegen mangelnder Stabilität und Akzeptanz der Zielgruppe wieder eingestellt.

Nachteilig bei all diesen Lösungen sind Beschränkungen von PST-Dateien (keine transaktionsorientierte Datenbank, 2 GB Größe, keine Online-Sicherung etc.). Für kleine Bürogemeinschaften sind diese Faktoren zumindest anfänglich zu vernachlässigen. Weiterhin fehlt ein zentraler Server, der die Nachrichten annimmt oder abholt und versendet sowie serverbasierte Regeln umsetzt. Aber auch dies ist in Bürogemeinschaften weniger von Belang, wenn die Anwender ihre Nachrichten selbst per POP3 aus dem Internet holen. Fraglich ist da der Schutz der Systeme. Der vermeintliche Kostenvorteil zu einem Server wird durch die Planung, Pflege und Wartung der lokalen Systeme relativiert.

2.11.4 Zusammenfassung

Es gibt im Wesentlichen drei Klassen von Nachrichtensystemen, die zu unterscheiden sind:

GroupWare-Systeme

Darunter fallen Microsoft Exchange, Lotus Notes, Novell GroupWise und Ähnliche, die mit zentralen Datenbanken, leistungsfähigen Clients, Programmierbarkeit und Formularen eine Funktionalität erreichen, die weit über „Mail“ hinausgeht.

Internet-Messaging-Systeme

Sie sind eigentlich nicht mehr als ein Mailserver für SMTP, einen POP3/IMAP4-Server für den Zugriff der Clients und vielleicht einen News-Server für Diskussionen. Zentrale Datenbestände und umfangreiche Funktionen werden durch den Client abgebildet. Standards sind zwar nett, aber zugleich die Grenze jeder leistungsfähigen Weiterentwicklung.

Zwittersysteme

Die mehr sein wollen als ein reines E-Mail-System und aufgrund der Limitierungen von POP3/IMAP4 vieles über Webbrowser oder eigene Transportdienste für bestehende Anwendungen (z.B. Outlook) verbinden, aber doch keine Lösung aus einem Stück wie Notes oder Exchange sein können.

Letztlich macht es keinen Sinn, die verschiedenen Produkte allgemein zu vergleichen, sondern sinnvoll ist nur die Bestimmung der Anforderungen, um einen Kriterienkatalog mit Gewichtung zu erstellen. Prüfen Sie dann, welches System diese Wünsche und Pflichten zu einem akzeptablen Preis erfüllt.

Teil II

Der zweite Teil widmet sich ganz
den Konzepten rund um Exchange 2003.

3

Active Directory

3 Active Directory

Exchange 2003 ist eines der wenigen Produkte, die zwingend auf die Funktion des Active Directory angewiesen sind und das bei Fehlern oder Engpässen des Domänenservices sehr schnell seinen einwandfreien Betrieb einbüßt. Daher ist es erforderlich, ein fehlerfreies, zuverlässiges, skalierbares und leistungsfähiges Active Directory (AD) einzurichten und zu verwalten.

Die vielen hilfreichen Assistenten und die so lieb gewonnenen „Plug and Play"-Funktionen erleichtern die Arbeit mit Exchange. Lassen Sie sich nicht von der Verfügbarkeit der Assistenten verführen, auf eine notwendige Planung eines Servers und den Aufbau eines Basiswissens zu verzichten. Exchange 2003 ist ein Teil der Netzwerkinfrastruktur, auf den Ihr Unternehmen nach kürzester Zeit nicht mehr verzichten kann. Eine falsche Implementierung belastet ganz empfindliche Geschäftsprozesse und führt zu erhöhten Betriebskosten.

In diesem Kapitel werden die wichtigsten Bereiche des Active Directory in Bezug auf die Bedeutung für Exchange ausführlich behandelt. Am Ende des Kapitels sollten Sie nicht nur die Zusammenhänge verstehen, sondern diese auch für die eigene Planung einsetzen.

Dazu gehören:

Wichtige Elemente

- Active Directory (AD)
- Internet
- Sicherheits- und Berechtigungskonzepte
- Datensicherung und Wiederherstellung

Machen Sie sich auch mit den anderen Themen des Active Directory-Systems vertraut, die auch Auswirkungen auf den Exchange-Server mit sich bringen. Diese Bereiche werden in anderen Publikationen detailliert beschrieben wie:

- Active Directory-Replikation
- Gruppenrichtlinien (GPO)
- Inventarisierung, Patch-Management, Softwareverteilung

Folglich sollten Sie über ein Active Directory-Basiswissen verfügen, bevor Sie sich an die Aufgabe Exchange 2003 begeben.

3.1 Basiskonzepte

Verzeichnisdienst

Das *Active Directory System* (ADS) ist ein Verzeichnisdienst, der alle erforderlichen Informationen der Windows-Netzwerkinfrastruktur in einer Daten-

bank ablegt. Der Dienst basiert auf einer Kombination von DNS, X.500-Namenskonvention und LDAP. Er unterstützt somit die Verzeichnisse von Applikationen sowie auch von Netzwerkbetriebssystemen. Für Exchange 2003 bedeutet dies, dass sich nicht nur Benutzer und Computer an diesem Verzeichnis anmelden, sondern dass dieses auch als Datenbank für alle Informationen über Postfächer, Verteiler, Kontakte und Server fungiert. Ein eigenes Verzeichnis wie die Vorgänger Exchange 5.5 und Windows NT 4 (SAM) wird durch das leistungsfähigere Active Directory ersetzt. Bei der Anmeldung verifiziert das System den Benutzer und erteilt anhand von Gruppenmitgliedschaften die Berechtigung zum System.

Hierarchische Strukturen und Sicherheitskonzept

Architektur

Ein Active Directory besteht aus mindestens einer Domäne mit einem oder besser mehreren Domänencontrollern, die einen gültigen DNS-Namen nutzen. Im Gegensatz zu Windows NT4 ist eine hierarchische Anordnung mehrerer Domänen in einem strukturierten Namensraum möglich. Alle Domänen der Struktur sind durch eine beidseitige transitive Vertrauensstellung verbunden. Über den DNS-Namen ist eine klare Zuordnung und einfache Lokalisierung im Netzwerk möglich. Innerhalb von Domänen können mittels organisatorischer Einheiten (OUs) kleinere Einheiten gebildet werden, auf die Rechte für Verwaltungsaufgaben zugeordnet werden können. Die Zusammenfassung einer oder mehrerer Strukturen (Tree) zu einer Gesamtstruktur (Forest) basiert auf einem gemeinsamen Schema.

Access Control Lists (ACL)

Auf Basis von Richtlinien (Policies) und Zugriffslisten (Access Control Lists) werden die Zugriffsrechte für die einzelnen Objekte vergeben. Eine Vererbung der Rechte ist ebenso möglich wie spezifische Rechte auf OU-Ebene. Um auch in weit verzweigten Strukturen schnell allgemeine Informationen auffinden zu können, gibt es gesonderte Globale Katalog-Server, die eine Teilmenge aller Informationen bereitstellen

DNS, WINS und TCP/IP

WINS erforderlich

Durch die Integration des Internet *Domain Name Systems* (DNS), das analog zu der Active Directory-Struktur aufgebaut wird, erfolgt eine effektive Namensauflösung und somit ein schnelles Auffinden aller Objekte im System. Jedoch gibt es einige Funktionen, die weiterhin auf die NetBIOS-Namensauflösung zurückgreifen und WINS benötigen. Dazu zählt die Funktion „Kennwort über OWA ändern“, ExMerge, der ESM sowie das Exchange Setup-Programm. In einer kleinen Umgebung mit nur einem Subnet kann das Broadcast-Verfahren problemlos die NetBIOS-Namensauflösung übernehmen. In großen Umgebungen mit Subnetting sowie in gerouteten Netzwerken benötigen Sie für die NetBIOS-Namensauflösung einen WINS-Server.

Datenbank und Partitionen

AD-Verzeichnis

Die AD-Datenbank ähnelt in Ansätzen der Verzeichnisdatenbank von Exchange 5.5. Die Informationen des Active Directory werden in einer ESE-Datenbank (Extensible Storage Engine) gespeichert. Durch die Transaktionsprotokolle wird die Konsistenz der Informationen sichergestellt. Über eine Sicherung des Systemstatus wird auch das Active Directory mit gesichert.

Die Datenbank selbst gliedert sich in drei Bereich (Partitionen). Die Schemapartition enthält die Definition der Datenbank. Die Konfigurationspartition enthält unter anderem die Verwaltungsinformationen des AD selbst und weitere Konfiguration von Applikationen wie die Exchange-Struktur. Diese Datenbereiche werden auf alle Server im Active Directory Forests repliziert.

Zuletzt gibt es die eigentliche Domänenpartition, in der die Benutzer, Computer und andere Objekte der Domäne gehalten werden. Diese Informationen werden nur auf den Domänencontrollern der gleichen Domäne repliziert und sind somit innerhalb eines Forests unterschiedlich.

Standortsensitiv und globale Kataloge

Active Directory-Standorte

Windows 2000 und höher ist in der Lage, anhand der eigenen IP-Adresse und dem Active Directory den Standort im Netzwerk zu bestimmen und sich dann mit einem netztechnisch nahe liegenden Domänencontroller zu verbinden. Dazu müssen jedoch im Active Directory die entsprechenden TCP/IP-Subnetze gepflegt und den definierten Standorten zugeordnet sein. Auch diese Standort-Technologie ist von Exchange 5.5 übernommen worden, inklusive der Replikation. Somit können alle Systeme ihren „Standort“ ermitteln und einen Domänencontroller vor Ort befragen. Bei Windows NT4 war dies nicht möglich.

Global Catalog Server (GC)

Einen weiteren wichtigen Part übernimmt der Globale Katalog-Server (GC), der von allen Objekten des gesamten Active Directory eine Teilmenge der Attribute vorhält. Im Gegensatz zur Domänenpartition, die nur in der eigenen Domäne bekannt ist, hält der GC einen Teil dieser Informationen über alle Domänen des Active Directory hinweg und kann zügig die am häufigsten gestellten Abfragen beantworten. Für Exchange 2003 ist dies unter anderem für das Routen von Nachrichten von großer Bedeutung, da Exchange über den GC alle Empfänger in allen Domänen der Organisation auflösen kann und muss.

Effektive Replikation

Replikationsservice

Die Partitionen im Active Directory beinhalten wichtige Details, die auf jedem Domänencontroller verfügbar sein und somit repliziert werden müssen. Die Verfügbarkeit auf mehreren Servern erhöht nicht nur die Zugriffsgeschwindigkeit auf Daten, sondern stellt auch eine Redundanz dar und

ergibt eine daraus resultierende höhere Betriebsbereitschaft. Durch die Kenntnis der Standorte können die Domänencontroller effektiv die Informationen untereinander austauschen. Innerhalb eines Standortes erfolgt die Replikation in kurzen Intervallen. Mit Hilfe von Standortverbindungen erfolgt ein kontrollierter Austausch der Daten zwischen Standorten. Während Schema und Konfiguration im gesamten Verzeichnis reproduziert werden, tauscht der Dienst die Domäneninformation nur innerhalb der Domäne aus, darüber hinaus werden die Globalen Katalog-Informationen bereitgestellt. Die Änderungen werden anhand einer USN (Update Sequence Number) erkannt und repliziert. Die sternförmige und objektorientierte Replikation von Benutzern und Computern, von Windows NT4 mit einem beschreibbaren primären Domänencontroller (PDC) und nur lesbaren Backup-Domänencontrollern (BDC) wurde somit durch ein leistungsfähigeres System ersetzt.

Einwirkungen von Exchange

Dies sind nur einige Vorteile, die ein Active Directory insgesamt für Ihr Unternehmen und das Netzwerk mit sich bringt. Für den Einsatz von Exchange 2003 sind im Hinblick auf das Active Directory zwei Dinge für den Administrator wichtig:

- Ablage

  Sie müssen wissen, wo und wie Exchange 2003 Informationen im Active Directory hinterlegt. Dies ist relevant für die Aufstellung der Domänencontroller. Abhängig davon ist auch die Steuerung von Berechtigungen auf einzelne Bereiche und die Abschätzung des Wachstums.

- Nutzung

  Sie sollten überblicken, welche Exchange-Prozesse das Active Directory nutzen und auf welche Weise dies geschieht. Exchange 2003 ist durchaus eine Anwendung, die eine hohe Last für das Active Directory erzeugen kann.

Die Planung steht im Vordergrund.

Da die Rolle des Active Directory für Exchange 2003 und zukünftige Entwicklungen dominiert, ist die Planung das A und O. Sie sollten sich unbedingt mit der Thematik „Verzeichnisdienst“ vertraut machen und sich nicht auf die Assistenten für die Installation und Konfiguration verlassen. Das Active Directory entwickelt sich immer mehr zu einem zentralen Verzeichnis aller Benutzer, Gruppen und Dienste und muss hohen Erwartungen an Verfügbarkeit, Performance und Sicherheit gerecht werden. Eine unbedarfte Vorgehensweise beeinflusst diese Kriterien, und eine Anpassung an geänderte Bedingungen ist, wie eine Stornierung ebenso, häufig nicht möglich.

Halten wir fest:

- Das Active Directory ist nicht nur eine Weiterentwicklung der bisherigen NT4-Domänen, sondern ein komplett neuer Verzeichnisdienst, der im „Mixed Mode“ die Kompatibilität für ältere Systeme bewahrt.
- Die Active Directory-Datenbank unterteilt sich in Partitionen. Die Schema- und die Konfigurationspartition sind dabei auf allen Domänencontrollern repliziert, die hierarchisch zusammengefasst sind (Tree) oder sich über transitive Trusts vertrauen (Forest). Die Domänenpartition wird auf den Domänencontrollern der entsprechenden Domäne vorgehalten.
- Exchange 2003 benötigt zwingend ein Active Directory. Eine Installation ohne Active Directory ist nicht möglich, da ein eigenes Verzeichnis fehlt.
- Der Exchange-Server muss kein Domänencontroller sein. Er kann diese Funktion zusätzlich übernehmen, wenn Performance-, Verfügbarkeits- und Sicherheitsaspekte dies erfordern.
- Die Struktur und Nutzung eines Active Directory muss sorgfältig geplant werden. Änderungen oder eine Aufhebung derselben erfordern eine konzeptionelle Darstellung und Entwicklung.

Die folgenden Abschnitte behandeln einige wesentliche Active Directory-Konzepte und gehen auf die Bedeutung für Exchange ein.

3.2 DNS-Konzeption

Namensauflösung

Die Funktion des Domain Name Service (DNS) ist einer der fundamentalen Faktoren für den Einsatz des Active Directory. Die Anforderung der Zuordnung von IP-Adressen zu Maschinennamen wird schon seit Jahren im Internet erfolgreich mit Hilfe des DNS umgesetzt. Diese Infrastruktur nutzt das Active Directory durch die „Ressource Records“, mit denen die Lokalisierung von Diensten wie. Domänencontroller, Kerberos-Server und Globale Kataloge realisiert wird.

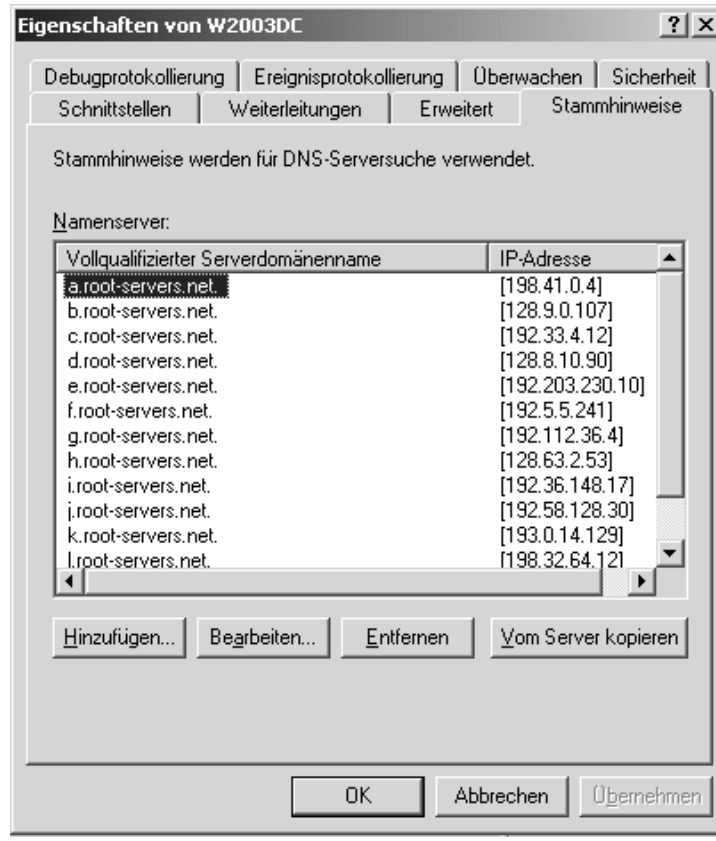
Bei der Planung gilt es, sowohl eine Absicherung gegen Ausfälle als auch eine geschickte Positionierung des DNS-Servers im Netzwerkverbund zu finden. Dazu zählen die Definition der Zonendateien, die Replikation der Informationen und die Pflege der Reverse Zonen. Für eine unkomplizierte Einführung des Windows-Verzeichnisdienstes sollten Sie immer den im AD enthaltenen DNS wählen und wenn erforderlich eine Verbindung zu weiteren DNS-Servern in der internen Umgebung herstellen. Die Auflösung externer Adressen kann z.B. über Forwarder realisiert werden, eine Trennung intern – extern ist gegebenenfalls zu klären.

Root und Knoten

DNS ist ein hierarchisches System, in dessen Datenbank sich jede Maschine mit Hostnamen und den zugehörigen Domänennamen befindet. Im Internet

gibt es eine ganze Vernetzung von DNS-Servern, davon einige Root-Server, die die Wurzel des Namensraums abbilden. Diese Server sind bei jedem DNS-Server hinterlegt.

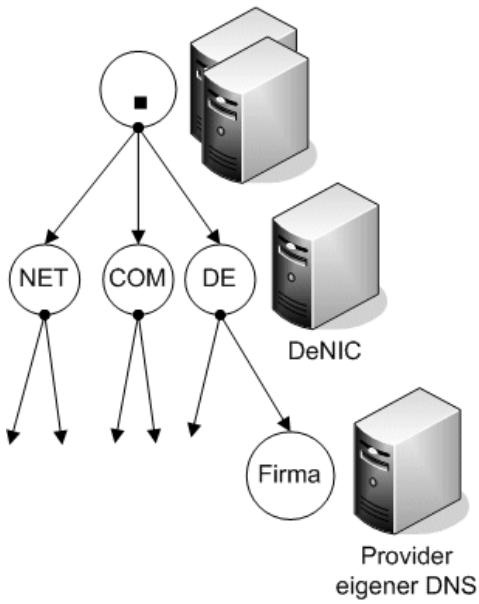
Abbildung 3.1 DNS-Stammserver



Ausgehend von dieser Wurzel oder auch *Top-Level-Domain* gibt es die erste Ebene, beispielsweise COM, NET, ORG, EDU, GOV, MIL, oder aber auch Länderkennzeichen wie DE. Eine weitere Einteilung erfolgt in Knoten, die die Domänen-Verzeichnisstruktur darstellen. Jede dieser Zonen kann von anderen Servern betrieben werden. So wird die „DE-Zone“ bei DeNIC in Karlsruhe gepflegt. Wenn ein Computer einen der Stammserver nach „firma.de“ befragt, dann wird der Server an die Name-Server des DeNIC verwiesen.

Für kleinere Firmen empfiehlt es sich, den DNS-Eintrag der eigenen offiziellen Domäne einem Internet-Provider zu überlassen. Dies vereinfacht die Administration und reduziert Angriffspunkte auf die eigenen Server. Weiterhin erspart diese Trennung meist einen Server für die externe Verbindung, da die internen DNS-Server aus dem Internet nicht erreichbar sein sollten. In der Regel werden diese Einträge nur sehr selten geändert.

Abbildung 3.2
DNS-Struktur



Weitere Informationen zur Funktion von DNS finden Sie in der Windows-Produktdokumentation und den Microsoft White Papers.

3.2.1 Der DNS-Zonenname

Domain-Name

Die Zone verkörpert einen zusammenhängenden Bereich, der von einem DNS-Server verwaltet wird. Alle zugehörigen Informationen werden in einer Zonendatei gespeichert, die auf mehrere Server repliziert werden kann.

Besonderes Augenmerk ist bei der Einrichtung des DNS auf die Wahl des Domänennamens zu legen. Dieser Name repräsentiert später auch den Active Directory-Namensraum. Bei der Wahl des Namens sollten keine Sonderzeichen verwendet werden, und der Name sollte noch nicht im Internet vergeben sein. Eine Expansion des Unternehmens sowie eine stärkere Bindung zum Internet erfordern vorausschauend einen weltweit eindeutigen Namen. Je nach strategischer Ausrichtung des Unternehmens gibt es mehrere Varianten für die Auswahl eines nutzbaren DNS-Namens mit ihren individuellen Vor- und Nachteilen.

Fantasiename, z.B. „firma.intern“

msxfaq.intern?

Um eine Eindeutigkeit sicherzustellen, werden derzeit gerne die Top-Level-Domains „.intern“ und „.local“ definiert. Eine Registrierung von „local“ als Root-Domäne ist unwahrscheinlich. Damit sind Konflikte mit bestehenden Namen im Internet auch in Zukunft unwahrscheinlich.

Interner DNS-Name = externer DNS-Name

msxfaq.de

Der interne Name kann identisch mit dem Namen im Internet sein. Allerdings ist eine Trennung der Zonen zur Sicherheit des internen LAN unbedingt zu beachten. Die externe Zonendatei sollte keine Daten der internen Zone beinhalten. Allerdings müssen Sie manuell dafür Sorge tragen, dass externe Namen auch in der internen Zone mitgeführt werden, damit der Zugriff auf die eigene externe Webseite möglich wird.

Registrierung des internen Namens

msxfaq.com

Eine dritte Option ist die Registrierung des gewünschten internen DNS-Namensraums im Internet. So könnte Ihre offizielle Domäne msxfaq.de heißen, während Sie intern msxfaq.com nutzen und diesen Namen im Internet vorsorglich reserviert haben, aber nicht aktiv nutzen. Damit halten Sie sich alle Wege offen, in Zukunft vielleicht doch die internen Adressen aus dem Internet auflösbar zu machen. Einige größere Organisationen machen hiervon Gebrauch, indem sie die Systeme in einem eigenen Namen installieren und damit flexibel für Veränderungen sind.

Subdomäne des eigenen Namensraums ad.msxfaq.de

ad.msxfaq.de

Fast alle Firmen haben mittlerweile einen offiziellen Domänennamen und möchten vielleicht die Zusatzkosten einer eigenen Domäne oder die Pflege bei gesplittetem DNS einsparen. Der interne DNS-Namensraum könnte als Subdomäne des offiziellen Namens definiert werden. Störend wirkt hier, dass der DNS-Name länger und bei einer späteren Veröffentlichung nach außen eben auch dieser Namen sichtbar wird.

Zielsetzung

Bei der Auswahl eines DNS-Namens ist zu beachten, dass eine spätere Umbenennung einen erheblichen Aufwand bedeutet. Eines der Ziele sollte sein, dass es zu jedem Gerät mit einer IP-Adresse auch einen entsprechenden Eintrag im DNS-Server gibt. Nur so kann eine schnelle Auflösung der Namen und damit eine gute Erreichbarkeit gewährleistet werden. Ein gut gepflegter und aktueller DNS-Server ist eine sehr gute Netzwerkdokumentation und Grundlage für das Active Directory und gleichzeitig auch für Exchange 2003. Die später genutzten E-Mailadressen sind jedoch vollständig unabhängig vom DNS-Namen des Active Directory.

3.2.2 Musterkonzept der DNS-Konfiguration

Die DNS-Implementierung in Unternehmen kennt viele unterschiedliche Modelle, von denen einige sehr oft aus Erfahrung umgesetzt werden. Am

Beispiel eines Unternehmens lassen sich alle wesentlichen Punkte des DNS in einem Active Directory aufzeigen

Annahmen für das Unternehmen:

Praxis-Beispiel

- Es sind ein oder mehrere Domänencontroller als DNS-Server im Einsatz. Diese Annahme ist zulässig, da die Funktion DNS wenig Last verursacht und die Daten bei der Speicherung im Active Directory schon repliziert sind.
- Der interne Name lautet „firma.local“. Damit ist sichergestellt, dass es keinen Konflikt mit externen Adressen gibt und eine Auflösung auf „www.firma.de“ über den externen DNS-Server möglich ist.
- Der Provider betreibt die Domäne „firma.de“ und bietet dem Kunden einen DNS-Server als Forwarder an. Damit kann der Kunde einen DNS-Server des Providers fragen. Dies ist meist schneller und zuverlässiger als der Rückgriff auf die Root-Server.

In solch einer Konstellation könnte die Firma intern zwei Domänencontroller betreiben, die beide den DNS-Dienst für die interne Zone „firma.local“ im AD redundant bereitstellen. Alle Clients und andere interne Server fragen die beiden internen DNS-Server. Die Information über die internen DNS-Server kann statisch oder per DHCP dem Client mitgeteilt werden.

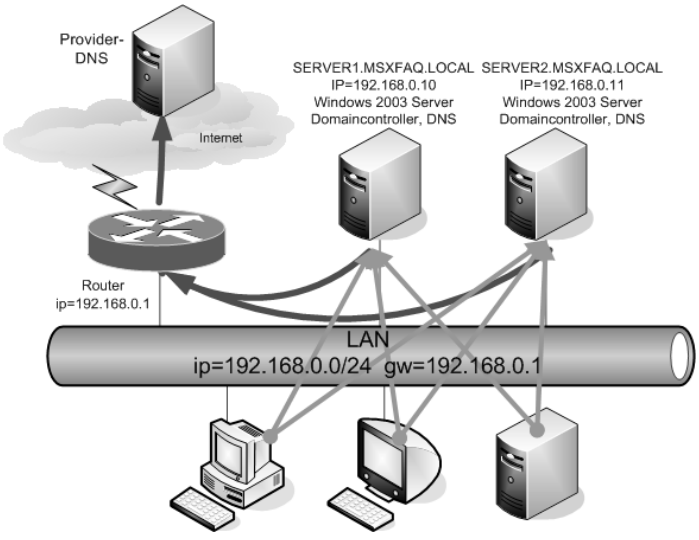


Abbildung 3.3 DNS-Konzept

Um nun auch eine Auflösung der externen Adressen zu ermöglichen, können die beiden DNS-Server einen konfigurierten Forwarder fragen. Der Forwarder, ein explizit definierter DNS-Server, darf Anfragen an andere DNS-Server weiterleiten und gibt die Antwort ins interne Netz zurück. Der Eintrag eines Forwarders bewirkt somit, dass die DNS-Server nicht direkt die externen Root-Server befragen.

Router als DNS-Proxy

DNS-Proxy

In der Abbildung wird der Router befragt. In diesem Fall ist der Router ein DNS-Proxy, der seinerseits den ihm zugewiesenen DNS-Server befragt. Im Gegensatz zum Forwarder reicht der Proxy die Anfrage durch und übernimmt selbst nicht die Aufgabe eines DNS-Servers. Dies ist ein typisches Szenario für Wählverbindungen oder DSL-Verbindungen.

DNS-Server des Providers

NAT

Alternativ dazu können die internen DNS-Server den fest vorgegebenen DNS-Server des Providers befragen. Im internen Netzwerk werden in der Regel private IP-Adressen verwendet, die entsprechend per NAT (Network Address Translation) umgesetzt werden müssen.

Eigener DNS-Forwarder in einer DMZ

DMZ

Die dritte Variante ist die Platzierung eines eigenen DNS-Forwarders in der demilitarisierten Zone (DMZ) der Firewall-Umgebung. Die internen Anfragen werden an den Forwarder geleitet, der wiederum einen DNS-Server im Internet befragt. Dieses Modell eignet sich auch, wenn das Unternehmen selbst den DNS-Server für seine offizielle Domäne betreiben möchte.

Filter und Regeln

Für die reibungslose Kommunikation sind entsprechende Filter und Regeln bei Firewall und Router einzutragen. DNS nutzt zur Abfrage von Namen den Port 53/UDP. Der Transfer von Zonen erfolgt über 53/TCP. Alle Funktionen können und sollten redundant ausgelegt werden. Ihr Provider kann z.B. die Funktion des Secondary DNS-Servers für Ihre Domäne übernehmen. Sie selbst können einen zweiten Forwarder in einer anderen DMZ betreiben.

Bei den vorgestellten Varianten kann der Client alle internen Maschinen sowie auch die Domänen im Internet über den Namen auflösen. Im Zweifel über die Notwendigkeit der externen Namensauflösung hilft nur der aktive Schutz des internen Netzes vor Angreifern aus dem Internet. Im Vergleich mit der Telekom wird ein wirkungsvoller Missbrauch von 0190er Nummern nicht erreicht, indem nur ein kleines Telefonbuch ohne diese Anbieter verteilt wird. Wirksam ist nur die aktive Sperre in der Telefonanlage. Oder anders ausgedrückt:

> Verbergen ist kein Schutz!

Denn im Internet ist das Absuchen ganzer IP-Adressbereiche nach offenen Systemen an der Tagesordnung. Selbst wenn ein System nicht über DNS auflösbar ist, dauert es in der Regel nur wenige Stunden, bis die ersten Verbindungen versucht werden.

3.2.3 Mehrere Domänen und Standorte

Sobald sich das Unternehmen über eine Umgebung mit mehreren Domänen erstreckt oder über Standorte hinweg verteilt ist, muss das DNS-Konzept entsprechend erweitert werden.

Um eine schnelle lokale Namensauflösung im WAN zu ermöglichen, sind DNS-Server vor Ort geeignet, die entweder als Caching-DNS arbeiten und die zentralen Server als Forwarder benutzen oder selbst eine Replikation der Zonendateien erhalten. Dabei ist eine Regel besonders wichtig:

> Es ist immer darauf zu achten, dass im gesamten Active Directory Forest alle verwendeten internen DNS-Zonen aufgelöst werden können.

Sind einige Server nicht zu erreichen, kann nachhaltig die AD-Replikation beeinträchtigt werden und damit auch ein lauffähiges Exchange verhindern. Unabhängig vom DNS-Namen ist die E-Mailadresse des Mitarbeiters. Als gute Praxis bei mittleren und kleinen Firmen hat sich bewährt, dass alle Domänencontroller zuerst den gleichen zentralen DNS-Server fragen und damit die Auflösung und Replikation sicher möglich ist.

3.3 Domänenkonzeption

DNS-Name = AD-Domain

Die Planung des DNS-Namensraums ist bereits der erste Teil der Active Directory-Konzeption. Aufbauend darauf erfolgt der weitere Entwurf der Domänenstruktur für eine strategische Entscheidung. Diese ist vorab mit den betroffenen Personen zu erörtern und bis zur Evaluierung der Konzeptphase im Testfeld nur vorläufig. Die folgenden Informationen sind als Vorbereitung für eine Entscheidung zu sehen und individuell in einer Laborumgebung auf das Unternehmen abzustimmen.

3.3.1 Domänenarchitektur

Mit der Installation des ersten Windows 2003-Domänencontrollers wird bereits die erste Domäne des AD angelegt und das Verzeichnis erstellt. Die Domäne erhält den DNS-Namenskontext und besteht aus vielen Objekten, die organisatorisch gegliedert sind.

Domäne

Die Domäne ist die logische Basiseinheit im Active Directory und besteht aus Objekten (Benutzer, Computer, Gruppen, Netzwerkdienste, Regeln und weitere) sowie einem oder mehreren Domänencontrollern. Sie ist gleichzeitig Verwaltungseinheit und Grenze für Sicherheitsrichtlinien. Die Aufgaben der DC können über so genannte FSMO-Rollen (Flexible Single Master Opera-

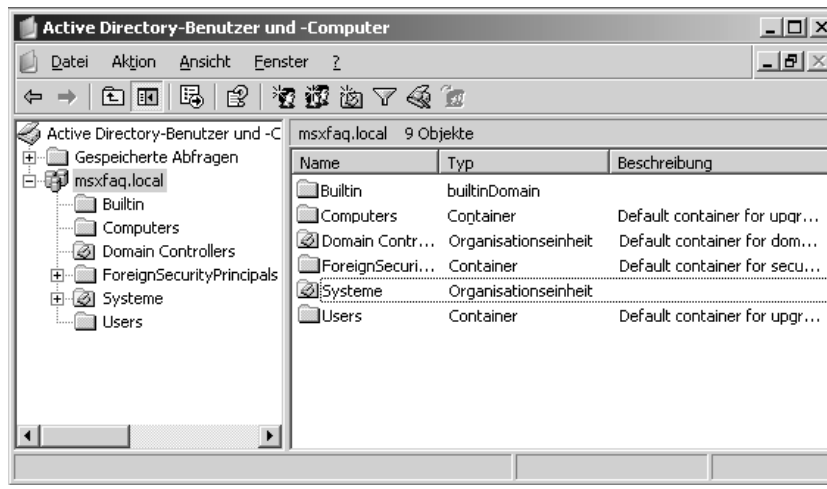
tion) gesteuert werden. Das Verzeichnis repliziert sich komplett auf alle Domänencontroller innerhalb der gleichen Domäne.

Abbildung 3.4 Benutzer, Gruppen und andere Domänen-Objekte

Organisationseinheiten

Innerhalb einer Domäne können Organizational Units (OUs) angelegt werden, die die hierarchische Strukturierung der Benutzer, Gruppen und Computer in Organisationseinheiten abbilden und auch als Ebene für die Delegierung von Zugriffsrechten fungieren.

Abbildung 3.5 Standard-OUs



Domänenstruktur

Tree

Mehrere Domänen, die einen fortlaufenden DNS-Namenskontext bilden, können zu einer hierarchischen Einheit, einem Tree, zusammengeschlossen werden. Dies ist häufig bei Unternehmen zu finden, deren Organisation geografisch verteilt ist oder die aus vielen eigenständigen Unternehmen mit dezentraler Administration bestehen. Innerhalb des Trees vertrauen sich die Domänen über two-way-transitive Trusts, dass heißt, die Vertrauensstellung wird durch die ganze Tree-Struktur von der ersten bis zur letzten Domäne

durchgegeben und ermöglicht, alle Netzwerkressourcen zu sehen. Die Domänen nutzen ein gemeinsames Schema.

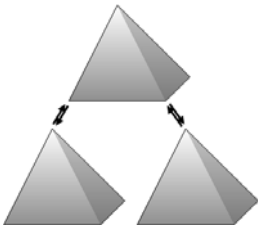


Abbildung 3.6 Mehrere Domänen

Gesamtstruktur

Forest

Im Gegensatz zu Domäne und Tree wird beim Zusammenschluss mehrerer Trees zu einem Forest kein kontinuierlicher Namensraum verwendet. Alle Domänen nutzen ein gemeinsames Schema und sind über beidseitige Vertrauensstellung miteinander verbunden. Einziger grober Unterschied sind die verschiedenen Namenskontexte der einzelnen Trees.

3.3.2 Ziele bei der Planung von Domänen

Das Active Directory besteht also aus Domänen, die in hierarchischen Strukturen zu Gesamtstrukturen (Trees) organisiert werden. Mehrere Trees bilden eine Gesamtdomänenstruktur (Forest). Welche Entscheidungskriterien gibt es, um ein passendes Modell der Domänenanordnung festzulegen?

Kriterien

- Administrative Belange

  Gerade die Berechtigungsstruktur innerhalb einer Verwaltungseinheit in Form der Domäne wirft die Frage auf, wer Rechte erhält und wie weit der Arm des Domänen-Administrators reichen darf. Hier spielt auch die Wechselaktivität der Benutzer zwischen Firmenteilen eine wichtige Rolle.

- Netzwerkbelange

  Der Austausch der AD-Verzeichnisinformationen in Verbindung mit der Netzwerkinfrastruktur erfordert eine genaue Planung, um den Replikationsverkehr zu optimieren und trotzdem eine schnelle Aktualisierung der lokalen Daten zu erreichen.

- Kostenaspekt

  Nicht unwesentlich ist die Anzahl der benötigten Server-Hardware, Lizenzen sowie auch der Umfang der Folgekosten für Wartung und Pflege. Je nach Wahl eines Modells ist eine gewisse Anzahl an Servern für eine redundante Windows 2003-Infrastruktur vorzusehen. Zusätzliche Domänen bedeuten weitere Domänencontroller.

- Gruppenrichtlinien

  Mit Hilfe der Gruppenrichtlinien (GPO) erhalten die Benutzer und Computer Sicherheits- und Konfigurationseinstellungen zentral zugewiesen. Wie können diese Funktionen effektiv eingesetzt werden unter Berücksichtigung der Domäne als Grenze für Sicherheitsrichtlinien?

- Migration und Koexistenz

  Bei einer bestehenden Windows NT-Domäne sind die Voraussetzungen für eine Migration zu beachten. Neben Update oder Übernahme der SID-History in eine neue Umgebung mit NT-Vertrauensstellung ist auch ein kompletter Neuaufbau zu überlegen. Nicht nur die Migrationsszenarien, sondern auch die Vor- und Nachteile sollten genau abgewägt werden.

- Dienste und Rechte

  Bei der Übernahme von bestehenden Programmen sollten Sie die zu erwartenden Ausfallzeiten prüfen und abschätzen können, inwieweit diese toleriert werden können.

Redundanz

Jede Domäne besteht aus mindestens einem Domänencontroller. Um eine Ausfallsicherheit zu gewährleisten, sollten jedoch zwei oder mehr Domänencontroller vorgesehen werden. Ist eine Domäne über mehrere Standorte verteilt, dann ist es eventuell sinnvoll, auch in den Standorten Domänencontroller vorzuhalten.

Administration

Domänen dienen zur administrativen Gliederung der Zuständigkeiten, da eine Domäne standardmäßig die Grenze einer Administration ist. Innerhalb einer Domäne können über Organisationseinheiten weitere Gliederungen vorgenommen werden. Modelle mit wenigen Domänen sind vorzuziehen, wenn dies die Netzwerkstrukturen und die personelle Besetzung zulassen.

Kosten

Verzeichnisdienste sind ein Schlüsselfaktor beim Einsatz eines Netzwerkes, da die geschickte Installation und Konfiguration ein hohes Potenzial für Einsparungen und effektive Nutzbarkeit bieten. Das Ziel ist die Vereinfachung der Administration durch eine zentrale Pflege der Benutzer. Auch die Nutzung des Verzeichnisdienstes durch mehrere Dienste wie z.B. für Datei- und Druckerzugriffe, E-Mail-Konfiguration, Radius-/VPN-Authentifizierung, Intranet- und Proxy-Autorisierung sowie Applikations-integration (SAP und andere) bedeutet ein Einsparungspotenzial.

3.3.3 Domänenmodelle

Anhand der folgenden exemplarischen Modelle können Sie sich eine Vorstellung über den möglichen Aufbau Ihrer Domäne(n) machen.

Single Domain-Modell

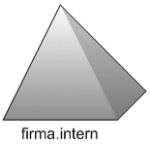


Abbildung 3.7 Single Domain-Modell

Eine einzige Domäne erstreckt sich über alle Standorte und enthält sowohl Computer, Benutzer, Gruppen sowie alle anderen Objekte. Dies erfordert administrativ eine genau strukturierte Unterteilung in Organisationseinheiten. Die Gruppe der Administratoren mit den meisten Rechten sollte nur wenige ausgewählte Mitglieder enthalten. Alle weiteren Verwaltungsaufgaben sollten über die OUs delegiert werden.

Forest-Root-Domäne

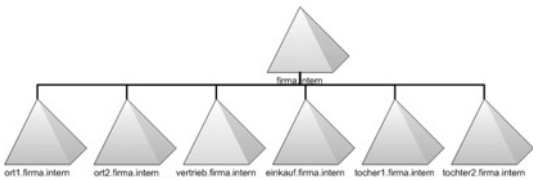


Abbildung 3.8 Root-Domänen-Modell

Eine besondere Domäne, die Root, ist allen anderen Domänen vorangestellt und gilt als Ausgangspunkt für den DNS-Namensraum. Hier sind wichtige Berechtigungsgruppen und FSMO-Rollen beherbergt, die für den ganzen Forest gelten. Alle anderen Domänen und Trees agieren sichtbar als Teilbaum und sind für die Verwaltung von Benutzern, Computern und anderen Objekten zuständig. Durch die gezwungene Struktur können zentrale Ressourcen anhand der DNS-Suchreihenfolge schnell und einfach gefunden werden.

Forest mit gleichberechtigten Domänen

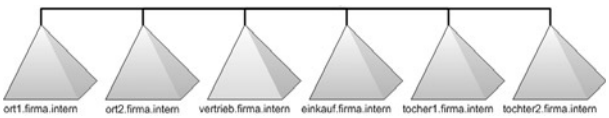


Abbildung 3.9 Gleichberechtigte Domänen

Hierbei steht die erste Domäne „neben“ allen anderen Domänen auf gleicher Ebene. Jede Firma hat damit die Möglichkeit, einen komplett eigenen DNS-Raum aufzubauen. Allerdings ist die Namensauflösung etwas aufwändiger zu konfigurieren.

Multi-Forest

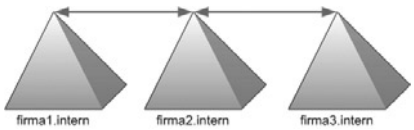


Abbildung 3.10 Multi-Forest-Modell

Exchange als Resource Forest?

Eine Sonderform stellt die Verbindung mehrerer Forests über Trust dar. Die Vertrauensstellungen sind nicht transitiv, und jeder Forest hält ein eigenständiges Schema und eigenständige Gruppen der Organisationsadministratoren und Schema-Administratoren. Solche Multi-Forest-Umgebungen finden sich oft in großen Konzernen, die aus vielen eigenständigen Unternehmen zusammengesetzt sind. Oftmals wird ein gesonderter Forest als Ressourcen-Forest für in Active Directory integrierte Programme wie Exchange 2003 genutzt, um eine gemeinsame Messaging-Plattform zu nutzen und die Eigenständigkeit der eigenen Netzwerkumgebung zu wahren. Vor dem Einsatz dieses Modells ist der Verwendungszweck des Ressource-Forests zu prüfen und dessen Platzierung zu definieren. Möglicherweise ist eine Verteilung der Domänencontroller an weiteren geograpfischen Standorten einzuplanen.

3.3.4 Exchange 2003 und Domänen

Exchange ist Forest-übergreifend

Der Fokus von Exchange liegt auf dem kompletten Active Directory, also dem Forest oder Tree. Somit ist das Domänenmodell nur indirekt für Exchange 2003 von Belang. In allen Domänen innerhalb des Forests kann ein Exchange-Server installiert werden, die E-Mail-Benutzer können in allen Domänen, ob mit oder ohne Exchange-Server, angelegt werden. Die Grenzen von Exchange werden an Administrativen Gruppen und Routinggruppen festgemacht.

Die Installation des Exchange-Servers erfolgt in getrennten Administrativen Gruppen, ist jedoch durch den Windows-Server an die Berechtigungen des (Domänen-)Administrators gebunden. Diese sind erforderlich für das Stoppen und Starten der Exchange-Dienste, die Sicherung des Servers, Installation von Updates und einige andere Verwaltungsaufgaben. Daher ist genau zu prüfen, ob eine Konzentration aller Exchange-Server in einer Domäne von Vorteil ist, um keinen anderen Domänenadministratoren Zugriffsrechte zu geben. Alternativ ist auch die Verteilung ein Mittel, Zugriffsrechte zu beschneiden unter Einrichtung mehrerer Administrativer Gruppen als Exchange-Autorität.

Trotz der scheinbaren Autonomie von Exchange muss das Active Directory jedoch für die Installation und den Betrieb des Mailservers entsprechend vorbereitet werden.

Wir halten fest:

- Exchange ist unabhängig von der Struktur des Active Directory-Forest. Die E-Mail-Objekte wie Benutzer und Verteiler müssen nicht in der gleichen Domäne wie die Postfachserver angelegt werden.
- Die SMTP-Adressen der Mailempfänger sind unabhängig vom AD-Namensraum und den einzelnen Domänen.

- Der Forest muss nur einmalig eine Schemaerweiterung erlangen und erhält dadurch das Umfeld für eine Exchange-Organisation (Forestprep).
- Alle Domänen, deren Objekte Exchange 2003-Eigenschaften annehmen sollen, müssen dafür vorbereitet sein (Domainprep) und später mit einem Empfängeraktualisierungsdienst versehen werden.

3.4 Das Konzept der Organizational Units

Neben der Entscheidung über die Domänen und deren Platzierung ist auch die Planung der Organisationseinheiten (OU) entscheidend für die Nutzbarkeit des Active Directory.

Organizational Unit (OU)

Innerhalb der Domäne sind Organisationseinheiten ein Mittel, die Objekte logisch zu gruppieren, auf dieser Ebene Rechte zu vergeben oder Einstellungen (Gruppenrichtlinien) darauf anzuwenden. Sie stellen jedoch keine Sicherheitsgruppe dar und können nicht dazu genutzt werden, den Objekten Rechte (z.B. auf Freigaben) zu erteilen. Die OU dient als Verwaltungsebene für Benutzer, um die Administration der darin enthaltenen Objekte zu delegieren. Ein Objekt kann immer nur in einer OU sein, diese kann in einer weiteren OU verschachtelt werden.

Aufgaben der OU

Es hat sich gezeigt, dass OU-Strukturen über mehr als drei Ebenen nicht sinnvoll administriert werden können. Folgende Entscheidungshilfsmittel sind wichtig.

- Die Standard-OUs und Systemcontainer

  System-Defaults

  Das Active Directory stellt bereits vordefinierte OUs und Systemcontainer mit Objekten zur Verfügung. Der Systemcontainer *Users* ist der Vorgabecontainer für alle weiteren Benutzerkonten und Gruppen. Es empfiehlt sich jedoch, diese in eigene OUs zu verschieben bzw. dort anzulegen. In der OU *Domain Controllers* sind alle DCs der Domäne fest verankert; die restlichen PCs landen per Default in den Container *Computers* und können in andere OUs verteilt werden. Weitere Systemcontainer (wie *Lost and Found*, *Exchange System Objects* etc.) erkennen Sie im „Active Directory-Benutzer und -Computer“ an einem Ordner ohne OU-Symbol.

- OUs zur Delegation administrativer Rechte

  Administration

  In eigene Organisationseinheiten können die Benutzer einer Abteilung zusammengefasst werden. Einem ausgewählten Benutzer werden dann spezifische Rechte auf dieser Ebene übertragen, um zum Beispiel Kennwörter zurückzusetzen. Die Rechte gelten dann für alle Objekte innerhalb der OU, und die Vergabe ist nicht an Sicherheitsgruppen gebunden. Dass heißt, die Rechte auf OU-Ebene müssen über den Menüpunkt

OBJEKTVERWALTUNG ZUWEISEN explizit übertragen werden, sofern sie nicht über die Vererbung durchgereicht werden.

GPO

- OUs für Gruppenrichtlinien

  OUs sind für die Zuweisung von Gruppenrichtlinien (GPO) relevant. Alle Objekte in der Verwaltungseinheit erhalten die entsprechenden Rechte und Einstellungen wie den Zugriff auf Systemdateien und die Ansicht des Arbeitsplatzes. Die Richtlinien werden mit einer oder mehreren OUs verbunden und auf alle Objekte des Containers angewandt. Dabei ist eine Addierung über die Struktur sowie von verschiedenen Objekten (Benutzer und Computer) möglich. Spätere Änderungen des OU-Konzepts innerhalb einer Domäne sind technisch problemlos, aber die Auswirkungen auf Rechte und Gruppenrichtlinien aufgrund der Vererbung der Regeln nicht immer einfach abzuschätzen.

- OUs als geografische Gliederung

  In der Regel eignet sich das OU-Konzept weniger für die Abbildung geografischer Strukturen, es sei denn, dies entspricht zugleich der administrativen Struktur. Gruppenrichtlinien können auf Standorte gebunden werden, um echte ortsabhängige Einstellungen zu erreichen.

Geltungsbereich

- OUs sind nur „pro Domäne“

  Die Organisationseinheit kann immer nur Elemente aus der Domäne enthalten, in der sie angelegt wird. Ebenso kann ein Objekt immer nur Mitglied genau einer OU sein. Ist z.B. eine OU „Einkauf“ in mehreren Domänen erforderlich, dann muss diese in jeder Domäne angelegt werden. Eine übergreifende Gruppierung ist nur über Sicherheitsgruppen möglich.

Letztlich wird es eine Diskussion über die Strukturierung und Definition von OUs und Domänen geben, die im Testfeld umzusetzen und zu prüfen sind. Denkbar sind Aufteilungen nach Abteilung und dann optional in Teams. Ebenso ist aber auch eine Aufteilung nach Administratoren oder Standorten möglich. Die Entscheidung ist sehr vom Einsatzzweck abhängig, so dass eine Konzeption im Vorfeld wichtig ist. In der nachfolgenden Abbildung finden Sie ein Beispiel für die OU-Struktur in „msxfaq.local“.

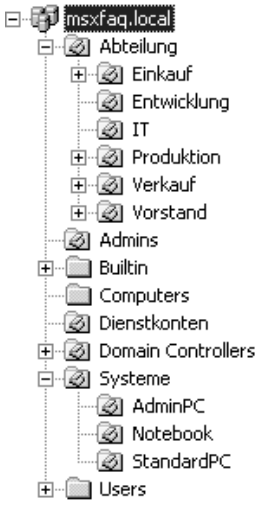


Abbildung 3.11 OU-Struktur „msxfaq.local“

Die *Organizational Units* werden vom Anwender kaum wahrgenommen. Sie stellen eine Gliederungshilfe für die Delegierung von administrativen Rechten auf Objekte in der Domäne dar und treten als Knotenpunkt für die Zuweisung von Gruppenrichtlinien auf. Sie sind kein Ersatz für Sicherheitsgruppen, sondern komplett unabhängig zu betrachten.

Exchange und OU

Wichtig für den Einsatz von Exchange ist die Betrachtung der OU als Verwaltungsknoten. Hier werden die Rechte für die Einrichtung von Postfächern und weiteren Exchange-Aufgaben vergeben. Mindestvoraussetzung dazu ist die Funktion als „Exchange-Administrator – nur Ansicht“. Die OU selbst kann nicht als Verteilerliste konfiguriert werden, für diese Aufgabe ist eine weitere Gruppe erforderlich.

Eine ausführlichere Behandlung der Active Directory-Thematik finden Sie auch in der Buchreihe zu Windows 2000/2003 und XP des Carl Hanser Verlages.

3.5 Benutzerobjekte

Für Exchange 2003 spielen die Benutzerobjekte des Active Directory eine besondere Rolle. Während die Informationen über ein Postfach in Exchange 5.5 in einer eigenen Datenbank hinterlegt waren, an dem nur das dazugehörige Windows-Konto gespeichert wurde, ist die Sichtweise in Exchange 2003 umgekehrt: Der Benutzer ist primär ein Active Directory-Objekt, bei dem auch zusätzlich Exchange-Eigenschaften abgelegt werden können.

Während Exchange 5.5 nur Postfächer enthalten hat, sind im Active Directory auch andere Benutzerobjekte gespeichert, die keine Bedeutung für Exchange haben. So kommen die Computerkonten ebenso wenig für ein

Postfach in Frage wie spezielle Dienstkonten. Es macht Sinn, neben den normalen Anwendern und Gruppen auch Funktionen und Dienste in dafür definierte OUs strukturiert abzulegen. Sie sollten all diese Benutzer auflisten und zur Benennung einem Namenskonzept folgen. Beachten Sie auch die nachfolgende Gruppierung.

Tabelle 3.1 Active Directory-Benutzer-Objekte

Objekte	Beschreibung des Objekts
Normale Benutzer	Der normale Benutzer im Netzwerk erhält ein Konto zur Anmeldung. Zwecks Sortierung und leichter Auffindung ist eine Gliederung nach Abteilungen wünschenswert. Dazu zählen auch Praktikanten und Auszubildende. Auf der Ebene der Domäne wird eine OU „Abteilung“ eingerichtet, in der alle Benutzer gesammelt werden. OU: ou=%abteilung% (ou=Einkauf.msxfaq.local) Name: %Benutzername% (%Nachname7%%Vorname1%)
Praktikanten und Auszubildende	Diese Benutzer werden wie normale Benutzer behandelt und in der gleichen OU angelegt, sind jedoch nicht Mitglied der Abteilungsgruppe. Es sollte eine eigene Gruppe für die Zuweisung der Rechte für diese Praktikanten in der jeweiligen Abteilung geben. OU: ou= ou=%abteilung% (ou=Einkauf.msxfaq.local) Name: %Benutzername% (%Nachname7%%Vorname1%)
Administrative Benutzer	Für die Verwaltung des AD werden eigene Benutzerkonten angelegt. Für administrative Tätigkeiten ist daher eine eigene Anmeldung (run as, Terminal-Dienste etc.) notwendig. Für diese Konten sollten nur ausgewählte Administratoren das Verwaltungsrecht haben. Eine besondere Richtlinie sichert diese Benutzer (strengere Bildschirmschoner, Password-/Lockout-Einstellungen etc). Auf der Ebene der Domäne wird eine OU „Admin“ eingerichtet, in der alle Konten mit Administrationsaufgaben angelegt werden sollten. OU: ou=AdminUser (ou=Admins.msxfaq.local) Name: ADM-%Benutzername% (ADM-%Nachname%)
Dienstkonten	Dienstkonten sind Zugänge für Netzwerkdienste wie SQL-Server, Exchange, IIS, Datensicherung, Batch-Prozesse etc. Diese sollten nicht als „Administrator“ laufen, sondern jeder Dienst erhält ein eigenes Benutzerkonto. Auf der Ebene der Domäne wird eine OU „Dienstkonten“ eingerichtet, in der alle Benutzer für die Dienste abgelegt werden. OU: ou=Dienstkonten (ou=Dienstkonten.msxfaq.local) Name: SVC-%NAME% (SVC-Exchange)

Objekte	Beschreibung des Objekts
Externe Benutzer	Durch die Anbindung an Zulieferer und Kunden ist es oft notwendig, fremden Anwendern auf interne Ressourcen Zugriff zu gewähren. Sie sind daher nicht Bestandteil der normalen Abteilungsstruktur, aber auch keine administrativen Konten. In der Regel ist man versucht, diese Konten zu vermeiden und mit Trusts die Domänen zu verbinden. OU: ou=Extern,ou=Abteilung (extern.einkauf.msxfaq.local) Name: EXT-%NAME% (EXT-%Nachname%)
Deaktivierte Benutzer	Ein Konto, das nicht mehr benötigt wird, löschen Sie in der Regel. Allerdings ist dies nicht immer erwünscht, da die SID gelöscht und damit verbundene Rechte, Profile, verschlüsselte Dateien nicht mehr nutzbar sind. Viele Unternehmen entscheiden sich diese Benutzer erst zu deaktivieren und das harte Löschen nach einer Karenzzeit auszuführen. Es bietet sich an, diese Benutzer in einer speziellen OU abzulegen, damit z.B. über Gruppenrichtlinien eine Anmeldung verhindert oder darüber informiert (Logon-Script) wird. OU: ou=deaktiviert (ou=deaktiviert.Verkauf,msxfaq.local) Name: #-%NAME% (#-%Nachname%)
Kontakte	Kontakte sind Benutzerkonten ohne SID und damit ohne Berechtigung. Sie dienen primär dazu, Adressinformationen und E-Mail-Adressen im Verzeichnis zu speichern. OU: ou=extern,ou=Abteilung,domain.de Name:%Kontaktname%

Sonderfall deaktivierte Benutzer

Im Regelfall handelt es sich dabei um Benutzerkonten, die zum Löschen angewiesen sind. Jedoch kommt es häufig vor, dass noch einige Informationen benötigt werden oder noch vorhandene Daten geprüft werden sollen. Viele Unternehmen deaktivieren diese Benutzer erst und löschen sie, wenn keine Informationen mehr benötigt werden. Durch das Deaktivieren ist zwar das Konto mit den Rechten noch vorhanden, der Benutzer hat jedoch keine Möglichkeit mehr, sich anzumelden und Ressourcen zu nutzen.

Hidden User

Die erste Ausnahme sind Benutzer, die für eine absehbare Zeit dem Unternehmen nicht zur Verfügung stehen und deaktiviert werden – sei es aufgrund Krankheit, Mutterschaft oder Wehr-/Zivildienst. Nachrichten, die weiterhin an dieses Postfach zugestellt werden, sollen von Kollegen abgerufen oder an diese weitergeleitet werden. Das Mailsystem ist nur dann in der Lage, eine Nachricht zuzustellen, wenn eine gültige SID hinter der E-Mail-Adresse steht. Beim Deaktivieren eines Benutzers verliert dieser aus Exchange-Sicht seine SID. Exchange bietet nun einen Workaround, um weiterhin Nachrichten zu empfangen. Dabei wird dem Systemeintrag „*SELBST*“ die Funktion des externen Kontos zugeordnet.

Single Login

Eine weitere Handhabung für „disabled User“ ist die Verwendung eines Windows-Benutzers in einem Ressourcen-Forest. Eine der Anforderungen in einer Multi-Forest-Umgebung ist auch die Nutzung aller Ressourcen mit nur einem Anmeldekonto. Um dieses „Single Login“ umsetzen zu können, muss in den Exchange-Eigenschaften der Besitzer die erforderlichen Postfachberechtigungen erhalten und zusätzlich die Aufnahme als ZUGEORDNETES EXTERNES KONTO sowie das Sicherheitsrecht SENDEN ALS.

3.5.1 Benutzer

Neben der logischen Gruppierung von Benutzern in ihre Funktion gibt es beim Einsatz des Active Directory auch eine technische Unterscheidung der Personen. Benutzer können als Kontakte oder als User angelegt werden.

- Benutzer

  Für jeden Anwender, der sich an einem System anmelden und die im zugewiesenen Rechte ausüben möchte, muss ein Konto angelegt werden. Dies ist der klassische User im Active Directory, welcher neben einem Namen und einem Kennwort auch eine SID (Security Identifier) hat. Diese eindeutige Nummer ist der Schlüssel, der den Zugriff auf bestimmte Ressourcen freischaltet. Nur Benutzer können später auch ein Exchange-Postfach bekommen.

- Kontakte

  Kontakte sind Objekte im Active Directory ohne SID und können demnach auch weder zur Anmeldung noch zur Vergabe von Berechtigungen genutzt werden. Kontakte dienen lediglich dazu, die Daten von Personen im Active Directory zu speichern, die keine Anmeldung benötigen. Sie können kein Exchange-Postfach bekommen, jedoch eine E-Mail-Adresse, und sind somit per Mail erreichbar.

- Lokale Benutzer

  Eine Sonderform sind lokale Benutzer, die nicht im Active Directory hinterlegt sind, sondern in der lokalen Datenbank des jeweiligen Mitgliedsservers. Diese Benutzer werden oft für Dienste eingesetzt, die keine domänenweiten Berechtigungen benötigen. Für Exchange sind diese Anwender nicht verwendbar.

Für den Einsatz mit Exchange sind nur die Benutzer und Kontakte im Active Directory nutzbar.

3.5.2 Benutzer, E-Mail-Adresse und Exchange

Beim Anlegen eines Benutzerkontos im Active Directory können Sie neben dem Vornamen, Nachnamen und den Adressdaten auch eine E-Mail-Adresse eintragen. Diese ist zunächst nicht für Exchange 2003 relevant.

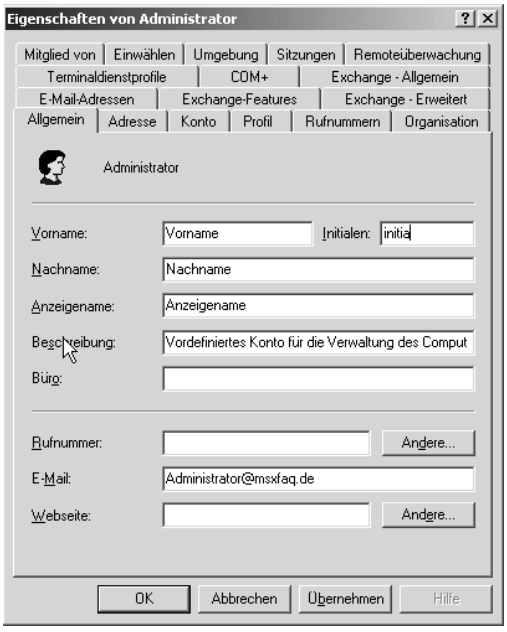


Abbildung 3.12 Benutzer einer E-Mail-Adresse

Der Eintrag einer E-Mail-Adresse bei einem Benutzer legt noch kein Exchange-Postfach an, sondern speichert nur die E-Mail-Adresse im Active Directory für die Nutzung mit anderen Programmen.

Sobald Sie den Anwender auch für Exchange aktivieren, erhalten Sie die zusätzlichen Karteikarten für die Exchange-Eigenschaften. Erst dann kann dieser Benutzer auch ein Exchange-Postfach verwenden. Die MMC schreibt dann in das Feld der E-Mail-Adresse die primäre SMTP-Adresse des Benutzers, unter welcher das Postfach erreichbar ist.

Die Exchange-Aktivierung eines Anwenders ist im Kontext-Menü der Management-Konsole (MMC) erreichbar.

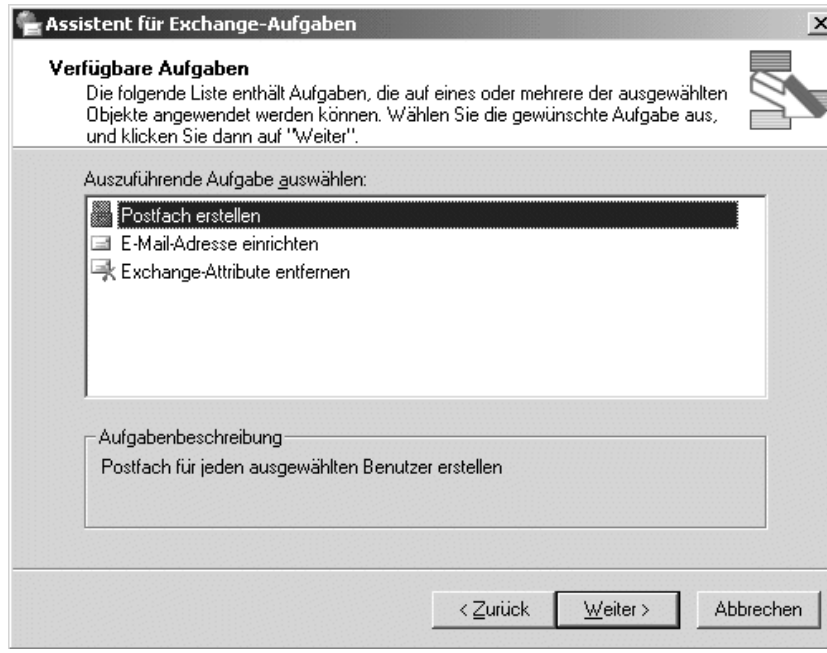


Abbildung 3.13 Exchange-Aufgaben

„Placeholder"-Konto

Es gibt eine weitere Variante eines Benutzers im Active Directory, die in Hinsicht auf Exchange gesondert behandelt wird. Der Benutzer des Postfachs besitzt kein Windows 2003-Anmeldekonto im Exchange-Forest. Diese Situation tritt nicht nur in der Multi-Forest-Umgebung auf, häufig befindet sich das Konto noch in einer Windows NT4-Domäne, die mit einer Vertrauensstellung an Windows 2003 gebunden ist. In diesem Fall wird das Active Directory-Konto als Platzhalter genutzt, dem die notwendigen Exchange-Informationen über E-Mail-Adresse, Postfachserver etc. hinterlegt werden. Das Konto wird deaktiviert, damit keine interaktive Anmeldung möglich ist und das „Externe Konto" als Besitzer des Postfachs erkannt wird.

Hinzufügen können Sie den externen Benutzer mittels der Optionen des Registers EXCHANGE – ERWEITERT. Unter den Postfachberechtigungen wird nun der externe NT4-Account als ZUGEORDNETES EXTERNES KONTO registriert und erhält Postfachzugriff, Leseberechtigung sowie das Recht SENDEN ALS. Beim Deaktivieren hat das Windows 2003-Konto keine SID mehr, Exchange erkennt die neue SID des externen Windows-Kontos für alle Zugriffe.

Für Exchange 2003 gibt es daher vier Benutzerobjekte im Active Directory, die für den Mailserver relevant sind.

Tabelle 3.2 Exchange-Benutzerübersicht

Benutzerobjekt	Beschreibung
Exchange-Postfach-aktivierter Benutzer (mailbox-enabled user)	Der Benutzer erhält ein Postfach zu seinem Active Directory-Konto innerhalb der Exchange-Organisation. Jedem Active Directory-Konto kann genau ein Postfach zugeordnet werden.

Benutzerobjekt	Beschreibung
Exchange-aktivierter Benutzer (mail-enabled user)	Der Benutzer erhält kein Postfach, sondern eine E-Mail-Adresse, über die alle Nachrichten z.B. an ein anderes Mailsystem weitergeleitet werden. Durch die Aktivierung taucht der Benutzer im Outlook-Adressbuch auf und kann Mitglied von Verteilern werden.
Exchange-aktivierter Kontakt (mail-enabled contact)	Ein Kontakt mit E-Mail-Adresse im Active Directory wird erst dann in Exchange als Adressbucheintrag nutzbar, wenn dieser „Exchange-aktiviert“ wird. Im Gegensatz zum Exchange-aktivierten Benutzer besitzt ein Kontakt keine SID und kann sich nicht am Netzwerk anmelden.
Deaktivierter Benutzer mit Exchange-Postfach (disabled-mailbox-enabled user)	Für Anwender, die zwar ein Postfach auf einem Exchange-Server der Organisation besitzen, aber keinen aktiven Windows-Benutzer, wird solch ein Platzhalter-Konto angelegt.

Bei diesen Objekten werden in *Active Directory-Benutzer und -Computer* (ADUC) weitere Karteikarten für die Exchange-Eigenschaften eingeblendet.

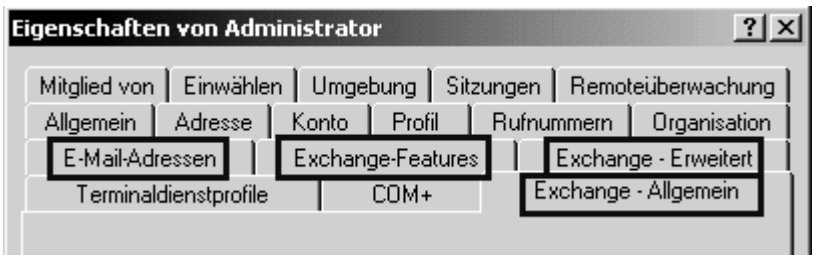


Abbildung 3.14 Exchange-Karteikarten

1:1-Beziehung

Durch die Integration von Exchange 2003 in Active Directory kann ein Benutzer immer nur genau ein Postfach besitzen. Dies gilt auch bei der Zuordnung für externe Benutzer. Die Beziehung Benutzerkonto und Postfach ist immer eindeutig, und Postfachrechte für weitere Benutzer oder Gruppen müssen explizit hinzugefügt werden. Besteht die Notwendigkeit, dem Benutzer zwei Postfächer zuzuweisen, sollten Sie ein zweites NT-Konto anlegen und dem Benutzer Rechte auf das weitere Postfach geben.

Halten wir fest:

- Nur Active Directory-Benutzer und -Kontakte sind für Exchange nutzbar und werden erst durch eine separate Exchange-Aktivierung verfügbar.
- Die E-Mail-Adresse in den Haupteigenschaften eines Objektes ohne Exchange-Verwaltung hat keine Auswirkung auf das Mailsystem.
- Alleine AD-Benutzer können ein Exchange-Postfach erhalten, und es besteht eine 1:1-Beziehung zwischen Benutzer und Postfach.

3.6 Gruppen und Verteiler

Gruppen im Detail

Die meisten Administratoren assoziieren mit dem Begriff Gruppe die Sicherheitsgruppe in Windows, deren Aufgabenstellung es ist, die Benutzer zusammenzufassen und die Zuweisung von Berechtigungen zu ermöglichen. Mit dem Einsatz von Exchange 2003 wird aus jedem Mailverteiler ebenfalls eine Gruppe. Dies kann auf der einen Seite zu einer vereinfachten Verwaltung führen, wenn beispielsweise die Gruppe „Einkauf“ nicht nur die Rechte auf einem Verzeichnis hat, sondern zugleich Verteiler für Nachrichten ist und Rechte auf einen Öffentlichen Ordner in Exchange erhält. Auf der anderen Seite nimmt die Anzahl der Gruppen im Active Directory sehr stark zu. Mit Exchange 5.5 waren die Verteiler im Mailsystem und die Windows-Sicherheitsgruppen getrennt. Dies ist mit Exchange 2003 nicht mehr so.

3.6.1 Einsatz von Gruppen

Basis: Aufgaben

Zur Vorbereitung einer entsprechenden Konzeption für Gruppen und Namen müssen Sie sich verdeutlichen, wofür die Gruppe im Active Directory eingesetzt wird. Es ist nicht ausreichend, einfach eine Gruppe für jede Abteilung zu erstellen, um die Mitarbeiter darin zusammenzufassen. Auch die Erweiterung derselben Gruppe als Verteiler für Exchange und die Vergabe von Rechten auf Dateifreigaben umfasst nicht die tatsächliche Bandbreite von Gruppen. Der Einsatz von Gruppen ist sehr viel globaler zu sehen.

Die folgende Tabelle zeigt einige verschiedene Einsatzmöglichkeiten von Gruppen. Sie werden vielleicht nicht alle Varianten in Ihrem Netzwerk benötigen, aber für die Gruppen, die Sie einsetzen, sollten Sie sowohl ein Namenskonzept als auch ein Position in Ihrer OU-Struktur definieren.

Tabelle 3.3 Gruppenübersicht

Objekte	Beschreibung OU-Konzept
Abteilungsgruppen	Diese Gruppen werden genutzt, um die Zugriffe auf Freigaben und Dokumente des Benutzers einer Abteilung zu steuern. Die Gruppen erhalten die entsprechenden Rechte und fassen die Mitarbeiter der Abteilung zusammen. OU: Diese Gruppen liegen in der jeweiligen Abteilungs-OU Name: G-%NAME% (G-Einkauf, ou=Einkauf.msxfaq.local)
Funktionsgruppen	Diese Gruppen werden genutzt, um Zugriffe auf Freigaben und Dokumente für verschiedene Abteilungen zu steuern. Die Gruppen erhalten die entsprechenden Rechte und die Mitarbeiter aus verschiedenen Abteilungen mit gleicher Aufgabe. OU: ou=Funktionen (ou= KundeA.msxfaq.local) Name f%NAME% (f-KundeA)

Objekte	Beschreibung OU-Konzept
Teamgruppen	Diese Gruppen werden genutzt, um Zugriffe auf Freigaben und Dokumente für zeitweilige Projekte einzurichten. Die Gruppen erhalten die entsprechenden Rechte und die Mitarbeiter aus verschiedenen Abteilungen. OU: ou=Projekte (ou= Bauphase1.msxfaq.local) Name: p%NAME% (p-Bauphase1)
Programmgruppen	Über die Mitgliedschaft in diesen Gruppen wird bestimmt, welcher Anwender ein Programm nutzen darf. Für Programme im Netzwerk sind damit Zugriffsrechte auf Freigaben möglich. OU: ou=Programme (ou= Word.msxfaq.local) Name: s%NAME% (s-word)
Ressourcengruppen	Diese Gruppen dienen zur Steuerung des Zugriffs auf Ressourcen, die nicht einem Programm oder einem Projekt zuzuordnen sind, z.B. Drucker, Internet und andere Dienste. OU: ou=Resourcen (ou= Drucker1OG.msxfaq.local) Name: r%NAME% (r-drucker1OG)
Administrative Gruppen	Diese Gruppen werden genutzt, um administrative Rechte auf Objekte im Active Directory und auf Systeme im Netzwerk zu vergeben. So kann über eine Richtlinie eine Gruppe zum lokalen Administrator bestimmter Server gemacht oder können einer Gruppe die Rechte auf bestimmte OUs gegeben werden. OU: ou=Admin (ou= AdminFileserver.msxfaq.local) Name: z%NAME% (z-AdminFileserver)
Verteiler	Werden besondere Gruppen nur für Verteiler benötigt, so können diese gesondert eingerichtet werden. OU: ou=Verteiler (ou=VertreterNord.msxfaq.local) Name: v%NAME% (v-VertreterNord)
Abfragebasierte Verteiler	Eine besondere Form der Gruppe, deren Mitgliedschaft sich aus selbst definierten Filtern automatisiert zusammensetzt. OU: ou=Verteiler (ou=Abteilungen.msxfaq.local) Name: q%NAME% (q-Einkauf)

Denken Sie bei der Wahl Ihrer Gruppennamen daran, dass diese auch im Adressbuch auftauchen und Sie als Administrator diese Namen sehr oft eingeben oder aus einer Liste auswählen müssen. Es gibt Unternehmen, die Ihre Gruppen mit einem besonderen Zeichen beginnen, um die Übersicht zu verbessern.

Für den Einsatz in Exchange sind primär die Verteiler und E-Mail-aktivierte Abteilungs- oder Funktionsgruppen interessant. Die Erweiterung der E-Mail-Funktionalität auch auf Gruppen für Programme oder Ressourcen erleichtert

die Informationsübermittlung bei Aktualisierungen und Betriebsunterbrechungen.

3.6.2 Fokus von Gruppen

Windows 2003 und das Active Directory kennen mehrere Gruppentypen, die einen unterschiedlichen Fokus und damit auch Einsatzzweck haben. Nicht alle Gruppen sind für Exchange nutzbar beziehungsweise zu empfehlen.

Tabelle 3.4 Typen von Gruppen

Gruppe	Beschreibung
Lokal	Lokale Gruppen auf einem Mitgliedsserver sind auf den Server beschränkt, auf dem sie definiert wurden. Sie können Mitglieder aus anderen Domänen enthalten, jedoch nur für Zugriffsrechte auf Ressourcen des lokalen Servers verwendet werden. Lokale Gruppen erscheinen nicht im Globalen Katalog und sind somit für Exchange nicht nutzbar.
Lokal (in Domäne)	Wird eine lokale Gruppe in der Domäne angelegt, so bezeichnet man diese als „domänenlokal“ und sie kann auf allen Systemen innerhalb der gleichen Domäne genutzt werden. Allerdings ist kein Zugriff von anderen Domänen im Forest oder in vertrauten Domänen möglich. Diese domänenlokalen Gruppen sind zugleich die lokalen Gruppen aller Domänencontroller der Domäne. Domänencontroller haben keine eigenen lokalen Gruppen, wie dies bei Mitgliedsservern oder Arbeitsstationen der Fall ist. Diese Gruppen könnten theoretisch für Exchange benutzt werden, aber praktisch verbietet sich der Einsatz, da diese Gruppen nicht aus anderen Domänen sichtbar sind und die Exchange-Server nur dann die Mitgliederliste auflösen können, wenn Sie einen Globalen Katalog der gleichen Domäne fragen. Diese Begrenzung auf die eigene Domäne gilt auch für die Verwendung für Berechtigungen auf andere Active Directory-Objekte und -Ressourcen.
Global	*Globale Gruppen* enthalten nur Mitglieder der eigenen Domänen. Sie können für Berechtigungen in anderen Domänen genutzt werden. Im Active Directory Native Mode ist eine Verschachtelung globaler Gruppen möglich. Die globale Gruppe selbst erscheint im Globalen Katalog ohne Angabe der Mitglieder. Für Exchange bedeutet dies eine eingeschränkte Nutzung als Verteiler.
Universal	Die universelle Gruppe ist erst mit dem Active Directory im Native Mode verfügbar. Sie kann sowohl globale Gruppen, lokale Gruppen und weitere universelle Gruppen enthalten, also Mitglieder aus dem gesamten Forest. Die besondere Eigenschaft ist ihre Replikation in den Globalen Katalog. Damit kann jeder Dienst im gesamten Forest die Mitgliedschaften auflösen. Dies prädestiniert diese Gruppen zum Einsatz als Exchange-Verteiler, für kleinere Unternehmen auch als Sicherheitsgruppe

Gruppe	Beschreibung
Abfragebasierte Verteilergruppe (QBDL)	Die abfragebasierten Verteiler (Query Based Distribution List) ermöglichen die Zusammenstellung der Mitglieder aufgrund definierter LDAP-Filter. Diese Gruppen können nicht als Sicherheitsgruppen und somit nicht zur Vergabe von Berechtigungen verwendet werden. QBDL's erfordern den einheitlichen Modus von Exchange 2003.

Die mangelnde Eignung von lokalen und globalen Gruppen für den Einsatz mit Exchange wird in der MMC beim Aktivieren der Exchange-Aufgaben angezeigt, aber nicht verhindert.

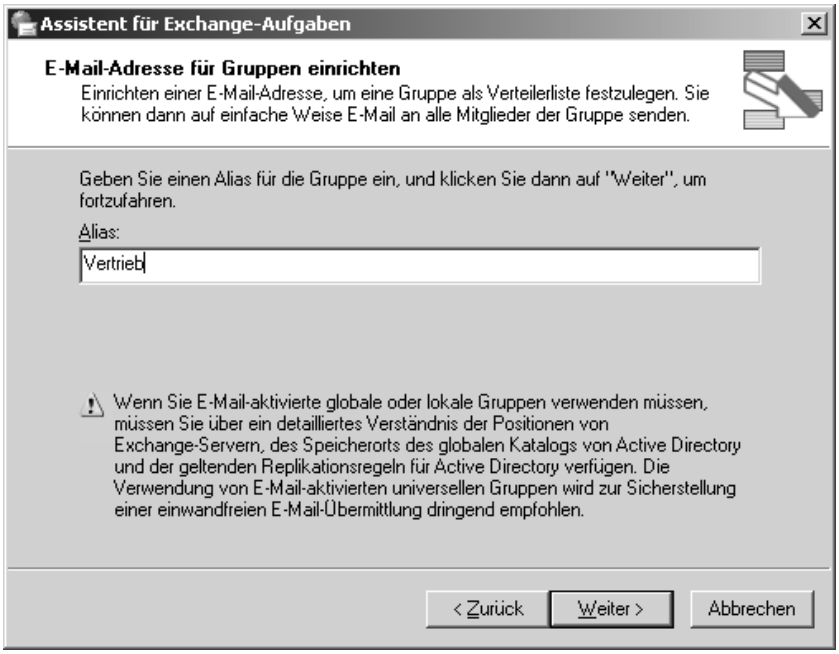


Abbildung 3.15 Warnung zu globalen Gruppen

Der Typ einer Gruppe kann im laufenden Betrieb zwischen Lokal, Global und Universal geändert werden. Um eine globale Gruppe in eine lokale Gruppe zu ändern, ist aber der Umweg über die universelle Gruppe notwendig. Ehe Sie nun aber alle Gruppen zu universellen Gruppen umstellen, sollten Sie bedenken, dass diese Gruppen auf alle Globalen Katalog-Server des Forests repliziert werden und für alle Personen sichtbar sind. Dies bedeutet in größeren Umgebungen eine gesteigerte Replikation, eine umfangreichere Active Directory-Datenbank und eine nicht immer gewünschte bzw. notwendige Sichtbarkeit.

Verschachtelung

Ein weiterer Faktor ist die Verschachtelung von Gruppen. Für Exchange 2003 ist die Mailerreichbarkeit zu prüfen. Solange nur eine Domäne besteht, ist die Verwendung von globalen und universellen Gruppen als Verteiler möglich. Bei einem Multi-Domänen-Modell sind nur universelle Gruppen anwendbar, auch für die Verschachtelung von Gruppen.

3.6.3 Gruppen und Rechte

Das zweite Unterscheidungsmerkmal der Gruppen ist die Eignung zur Vergabe der Berechtigung. Eine Gruppe kann erst dann zur Vergabe von Rechten genutzt werden, wenn die Gruppe auch eine SID (Security Identifier) besitzt:

Tabelle 3.5 Gruppenarten

Active Directory-Gruppe	Beschreibung
Verteiler	Gruppen vom Typ Verteiler haben keine SID und können daher nicht für die Vergabe von Berechtigungen verwendet werden. Verteiler sind nur für den Mailversand geeignet.
Security-Gruppen	Eine Sicherheitsgruppe besitzt eine SID und eignet sich somit für die Vergabe von Rechten auf Ressourcen und Objekte.
QBDL	Abfragebasierte Verteilergruppen existieren nur in Verbindung mit Exchange 2003 (und Windows 2000) im Native Mode und haben keine SID. Sie sind daher nicht für die Vergabe von Berechtigungen geeignet.

Im praktischen Einsatz bedeutet dies, dass die meisten Administratoren mit Sicherheitsgruppen arbeiten. Verteiler im Active Directory werden erst dann interessant, wenn das Active Directory als Verzeichnisdatenbank für Anwendungen genutzt wird, die keine Sicherheitsgruppen benötigen. Eine Sicherheitsgruppe kann in einen Verteiler konvertiert werden und umgekehrt. Somit wird ein Verteiler, der Berechtigungen auf einen Öffentlichen Ordner erhält, automatisch vom System in eine Sicherheitsgruppe mit E-Mail-Funktionalität umgewandelt. Beachten Sie jedoch, dass beim Verschachteln von abfragebasierten Verteilern in Sicherheitsgruppen keine Berechtigung für die Mitglieder dieser speziellen Verteilergruppe vergeben werden.

3.6.4 Gruppen, E-Mail-Adressen und Exchange

Wie schon bei den Benutzern, so macht eine E-Mail-Adresse der Sicherheitsgruppe diese nicht automatisch zum Exchange-Verteiler. Erst mit der expliziten Aktivierung in Exchange ist die Gruppe als „Distribution List“ im Adressbuch sichtbar. Die Gruppe als Active Directory-Objekt enthält auch die Liste der Mitglieder und kann wie jedes andere AD-Objekt auch per LDAP für andere Programme verwendet werden, so auch die eingetragene E-Mail-Adresse.

Abbildung 3.16 Exchange-aktivierte Gruppe

Mit Hilfe der Exchange-Aufgaben kann die bereits vorhandene Gruppe „Exchange-aktiviert“ werden und ist für den Outlook-Anwender nutzbar.

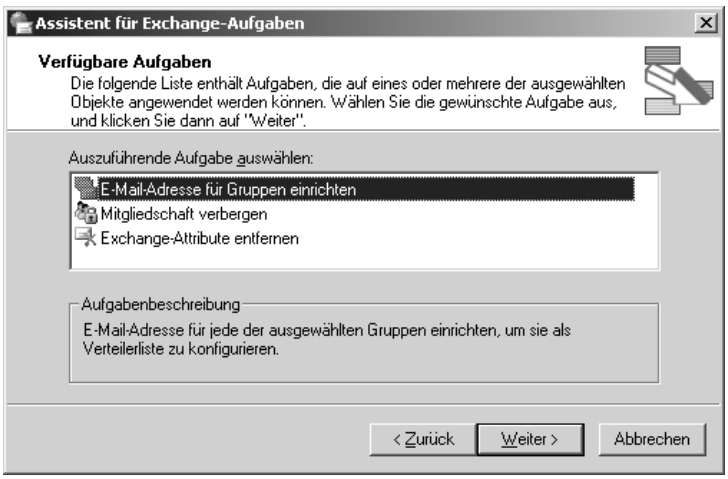
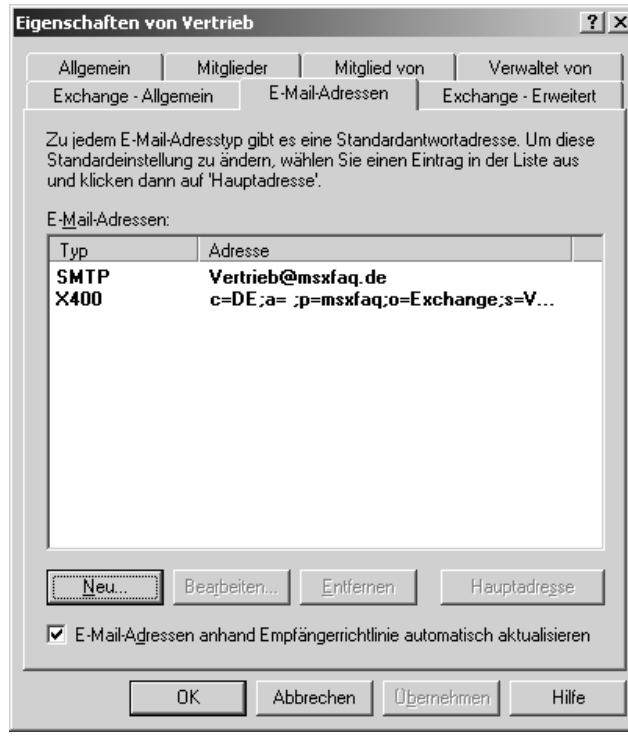


Abbildung 3.17 Exchange-Aufgaben für Gruppen

Abhängig von der Platzierung und Replikation der Domänencontroller und der Arbeit des Empfängeraktualisierungsdiensts wurde die Gruppe mit den notwendigen Attributen ausgestattet.

Abbildung 3.18 Exchange-Eigenschaften einer Gruppe



Nunmehr kann die Gruppe in Exchange für alle möglichen Aufgaben eingesetzt werden. Voraussetzung ist dabei die Auflösung aller Mitglieder der Gruppe über den Globalen Katalog. Exchange-Gruppen können sowohl als Verteiler dienen als auch zur Vergabe von Berechtigungen auf Ordner innerhalb eines Postfachs, Öffentliche Ordner, Connectoren und für weitere Einträge. Exchange erkennt das Hinzufügen von Rechten bei einem „normalen“ Verteiler und wandelt diesen automatisch in eine E-Mail-aktivierte Sicherheitsgruppe um.

Keine Berechtigungen für QBDL

Die abfragebasierten Verteilergruppen (QBDL) beanspruchen einen Sonderstatus. Im Gegensatz zu den „normalen“ Gruppen verfügen die QBDL nicht über die Reiter MITGLIEDER und MITGLIEDER VON. Stattdessen werden die Mitglieder unter VORSCHAU angezeigt und laufend aktualisiert, der entsprechende LDAP-Filter kann unter ALLGEMEIN angepasst werden. Diese Gruppen können nicht in eine Sicherheitsgruppe umgewandelt und für Berechtigungen eingesetzt werden.

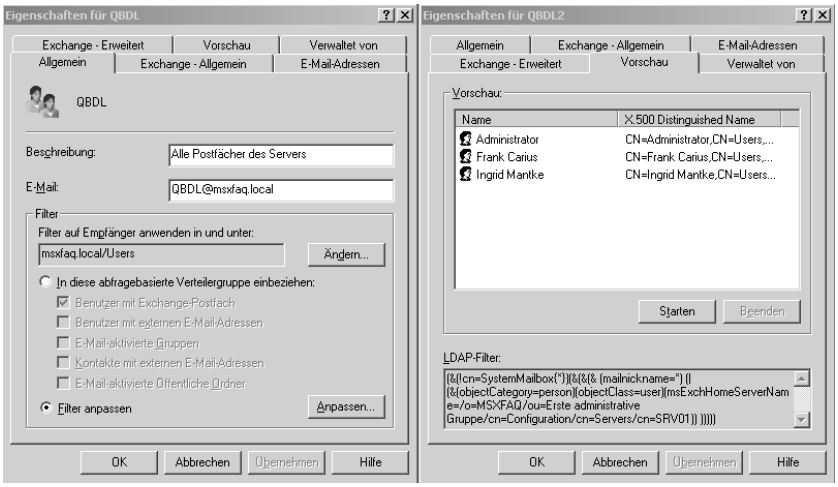


Abbildung 3.19 Abfragebasierte Verteilergruppe

Vermeiden Sie es, die Gruppe „Domänen-Benutzer“ für Exchange zu aktivieren, da sonst auch externe Berater, Praktikanten und andere Personen, die ein Postfach haben, aber nicht zur Belegschaft gehören, Ihre Firmeninformationen erhalten. Weiterhin sollten Sie weder eine „Built In“-Gruppe (Administratoren) noch einen Verteiler zur Primären Gruppe des Benutzers machen. Die ordnungsgemäße Funktionalität der Gruppe als Verteiler ist dann nicht mehr gegeben.

Achtung!

Halten wir fest:

- Werden in Exchange mehrere Personen in einem Verteiler zusammengefasst, dann sollte dies in einer universellen Sicherheitsgruppe erfolgen (Universal Group).
- Die Nutzung von lokalen Gruppen ist nur mit besonderer Vorsicht und Kenntnis um deren Einschränkungen möglich.
- Die Nutzung von Verteilern ohne SID ist zwar möglich, aber nicht als solche für Berechtigungen (Public Folder) innerhalb von Exchange einsetzbar.
- Exchange konvertiert Verteiler selbstständig in Sicherheitsgruppen, wenn die Verteiler für den Einsatz von Rechten (Public Folder) benutzt werden.
- Universelle Gruppen sind für die Exchange-Funktionen zwingend erforderlich, wenn mehr als eine Domäne mit Globalen Katalog-Servern (GC) im Forest existieren und die Exchange-Server verschiedene GCs befragen.
- Universelle Sicherheitsgruppen können nur in Domänen im Windows 2000/2003-Native Mode angelegt werden. Dies schließt die Nutzung von NT4-Domänencontrollern aus.

- Reine Verteiler (Gruppen ohne SID) werden in der Regel kaum eingesetzt, da in vielen Unternehmen die „Security Group“ die erforderlichen Mitglieder bereits repräsentiert.
- Abfragebasierte Verteiler (QBDL)sind nur im Native Modus möglich und die Mitglieder setzen sich automatisch anhand eines LDAP-Filters zusammen. Sie können weder in eine Sicherheitsgruppe umgewandelt werden, noch Mitglied von anderen Gruppen sein.

3.7 Computer und Gruppenrichtlinien

Das Computerkonto als Active Directory-Objekt spielt eine nicht ganz unwesentliche Rolle für die Exchange 2003-Umgebung. Das Active Directory bietet die Möglichkeit, mittels Gruppenrichtlinien (Group Policy) bestimmte Einstellungen nicht nur für Benutzer, sondern auch für Computer zu verteilen. Sie sollten die Computer ebenfalls in entsprechende Organisationseinheiten einordnen, um die Reichweite der Gruppenrichtlinien (GPO) zu steuern. Es macht Sinn, diese Objekte in einer dedizierten OU „Systeme“ zu gruppieren. In der nachfolgenden Tabelle finden Sie einige Anregungen dazu.

Tabelle 3.6 Beispiel für Rechner-konventionen

Objekte	OU-Konzept
Arbeitsplatz-PCs	Alle „normalen“ Arbeitsplätze, die im täglichen Gebrauch den PC des Benutzers repräsentieren. OU: ou=Workstation (ou=WST.Systeme.msxfaq.local) Name: PC%Nummer4% (PC0025)
Notebooks	Mobile Rechner beispielsweise von Außendienstmitarbeitern. OU: ou= Workstation (ou=WST.Systeme.msxfaq.local) Name: NB%Nummer4% (NB0123)
Öffentliche PCs	Systeme, die im öffentlich zugänglichen Bereich des Unternehmens stehen und die nicht bestimmten Personen zugeordnet sind (Internet-Terminals, Systeme in Konferenzräumen, Maschinenterminals usw.). OU: ou=Public (ou=Public.Systeme.msxfaq.local) Name: PC%Nummer4% (PC0256)
Domänen-controller	Die Domänencontroller sind die Infrastrukturserver der Firma und dafür vorgesehen, nur diese Dienste bereitzustellen. Dies sind: Verzeichnisdienste (Active Directory, NDS, LDAP, RADIUS) sowie Server für IP-Verwaltung und Namensauflösung (DNS, DHCP, WINS) und für Anmeldedienste (NETLOGON, SYSVOL-Freigaben). OU: ou=DomainControllers(ou=DomainControllers.msxfaq.local) Name: SRVDC%Nummer2% (SRVDC05)

Objekte	OU-Konzept
Dienstserver	Die meisten Server fallen unter diese Kategorie. Es handelt sich dabei um Mailserver, Datenbankserver, Faxserver etc. Auch hier ist denkbar, bei einem entsprechenden Bedarf diese Server nach Klassen in weiteren OUs anzulegen. OU: ou=SRV oder SRVart (ou= SRV.Systeme.msxfaq.local) Name: SRVFS%Nummer2% (SRVFS03) Name: SRVSQL&Nummer2% (SRVSWL01) Name: SVRMAIL%Nummer2% (SRVMAIL01)

Besonders im Hinblick auf Gruppenrichtlinien und Berechtigungen macht es in größeren Unternehmen Sinn, dedizierte Server für bestimmte Funktionen zu installieren.

Konfiguration über GPO

Nachfolgende Gruppenrichtlinien können für Computer angewendet werden:

- Dienste, die automatisch gestartet werden.
- Dienste, die nie gestartet werden.
- Die Größe des Eventlogs.
- SNMP-Parameter zur Meldung von Fehlern.
- Explorer-Einstellungen im Hinblick auf Sicherheit (zum Beispiel: jeder Server hat unabhängig vom angemeldeten Benutzer einen Bildschirmschoner mit Kennwort).
- Mitgliederliste der lokalen Administratorgruppe.

Eine Reihe weiterer Einstellungen ist möglich, um den Betrieb von Exchange und den Clients stabiler zu machen. Für die Sicherheit der Server mittels Gruppenrichtlinien finden Sie in der TechNet und auf der CD-ROM ein White Paper.

3.8 Vorschlag für eine OU-Struktur

Unternehmens-organisation

Die Planung und der Entwurf einer OU-Struktur im Unternehmen ist ein Bereich, der sehr zeitintensiv sein kann. Alle Anforderungen und Möglichkeiten müssen ausgelotet und analysiert werden. Ferner sind auch administrative Berechtigungen und der Einsatz von Gruppenrichtlinien wichtige Faktoren bei der Planung und Umsetzung einer Organisationsstruktur. Zuletzt werden auch unternehmenspolitische und persönliche Kriterien in die Waagschale gelegt, da die Anforderungen der Abteilungen oder die Ausrichtung der Geschäftsbereiche differieren.

Für Exchange spielt die OU-Struktur eine nebensächliche Rolle, obwohl sie für die Installation und zur Darstellung einiger Elemente benötigt wird. Primär ist die Struktur in einer Domäne ein Teil der Active Directory-Planung. Für die weiteren Kapitel wird die vorgestellte OU-Struktur zu-

grunde gelegt. Aufgrund von Erfahrungswerten passt dieses Konzept für viele kleine und mittlere Unternehmen oder ist zumindest als Ausgangssituation anwendbar. Sie sollten immer die Gelegenheit nutzen, neue Impulse in einem Testfeld zu prüfen, und die Chance der Weiterentwicklung ergreifen.

Die Einordnung der Benutzer und Rechnersysteme hat schon die erforderliche Organisationsstruktur ahnen lassen. In der nachfolgenden Übersicht wird die Nutzung der Standard-OUs sowie auch der Gebrauch eigener Organisationseinheiten veranschaulicht.

Tabelle 3.7 Realisierbare OU-Struktur

Name der OU	Verwendung
Users	In der OU „User“ liegen die Standardbenutzer und -gruppen, die das Active Directory und einige Anwendungen mitbringen. Sie sollte nicht in andere OUs verschoben werden.
Computers	Bei der Aufnahme eines Computers in die Domäne wird normalerweise ein Computerobjekt in der OU „Computers“ angelegt. Diese Objekte sollten Sie dann in die gewünschte Ziel-OU verschieben.
Domänen-controllers	Vom AD für alle Domänencontroller reservierte OU. Eine eigene Richtlinie konfiguriert alle Domänencontroller. Die Objekte sollten nicht verschoben werden.
Abteilung	Eine Strukturierung nach Abteilungen oder/und Geschäftsbereichen ist häufig sinnvoll, und die Zuordnung der logischen Benutzer und Gruppen vereinfacht die weitere Administration. Auf dieser OU kann mittels einer GPO eine Standardkonfiguration für alle User durchgesetzt werden, ohne Computer, Server, Administratoren oder Dienstkonten zu beeinflussen. Bei Bedarf ist eine OU für externe Mitarbeiter ohne Abteilungszuordnung einzuplanen.
Admin	Für administrative Aufgaben sollten generell Gruppen oder spezielle administrative Konten eingerichtet werden. Die Ablage in einer OU „Admin“ lässt über Gruppenrichtlinien bestimmte Einstellungen zu, die dann auf die Mitglieder der Gruppen angewandt werden. So können OU-Rechte delegiert werden, ohne Domänenrechte zu vergeben.
Dienste	Konten für Dienste und Prozesse sind in einer eigenen OU „Dienstkonten“ gegen Gruppenrichtlinien für Benutzer und administrative Fehlzugriffe besser geschützt und leichter zu finden.

Name der OU	Verwendung
Systeme	Ähnlich wie die Strukturierung der Benutzer nach Abteilungen sind hier die Arbeitsplätze nach entsprechenden Funktionen unter „Systeme“ gegliedert. Auf oberer Ebene können Systemstandards festgelegt werden, die auf alle darunter liegenden OUs angewendet werden (Beispiel: Inventarsoftware, Fernsteuerung etc.). Systeme\Admin Alle administrativen Arbeitsplätze, denen keine Gruppenrichtlinien zuzuordnen sind, befinden sich hier. Systeme\Fertigung Hier liegen alle „gesicherten“ Fertigungssysteme mit begrenzten Funktionen. Systeme\Notebook Notebooks erfordern eine eigene Richtlinie für die Sicherheit der Systeme außerhalb des Betriebes. Systeme\PublicPC Hier sind „öffentlich“ zugängliche Systeme untergebracht (Surfstationen in Kantine, Konferenzräumen etc.), die per Richtlinie extrem geschützt sind. Systeme\Workstation Hier liegen alle Standard-Arbeitsplätze, sofern keine Untergruppierung benötigt wird.
Server	Alle Server, die keine Domänencontroller sind, sollten differenziert betrachtet werden. Bei Anwendung von Gruppenrichtlinien ist keine Vererbung der Konfiguration normaler Systeme sowie der Domänencontroller erwünscht. Es macht Sinn, diese nach Art der Anwendung oder Funktionalität in Unter-OUs zu gruppieren (wie Exchange, Dateiserver, Datenbank usw.).
Migration	Bei einer Migration sollten alle Objekte in einer spezifischen OU abgelegt und erst nach der kompletten Umstellung in die Ziel-OU verschoben werden. Dies kann sich auf die Migration eines einzelnen Users bis hin zu ganzen Systemen beziehen. Gerade bei einer Migration von Exchange 5.5 erleichtert dies oft die Einrichtung des Active Directory Connectors (ADC).

Die OU-Struktur ist eine logische Sichtweise auf Elemente in der Active Directory-Datenbank. Sie sollten diesen Entwurf nicht ungeprüft in Ihr Netzwerk übernehmen, obgleich er für die Installationen im Buch vorausgesetzt wird. Jedes Unternehmen hat eigene Bedürfnisse, die ermittelt und berücksichtigt sein sollten.

3.9 Die Active Directory-Datenbank

Das Active Directory stellt keine monolithische Datenbank dar, sondern unterteilt sich in drei Partitionen, um diese später effektiv zu replizieren und zu organisieren.

- Schema
- Konfiguration
- Domain

Darüber hinaus bietet Windows 2003 eine Anlage von weiteren Partitionen im „Applikationsmodus“.

3.9.1 Das Schema

Schema-Partition

Im Schema sind alle Definitionen und Gültigkeitsregeln von Attributen und Klassen des Active Directory gespeichert. Jedes AD-Objekt (z.B. User, Group, Computer) besteht aus vielen definierten Feldern, die zusammen eine Objektklasse ergeben. Ein konsistentes Verzeichnis kann nur mit einem Reglement gewährleistet werden, in dem die Definition der Attribute festgelegt wird. Für Exchange werden nun weitere Attribute benötigt wie E-Mail-Adresse und *mailNickname* (Alias). Microsoft hat Attribute und Klassen für das Mailsystem vordefiniert. Mit dem Schema-Update wird das AD-Verzeichnis mit den Exchange-Attributen erweitert.

Mit dem *Snap-In* für das Active Directory-Schema können Sie sich alle Klassen und Attribute anschauen. Sie können dieses Snap-In in der Management-Konsole (MMC) hinzufügen, nachdem Sie Folgendes auf der Konsole des Servers eingegeben haben:

```
regsvr32 schmmgmt.dll
```

Das Schema zeigt auf, welche Felder optional und welche verbindlich sind. Folgendes Bild zeigt das Schema und die Klasse „user“ im Detail.

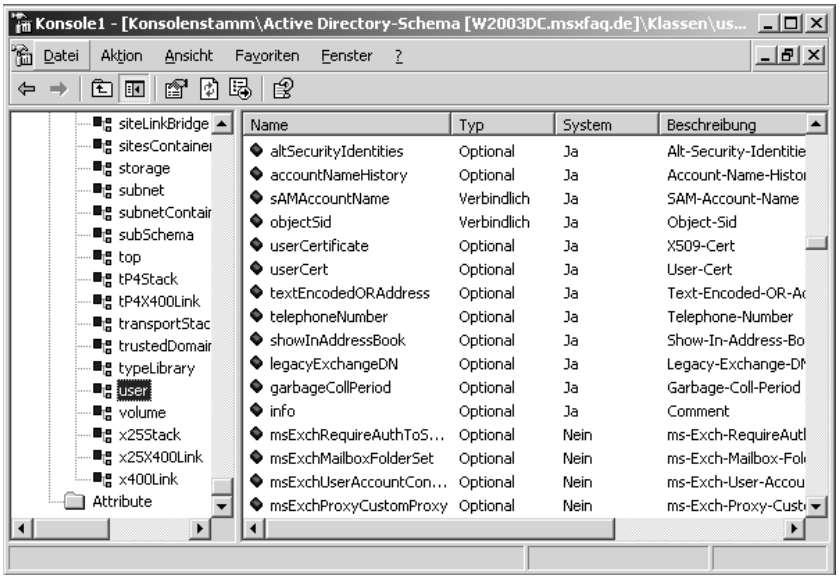


Abbildung 3.20 Anzeige des Active Directory-Schemas

Bei genauer Ansicht der Klasse „user“ ist zu erkennen, welche Felder verbindlich sind und welche Felder optional gefüllt sein können, darüber hinaus auch die Syntax und aus welcher Quellklasse das Attribut kommt.

Das Objekt „user“ enthält Pflichtfelder wie den Anmeldenamen (sAMAccountName), die SID (objectSID) und das Kennwort sowie jede Menge optionaler Felder (Telefonnummer etc.). Wird nun das AD-Verzeichnis von Exchange mitgenutzt, muss folgendermaßen das Objekt „Benutzer“ um die entsprechenden Felder erweitert werden (z.B. Exchange-Stammserver, Exchange-Speicher, Exchange-E-Mail-Adresse etc.).

Unter „Attribute“ können Sie alle Felder einsehen, die im Schema definiert sind. Exemplarisch sehen Sie in Abbildung 3.20 die Schema-Definition von „msExchHomeServerName“. Dieses Feld ist im globalen Katalog präsent und besteht aus einer Zeichenfolge.

Abbildung 3.21 Schema-Definition eines Attributs

Achtung!

Bitte beachten Sie, dass eine Änderung im Schema wesentlich prekärer ist als ein Eingriff in die Registrierung. Jede noch so kleine Anpassung wird in der gesamten Organisation auf jeden Domänencontroller repliziert und kann bei falscher Anwendung verheerende Folgen haben.

Bevor Sie im Schema Änderungen vornehmen, sollten Sie hundertprozentig genau wissen, welche Auswirkungen dies hat und welche Objekte und Klassen gegebenenfalls noch betroffen sind.

3.9.2 Die Konfigurationspartition

Konfigurations-partition

Die Konfigurationspartition enthält alle Daten über Aufbau und Struktur des Active Directory und auch von Exchange. Mit der Microsoft-Konsole *Active Directory-Standorte und -Dienste* erhalten Sie einen Einblick in die Konfigurationspartition.

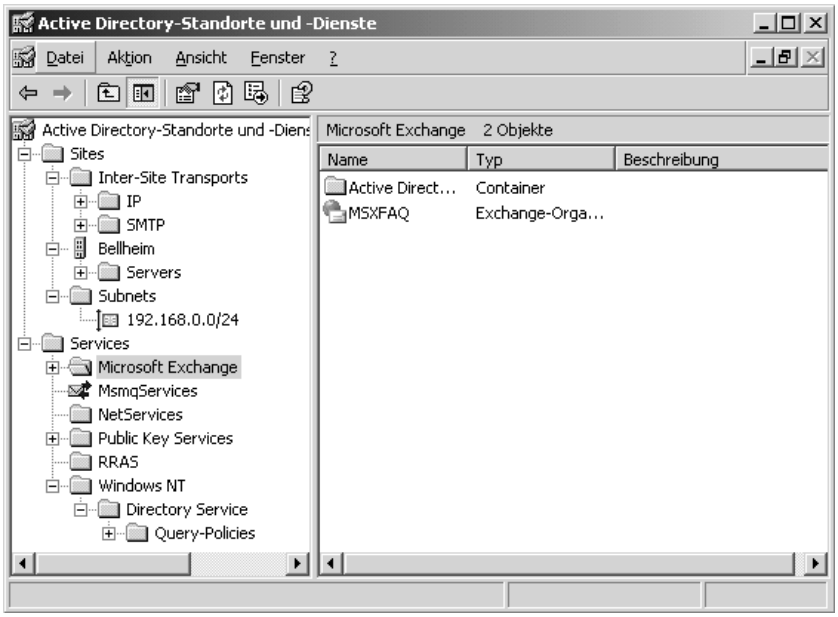


Abbildung 3.22 Active Directory-Konfigurationspartition

Alle diese Informationen liegen in der Konfigurationspartition und können von allen Systemen bei jedem Domänencontroller ausgelesen werden. In diesem Bereich des Active Directory liegen zum Beispiel die Standorte und Replikationsverbindungen ebenso wie die Liste der autorisierten DHCP-Server, Organisationszertifikatsstellen und RAS-Richtlinien. Hier können auch für das Active Directory so lebenswichtige Parameter wie das „TombStoneInterval“ gesetzt werden, nach dessen Ablauf gelöschte Elemente wirklich entfernt werden.

Auch Exchange verfügt über eine ganze Menge Konfigurationen, die festzuhalten sind. Unter anderem zählen dazu die Organisation selbst, welche Dienste und Verbindungen bereitgestellt werden sowie alle Datenbanken und deren Aufbau und Struktur innerhalb der Organisation. Diese Informationen speichert Exchange 5.5 in der Verzeichnisdatenbank (DIR.EDB).

In der Service-Ebene legt das Exchange-Setup einen eigenen Zweig an, in dem alle Server-Informationen gesammelt werden. Daher ist es notwendig, dass bei der Installation des ersten Servers oder des Active Directory Connectors die erforderlichen Rechte vorhanden sind. Für Folgeinstallationen werden die Schema- und Enterprise-Rechte nicht mehr benötigt.

Bei der Durchsicht der Exchange-Server-Struktur erkennen Sie den Umfang der Konfigurationspartition. In dem TechNet-Artikel „252370 XADM: Layout of Exchange 2000 Server Configuration within Active Directory” finden Sie diese Struktur textbasiert mit bezeichnenden Kommentaren.

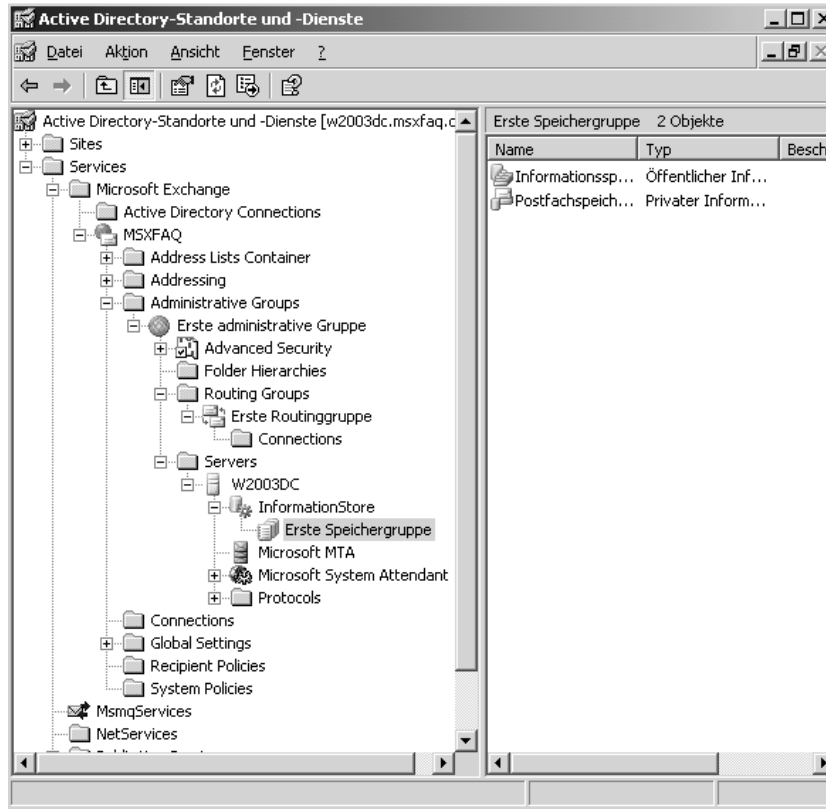


Abbildung 3.23 Exchange-Konfiguration im Active Directory

Diese Konfigurationsstruktur finden Sie später im Exchange System-Manager wieder. Der Exchange System-Manager liefert Ihnen eine effektive und sichere Möglichkeit, Exchange zu konfigurieren. Trotz der anscheinend großen Übereinstimmung in der Ansicht sollten Sie nur über den Exchange System-Manager konfigurieren, da dieser viele Eingaben und Änderungen auf Plausibilität prüft und zusammenhängende Änderungen korrekt durchführt. Dadurch werden Fehlfunktionen verhindert, die außerordentlich schwer oder nur durch eine Neuinstallation zu beheben sind.

Eine Änderung in der Exchange-Konfiguration bedarf einiger Rechte, die über die Mitgliedschaft in bestimmten Gruppen geregelt wird. Ein Domänenadministrator ist nicht automatisch für Änderungen an Exchange legitimiert.

Sie wissen nun, wo Exchange 2003 einen großen Teil der Konfiguration ablegt.

3.9.3 Die Domänenpartition

In der dritten Active Directory-Partition werden schließlich die Mailobjekte gespeichert, denn ein Exchange-Server ohne Anwender ist wie eine Straße ohne Fahrzeuge. Hier finden sich alle Benutzer, Gruppen, Computerkonten und weitere AD-Objekte der definierten OU-Struktur einer Domäne. Die Microsoft Management Console (MMC) namens „Active Directory-Benutzer und -Computer“ zeigt genau den Bereich der Domänenpartition an.

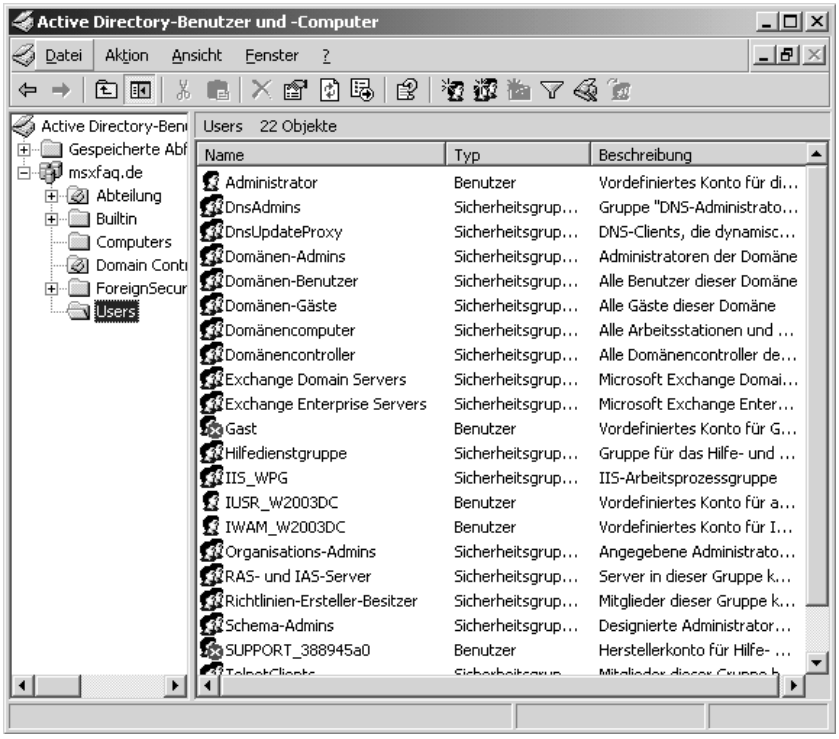


Abbildung 3.24 Active Directory-Domäne

Im Gegensatz zu den Partitionen für Schema und Konfiguration wird die Domäne nur auf den Domänencontrollern der gleichen Domäne repliziert. Die Informationen über die Benutzer einer Domäne sind auf Domänencontrollern in anderen Domänen nicht gespeichert. Ein Dienst muss daher immer einen passenden Domänencontroller suchen. Um dies zu vereinfachen, gibt es den Globalen Katalog, der neben den Domänenangaben eine Auswahl bestimmter Informationen über alle weiteren Domänen hinweg bereitstellt.

Exchange 2003 verwendet alle Active Directory-Partitionen und ist somit vollkommen abhängig von der ordnungsgemäßen Bereitstellung in Windows.

Die enge Verbindung von Exchange mit dem Active Directory bringt auch einige Einschränkungen in der Administration mit sich. Dies bedeutet eine extreme Veränderung zu Exchange 5.5 und ein Umdenken für Sie.

Neues Berechtigungskonzept

Die Ablage der Exchange-Informationen als zusätzliches Attribut an einen Benutzer oder eine Gruppe hat gleich mehrere Dinge zur Folge:

- Der Systemadministrator des Exchange-Servers ist berechtigt, alle Dienste auf dem Server zu stoppen, zu starten oder zu verändern. Das Recht erlaubt ihm jedoch nicht, die Exchange-Konfiguration oder Exchange-Attribute eines Benutzers anzupassen.
- Im Gegensatz dazu kann der Exchange-Administrator Eingriffe in der Konfiguration vornehmen (z.B. neue Routinggruppen anlegen, Grenzwerte für Benutzer über den Postfachspeicher definieren etc.), ohne eine Berechtigung auf dem Server oder der OU zu haben sowie Mitglied der Domänenadministratoren zu sein.
- Die Eigenschaften des Benutzers (Mailadresse, Speicherbeschränkungen, erlaubte Protokolle, Gruppenmitgliedschaften etc.) werden durch den Administrator der Domäne oder OU bestimmt. Dazu muss er kein Exchange-Administrator sein. Für einige Aktionen muss er jedoch die Konfiguration lesen können, um z.B. einen Postfachspeicher auszuwählen.
- Werden Exchange 2003-Server in mehreren Domänen betrieben, in denen unterschiedliche Personen Administratoren sind, erfordert dies eine detaillierte Abstimmung bei der Zusammenarbeit.
- Werden alle Exchange 2003 in einer Domäne aufgestellt, aber im Forest sind die Benutzer über viele Domänen verteilt, sind ebenfalls entsprechende Vorkehrungen zu treffen.

Die Aufteilung der Berechtigungen erlaubt eine umfangreiche Delegierung von Aufgaben an verschiedene Personenkreise. Die Begrenzungen, die mit Exchange 5.5 vorgegeben waren, lösen sich auf. Die Trennung der Funktion des Administrators des „Ressource-Servers“ und des OU-Administrators für Benutzer und Gruppen lässt eine ganz neue Gliederung von Aufgaben zu.

Spezifische Exchange-Objekte, die nicht zur Gruppe der neuen Objekte im AD gehören, müssen ebenfalls in der Domänenpartition sichtbar sein. Dazu gehören die E-Mail-aktivierten Öffentlichen Ordner sowie der Server selbst und die Datenbanken. Für die internen Prozesse wie die Replikation Öffentlicher Ordner über den normalen Nachrichtenaustausch werden diese Informationen ebenfalls in der Domänenpartition aufbewahrt.

Mittels der Ansicht „Erweiterte Funktionen“ im ADUC (Active Directory Users and Computers) wird eine neue OU sichtbar. Unter „Microsoft Exchange System Objects“ finden Sie alle Exchange-Objekte, die Exchange für seine eigene Verwaltung benötigt.

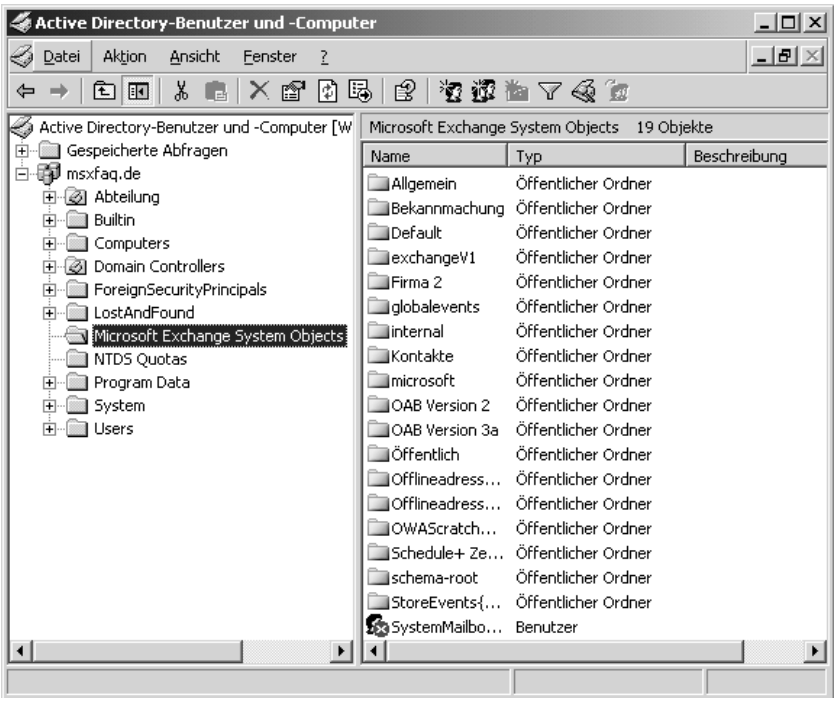


Abbildung 3.25 Exchange-System-Objekte im AD

Dies sind z.B. alle Öffentlichen Ordner, die über Mail erreichbar sind, und einige Systemobjekte. So können alle Exchange-Server über das Active Directory auch die E-Mail-Adressen dieser Objekte auflösen und die Nachrichten weiterleiten.

3.10 Die Flexible Single Master Operators

Flexible Single Master Operation (FSMO)

Durch die Existenz mehrerer Domänencontroller können verschiedene gegensätzliche Änderungen theoretisch zeitgleich auf unterschiedlichen Domänencontrollern durchgeführt werden. Erst bei der Replikation würde dann der Konflikt erkannt werden. Um dies zu reduzieren, gibt es im Active Directory besondere Rollen (Betriebsmaster), die solche Aktionen abstimmen. Bestimmte Änderungen und Funktionen werden dann von dem für diese Rolle zuständigen Server durchgeführt. Das Active Directory kennt folgende Rollen:

Schema-Master

Änderungen am Schema dürfen nie auf mehreren Systemen durchgeführt werden. Daher ist ein Server in der gesamten Organisation der *Schema-Master*. Alle Änderungen am Schema werden auf diesem Server durchgeführt und von dort auf alle anderen Domänencontroller repliziert.

Domain-Naming-Master

Diese Rolle ist für das Hinzufügen und Entfernen von Domänen in das Active Directory zuständig. Beim Hinzufügen einer Domäne verbindet sich der Assistent DCPROMO mit dem Domain-Naming-Master. Somit ist sichergestellt, dass nicht mehrere neue Domänen zur gleichen Zeit hinzugefügt werden.

RID-Master

Wenn Sie neue Objekte anlegen, dann erhalten diese Objekte eine Object-SID, die aus der Domäne und einer relativen ID (RID) gebildet wird. Um zu verhindern, dass zwei Objekte die gleiche RID erhalten, wenn sie auf verschiedenen Domänencontrollern angelegt werden, verteilt der RID-Master diese Nummern. Objekte mit gleicher SID darf es in einem Active Directory nicht geben. Diese Funktion gibt es einmal je Domäne.

PDC-Emulator

In einer Migrationsumgebung, aber auch für andere Funktionen ist eine Abwärtskompatibilität mit Windows NT-Domänen erforderlich. So existiert, wie der RID-Master auch, in jeder Domäne ein Primary-Domaincontroller-Emulator. Windows NT4 Backup-Domänencontroller (BDC) replizieren die Kontendatenbank von diesem Windows-Server. Zudem hat der PDC-Emulator eine besondere Rolle bei der Sperrung und Entsperrung von Benutzerkonten.

Infrastrukturmaster

Über diese Rolle ist in der Regel sehr wenig bekannt, obgleich sie eine wichtige Rolle in großen Active Directory-Umgebungen spielt. Der Infrastrukturmaster existiert einmal in jeder Domäne und verfolgt globale Änderungen, die Objekte in der eigenen Domäne betreffen. Dies wird anhand von Gruppenzugehörigkeiten klar. Ein Benutzer von Domäne A kann in einer Gruppe der Domäne B aufgenommen werden. Der Administrator von Domäne B ändert dazu das Feld „Mitglieder“ bei der Gruppe in Domäne B. Allerdings hat der Administrator keine Berechtigung, beim Benutzer in der Domäne A das Feld „Gruppenmitgliedschaften“ zu ändern. Der Infrastrukturmaster aus Domäne A erkennt dies und korrigiert den Eintrag beim Benutzer in der Domäne A. Damit der Infrastruktur-Server diese Änderung erkennt, darf dieser nicht auf einem Globalen Katalog-Server ausgeführt werden.

Auswirkungen auf Exchange

Eine direkte Auswirkung der Rollen im Active Directory auf Exchange 2003 ist nicht gegeben. Allerdings kann eine Störung der Betriebsmaster sehr bald

auch zu Problemen mit dem Active Directory führen und damit auch Exchange betreffen. Dies könnte sein.

Betriebsmaster beeinflussen Exchange indirekt

- Schema-Master
  Die Installation von Exchange erfordert auch die Erweiterung des Schemas, die ohne funktionierenden Master nicht ausgeführt werden kann. Nachdem „Forestprep“ erfolgreich ausgeführt und das Schema repliziert wurde, ist ein Ausfall des Schema-Masters für Exchange nicht mehr kritisch.
- RID-Master
  Ohne dessen Funktion können Sie nach einiger Zeit keine neuen Objekte (Benutzer, Verteiler, Öffentliche Ordner) mehr anlegen, da der Pool auf dem DC aufgebraucht ist.
- Infrastrukturmaster
  Die korrekte Pflege der Gruppenmitgliedschaften bei den Benutzern ist für die Prüfung der Berechtigungen wesentlich. Fehler hier sind nur sehr schwer zu diagnostizieren, aber äußern sich z.B. in angeblich nicht ausreichenden Berechtigungen beim Zugriff auf Öffentliche Ordner oder andere Postfächer.

Die FSMO-Rollen sind nur ein Baustein des Active Directory, aber auch für die Exchange-Funktion indirekt sehr wichtig.

3.11 Native Mode und Mixed Mode

Ein Tribut an die Kompatibilität zu früheren Systemen ist die Wahl des Betriebsmodus, in dem sowohl Exchange als auch das Active Directory betrieben werden können. Standardmäßig wird jede Domäne im Active Directory im so genannten „*Mixed Mode*“ installiert. Der Betrieb von Windows NT4-Domänencontrollern ist möglich. Mit der Einführung von Windows 2003 wurde auch für den Forest ein Betriebsmodus definiert. Je nach Betriebsmodus sind einige Funktionen nicht oder nur teilweise verfügbar.

Bei der Migration einer Windows NT4-Domäne mittels Update auf Windows 2003 werden einige Zeit lang einige Windows NT4-Backup-Domänencontroller (BDC) im Netzwerk betrieben. Erst nach Entfernen des letzten BDC kann die Domäne in den *Native Mode* umgestellt werden. Die Umschaltung erfolgt für jede Domäne im Forest einzeln und kann nicht rückgängig gemacht werden.

Einschränkungen

Solange die Domäne noch nicht im Native Mode ist, können drei wesentliche Funktionen nicht genutzt werden:

- Die für Exchange wichtigen „Universal Security Groups“ (USG) können nicht angelegt werden. Dies kann speziell in Umgebungen mit mehreren

Domänen zu Problemen führen, weil nur diese universellen Sicherheitsgruppen im globalen Katalog komplett mit den Mitgliedern geführt werden. Dies ist notwendig, um Nachrichten an diese Verteiler auch erfolgreich an alle Personen zustellen zu können.

- Der zweite Faktor für die Umstellung einer Domäne in den Native Mode ist die Nutzung der SID-History. Bei der Konsolidierung mehrerer Domänen müssen auch Benutzer und Dienste in das Active Directory übernommen werden. Bei der Migration mit dem Programm ADMT (Active Directory Migration Tool) kann die frühere SID als SID-History an den neuen Account angehängt werden. Die Berechtigungen des früher genutzten Kontos bleiben somit weitestgehend erhalten.
- Befinden sich Exchange 2003 und Windows 2003 im Native Mode, können auch die abfragebasierten Verteilergruppen (Query Based Distribution Lists, QBDL) als dynamische Verteiler genutzt werden. Die Mitgliedschaft wird zur Laufzeit anhand einer LDAP-Abfrage ermittelt. Dies erspart die manuelle Pflege von Gruppen z.B. anhand von Firmen- oder Abteilungsbezeichnungen.

Native Mode für Verteiler

Die Begrenzung des gemischten Modus für Gruppen ist so lange nicht kritisch, wie das Active Directory aus genau einer Domäne besteht. Hier können globale Sicherheitsgruppen trotz entsprechender Warnmeldungen im Eventlog die Funktion in Exchange ausreichend übernehmen. Um auf der sicheren Seite zu sein, sollten Sie bei zwei oder mehr Domänen in einem Active Directory-Forest mindestens eine Domäne in den Native Mode umstellen und lediglich in dieser Domäne die universellen Gruppen für Exchange-Verteiler und -Berechtigungen sowie die universellen Sicherheitsgruppen ablegen. In der Microsoft TechNet

- Q271930 Message Delivery to Global Groups Does Not Work
- Q231273 Group Type and Scope Usage in Windows 2000

finden Sie dazu einige Hinweise.

Exchange Native Mode

Auch die Exchange-Organisation wird bei der Installation im „Mixed Mode“ betrieben. In dieser Konfiguration ist der Betrieb von Exchange 5.5-Servern in der gleichen Organisation möglich. Erst wenn alle Exchange 5.5-Server entfernt sind, kann auch Exchange im „Native Mode“ genutzt werden. Einer der Vorteile ist z.B. die Lockerung der starren Administrativen Gruppen. Benutzer können dann zwischen administrativen Gruppen verschoben werden, und Routinggruppen sind nicht auf Server innerhalb einer Administrativen Gruppe beschränkt.

Halten wir fest:

- Für den Betrieb von Exchange 2003 sind universelle (Sicherheits-) gruppen die beste Wahl für Verteiler und Berechtigungen.

- Universelle Gruppen für Sicherheit und Verteilung sind nur in einer Native Mode-Domäne verfügbar.
- Sind die Anwender in mehreren Domänen verteilt, dürfen die Exchange-Verteiler nur als universelle Gruppe angelegt werden, wozu mindestens eine Domäne im Native Mode existieren muss.

3.12 Globale Kataloge

Bisher war schon mehrfach vom Globalen Katalog (GC) die Rede. Dies ist eine besondere Datenbank mit einer lokalen Kopie einer Teilmenge aller Informationen des gesamten Active Directory. Diese Funktion ist für Exchange 2003 lebenswichtig und einer der Punkte, für die es keine automatische Konfiguration im Active Directory gibt.

3.12.1 Funktion des Globalen Katalogs

Globale Verzeichnissuche

Der Globale Katalog ist eine Funktion, die zusätzlich auf einem DC aktiviert werden kann. Bestimmte Attribute von Objekten, wie der Name oder die E-Mail-Adresse eines Benutzers, werden in einem übergreifenden Index zusammengefasst. Im Gegensatz zu der Domänenpartition beinhaltet der Katalog nur ausgewählte Informationen als Teilmenge aller Domänen und erfüllt somit eine partielle Replikation des Active Directory. Im Schema ist definiert, welche Attribute dabei Teil des Globalen Katalogs werden.

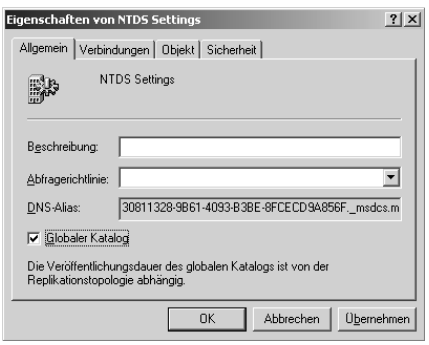


Abbildung 3.26 Einstellungen des GC

„Global Catalog“ (GC)

Dadurch, dass der GC alle Objekte des Active Directory beinhaltet, können Anfragen von Diensten wie Exchange von einem GC-Server in der Nähe beantwortet werden, auch wenn das eigentliche Objekt in einer ganz anderen Domäne abgespeichert ist.

Das Schema definiert dabei, welche Attribute eines Objekts in den globalen Katalog repliziert werden. Die Schemaerweiterung von Exchange mittels Forestprep fügt weitere Felder hinzu. Exchange befragt den GC z.B. für jede Nachricht, die Exchange zustellen muss, um den richtigen Postfachserver

zum gewünschten Empfänger zu ermitteln. Ohne mindestens einen Globalen Katalog kann Exchange keine Nachrichten zustellen.

3.12.2 Planung und Design

Die Planung, welcher Server die Funktion eines Globalen Katalogs übernimmt, lässt sich relativ einfach durchführen. Für das Konzept sind einige Eigenschaften zu berücksichtigen.

- Der Globale Katalog enthält alle Namenskontexte der Gesamtstruktur und dient als zentrale Datenbank zur Abfrage nach Objekten.
- Alle Objekte aller Domänen sind im GC enthalten sowie ein Auszug der am häufigsten genutzten Attribute dieser Objekte. Neben den universellen Gruppen werden auch deren Mitglieder im GC gespeichert.
- In jedem Windows-Standort (AD-Site) sollte es mindestens einen GC geben, damit der Exchange-Server, aber auch die Windows-Anmeldedienste im lokalen Netzwerk ihre Anfragen stellen können. Ansonsten muss die Anfrage über weniger zuverlässige und langsamere WAN-Verbindungen durchgeführt werden.
- Mehrere GC-Server erhöhen die Zuverlässigkeit und Geschwindigkeit durch die Verteilung der Anfragen. Somit ist immer ein weiterer Server im Netz, um bei Ausfällen oder dem Neustart eines GC den Dienst bereitzustellen.
- Viele Globale Kataloge erhöhen die Belastung durch die notwendige Replikation. Daher gilt es abzuwägen, ob durch einen zusätzlichen GC eine Optimierung der Client-Anfragen erreicht wird oder die Replikation den Vorteil zunichte macht.
- Beim Einsatz mehrerer Domänen darf der GC nicht mit dem Infrastrukturmaster kombiniert werden.

Mit diesen Grundregeln sollten Sie ein Konzept entwerfen, in dem genau definiert ist, welche Domänencontroller zusätzlich den Globalen Katalog-Dienst erhalten und auf welchen DC der Suchdienst nicht benötigt bzw. erwünscht ist.

3.12.3 Einstellen und prüfen

Der erste Server in Ihrem Active Directory wird immer automatisch zum Globalen Katalog. Jeder weitere Domänencontroller ist aber kein Globaler Katalog mehr. Es liegt in Ihrer Verantwortung, die Funktion auf den gewünschten Servern zu aktivieren.

GC-Einsatz

- In einem sehr kleinen Netzwerk mit einem Domänencontroller bedeutet dies, dass Sie nichts ändern müssen.
- In einem kleinen Netzwerk mit einer einzigen Domäne, aber mehreren Domänencontrollern können Sie auf allen die Globale Katalog-Option aktivieren.
- In einem größeren Netzwerk mit mehreren Domänen und Standorten müssen Sie planen, welche Server an welchem Standort als Domänencontroller und Globaler Katalog dienen.

Windows bietet leider keinen Assistenten oder Automatismus für die Einstellungen des Globalen Katalog-Servers an. Ohne entsprechende Konfiguration wird der Ausfall des einzigen GC im Forest zu ernsten Funktionsstörungen führen.

Welcher Server in Ihrem Forest die Funktion des GC ausführt, können Sie über mehrere Werkzeuge prüfen.

- DNS

  Der schnellste Weg ist die Abfrage des DNS-Servers. Jeder GC-Server registriert sich im DNS an mehreren Stellen.

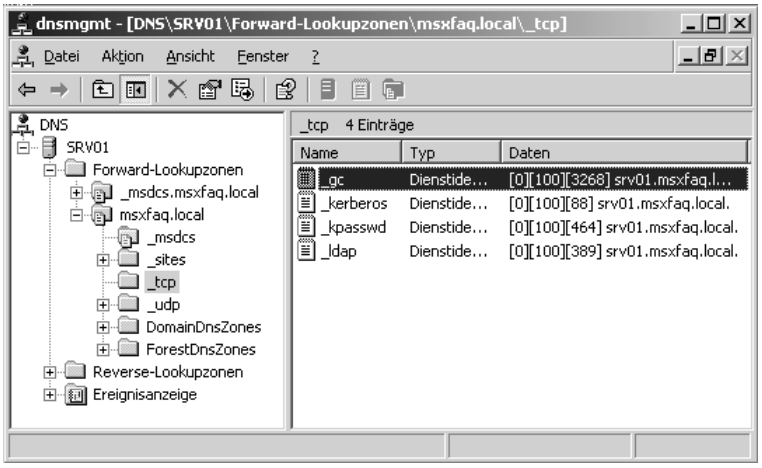


Abbildung 3.27 GC-Einträge im DNS

- REPLMON (*Active Directory Replication Monitor*)

  Ein weiteres Programm zur Kontrolle der Replikation und Funktion des Globalen Katalogs heißt REPLMON, das Teil der Support-Tools ist (Verzeichnis SUPPORT auf der Windows-CD). Bei der Verbindung mit dem Domänencontroller wird durch das Symbol einer Weltkugel der GC verifiziert. Zusätzlich können Sie mit REPLMON zugleich prüfen, ob die Replikation mit anderen Domänencontrollern funktioniert.

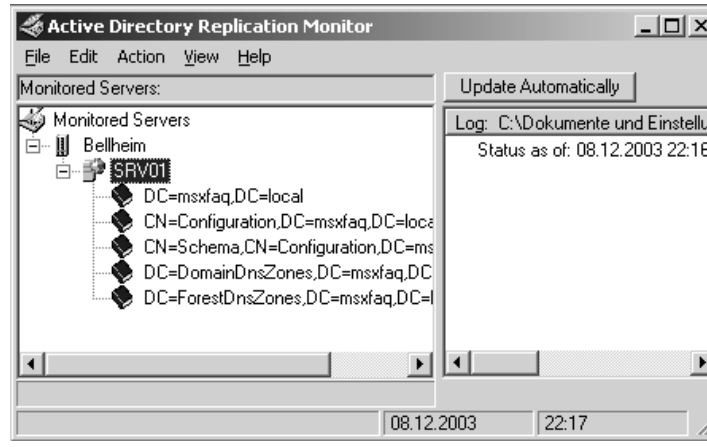


Abbildung 3.28 REPLMON zeigt den GC an

- Management-Konsole „*Active Directory-Standorte und -Dienste*“

  Mit der Management-Konsole für die Active Directory-Standorte und -Dienste können Sie ebenfalls die Einstellungen pro Server bei den Eigenschaften der NTDS-Settings kontrollieren und auch sofort ändern.

Wenn Sie einen Domänencontroller als Globalen Katalog konfigurieren, sollten Sie einige Zeit abwarten, bis diese Information repliziert wurde. Die Einstellung wird nicht sofort durch einen Eintrag auf dem Server selbst, sondern in der Konfigurationspartition des Active Directory vorgenommen und erst nach der Replikation aktiv. Kontrollieren Sie im DNS oder mit REPLMON, ob der Server die Einstellungen schon übernommen hat.

Aufgrund einer Besonderheit von Exchange kann ein neuer Domänencontroller als GC erst dann auch für Outlook vollwertig funktionieren, wenn der Domänencontroller durchgestartet wurde. Erst dann wird die „NSPI-DLL“ geladen, über die der Domänencontroller eine dem früheren Exchange 5.5 vergleichbare Schnittstelle für Verzeichnisabfragen bereitstellt.

4

Exchange-Basiswissen

4 Exchange-Basiswissen

In diesem Kapitel dreht sich alles um die Exchange 2003-Konzepte. Zwar sind die Exchange 2003-Assistenten bei der Installation sehr hilfreich und ausführlich, aber ohne ein Grundverständnis über Server und Komponenten kann weder Installation noch Betrieb in der Praxis erfolgen. Bevor Sie nun den ersten Exchange-Server installieren, sollten Sie damit vertraut sein, wie bestimmte Komponenten ineinander greifen und welche Voraussetzungen für die Funktion notwendig sind. Bei der Installation werden wichtige Einstellungen festgelegt, die Grundlage des Systems sind und später nicht mehr einfach geändert werden können.

Namensgebung

Konkret ist hier der Name der Organisation eines der Kriterien, die ohne komplette Neuinstallation aller Exchange-Server in einem Forest nicht zu ändern ist. Sie sollten einen Namen wählen, der auch eine Erweiterung der Exchange-Umgebung zulässt. In großen Unternehmen bildet häufig der Organisationsname den Konzernnamen ab und lässt somit eine offene Struktur für die Integration weiterer Unternehmen zu.

Im Anschluss an dieses Kapitel sollten Sie in der Lage sein, eine Exchange-Infrastruktur für ein klein- und mittelständisches Unternehmen zu entwerfen. Hinweise für den Enterprise-Bereich finden Sie im Teil III.

4.1 Organisation und SMTP-Domänen

Verbund von Mailservern

Exchange 2003 ist ein Client-/Server-Messaging-System, das aus einem ganzen Verbund von Servern bestehen kann. Diese Verbindung der Systeme für Messaging und Personal Information Management wird auch als Organisation bezeichnet. Über ausgeklügelte Mechanismen stellen sich alle Server wie ein einziges Verbundsystem dar.

Im Gegensatz zu anderen E-Mail-Systemen bringt eine Organisation viele Vorteile:

Vorzüge einer Organisation

- Alle Server in der Organisation bedienen die gleiche SMTP-Domäne, die unterschiedlich zum Namen des Active Directory sein kann. Weitere hinzugefügte SMTP-Domänen werden von allen Servern im Verbund bedient.
- Alle Server nutzen die gleichen Adresslisten, das heißt, es gibt keinen Unterschied zwischen lokalen Anwendern und Anwendern auf anderen Servern.

- Sie können Benutzer von einem Server zum anderen Server verschieben, inklusive Übernahme der E-Mail-Adresse des Anwenders und seiner Rechte.
- Verteiler sind unabhängig vom Exchange-Server zu pflegen.
- Informationen in Öffentlichen Ordnern können auf mehrere Server repliziert werden und allen Mitarbeitern zu Verfügung stehen.
- Alle Server untereinander kennen die Verbindungen und können die Route der Nachrichten optimieren. Ausfälle in Verbindungen werden erkannt und Umwege berechnet.

Dies sind nur einige Punkte, die praktisch deutlich machen, wie flexibel und skalierbar Exchange 2003 ist. Eine Exchange-Organisation ist also eine Gruppe von Servern, die zu einer Einheit zusammengefasst sind. Diese Ansicht gibt es schon seit der ersten Version von Exchange 4.0.

AD-Forest = Exchange-Organisation

Neu mit Exchange 2003 ist hingegen, dass ein Active Directory-Forest zugleich auch die Exchange-Organisation umfasst. In einem Forest kann es nur genau eine Exchange-Organisation geben. Eine Exchange-Organisation in einem Forest kann darüber hinaus auch Personen bedienen, die in einer vertrauten NT4-Domäne oder in einem anderen Forest sind. Aufgrund der Konfigurationspartition des Active Directory, die die Exchange-Infrastruktur beherbergt, müssen alle Exchange-Server in diesem Forest installiert sein.

Durch diesen Denkansatz unterscheidet sich Exchange von den meisten anderen E-Mail-Systemen, die in der Regel serverbasiert arbeiten. Für Unternehmen, die nur einen Server installieren, auf dem alle Benutzer ihr Postfach haben, würde dies ausreichend sein. Bei einer Ausbreitung über Standorte hinweg hemmt dieser Aufbau die Skalierung und Anpassung nach geografischen Gegebenheiten. Wie können Sie nun mehrere Mailserver zusammenschalten, um eine einheitliche Adressliste zu kreieren, die untereinander ausgetauscht wird?

Einheitlicher SMTP-Adressraum

Unabhängig vom Namen des Active Directory ist die SMTP-Domäne, als Teil der E-Mail-Adresse aller Empfänger im gesamten Forest. Die Domäne des Benutzers ist ebenfalls kein Kriterium, auf welchem Exchange-Server das Postfach angelegt wird. Exchange nutzt domänenübergreifend den gleichen SMTP-Adressraum. Somit bleibt auch die E-Mail-Adresse des Benutzers bestehen, selbst wenn dieser in eine andere Niederlassung umzieht. Wettbewerber, die keine globale Adresse nutzen können, erkennen Sie häufig an einer SMTP-Domäne, die eine geografische Aufteilung vermuten lässt (z.B.: name@de.firma.com).

Halten wir fest:

- Die Wahl der SMTP-Adressen für alle Benutzer in einem Forest ist unabhängig vom Server und von der Domäne, auf dem bzw. in der das Postfach liegt.
- Es gibt genau eine Organisation in einem Forest – eine Organisation kann auch nur in einem Forest existieren.
- Der Domänenname der Active Directory-Domänen ist unabhängig von den SMTP-Adressen.
- Eine Exchange-Organisation beschreibt eine Gruppe von Exchange-Servern, die als Verbund zusammengeschaltet sind und eine gemeinsame Konfigurationsbasis und Benutzerinformationen nutzen.

4.2 Exchange-Komponenten und -Dienste

Einige Grundlagen sind unerlässlich, und ein generelles Verständnis über die Zusammenhänge elementarster Dienste und Komponenten erleichtert Ihnen die Tätigkeit mit Exchange 2003.

- SMTP-Service

Simple Mail Transfer Protocol

Das Herzstück des Nachrichtenverkehrs ist der SMTP-Dienst von Microsoft Windows 2003. SMTP ist nicht nur sehr stark verbreitet, das Protokoll ist auch wesentlich leistungsstärker als X.400 unter Exchange 5.5, und zwar bis zu 300 % schneller. Der virtuelle SMTP-Server ist einfach zu konfigurieren, verbirgt aber einige Tücken bezüglich der Sicherheit. Der SMTP-Connector ermöglicht eine einfache Anbindung ans Internet.

- Informationsspeicher

Information Store

Betrachten Sie den Information Store-Dienst (IS) und seine Datenbanken als wichtigste Komponenten in Exchange 2003, da nur er alleine für die Strukturierung aller Daten zuständig ist. Das Programm STORE.EXE bewerkstelligt die Zuweisung von E-Mails, Terminen, Öffentliche Ordner-Einträgen und weiterer Informationen im System.

- Private und öffentliche Daten

Public Folder und Mailbox

Der Informationsspeicher unterteilt die Daten in zwei Kategorien: privat und öffentlich. Die privaten Nachrichten werden den Postfächern der Anwender zugestellt. Die öffentlichen Daten können von vielen Benutzern gleichzeitig genutzt werden. Der Informationsspeicher besteht also aus zwei Datenbanktypen, die zusammen eine Einheit darstellen und im Outlook-Client über den MAPI-Zugriff erreichbar sind. Der öffentliche Informationsspeicher enthält alle Informationen der Öffentlichen Ordner

(Public Folder). Der Postfachspeicher (Mailbox) pflegt alle Nachrichten, die an Personen oder Gruppen in einem Postfach zugestellt werden.

- Speichergruppe

  Storage Group

  Der Informationsspeicher ist in eine Speichergruppe (Storage Group) integriert, die wiederum Postfachspeicher, Öffentlichen Informationsspeicher oder beides enthalten kann. Eine Speichergruppe ist eine Zusammenfassung mehrerer Datenbanken, die sich ein Transaktionsprotokoll teilen. Dies ist vor allem bei der Wiederherstellung wichtig. Ein Exchange-Standard-Server kann jeweils nur einen Mailbox Store und einen Public Folder Store enthalten. Im Gegensatz dazu fällt beim Enterprise-Server nicht nur das mit SP2 auf 75 GB-Limit angehobene Datenbanklimit komplett weg, sondern die Version ermöglicht auch die Verwaltung von bis zu 20 Datenbanken auf einem Server. Bis zu vier Storage Groups mit jeweils fünf Mailbox/Public Folder Stores, jedoch nur einem MAPI-Public Folder Store können auf einem Server angelegt werden. Microsoft empfiehlt die Festsetzung eines Limits pro Datenbank, das mit SP2 problemlos ermöglicht wird, und erst nach Erreichen desselben die Erweiterung um eine neue Datenbank.

  Legen Sie daher nur so viele Datenbanken an, wie Sie in absehbarer Zeit auch benötigen. Der Einsatz weiterer Speichergruppen und Datenbanken ist nur bei entsprechender Planung von Service Level Agreements, Sicherungsaufträgen, Richtlinien oder im Cluster sinnvoll.

- Systemaufsicht

  System Attendant

  Der Informationsspeicher ist abhängig von der Systemaufsicht (SA), die als Dienst in Windows 2003 realisiert ist. Mit dem Programm MAD.EXE werden viele Wartungsaufgaben ausgeführt wie die Überwachung der Dienste und Connectoren. Weiterhin startet der SA die Online-Defragmentierung des Informationsspeichers und unterstützt die MAPI-basierten Adressbuchabfrage (DSProxy) an den Globalen Katalog-Server. Im Ereignisprotokoll für Anwendungen erhalten Sie einen Überblick aller Zuständigkeiten des SA. Dieser Dienst muss auf dem Exchange-Server laufen, bevor andere Exchange-Dienste gestartet werden können.

- Internet Information Service (IIS)

  IIS

  Der IIS ist nahtlos in Exchange 2003 integriert worden und unterstützt die Protokolle SMTP, NNTP, IMAP4, POP3 und HTTP/WebDAV. Die Kommunikationsprotokolle ermöglichen folgende Funktionen: SMTP erlaubt das Senden und Empfangen von Internet-Nachrichten; NNTP stellt News über Öffentliche Ordner bereit; IMAP4 erlaubt eine Synchronisation mit dem Postfach oder Öffentlichen Ordnern; POP3 ermöglicht ein einfaches Herunterladen des Posteingangs; und HTTP stellt eine Webbrowser-Lösung für den täglichen Einsatz dar; RPC over HTTP

ermöglicht den Outlook-Zugriff über das Protokoll HTTP und ist dadurch sehr viel einfacher in Verbindung mit Firewalls zu nutzen. Viele Informationen des Exchange System-Managers (ESM) und des Internet-Service-Managers finden Sie in einer separaten IIS-Metabase statt in der Registrierung.

- Outlook Web Access (OWA)

OWA

OWA ist Teil der Standardinstallation von Exchange 2003 und erlaubt den Zugriff auf Postfach und Öffentliche Ordner über HTTP. Mit der Einrichtung von OWA werden verschiedene DLLs, Web-Seiten und Skripte eingesetzt, die letztlich zu der Ansicht von Exchange-Server-Ressourcen im Webbrowser verhelfen.

Es gibt eine ganze Reihe weiterer Dienste und Komponenten, die optional zum Einsatz kommen. Bei der Umstellung von Exchange 5.5 nach Exchange 2003 spielen der Message Transfer Agent (MTA), der Site Replication Service (SRS) und der Active Directory Connector (ADC) eine ganz besondere Rolle und werden im Kapitel „Migration“ erläutert. Ferner sind die Connectoren für MS Mail, Lotus Notes und Novell GroupWise nennenswert. Die „Real-Time Collaboration Services“ wurden mit 2003 in einen gesonderten Server ausgelagert.

4.3 Administrative Gruppen

Alle Exchange-Server nutzen die gleiche Konfigurationsinformation aus dem Active Directory. Dies bedeutet für den Administrator aber nicht, damit auch alle Exchange-Server in der Organisation administrieren zu können. Damit die Verwaltung sauber getrennt werden kann, ermöglicht Exchange 2003 die Bildung so genannter *Administrativer Gruppen* (AG). Genau genommen handelt es sich hierbei um eine Trennung der Konfiguration, damit angepasste Rechte vergeben werden können.

Administrative Groups (AG)

Der Name „Administrative Gruppe“ sagt schon einiges über den Einsatzbereich aus. Während der Serverinstallation wird eine „Erste Administrative Gruppe“ (First Administrative Group) angelegt, in die der erste Server installiert wird. Sie können weitere Administrative Gruppen definieren. In einer gemischten Exchange-Umgebung wird aus jedem Exchange 5.5-Standort eine eigene Administrative Gruppe. Mittels der Administrativen Gruppen gestalten große Unternehmen in einem Forest ihre Exchange-Organisation, so dass eine enge Zusammenarbeit der Einzelfirmen möglich ist und jeder Bereich seine eigenständige Administration erhält. Auf der Basis von Administrativen Gruppen können beispielsweise auch Richtlinien angewendet werden, die die Verwaltung vereinfachen.

Kleinere und mittlere Unternehmen verwenden in der Regel jedoch nur eine Administrative Gruppe. Ein Server kann nur über eine Neuinstallation in eine andere Administrative Gruppe verschoben werden. Postfächer hingegen können im Exchange-Native Mode problemlos von einem Server einer Administrativen Gruppe auf einen anderen Server in einer anderen Administrativen Gruppe verschoben werden. Seit Service Pack 1 steht diese Funktion mit dem *Site Consolidation Tool* auch im Exchange Mixed Mode zur Verfügung. Dabei sind jedoch einige Voraussetzungen und Abläufe zu beachten. Das Tool ist in den *Exchange Server Deployment Tools* enthalten.

Halten wir fest:

- Eine *Administrative Gruppe* stellt den Verwaltungsrahmen der Exchange-Server dar und somit Teil eines Exchange 5.5-Standortes.
- Sie können zusätzlich eigene Administrative Gruppen nach Bedarf definieren.
- Im Exchange-Native Mode können Postfächer zwischen Administrative Gruppen verschoben werden.
- Im Migrationsmodus werden die Exchange 5.5-Standorte als AG eingerichtet.
- In Administrativen Gruppen können Richtlinien angewendet werden.

4.4 Routinggruppen

High-Speed-Netzwerkbereich

Abgesehen von der Aufteilung in Administrative Gruppen, die eine Verwaltungsgrenze darstellen, ist auch eine Berücksichtigung der physikalischen Gegebenheiten notwendig. In Exchange 2003 sind dazu die Routinggruppen (RG) vorgesehen, mit denen Server an einem Standort logisch zusammengefasst werden. Alle Nachrichten zwischen Servern derselben Routinggruppe (Routing Group) werden unmittelbar direkt über SMTP versendet. Eine Exchange 2003-Routinggruppe entspricht meist einem Active Directory-Standort. Beide erwarten, dass die Server in dieser Einheit ohne Beschränkungen miteinander kommunizieren können.

Die altbekannte Standortgrenze unter Exchange 5.5 wurde nach ihren Aufgaben in Administrative Gruppen und Routinggruppen aufgelöst. Aufgrund der geografischen Lage wurden in Exchange 5.5 Standorte aufgebaut, die nicht nur von der Verwaltung abhängig waren, sondern auch von den schmal-bandigen WAN-Leitungen. Der Nachrichtenaustausch über RPC innerhalb der Standorte erlaubte keine Kontrollmöglichkeit. Zumeist unterliegt die Verantwortung der Exchange-Server einer Gruppe von Administra-

toren, die einen Teil der Berechtigungen an den Standort der Niederlassungen abtreten musste.

Im Exchange 2003-Native Mode sprengen Routinggruppen die Grenzen der Administrativen Gruppe und können komplett unabhängig eingerichtet werden. Im praktischen Fall bedeutet dies, Sie können für jeden Geschäftsbereich eine Administrative Gruppe einrichten, die von einer einzigen Routinggruppe umspannt werden. Im anderen Fall ist eine Zusammenfassung aller 20 Niederlassungen in eine Administrative Gruppe möglich, die pro Niederlassung über eine Routinggruppe verfügt, also 20 Routinggruppen. Ein sicherlich etwas konstruierter Fall ist die Aufteilung nach Produktgruppen. Am Beispiel eines Fahrzeugherstellers wird in drei Bereiche unterteilt, LKW, PKW und Zweirad, die an fünf verschiedenen Produktionsstätten produziert werden. Aufgrund der Verwaltung besitzt jede Produktgruppe einen eigenen Exchange-Server an allen Standorten. Für Exchange 5.5 konnte dies nur mittels 15 eigenen Exchange-Standorten realisiert werden. In Exchange 2003 wird für jede Produktgruppe eine Administrative Gruppe benötigt, also insgesamt drei. Die Routinggruppen werden pro Standort eingerichtet und umfassen jeweils einen Server für LKW, PKW und Zweiräder.

Alternative: Ein Konzern, der sich aus vielen kleinen eigenständigen Firmen zusammensetzt, nutzt global Exchange als E-Mail-System. Beispielsweise befinden sich in Hamburg und München jeweils drei kleine Gesellschaften, die für ihre Exchange-Server selbst zuständig sind. Von diesen Gesellschaften fusioniert eine in Hamburg mit einer in München. Die Administrationsfreiheit soll weiterhin bei den Gesellschaften bleiben. Was in Exchange 5.5 nun mit insgesamt sechs Standorten umzusetzen war, wird in Exchange 2003 stark vereinfacht. Aufgrund der Verwaltung können nun fünf Administrative Gruppen erstellt werden, und die Verbindung untereinander findet mit einem Connector zwischen nur zwei Routinggruppen statt.

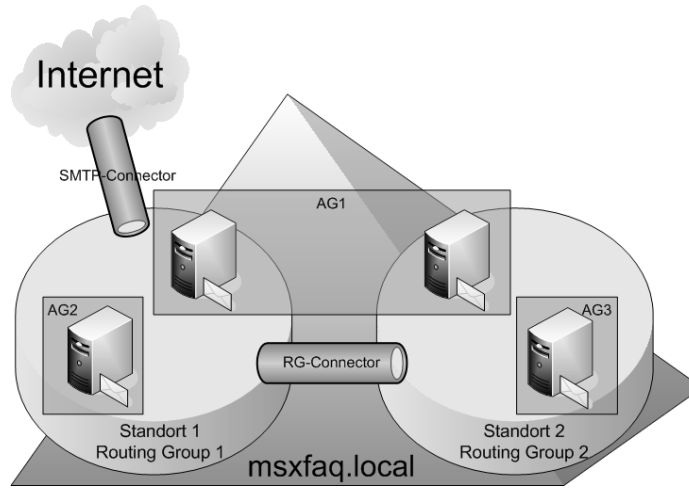


Abbildung 4.1 Administrative Gruppen und Routinggruppen

Dies gilt jedoch nicht im gemischten Betriebsmodus mit Exchange 5.5. Hier kann eine Routinggruppe nur Server innerhalb einer Administrativen Gruppe beinhalten. Allerdings können mehrere Routinggruppen in einer AG eingerichtet werden.

Connectoren

Zur Verbindung von Routinggruppen und Steuerung der Übermittlung von Nachrichten dienen Connectoren. Ohne die Einrichtung von Connectoren zwischen Routinggruppen werden keine Nachrichten ausgetauscht. Die Verbindung kann mittels eines Routinggruppen- oder eines X.400-Connectors oder via SMTP-Connector hergestellt werden.

Halten wir fest:

- Routinggruppen fassen Server an einem Standort zusammen, damit diese direkt miteinander Nachrichten austauschen. Die Definition entspricht häufig der Definition der Standorte im Active Directory.
- Die RG werden entsprechend den WAN-Leitungen mit Connectoren verbunden. Diese Verbindungen entsprechen meist den Verbindungsvereinbarungen (Site-Connector) zur Replikation im AD.
- Bevorzugter Connector ist der Routinggruppen-Connector. Dieser verbindet gleich mehrere Server zweier Routinggruppen redundant miteinander auf Basis von SMTP.
- Die meisten Unternehmen werden eine Administrative Gruppe mit einer oder mehreren Routinggruppen einsetzen.
- Bei einer Migration von Exchange 5.5 wird für jeden vorhandenen Standort eine Administrative Gruppe angelegt.
- Ein Server kann immer nur in genau einer Administrativen Gruppe und genau einer Routinggruppe sein.

4.5 Exchange und das Active Directory

Die Bedeutsamkeit des Active Directory als Grundlage für Exchange haben Sie bereits in den Active Directory-Konzepten gelesen.

AD-Integration

Hier finden Sie die Informationen, wie Exchange 2003 das Active Directory für seine Zwecke vorbereitet, aber vor allem auch, wie die Exchange-Server das Active Directory im Betrieb nutzen. Dieses Wissen ist notwendig, um später bei Fehlern und Performance-Problemen die Ursache einzukreisen und andererseits die Planung Ihrer Domänencontroller zu unterstützen. Gerade in größeren Unternehmen mit getrenntem Administrationsbereich für Exchange und das Active Directory ist es wichtig, dass beide ausreichend Know-how über den Tätigkeitsbereich der anderen Gruppen haben.

In umfangreicheren Exchange 5.5-Umgebungen wurden die Aufgaben des E-Mail-Systems von der Domänenadministration getrennt, ein enger Kontakt war nicht erforderlich. Beide Systeme konnten relativ unabhängig voneinander existieren, Fehler sehr einfach einer Gruppe zugeordnet werden. Mit Exchange 2003 ist dies durch die intensive Nutzung des Active Directory nicht mehr so einfach möglich.

4.5.1 ForestPrep

Schema-Update

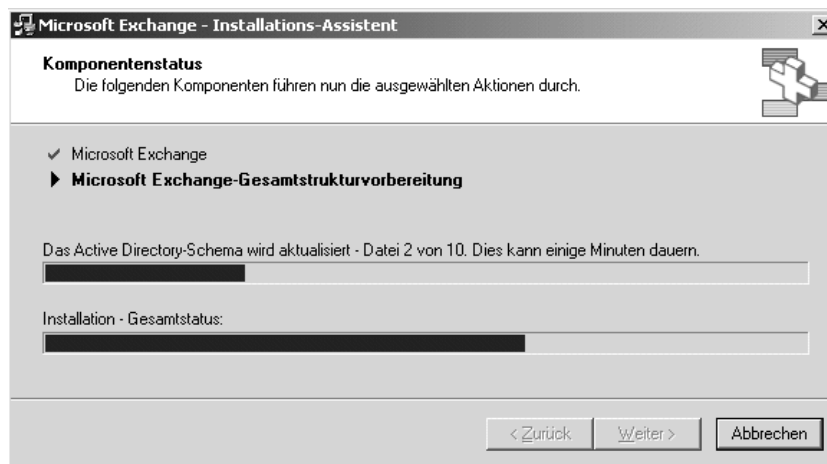
Der erste Schritt in Richtung Exchange 2003 ist die Erweiterung des Schemas um die Exchange-spezifischen Klassen und Attribute. Dafür werden die Rechte folgender Administratoren vorausgesetzt: Unternehmensadministrator, Schemaadministrator, Domänenadministrator, Administrator des lokalen Computers (bei DC nicht nötig). Ebenso muss das AD „richtig" funktionieren, das heißt, per DNS muss die Installationsroutine den Schema-Master (FSMO-Rolle) finden und im Netzwerk erreichen können. Die Installationsroutine erweitert alsdann das Schema durch den Import mehrerer LDIF-Dateien. Dieser Prozess dauert in der Regel einige Minuten auf dem aktiven Server. Anschließend müssen die Änderungen auch auf alle anderen Domänencontroller im Forest repliziert werden. Den Status der Replikation können Sie mit dem Replikationsmonitor (REPLMON.EXE) aus dem Windows Support-Tool überprüfen.

Die Erweiterung ist ein einmaliger Prozess, der auch unabhängig vom Exchange-Setup ausgeführt werden kann. Der Aufruf von

```
setup /forestprep
```

startet diese Aktualisierung. Sollte das Schema bei der Installation von Exchange noch nicht aktuell sein, führt das Setup diesen Schritt automatisch durch. Die Rechte für Schema und Organisation sollten Sie danach entfernen.

Abbildung 4.2 ForestPrep



ForestPrep erweitert nicht nur das Schema, sondern konfiguriert auch die ersten Einträge für die Exchange-Organisation im Active Directory:

- Hinzufügen aller Exchange-Attribute und -Klassen im AD-Schema.
- Anlegen des Exchange-Organisationsobjekts im Active Directory (Configuration-Partition\Services\Microsoft Exchange).
- Setzen der Basisberechtigungen des ersten Exchange-Administrators

Der Name der Organisation wird hier noch nicht erfragt, die Einträge erhalten einen zufälligen Namen, bis der erste Exchange 2003-Server in die Organisation installiert wird.

Die Änderungen der Ausführung von ForestPrep im Active Directory könnten Sie mit der Management-Konsole für Standorte und Dienste oder mit *ADSI Edit* betrachten. Mit den genügenden Rechten könnten Sie auch hier die Veränderungen vornehmen. Davon ist aber dringend abzuraten. Nutzen Sie später nur den Exchange System-Manager zur Konfiguration von Exchange 2003!

„Remove Organization“

Einmal „ForestPrep“ ausgeführt, lassen sich die Schema-Erweiterungen nicht mehr entfernen, wohl aber die Exchange-Konfigurationseinstellung. Hierzu können Sie das Exchange-Setup mit dem Parameter „removeorg“ aufrufen (`setup /removeorg`). Starten Sie den Aufruf nur dann, wenn die komplette Organisation neu aufgesetzt und alle bisherigen Exchange-Server deinstalliert werden. Der Parameter „removeorg“ ist erst ab SP 1 (update.exe) enthalten.

Halten wir fest:

- Das Schema des Active Directory wird um Attribute und Klassen für Exchange erweitert.
- Diese Erweiterung muss der Schema-Administrator einmalig für den gesamten Forest durchführen.
- Die Konfigurationen können Sie mit „removeorg“ zurücknehmen, das Schema bleibt bestehen.

4.5.2 DomainPrep

Nachdem das Schema erweitert wurde, muss die Domäne, in der Exchange 2003 installiert werden soll, entsprechend vorbereitet werden. Auch diesen Schritt kann man manuell ausführen, und zwar als Domänenadministrator. Für die Exchange-Installation ist dieser Benutzer dann nicht mehr notwendig. Sie sehen, dass Exchange 2003 auf große Organisationen mit verteilten administrativen Funktionen vorbereitet ist.

```
SETUP /domainprep
```

startet diesen Prozess, der je Domäne im Forest zu wiederholen ist. Das Exchange-Setup prüft für die aktuelle Domäne die Voraussetzungen und führt gegebenenfalls DomainPrep eigenständig durch. Dabei werden Gruppen erstellt und Berechtigungen eingerichtet, die der Exchange-Server zum Bearbeiten der Attribute benötigt:

Vorbereitungen für Exchange 2003

- Anlegen der spezifischen globalen Sicherheitsgruppe „Exchange Domain Servers“ und der lokalen Sicherheitsgruppe „Exchange Enterprise Servers“ in der OU „Users“. Bitte verschieben Sie diese Gruppen nie in eine andere OU.
- Aufnehmen der „Exchange Domain Servers“-Gruppe in die „Exchange Enterprise Servers“-Gruppe.
- Vergeben verschiedener Zugriffsberechtigungen für die „Exchange Enterprise Servers“-Gruppe auf das Domänenobjekt, damit der Empfängeraktualisierungsdienst ausgeführt werden kann.
- Anpassen der Berechtigungen der Gruppe „Exchange Enterprise Servers“ auf das Objekt „AdminSDHolder“.
- Anlegen des „Microsoft Exchange System Objects“-Containers unterhalb der Domäne. (Versteckt und nur in der erweiterten Ansicht sichtbar!)

Beim Einsatz mehrerer Domänen müssen Sie neben dem DomainPrep später auch den Empfängeraktualisierungsdienst von Exchange konfigurieren.

Halten wir fest:

- DomainPrep wird einmal pro Domäne ausgeführt, in der sich Exchange-Server und Objekte befinden (Benutzer, Kontakte, Gruppen, Administratoren).
- DomainPrep legt eine OU für Exchange an sowie einige Gruppen.
- DomainPrep vergibt Rechte, damit jeder Exchange-Server die Empfänger auflösen und anpassen kann.

4.5.3 Exchange 2003-Zugriffe auf AD

Nach der Vorbereitung des Active Directory werden durch die Exchange-Installation weitere Informationen in das Active Directory geschrieben. Dazu gehören die Server und die verfügbaren Datenbanken, die Adressierungsrichtlinien für die Bildung von E-Mail-Adressen und die Connectoren für den Nachrichtenaustausch. Durch das Anlegen von Postfächern und Verteilern werden bei den Anwendern der Domänen die Felder mit Informationen gefüllt. Es gibt nun gleich mehrere Prozesse, die nach der Installation auf diese Informationen im Active Directory zugreifen.

- SMTP-Server und Empfängerrichtlinien

  SMTP-Adressen als Zugangsschleuse für eingehende Mails

  Die Empfängerrichtlinien beschreiben, nach welchen Regeln die Standard-E-Mail-Adressen unter anderem für Benutzer und Verteiler erstellt werden. Zudem definieren sie, welche SMTP-Adressräume überhaupt in der Exchange-Organisation gültig sind. Genau diese Informationen lesen die virtuellen SMTP-Server aus, um schon beim Empfang der Nachricht die Existenz der Empfängerdomäne zu erkennen. Exchange 2003 lehnt bereits beim Empfang nicht definierte Empfängerdomänen ab.

- Recipient Update Service (RUS)

  Recipient Update Service pflegt Adresslisten

  Der Empfängeraktualisierungsdienst erzeugt und pflegt die Adresslisten und aktualisiert alle Änderungen, die an den Empfängerrichtlinien durchgeführt wurden. Durch den Dienst erhalten neue Empfänger ihre E-Mail-Adressen, und bei existenten Empfängern wird die Adressaktualisierung mittels der Empfängerrichtlinien sichergestellt. Der RUS garantiert somit brandaktuelle Adressinformationen ohne großen Verwaltungsaufwand. Voraussetzung dafür ist eine Empfängerrichtlinie pro Domäne im Forest, in der sich E-Mail-Benutzer befinden.

- Nachrichten-Routing (Mailrouting)

  Der Weg einer E-Mail

  Der weitaus größte Anteil an Active Directory-Zugriffen erfolgt über das Mailrouting. Jede Nachricht, die von einem Exchange-Server verarbeitet wird, veranlasst eine Abfrage, wohin diese Nachricht überhaupt gesendet werden muss. Dazu ermittelt der Server über den Globalen Katalog den Home-Server des Empfängers und über die Routing-Schnittstelle die nächste Station auf dem Weg dorthin. Dementsprechend bedeutet jede Nachricht eine oder mehrere Anfragen an das Active Directory.

- Information Store und Client-Zugriff

  Damit Clients wie Outlook, Outlook Web Access, POP3- und IMAP4-Programme auf das Postfach zugreifen dürfen, überprüft Exchange, ob der Benutzer die entsprechenden Rechte im IS besitzt. Die Rechte sind seit Exchange 2000 an die SIDs der Benutzer und Gruppen gebunden.

Abfrage-Cache

Die enge Einbindung in das Active Directory erfordert auch einen ständigen Zugriff auf die Verzeichnisinformationen, die vom Verzeichnissuchdienst (DSAccess) von Exchange koordiniert werden. Alle Serverprozesse nutzen diese Komponente. DSAccess ist dafür zuständig, die netztechnisch nahe stehenden Domänencontroller zu ermitteln und die Daten zu erfragen. Die ermittelten Daten werden einige Zeit im Cache gehalten. Für die Anfragen von älteren Outlook-Clients bietet der Exchange-Server weiterhin einen Verzeichnisdienstproxy (DSPROXY) an, der die Anfragen des Clients auf das Active Directory umleitet. Genau dieser Cache kann natürlich auch

kontraproduktiv sein, da Einträge nicht sofort bekannt werden. Diesen Cache können Sie mit dem Programm DSCFLUSH (Exchange CD) leeren.

Auf der anderen Seite sollten Sie die Verfügbarkeit der Dienste nicht von einem einzigen Domänencontroller abhängig machen. Sobald eine bestimmte Größe erreicht ist, sollten Sie mindestens zwei oder drei Domänencontroller einsetzen. Es gilt zu verhindern, dass ein Ausfall oder eine geplante Downtime, z.B. durch die Installation eines Service-Packs, möglicherweise die gesamte Firma „lahm“ legt.

Bei kleinen Firmen mit einem Server ist dieser zugleich Domänencontroller und Exchange-Server. Wenn Sie nur wenige Server haben, dann sollten Sie mindestens zwei Domänencontroller betreiben, auch wenn einer davon zugleich der Exchange-Server ist. Größere Installationen sollten über dedizierte Domänencontroller nachdenken, damit alle Dienstserver als Mitgliedsserver (Member Server) installiert werden können. Zudem sollten einige Domänencontroller auch den Globalen Katalog bereitstellen. Da Exchange sich an den Active Directory-Standorten orientiert, sollten Sie auch IP-Subnetze und Standorte im Active Directory pflegen.

Halten wir fest:

- Exchange 2003 nutzt das Active Directory sehr intensiv.
- Durch Empfängerrichtlinien wird die E-Mail-Domäne eingerichtet, für die Exchange eingehende Nachrichten annimmt.
- Wenn Sie über keinen Empfängeraktualisierungsdienst für eine Active Directory-Domäne verfügen, können Sie in dieser Domäne keine Empfänger erstellen.
- Ein Exchange 2003-Server sollte mindestens einen, besser zwei Globale Katalog-Server im gleichen Standort finden.
- Bei unzureichenden AD-Servern kann auch der Exchange-Server zum Domänencontroller werden.
- Pflegen Sie die Subnetze im Active Directory, damit die Exchange-Server auch die netztechnisch günstigen Domänencontroller ansprechen.

4.5.4 Globaler Katalog und NSPI

Bei den Active Directory-Konzepten wurde schon erläutert, wie unentbehrlich die Funktion des Globalen Katalogs für das Active Directory ist. Durch den Einsatz von Exchange 2003 erhält diese Funktion einen sehr hohen Stellenwert in Ihrem Unternehmen. Die meisten Betriebe sehen heute die Funktion des Nachrichtensystems als unternehmenskritisch an. Wenn Ihr

Exchange-Server keinen Globalen Katalog erreicht, ist das Routen von Nachrichten erheblich gestört.

Für Exchange 2003 ist der Globale Katalog die Informationsquelle über alle in der Exchange-Organisation erreichbaren Empfänger und Server. Für jede Nachricht des Mailservers wird die Adresse des Empfängers im Active Directory abgefragt, um den dazugehörigen Postfachserver zu erhalten.

Ganz so kritisch ist dieses Zugriffsverhalten indessen nicht, da Exchange mittels DSPROXY viele Anfragen aus einem lokalen Cache bedient. Aber je größer die Exchange-Organisation wird, desto häufiger muss auch der Exchange-Server direkt auf den Globalen Katalog zurückgreifen.

DSPROXY-Verbesserungen

Service Pack 2 optimiert das bisherige DSProxy-Verhalten. Einige Probleme bereiteten die Domänen-übergreifende Vergabe von Stellvertreterberechtigungen sowie die Pflege von Gruppenmitgliedschaften innerhalb eines Forest, da der DSProxy nur den GC der aktuellen Domäne abfragte. Mittels eines fünfstufigen Algorithmus findet der Dienst nun den für die entsprechende Domäne zuständigen Globalen Katalog Server. Allerdings kann dieser bei ungünstiger Konstellation auch in einem anderen Standort installiert sein. Auch die Veröffentlichung von Zertifikaten – sowohl für die E-Mail-Verschlüsselung sowie zur digitalen Unterschrift durch den Client – wird mit dem aktualisierten DSProxy-Dienst unterstützt.

Welche Server von Exchange 2003 tatsächlich benutzt werden, können Sie im Exchange System-Manager kontrollieren.

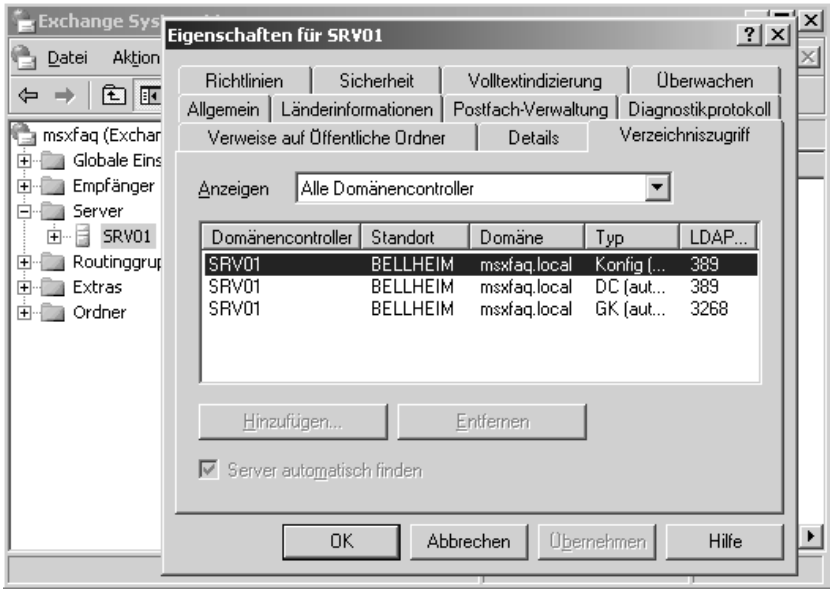


Abbildung 4.3 Verzeichniszugriff des Servers

Eine weitere Besonderheit beim Einsatz von Exchange ist die NSPI-Schnittstelle (Name Service Provider Interface). Über diese Schnittstelle greifen Anwendungen wie ältere Outlook- und Exchange-Clients etc. auf das Adressbuch von Exchange zu. Mit dem Wegfall der Exchange 5.x-Verzeichnisdatenbank DIR.EDB übernehmen teilweise Exchange 2003-Server und die Domänencontroller diese Funktion.

Der Outlook-Client strebt die ständige Verbindung mit dem Postfach auf dem Exchange-Server an und versucht die Namen im Adressbuch aufzulösen. Abhängig von der Version des Clients wird die Anfrage beantwortet.

Tabelle 4.1 Anmelde-verhalten

Client Version	Prozess
Exchange-Client 4.0 Exchange-Client 5.0 Outlook 97 Outlook 98	Der Exchange-Server leitet die Anfrage an den Globalen Katalog weiter. Dies bedeutet im Einzelnen: - Der Client stellt eine Anfrage an den Exchange-Server. - Der Exchange-Server fragt den GC und erhält eine Antwort. - Der Exchange-Server leitet diese dem Client zu. - Die Quittung des Clients wird vom Exchange-Server wieder an den GC weitergeleitet.
Outlook 2000	Ab Outlook 2000 und höher sendet der Exchange-Server eine Weiterleitung an Outlook zurück. Outlook erhält eine Liste der Globalen Kataloge und wählt selbst einen Server aus, den Outlook zukünftig anspricht. Leider speichert Outlook 2000 diesen Server im Profil mit ab. Wird der Domänencontroller später deinstalliert oder ist nicht verfügbar, dann kann Outlook sich nicht mehr verbinden. Hier hilft die Neuanlage des Profils oder das Löschen des Schlüssels in der Registrierung.
Outlook 2000 SR2 Outlook 2002 Outlook 2003	Die neueren Versionen von Outlook wurden dahingehend verbessert, dass bei Nichterreichbarkeit des Globalen Katalogs ein neuer Server gefragt wird.

Ist der Exchange 2003-Server allerdings selbst Globaler Katalog, dann werden die Anfragen nicht weitergeleitet. Dies stellt die Systemaufsicht beim Start fest.

Update DC zum GC erfordert Neustart

Wenn ein Domänencontroller nachträglich zum Globalen Katalog konfiguriert wird, dann müssen Sie den Domänencontroller nach der Replikation neu starten. Das Active Directory lädt nur beim Neustart die NSPI.DLL nach, damit der Server auch die NSPI-Schnittstelle unterstützt.

Halten wir fest:

- Die Erreichbarkeit eines Globalen Katalogs ist für die Funktion von Exchange zwingend notwendig.

- Je größer das Nachrichtenaufkommen und die Anzahl der Empfänger ist, desto mehr wird der Globale Katalog von Exchange in Anspruch genommen.
- Wird ein Domänencontroller nachträglich zum GC gemacht, muss der Domänencontroller nach erfolgter Replikation neu gestartet werden.
- Ein Exchange-Server sollte nicht nachträglich zum Domänencontroller hochgestuft bzw. zum Member-Server heruntergestuft werden.

4.5.5 Exchange-Systemgruppen

Durch die Installation von Exchange 2003 und die Vorbereitung der Domänen mittels DOMAINPREP werden in jeder Domäne spezifische Gruppen angelegt:

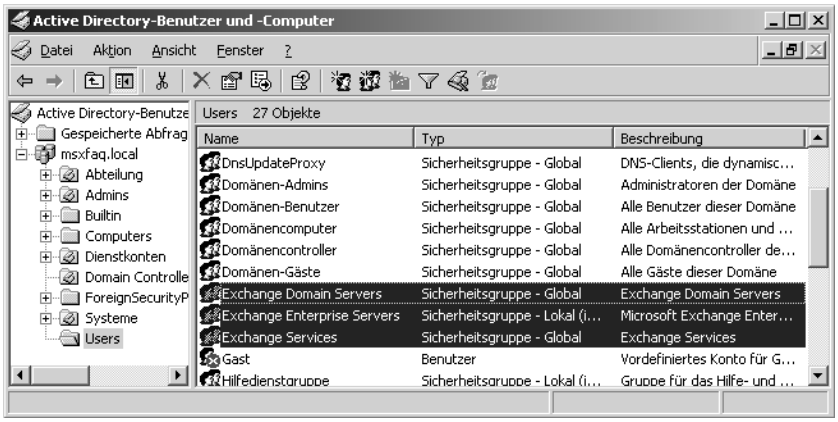


Abbildung 4.4 Exchange-Domänen-Gruppen

Exchange Domain Servers (Global)

Globale Server-Gruppe

Diese globale Gruppe enthält alle Exchange-Server, die in dieser Domäne installiert sind. Mittels der Zusammenfassung in eine globale Gruppe pro Domäne kann diese Gruppe später in anderen lokalen Gruppen der gleichen oder anderer Domänen hinzugefügt werden.

Exchange Enterprise Servers (Domain Lokal)

Lokale Gruppe für Berechtigungen

Diese lokale Gruppe enthält alle globalen Gruppen „Exchange Domain Servers“ des gesamten Forests. Während der Installation des ersten Exchange-Servers wird die Gruppe an vielen Stellen der Konfiguration in die Berechtigungen eingetragen. Damit erhalten auch die Mitglieder dieser Gruppe die Berechtigungen. Auch die weiteren Installationen erfordern diese Gruppe, die nicht verschoben werden darf.

Exchange Services (Global)

Kompatibilität zu Exchange 5.5

Bei der Migration von Exchange 5.5 in der gleichen Organisation wird diese zusätzliche Gruppe angelegt, die Rechte in der Exchange-Konfiguration erhält. Mitglied dieser Gruppe ist z.B. das Exchange 5.5-Dienstkonto. Bei der Migration nach Exchange 2003 ist die zuvor in das AD geschobene Gruppe sehr hilfreich, da dort die Konten enthalten sind, mit denen der Zugriff auf Exchange 5.5 möglich ist.

Exchange-Administrator-Gruppen

Gruppe für administrativen Zugriff

Zusätzlich zu den Exchange-Gruppen sollten größere Firmen überlegen, weitere Gruppen für die Zuweisung von Rechten anzulegen. Vermeiden Sie es z.B. auf Administrative Gruppen, einzelnen Personen Rechte zu geben. Wird der Anwender später gelöscht oder erhält andere Aufgaben, müssen Sie mühselig die Rechte wieder entfernen. Daher sollten Sie immer nur Gruppen als berechtigt eintragen und über die Mitgliedschaften den Mitarbeitern den Zugriff erlauben.

Diese Konstruktion hat sich in der Praxis sehr bewährt, um nicht die notwendigen Berechtigungen auf allen Servern für die Objekte einzeln zu pflegen. Dadurch wird die Zugriffssteuerungsliste (ACL) übersichtlich gehalten. Microsoft folgt selbst dem Prinzip, Berechtigungen über Gruppen zu vergeben, die auch verschachtelt sein können.

Verändern Sie möglichst nicht diese System-Gruppen, und legen Sie auch keine gleichnamigen Gruppen manuell an. Eine Änderung der Mitgliedschaften oder Verschiebung in eine andere Organisationseinheit bewirkt, dass die Exchange-Systemaufsicht dies permanent im Eventlog meldet und eine weitere Installation von Exchange-Servern nicht möglich ist. Im „Exchange Server Setup Progress.log“ findet sich folgende Fehlermeldung dazu:

Listing 4.1 Auszug: Exchange Server Setup Progress

```
[12:59:49] Leaving ScIsDomainPrepped
[12:59:49] Entering ScGetExchangeServerGroups
[12:59:49] Getting DOB for group 0
[12:59:49] ScGetExchangeServerGroups
(K:\admin\src\libs\exsetup\dsmisc.cxx:301)
Error code 0X80072030 (8240): Ein solches Objekt ist auf dem
Server nicht vorhanden.
```

4.6 Native Mode und Mixed Mode

Auch Exchange kennt ähnlich dem Active Directory verschiedene Betriebsarten. Der Unterschied der Betriebsart zwischen dem gemischten Modus (Mixed Mode) und dem einheitlichen Modus (Native Mode) ist im

Vergleich zum Active Directory sehr viel größer. Solange noch Exchange-Server der Version 5.5 in der gleichen Organisation eingesetzt werden, ist ein Wechsel zum einheitlichen Modus nicht möglich. Jedoch hat dieser einige Einschränkungen, die einen schnellen Wechsel zum Native Mode erstrebenswert gestalten.

Einschränkungen Mixed Mode

- Die Administrativen Gruppen sind nur in der gleichen Weise wie die Exchange 5.5-Standorte zu handhaben, also in einer 1:1-Beziehung.
- Sie können Postfächer zwischen den Servern in unterschiedlichen Administrativen Gruppen nur mittels *Site Consolidation Feature* aus Exchange Service Pack 1 verschieben.
- Eine Administrative Gruppe kann mehrere Routinggruppen überspannen, eine Routinggruppe ist jedoch nur in derselben AG möglich.

Aktivierung Native Mode

Die Umschaltung in den Native Mode erlaubt die Nutzung einiger interessanter Funktionen. Diese neuen Möglichkeiten müssen jedoch auch bei der Planung und späteren Umsetzung berücksichtigt werden.

- Die Benutzer können problemlos auf einem Server zwischen den unterschiedlichen Administrativen Gruppen verschoben werden.
- Routinggruppen sind nicht mehr auf Administrative Gruppen beschränkt, sondern komplett losgelöst. Server verschiedener Administrativer Gruppen können in der gleichen Routinggruppe sein.
- Es können keine Exchange 5.5-Server mehr in der Organisation installiert und betrieben werden. Damit entfällt auch die Notwendigkeit für den SRS-Dienst und den Active Directory Connector.
- Die Umschaltung in den einheitlichen Modus erfolgt auf Ebene der Organisation und kann nicht mehr rückgängig gemacht werden. Der Assistent überprüft dabei, ob alle Voraussetzungen für die Umschaltung vorliegen. Somit wird eine vorschnelle native Aktivierung verhindert.
- Nur im Native Mode von Exchange mit Windows 2003 sind abfragebasierte Verteiler möglich.

Exchange wird immer im gemischten Modus installiert. Die Umschaltung in den einheitlichen Modus muss manuell über den Exchange System-Manager erfolgen. In den Eigenschaften der Organisation kann der Wechsel durchgeführt werden.

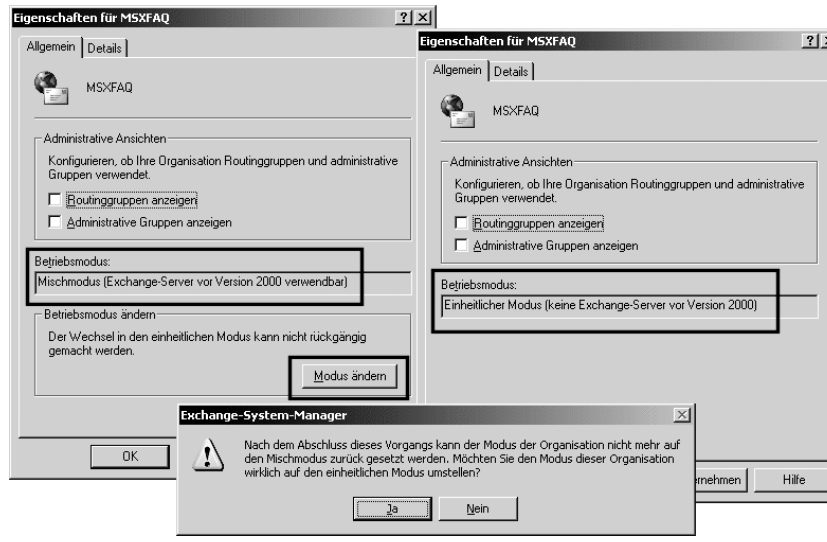


Abbildung 4.5 Exchange-Wechsel in den Native Mode

Zum Thema der Umschaltung in den Native Mode finden Sie sehr viele weiterführende und detaillierte Artikel in TechNet und Dokumentation. Einige davon sind:

- Q270143 XADM: Mixed Mode vs. Native Mode
- Q272314 XADM: Preparing a Mixed Mode Organization for Conversion to Native Mode
- Q280787 XADM: Benefits and Limitations of a Mixed Mode Environment
- Q281088 XADM: When to Change an Exchange Organization to Native Mode

Halten wir fest:

- Der einheitliche Modus ist nur für die gesamte Exchange-Organisation aktivierbar und nicht widerrufbar.
- Die Routinggruppen können optimal auf die physikalische Netzwerkstruktur angepasst werden, ohne auf Administrative Grenzen Rücksicht zu nehmen.
- Benutzer können zwischen Administrativen Gruppen verschoben werden.
- Server können NICHT zwischen Administrativen Gruppen verschoben werden.

4.7 Berechtigungen

Ein großes Kapitel bei der Planung und Umsetzung von Microsoft Exchange ist das Verständnis der verschiedenen Wege, Rechte zu erhalten oder zu verweigern. Genauso wie der Zugriff für den Anwender auf sein Postfach gesteuert wird, muss auch gewährleistet werden, dass kein anderer Benutzer auf den Inhalt des Postfachs zugreifen kann, sofern ihm die Rechte dazu fehlen. Dann stellt sich aber auch die Frage, woher der Anwender das Recht hat, Berechtigungen auf sein Postfach zu vergeben.

Allow, Deny, Inherited

Hier ist nun der Zeitpunkt erreicht, die Berechtigung für Benutzer und Gruppen zu klären. Auf welche Objekte darf zugegriffen werden, und welche Felder sind einbezogen? Sie sollten auch die Auswirkungen der Aktivierung von „Zulassen“ (allow) oder „Verweigern“ (deny) kennen genauso wie bei der Vererbung (inherited).

Im Gegensatz zu Exchange 5.5, bei dem die Rechte mit dem Verzeichnisnamen (Exchange 5.5-Objektbezeichnung) des Benutzers verbunden waren, setzt Exchange 2003 komplett auf die Verwaltung der SIDs im Active Directory. Die SID stellt den primären Schlüssel dar, an den alle Rechte gekoppelt sind. Stellen Sie sich die Auswirkungen für Exchange in Verbindung mit dem Active Directory vor, wenn keine SID vorhanden wäre. Jedes Objekt, das Rechte erhalten soll, muss zwingend im AD vorhanden sein. Damit ist auch klar, warum einfache Kontakte oder Verteiler im AD, die keine SID haben, nicht für die Vergabe von Berechtigungen genutzt werden können. Die Rechte werden in *Access Control Lists* (ACL) der jeweiligen Objekte gespeichert. Eine Besonderheit bietet der Einsatz von deaktivierten Konten, die für ihre Postfachberechtigung eine SID aus einer vertrauten Domäne erhalten (Associated External Account).

Warnung

Achtung!

Machen Sie sich zuerst mit den einzelnen Rechten vertraut, bevor Sie diese anhand der Bilder, Beschreibungen und Assistenten anpassen. Die Optimierung nach Ihren eigenen Vorstellungen muss immer getestet und dokumentiert werden. Die Erfahrung zeigt, dass die Anzahl der unabsichtlich beschädigten Installationen immens hoch ist aufgrund der geänderten Setup-Einstellungen; diese werden bei Neuinstallation nicht auf die Standardwerte zurückgesetzt. Vermeiden Sie das Ändern der Vererbung oder das „Verweigern“, erstellen Sie besser eine weitere Gruppe zu diesem Zweck.

DENY vor ALLOW

Vermeiden Sie auf jeden Fall immer das Recht „Verweigern“, da es auch den Zugriff sperrt, der an eine Gruppe oder einen Benutzer delegiert wurde. Das „Deny“-Recht steht immer vor dem „Allow“-Recht und hat die höchste Priorität. Denken Sie daran, dass auch der Administrator zur Gruppe „Jeder“ oder „Authentifizierte Benutzer“ gehört.

Rechte anzeigen

ShowSecurityPage

Nicht umsonst verbirgt Microsoft die Berechtigungen in der normalen Ansicht des Exchange System-Managers. Erst mit der folgenden Einstellung in der Registrierung erhalten Sie Zugriff auf die Sicherheitseinstellungen der Exchange-Konfiguration:

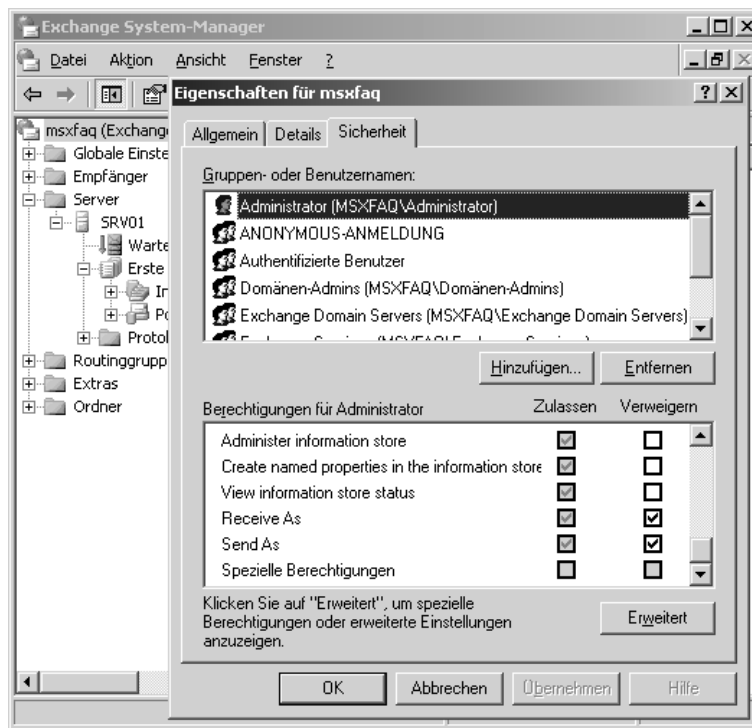
```
[HKEY_CURRENT_USER\Software\Microsoft\Exchange\EXAdmin]
 "ShowSecurityPage" REG-DWORD: Wert: 0x00000001
```

Die entsprechenden Microsoft-Informationen finden Sie auch in der TechNet:

- Q259221 XADM: Security Tab Not Available on All Objects in System-Manager
- Q264733 ADM: How to Enable the Security Tab for the Organization Object

Erst dann ist im Exchange System-Manager die Karteikarte „Sicherheit“ bei vielen Objekten sichtbar. Sie können dann einige Rechte unabhängig vom Assistenten verändern.

Abbildung 4.6 Berechtigungen in der Exchange-Organisation



Im Bild ist die Standardeinstellung, in der der Administrator keinen Zugriff auf Postfächer erhält, gut zu erkennen. Dieses „Verweigern“-Recht wird bei allen Postfachspeichern vererbt. Setzen Sie aber als Lösung nicht die Vererbung von Rechten außer Kraft, sondern nutzen Sie einfach einen anderen Benutzer, oder entfernen Sie das Verbot, wenn Sie vollen Durchgriff auf alle Postfächer brauchen. Dies ist für Virenscanner, Archivlösungen, Einzelinstanzsicherungen und andere Programme oft erforderlich. Der Datenschutz muss dabei jedoch immer beachtet werden.

Wenn Sie Berechtigungen ändern und setzen, dann sollten Sie sich an die Active Directory-Einstellungen und die dort getroffenen Vereinbarungen zum Einsatz von Gruppen erinnern. Es ist vorteilhaft eine entsprechende Sicherheitsgruppe mit aussagekräftigem Namen anzulegen, zu dokumentieren und dieser Gruppe die Rechte zu geben. So können später einfach durch Änderung der Gruppenmitgliedschaft diese Rechte an einzelne Personen weitergegeben werden. Die Objekte, die Sie mit Rechten versehen können, sowie deren Bedeutung werden nachfolgend erläutert.

4.7.1 Exchange-Serversystem

Exchange 2003 wird auf einem Windows 2000- oder 2003-Server installiert. Damit besitzt ein Administrator auf diesem Rechner auch im Hinblick auf Exchange gewisse Berechtigungen. Er kann Dienste stoppen und starten, Service-Packs installieren und zum Beispiel auch Sicherungen starten.

Die Rolle des Server-Administrators unterscheidet sich stark von dem Exchange-Administrator, da auf dem System selbst nur wenige Exchange-relevante Informationen der Organisation liegen. Idealerweise richten Sie den Exchange-Server als Mitgliedsserver ein, um über entsprechende Richtlinien und Gruppenzugehörigkeiten die Administration des Servers zu steuern. Unvermeidlich ist diese Vorgehensweise bei einer strikten Trennung, bei der der Server-Administrator keinerlei Rechte auf einen Exchange-Server erhalten soll. Solche Anpassungen sollten Sie jedoch mit äußerster Sorgfalt vornehmen und darauf achten, die erforderlichen Exchange-Gruppen oder Computerkonten zu entfernen.

Funktionen trennen

Ganz besondere Vorsicht ist geboten, wenn der Exchange-Server zugleich auch Domänencontroller und somit der Server-Administrator gleichzeitig der Domänen-Administrator ist. Auch das Anmelderecht für normale Anwender auf einem Domänencontroller ist verweigert, was Auswirkungen auf den Zugriff bestimmter Clients per Outlook Web Access mit sich bringt.

Bei kleinen Exchange-Umgebungen findet dieser Aspekt keine Beachtung, für große Unternehmen bedeuten diese Einschränkungen die Pflicht zur strikten Funktionstrennung der Exchange-Server und der Domänencontroller.

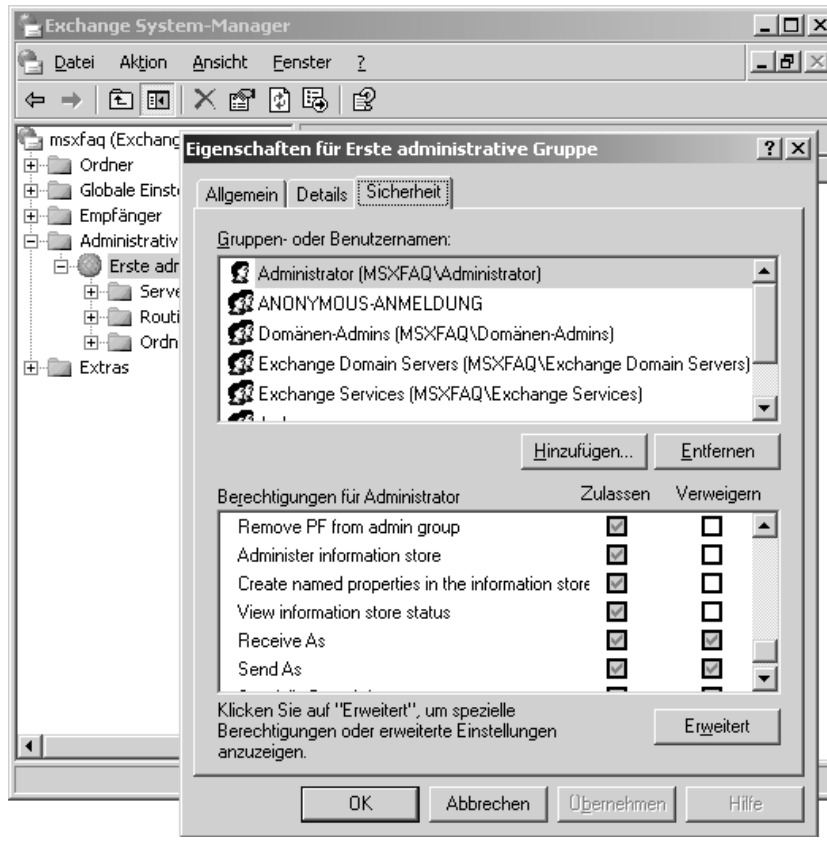
4.7.2 Exchange-Konfiguration

Wie bereits im Active Directory-Kapitel erläutert besteht die Verzeichnisdatenbank aus drei Partitionen. Den für Exchange wichtigsten Part enthält die Konfigurationspartition mit dem Großteil aller Informationen über Administrative Gruppen, Server, Connectoren, Datenbanken und Routinggruppen. Jedem dieser Elemente können unterschiedliche Berechtigungen zugeordnet werden.

Objektverwaltung

Verwenden Sie ausschließlich den Exchange System-Manager mit den Assistenten für die Zuweisung von Verwaltungsberechtigungen. In der Praxis beschränkt sich die Vergabe von Rechten auf die Ebene der Administrativen Gruppe.

Abbildung 4.7 Rechte auf einer Administrativen Gruppe



Das Bild zeigt einen Ausschnitt der Rechte auf dem Objekt „Erste administrative Gruppe“. Gut zu erkennen ist das vererbte „Verweigern“-Recht des Administrators.

Die Rechte sollten Sie jedoch nur über den Assistenten zur Objektverwaltung zuweisen, den Sie über das Kontextmenü erreichen.

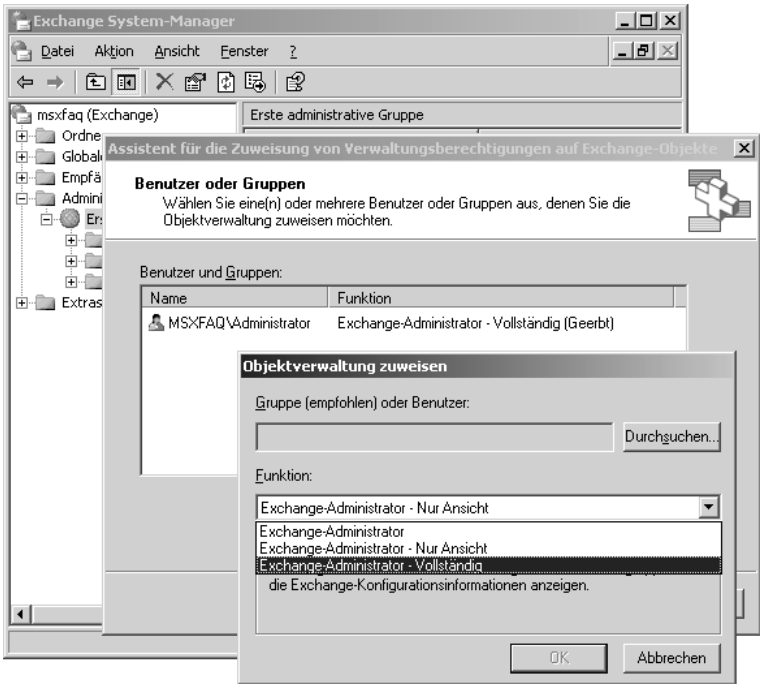


Abbildung 4.8 Berechtigung auf Administrative Gruppen mit dem Assistenten einrichten

4.7.3 Exchange-Benutzerobjekte

Die Informationen über Benutzer und Verteiler liegen in der Domänenpartition des Active Directory. Auch auf diese Objekte können Gruppen oder Personen berechtigt werden, um Exchange-Einstellungen zu ändern. Da die Anwender in der Regel in Organisationseinheiten eingeordnet sind, ist eine Vergabe von Berechtigungen auf der OU-Ebene der häufigste Fall.

„Erweiterte Ansicht“

Die Anzeige der Berechtigungen im Bereich Sicherheit erfordert die „erweiterte Ansicht“ in der Management-Konsole für Benutzer und Computer. Gleichzeitig erscheinen mit den erweiterten Funktionen in der Ansicht weitere Karteikarten der AD-Objekte.

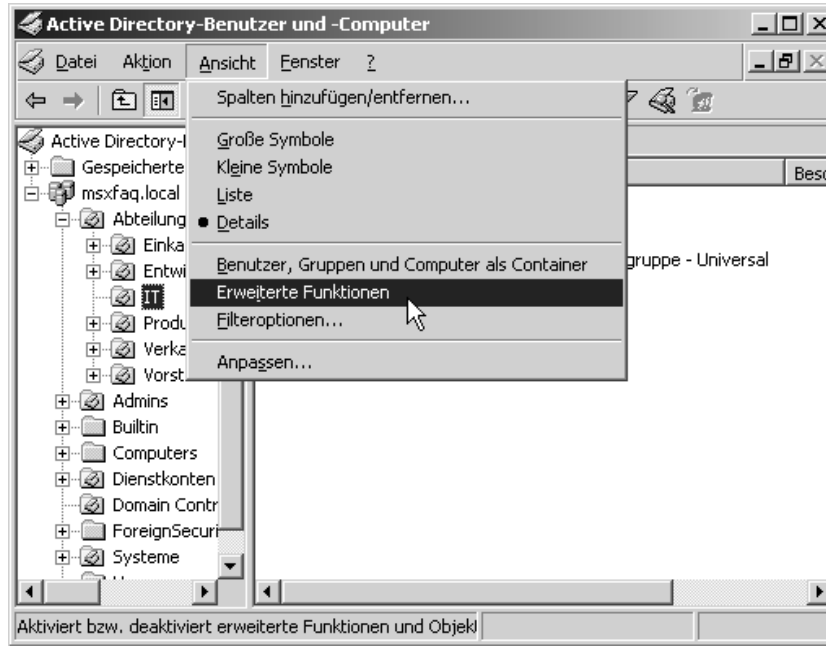


Abbildung 4.9 Erweiterte Funktion der Management-Konsole aktivieren

Erst dann wird an den einzelnen Objekten die Karteikarte „Sicherheit“ mit eingeblendet.

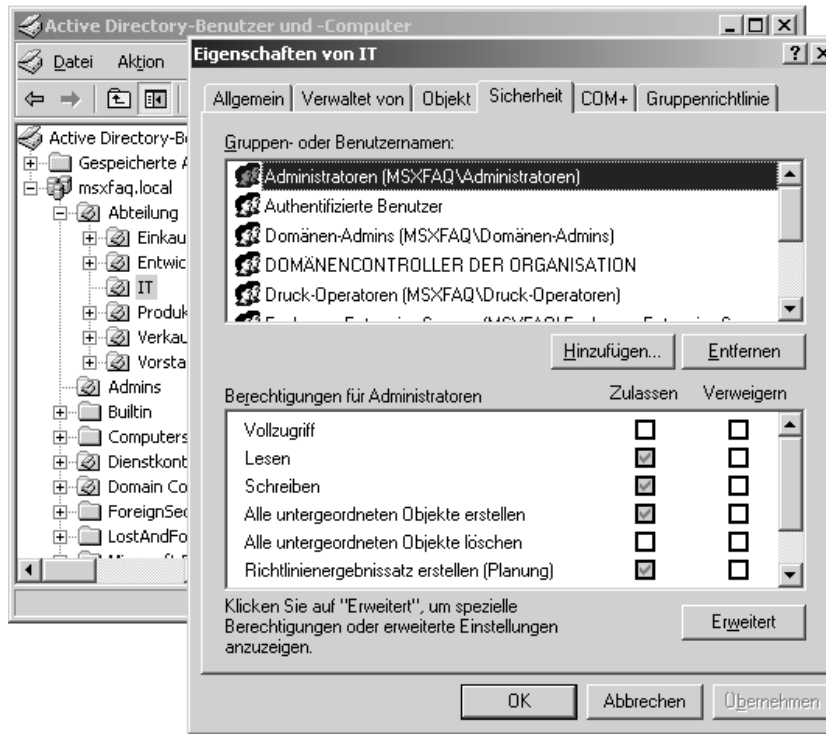


Abbildung 4.10 Rechte auf der OU

Auch hier gilt, dass Sie Berechtigungen am besten über den Assistenten auf der Ebene der Organisationseinheiten und nicht auf einzelne Objekte zuweisen. Den Assistent für die Objektverwaltung finden Sie im Kontextmenü der jeweiligen OU.

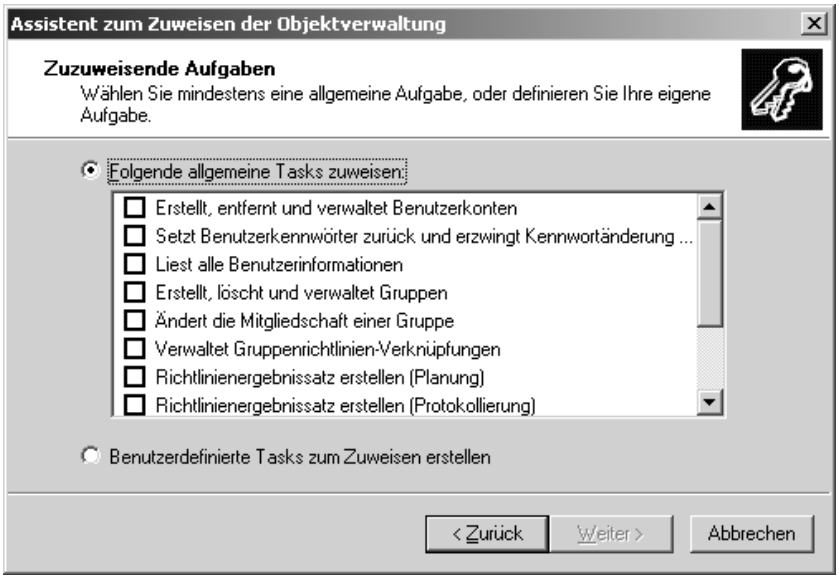


Abbildung 4.11 Rechte mit dem Assistenten zuweisen

Damit ist es auch Personen ohne die Rolle eines Domänen-Administrators möglich, Benutzer anzulegen und zu verwalten und die Exchange-E-Mail-Adresse und Gruppenzugehörigkeiten zu pflegen.

4.7.4 Berechtigungen auf das Postfach

Nach der Installation der Exchange-Verwaltungsprogramme werden bei den Benutzern auch die Eigenschaften „Exchange - Erweitert“ angezeigt. Hier können Sie weitere Postfachberechtigungen setzen, die ebenfalls im AD abgelegt und dort auch für den Zugriff auf das Postfach kontrolliert werden.

Mailboxrechte für den erweiterten Zugriff

Mit diesen Berechtigungen steuern Sie die Aktionen, die ein Benutzer auf sein Postfach oder das des Kollegen ausführen darf, wie das Löschen des Postfachspeichers oder die Lese- und Änderungsberechtigungen.

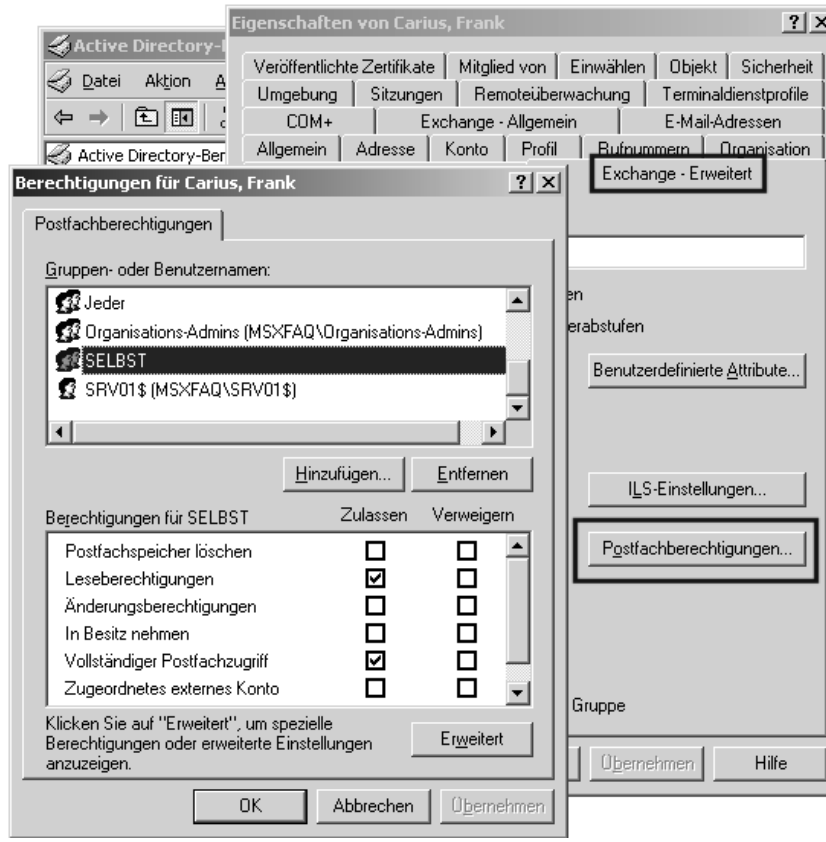


Abbildung 4.12
Berechtigungen auf das Postfach

Es ist interessant zu wissen, dass für Domänen-Administratoren, den Administrator und einige andere Gruppen immer ein explizites „Verweigern"-Recht auf „Send as" und „Receive as" gesetzt ist. Dies fällt unter die erweiterten Sicherheitseinstellungen, mit der der unberechtigte Zugriff auf Postfachinhalte verhindert wird, auch wenn sonst alle Rechte auf den User vorhanden sind. Unter anderem übt dies auch einen gewissen Einfluss auf Exchange aus. Häufig wird ein „Exservice"-Konto angelegt mit der Berechtigung auf alle Postfächer und dem Status des Domänen-Administrators. Aus Datenschutzgründen sollten Domänen-Administratoren auch weiterhin keinerlei Rechte auf Postfachinhalte erhalten. Legen Sie dazu ein eigenes Konto nur zu diesem Zweck mit den entsprechenden Berechtigungen an, und vergessen Sie nicht, dies mit dem Betriebsrat abzustimmen.

In der Migrationsumgebung benötigen Sie ein Konto mit diesen Rechten für das Verschieben der Postfächer von Exchange 5.5 nach Exchange 2003.

4.7.5 Exchange-Inhalte in Postfächern

Unabhängig von den Berechtigungen im Active Directory speichert Exchange auch innerhalb des Informationsspeichers Berechtigungen ab. Die Stellvertreterberechtigungen auf Ihrem Kalender für den Kollegen werden im Postfach selbst am Ordner „Kalender“ geschrieben und stehen nicht im Active Directory.

In Exchange 2000 war es möglich, über das Laufwerk M: auf die Informationen zuzugreifen und über den Windows Explorer die Berechtigungen anzupassen. Diese Möglichkeit wird mit Exchange 2003 nicht mehr standardmäßig zur Verfügung gestellt. Dies ist auch besser, da der Zugriff auf Laufwerk M: in der Regel die Inhalte der Datenbank oft unbrauchbar gemacht hat.

Rechte auf Informationsspeicher-Ebene

Der Exchange-Administrator kann auf der Ebene des Postfachspeichers und des Objektes die Berechtigungen auf das Postfach im Active Directory setzen. Mittels Vererbung sind diese auch in den untergeordneten Bereichen gültig. Besonders bei der Sicherung von einzelnen Elementen, dem Virenscannen nach Schädlingen in E-Mails oder der Archivierungslösung, die alte Elemente aus dem Postfach raus ins Langzeitarchiv überführt, stellt sich diese Objektverwaltung als sehr hilfreich heraus.

4.7.6 Öffentliche Ordner-Rechte

Ähnlich der Berechtigungen auf Postfächer sind auch die Rechte der Öffentlichen Ordner auf der Ebene des Informationsspeichers konfigurierbar. Die Verwaltung der Ordner erfolgt über den Exchange System-Manager. Die Verwaltung der Clientberechtigungen kann sowohl mit dem Exchange System-Manager als auch mit dem Outlook-Client erfolgen. Die Clientberechtigungen können auch über Outlook verwaltet werden.

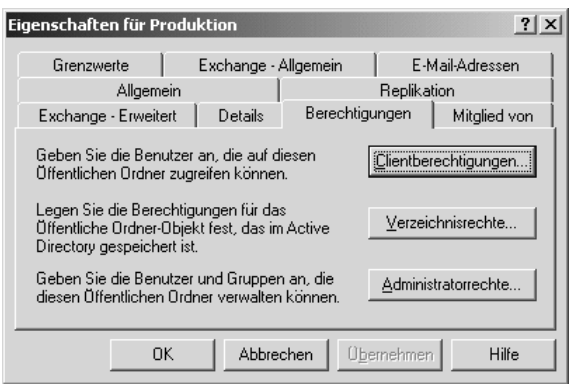


Abbildung 4.13 Ordner Berechtigungen

In jedem der drei folgenden Fenster können Rechte eingestellt werden.

4.7.6.1 Clientberechtigungen

Hierüber steuern Sie die Rechte der Benutzer und Verteiler auf den Öffentlichen Ordnern. Ebenso wie bei den Postfachordnern ist eine dedizierte Zuordnung der Rechte bestimmbar und somit auch, wer die Elemente lesen oder sogar auch Nachrichten ablegen darf. Diese Einstellung ist nur auf dem Ordner gültig, wo das Recht eingestellt wurde. Eine explizite Vererbung auf alle Unterordner ist möglich, jedoch werden dabei die Rechte aller Unterordner ersetzt.

Abbildung 4.14 Standard-MAPI-Clientrechte

Diese Berechtigungen können im Outlook-Client eingesehen und vom Ordnerbesitzer verändert werden. Hinterlegt sind die Rechte im Informationsspeicher. Standardmäßig sind die Einstellungen für Standardbenutzer, Administratoren und den anonymen Zugriff gesetzt. Diese Rechte erlauben allen Benutzern in der Organisation den Zugriff auf Ordner als Autor. Weiterhin können anonyme Absender in diesem Ordner schreiben. Dies ist wichtig, wenn der Ordner eine E-Mail-Adresse erhält und aus dem Internet erreichbar sein soll. Für den internen Einsatz sollten Sie die Berechtigungen hingegen anpassen.

Tabelle 4.2 Standard-Clientberechtigungen

Client	Rechte	Beschreibung
Standard	Stufe: Autor	Diese Rechte gelten für alle Benutzer mit einem Exchange-Postfach in der Organisation. Gleichzeitig gilt die Einstellung „Standard“ als Vorgabe für alle Benutzer, die hier hinzugefügt werden.
Administrator	Stufe: Besitzer	Der erste Besitzer ist der Administrator, der für die Anlage der ersten Ordner (Top Level Folder) zuständig ist und

Client	Rechte	Beschreibung
		die Rechte entsprechend an andere Personen oder Gruppen weitergeben kann.
Anonym	Stufe: Mitarbeiter	Dieses Konto bezeichnet alle Absender, die keine E-Mail-Adresse in der Exchange-Organisation haben. Mit der einzigen Berechtigung „Erstellen von Objekten“ ist es möglich, dass auch unbekannte, also anonyme Absender eine Nachricht an den Öffentlichen Ordner senden dürfen. Somit können wieder E-Mails aus dem Internet an E-Mail-Adressen eines Ordners zugestellt werden, wie in Exchange 5.5 üblich und in Exchange 2000 fatalerweise deaktiviert.

Exchange fasst die einzelnen Clientberechtigungen in Stufen zusammen, damit Anwender leichter damit umgehen können. Es ist sehr viel einfacher, jemandem zu erklären, er möge eine Gruppe als „Autor“ hinzufügen anstatt die Rechte einzeln aufzuführen. Ob ein Ordner jedoch im Outlook sichtbar ist, hängt nicht von diesen Vorlagen ab, sondern kann separat gesetzt werden:

Tabelle 4.3 Berechtigungsstufen

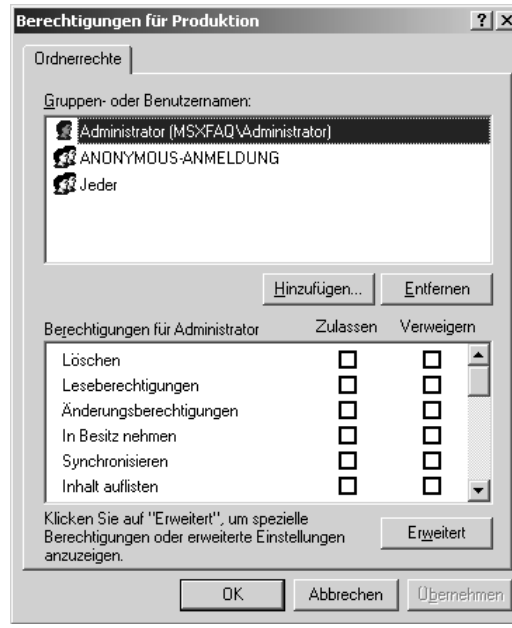
Vorlage	Berechtigungen
Keine	Der Ordner ist nur sichtbar. Dies ist dann notwendig, wenn der Benutzer auf untergeordnete Ordner zugreifen muss, also auf die Struktur.
Mitarbeiter	Der Ordner ist sichtbar, und der Anwender kann neue Elemente erzeugen, aber nicht mehr lesen. Dies ist erforderlich, um eine E-Mail an den Ordner senden zu können.
Lektor	Diese Benutzer können nur Elemente lesen und natürlich den Ordner sehen.
Nicht herausgebender Autor	Das Erstellen und Lesen von Objekten ist möglich, ebenso können eigene Objekte gelöscht werden.
Autor	Lesen und Erstellen von Objekten ist ebenso möglich wie das Bearbeiten und Löschen der eigenen Objekte.
Veröffentlichender Autor	Zusätzlich zum Autor kann dieser Anwender Unterordner anlegen.
Herausgeber	Dieser Personenkreis hat fast alle Rechte eines Autors, nur dass zusätzlich auch fremde Objekte geändert und gelöscht, dafür aber keine Unterordner erstellt werden dürfen.
Veröffentlichender Herausgeber	Zusätzlich zum Herausgeber können Unterordner angelegt werden.
Besitzer	Der Besitzer hat auf die Inhalte des Ordners die gleichen Berechtigungen wie der veröffentlichende Herausgeber, allerdings kann er zusätzlich auch die Berechtigungen auf den Ordner ändern.

Diese neun Stufen sind seit Exchange 4.0 unverändert geblieben. Ähnlich wie bei Dateisystemen sollten Sie vermeiden, einzelnen Personen Berechtigungen zu erteilen. Arbeiten Sie bei der Vergabe von Berechtigungen in Öffentlichen Ordnern besser mit Verteilern.

Umrechnung Exchange-DN in Windows-SID

Im Gegensatz zu Exchange 5.5 werden die Rechte im Informationsspeicher anhand der SID gespeichert. Bei einer Migration muss der Informationsspeicher daher die Berechtigungen der Exchange 5.5-Server konvertieren. Dieser Vorgang ist dann problematisch, wenn nicht alle Benutzer im Active Directory angelegt bzw. mit eindeutigen Rechten durch den Active Directory Connector repliziert wurden. Welche Berechtigungen im Informationsspeicher aufgelöst werden, können Sie prüfen, indem Sie mit gedrückter Steuerungstaste (STRG) auf Clientberechtigungen klicken.

Abbildung 4.15 NTFS-Rechte auf Öffentliche Ordner



Diese Ansicht sollten die gleichen Benutzer und Gruppen anzeigen wie die Ansicht der MAPI-Rechte.

Dies sind die effektiven Rechte, die Exchange 2003 beim Zugriff des Clients auswertet und auf die es dazu passend den Zugriff erlaubt oder verweigert. Mit Exchange 2000 war es möglich, diese Rechte auch über das Laufwerk M: zu sehen und mit teils schwerwiegenden Folgeerscheinungen zu ändern. Mit Exchange 2003 kann es zu den gleichen Problemen kommen, allerdings ist das Laufwerk M: hier standardmäßig nicht vorhanden.

Die Datenbank von Exchange 2003 erlaubt noch sehr viel feinere Berechtigungen. Rechte können sogar auf einzelne Elemente und Felder eines Elements vergeben werden. Allerdings kann Outlook damit nicht umgehen, und daher sollten Sie dies auch nicht weiter verwenden.

Berechtigungen propagieren

Neu mit Exchange Service Pack 2 ist die Möglichkeit, einzelne Berechtigungen auf alle Unterordner weiterzuleiten, ohne den Verlust der vorhandenen Rechtestruktur. Über die neue Option EINSTELLUNGEN VERWALTEN können Sie mit Hilfe eines Assistenten Benutzer hinzufügen, entfernen und ersetzen sowie Berechtigungen eines Benutzers ändern. Diese einzelnen Zugriffsrechte werden nun gezielt – ausgehend vom gewählten Ordner im ESM – auf alle darunter befindlichen Ordner gesetzt. Bislang wurde die komplette ACL auf alle Unterordner vererbt, wodurch die bisherigen Berechtigungen drakonisch überschrieben wurden.

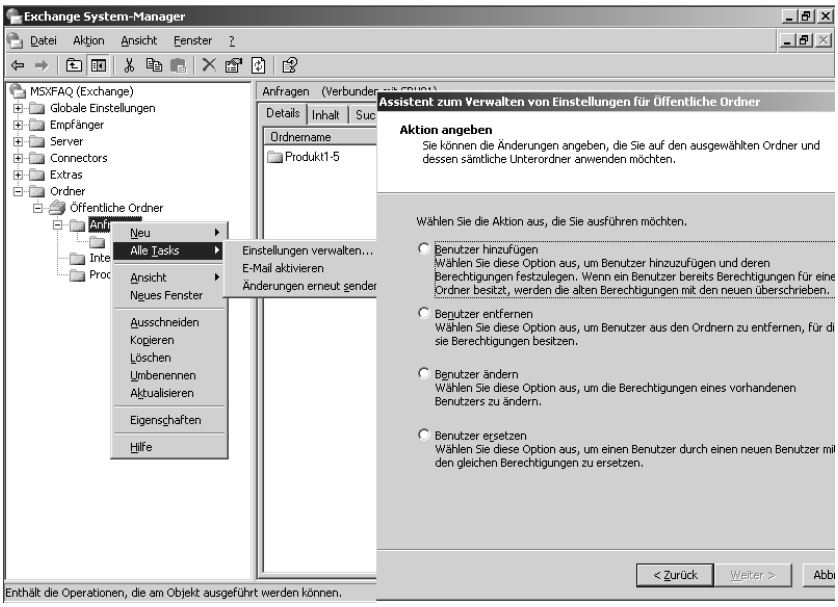


Abbildung 4.16 Einzelne Berechtigungen setzen

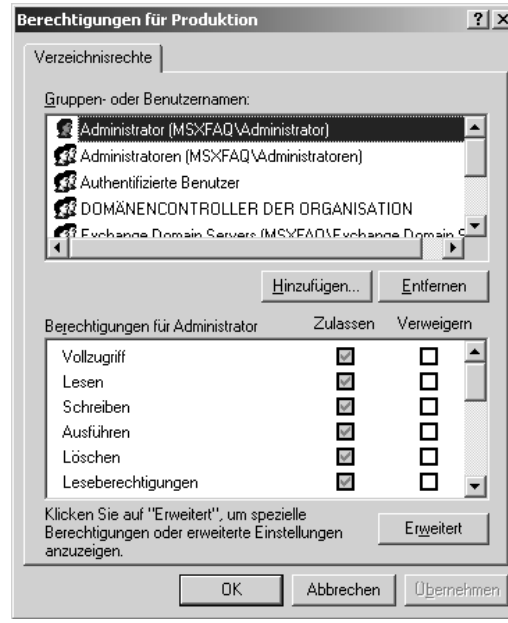
Unter diesem Menüpunkt können Sie unter anderem auch Einstellungen wie Ordnerrechte, Speichergrenzwerte und Replikate überschreiben oder Replikateserver verändern.

4.7.6.2 Verzeichnisrechte

Die zweite Schaltfläche öffnet das Fenster mit den Verzeichnisrechten. Nicht nur die Benutzer und Verteiler sind im Active Directory als Objekt vorhanden, sondern auch die Öffentlichen Ordner mit einer E-Mail-Adresse erhalten einen Eintrag im AD. So können eingehende Nachrichten an

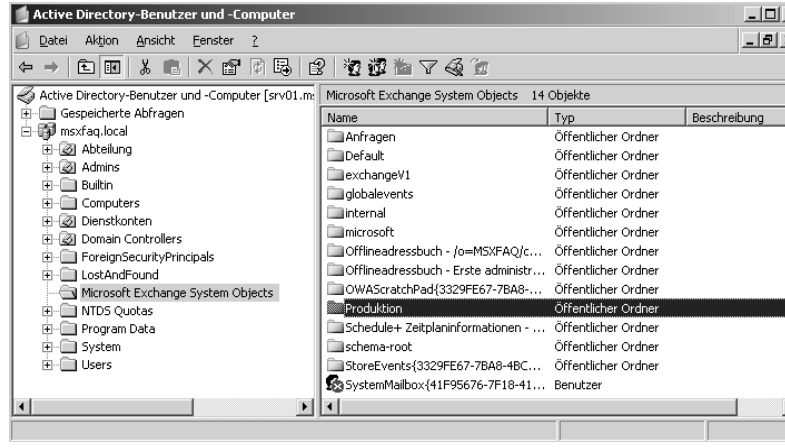
Öffentliche Ordner einem Exchange-Server zugestellt werden. Auf diese Objekte selbst können ebenfalls Rechte vergeben werden, die mehr den Sicherheitseinstellungen entsprechen.

Abbildung 4.17 Rechte auf das Verzeichnisobjekt eines Öffentlichen Ordners



Diese E-Mail-aktivierten Öffentlichen Ordner-Objekte liegen in einer besonderen OU, die bei der Ausführung von DOMAINPREP angelegt und nur in der erweiterten Ansicht den Inhalt anzeigt. Wählen Sie im Menü unter Ansicht die ERWEITERTE FUNKTIONEN, da diese OU sonst nicht sichtbar ist.

Abbildung 4.18 Systemobjekte für Öffentliche Ordner



Die Verzeichnisrechte beziehen sich auf diese Active Directory-Objekte.

4.7.6.3 Administratorrechte

Von „deleted item retention time“ bis „Public Folder quotas“

Der letzte Punkt sind die administrativen Rechte des Ordners selbst. Jeder Ordner hat neben dem Inhalt und dem Eintrag als Active Directory-Objekt einen Eintrag im Informationsspeicher. In einem speziellen Systemordner wird unter anderem hinterlegt, auf welchem Server ein Replikat liegt, welche Grenzwerte gelten und welche Replikationsintervalle eingestellt sind.

Exchange versieht auch diese Eigenschaften mit einer Zugriffssteuerungsliste, die Sie in dem Fenster bearbeiten können.

So könnten Sie bestimmen, welche Personen oder Gruppen die Konfiguration der Ordner verändern dürfen. Die wenigsten Unternehmen ändern diese Einstellungen.

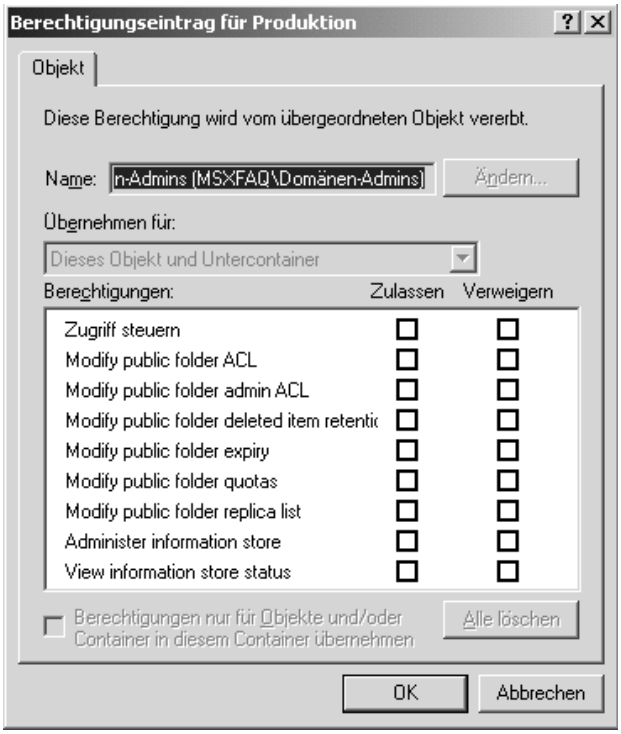


Abbildung 4.19 Administrative Rechte auf Öffentliche Ordner

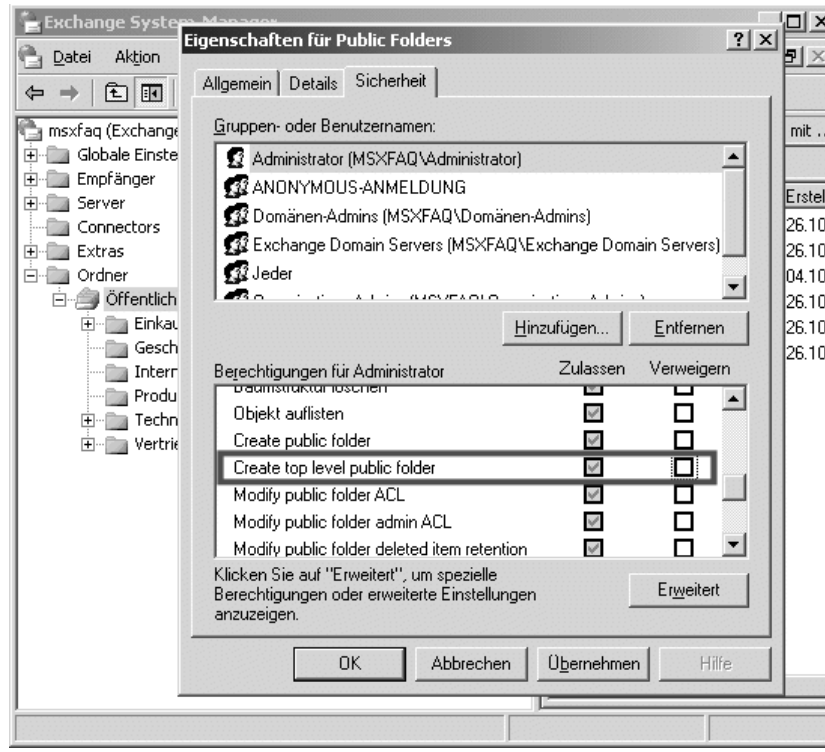
4.7.7 Top Level Folder

Eine signifikante Änderung in Exchange 2003 zu allen bisherigen Exchange-Versionen ist die Berechtigung auf die erste Ordnerstufe. Bislang konnte in der Standardeinstellung jeder Benutzer ohne Einschränkungen neue Ordner auf der obersten Hierarchiestufe anlegen. Durch eine geeignete Konfiguration ließ sich dies verhindern. Bei der Installation eines neuen Exchange 2000-Servers wurde der Eintrag immer wieder auf den Standardwert zurückgesetzt.

Exchange 2003 setzt die Berechtigungen so, dass nur noch die Gruppen „Exchange Domain Servers“, „Organisations-Admins“, „Domänen-Admins“ und der Administrator neue Ordner auf der höchsten Hierarchiestufe anlegen können („Create top level public folder“ zulassen). Dies hat den Vorteil, dass Sie die Kontrolle über die Öffentlichen Ordner behalten und die erste Ebene strukturiert aufbauen können.

Allerdings ist es nicht ratsam, sich immer als Administrator anzumelden, um einen neuen Öffentlichen Ordner auf der obersten Ebene anzulegen. Sie können diese Aufgabe delegieren, indem wenige Anwender oder eine Gruppe das Recht zum Anlegen neuer Top Level Folder erhält. In den Eigenschaften der „Öffentlichen Ordner“ erteilen Sie den entsprechenden Benutzern das Recht „Top Level Public Folder“ anzulegen.

Abbildung 4.20 Rechte für erste Ordnerebene vergeben



Sie sollten auch hier bevorzugt Gruppen berechtigen und nicht einzelne Personen.

4.8 Datenbank-Grundlagen

Bislang haben wir uns nur Gedanken darüber gemacht, wo Exchange seine Konfiguration ablegt. Ebenso wichtig ist das Wissen über die Datenbank, in der Exchange die Nachrichten abspeichert sowie viele andere Informationen.

4.8.1 Wie arbeitet Exchange?

Die Exchange-Datenbank basiert auf einer Weiterentwicklung der ESE (Extensible Storage Engine), die schon seit den Anfängen von Exchange und mit Windows 2000 auch beim Active Directory eingesetzt wird. Die Exchange-Datenbank ist transaktionsorientiert, aber was bedeutet das für Sie?

Nachrichten bewahren

Das wichtigste Ziel und somit bestimmend für die Entwicklung der Exchange-Datenbank war der Leitspruch „Never loose a message“. Egal was passiert, es sollten bei einem ordentlichen Design keine Nachrichten verloren gehen. Im Umkehrschluss bedeutet dies auch, alle Eventualitäten, wie ungeplante Ausfälle, Speicherdefekte und andere Dinge, abzufangen.

Der Betrieb von Exchange basiert auf dem Versenden und Empfangen von Nachrichten. Diese Veränderungen bewirken somit Schreib- und Lesezugriff, die jedoch nicht direkt in der Datenbank abgelegt werden. Alle Änderungen erfolgen im Datenbank-Cache und sind damit erst einmal nur im flüchtigen Hauptspeicher verfügbar. Festgehalten werden die Abweichungen zur Datenbank in einer Transaktionsdatei, die somit alle geschriebenen Informationen sequenziell enthält und nachträglich nicht verändert. Die Summe aller Transaktionsdateien enthält alle Änderungen seit der letzten erfolgreichen Datensicherung (Online-Backup).

Weiterhin wird beim Ausfall eines Servers während des Schreibprozesses die Beschädigung der Exchange-Datenbanken verhindert, soll bedeuten, dass eine nur teilweise geschriebene Nachricht keine korrupte Datenbank erzeugen kann. Alle Änderungen werden beim erneuten Starten von Exchange anhand der Transaktionsprotokolle reproduziert und in einem „roll forward“-Verfahren wieder hergestellt. Bei der Wiederherstellung der letzten Online-Sicherung und dem „roll forward“ der Transaktionsprotokolle kann der aktuelle Zustand von Exchange wiederhergestellt werden.

Bei einem Ausfall kann somit trotz permanenter Schreibaktivität auf der Datenbank auch bei einem unerwarteten Stillstand (Stromausfall, Hardware-Defekt, Bluescreen etc.) diese immer wieder in einen konsistenten Status geführt werden.

Zwischenspeicher für Änderungen

Die Geschwindigkeit der Transaktionsprotokolle wirkt sich auf den Client aus, denn nur nachdem die Transaktion in der Protokolldatei steht, wird der Client wieder freigegeben. Solange die „Sanduhr“ im Outlook erscheint,

schreibt Exchange die Änderungen in die Transaktionsdatei. Zwischen den tatsächlich in die Datenbank geschriebenen Bits und dem aktuellen Stand in den Protokolldateien können also einige Megabytes Differenz liegen.

Erst beim Herunterfahren der Exchange-Dienste werden alle offenen Transaktionen in die Datenbank übernommen und diese somit erst in einen konsistenten Status gebracht. Daher dauert das Beenden von Exchange manchmal etwas länger. Beenden Sie Exchange mangels Zeit etwas unsanft, dann erkennt Exchange beim Hochfahren die Inkonsistenz der Datenbank und arbeitet die Transaktionsdateien ab. Die eingesparte Zeit müssen Sie beim Start wieder ausharren.

Das Prinzip der Protokolldateien nutzen auch andere Dienste wie das Active Directory in Windows 2000/20003. Die Datenbank heißt hier allerdings NTDS.DIT, und die Protokolldateien sind 10 MB groß. Auch der Exchange 2003-SRS nutzt die gleiche Technik, um gegenüber dem Exchange 5.5-Server eine alte DIR.EDB zu simulieren. Ein SQL-Server nutzt ähnliche Techniken, um die Zuverlässigkeit zu erhöhen und die Konsistenz der Datenbank zu gewährleisten.

4.8.2 Transaktionsdateien

Seit der Version 2000 betreibt Exchange für jede Speichergruppe einen eigenen Satz Transaktionsprotokolle. Alle Datenbanken (maximal fünf) in dieser Speichergruppe nutzen demzufolge die gleichen Protokolldateien. Dies ist im Hinblick auf Performance und Datensicherung wichtig. Exchange 5.5 arbeitet generell mit nur zwei Protokolldateisätzen, einen für das Verzeichnis und den zweiten für den Informationsspeicher. Die Exchange 5.5-Verzeichnisdatenbank DIR.EDB wird nun durch das Active Directory ersetzt. Ein Exchange 2003 Standard-Server hat daher nur einen Protokolldateisatz. Bei der Enterprise Edition sind bis zu zwanzig Datenbanken in vier Speichergruppen möglich, folglich auch bis zu vier eigenständige Protokolldateisätze pro Server.

Der sequenziell schreibende Zugriff von Exchange erfolgt dann unverzüglich, wenn der Speicherbereich, in dem sich die Transaktionsdateien befinden, nicht durch andere Prozesse belastet ist. Sie können daher unnötige Wartezeiten, die durch den Abschluss anderer Dateioperationen oder Kopfpositionierung verloren gehen, reduzieren, indem die Transaktionsdateien auf einem eigenen unabhängigen Speicherbereich abgelegt werden. Deaktivieren Sie auf diesem Speicherbereich den Schreibcache, damit bei einem Stromausfall auch wirklich alle Schreibbefehle unlängst ausgeführt wurden, oder sichern Sie das System mit Batterien (USV) ab.

Aber es gibt noch einen zweiten Grund, die Transaktionsdateien auf einen eigenen Speicherbereich abzulegen. Beim Verlust der Datenbank durch einen Festplattendefekt sollten die Transaktionsdateien noch fehlerfrei erhalten sein, um mit der letzten Sicherung alle Nachrichten bis zum Moment des Ausfalls wiederherzustellen.

Die „Transaktionsprotokolle“ heißen immer EDB*.LOG und sind 5 MB groß. Die aktuelle Datei ist immer „EDB.LOG“ und wird bei 5 MB geschlossen, umbenannt und in eine neue Datei angelegt. Um im Falle von zu wenig Plattenplatz eine ordentliche Beendigung des Systems zu gewährleisten, nutzt Exchange zwei Reservedateien res1.log und res2.log.

Umlaufprotokollierung

Exchange bietet die Möglichkeit, die so genannte Datenbankumlaufprotokollierung (Circular Logging) zu aktivieren. Bei Exchange 5.5 ist diese Einstellung per Default aktiv, während seit Exchange 2000 diese Umlaufprotokollierung per Default abgeschaltet ist. Damit hat sich Microsoft zugunsten der Betriebssicherheit und der Möglichkeiten eines „roll forward“ entschieden. Es bedeutet aber auch, dass die Transaktionsdateien ohne Datensicherung sehr schnell beträchtlich viel Platz einnehmen. Dies gilt umso mehr bei Migrationen und dem Import von Fremdsystemen, dem Verschieben von Postfächern zwischen Servern und der Replikation Öffentlicher Ordner.

„Circular Logging“ deaktivieren verhindert Datenverlust

Die Umlaufprotokollierung hat das Ziel, den Platzbedarf der Transaktionsprotokolle zu begrenzen. Exchange nutzt mit der Einstellung nur bis zu fünf Protokolldateien à 5 MB. So oder so bleibt Exchange bei seiner „transaktionsorientierten“ Datenbankverwaltung, die für die Konsistenz der Datenbank bürgt. Bei vielen Nachrichtentransaktionen und entsprechenden Dateien können Sie bei einem Restore in der Regel aber nicht mehr bis zum Moment des Ausfalls die Datenbank wiederherstellen, sondern nur bis zum Zeitpunkt der Sicherung.

Sie sollten auf jeden Fall eine Besonderheit der Umlaufprotokollierung beachten. Die Umlaufprotokollierung wird temporär außer Kraft gesetzt, wenn Sie eine der Datenbanken innerhalb der Speichergruppe „offline“ nehmen. Solange noch Transaktionen der nicht verfügbaren Datenbank in der Protokolldatei enthalten sind, kann der IS keine Protokolldateien löschen. Vermeiden Sie daher diesen „Offline“-Zustand über längere Zeit, und überwachen Sie den freien Festplattenplatz des Servers.

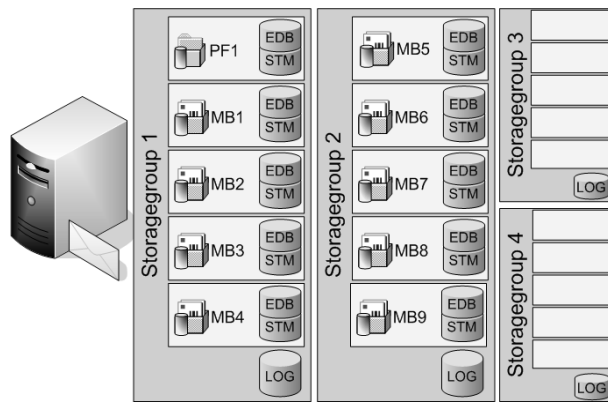
4.8.3 Die Datenbanken

Während Exchange 5.5 noch mit drei Datenbanken (PRIV.EDB, PUB.EDB, DIR.EDB) ausgekommen ist, wurde mit Exchange 2000 das Datenbankdesign grundlegend geändert:

EDB und STM

Die bisherige Verzeichnisdatenbank DIR.EDB ist zwar zugunsten des Active Directory entfallen, aber dafür besteht jede Datenbank des Informationsspeichers nun aus zwei Datenbankdateien. Neben der EDB-Datei gibt es jeweils eine zusätzliche STM-Datei. Die letzten Jahre haben gezeigt, dass das Internet immer wichtiger wird und die hier übertragenen Daten entsprechend anders codiert werden. Exchange 5.5 basiert auf X.400 und speichert die Daten als 8-Bit-Informationen ab. Im Internet werden jedoch die meisten Informationen MIME-codiert. Diese Inhalte mussten mit Exchange 5.5 immer aufwändig konvertiert werden. Exchange 2003 stellt mit den STM-Dateien eine geeignete Ablage für MIME-codierte Inhalte bereit. Der Informationsspeicher besteht zwingend aus beiden Daten. Die EDB- und STM-Datei gehören untrennbar zusammen und können weder getrennt genutzt noch von unterschiedlichen Versionsständen gestartet werden.

Abbildung 4.21 Speichergruppen und Datenbanken



Exchange 2003 Enterprise erlaubt zusätzlich die Anlage von bis zu vier Speichergruppen mit mehreren Datenbanken. Somit wird ermöglicht, auf einem Server statt einer großen mehrere kleinere Datenbanken zu betreiben. Dies ergibt Vorteile bei der Sicherung und Wiederherstellung, der Verteilung der Belastung auf mehrere Speicherorte und der Anwendung von Richtlinien im Hinblick auf anspruchsvolle Service-Level-Agreements (SLA).

Exchange 2003 Standard erlaubt nur genau eine Speichergruppe mit je einer Datenbank für Postfächer und einer Datenbank für Öffentliche Ordner. Zudem können beide Bereiche je maximal 75 GB groß werden. Die Enterprise Edition ist dagegen unbeschränkt, d.h., nach heutigen Maßstäben liegt die Grenze bei 8 TB und ist nicht wünschenswert zu erreichen. Unab-

hängig von der notwendigen Hardware dürfte die zeitgemäße Sicherung und Wiederherstellung solcher Daten noch einige Zeit benötigen.

4.8.4 Die einzelnen Dateien

Folgende Datenbanken finden Sie auf Ihrem Exchange 2003-Server.

Tabelle 4.4 Exchange-Dateien

Datenbankdatei	Name	Funktion
Datenbank	*.EDB	In dieser Datenbank stehen alle Objekte in 4 KB-Seiten. Die Datei ist nur dann konsistent, wenn alle Transaktionen aus den Protokoll-dateien verarbeitet wurden. (Also nur wenn Exchange sauber beendet wurde.)
Streaming-Datenbank	*.STM	Diese Dateien existieren erst seit Exchange 2000 und enthalten den unveränderten MIME-Inhalt der Nachrichten von Internet-Clients. Die Struktur besteht aus 4 KB-Seiten in 64 KB-Blöcken, die typischerweise mit vielen 64 KB-Zugriffen verwendet werden. Das ist z.B. wichtig für die Festlegung der Größe des Stripe eines RAID-Controllers.
Dateien für die Protokolle der Transaktionen	E00.LOG Ennnnnn.LOG E00temp.LOG res1.log res2.log	Jeweils 5 MB-Dateien, in denen die Transaktionen protokolliert werden, d.h. alle Veränderungen während der Laufzeit. Diese Dateien sind für alle Fälle einer Wiederherstellung notwendig.
Patch-Datei	*.PAT	Bis Exchange 2000 SP2 wurden diese Dateien während der Datensicherung erstellt und enthielten die während der Sicherung veränderten Datenbankseiten. Sie waren zum Restore unbedingt notwendig. Exchange 2003 nutzt diese Datei nicht mehr.
Checkpoint-Datei	*.CHK	Die Checkpoint-Datei enthält die Information, wie weit die Transaktionsprotokolle schon in die Datenbank übernommen wurden. Ohne diese Datei durchläuft Exchange beim Start alle Protokolldateien noch einmal, bis es an die richtige Stelle kommt. Die CHK-Datei beschleunigt den Start, indem Exchange die älteren Protokolldateien überspringt.

Alle Dateien sind mit Prüfsummen und Versionsnummern versehen, so dass der Informationsspeicherdienst immer feststellen kann, ob die korrekten Dateien vorliegen und unverändert sind. Damit ist sichergestellt, dass keine unpassenden Dateien miteinander kombiniert werden und Festplattenfehler unerkannt bleiben.

4.8.5 Datenzugriffe

Wenn Sie die Zugriffe auf die verschiedenen Datenbankdateien kennen, dann erfüllen Sie die besten Voraussetzungen für eine effektive Planung und Partitionierung der Festplatten Ihres Exchange-Servers.

Tabelle 4.5 Dateizugriff und Festplatten-design

Datenbankteil	Zugriff und Designempfehlungen
Transaktionsprotokolle der Speichergruppe	Sequenzieller Zugriff: Dedizierte RAID1- oder RAID 0-1-Arrays.
Objektspeicher (*.EDB)	Kleiner wahlfreier Zugriff (Random I/O (4 KB)): Dedizierte RAID1-, RAID 0+1- oder RAID 5-Arrays je Datenbank. Je nach Last kann dieser Bereich mit der STM-Datei gemeinsam genutzt werden.
Streaming Store (*.STM)	Große wahlfreie Zugriffe (Random I/O (64 KB)): Dedizierte RAID1- RAID 0+1- oder RAID 5-Arrays je Speichergruppe. Je nach Last kann dieser Bereich mit dem Objektspeicher (*.EDB) kombiniert werden.

Mit dem Wissen um diese Zugriffe ist es nun möglich, einen Server entsprechend zu dimensionieren und optimal auf Exchange anzupassen. Allerdings sollten Sie dies in kleinen und mittleren Unternehmen nicht übertreiben. Die Aufteilung macht erst Sinn, wenn Sie sehr hohe Belastungen erwarten, und dann bedeutet es auch den Einsatz mehrerer Festplatten und Controller.

Festplatten-Dimensionierung

Achten Sie primär auf die beiden Ziele: die Verfügbarkeit mittels RAID sowie die Trennung der Protokolldateien aus den Aspekten der Größe und Unabhängigkeit in Schreibzugriff und Recovery bei einem Datenbankwegfall.

4.8.6 Single Instance Store

Nachrichten werden „verlinkt".

Eine Besonderheit von Exchange ist der so genannte „Single Instance Store". Dies bedeutet, dass eine Mail an mehrere Personen innerhalb der gleichen Datenbank nur einmal physikalisch abgelegt wird. Die Benutzer selbst erhalten nur eine Referenz. Da immer mehr Nachrichten „in Kopie" an weitere Kollegen gesendet werden und auch Termineinladungen häufig viele Personen betreffen, wird dadurch Platz gespart. Dies gilt im Besonderen für Anlagen, die meistens ein Vielfaches des Nachrichtenspeichers einnehmen.

Allerdings funktioniert der *Single Instance Store* nur innerhalb der gleichen Datenbank. Schon wenn eine Nachricht an zwei Anwender in zwei unterschiedlichen Datenbanken gesendet wird, ist die Nachricht in beiden Datenbanken vorhanden.

Die Technik eines „Single Instance Store" wird auch anderweitig eingesetzt. So bedient sich der RIS-Server mit dem Groveler ebenfalls einer ähnlichen

Technik, um den Platzbedarf mehrerer Windows-Installationsquellen zu minimieren. Auch Lotus Notes erlaubt es seit einiger Zeit, mehrere Postfächer in einer Datenbank abzulegen. Verschiedene Archivierungssysteme und Datensicherungsprogramme nutzen ähnliche Verfahren, um Platz zu sparen.

4.8.7 Defragmentierung

Ähnlich einem Dateisystem unterliegt auch die Exchange-Datenbank einer Fragmentierung, da im Betrieb immer neue Informationen abgelegt und alte Informationen gelöscht werden. Entsprechend gibt es in der Datenbank freie Bereiche. Exchange startet in der Standardeinstellung jede Nacht ab 02:00 Uhr eine Online-Defragmentierung, bei der Exchange solche als gelöscht markierten Speicherseiten intern wieder freigibt und das tatsächliche Datenvolumen zusammenfasst.

Reicht der freie Bereich nicht mehr aus, so wird die Datenbank in 16 MB-Schritten vergrößert. Allerdings reduziert Exchange die Größe seiner Datenbankdatei nie von alleine. In der Regel wird der freie Bereich immer wieder mit neuen Nachrichten langsam aufgefüllt.

Event-ID 1221 zeigt freien Speicher.

Wenn Sie jedoch sehr große Datenbestände in einer Datenbank löschen, z.B. Benutzer entfernen oder auf einen anderen Server verschieben, dann kann die Verkleinerung von Exchange-Datenbanken wünschenswert sein, um unter anderem die Sicherungszeit zu verringern. Eine Exchange-Datenbank kann „offline“ mit dem Programm ESEUTIL defragmentiert und verkleinert werden. Vorher sollten Sie nicht nur eine Sicherung anfertigen und für ausreichend temporär freien Speicherplatz sorgen, sondern auch in das Eventlog kurz nach 02:00 Uhr schauen. Hier schreibt Exchange hinein, wie viel Platz innerhalb der Datenbank überhaupt frei ist.

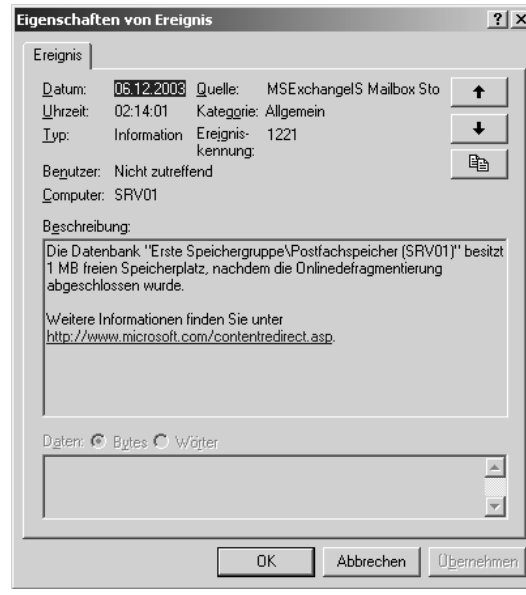


Abbildung 4.22 Eventlog-Meldung freier Speicherplatz in der Datenbank

Diese Meldung finden Sie je Datenbank. In den Eigenschaften der jeweiligen Datenbank können Sie das Wartungsintervall angeben. Achten Sie darauf, dass die Defragmentierung nicht zur gleichen Zeit gestartet wird wie eine Online-Sicherung oder eine Volltextindizierung.

4.8.8 Datenbank-Grenzwert

Datenbanklimit manuell setzen

Exchange Service Pack 2 bietet nun die Möglichkeit, das Datenbank-Limit Ihren individuellen Bedürfnissen anzupassen. Gab es bislang einen festen Grenzwert, bei dessen Erreichung Sie gewarnt wurden, können Sie dieses Limit anpassen, z.B. an der Größe Ihrer Festplatten oder der gewünschten Restore-Zeiten. Der Grenzwert basiert auf der logischen Größe der Datenbanken, also der *.edb-/*.stm-Dateien. Dabei wird zuerst die physikalische Größe der Datenbank ausgelesen und daraufhin der logische Wert ermittelt. Überschreitet dieser Wert das gesetzte Limit oder den Warnpuffer, erhalten Sie eine Fehlermeldung.

Limit entspricht logischer DB-Größe

Im Gegensatz zum bisherigen Verfahren erhalten Sie bei der erstmaligen Erreichung des gesetzten Limits eine Fehlermeldung im Eventlog. Erst 24 Stunden später wird bei anhaltender Überschreitung die Datenbank von Exchange Offline gesetzt. Sie haben infolgedessen 24 Stunden Zeit, die Datenbanken zu minimieren. Für die Reduzierung der Datenbankgröße benötigen Sie nun keine explizite Offline-Defragmentierung mehr. Sie sollten diese Eventlog-Fehlermeldung (Warnpuffer ID 9688, Limit erreicht ID 9689) im Monitoring berücksichtigen.

In der Praxis bietet es sich an, auch bei Enterprise-Servern, dessen Datenbankgrenzwert bei 8000 GB liegt, für jeden Informationsstore den Grenzwert niedriger zu setzen. So können Sie sicherstellen, dass die Datenbanken nie über die Kapazität der Festplatte hinaus wachsen.

Registry-Key: Limit setzen

Die erforderlichen Werte sind nicht im ESM sichtbar und müssen manuell in der Registrierung gesetzt werden. Sie finden die Werte unter dem folgenden Registrierungsschlüssel:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
MSExchangeIS\<SERVER NAME>\Private-<objectGUID>.
```

Datentyp	Name des Werts	Möglicher Wert	Standard-Wert
REG_DWORD	Database Size Limit in GB	Standard-Server: 1-75 GB Enterprise-Server: 1-8000 GB	Standard-Server: 18 GB Enterprise-Server: 8000 GB Unlimited
REG_DWORD	Database Size Buffer in Percentage	1% - 100%	10%
REG_DWORD	Database Size Check Start Time in Hours from Midnight	1 – 24 Stunden	5 Stunden

Neben dem Grenzwert der Datenbank ist hier auch das Setzen des Prozentwertes für die Warnmeldung sowie der Uhrzeit der Prüfung möglich. Den Schlüssel „Database Size Limit in GB“ benötigen Sie ebenfalls, wenn Sie das Limit eines Standardservers nach dem SP2-Update erhöhen möchten. Berücksichtigen Sie jedoch immer die Kapazität des Laufwerks.

4.9 Öffentliche Ordner

Public Folder-Strategien

Exchange ist nicht nur ein System für die Verarbeitung von individuellen Nachrichten in Postfächern, sondern erlaubt auch die gemeinsame Nutzung von Informationen. Hierzu dienen die Öffentlichen Ordner, die Exchange zusätzlich zu den Postfächern bereitstellt. Öffentliche Ordner, oder auch *Public Folder* (PF), sind aber mehr als nur ein weiterer Ablageplatz für Nachrichten. Diese Ordner können mit Hilfe von eigenen Formularen und Ansichten, aber auch mittels Skripten zu sehr leistungsfähigen Plattformen der Zusammenarbeit werden.

Dafür ist es notwendig, auch für den Einsatz der Öffentlichen Ordner ein Konzept zu entwickeln, damit nicht später umfangreiche Umstellungen und Änderungen hohe Kosten verursachen.

Auf die Berechtigungen im Bezug auf Öffentliche Ordner wurde schon im Kapitel 4.7.6 genauer eingegangen. Nachfolgend werden Sie die wesentlichen Informationen für die MAPI-„Top Level Folder“ vorfinden, da diese

beim täglichen Einsatz mit Outlook eine maßgebliche Rolle spielen. Andere Public Folder-Strukturen, aufbauend auf der WebDAV-Schnittstelle, sind für Programmierer interessant, die individuelle Lösungen auf Basis des E-Mail-Systems umsetzen.

4.9.1 Systeminformationen

Nachdem Sie Exchange 2003 installiert haben, finden Sie im Exchange System-Manager neben der Datenbank für die Postfächer auch eine zweite Datenbank für Öffentliche Ordner auf dem Server. In dieser ähnlich aufgebauten Datenbank liegen alle Inhalte, die in den Öffentlichen Ordnern abgelegt werden. Diese Datenbank ist ebenso wie die Postfächer zu sichern und nutzt die gleichen Transaktionsprotokolle wie alle anderen Datenbanken der gleichen Speichergruppe.

Outlook erkennt nur die MAPI-Hierarchie.

Allerdings kann jeder Exchange 2003-Server immer nur genau eine Datenbank für die Öffentlichen Ordner, zugänglich über die MAPI-Schnittstelle in Outlook, betreiben. Neben der eigentlichen Datenbank für Öffentliche Ordner können weitere Datenbanken für die gemeinsame Nutzung angelegt werden. Diese Strukturen sind jedoch über den Outlook-Client nicht erreichbar, indessen eignen sie sich zur Ablage von Daten eigener Anwendungen. Diese zusätzlichen Ordnerdatenbanken sind nicht über MAPI mit Outlook zu erreichen. Aber auch die so genannte MAPI-TLH (MAPI-Top Level-Hierarchie) bietet hinreichende Möglichkeiten, mit dem Standardumfang von Outlook und Exchange 2003-Lösungen zu entwickeln. Doch ehe Sie nun vorschnell Ordner anlegen, sollten Sie ein durchdachtes Konzept ausarbeiten.

Seit Exchange 2003 ist es dem Anwender nicht mehr möglich, selbst Öffentliche Ordner auf oberste Ebene anzulegen. Dies war bei Exchange 5.5 und Exchange 2000 noch möglich und führte überaus schnell dazu, dass die Anzahl der Öffentlichen Ordner außerordentlich rasch und chaotisch anstieg und letztlich nicht mehr effektiv nutzbar waren. Hinzu kam, dass die wenigsten Personen wussten, wie die Ordner verborgen werden konnten. Das Ergebnis sind dann Ordnerstrukturen mit mehreren tausend Ordnern ohne Gliederung, Berechtigungskonzept und Namenskonzept.

4.9.2 Planung der Struktur

Alle öffentlichen (MAPI-)Ordner werden in einer baumartigen Struktur ähnlich einem Dateisystem angezeigt und verwaltet. Diese Struktur, nicht die Inhalte, wird über die gesamte Organisation repliziert. Für Sie bedeutet dies, dass keine Abteilung, kein Standort oder Tochterunternehmen in der Organi-

sation seine eigene Öffentliche Ordner-Struktur unabhängig von den anderen Teilnehmern im Outlook aufbauen kann. Alle Öffentlichen Ordner nutzen die gemeinsame Wurzel und können von allen Personen auch gesehen werden. Damit wird die Planung und Benennung der ersten Ebenen sehr wichtig.

Konzept für MAPI-Ordner-Struktur

Ein kleines Unternehmen mit einem Standort könnte sich darauf festlegen, dass die erste Ebene die Abteilungen repräsentiert. Für jeden Ordner gibt es einen Verantwortlichen, der Berechtigungen vergibt und Unterordner anlegt. Ist das Unternehmen hingegen räumlich verteilt, dann könnten die geografischen Standorte ein Kriterium für die Aufteilung der Ordner sein, auch wenn Sie aus Sicht von Exchange weder notwendig noch sinnvoll erscheint.

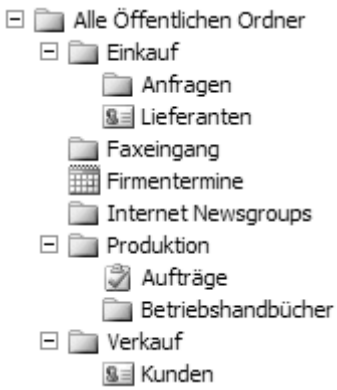


Abbildung 4.23 Öffentliche Ordner-Struktur

Eine Exchange-Organisation, die hingegen aus mehreren Betrieben besteht oder als Service-Provider mehrere Unternehmen bedient, könnte als erste Ebene die Namen der einzelnen Firmen nutzen. Damit jedoch hier eine Abgrenzung besteht, müssen die Berechtigungen von Anfang an stimmen. Bei der Anlage eines neuen Ordners ererbt dieser die Einstellungen der Berechtigungen des übergeordneten Ordners. Unabhängig davon sind die Einstellungen für Replikation und Grenzwerte.

Für den Exchange-Server sind alle Ordner gleichartig, da die Datenbank die Form der Inhalte nicht kennt. Ob ein Ordner für Kontakte, Aufgaben oder Nachrichten vorgesehen ist, erkennt der Client und nicht der Server. Sie können die Ordner zwar mit dem Exchange System-Manager anlegen, doch damit sollten nur die ersten Ebenen vorgegeben werden. Alle weiteren Ordner sollte der jeweilige Verantwortliche mit dem Outlook-Client anlegen und auch hier die Berechtigungen vergeben. Die MAPI-Ordner-Berechtigungen greifen auch, wenn Anwender ohne Outlook über das Protokoll NNTP auf den Exchange-Server zugreifen.

Jedem Ordner können Sie auch eine E-Mail-Adresse zuteilen. Über die E-Mail-Aktivierung eines Ordners können Nachrichten per SMTP an den Ordner gesendet werden.

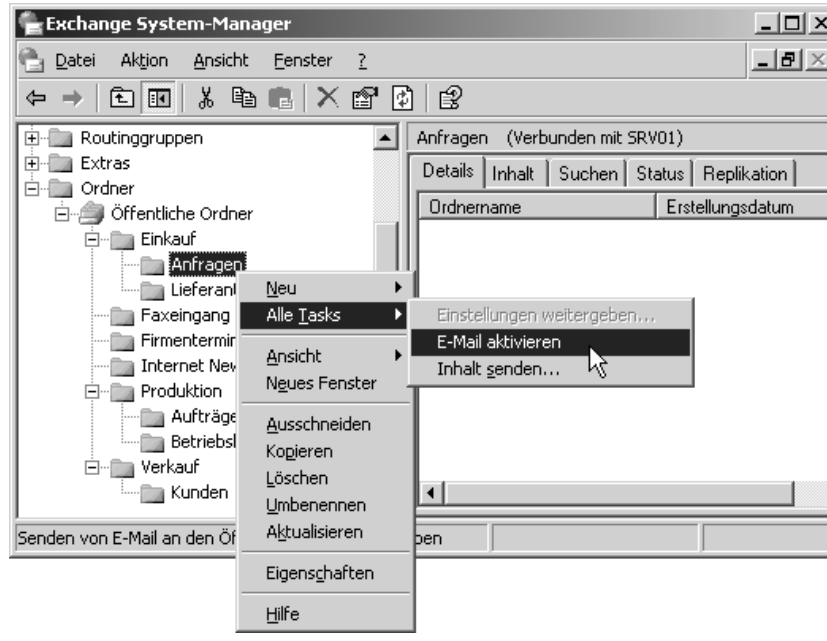


Abbildung 4.24 Öffentliche Ordner: E-Mail aktivieren

Wenn Sie von Exchange 5.5 migrieren, ist jeder Öffentliche Ordner automatisch E-Mail-aktiviert.

Public Folder Einstellungen anpassen

Aufgrund häufiger Probleme wurde die Option EINSTELLUNGEN WEITERGEBEN mit Service Pack 2 durch EINSTELLUNGEN VERWALTEN ersetzt. Bislang war eine gezielte Änderung der Zugriffsrechte ohne Verlust der vorhandenen Rechtestruktur nicht möglich. Nun können Sie einzelne Berechtigungen setzen, Replikate verändern oder Ordnereinstellungen aller Unterordner überschreiben.

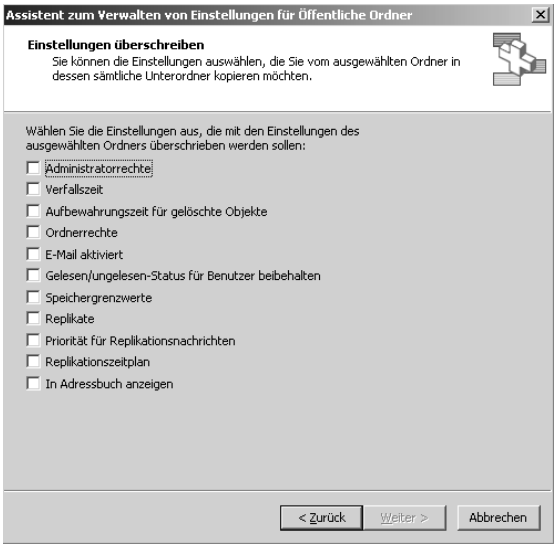


Abbildung 4.25 Einstellungen der Unterordner überschreiben

4.9.3 Replikation

Sobald der zweite Server oder ein weiterer Standort aufgebaut wird, kommt der Faktor Replikation mit in die Diskussion. Öffentliche Ordner können auf mehrere Server repliziert werden. Exchange 2003 sorgt dann dafür, dass die Inhalte dieser Ordner auf allen Servern synchron sind. Der Abgleich selbst erfolgt über einfache E-Mails, die sich die Server gegenseitig zusenden. Spätestens jetzt verstehen Sie auch, warum die Server eine E-Mail-Adresse benötigen.

Für die Replikation gibt es zwei wesentliche Parameter:

- Replikate

  Pro Ordner wird definiert, auf welchem Server ein Replikat des Ordners abgelegt wird. Replikate können in der gleichen Routinggruppe verwendet werden, um die Belastung auf mehrere Server zu verteilen und eine höhere Verfügbarkeit zu erreichen. Allerdings kostet eine Replikation auch Bandbreite, so dass Sie pro Ordner entscheiden müssen, ob der komplette Inhalt auf Dauer z.B. in einer Niederlassung vorgehalten werden muss oder ob es nicht günstiger ist, wenn der Anwender die Informationen die wenigen Male über die WAN-Leitung liest (Referrals).

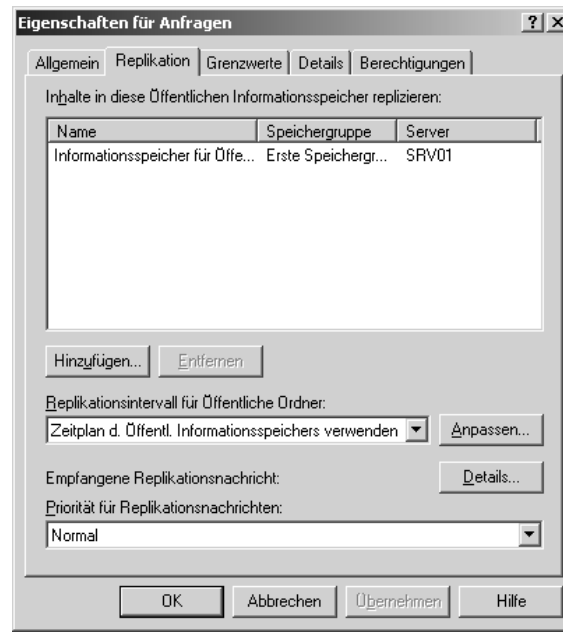
- Replikationszeitplan

  Der Versand der Replikationsnachrichten selbst wird auf dem jeweiligen Informationsspeicher vorgegeben. Zusätzlich können davon aber auch abweichend entsprechende Zeitpläne pro Ordner definiert werden.

Replikations-konflikte

Das generelle Problem bei der Replikation ist indessen die Verzögerung. Legt ein Anwender in einem Ordner etwas ab, so kann es einige Minuten oder gar Stunden dauern, bis die Information auch auf den anderen Servern vorhanden ist. Das Intervall kann zwar bis auf 15 Minuten heruntergesetzt werden, aber es kann trotzdem zu Konflikten kommen. Bearbeiten zwei Anwender auf unterschiedlichen Servern die gleiche Information, beispielsweise den gleichen Kontakt, entsteht ein Konflikt. Exchange erkennt das Dilemma und meldet es dem Ordnerbesitzer. Dieser muss den Konflikt manuell auflösen.

Abbildung 4.26 Einstellen der Replikation bei einem Ordner



Neu in Exchange 2003 hinzugekommen ist die Möglichkeit, die Replikation manuell anzustoßen. Musste mit früheren Versionen gewartet werden, bis die Änderungen entsprechend des Replikationszeitplans auf allen Servern verbreitet waren, veranlasst der Exchange 2003-Administrator mittlerweile den Versand von Änderungen der ganzen Struktur und pro Ordner oder synchronisiert auch die komplette Hierarchie der Öffentlichen Ordner.

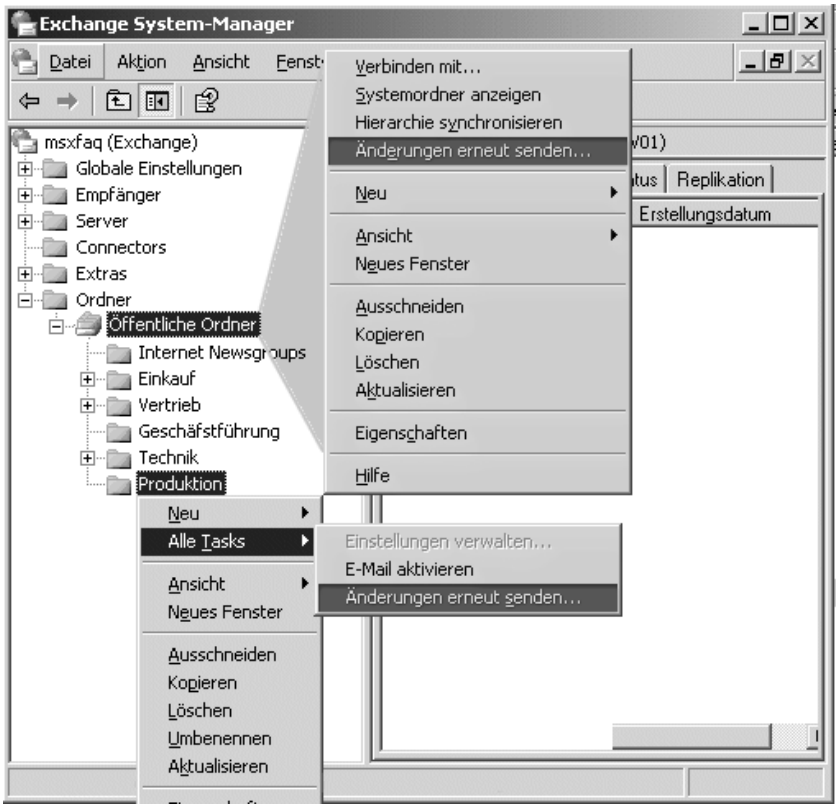
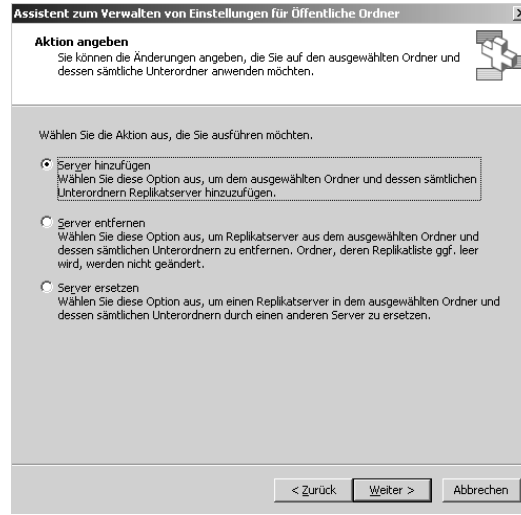


Abbildung 4.27 Replikate und Hierarchie senden

Das Management von Replikaten

Alle Einstellungen bezüglich der Replikation sind nur mit dem Exchange System-Manager ausführbar. Der Zugriff auf diese Informationen für Anwender mit Outlook ist nicht möglich. Über das Kontextmenü im Exchange System-Manager können Sie seit SP 2 die Einstellungen der Ordners verwalten. Neben dem Setzen von Zugriffsrechten und Ordnereinstellungen ist die Replikation Teil des Menüs. Ein Assistent sendet, löscht und verschiebt die Replikate von einem Server auf einen anderen, unter Berücksichtigung der abgeschlossenen Replikationsprozesses.

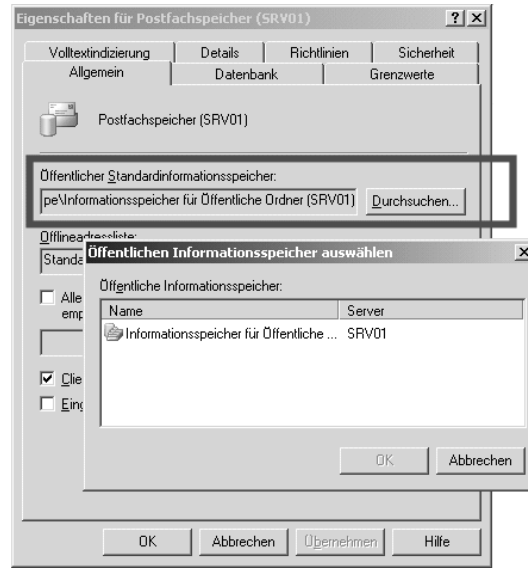
Abbildung 4.28 Replikations-Assistent



4.9.4 Verweise und Affinität

Benutzt der Anwender die Öffentlichen Ordner, holt sich Outlook die Information, welcher Server für Öffentliche Ordner zuständig ist, aus der Datenbank des Postfachservers.

Abbildung 4.29 Standard Öffentlicher Ordnerspeicher



Je Postfachdatenbank wird ein Informationsspeicher für Öffentliche Ordner definiert. Outlook greift dann auf diesen Informationsspeicher zu und zeigt die gewünschten Informationen an.

Die Information über die Existenz aller Öffentlichen Ordner, und welche Berechtigungen darauf gesetzt sind, kennt jeder Exchange-Server mit einem Informationsspeicher für Öffentliche Ordner innerhalb der Organisation. Diese Information liegt selbst in einem versteckten Systemordner und wird wie alle anderen Ordner repliziert.

Greift ein Anwender nun auf einen Ordner zu, der nicht auf dem Server verfügbar ist, erhält der Client von dem Server eine Liste der Informationsspeicher, die ein Replikat des Ordners tragen. Outlook wendet sich dann an einen dieser Server. Hierbei werden Server in der gleichen Routinggruppe zuerst genutzt. Der Zugriff auf Server in anderen Routinggruppen ist ebenfalls möglich. Dazu werden die Kosten anhand der Connectoren zwischen den Routinggruppen berechnet.

In Exchange 5.5 musste diese Funktion noch explizit konfiguriert werden (Stichwort: Öffentliche Ordner-Affinität). Schließlich konnte ein Exchange 5.5-Server nicht davon ausgehen, dass zur Domäne des anderen Standortes eine Vertrauensstellung eingerichtet war, die erst den Zugriff der Benutzer auf die Öffentlichen Ordner des entfernten Standortes ermöglicht hätte.

„disallow referral“

Bei Exchange 2003 ist diese Funktion standardmäßig aktiv, da alle Server im gleichen Forest sind und somit eine Verbindung möglich ist. Allerdings kann der Administrator diese Verweise (Referrals) beim jeweiligen Connector auch deaktivieren, um so den Zugriff über Standorte mit geringer Netzwerkbandbreite zu unterbinden:

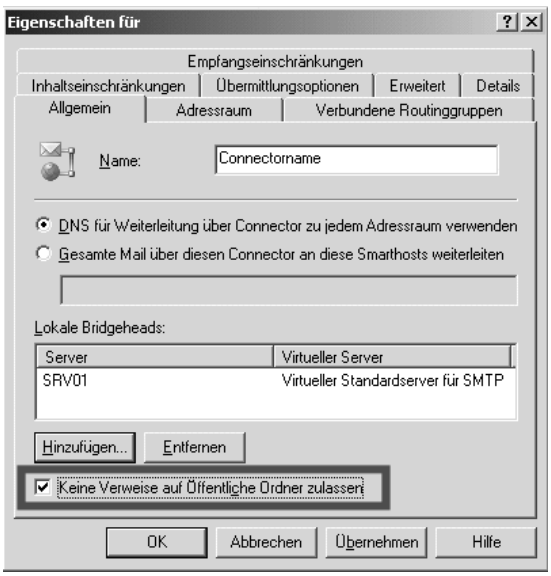


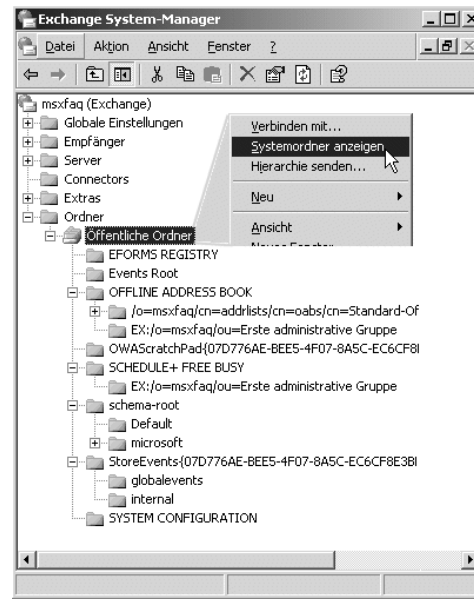
Abbildung 4.30 Verweise auf Öffentliche Ordner zulassen

Welcher Server letztlich vom Anwender genutzt wird, hängt maßgeblich von den oben genannten Einstellungen und der Verfügbarkeit von Replikaten ab.

4.9.5 Systemordner

Ein auf den ersten Blick nicht sichtbarer Teil der Öffentlichen Ordner sind die Systemordner. Sie sind in der gleichen Datenbank abgespeichert wie alle anderen Öffentlichen Ordner auch. Im Exchange System-Manager können die Ordner über das Kontextmenü sichtbar gemacht werden.

Abbildung 4.31 Systemordner anzeigen



Exchange und Outlook nutzen Systemordner für viele Zusatzfunktionen, die für Anwender nicht sichtbar sein sollen. Die wichtigsten Ordner sind:

Tabelle 4.6 System Public Folder

Ordner	Beschreibung
EFORMS Registry	Hier werden globale Formulare für Outlook bereitgestellt, die Struktur kann um weitere Ordner ergänzt werden.
Events Root	In diesem Ordner gibt es für jeden Server, auf dem der Event-Service gestartet wird, einen Ordner. Dort liegen die auszuführenden Skripte.
Offline Address Book (OAB)	In mehreren Unterordnern liegen hier die Adressbücher, die von Exchange 2003 regelmäßig erzeugt werden. Outlook kann diese herunterladen, um die Adressen auch ohne Verbindung zum Server zu nutzen.
OWAScratchpad	Dies sind temporäre Ordner für den Outlook Web Access.
SCHEDULE+ FREE	Die Belegungspläne der Mitarbeiterkalender werden hier in

Ordner	Beschreibung
BUSY	mehreren Ordnern gespeichert. Somit kann bei einer Termineinladung erkannt werden, ob für den Mitarbeiter im fraglichen Zeitraum andere Termine vorliegen.
„schema-root“	Dieser Systemordner enthält die Schemabeschreibungen für Exchange.

Wenn Sie mehrere Exchange 2003-Server betreiben, kann es sinnvoll sein, die Frei-/Belegt-Zeiten von anderen Servern auf Ihren Server zu replizieren und damit den Zugriff auf die Terminvereinbarungen zu beschleunigen.

Sie können mit dem WSS-Explorer (Exchange SDK) oder mit Outlook Web Access in die Systemordner hineinschauen. Die URL dazu lautet

http://<servername>/public/non_ipm_subtree.

Für die Fehlersuche kann dies sehr hilfreich sein, aber vermeiden Sie Änderungen in den Ordnern.

4.9.6 Beispiele zur Nutzung

In Öffentlichen Ordnern werden, wie in Postfachordnern auch, verschiedene Inhalte gespeichert. Sie können Ordner für Nachrichten, Notizen, aber auch für Termine, Kontakte und Aufgaben anlegen. Allerdings ist Outlook das Programm, das diese Unterscheidungen herstellt. Die Nutzung der Öffentlichen Ordner ist nicht nur für die Ablage von Nachrichten gedacht. Die nachfolgenden Beispiele sollen einen Eindruck über den Einsatz von Öffentlichen Ordnern im Unternehmen vermitteln.

Gemeinsame Kontakte

Sharing von Firmenkontakten

In Unternehmen besteht immer die Notwendigkeit, außerhalb der Buchhaltungssoftware Kontaktdaten zu erfassen. Die Nutzung von Kontakten im Postfach ist für die meisten Outlook-Anwender eine Selbstverständlichkeit. Als gemeinsamen Ordner können mehrere Personen zugleich die identischen Daten nutzen und pflegen. So können ganze Abteilungen Kontakte über Lieferanten oder Interessenten führen. Durch die Möglichkeit der Einbindung in das Outlook-Adressbuch können auch alle E-Mail-Adressen dieses Ordners einfach genutzt werden. Dies ist eine Alternative zur Anlage von Kontakten im Active Directory.

Da solch ein Ordner auf dem Server vorliegt, sind Lösungen für den Abgleich mit anderen Datenquellen denkbar. Es gibt fertige Produkte, die Adressen aus anderen Datenbanken in gemeinsame Kontaktordner ablegen.

Faxeingang

Ein weiterer Einsatzzweck ist der gemeinsame Faxeingang für das Unternehmen. Statt der direkten Zustellung eingehender Faxe an ein Postfach oder einen Verteiler hat sich ein Ordner als Ziel bewährt. Dies spart Platz und verhindert doppelte Bearbeitungen. Objekte im Öffentlichen Ordner sind mit Outlook entsprechend zu kennzeichnen, so dass andere Kollegen die Bearbeitung des Vorgangs bereits erkennen. Gegen ein allzu starkes Wachstum kann die Verfallszeit des Ordners aktiviert werden, damit alte Objekte nach einiger Zeit automatisch gelöscht werden.

Support

Abwicklung von Anfragen und Aufgaben im Team

Eine ähnliche Verwendung stellt die Lösung der Supportabwicklung dar. Viele Unternehmen nutzen eine eindeutige Adresse „Support@firma.tld“, um zentral die Anfragen zu erhalten. Ein Verteiler ist weniger gut für diese Anforderung geeignet, da dieser die Anfragen auf alle Mitglieder verteilt und so einen hohen Abstimmungsaufwand erfordert oder eine Doppelbearbeitung mit sich bringt. Eine Besonderheit des gemeinsamen Ordners ist das „Senden im Namen des Ordners“, das als Recht dem Mitarbeiter zugeteilt wird. Auf diese Weise werden ausgehende E-Mails ebenfalls mit „support@firma.tld“ gesendet. Über entsprechende Formulare in diesem Ordner lassen sich weitere Funktionen integrieren. Es gibt sogar komplette Helpdesk-Systeme, die auf Öffentliche Ordnern basieren. Auch eine Aufgabenbearbeitung lässt sich damit wunderbar realisieren, wiederkehrende Tätigkeiten sind für einen ganzen Personenkreis sichtbar, und statt einer Terminierung nutzen Sie die Priorität der Aufgaben.

Systemmeldungen

Monitoring-Funktion

Die Installation vieler Überwachungsprogramme erfordert eine zentrale Stelle, auf der die Meldungen auflaufen. So senden Virenscanner, Datensicherung, Notstromversorgung und viele andere Dienste bei Fehlern eine E-Mail. Auch hierfür bietet sich ein Öffentlicher Ordner an, in dem alle Meldungen ankommen und von einer Gruppe bearbeitet werden. Damit Sie wichtige Meldungen nicht verpassen, aktivieren Sie ein Skript auf diesem Ordner, das bestimmte Nachrichten weiterleitet oder per SMS benachrichtigt.

Offline-Ordner

Vielfach wird von den Außendienstmitarbeitern auch die Offline-Verfügbarkeit der Öffentlichen Ordner gewünscht. Über einen kleinen Umweg lassen sich seit jeher alle öffentlichen Ordner für den Offline-Gebrauch synchronisieren. Sie müssen dazu die gewünschten Ordner als Favoriten im Outlook eintragen und können dann die Offline-Funktionalität nutzen. Unter den Übermittlungsoptionen ist eine dedizierte Auswahl der zu

synchronisierenden Ordner möglich. Beachten Sie jedoch, dass eine lange Offline-Zeit der Mitarbeiter eventuell zu Komplikationen bei der Replikation führen kann.

Diese wenigen Beispiele zeigen auf, wie Sie die Public Folder in Ihrem Unternehmen erfolgreich einsetzen können. Prüfen Sie die Arbeitsabläufe in den Abteilungen, die bestimmt noch weitere Möglichkeiten offen lassen.

4.10 Management der Empfänger

Eine bedeutende Komponente der Exchange-Organisation ist der Aktualisierungsprozess für die E-Mail-Adressen der Empfänger in Ihrer Exchange-Organisation. Wann immer Sie einen Benutzer, Verteiler oder Öffentlichen Ordner für Exchange aktivieren, muss der Empfängeraktualisierungsdienst (Recipient Update Service) für diese neuen Objekte die korrekten E-Mail-Adressen erzeugen und andere Einstellungen vornehmen.

Recipient Update Service (RUS)

Der Empfängeraktualisierungsdienst orientiert sich dabei an den Empfängerrichtlinien, die Sie in der Exchange-Organisation global definieren und im Active Directory abgespeichert werden. Bei Änderungen müssen Sie daher den Zeitbedarf für die Replikation dieser Konfigurationsinformation berücksichtigen.

Das Konzept von Exchange 2003 unterscheidet sich daher grundlegend von der Standortadressierung, wie Sie diese aus einer Exchange 5.5-Umgebung kennen.

Die beiden folgenden Abschnitte erklären die Funktion des RUS und der Empfängerrichtlinien.

4.10.1 Die Empfängeraktualisierungsdienste

Die Funktion des RUS ist kein eigenständiges Programm. Daher finden Sie diesen Dienst auch nicht in der Liste der Exchange-Dienste auf dem Server. Die Funktion des RUS ist Bestandteil der Exchange-Systemaufsicht. Die Funktion des RUS teilt sich in zwei Bereiche:

- Enterprise-RUS

  „RUS (Enterprise Configuration)“

  Der Enterprise-RUS wird bei der Installation des ersten Exchange 2003-Servers erstellt und aktualisiert alle Systemobjekte der Organisation. Damit ist sichergestellt, dass alle Exchange-Server und andere Exchange-Objekte eine E-Mail-Adresse erhalten und innerhalb der Exchange-Organisation erreichbar sind. Dies ist beispielsweise notwendig, damit auch öffentlichen Ordner repliziert werden können.

- Domänen-RUS

„RUS (MSXFAQ)“

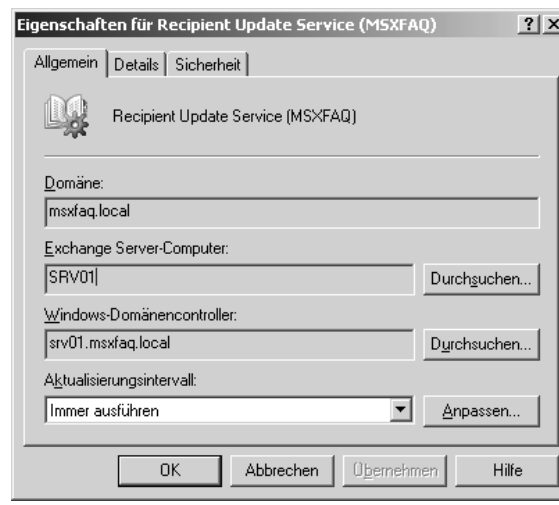
Der Domänen-RUS ist für die Aktualisierung der Exchange-Objekte in einer Domäne zuständig. Wenn Sie mehrere Domänen in Ihrem Active Directory betreiben, müssen Sie manuell für jede Domäne einen eigenen Domänen-RUS hinzufügen. Nur der Eintrag für die erste Domäne wird durch das Setup automatisch erstellt.

Sie müssen dazu in den anderen Domänen des Forests ebenfalls das Exchange-Setup mit der Option „DOMAINPREP“ durchführen, damit die Exchange-Server die notwendigen Rechte zur Verwaltung der Empfänger in dieser Domäne erhalten.

Ohne diese Tätigkeiten können Sie in der Management-Konsole zwar Objekte „Exchange enablen“, aber ohne den entsprechenden Domänen-RUS erhalten die Benutzer keine E-Mail-Adressen und somit auch keine Exchange-Funktionalität.

Ähnlich wie bei der Planung eines Active Directory Connectors ist auch beim RUS zu überlegen, welcher Server die Funktion ausführt. Jeder Eintrag für den RUS bestimmt einen Exchange-Server, der die Änderungen durchführt, und einen Domänencontroller der Zieldomäne, der vom RUS befragt wird.

Abbildung 4.32 RUS-Eigenschaften



Sie können für eine Domäne mehrere Empfängeraktualisierungsdienste einsetzen mit dem Ziel, die Arbeit zwischen mehreren Servern aufzuteilen oder eine Fehlerredundanz zu erreichen. Dies ist aber nur in großen Umgebungen sinnvoll und kann bei falschem Einsatz zu Konflikten bei der Replikation im Active Directory führen.

RUS weist SMTP-Adressen zu.

Der RUS liest von diesem Domänencontroller die neuen oder geänderten AD-Objekte und ändert die Eintragungen entsprechend der Empfängerrichtlinien. Diese Modifikationen werden über das Active Directory wieder zwischen allen DCs der Domäne und auf alle GCs im Forest repliziert.

Nach der Deinstallation eines Domänencontrollers oder eines Exchange-Servers müssen Sie manuell sicherstellen, dass die Konfigurationen der Empfängeraktualisierungsdienste noch gültig sind.

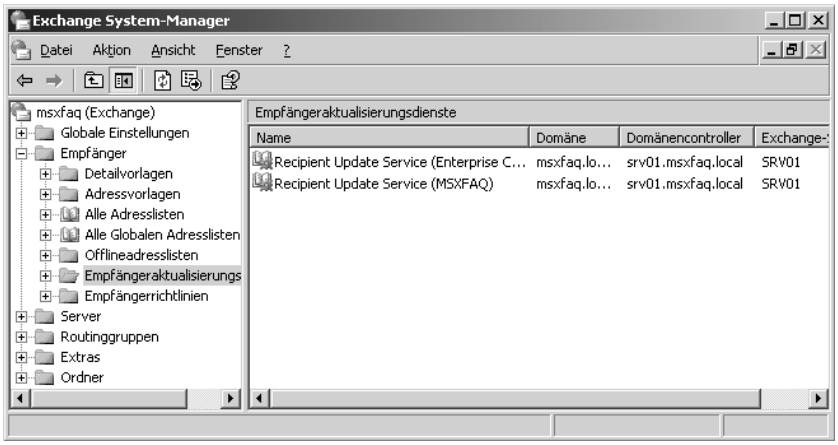


Abbildung 4.33 Empfänger-aktualisierungs-dienste

Richtig konfiguriert verrichtet der RUS problemlos seine Dienste. Durch die Replikation des Active Directory und die Arbeitsweise des RUS können einige Minuten vergehen, bis die Änderungen durchgeführt wurden.

Wartezeit für Replikation berücksichtigen

Der RUS kontrolliert regelmäßig die Domänen auf Veränderungen und arbeitet für jeden geänderten Empfänger die Empfängerrichtlinien nach ihrer Priorität ab. Sobald der Empfänger in eine Richtlinie fällt, wird diese Richtlinie angewendet, und die weiteren Richtlinien werden ignoriert. Somit wird je Objekt nur die Richtlinie mit der höchsten Priorität angewendet, deren Filterkriterien auf das Objekt zutreffen. Wurde der Benutzer bereits vorher durch eine andere Richtlinie konfiguriert, so werden die früheren E-Mail-Adressen jedoch nicht entfernt, sondern bleiben erhalten. Der RUS entfernt niemals eine E-Mail-Adresse von einem Objekt. Dies führt dazu, dass Mitarbeiter, die nun eine andere E-Mail-Adresse erhalten haben, die alten E-Mail-Adressen behalten. Einem neuen Mitarbeiter werden diese alten E-Mail-Adressen nicht mehr zugewiesen. Der RUS stellt ebenso sicher, dass E-Mail-Adressen niemals zweimal vergeben werden. Dies kann jedoch auch beim Einsatz von zwei RUS-Diensten fehlschlagen, wenn diese verschiedene Domänencontroller befragen, die nicht synchron sind.

4.10.2 Die Empfängerrichtlinien

Recipient Policy

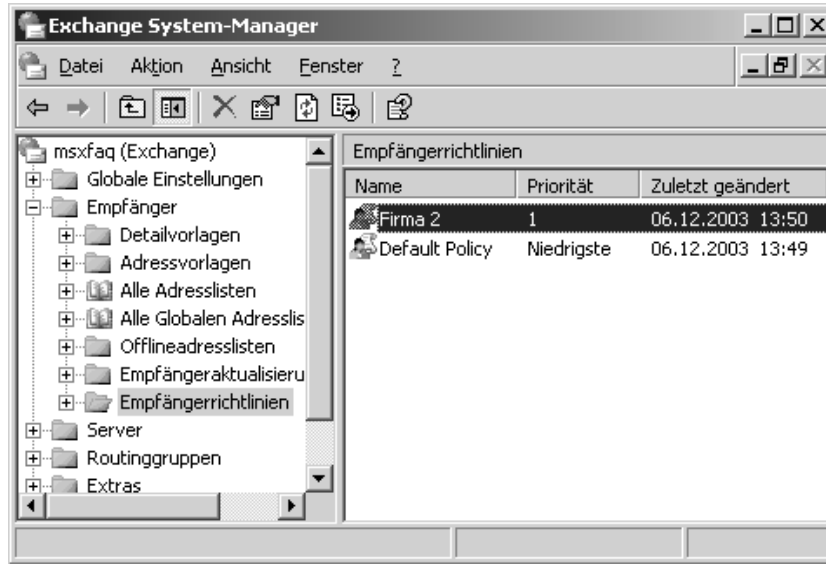
Damit der RUS die Empfänger in den Domänen konfigurieren kann, sind Empfängerrichtlinien zu definieren. Mit dem Exchange System-Manager können Sie viele Richtlinien definieren. Jede Richtlinie (Policy) besteht aus einer LDAP-Abfrage, die eine Auswahl der gewünschten Objekte im Active Directory vornimmt, sowie einer Vorlage zur Bildung der Mailadressen.

Sie können damit z.B. anhand der Anschrift oder dem Firmennamen von AD-Benutzern eine entsprechende E-Mail-Adresse vergeben. Mit diesem Konzept ist Exchange 2003 auch für sehr große Installationen optimal geeignet. Der Exchange-Administrator gibt über die Richtlinien die gewünschten E-Mail-Adressen vor, während der Administrator für die korrekte Pflege der Adress- und Firmendaten beim Benutzer zuständig ist, die die Grundlage der generierten E-Mail-Adressen aller Art (SMTP, X.400 etc.) bildet.

Abhängigkeit von Standort-adressierung

An der höchsten Stelle (Priorität 1) stehen alle Richtlinien, die durch Migration und Koexistenz von Exchange 5.5 übernommen wurden und damit die Funktion der Standortadressierung in Exchange 5.5 sicherstellen. Diese Richtlinien sind nicht änderbar. Erst wenn in einer Administrativen Gruppe kein Exchange 5.5-Server mehr vorhanden ist, können die Richtlinien für diese AG entfallen und die höhere Flexibilität genutzt werden.

Abbildung 4.34 Empfänger-richtlinien



Default Policy nicht ändern!

Es gibt immer eine „Default Policy“, die dann angewendet wird, wenn keine andere Empfängerrichtlinie greift. Diese Standardrichtlinie wird auf alle Exchange-Systemobjekte angewandt, die eine E-Mail-Adresse benötigen, wie die Systemaufsicht. Ändern Sie die Richtlinie niemals, da sonst Fehlfunktionen im Exchange auftreten (siehe auch “Q271339 XADM: Cannot Mount Database and Event ID 9546 occurs”). Diese Standardrichtlinie enthält häufig den gleichen DNS-Namen wie das Active Directory. Wenn Sie individuelle SMTP-Adressen erstellen wollen, können Sie eine neue Richtlinie anlegen, mit dem Filter auf alle Benutzer, Verteiler und Ordner. Diese neue Policy weist den ausgewählten Objekten die gewünschte E-Mail-Adresse zu.

4.10.3 Empfängerrichtlinien und SMTP

Die Informationen in den Empfängerrichtlinien sind auch für die Kommunikation über SMTP essenziell wichtig. So steuern die Empfängerrichtlinien nicht nur die E-Mail-Adresse der Anwender, sondern sind zugleich die Liste der „Inbound-Domains“. Die SMTP-Server erkennen anhand der SMTP-Domänen aller Empfängerrichtlinien, für welche SMTP-Domänen Nachrichten angenommen werden dürfen. Zugleich wird damit auch gesteuert, ob Exchange als Relay eine E-Mail an eine bestimmte Domäne weiterleiten darf.

Mit der Option „autoritativ“, die Exchange verantwortlich für einen SMTP-Adressraum macht, wird die Zustellung der Nachrichten gesteuert, die zwingend intern und nicht über ein Relay zu erfolgen hat. Da die Adressräume in mehreren Richtlinien genutzt werden können, müssen Sie darauf achten, dass die Einstellungen überall identisch sind.

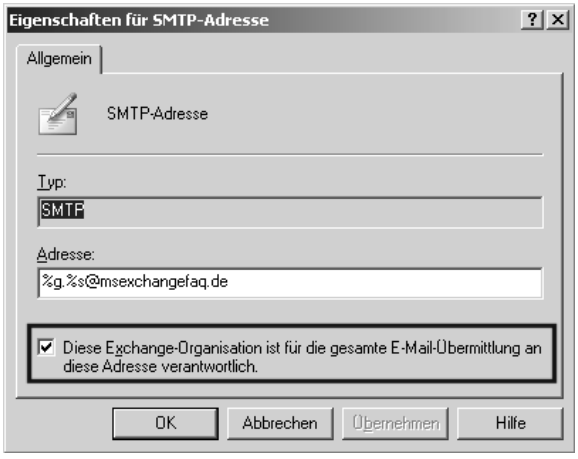


Abbildung 4.35 Autoritative Einstellungen für SMTP

Dabei gilt es zu beachten, dass die primäre SMTP-Domäne (Hauptadresse) der *Default Policy* immer „autoritativ“ sein muss. Wird die gleiche SMTP-Domäne in anderen Empfängerrichtlinien verwendet, dann muss diese auch dort immer als autoritativ aktiviert sein, da ansonsten das Weiterleiten und Zustellen von Nachrichten innerhalb der Exchange-Organisation eventuell nicht mehr möglich ist.

SMTP-Domain-Sharing

Einige Unternehmen setzen mehr als ein E-Mail-System ein und benötigen für alle Systeme die gleiche SMTP-Domäne. Erfordert Ihr Umfeld nun die Mitbenutzung der primären Exchange SMTP-Domäne von anderen fremden E-Mail-Systemen, müssen Sie eine alternative Lösung in Betracht ziehen. Es gibt hier drei Lösungsansätze, die in Frage kommen:

- Fremdes System zuerst

  Vorausgesetzt das fremde E-Mail-System lässt diese Konfiguration zu, dann können Sie alle eingehenden Nachrichten an dieses System zustellen und alle nicht zustellbaren Nachrichten an Exchange weiterleiten lassen. Weiterhin müssten Sie in Exchange mittels eines SMTP-Connectors den Weg zu diesem Fremdsystem weisen für alle nicht auflösbaren Adressen.

- Weiterleitung mit Kontakten

Austausch über Kontakte

  Sofern Exchange Ihr primäres E-Mail-System ist, können Sie alle Benutzer des Fremdsystems in ihrem Active Directory entweder als Kontakt oder als Benutzer mit E-Mail-Adresse anlegen. Dort hinterlegen Sie die E-Mail-Adresse des Benutzers des Fremdsystems (z.B. USER@fremdsystem.firma.de). Eingehende Nachrichten werden dann an die Adresse weitergeleitet. Dieses Verfahren wenden auch die Connectoren zu Notes und GroupWise an. Der ADC bietet für die Synchronisation zwischen zwei E-Mail-Systemen die Möglichkeit von Inter-Org-Verbindungsvereinbarungen an, die häufig in Migrationsumgebungen eingesetzt werden.

- Veränderte Empfängerrichtlinie

  Nutzen Sie mehrere registrierte E-Mail-Domänen, sollten Sie überlegen, die Default-Richtlinie mit einer nicht gemeinsam benutzten SMTP-Domäne als „primäre autoritative Domäne“ einzurichten. So können Sie Ihre eigentliche Domäne mit dem Fremdsystem gemeinsam nutzen. Ein Eintrag wie „firma.local“ ist indessen nicht zweckmäßig, da diese SMTP-Adresse auch für Unzustellbarkeitsnachrichten genutzt und damit oft durch Spam-Filter blockiert wird.

Siehe auch Microsoft TechNet: Q319759 “XADM: How to Configure Exchange 2000 Server to Forward Messages to a Foreign Messaging System That Shares the Same SMTP Domain Name Space“.

4.10.4 Vorlage für E-Mail-Adressen

Jede Richtlinie kann mit Variablen angepasst werden. Hier eine Auswahl:

Tabelle 4.7 Variablen für „Recipient Policy“

Feld	Wert
%g	Vorname (givenName)
%s	Nachname (name)
%i	Initialen (initials)
%m	Alias bzw. Anmeldename (mailNickname)
%d	Anzeigename (displayName)

Kombinieren Sie die Variablen wie häufig verwendet „%g.%s@firma.de“, so werden die E-Mail-Adressen aus Vorname.Nachname@firma.de generiert.

Die Nutzung der Variablen kann noch angepasst werden. Mit dem Eintrag "%1g.%s@firma.de" werden der erste Buchstabe des Vornamens und der Nachname kombiniert. Das Ergebnis wäre dann z. B. „f.carius@firma.de“.

Die Umsetzung der Änderungen kann freilich etwas dauern. Der RUS muss dazu alle Empfänger, auf die das Filterkriterium zutrifft, anpassen. Diese Änderungen im AD müssen wieder repliziert werden und im Globalen Katalog auftauchen. Den RUS können Sie antriggern (anstoßen), damit zumindest der erste Schritt schneller gestartet wird. Die Replikation des Active Directory können Sie z.B. mit REPLMON forcieren.

Deaktivieren des RUS erfordert alternative Prozesse.

Der Administrator hat die Möglichkeit, den RUS pro Benutzer abzuschalten, und damit die Anpassung der E-Mail-Adressen. Dazu wird auf der Karteikarte „E-Mail-Adressen“ des Benutzers die Checkbox für den RUS deaktiviert. In diesem Moment ist der Administrator selber für die Pflege der E-Mail-Adressen verantwortlich. So kann er einem Skript, einem eigenen Administrationsportal oder anderen Diensten wie *Microsoft Identity Integration Server 2003* (MIIS) diese Funktion überlassen.

Es existieren Umgebungen, in denen der RUS für die Domänen komplett abgeschaltet wird und der Administrator mit Hilfe anderer Methoden die korrekte Einstellung für die E-Mail-Adressen sicherstellt. Allerdings sollte der Enterprise-RUS nicht abgeschaltet werden und zudem ein genaues Verständnis der Thematik vorliegen, ehe Sie sich für die Deaktivierung des RUS entscheiden. Weitere Informationen dazu finden Sie im TechNet-Artikel „Q296479 XADM: Requirements for Disabling the Recipient Update Service“.

4.10.5 Update oder Neuaufbau

Eine Änderung in den Richtlinien wird erst dann wirksam, wenn die betroffenen Objekte geändert werden. Selbst wenn Sie eine Richtlinie löschen oder der Filter nicht mehr für bestimmte Objekte zutrifft, erfolgt die Anpassung dieser Objekte erst, wenn Sie die Objekte ändern. Auch eine neue Richtlinie wird nicht auf bestehende Objekte angewendet. Die Ursache liegt darin, dass der RUS nur geänderte Objekte erkennt und anpasst.

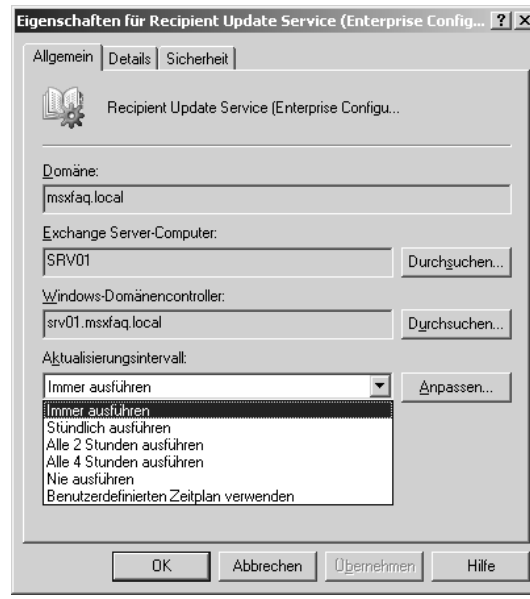
Es ist ratsam, in diesem Fall manuell einen Neuaufbau anzufordern. Hierbei werden dann alle Objekte neu „gestempelt“. Nur so werden alte Objekte, die sich zwischenzeitlich nicht geändert haben, entsprechend der aktuellen Regeln mit den Adressen versehen.

USN als Kennzeichen

Der RUS läuft regelmäßig im Hintergrund und kontrolliert den Globalen Katalog auf Änderungen seit der letzten Abfrage. Bei der Änderung eines

Users ändert sich auch die USN (Update Sequence Number) des Objektes im Active Directory. Der RUS sucht nach Elementen mit einer neueren USN und bearbeitet diese Objekte. Dieser Prozess dauert manchmal länger als erwartet und kann vom Administrator über den Exchange System-Manager beschleunigt werden. Der Standardzeitplan liegt bei 15 Minuten und ist in den Eigenschaften des jeweiligen Aktualisierungsdienstes manuell änderbar.

Abbildung 4.36 Zeitplan des RUS anpassen



Um manuell einen Durchlauf zu starten, können Sie mit der rechten Maustaste im Kontextmenü des jeweiligen RUS die Funktion JETZT AKTUALISIEREN oder NEU ERSTELLEN auswählen. Wann sollten Sie welche Funktion wählen, und worin liegt nun der Unterschied?

- JETZT AKTUALISIEREN

  Diese Funktion triggert den RUS an, seine normale Tätigkeit JETZT auszuführen. Der RUS sucht nach geänderten Objekten und vergibt E-Mail-Adressen. Damit können Sie manuell die Verzögerung anhand eines Zeitplans einmalig außer Kraft setzen.

- NEU ERSTELLEN

  Hierbei werden alle E-Mail-Adressen für diese Domäne anhand der Richtlinien neu gebildet. Auch Objekte, die in der Zwischenzeit nicht geändert wurden, stempelt der RUS neu. Dies bedeutet mehr Aufwand, mehr Zeit, mehr Belastung und sollte nur in Ausnahmefällen durchgeführt werden. Ein Neuaufbau ist beispielsweise nach umfangreichen Änderungen an den Empfängerrichtlinien sinnvoll.

In beiden Fällen werden die bereits vorhandenen E-Mail-Adressen nicht gelöscht, sondern nur die geänderten Adressen hinzugefügt. Somit bleiben alle E-Mail-Adressen erhalten, egal ob sie manuell oder von anderer Richtlinie generiert wurden. Berücksichtigen Sie auch die Replikation durch die Änderung der Benutzer im Active Directory, die zugleich Belastung des AD und Verzögerung der Aktualisierung bedeutet.

Entsprechend können Sie auch bei der Empfängerrichtlinie selbst die Option RICHTLINIE JETZT ANWENDEN im Kontextmenü auswählen und damit Forest-weit eine bestimmte Richtlinie erneut durch den RUS anwenden lassen.

4.10.6 Fehlersuche beim RUS

Probleme mit dem RUS und den Empfängerrichtlinien bemerken Sie häufig dann, wenn Sie ein neues Postfach anlegen und der Anwender das Postfach nicht nutzen kann und nicht im Adressbuch erscheint. Für die Fehlersuche ist der Ablauf vom Erstellen eines Benutzers bis zur tatsächlichen Empfangs-bereitschaft hilfreich, der in den folgenden Schritten dargestellt wird:

1. Benutzer im AD anlegen und Exchange aktivieren.
2. Replikation der Änderungen auf die anderen Domänencontroller, die je nach Einstellung mehrere Minuten dauert. Windows 2003 repliziert innerhalb eines Standorts ca. alle 15 Sekunden. Windows 2000 lässt sich hierfür bis zu fünf Minuten pro Server Zeit. Mit REPLMON können Sie die Replikation beschleunigen und kontrollieren. Sie können auch in der Management-Konsole konfigurieren, dass Ihre Änderungen auf dem DC durchgeführt werden, der auch vom RUS befragt wird. Wenn Sie nur einen DC betreiben, sind die Änderungen sofort verfügbar.
3. Der für diese Domäne zuständige RUS erkennt entsprechend dem eingestellten Zeitplan die Änderung und wendet die Richtlinien an. Der Benutzer oder Verteiler erhält die vorgesehene E-Mail-Adresse. Auch diese Änderungen müssen bei mehreren Domänencontrollern erst wieder repliziert werden. In der Management-Konsole ADUC können Sie nun diese E-Mail-Adressen kontrollieren. Vergessen Sie nicht mit der F5-Taste die Ansicht zu aktualisieren, damit die MMC die Daten aktualisiert.
4. Diese Informationen müssen nun noch auf alle Globalen Kataloge im Forest repliziert werden, damit wirklich alle Exchange-Server das Postfach kennen und Nachrichten zustellen können. Daher dauert es einige Zeit, bis auch alle anderen Benutzer in Outlook das neue Postfach sehen und erreichen können.
5. Erst wenn das Postfach die erste Mail erhält, wird auch ein Eintrag in der Datenbank vorgenommen. Erst dann ist auch das Postfach in den Ressourcen des Postfachspeichers sichtbar.

Nachdem Sie nun einen neuen Benutzer für Exchange aktivieren, können Sie anhand der aufgezeigten Schritte kontrollieren, wie weit diese Konfiguration schon durchgeführt wurde. Ist bei all diesen ineinander greifenden Prozessen „der Wurm“ drin, dann dauert es noch länger bzw. findet niemals statt. Getreu dem Motto:

- 70 % aller Exchange-Fehler sind in der Regel Active Directory-Probleme.
- 50 % aller Active Directory-Probleme werden durch DNS-Probleme oder Fehlkonfigurationen des Netzwerks verursacht.

Kontrollieren Sie daher regelmäßig die Funktionsweise des Active Directory und des RUS. Hierzu stehen Programme wie REPLMON und DSASTAT aus dem *Windows Server 2003 Resource Kit* zur Verfügung. Weitere Hilfsmittel zur Fehlersuche und Hinweise auf Probleme sind:

Das Diagnoseprotokoll

Der RUS ist ein Bestandteil des Prozesses „ExchangeAL“. Weitere Informationen in der Ereignisanzeige (Eventlog) des Servers erhalten Sie, indem Sie das Diagnoseprotokoll des Exchange-Servers für den Bereich *ExchangeAL* hoch setzen.

DC verändert sich

“Single Point of Failure”

Der RUS wird im Exchange System-Manager konfiguriert und baut eine Verbindung mit genau einem Domänencontroller auf, über den er Änderungen an den Objekten feststellt und die E-Mail-Adressen einträgt. Sobald der DC nicht „online“ ist oder gar deinstalliert wurde, führt der RUS keine Adressaktualisierungen mehr durch. Der Fehler wird im Eventlog gemeldet. Ändern Sie einfach den DC in den Eigenschaften des RUS, um das Problem zu beheben.

3rd Party-Adressgeneratoren

Oftmals gibt es in einer Exchange-Organisation neben den Adresstypen SMTP und X.400 noch weitere Adressen wie GSM, FAX, TELEX, SMS etc. Wird eine Empfängerrichtlinie mit solchen Adressen erstellt oder bei der Migration von Exchange 5.5 übernommen, so muss der RUS natürlich auch für diese Adressen die notwendigen DLLs finden können.

Eigene DLL für Fax usw.

Fehlen diese DLLs auf dem Server, dann erstellt der RUS überhaupt KEINE Adressen mehr für neue Anwender. Um das Problem zu lösen, müssen Sie die entsprechenden DLLs z.B. vom Exchange 5.5-Server kopieren oder vom Hersteller anfordern. Sie finden die DLL in der Freigabe „ADDRESS“ und können die entsprechenden Unterverzeichnisse in das ADDRESS-Verzeichnis des Exchange 2003-Servers kopieren, auf dem der RUS ausgeführt wird. Welche DLL genau fehlt, finden Sie in der Beschreibung im Eventlog,

nachdem Sie die Diagnoseprotokollierung des *ExchangeSA* auf dem Exchange-Server hochsetzen.

Halten wir fest:

- Der RUS ist elementar für das Setzen der E-Mail-Adressen aller Empfängerobjekte nach den definierten Richtlinien.
- Der Enterprise-RUS versorgt die Systemobjekte mit E-Mail-Adressen, der Domänen-RUS alle Empfängerobjekte in seiner Domäne.
- Ändert sich der Domänencontroller, der vom RUS genutzt wird, müssen Sie dies in den RUS-Eigenschaften anpassen.
- Deinstallieren Sie einen Exchange-Server, müssen Sie ebenfalls prüfen, ob davon ein RUS betroffen ist und gegebenenfalls umkonfiguriert werden muss.
- Exchange bietet keinen Automatismus, der neue Domänen im Active Directory erkennt und den RUS konfiguriert. Die Domänen müssen mit `Setup /domainprep` vorbereitet und der RUS manuell angelegt werden.

4.11 Filtern, blockieren und begrenzen

Exchange 2003 erlaubt an vielen Stellen die Kontrolle der Nachrichten und Inhalte über verschiedene Optionen. Solche „Sperren“ sind global oder auch pro Connector, pro Server oder je Datenbank und Anwender möglich.

4.11.1 Globale Blockaden und Grenzen

Im Exchange System-Manager können global wirksame Konfigurationen für die gesamte Organisation eingestellt werden.

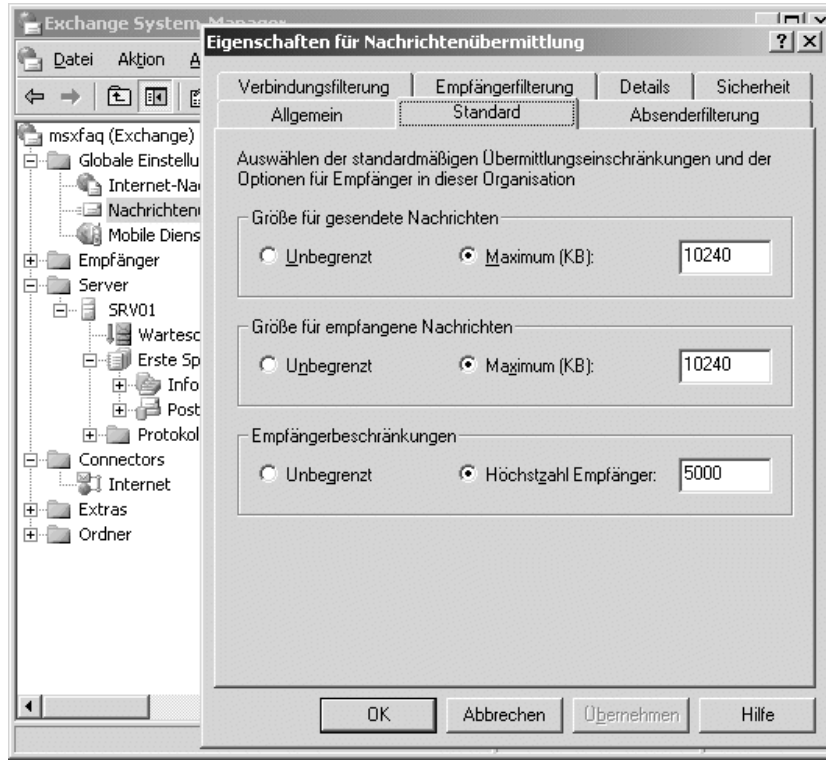


Abbildung 4.37 Globale Grenzen der Nachrichtenübermittlung

Im Bereich der Nachrichtenübermittlung sind folgende Werte gesetzt:

- *Standard*: Größe für gesendete und empfangene Nachrichten.

  E-Mail-Limit

  Hiermit wird organisationsweit die maximale Größe für Nachrichten gesetzt. Der Standardwert beträgt 10240 Kilobyte. Die Begrenzung dieser Größe bedeutet nicht, dass die verfügbare Bandbreite zwischen Servern und Clients weniger stark belastet wird. Um auf dem Netzwerk Begrenzungen für die Belastung durch den Mailverkehr einzusetzen, sind Hilfsmittel wie QoS (Quality of Service) von Windows 2003 einzusetzen.

- *Standard*: Anzahl der Empfänger

  Maximal 5000 Empfänger können in einer Nachricht innerhalb der Exchange-Organisation adressiert werden.

- *Absenderfilterung*: Absenderadressen blockieren

  Die hier eingetragenen Adressen können global von allen virtuellen Servern blockiert werden. Dazu ist jedoch die Aktivierung der Filterung auf jedem virtuellen SMTP-Server erforderlich, der eingehende Nachrichten annimmt.

- Verbindungsfilterung von IP-Adressen

  Exchange ermöglicht die Abfrage von Sperrlisten verschiedener Anbieter. Diese werden über das DNS-Suffix eingetragen und verhindern die Verbindungsaufnahme mit bestimmten IP-Adressen und DNS-Namen. Zudem können statisch spezifische Adressen abgelehnt oder generell zugelassen werden. Ebenso wie die Absenderfilterung muss die Verbindungsfilterung auf jedem virtuellen SMTP-Server aktiviert werden.

- Empfängerfilter

  Ebenso gehört auch der Empfängerfilter zu den Nachrichtenübermittlungseinstellungen, der im virtuellen SMTP-Server explizit aktiviert werden muss. Gelistet werden hier Empfänger, deren E-Mail-Adressen aus dem Internet nicht erreichbar sein sollen. Eine weitere Option beschränkt den Empfang der Nachrichten auf alle existierenden Empfänger. Nachrichten für unbekannte Empfänger werden aus dem Internet nicht angenommen.

Diese Filter für eingehende Nachrichten und Verbindungen funktionieren jedoch nur dann, wenn Exchange die E-Mails aus dem Internet erhält. Sobald Sie ein Relay oder einen POP3-Sammler vor dem eigentlichen Exchange-Server einsetzen, sind die Nachrichten schon in Ihrer Firma. Lehnt Exchange dann diese Nachrichten ab, müssen Sie Vorsorge treffen, dass das zwischen Internet und Exchange geschaltete Programm nicht auf Probleme läuft.

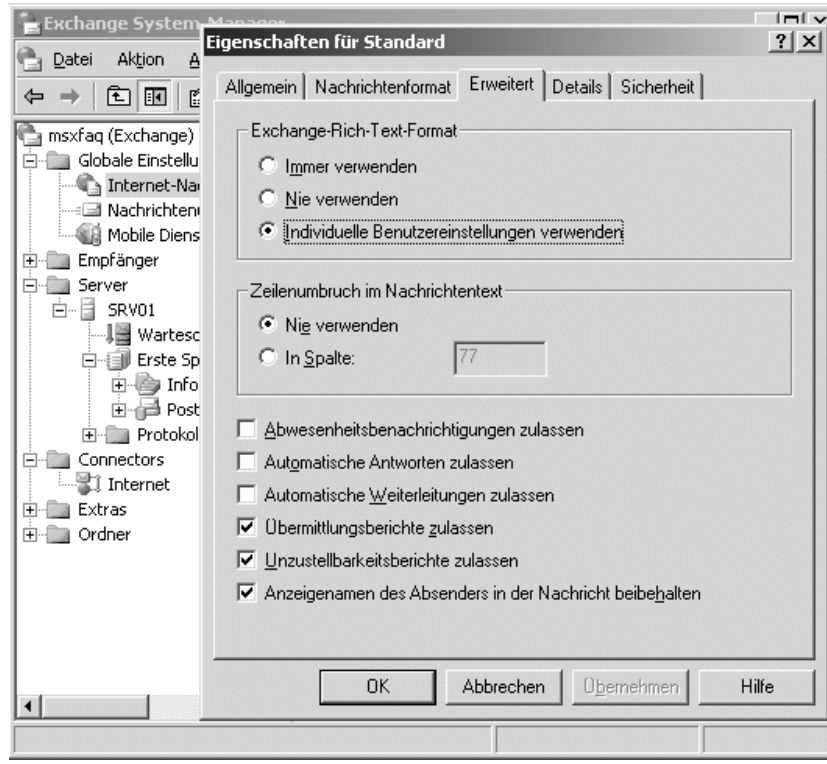
Einschränkungen der „out of the box“-Filter

Der Einsatz von solchen Filtern ist immer eine Abwägung des tatsächlichen Nutzens. Die Begrenzung der maximalen Nachrichtengröße ist sinnvoll, um eine Überlastung oder den Missbrauch der Server zu erschweren. Allerdings sind gerade diese Filter, gegen Spam und andere unerwünschte Nachrichten, nicht ausreichend, um einen effektiven Schutz zu erhalten. Hier sind zusätzliche Produkte weiterhin einzuplanen.

4.11.2 Internet-Einstellungen

Auch für den Betrieb mit dem Internet sind leistungsfähige Filter und Blockaden einsetzbar. Diese Sperren werden pro SMTP-Domäne definiert und steuern die ausgehenden Nachrichten. Für jede Domäne ist ein eigener Eintrag notwendig.

Abbildung 4.38 Begrenzungen für Internet-Nachrichten



Die Einstellungen gelten für die gesamte Organisation. Die Standardeinstellungen sind in dem Eintrag „*“ der Internet-Nachrichtenformate hinterlegt.

- Nachrichtenformat

  Sie können einstellen, ob Exchange für die konfigurierte SMTP-Domäne nicht die Standardeinstellungen (MIME) zur Übertragung nutzt, sondern abweichend z.B. UUENCODE oder einen anderen Zeichensatz. Es kann ebenfalls gesteuert werden, ob Nachrichten nur als Text, als HTML oder in beiden Formaten übertragen werden.

- Erweitert

  Diese Einstellungen sind sehr viel interessanter, da sie die Übermittlung von Abwesenheitsnachrichten, automatische Antworten oder Quittungen an die Domäne steuern. So kann es durchaus sinnvoll sein, nur an bestimmte vertrauenswürdige Domänen die Information zu senden, dass ein Mitarbeiter nicht erreichbar ist, und an alle anderen Absender diese Abwesenheitsmeldung zu unterdrücken. Auch die Blockade von Zustell- oder Gelesen-Quittungen schützt die Privatsphäre, wenn der Absender nicht nachverfolgen kann, ob das Postfach existiert und wann Sie Ihre Nachrichten lesen.

Für den Versand der E-Mails ist die Einstellung „Exchange Rich Text“-Format wichtig. Vorausgesetzt Sie wissen, dass die Empfängerseite ebenfalls Exchange nutzt, dann können Sie durch die Aktivierung dieses Formats auch über die Grenzen der Organisation hinaus unter anderem auch Outlook-Einladungen so versenden, dass die Gegenseite zusagen kann.

Möchten Sie zusätzlich je SMTP-Domäne auch die maximale Größe der Nachrichten oder einen speziellen Server bestimmen, dann sind hierzu die Einstellungen beim SMTP-Connector zu konfigurieren.

4.11.3 SMTP-Connector-Einstellungen

Globale Filter

Für den Versand in das Internet dient der SMTP-Connector, der etwas später noch beschrieben wird. Auch auf dem SMTP-Connector sind Grenzwerte und Beschränkungen einstellbar.

- Nachrichtengröße

  Für jeden Connector kann die maximale Größe einer Nachricht eingestellt werden. Da ein Connector oft mehrere Domänen bedient, können so recht einfach bestimmte Domänen mit gleichen Einstellungen zusammengefasst werden.

- Empfangsbeschränkungen für ausgehende Mails

  Sie können pro Connector steuern, welche Personen eine Nachricht hierüber senden dürfen. Damit kann verhindert werden, dass bestimmte Personen oder Gruppen eine Nachricht in das Internet senden.

Diese Einstellungen sind global in der ganzen Organisation bekannt und sollten deshalb aufeinander abgestimmt sein.

4.11.4 Servergrenzwerte auf den Datenbanken

Spezifische Konfigurationen nicht zu stark eingrenzen.

Auch auf den Datenbanken des Servers sind Grenzwerte einstellbar. Standardmäßig gibt es keine Begrenzung auf Postfachgrößen und Nachrichtengrößen. Es ist absolut sinnvoll, Limits einzuführen, um zum einen absichtlichen oder unabsichtlichen Missbrauch des Servers zu verhindern und andererseits die Verfügbarkeit des Systems für alle Mitarbeiter zu erhalten. Die Grenzen sollten aber nicht so gewählt werden, dass die Anwender zu Alternativen genötigt werden. Spätestens wenn die Anwender beginnen, Firmennachrichten als PST-Datei auf lokale Festplatten auszulagern, über Mailserver im Internet (wie GMX oder WEB.DE) ihre Nachrichten zu senden oder größere Anlagen in kleine Portionen aufzuteilen, sind die Grenzen zu eng gesetzt. Auf der anderen Seite muss aber auch sichergestellt werden, dass ein Anwender nicht versehentlich die komplette Festplatte an einer E-Mail anhängt oder das Postfach extrem wächst und dies

zu Lasten der anderen Mitarbeiter geht. In der Vergangenheit haben Postfachgrenzen sehr oft schlimmeres verhindert, wenn ein Mailvirus in dem Unternehmen sein Unwesen treibt.

Bei Migrationen sollten Sie erst nach der Migration des Postfachs die Grenzen setzen, damit die Migration selbst nicht mangels Platz abbricht und zu Fehlern führt.

Postfachspeicher

Auf den Datenbanken für Postfächer sind folgende Einstellungen möglich:

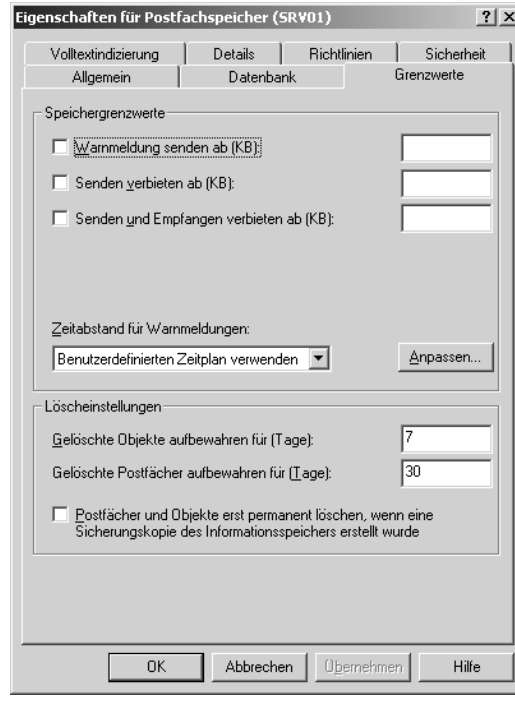


Abbildung 4.39 Grenzen des Postfach-speichers (Mailbox Store)

Die Werte greifen für den kompletten Mailbox Store und bedeuten:

- Speichergrenzwerte

  Diese Einstellungen definieren global für alle Anwender in dieser Datenbank die maximale Größe des Postfaches und bei welchen Grenzen der Anwender eine Warnung erhält, und ab wann er keine Nachrichten mehr senden darf. Es ist sinnvoll, hier Obergrenzen zu setzen, damit die Anwender sich frühzeitig melden oder bei Missbrauch oder Virus-einbruch nicht die Funktionalität der anderen Anwender beeinträchtigt wird. Ohne manuelle Konfiguration sind keine Grenzwerte vorhanden.

- Löscheinstellungen Mails

  Beim Löschen einer Nachricht durch den Anwender macht es Sinn, diese nicht gleich von Exchange hart in der Datenbank entfernen zu lassen, sondern für eine bestimmte Zeit vorzuhalten. So können versehentliche Löschvorgänge oft wieder ungeschehen gemacht werden. Allerdings ist der Standardwert auf 0 Tage gestellt, so dass erst eine Anpassung durch den Administrator diese Funktion freischaltet.

- Löscheinstellungen Postfächer

  Ebenso werden Postfächer, zu denen das dazugehörige Benutzerkonto gelöscht worden ist, für die Dauer von 30 Tagen nicht aus der Datenbank entfernt. Auch dieser Wert ist einstellbar. Die erneute Verbindung mit dem Benutzer erleichtert das Wiederherstellen von Postfächern.

Service Pack 2 ermöglicht nun auch die individuelle Begrenzung der Datenbankgröße. Diese wird nicht in dem Exchange System-Manager gesetzt, sondern durch einen harten Eintrag in der Registrierung für jede Datenbank einzeln festgelegt (Database Size Limit in GB).

Öffentliche Ordner-Grenzwerte

Public Folder Limits

Auf Öffentliche Ordner-Speicher können ebenfalls globale Grenzwerte gesetzt werden. Ähnlich den Postfachgrenzwerten sendet Exchange eine Warnung an den Ordnerbesitzer beim Erreichen des Limits. Dieser Prozess wird ausgelöst, wenn der Ordner eine bestimmte Größe erreicht hat und damit die Ablage neuer Elemente verhindert, oder wenn das einzelne Element zu groß und das Limit erreicht ist. Besonders praktikabel sind diese übergreifenden Einstellungen im Gegensatz zum Setzen von Grenzwerten pro Ordner. Andererseits können die Anwender diese Bereiche sehr unkontrolliert mit allen möglichen Daten füllen, so dass Sie entsprechende Maximalwerte vorgeben sollten:

- Warnmeldung

  Die maximale Objektgröße ist mit 10 Megabyte für die Musterumgebung ausreichend. Allerdings sollten Sie zumindest eine obere Warngrenze einführen, damit die Ordnerbesitzer über fehlende Ordnereinstellungen informiert werden.

- Bereitstellen

  Die zweite Grenze verbietet den Anwendern, weitere Objekte einzustellen. Auch wenn hier pro Ordner ein individueller Wert sinnvoller erscheint, sollten Sie einen globalen Maximalwert definieren.

- Maximale Objektgröße

  Die Obergrenze von 10240 KB kann heutzutage schon sehr klein bemessen sein. Alternativ zur Änderung des Standards sollten Sie sehr

genau die einzelnen Ordner prüfen, welche durch diese Grenze in der Funktion behindert würden, und diese Werte setzen.

Auch im Speicher für Öffentliche Ordner können Vorgaben für das Löschen von Elementen gesetzt werden:

„Lösch-Optionen“

- Gelöschte Objekte

  bewahrt Exchange 2003 grundsätzlich für sieben Tage auf, vorausgesetzt der Standardwert wurde nicht angepasst.

- Die Verfallszeit

  bestimmt, zu welchem Zeitpunkt alte Elemente automatisch gelöscht werden. Ein Eintrag hier sorgt unweigerlich für den Verlust aller Daten, die älter als der festgelegte Zeitraum sind. Sie sollten den Wert daher nie global setzen, sondern bei Bedarf pro Ordner individuell eintragen.

Um die Verwaltung zu vereinfachen, erlaubt Exchange 2003 die Konfiguration dieser Einstellungen über Richtlinien. Damit können die Einstellungen vieler Server zentral gesteuert werden. Die Zuweisung durch Richtlinien ist in größeren Umgebungen sehr hilfreich, beim Einsatz weniger Server durchaus nicht erforderlich.

4.11.5 Individuelle Grenzwerte für Öffentliche Ordner

Neben den Standardbegrenzungen auf Informationsspeicherebene der Öffentlichen Ordner können auch pro Ordner individuelle Einstellungen gesetzt werden.

Über den Exchange System-Manager werden dazu auf jedem Ordner abweichend vom Standard des Informationsspeichers die Werte für Warnmeldungen, maximale Objektgröße und maximale Ordnergröße konfiguriert und damit eine Zustellung von Nachrichten verhindert.

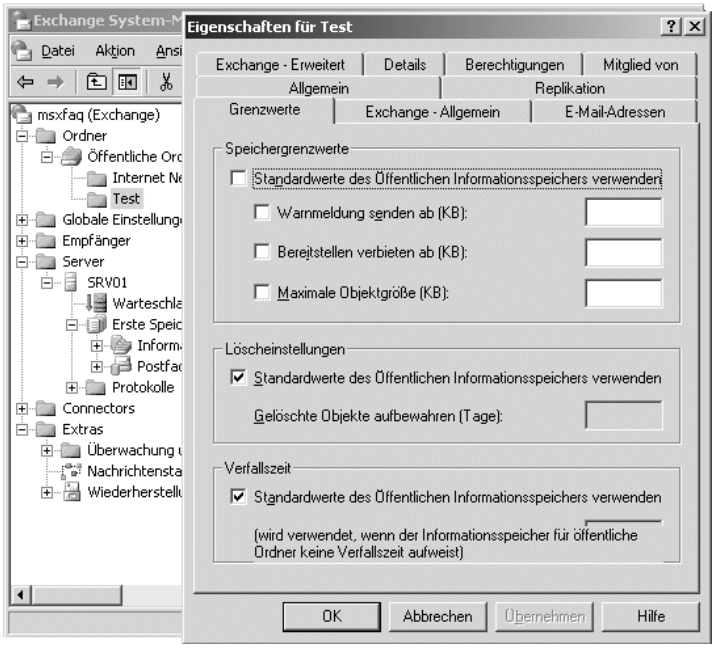


Abbildung 4.40 Individuelle Grenzwerte pro Öffentlichen Ordner

Neben den Einstellungen für Grenzwerte können weiterhin Empfangsbeschränkungen eingetragen werden. Diese wirken auf Nachrichten an E-Mail-aktivierte Ordner.

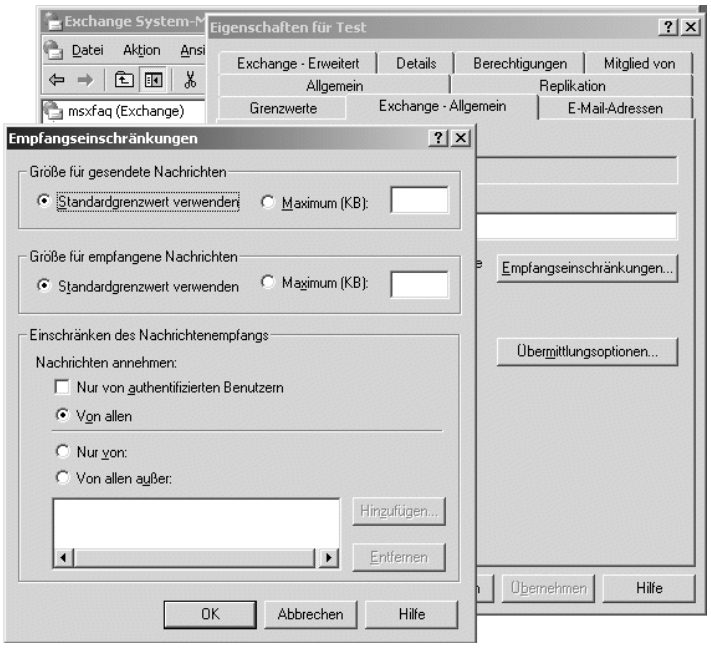


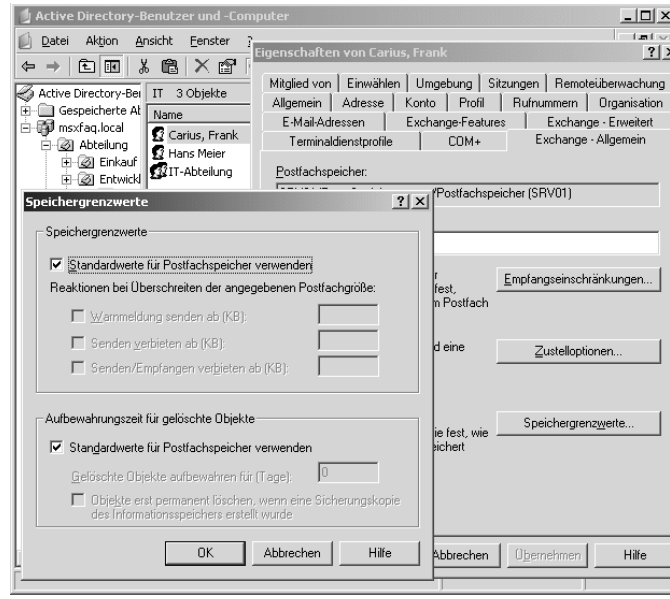
Abbildung 4.41 Empfangsbeschränkungen und Größen auf einem Ordner

So lässt sich die Größe der E-Mails an die Ordner steuern sowie der Kreis der Benutzer, die Nachrichten einem Ordner zustellen dürfen.

4.11.6 Grenzwerte für einzelne Postfächer

Unabhängig von den gesetzten Limits des jeweiligen Postfachspeichers sind für die Benutzer abweichende Grenzwerte möglich. Diese individuellen Limits sind manuell in der Management-Konsole für Active Directory-Benutzer und -Computer beim Benutzer zu pflegen.

Abbildung 4.42 Grenzwerte für Postfachgrößen



Die Werte der Speichergrenzen des Benutzers können die gleichen Einstellungen wie beim Postfachinformationsspeicher enthalten. Die spezifischen Einstellungen überschreiben immer den Standardwert der Datenbank. Zusätzlich können je Anwender in den Empfangsbeschränkungen und Zustelloptionen Grenzen für die individuelle Postfachnutzung konfiguriert werden.

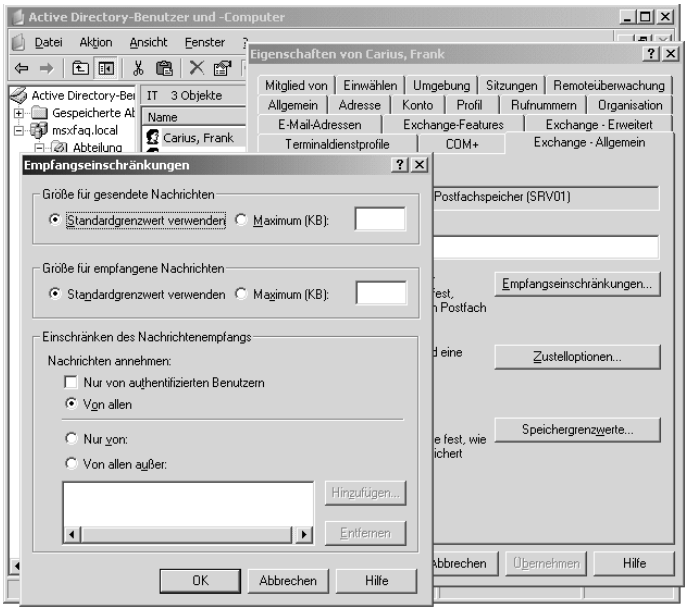


Abbildung 4.43 Grenzen für Nachrichtengrößen bei Anwendern

- Größe für gesendete und empfangene Nachrichten

  Unabhängig von den globalen Werten für die Nachrichtengröße allgemein und auf den Connectoren kann pro Anwender ein noch niedrigeres Limit eingestellt werden.

- Einschränken des Nachrichtenempfangs

  Diese Einstellung ist sehr hilfreich zum Schutz von Systemkonten oder speziellen Anwendern (z.B. der Vorstand ist nur für bestimmte Personen oder Verteiler zu erreichen). In der Praxis hat es sich allerdings bewährt, das offizielle Mailkonto durch Vertreter betreiben zu lassen und derart wichtigen Personen intern eine nicht allgemein bekannte Adresse zuzuordnen.

- Maximale Anzahl der Empfänger

  Pro Benutzer ist regulierbar, an wie viele Empfänger ein Rundschreiben maximal gleichzeitig gesendet werden kann. Sofern in Ihrem Unternehmen nur wenige Nachrichten an einen großen Personenkreis gehen, ist ein Limit hier ein nützlicher Schutz vor Missbrauch.

Die Vielzahl der möglichen Grenzen, Blockaden, Filter und Warneinstellungen erlaubt eine sehr effektive Konfiguration der Exchange-Umgebung. Die Anwender können problemlos damit arbeiten, und Sie haben die Gefahr von Missbrauch und Überlastungen reduziert. Allerdings ist eine klare Konzeption und Dokumentation der einzelnen gesetzten Parameter unerlässlich, um später notwendige Anpassungen schnell zu finden.

4.11.7 Sinnvolle Werte

Erfahrungswerte einsetzen

Im praktischen Einsatz haben sich einige Limits bewährt, die schon bei der Erstinstallation sinnvoll wirken. Exchange 2003 legt durch die Installation einige Grenzwerte fest, die Sie überprüfen und gegebenenfalls anpassen sollten:

- Postfachlimits

  Exchange 2003 stellt keine Grenzwerte ein. Hier sollten Sie zumindest überlegen, ob Sie auf dem Postfachspeicher für alle Postfächer eine Limitierung vornehmen, die die Anwender nicht gängelt, aber rechtzeitig über das Wachstum informiert. Sie müssen auf jeden Fall verhindern, dass Anwender aus Platzmangel die Daten in ungesicherte PST-Dateien verschieben. Einzelne Power-User können über individuelle Einstellungen gesondert behandelt werden.

- Transportlimit innerhalb der Organisation

  Exchange 2003 führt hier eine Grenze von 10240 Kilobyte ein. Den meisten Unternehmen ist der Wert ausreichend, da größere Dateien besser über gemeinsame Zugriffe auf Dateiserver, *SharePoint Team Services* oder andere Wege auszutauschen sind. Aber für einige Geschäftsfelder sind hier höhere Werte erforderlich.

- SMTP-Connector-Grenzen

  Es gibt sehr viele SMTP-Domänen, die nur Nachrichten bis 2 Megabyte annehmen (T-Online, WEB.DE, GMX etc.). Dank eines SMTP-Connectors mit entsprechendem Adressraum und Mailbegrenzung wird bereits in Exchange verhindert, dass zu große Nachrichten auf den Weg gebracht werden, deren Annahme verweigert wird.

- Datenbank-Limit (neu mit SP2)

  Bei einem Standardserver, dessen Laufwerk größer als 18 GB ist, sollten Sie den Wert „Database Size Limit in GB“ in der Registrierung hoch setzen. Bei Enterpriseservern können Sie mit der Begrenzung der Datenbank auf Laufwerksgröße ein unkontrolliertes Anwachsen der Datenbank verhindern. Auch hier sollten Sie sich an die Kapazität des Laufwerks orientieren, ggf. ist auch die Restore-Zeit Maßstab der Datenbankgröße. Beachten Sie jedoch, dass bei mehreren Datenbanken auf einem Laufwerk die Gesamtlimitierung nicht die Laufwerksgröße überschreiten darf.

Beachten Sie die Verbindung zwischen Internet-Mails und Intranet-Mails und die damit verbundenen Grenzen für die Exchange-Organisation und den SMTP-Connectoren.

4.12 Connectoren und Routing

Exchange als E-Mail-System kann aber mehr als nur Nachrichten aus dem Internet annehmen und versenden. Exchange ist ein leistungsfähiges System zur Weiterleitung von Nachrichten zwischen allen Servern innerhalb der gesamten Organisation.

Dazu nutzt Exchange 2003 die Informationen im Active Directory, um den Postfachserver des Empfängers ausfindig zu machen. Zusätzlich kennt jeder Server den Status der Verbindungen in der gesamten Organisation. Mittels der „Routing"-Informationen wird entsprechend der Nachrichtengröße, der Kosten und anderer Parameter der optimale Weg für die einzelne Nachricht ermittelt.

Im Gegensatz zu Exchange 5.5 nutzt Exchange 2003 das Protokoll SMTP und die Internet-Mail-Adressen zur Zustellung. Aus Gründen der Kompatibilität erhält jeder Empfänger zusätzlich eine X.400-Adresse. Exchange 5.5 und frühere Exchange-Server haben ihre Zustellung an diesen Adressen fest gemacht.

Mailtransfer anhand von Leitwegen

Der wichtigste Hinweis zum Verständnis von Exchange und dessen Routingfunktionen ist die Betrachtung der Exchange-Organisation als ein gemeinsames zusammenhängendes Verbundnetzwerk von Servern, die alle über die gleichen Informationen verfügen. Dazu trägt das Active Directory gravierend bei, dem alle Server die gleichen Angaben entnehmen. Darin eingeschlossen ist auch die Auskunft über die verschiedenen Verbindungen zwischen den Servern und Routinggruppen, die alle Exchange-Server zusätzlich untereinander austauschen. Zudem ist der erste Server, auf dem die Nachricht für einen Empfänger der Organisation eingeliefert wird, nicht relevant für die Zustellung, die sicher an den Benutzer erfolgt.

4.12.1 Routing von Nachrichten

Wege der Nachrichtenübermittlung

Exchange 2003 orientiert sich an den Kosten für eine Verbindung, um den günstigsten Leitweg zu ermitteln und die E-Mail darüber zuzustellen. Folgende Verbindungen sind möglich:

- Auf dem gleichen Server

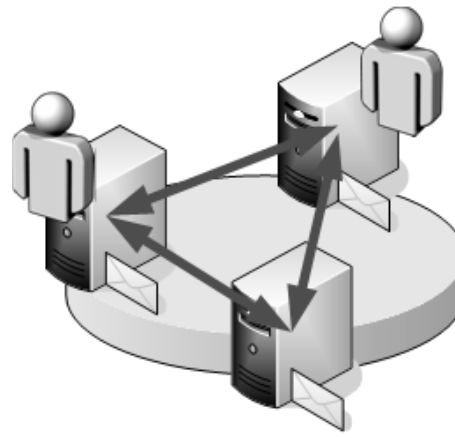
  Befindet sich der Empfänger auf dem gleichen Server wie der Absender, dann stellt der Exchange-Server die Nachricht direkt zu. Die direkte Übermittlung erfolgt auch, wenn die E-Mail direkt per SMTP auf dem Server eingeliefert wird, auf dem Exchange das Postfach des Empfängers ausmacht. Eine Betrachtung der Kosten und Connectoren ist nicht erforderlich.

Abbildung 4.44 Routing auf dem gleichen Server

- Servern in der gleichen Routinggruppe (RG)

  Existiert der Empfänger nicht auf dem gleichen Server, dann löst Exchange den Empfänger anhand des Globalen Katalogs auf und findet seinen Postfachserver. Macht er den Server in der gleichen Routinggruppe aus, wird eine direkte Verbindung zwischen den beiden Servern aufgebaut und die Nachricht übermittelt. In der Exchange 2003-Umgebung wird dabei das SMTP-Protokoll verwendet, in Verbindung mit Exchange 5.5 das RPC-Protokoll.

Abbildung 4.45 Routing in der gleichen Routinggruppe



- Zwischen Routinggruppen (RGs)

  Sind Absender und Empfänger auf Servern in unterschiedlichen Routinggruppen, muss Exchange die Informationen über Verbindungen und Connectoren abfragen und den besten Weg zur Routinggruppe des Empfängers ermitteln. Der Server sendet die Nachricht dann an den nächsten Server auf dem Weg zum Empfänger.

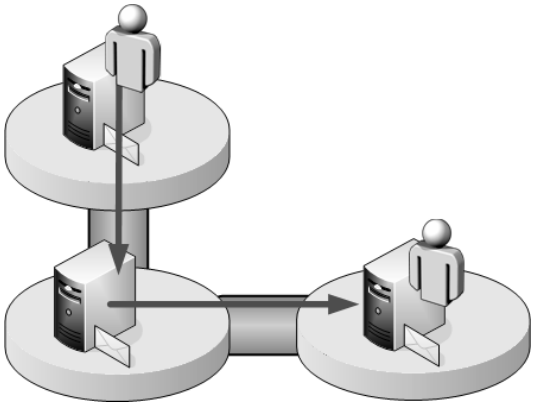


Abbildung 4.46 Routing über mehrere Routinggruppen

Die Routinggruppen werden mittels Connectoren verbunden. Jeder Connector wird mit den entsprechenden Kosten und Grenzen versehen, so dass die Kosten der Infrastruktur in Exchange abgebildet werden. Die Connectoren sollten entlang der physikalischen Verbindungen aufgebaut werden.

- Außerhalb der Organisation

  Nachrichten an Empfänger außerhalb der Organisation werden ebenfalls über entsprechende Connectoren geleitet. In diesem Fall zählt neben den Kosten des Connectors auch der Adressraum, der die externen Ziele bestimmt.

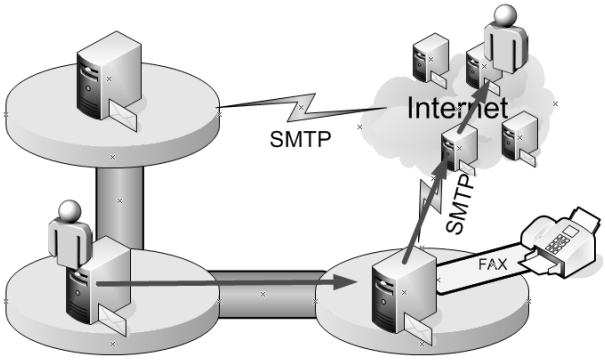


Abbildung 4.47 Routing an externe Adressen

Der klassische SMTP-Connector mit dem Adressraum „SMTP:*“ verarbeitet demnach alle Nachrichten vom Typ SMTP. Ein Connector zu einem Faxserver wird mit dem Adressraum „FAX:*“ eingetragen, und damit erkennt die komplette Exchange-Organisation, über welchen Weg Adressen dieses Typs übertragen werden.

4.12.2 Connectoren

Die Exchange 2003-Server werden anhand von Netzwerkstandorten in Routinggruppen zusammengefasst. Damit die Server der verschiedenen RG miteinander Nachrichten austauschen können, müssen Sie manuell Connectoren konfigurieren. Über die Auswahl der Verbindungsserver (Bridgehead-Server) und die Angabe von Kosten und anderen Beschränkungen steuert Exchange die Übertragung der Nachrichten. Exchange 2003 unterstützt drei Arten von Connectoren zwischen Routinggruppen.

Routing Group-Connector

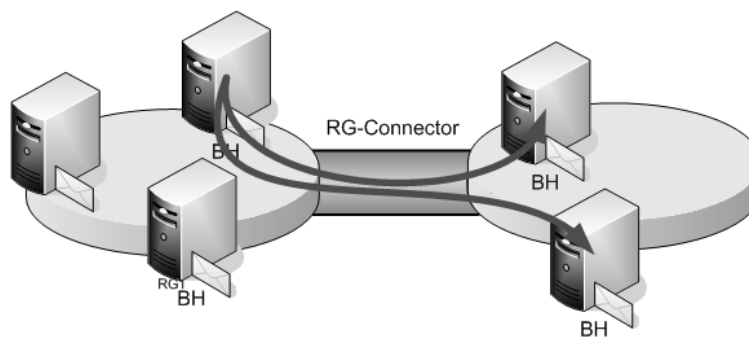
Der Routing Group-Connector ersetzt den früheren Standortconnector von Exchange 5.5. Er verbindet zwei Routinggruppen mittels SMTP. Hierbei kommt das erweiterte SMTP-Protokoll zum Einsatz, bei dem neben den Nachrichten auch Statusinformationen zu den Verbindungen in der Organisation übermittelt werden.

Der Einsatz von SMTP als Protokoll erlaubt sehr viel einfacher die Verbindung von RGs über Firewalls und langsame Verbindungen. SMTP nutzt nur den Port 25 und DNS und ist dadurch sehr viel robuster. Der Standortconnector nutzte RPC. Der Verzicht auf RPC als Transportprotokoll bedeutet auch einen höheren Schutz, da die Erreichbarkeit von RPC auch viele andere Dienste zulässt.

Kanal für Mailtransfer über SMTP

In den Eigenschaften des Connectors werden die Server aufgenommen, die der Connector als Quelle und Ziel für die Nachrichtenübermittlung verwendet. Hierbei können auf beiden Seiten mehrere Server eingetragen werden, so dass alle Server miteinander kommunizieren. Fällt ein Server aus, dann nutzen die verbliebenen Server den Connector weiter.

Abbildung 4.48 Routinggroup-Connector



n:n-Verbindung mit Leitwege-berechnung

Ein Routinggruppen-Connector definiert die Verbindung zwischen zwei Routinggruppen und nicht zwischen zwei einzelnen Servern, so dass eine Redundanz gegeben ist und keine 1:1-Beziehung. Ferner erlaubt er die effektive Kalkulation der Leitwege.

Der Exchange 2003-Routinggruppen-Connector ähnelt dem früheren Standortconnector von Exchange 5.5. Der große Unterschied ist jedoch der Verzicht auf RPC und damit den kritischen Port 135 sowie alle „High-Ports“ (>1024). Die Verbindung zwischen Standorten mit einer Firewall lässt sich nun viel einfacher und sicherer konfigurieren.

Aufgrund der Probleme des Exchange 5.5-Standort-Connectors mit dünnen Bandbreiten gab es auch in der Version 5.5 die Möglichkeit, Standorte mit X.400- oder SMTP-Connectoren zu verbinden.

X.400-Connector

In der Exchange 2003 Enterprise Edition ist auch der X.400-Connector zur Anbindung an X.400-Nachrichtensysteme und zur Kopplung von Routinggruppen verfügbar.

1:1-Verbindung ohne Ausfallsicherheit

Der X.400-Connector verbindet im Gegensatz zum Routingruppen-Connector nicht die beiden Routinggruppen, sondern explizit zwei Server miteinander. Dazu ist auf beiden Servern der Connector zu konfigurieren. Bei Exchange 5.5 wurde besonders in größeren Firmen der X.400-Connector bevorzugt zur Verbindung von Standorten eingesetzt, weil dieser im Gegensatz zum SMTP-Connector eine abgebrochene Verbindung wieder aufsetzen kann und die Nachrichten ohne MIME-Konvertierung überträgt. Dies spart Bandbreite und Übertragungsvolumen.

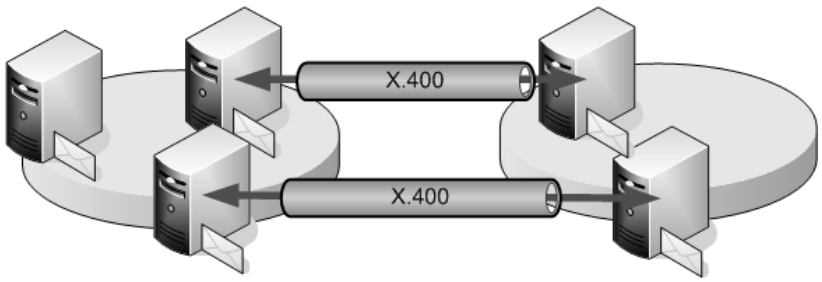


Abbildung 4.49 X.400-Connectoren

Zudem konnte der X.400-Connector mit langsamen Verbindungen und Beschränkungen in Firewalls sehr viel besser umgehen als der Standortconnector. Der höhere Preis der Exchange Enterprise Edition wurde durch die Vorteile wettgemacht.

Mit Exchange 2003 ist diese Funktion dank des RG-Connectors einfacher und flexibler realisierbar, so dass der X.400-Connector mit der neueren Exchange-Version nur noch für Verbindungen zu Exchange 5.5-Standorten und zur Anbindung an externe X.400-E-Mail-Systeme eingesetzt werden wird.

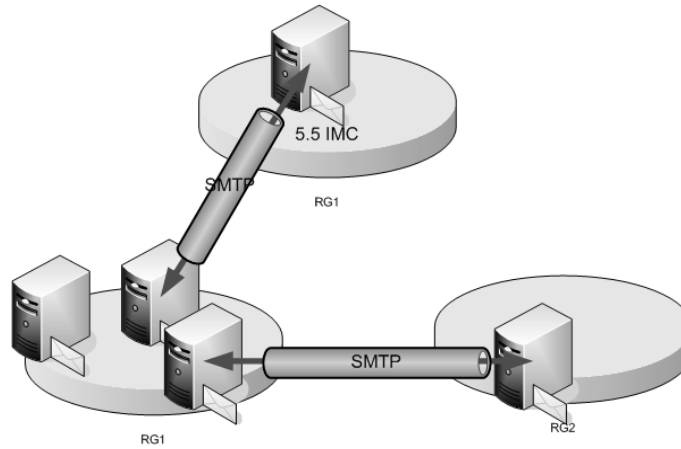
Eine Verbindung der Exchange 2003-Routinggruppen mit den Exchange 5.5-Standorten ist über die Option „Verbundene Standorte“ im Connector möglich. Damit werden Exchange-Nachrichten in X.400-Mitteilungen eingepackt und vom MTA übermittelt.

SMTP-Connector

n:n-Verbindung

Auch der SMTP-Connector, auf den später im Rahmen der Internet-Anbindung konkret eingegangen wird, kann für die Verbindung von RGs genutzt werden. Dazu dient die Option der „verbundenen Standorte“. Zugleich wird hiermit eine Kompatibilität zu Exchange 5.5 erreicht.

Abbildung 4.50 SMTP-Connectoren verbinden Routinggruppen



Auch wenn die Kopplung zweier Routinggruppen über SMTP-Connectoren möglich ist, sollte der Vorzug dem Routinggruppen-Connector gegeben werden. Nur wenn beide Routinggruppen über SMTP nicht direkt zu erreichen sind, sondern über einen Relay-Server (z.B. Antispam, anderes E-Mail-System) Nachrichten austauschen, ist ein SMTP-Connector mit verbundenen Standorten unvermeidlich.

4.12.3 Link State Routing

Exchange 2003 führt genau Buch, welche Verbindungen verfügbar sind und welche Verbindungen aktuell nicht funktionieren. Aus dem Active Directory erhalten alle Exchange-Server die aktuelle Topologie der Exchange-Organisation. Hinzu kommt, dass die Server nicht nur per SMTP miteinander Nachrichten austauschen, sondern am Anfang jeder Verbindung auch die Informationen über den Verbindungsstatus.

Zusätzlich gibt es in jeder Routinggruppe einen Routinggruppen-Master, der die Informationen an die anderen Exchange-Server in der gleichen Routinggruppe verteilt.

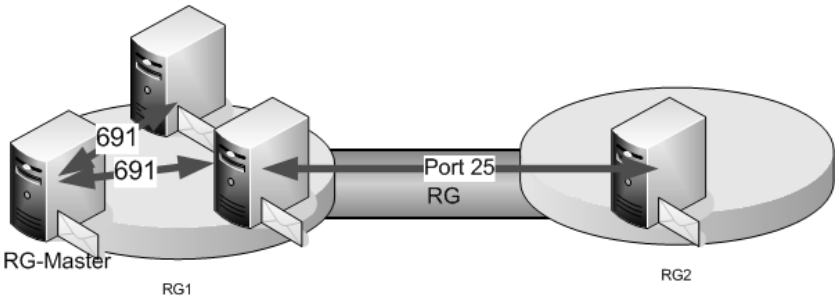


Abbildung 4.51 Kommunikation für die Leitwege

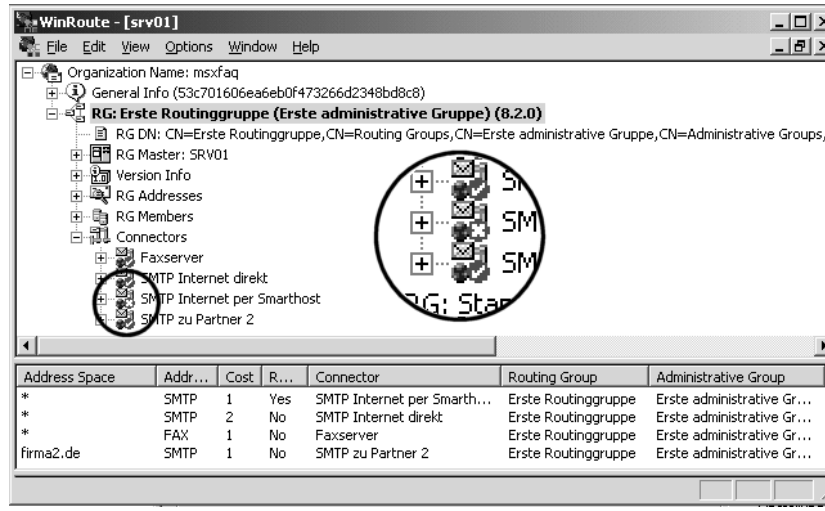
Flexible Anpassung der Leitwege

Fällt nun ein Connector aus, so stellt der Bridgehead-Server (BH) dies beim Verbindungsversuch fest und informiert den Routinggruppen-Master. Dieser informiert alle anderen Server der gleichen Routinggruppe. Alle Exchange-Server mit Routinggruppen-Connectoren bauen daraufhin eine Verbindung zu ihren Partnern in der anderen Routinggruppe über SMTP auf, um die veränderten Verbindungen mitzuteilen. Ähnlich dem OSPF-Routing bei TCP/IP-Routern wird damit sehr schnell in der gesamten Organisation bekannt, welche Leitwege funktionieren und welche gestört sind. Ein Server versucht regelmäßig wieder Kontakt zu der ausgefallenen Gegenstelle zu erhalten.

Der aktuelle Status der Leitwegetabelle (Routingtable) ist weder in der Exchange-Datenbank noch im Active Directory gespeichert, sondern wird nur im Hauptspeicher von Exchange 2003 gehalten. Sobald ein Server neu gestartet wird, holt er sich die aktuelle Information vom Routinggruppen-Master in seiner Routinggruppe. Exchange 5.5 löst diese Problematik mit der GWART-Tabelle, welche dagegen nur einmal am Tag neu erstellt wird. Dies ist einer der Gründe, warum viele größere Organisationen sehr schnell Exchange 2003 auf den Connector-Servern einführen.

Das Programm „WinRoute“ auf der Exchange-CD liest die Leitwegetabelle ebenfalls über SMTP vom angegebenen Server aus und zeigt den aktuellen Status an.

Abbildung 4.52 Ausgabe von WinRoute



Das Bild zeigt einen Musterserver, bei dem der Connector zum Internet über einen Smarthost nicht mehr funktioniert. Anhand der Leitwegetabelle im unteren Bereich ist ersichtlich, dass es einen zweiten Connector gibt, der die Kosten 2 hat, aber verfügbar ist. Damit werden die Verbindungen über diesen Connector weitergeleitet. Über den Eintrag der Kosten steuern Sie somit die Leitwege der Nachrichten. Nur wenn der „günstigste Weg“ ausgefallen ist, entscheidet Exchange sich, die Nachricht mit erhöhten Kosten zu senden.

Intelligentes Routing

Kann eine Nachricht anhand einer Unterbrechung nicht an das Ziel zugestellt werden, erkennt dies schon der erste Server und hält die Nachricht an, bis wieder eine Verbindung verfügbar wird. Exchange 5.5 hat die Nachricht immer entlang des Leitwegs gesendet, bis diese bei dem Server angekommen ist, bei dem die Verbindung zum Zielserver unterbrochen ist. Wird dann ein alternativer Leitweg verfügbar, musste die Mail eventuell einen Teil des Weges wieder zurück übertragen werden. Exchange 2003 löst dies, indem die Mail erst dann weitergeleitet wird, wenn ein Weg bekannt ist. Dieses Verfahren reduziert mehrfache Übertragungen der Mails und Schleifen.

4.12.4 Warteschlangen

Da in einer größeren Umgebung immer wieder Nachrichten für einige Zeit vorgehalten werden und auf ihre weitere Verarbeitung warten, hat Exchange 2003 ein ausgeklügeltes System von Warteschlangen (Queues) entwickelt, in denen die Nachrichten lagern. Im Exchange System-Manager können bei jedem Server die Warteschlangen eingesehen werden.

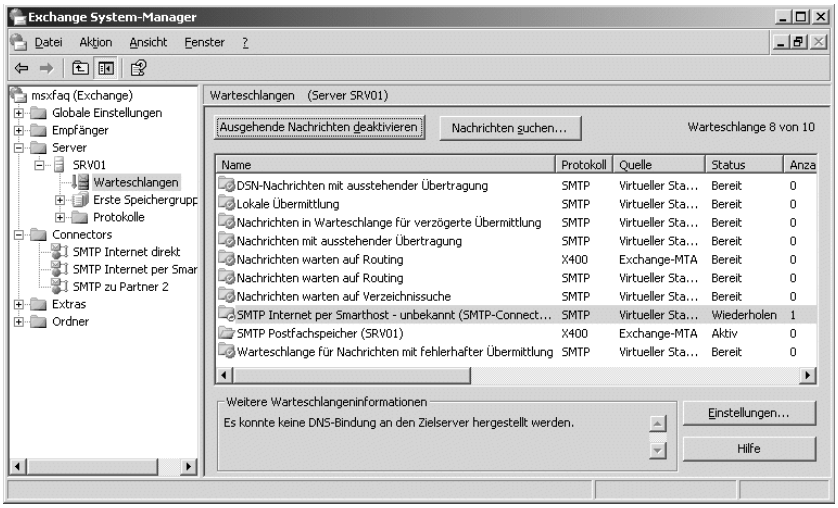


Abbildung 4.53 Warteschlangen der Nachrichtenübertragung

Aufteilung in System- und Verbindungswarteschlangen

Seit Exchange 2003 können Sie alle Warteschlangen pro Server an einer Stelle im Exchange System-Manager kontrollieren. Neben den Standardwarteschlangen für die Connectoren legt Exchange 2003 zusätzlich dynamisch Warteschlangen für weitere Ziele an, an die eine Nachricht übermittelt werden muss. Eine länger nicht benutzte Warteschlange wird automatisch wieder gelöscht. Folgende System-Warteschlangen sind auf einem Exchange-Server vorhanden und dem virtuellen Standardserver für SMTP zugeordnet:

- DSN-Nachrichten mit ausstehender Übermittlung

  Hier stehen Quittungen und Unzustellbarkeitsberichte, die Exchange noch nicht versendet hat.

- Lokale Übermittlung

  Die Empfänger von Nachrichten in dieser Warteschlange befinden sich auf dem lokalen Server. Die Daten wurden nur bislang noch nicht an den Informationsspeicher übermittelt, weil dieser zu beschäftigt oder nicht verfügbar ist. Prüfen Sie in dem Fall, ob die entsprechende Datenbank online geschaltet ist.

- Nachrichten warten auf Verzeichnissuche (PreCAT)

  Diese Nachrichten wurden gerade eingeliefert und warten auf die Bearbeitung durch den Categorizer. Sollten hier Nachrichten längere Zeit liegen, dann könnte ein Problem mit dem Domänencontroller vorliegen, da beispielsweise Empfänger und Verteiler nicht auflösbar sind.

- Nachrichten warten auf Routing (PreRouting)

  Diese Nachrichten wurden durch den Categorizer bereits verarbeitet und warten nun auf die Bearbeitung durch das Routingmodul, um in die richtige Warteschlange zum nächsten Server eingeordnet zu werden.

- Nachrichten in Warteschlange für verzögerte Übermittlung (SMTP)

  Sie können bei Nachrichten angeben, zu welchem Termin sie übermittelt werden sollen. Die E-Mails werden bis zum Eintritt des beauftragten Zeitpunkts in dieser Warteschlange gepuffert. Zudem werden hier Nachrichten für Postfächer geparkt, die gerade verschoben werden.

- Nachrichten mit ausstehender Übertragung

  Diese Nachrichten warten darauf, dass der SMTP-Service diese E-Mails aufgreift und übermittelt.

- Warteschlange für Nachrichten mit fehlerhafter Übermittlung

  Diese Nachrichten konnten beim letzten Versuch nicht übermittelt werden und wurden für einen späteren Versuch zurückgestellt. Probleme bei der Namensauflösung mit DNS könnten eine Ursache sein, wenn diese Warteschlange wächst.

Die Verbindungswarteschlangen werden erst bei Bedarf erstellt, also wenn der virtuelle SMTP-Server, das X.400-Objekt oder ein Connector zurzeit Nachrichten erhält oder an einen anderen Server versendet.

- Connector-Warteschlangen

  Für jeden Connector wird eine eigene Warteschlange angelegt. Im Bild ist nur der Connector „SMTP via Smarthost“ sichtbar.

- Server-Warteschlangen

  Sendet Exchange-Server eine Nachricht zu einem anderen Server der gleichen Routinggruppe, wird ebenfalls eine Warteschlange für diesen Server angelegt. Tauchen hier Nachrichten auf, könnte der andere Server aktuell nicht aktiv sein, oder die Verbindung dorthin ist unterbrochen oder gestört.

- Exchange-MTA

  Diese Warteschlange enthält Nachrichten, die in einer Migrationsumgebung an einen Exchange 5.5-Server übermittelt werden.

Exchange 2003 nutzt für das Routing von Nachrichten den SMTP-Dienst von Windows 2003, der um zusätzliche Filter erweitert wird. Ferner gibt es die *Exchange Routing Engine*, die mehrere Funktionen beinhaltet:

- Categorizer

  Mittels des Active Directory löst der *Categorizer* die Verteiler und Empfänger auf, konvertiert bei Bedarf die Nachrichten und teilt diese in mehrere E-Mails auf, wenn verschiedene Ziele angesprochen werden.

- Routing Engine

  Die *Routing Engine* nutzt die Informationen aus der Link State Table, um die Nachrichten in die entsprechenden Warteschlangen einzuordnen.

- Event Sink

  Nicht eingezeichnet sind die verschiedenen Stellen, an denen Entwickler ihren Code einbinden, um Nachrichten während der Verarbeitung und Übertragung zu modifizieren. Diese *Event Sinks* greifen in verschiedenen Situationen ein und erlauben sehr umfangreiche Modifikationen der E-Mails beim Routing.

Folgendes vereinfachtes Bild soll grob einen Überblick über die Zusammenhänge geben.

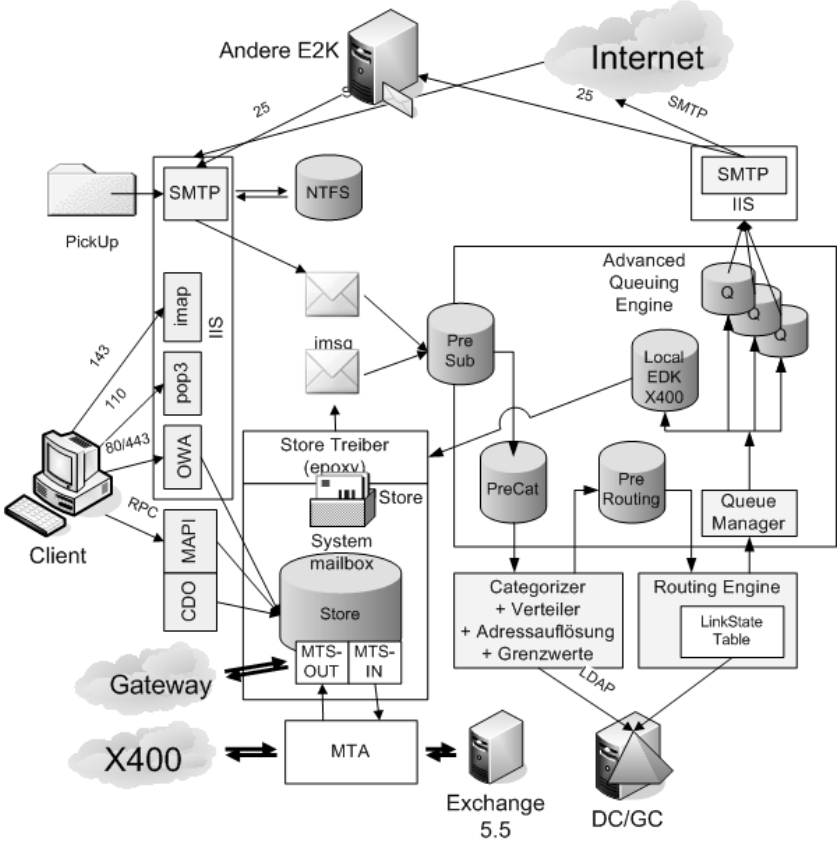


Abbildung 4.54 Exchange Routing Internals

Während der MTA und die Connectoren zu X.400 bei Exchange 5.5 noch den Mittelpunkt des Routings gebildet haben, ist bei Exchange 2003 die *Advanced Queuing Engine* der eigentliche Dreh- und Angelpunkt. Der Zugriff über OWA, POP3 und IMAP4 nutzt wie SMTP den IIS und dessen Komponenten.

Für die Installation und den Betrieb ist es nicht notwendig, diese Zusammenhänge auswendig zu kennen. Allerdings sollten Sie schon wissen, welche Warteschlange welche Funktion einnimmt und wie Sie die Ursache für eine stecken gebliebene Nachricht finden können.

4.13 Exchange-Clients

Ohne die Anwender, die auf den Exchange-Server zugreifen, fehlte dem Server die Daseinsberechtigung. Aus diesem Grunde erhalten Sie hier einen kurzen Überblick der Clients und wie sie auf die Server zugreifen.

Client-Protokolle

Exchange 2003 erlaubt den Zugriff über die verschiedensten Protokolle.

- SMTP

  Exchange 2003 akzeptiert von jedem Client eine Nachricht über das Protokoll SMTP (TCP/IP Port 25). Exchange leitet diese Nachrichten auch in das Internet weiter, wenn die Verbindung autorisiert wurde. Damit können POP3- und IMAP4-Clients nach einer Anmeldung am Exchange-Server über SMTP (Relay) E-Mails versenden.

- POP3

  Der Zugriff über das Internet-Protokoll „POP3“ erfolgt über den TCP/IP-Port 110 oder bei verschlüsselten Verbindungen über Port 995. POP3 ist ein einfaches Protokoll, auf dessen Basis sehr unterschiedliche Programme auf nahezu allen Betriebssystemen neue Nachrichten aus dem Posteingang abholen können. Der Versand von Nachrichten erfolgt jedoch nicht über POP3, sondern meist über SMTP. Allerdings wird beim Einsatz von POP3 nur die Minimalfunktion des Exchange 2003-Servers genutzt. Der Zugriff auf andere Ordner im Postfach, die Nutzung von Regeln sowie Stellvertreterfunktionen, Formularverwendung und viele andere Dinge, die Exchange 2003 erst ausmachen, sind nicht nutzbar.

- IMAP4

  Als Nachfolger für POP3 wurde das Protokoll IMAP4 entwickelt, das die Bearbeitung von Nachrichten in allen Ordnern auf dem Postfachserver erlaubt. Nachrichten werden nicht mehr zwingend heruntergeladen und lokal verwaltet, sondern können auf dem Server verbleiben und in Strukturen einsortiert werden. Dies ermöglicht so auch den Zugriff auf den Posteingang von mehreren PCs. Für die Unterscheidung, ob Elemente

in einem Ordner als Aufgaben, Termine oder Kontakte anzusehen sind, gibt es keine einheitlichen Vorgaben. Einen Großteil der Funktionalität von Exchange 2003 kann auch mit IMAP4 nicht genutzt werden.

- HTTP/HTTPS

  Mit jeder Version von „Outlook Web Access“ verbesserte sich der Zugriff über einen Webbrowser auf die Exchange-Informationen. Der Exchange 2003-Web-Zugriff ist sehr ausgereift und kann oftmals Outlook ersetzen. Zudem bietet OWA mit einem Browser den Zugriff auf Exchange-Funktionen über ein Fremdsystem ohne den Outlook-Client (z.B. diverse Unix-Systeme).

- NNTP

  Alle Öffentlichen Ordner sind über das Protokoll NNTP erreichbar. Über diesen Weg erhalten Systeme, die keinen Zugriff mit Outlook oder OWA nutzen, zumindest einen eingeschränkten Zugriff auf Public Folder-Informationen. Outlook-Formulare und -Ansichten sind dabei nicht möglich.

- WAP, PocketPC und ActiveSync

  Exchange 2003 beinhaltet alle notwendigen Komponenten, um mit einem WAP-fähigen Endgerät oder einem PocketPC über ActiveSync einen Zugriff auf das Postfach zu erhalten. So können Sie schnell über den Outlook Mobile Access-Server (OMA) auf Ihrem Mobiltelefon einen Kontakt oder eine Rufnummer nachschlagen. Über ActiveSync können Sie einen Teil des Postfachs direkt auf einem mobilen Gerät mit PocketOutlook replizieren.

- RPC und RPC over HTTP

  Der am häufigsten eingesetzte und leistungsfähigste Zugriff erfolgt mit Outlook direkt über das Protokoll RPC. Seit Exchange 2003 kann die Übertragung auch in http-Paketen eingekapselt werden, so dass der Zugriff über Firewalls und Proxy-Server wesentlich einfacher möglich ist (*RPC over HTTP*). Dies spart in einigen Situationen den Aufbau von VPN-Verbindungen.

Schwierigkeiten mit Laufwerk M:

Exchange 2000 ermöglichte den Zugriff auf Informationen in der Datenbank über das Laufwerk M:. Durch die Einrichtung entsprechender Freigaben konnte damit sogar ein Zugriff über Netzwerklaufwerke, FTP-Server, NFS und andere dateibasierte Protokolle realisiert werden. Allerdings haben viele Firmen nicht die Randbedingungen für den Zugriff auf dieses virtuelle Laufwerk beachtet. Unbewusst wurden die Berechtigungen im Informationsspeicher so verändert, dass ein Zugriff mit Outlook nicht mehr möglich war. Microsoft reagierte in Exchange 2003 mit der Deaktivierung dieser Funktion per Default, die Sie wirklich nur nach gründlicher Überlegung wieder aktivieren sollten.

Neben den direkten Protokollen für den Zugang sind weitere Möglichkeiten der Postfachnutzung denkbar. Dazu zählen:

- Microsoft Terminal Server oder Citrix Metaframe

Mobile Office

  Outlook lässt sich problemlos auf Terminal-Servern installieren und betreiben. Der Zugang erfolgt über das RDP-Protokoll oder mit dem Zusatzprodukt Citrix Metaframe über das ICA-Protokoll. Über diesen Weg ist es vielen anderen Betriebssystemen möglich, die volle Leistungsfähigkeit von Outlook zu nutzen, auch wenn Outlook nicht direkt auf dem Arbeitsplatz installiert werden kann. Speziell die Verfügbarkeit des ICA-Clients für verschiedene Unix-Derivate, OS/2-Systeme, Thin Clients und andere Desktops erlauben damit eine universelle Nutzung von Outlook. Der Zugriff von öffentlichen Systemen über das Internet ist mit dem Citrix Secure Gateway ebenfalls möglich. Damit steht eine Alternative zum Outlook Web Access zur Verfügung.

- Blackberry und andere mobile Geräte

Mobile Geräte für Mail und Telefon

  Gerade der Markt mobiler Endgeräte ist sehr flexibel, und mit passenden Produkten werden auch hier Lösungen geschaffen. So ist ein Blackberry der Firma RIM ein mobiles Telefon mit PDA und Mailfunktionen. Anstatt per POP3 eine Verbindung zum Server aufzubauen, kommuniziert der Blackberry mit dem Blackberry-Server, der direkt auf die freigeschalteten Postfächer in Exchange zugreift und die Informationen geeignet umsetzt. Zum Versand einer Nachricht sendet der Blackberry die Mitteilung an den Server, der diese in den Postausgang des Benutzers auf dem Exchange-Server stellt. Für Exchange stellt sich der Vorgang so dar, als habe ein Outlook-Client eine Nachricht gesendet. So können Drittanbieter sehr einfach Exchange um zusätzliche Funktionen erweitern.

- Client für HTTP

  Andere Anbieter entwickeln eigene Produkte, die basierend auf dem HTTP-Protokoll jede Nachricht im Postfach lesen und verändern. Diese sind zumeist Outlook nachempfunden, aber nutzen nicht RPC, sondern den Zugriff per WebDAV, um mit dem Informationsspeicher zu kommunizieren.

Für die meisten Methoden finden Sie in Kapitel 9 entsprechende Beispiele. Für den Exchange-Administrator ist ein Blick hinter die Kulissen von Outlook interessant.

4.13.1 Outlook, MAPI und Profile

Ungeachtet der umfangreichen Funktionen des Outlook-Clients als Anwendung verbirgt sich in der Tiefe von Outlook das *Windows Messaging*

Subsystem. Die Hauptaufgabe des Clients ist die Präsentation der Nachrichten, die Anzeige von Informationen mit verschiedenen Ansichten, Filtern oder Formularen und die Eingabe von Informationen.

Für die Übermittlung, den Empfang und die Speicherung der Nachrichten wie auch die Auswahl von Adressen ist Outlook nur bedingt zuständig. Diese Aufgabe obliegt dem Windows Messaging Subsystem, das durch die Installation von Outlook entsprechend aktualisiert wird. MAPI als Programmierschnittstelle ist schon seit den Tagen von Microsoft Mail bekannt und wurde im Laufe der Zeit immer weiter ausgebaut. Schon der erste „Posteingang", der in Windows 95 installierbar war, brachte ein komplettes MAPI-Subsystem mit. Auch die Installation von Exchange 2003 auf einem Windows-Server installiert die Kernkomponenten von MAPI. Daher können Anwendungen auch auf dem Server selbst über MAPI mit Exchange kommunizieren. Dies ist auch einer der Gründe, warum Microsoft von der Installation des Clients auf dem Exchange-Server abrät, da unweigerlich Konflikte mit DLLs die Funktion des Servers empfindlich stören können. Einige Hersteller von Drittprodukten erwarten die Installation von Outlook auf dem Server, um Profile erstellen und anzupassen, mit denen MAPI konfiguriert wird.

Die Struktur von MAPI

Wichtige MAPI-Dienste

Der MAPI-Spooler ist das Bindeglied zwischen den Anwendungen, die auf MAPI aufsetzen, und den Diensten, die ihre Funktion einbringen. Es werden drei Dienste unterschieden:

- Transportdienste

  Diese Module erlauben den Versand und Empfang von Nachrichten. Hierzu zählen z.B. der Dienst zum Abholen von Mailboxen über POP3 und das Versenden von Nachrichten per SMTP. Dazu zählen aber auch andere Dienste, die Outlook an alte oder fremde Systeme anbinden, wie Microsoft Mail, Lotus Notes etc. Auch der Dienst für die Exchange-Anbindung enthält eine Komponente zum Senden von Nachrichten. Diese werden allerdings einfach im Postausgang auf dem Server abgelegt und von da zugestellt.

- Speicherdienste

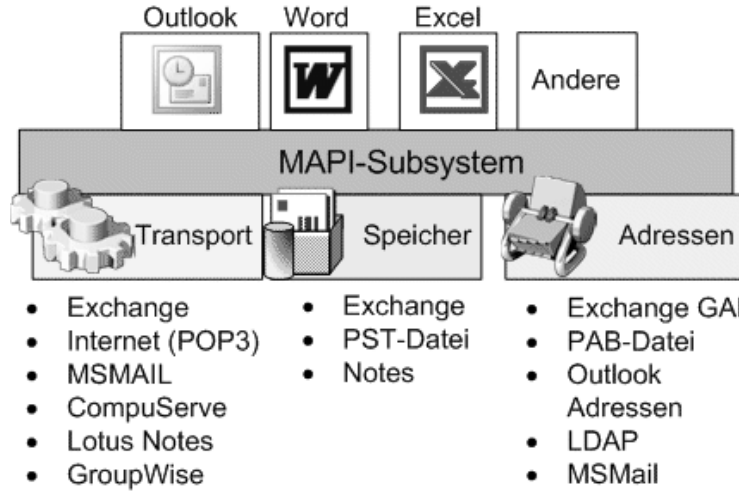
  Eine zweite wichtige Komponente sind die Dienste zur Bereitstellung von Informationsspeichern. Der „Persönliche Ordner" in Form einer PST-Datei ist eine Möglichkeit, Nachrichten zu speichern. Beim Einsatz mit Exchange wird auch diese Funktion durch den Exchange-Server übernommen, und eine DLL des Clients stellt diese MAPI-Funktion zur Verfügung.

- Adressdienste

  Anwender haben den Bedarf, die Empfänger in Adressbüchern zu suchen und auszuwählen. Die entsprechenden Treiber erlauben den Zugriff auf LDAP-Dienste, persönliche Adressen in einer PAB-Datei oder die Kontakte in Outlook. Auch die Einrichtung der Exchange-Anbindung fügt hier die notwendigen Komponenten hinzu, um das Globale Adressbuch zu nutzen.

Sie können problemlos mehrere Dienste parallel einrichten und betreiben. Für die Transportdienste können Sie eine Reihenfolge festlegen. Hier sollte der Exchange Transport Service immer ganz oben stehen. Bei den Speicherdiensten definieren Sie einen der Dienste als primären Speicher. Hier legt Outlook die Systemordner Posteingang, Postausgang etc. an. Alle eingehenden Nachrichten landen in diesem Ordner. Ein Wechsel der Reihenfolge bewirkt eine Verschiebung aller Nachrichten aus dem alten Speicherordner in den neuen Speicher.

Abbildung 4.55
MAPI-Subsystem



Auf der MAPI-Schnittstelle selbst setzen die verschiedensten Anwendungen auf. Beim Senden eines Dokuments aus Microsoft Word heraus wird ebenso die MAPI-Schnittstelle initialisiert wie beim Start von Outlook. Nach dem Beenden des letzten Programms auf dem Rechner beendet sich MAPI nach einigen Sekunden ebenfalls. Mit jeder neuen Outlook-Version wird die Verbindung der Exchange-Dienste und Outlook immer enger. Viele Menüs von Outlook werden erst sichtbar, wenn Exchange als Dienst eingegliedert ist. Erst dann sind z.B. auch Offline-Ordner möglich, die Replikation von Inhalten sowie serverbasierte Regeln. Da aber viele dieser Funktionen nicht über die MAPI-Schnittstelle offen gelegt sind, ist eine Nutzung von anderen Programmen nicht realisierbar.

Profile

Profile enthalten Dienstkonfiguration.

MAPI ist eine sehr modulare Struktur, in der verschiedene Dienste eingebunden werden können. Die Konfiguration der verschiedenen Einstellungen wird in Profilen zusammengefasst. Die meisten Anwender haben genau ein Profil, in dem die notwendigen Dienste eingetragen sind. Sie könnten jedoch auch mehrere Profile konfigurieren, von denen jedoch immer nur genau ein Profil aktiv sein kann.

Die Profile werden getrennt pro Benutzer verwaltet. Die Konfiguration kann neben Outlook auch mit Programmen wie NEWPROF, PROFGEN, MODPROF oder PROFMAN erstellt und verändert werden. Sie sind Bestandteil von früheren Outlook-Versionen oder dem Exchange Resource Kit. Die meisten Programme nutzen die Vorlagendatei „*.PRF“, in der die zu installierenden Dienste hinterlegt sind.

Eine elegante grafische Umsetzung ist mit dem Office Customization Wizard aus dem Office Resource Kit (ORK) möglich, mit dem Sie ein Outlook-Profil vordefinieren und mit in die Office-Installation integrieren können.

Das Programm PROFMAN hingegen erlaubt Ihnen die interaktive Erstellung von Profilen ohne installiertes Outlook. Das Tool EXMERGE und die Exchange-Administrationsprogramme erstellen selbstständig die für ihre Funktion notwendigen temporären Profile.

Damit all diese Programme überhaupt wissen, welche Dienste auf dem Computer installiert und eingerichtet werden können, enthält die Datei MAPISVC.INF die Daten über die installierbaren Komponenten. Auf dem Exchange 2003-Server findet sich diese Datei im System32-Verzeichnis. Die Installation von Outlook 2003 verlegt diese Datei aber nach „C:\Programme\Gemeinsame Dateien\System\MSMAPI\1031“. Damit wird nun auch klar, dass Outlook auf einem Exchange-Server beträchtlichen Schaden anrichten kann.

MAPI-Zugriff steuern

MAPI deaktivieren, Cached Mode fokussieren

Einige Unternehmen möchten den Zugriff über RPC over HTTP mit Outlook Cache Modus fokussieren, im Gegensatz dazu wünschen einige E-Mail-Provider nur den Zugriff über Outlook Web Access. Mit der Installation von Service Pack 2 kann der MAPI-Zugriff für einzelne Benutzer deaktiviert, der Outlook Cache Modus zur Pflicht gemacht werden. Leider lässt sich dieser Wert nicht über die ESM setzen, Sie müssen ihn mittels eines Tools wie *ADSIEDIT* oder *ADModify.NET* in das Attribut `ProtocolSettings` schreiben. Die Syntax sieht wie folgt aus: `MAPI§<Wert1>§Wert2>§§§§§§`.

ProtocolSettings	Bedeutung
MAPI§<Wert1>§Wert2>§§§§§§	MAPI definiert nachfolgende Einstellung für das MAPI-Protokoll, Wert1 steuert den MAPI-Zugriff, Wert2 definiert die Cache-Modus-Nutzung
MAPI§0§0§§§§§§	Deaktivierung MAPI-Zugriff, kein Cache-Modus erforderlich
MAPI§1§1§§§§§§	MAPI-Zugriff nur mit Cache-Modus möglich
MAPI§1§0§§§§§§	Generell MAPI-Zugriff möglich

Eine Kombination Wert1=0 und Wert2=1 macht keinen Sinn, da ein gesperrter MAPI-Zugriff auch für Cache-Modus-Benutzer gilt.

4.13.2 Outlook-Kontakte und -Adressen

Eine der Komponenten eines MAPI-Profils sind die Adressbuchdienste. Diese Dienste erlauben dem Anwender den Zugriff auf die E-Mail-Adressen möglicher Empfänger. Outlook kann dabei mehrere Adressbücher parallel durchsuchen und dem Anwender anzeigen. Für den Exchange-Administrator ist es wichtig, die unterschiedlichen Adressbücher zu kennen und entsprechend in das Konzept einzubinden.

Persönliche Adressen (PAB-Datei)

Schon seit der ersten Version des Exchange-Clients, lange vor Outlook, speicherten die Anwender private persönliche Kontakte. Dazu werden im MAPI-Profil über den entsprechenden Dienst PAB-Dateien integriert. Dort kann ein Anwender neben den Adressen auch persönliche Verteiler speichern. Diese Dateien haben allerdings den großen Nachteil, dass die Informationen nicht im Exchange-Postfach abgelegt werden und deshalb nur bedingt für andere Benutzer oder Clients verfügbar sind. Für den Einsatz in einem Netzwerk sind diese Dateien praktisch bedeutungslos.

Kontakte

Kontaktordner in Postfach oder Öffentlicher Ordner

Aus diesem Grund wurde mit Outlook der Kontaktordner für jeden Benutzer eingeführt, in dem er seine persönlichen Ansprechpartner mit vielen Zusatzinformationen ablegen kann.

Diese Kontaktordner sind Teil des Postfachs und können auch von anderen Mitarbeitern mit Stellvertreterrechten eingesehen werden. Zusätzlich können Kontaktordner auch im Bereich der Öffentlichen Ordner angelegt werden, um eine firmenübergreifende Nutzung zu ermöglichen. Um diese Adressen in Outlook als Mailempfänger zugänglich zu machen, ist allerdings erst der Dienst „Outlook-Adressbuch“ in das MAPI-Profil aufzunehmen. Erst dann

erscheint bei den Kontaktordnern die Option, diese zusätzlich im Adressbuch anzuzeigen.

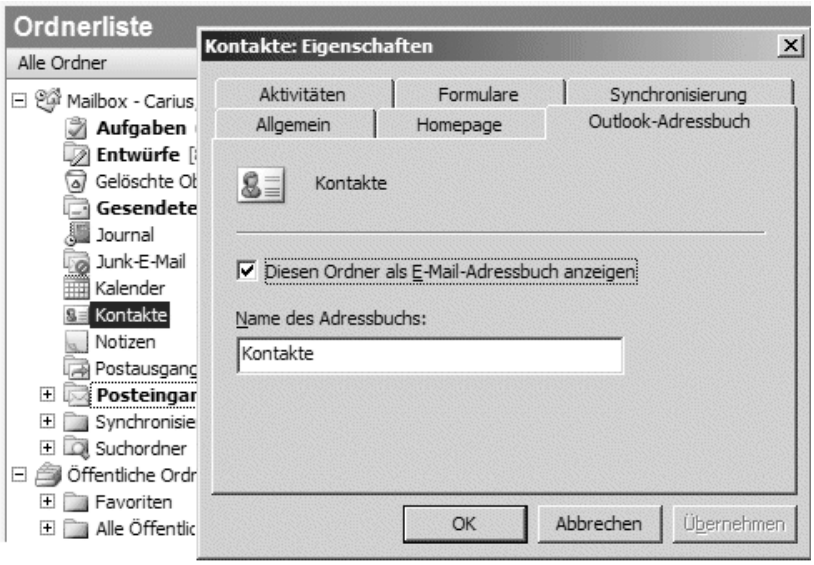


Abbildung 4.56 Kontakte in Outlook als Adressbuch

Eine Ausnahme bilden Kontakte in PST-Dateien, die keine gemeinsame Nutzung erlauben. Wurden früher die persönlichen Adressbücher (PAB) für eigene Verteiler benötigt, können diese seit der Outlook-Version 2000 auch in dem Kontaktordner gespeichert werden. Ein Import bestehender Kontakte ist über Outlook aus verschiedenen Fremdformaten wie auch Excel, Access und einfachen TXT-Dateien möglich.

Active Directory-Kontakte

Neben den Kontakten, die der Anwender selbst verwaltet, greift Outlook auch auf die Adressen der Exchange-Server zurück. Im Active Directory können ebenfalls Kontakte angelegt und mit Exchange-Attributen versehen werden. Diese sind für den Outlook-Anwender als Empfänger nutzbar, allerdings von ihm nicht änderbar. Diese zentral pflegbaren Kontakte eignen sich primär dazu, die Adressen anderer verbundener E-Mail-Systeme in Exchange bekannt zu machen. Über diesen Weg kommen zum Beispiel Adressen eines Lotus Notes-Connectors oder GroupWise-Connectors in das Active Directory.

Exchange-Kontakte verbinden Unternehmen.

Über eine Verzeichnisreplikation mit dem Active Directory-Connector, Microsoft Meta-Directory oder dem neuen Microsoft Identity Integration Server 2003 (MIIS) können zentral die Adressen verschiedener Unternehmen ausgetauscht werden. Die Sichtbarkeit für die verschiedenen Anwender kann über angepasste Adressbuchansichten in Exchange und mittels Berechtigungen kontrolliert werden.

Denkbar wäre auch eine Ablage der Adressen aller Kunden aus der Buchhaltung als Kontakte im Active Directory. Ein Massenimport ist beispielsweise mit LDIFDE, CSVDE oder einem einfachen VBScript möglich.

Andere Adressdienste (LDAP)

Outlook kann mit dem LDAP-Adressbuchdienst aber auch direkt LDAP-konforme Verzeichnisdienste abfragen. Neben dem Active Directory kann es im Unternehmen und im Internet weitere Adressbuchdienste wie z.B. eine Novell-NDS oder andere unternehmensweite Datenbanken geben. Allerdings muss dieser Zugriff auf jeden Client individuell konfiguriert werden.

Kontakte durchsuchen

Auflösung anhand der Adressdienste

Bei der Erfassung einer neuen Nachricht können Sie in dem Adressfenster die Namen der Empfänger eintragen. Outlook durchsucht in den konfigurierten Adressdiensten nach Übereinstimmungen und ersetzt so weit wie möglich die Eingabe mit der kompletten Empfängeradresse. Farbig gemusterte Linien zeigen das Ergebnis der Suche an.

Tabelle 4.8 Kennzeichnungen im Adressfeld

Kennzeichnung	Bedeutung
Schwarze Unterstreichung	Adresse wurde eindeutig aufgelöst.
Grün gestrichelt	Adresse ist nicht eindeutig, sie wurde aufgrund früherer Eingaben als wahrscheinlich angenommen.
Rote Wellenlinie	Adresse nicht eindeutig.
Keine Unterstreichung	Adresse noch nicht aufgelöst.

Schon bei der Eingabe der Adresse schlägt Ihnen Outlook 2003 die letzten ähnlichen Eingaben vor. Diese Informationen werden in Ihrem Profil in der Datei „...\Anwendungdaten\microsoft\outlook\profilename.NK2“ abgelegt. Geänderte Adressen können Sie aus dem Cache des „AN:“-Feldes löschen, die neue Adresse wird automatisch nach dem ersten Gebrauch gemerkt.

Suchreihenfolge

Sie können im Profil bestimmen, welche Adressbücher in welcher Reihenfolge durchsucht werden. Viele Adressbücher verlängern natürlich die Suche und erhöhen die Netzwerkbelastung. In Outlook 2003 finden Sie die entsprechenden Punkte im Menü unter „Extras – Adressbuch“ und in „Extras – Optionen“.

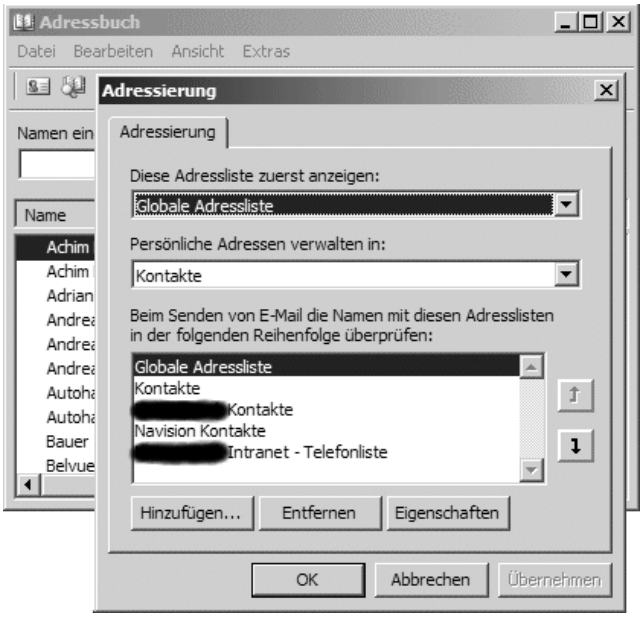


Abbildung 4.57 Suchreihenfolge für Adressbücher einstellen

4.13.3 Termine

Eine der Stärken von Outlook, die es von einfachen Mail-Programmen unterscheidet, ist die Verwaltung und Koordination von Terminen. Dazu legt Outlook im Posteingang einen eigenen Ordner „Kalender“ an, in dem die Mitarbeiter ihre Termine eintragen. Über entsprechende Berechtigungen als Stellvertretung können auch andere Mitarbeiter hier Einblick erhalten.

Für den Exchange-Administrator sind folgende Informationen im Hinblick auf die Terminverwaltung wichtig:

- Zeitzone

  Alle Termine werden in der Exchange-Datenbank mit der Zeitzone „GMT“ gespeichert. Dies bedeutet, dass Outlook beim Abspeichern die eingegebene Zeit anhand der Zeitzone des Arbeitsplatzes umrechnet und die „normalisierte Zeit“ speichert. Stimmt die Zeitzone auf dem Arbeitsplatz nicht oder ist die automatische Umschaltung der Sommerzeit deaktiviert, werden die Terminzeiten nicht richtig angezeigt.

  Reist ein Anwender um die Welt und meldet sich in einer anderen Zeitzone an, werden die Termine in Outlook zu den korrigierten Zeiten des Arbeitsplatzrechners angezeigt. Ein Meeting in Frankfurt um 13:00 Uhr wird in Seattle als Meeting um 06:00 Uhr Ortszeit korrekt angezeigt. Der Wechsel zwischen Sommer- und Winterzeit ändert nichts an den Terminen selbst, sondern wirkt sich nur auf die Berechnungsvorschrift aus.

- Feiertage

  Outlook selbst trägt die Feiertage der nächsten Jahre in den Kalender des Anwenders ein. Ältere Versionen des Clients zeigen daher nicht mehr die aktuellen Feiertage an. Ein entsprechendes Update von Microsoft liefert eine Feiertagsdatei (*.HOL), die dieser Anwender importieren kann. Drittprodukte erlauben einen zentralen Import.

- Caching und OST-Dateien

  Seit Outlook 98 kopiert Outlook die Termine in eine lokale OST-Datei, auch wenn der Anwender überhaupt nicht „offline“ arbeiten möchte. Dadurch entlastet Outlook den Exchange-Server, der ansonsten beim Öffnen des Kalenders alle Terminelemente aktuell vom Server lesen müsste. Dies verursacht sonst eine hohe Netzwerk- und Serverbelastung. Die lokale Datei wird als Cache eingesetzt und regelmäßig mit dem Server synchronisiert.

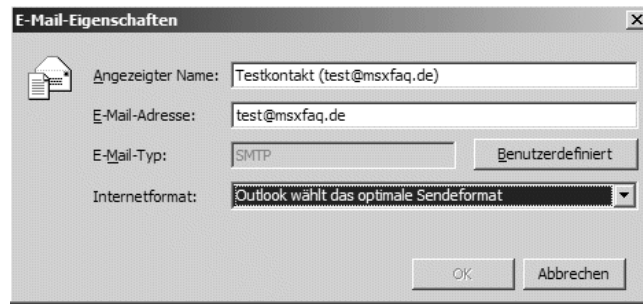
Erweitertes Caching mit Outlook 2003

Genau diese Funktion des Caching hat Outlook 2003 noch erweitert, so dass nun der komplette Posteingang und weitere Outlook-Ordner sowie Öffentliche Ordner lokal als Cache gehalten werden kann.

- Einladungen und Terminabsprachen

  Outlook selbst erlaubt weiterhin die Organisation von Terminen. Aus technischer Sicht erfolgt dies über den Versand von besonders formatierten Nachrichten an alle Teilnehmer. Die Empfänger können einer Besprechung einfach zusagen, wenn sie selbst ebenfalls Outlook nutzen. Diese Funktion ist auch über die Exchange-Organisation hinaus nutzbar. Allerdings muss dann der Anwender oder Administrator dafür sorgen, dass der Empfänger die Nachricht als „RTF-Text“ erhält. Der Anwender kann dies direkt beim Empfänger spezifizieren.

Abbildung 4.58 Mail als RTF senden



Alternativ kann der Administrator im Exchange System-Manager für eine bestimmte Domäne das Format vorgeben.

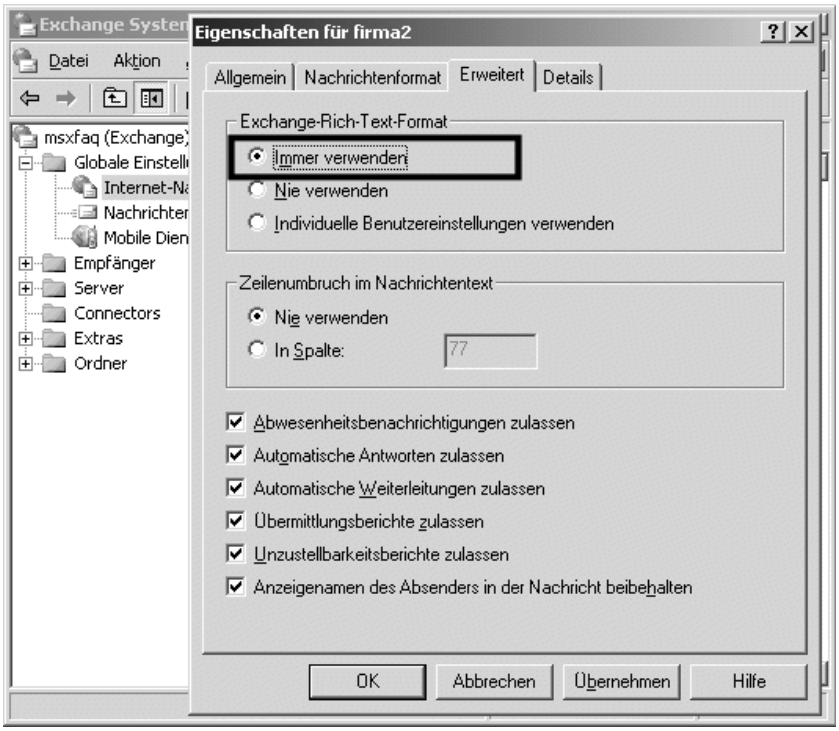


Abbildung 4.59 RTF pro Domäne vorschreiben

- Erinnerungen

  Outlook überwacht alle Termine und informiert den Anwender bei Fälligkeit. Diese Funktion bietet Outlook aber nur für die primären Termin- und Aufgabenordner im eigenen Postfach. Nicht überwacht werden können Termine und Aufgaben in Öffentlichen Ordnern, zusätzlichen Postfächern oder anderen Ordnern im eigenen Postfach. Die Hausmittel von Outlook sind nicht geeignet, um über ein eingeplantes Meeting in einem Team-Kalender zu informieren.

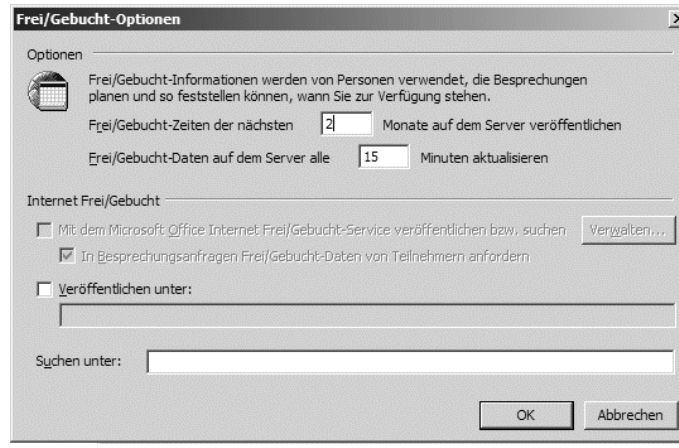
- Erinnerung an Termine

  Die Einhaltung von Terminen ist wichtig, und daher sollte der PC den Anwender unterrichten, sobald ein Termin fällig ist. Der Exchange-Server selbst kann den Anwender nicht informieren, da der Server die Inhalte nicht analysiert. Es ist Outlook, das den Terminkalender des Benutzers überwacht und dann „piept“. Allerdings überwacht Outlook nur die Termine und Aufgaben im eigenen Postfach. Daher sind von Hause aus keine Alarme auf Öffentliche Ordner möglich. Allerdings ist es denkbar, durch eigene Programme und Skripte auch auf Öffentlichen Ordnern eine ähnliche Funktion zu realisieren.

- Frei-/Belegt-Zeiten

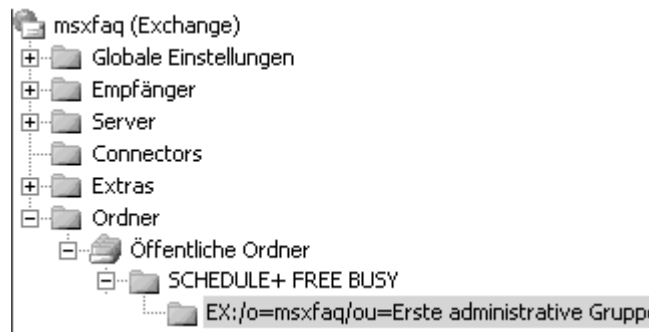
  Eine besondere Form bei der Abstimmung von Terminen ist die Ansicht der freien Zeiten aller Teilnehmer. Hierbei greift Outlook nicht auf den Terminplan des Mitarbeiters selbst zu, sondern auf einen Systemordner. In diesem Ordner befindet sich pro Benutzer ein Eintrag mit den freien und belegten Zeiten der nächsten Wochen. Outlook erstellt diesen Eintrag, den Sie unter „Optionen – Kalender – Frei/Gebucht“ anpassen können.

Abbildung 4.60 Veröffentlichung der Frei-/Belegt-Zeiten anpassen



Diese Informationen werden von Outlook getrennt je AG in einem Systemordner abgelegt und ggf. repliziert.

Abbildung 4.61 Systemordner für Frei-/Belegt-Zeiten



Als Administrator mehrerer Server sollten Sie prüfen, auf welche Server Sie ein Replikat der Frei-/Belegt-Zeiten ablegen sollten. Die Verteilung der Anzeige über mehrere Server hinweg unterstützt eine problemlose und schnelle Terminverwaltung. Der Anwender erkennt in seiner Terminplanung anhand der Farben selbstständig mögliche Terminüberschneidungen.

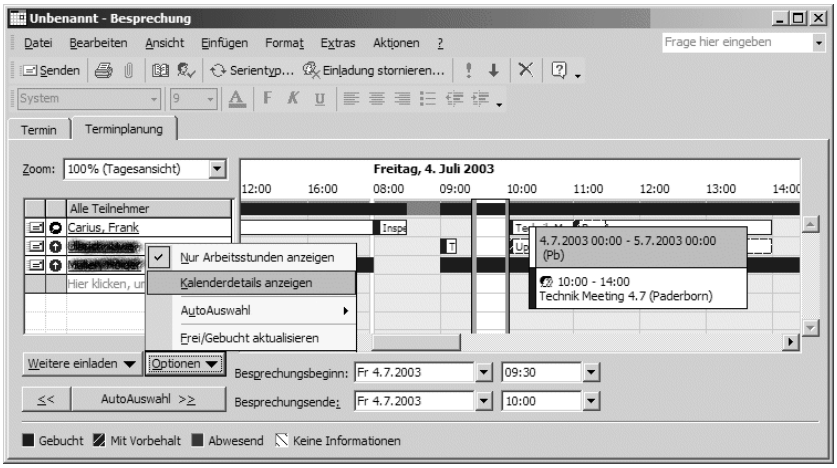


Abbildung 4.62 Terminplanung in Outlook

Wenn statt der Termine nur graue Balken in der Ansicht zu sehen sind, dann bedeutet dies, dass Outlook die Terminübersicht des fraglichen Benutzers nicht finden konnte. Entweder hat der Anwender noch kein Outlook gestartet und die Informationen veröffentlicht, oder die Informationen im Systemordner sind für den anderen Client nicht erreichbar.

Diese Informationen werden jedoch nur für den primären Kalender des Anwenders veröffentlicht. Zusätzliche Terminordner im Postfach oder in öffentlichen Ordnern sind nicht sichtbar.

Web-Ansicht Free-/Busy-Folder

Über den Outlook Web Access ist es dem Administrator möglich, einen schnellen Einblick zu erhalten. Unter der Systemordner-URL „http://servername/public/non_ipm_subtree/“ können Sie einen Blick in die Systemordner wagen. Sie sehen den Status und die Zeiten, an denen die Benutzer das letzte Mal die Termine aktualisiert haben, und ob Replikationen anderer Standorte schon übertragen wurden. In Verbindung mit Connectoren zu Lotus Notes und Novell GroupWise werden optional auch für diese externen Empfänger mit dem Calendar-Connector Einträge angelegt.

Outlook 2003 und Termine

Neue Kalender-Ansicht

Das „neue“ Outlook bringt auch im Bereich Kalender eine sehr hilfreiche Funktionalität mit sich. War bislang die Ansicht des Kollegen-Kalenders nur über die Einbindung bzw. den separaten Aufruf des Ordners möglich, löst Outlook 2003 dies geschickt mit einer neuen Ansicht. Sie können nun mehrere Kalender in Ihrem Outlook einbinden und diese in der Ansicht nebeneinander stellen. Dies gilt sowohl für Kalender des gleichen Postfachs, des Kollegen-Kalenders sowie Öffentlicher Ordner-Kalender, die als Favoriten eingebunden wurden.

4.13.4 Outlook unterwegs

Ein weiteres umfangreiches Kapitel ist der Einsatz von Outlook unterwegs auf Notebooks, in kleinen Niederlassungen ohne eigenen Exchange-Server oder auf Heimarbeitsplätzen. Allen Endgeräten ist gemein, dass sie immer oder zeitweise über keine schnelle Verbindung zum Exchange-Server verfügen. Outlook ist auch für diese Einsatzfelder geeignet, da eine Kommunikation nicht unbedingt RPC voraussetzt, um dem Anwender Zugriff auf ausgewählte Ordner und Nachrichten zu gewähren.

Offline

Outlook unterstützt den Betrieb mit einer OST-Datei, in die Inhalte des Postfachs und öffentlicher Ordner (aus den Favoriten) repliziert werden. Bis Outlook 2002 wurde beim Start automatisch oder durch Rückfrage beim Anwender bestimmt, ob er „online“ oder „offline“ arbeiten wollte. Entsprechend hatte Outlook eine Verbindung zum Exchange-Server aufgebaut oder lokal die OST-Datei des Exchange-Servers als Cache genutzt. Der Abgleich der lokalen OST-Datei erfolgt manuell (F9-Taste), über einen Zeitplan oder beim Starten und Beenden von Outlook. Anwender mit Notebooks können in dem Unternehmen vor dem Verlassen des Gebäudes schnell eine Synchronisation starten und unterwegs mit dem letzten Datenbestand arbeiten.

Allerdings war der Wechsel zwischen den beiden Betriebsmodi immer mit einem Neustart von Outlook verbunden. Selbst im Online-Modus wurden alle Informationen immer vom Exchange-Server geholt, ungeachtet der aktuellen lokalen Kopie.

Cache-Modus

Nutzung geringer Bandbreite

Dieses Verhalten hat Outlook 2003 mit der Einführung eines neuen „Cache-Modus“ (Zwischenspeichermodus) vereinfacht. Die OST-Datei wird im Cached Mode als lokaler Cache genutzt, so dass Zugriffe auf Informationen, die lokal vorhanden sind, auch von dort und nicht vom Server gelesen werden. Dies entlastet Server und Netzwerk. Ist der Exchange-Server nicht verfügbar, bleibt Outlook nicht hängen wie bisher, sondern nutzt weiter die Offline-Datei. Der Übergang ist fließend und fällt dem Anwender kaum auf. Der Einsatz des Cached Modus ist nicht abhängig von Exchange 2003, sondern funktioniert auch mit Exchange 2000. Beachten Sie jedoch, dass bei der Umstellung aller Clients auf den Cache-Modus beim ersten Starten von Outlook alle Daten vom Exchange-Server synchronisiert werden. In großen Unternehmen führt die Einstellung zu einer Überlastung des Servers, insbesondere wenn es sich hierbei um recht große Postfächer handelt.

Offline Adressbuch

OAB versorgt Client mit Adressen

Outlook im Offline-Modus nutzt eine Kopie des Adressbuchs, das sogenannte Offline-Adressbuch (OAB). Das Adressbuch wird standardmäßig einmal täglich um 6 Uhr morgens auf einem Server erstellt und steht für die Synchronisation aller Offline-Clients also auch den Cache-Modus-Clients zur Verfügung. In der Praxis hat sich dies manchmal als sehr fehleranfällig oder unkomfortabel erwiesen, da häufig ein vollständiger Download des Offlineadressbuchs durchgeführt wurde. Microsoft hat das OAB 4.0 mit dem Service Pack 2 veröffentlicht. Vorteile der neuen Version sind die lokale OAB-Indizierung, die binäre Komprimierungstechnologie (BinPatch) der Updates und die damit verbundenen Reduzierung der OAB-Größe. Auch können Sie jetzt angepasste Eigenschaften und Indizes verwenden. Voraussetzung für das neue Offline-Adressbuchformat ist Outlook 2003 Service Pack 2 sowie die Verwendung des Unicodemodus. Outlook 2003 verwendet generell diesen Modus, der im Outlook-Profil unter den erweiterten Optionen definiert wird.

Praktische Bedeutung

Für den Mitarbeiter bedeutet dies eine erhebliche Erleichterung, da er nun nicht mehr ständig sein Outlook neu starten muss, um den gewünschten Betriebsmodus zu erreichen. Der Administrator gewinnt durch die Entlastung des Servers die Möglichkeit, mehr Anwender auf einem Server zu konsolidieren. Sogar kurze Unterbrechungen des Serverbetriebs z.B. durch Updates und Patches werden von vielen Anwendern nicht mehr bemerkt, da sie fast wie gewohnt weiter arbeiten können. Nur Zugriffe auf Informationen außerhalb des lokalen Caches führen zu Meldungen.

Synchronisation von Outlook

Outlook 2003 mit Offline-Datei und Cached Mode erlaubt dem Anwender eine umfangreiche Anpassung des Synchronisationsverhaltens. Entsprechend der Anbindung an den Server können unterschiedliche Übermittlungsgruppen angelegt werden, so dass abhängig von der Anbindung nur selektiv repliziert wird.

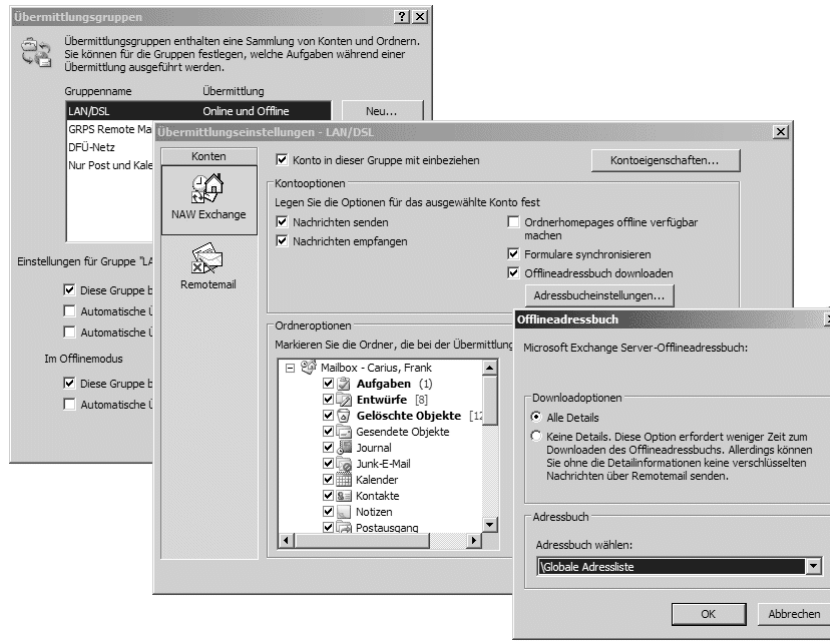


Abbildung 4.63
Outlook-Offline-Einstellungen

Allerdings sind diese Vorgaben je Benutzer individuell einzustellen und können nicht auf dem Server konfiguriert werden. Als Unternehmen sollten Sie Ihre Außendienstmitarbeiter speziell unterweisen, damit über Mobiltelefone aus Kostenaspekten keine kompletten Replikationen durchgeführt werden. Für jede Übermittlungsgruppe kann bestimmt werden, ob diese beim Druck der Funktionstaste „F9“ in den Abgleich mit einbezogen wird. Die Auswahl der gewünschten Replikation erfolgt über das Menü.

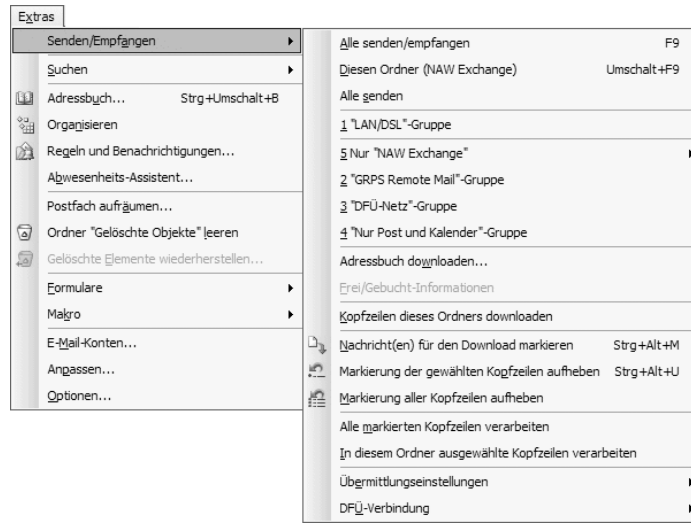


Abbildung 4.64
Outlook-Synchronisationsmenü

In der Fußzeile von Outlook ist der aktuelle Status zu erkennen. Analog dazu blendet Outlook ein Icon in der Symbolleiste des Windows-Startmenüs ein.

Abbildung 4.65 Statusanzeige in Outlook

Über diese Statusanzeige kann der Anwender auch manuell die Umschaltung in den echten Offline-Betrieb durchführen, da Outlook sonst immer wieder einen Verbindungsversuch startet. Die einzelnen Statusmeldungen bedeuten:

Tabelle 4.9 Outlook-Statusmeldungen

Anzeige	Bedeutung
Offline	Outlook nutzt nur die OST-Datei und versucht nicht selbstständig, den Exchange-Server zu erreichen.
Getrennt	Outlook kann den Exchange-Server im Moment nicht erreichen, wird es dennoch weiter versuchen.
Verbindungsversuch	Outlook versucht den Exchange-Server zu erreichen. Den Prozess wiederholt Outlook immer dann, wenn eine Änderung der Netzwerkkonfiguration erfolgt ist, z.B. eine DFÜ-Verbindung aufgebaut wurde. Sie können dies unterbinden, indem Sie den „Offline-Betrieb“ erzwingen.
Verbunden	Outlook ist mit dem Exchange-Server verbunden und gleicht die Daten permanent ab.

Die neue Variante von Outlook 2003 mit Cached Mode eröffnet für verschiedene Einsatzbereiche ganz neue Möglichkeiten. Bislang musste bei der Planung einer Exchange-Infrastruktur die Netzwerkanbindung des Clients an den Server sehr stark berücksichtigt werden. Dies bedeutete häufig, dass auch kleine Niederlassungen mit wenigen Anwendern einen eigenen Server vor Ort erhielten, damit die Antwortzeiten akzeptabel waren. Eine Alternative wäre der Einsatz von Terminal-Servern in solchen Umfeldern. Der Betrieb von Outlook 2002 und älter im Offline-Betrieb bringt für den Einsatz innerhalb eines Unternehmens jedoch starke Einschränkungen mit. So kann offline kein Zugriff auf andere Termine oder Frei-/Belegt-Zeiten erfolgen, und Öffentliche Ordner außerhalb der Favoriten sind ebenfalls nicht erreichbar. Seit Outlook 2003 können solche Anwender auch über schmalbandige Leitungen dank des lokalen Caches zügig online arbeiten.

Verbindungsstatus prüfen

Sie können den Verbindungsstatus beim Client auf mögliche Fehlerquellen prüfen. Klicken Sie auf dem Arbeitsplatz mit der Kombination „STRG + rechte Maustaste“ auf das Outlook-Symbol in dem Infobereich der Taskleiste. In dem Kontextmenü können Sie über VERBINDUNGSSTATUS

manuell eine Verbindung wiederherstellen und somit die Konnektivität zum Exchange-Server prüfen.

RPC over HTTP

Outlook-Client mit HTTP-Verbindung

Mit Outlook 2003 und Exchange 2003 ist es erstmals möglich, diese Synchronisation nicht nur über die übliche RPC-Verbindung zu betreiben, sondern in http-Pakete einzupacken. Diese „RPC over HTTP“ genannte Funktion umgeht viele Probleme und Einschränkungen, die RPC mit sich bringt. So muss bei einer RPC-Verbindung der Client den Port 135/TCP des Exchange-Servers und die Domänencontroller erreichen können. Diesen Zugang blockieren viele Administratoren jedoch aus gutem Grund.

Demzufolge konnte Outlook sich immer nur dann replizieren, wenn der Anwender sich entweder direkt in der Firma einwählt oder der Zugriff über das Internet auf RPC erst nach einer expliziten Autorisierung erfolgt. Dies wurde in der Regel über VPN oder umständliche Anmeldungen an einer Firewall gelöst. Selbst wenn die eigene Firewall den Zugriff erlaubt, kann der Anwender immer noch hinter einer anderen Firewall vor Ort sitzen, die den Zugriff verhindert.

Der Zugriff auf das Internet mit einem Webbrowser ist jedoch meist möglich. Genau die gleiche Kommunikation nutzt Outlook mit RPC over HTTP. Um diese Funktion zu erreichen, müssen Sie Windows 2003 Server, Exchange 2003, Windows XP mit SP1 und dem Hotfix aus dem TechNet-Artikel 331320 sowie Outlook 2003 einsetzen.

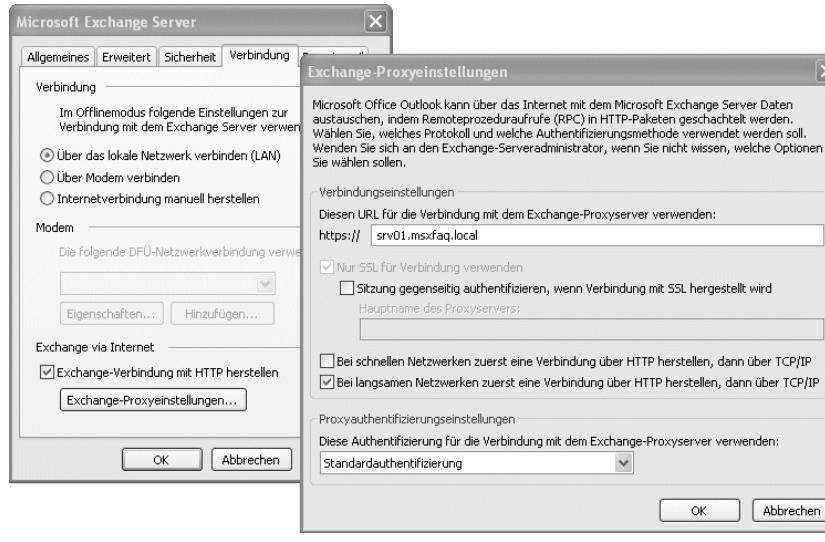


Abbildung 4.66 RPC over HTTP-Einstellungen in Outlook

Die Autorisierung NTLM ist zwar sicherer, aber nicht mit allen Proxy-Servern kompatibel, so dass die Standardauthentifizierung und der Einsatz von SSL der beste Weg sind.

Remote Mail

Für sehr geringe Bandbreiten oder Verbindungen mit hohen Volumenkosten (z.B. Mobilfunk) bietet Outlook schon länger die Option „Remote Mail“ an. Hierbei werden nur die Kopfzeilen der Nachrichten im Posteingang übertragen. Der Anwender kann dann entscheiden, ob die Nachricht komplett übertragen oder gelöscht werden soll. In einem zweiten Durchlauf werden die angegebenen Optionen umgesetzt.

Diese Methode erlaubt die Menge der übertragenen Daten zu reduzieren, bedeutet aber mehr Aufwand für die Bedienung von Outlook und entsprechendes Know-how bei den Anwendern.

Datenvolumen und Replikationsdauer

Bei aller Weiterentwicklung von Outlook und Exchange bleibt einer der wesentlichen Punkte die zu übertragende Datenmenge zwischen Client und Server. Auch hier hat sich mit der Kombination Exchange und Outlook Version 2003 maßgeblich einiges verbessert.

Kompression des Datenvolumens

Nicht nur der Ersatz des Protokolls RPC durch HTTP bei der Anbindung über das Internet ist ein Grund für eine schnellere Replikation, sondern auch die Kompression der Daten bei der Übertragung zwischen Server und Client. Für eine generelle Aussage ist es sicher noch etwas früh, aber erste Tests haben sehr positive Ergebnisse gezeigt. Bei identischen Nachrichten erfolgte die Replikation von Outlook 2003 in Verbindung mit Exchange 2003 fast doppelt so schnell. Im Gegensatz zum gleichen Client mit Exchange 2000 reduzierte sich auch die übertragene Datenmenge etwa um die Hälfte.

Durch den Cached Mode von Outlook 2003 wird der Exchange-Server zudem von der wiederholten Lieferung von Informationen entlastet, wodurch viel mehr Anwender auf einem Server betrieben werden können. Dies erfordert natürlich die entsprechende Verfügbarkeit der Server. Auch hier kann Exchange 2003 mit einer sehr viel kürzeren Umschaltzeit beim Betrieb auf einem Cluster-Server punkten.

All diese Neuerungen können jedoch nicht darüber hinwegtäuschen, dass jede nicht übertragene oder replizierte Nachricht eingesparte Kosten darstellt. Viele Regeln und der Spam-Schutz von Outlook 2003 greifen erst auf dem Client. Daher sind zusätzliche Schutzmaßnahmen auf dem Server gegen Spam und Viren unverzichtbar.

4.14 Programmieren mit Exchange

Exchange 2003 ist im Gegensatz zu Exchange 5.5 sehr viel leistungsfähiger und offener für Eigenentwicklungen geworden. Zahlreiche neue Möglichkeiten und Schnittstellen erlauben es, die Leistung von Exchange um eigene Funktionen zu erweitern und das System den individuellen Bedürfnisse anzupassen. Das Thema Exchange-Programmierung ist so umfangreich, dass auch ein eigenes Buch nur einen Teil davon abdecken könnte. So gibt es von Microsoft ein Exchange SDK zum Download. Auch zu Outlook gibt es umfangreiche Bücher und Webseiten mit Beispielen und Skripten.

Für Sie, der Exchange plant, installiert und administriert, kann es entscheidend sein, die entsprechenden Schnittstellen und Möglichkeiten zu kennen. Mit diesem Know-how sind Sie imstande abzuwägen, wie Programme in Ihren Server eingreifen, welche Berechtigungen und sonstigen Randbedingungen zu erteilen und Fehler einzukreisen sind.

Aber auch als Entwickler, der eine Lösung schaffen soll, ist es wichtig, die unterschiedlichen Ansätze zu kennen, die Exchange und Outlook für die Entwicklung eigener Anwendungen bieten. Die Kombination aus Server und Client besteht aus mehreren Komponenten, die individuell erweitert und ergänzt werden können.

Als Entwickler müssen Sie überlegen, ob Ihr Programm auf dem Exchange-Server selbst ablaufen soll oder ob die Anwendung eher wie ein Client auf den Server zugreift.

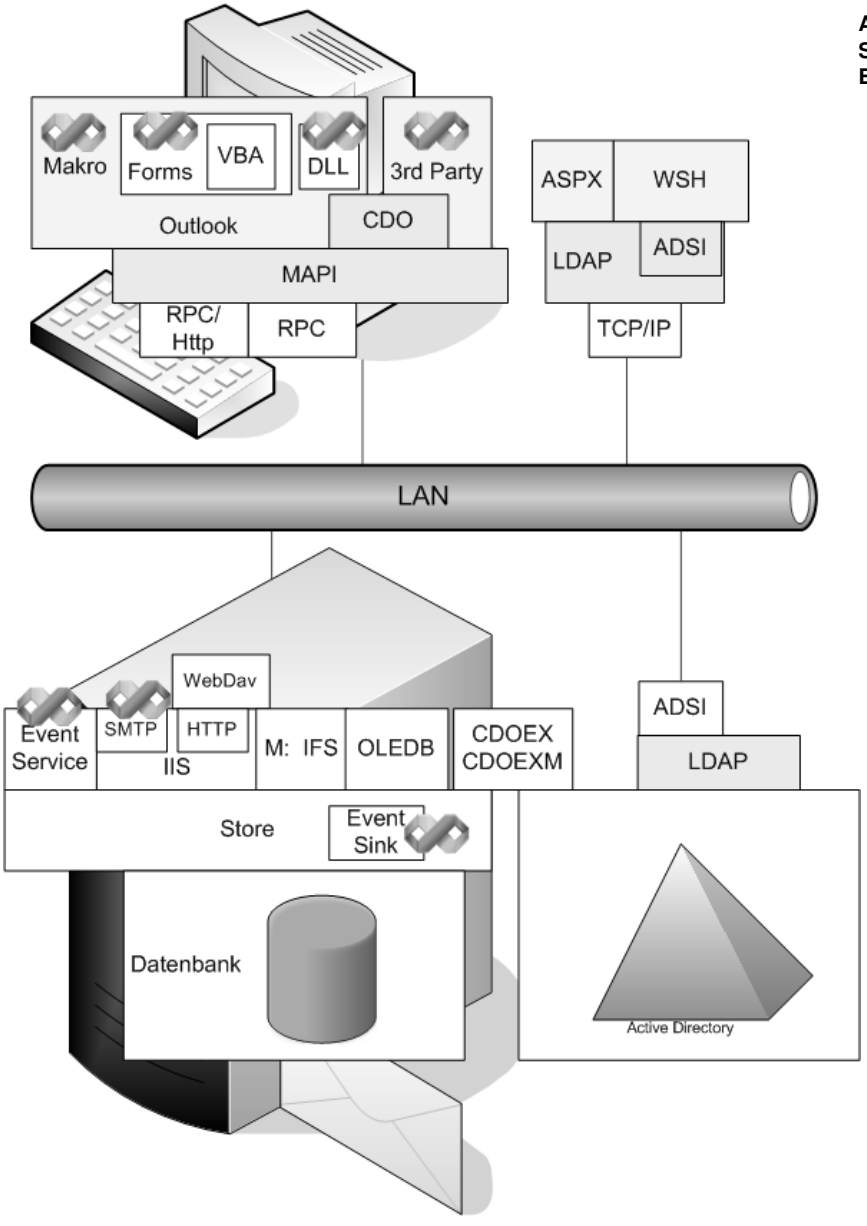


Abbildung 4.67
Schnittstellen für Entwickler

4.14.1 Client

Für den Zugriff als Client bietet sich Outlook an oder eine eigene Anwendung, welche die Dienste von Outlook nutzt.

Outlook-Formulare und -Ansichten

Der erste und einfachste Anfang betrifft die Anpassung von Ordneransichten und Formularen für Outlook. Hiermit sind einfache Veränderungen sehr schnell und einfach zu realisieren.

Outlook erlaubt zusätzlich auch den Einsatz von Skripten und ActiveX-Controls innerhalb von Formularen. So ist der Zugriff aus einem Formular auf fremde Datenquellen ebenso problemlos möglich wie die Ansichtsoptimierung der enthaltenen Daten. Oft finden Sie entsprechende Formulare in Verbindung mit Faxservern, die so eine eigene Ansicht der eingegangenen Faxe erlauben. Der Entwurf und die Veröffentlichung von Formularen erfolgt in Outlook selbst über das Menü „EXTRAS – FORMULARE“. Hier finden Sie auch die zweite Möglichkeit, bestimmte Dinge in Outlook über Makros zu automatisieren. Formulare können je Ordner, je Benutzer oder global veröffentlicht werden. Auf diese Weise übernimmt Outlook auch die Verteilung der Formulare auf die Clients, nicht jedoch eventuell eingebetteter Objekte.

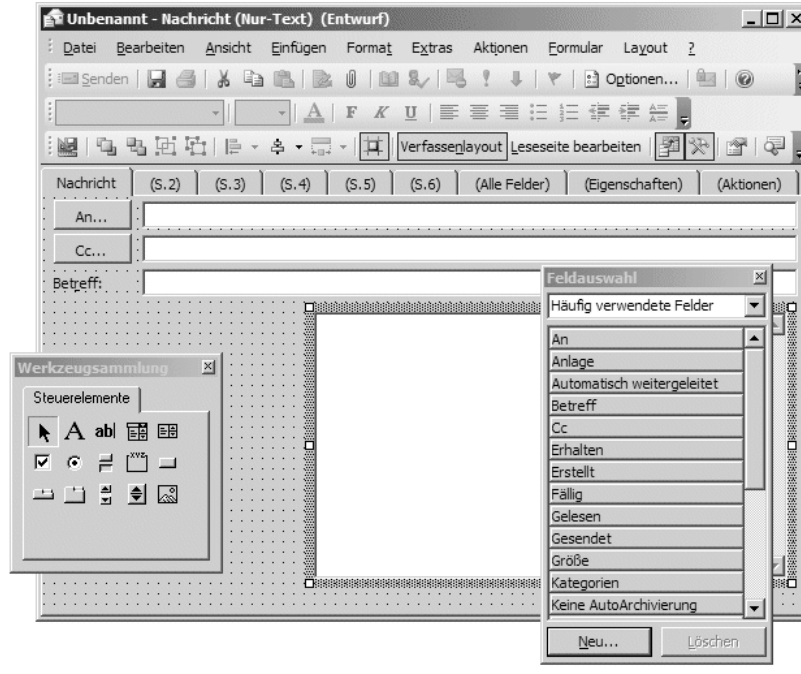


Abbildung 4.68 Entwurf eines Outlook-Formulars

Ähnlich einer Entwicklungsumgebung können Sie direkt in Outlook Formulare entwerfen, Felder hinzufügen und unter „Aktionen“ auch Skriptcode hinterlegen, der von Outlook später ausgeführt wird. Für den Exchange-Server sind diese Formulare und der Code jedoch nicht sichtbar. Der Exchange-Server dient nur als Informationsspeicher.

Ein weiteres Mittel besteht in der Erweiterung von Outlook dank entsprechender Add-Ins oder COM-Add-Ins.

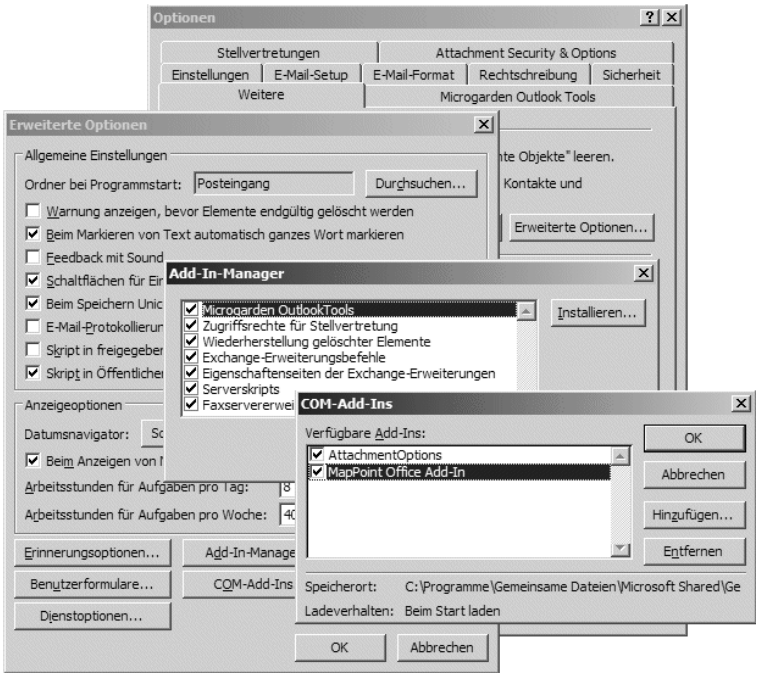


Abbildung 4.69 AddIns in Outlook

Einige Outlook-Add-Ins werden erst in Verbindung mit dem Exchange-Server aktiviert. Dazu zählt neben der Funktion, gelöschte Elemente wieder zu retten auch, das Add-On für Server-Skripte. Sehr hilfreich bei der Entwicklung ist das *Outlook Objekt-Modell*, das ebenfalls im SDK zu finden ist.

Sonstige Client-Programme

Neben Outlook kann natürlich jedes beliebige Programm die auf dem Arbeitsplatz angebotenen Schnittstellen nutzen, um Daten zu verarbeiten und Lösungen zu schaffen. Der Zugriff auf die verschiedenen Informationen in der Exchange-Datenbank oder dem Active Directory erfolgt über MAPI und CDO; aber auch WebDav, ADSI und LDAP sind gängige Schnittstellen. Hierbei sind Sie nicht auf Outlook beschränkt. So sind Programme denkbar,

die regelmäßig Informationen im Exchange-Server prüfen und entsprechende Aktionen auslösen.

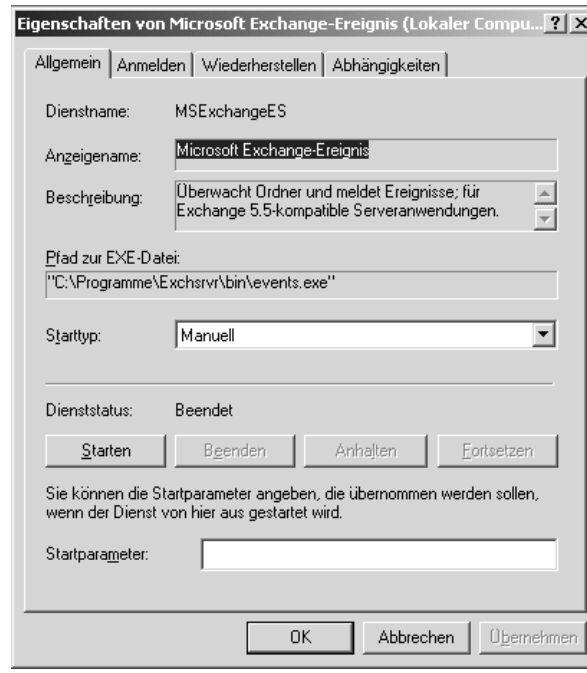
4.14.2 Server

Sehr viele Optionen zur Einbindung eigener Programme bietet auch der Exchange 2003-Server. Durch die Installation von Exchange wird bereits ebenfalls eine vereinfachte MAPI-Umgebung geschaffen, die es vielen clientseitigen Programmen erlaubt, auch auf dem Exchange-Server zu laufen. Die Installation von Outlook auf dem Server ist, wie bereits erwähnt, nicht erforderlich, ja sogar schädlich.

Event-Service

Eine der Schnittstellen für serverbasierte Anwendungen ist der Microsoft Exchange Event-Service, der schon seit Exchange 5.5 verfügbar ist. Der Dienst wird mit Exchange 2003 installiert, aber nicht gestartet.

Abbildung 4.70 Exchange-Ereignisdienst



Für den Einsatz von Ordnerskripten muss dieser Dienst gestartet sein. Beim ersten Start legt er einen Systemordner an, in dem die Skripte gespeichert werden. Der Administrator muss den Entwicklern der Skripte in diesem Ordner erst die Berechtigungen zur Ablage derselben erteilen.

Abbildung 4.71
Systemordner für Event-Skripte

Die Einrichtung und Programmierung der eigenen Skripte erfolgt über Outlook. Nach der Einbindung der Erweiterung „Server-Skripte“ findet sich eine weitere Karteikarte „Agenten“ in den Eigenschaften des Systemordners, über die der Service programmiert werden kann.

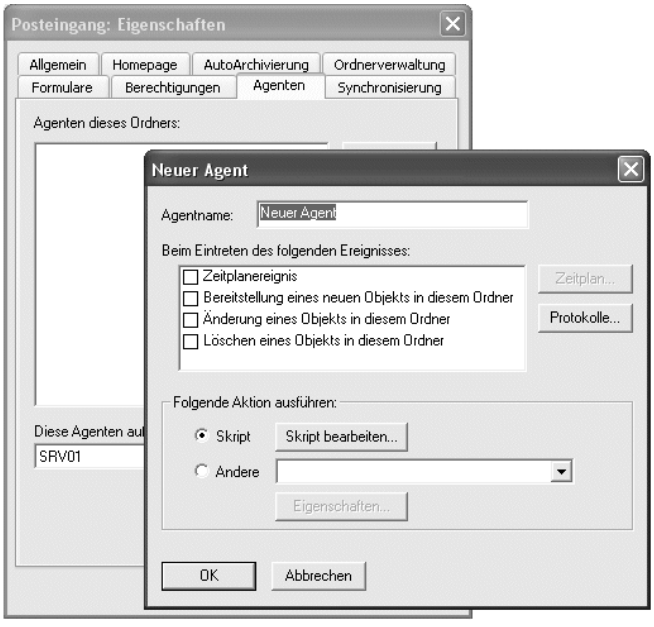


Abbildung 4.72
Einrichten von Server-Events

All diese Skripte laufen später auf dem ausgewählten Server asynchron ab. Allerdings kann die Ausführung zeitverzögert zum Eintreffen der Ereignisse erfolgen. Skripte können für vier verschiedene Aktionen gestartet werden:

- Zeitplan (Folder_OnTimer)

  Entsprechend einem Zeitplan kann das Skript regelmäßig zu bestimmten Tagen und Zeiten gestartet werden. So können Skripte den Status einer Nachricht prüfen und diese nach Ablauf einer Zeit weiterleiten.

- Neues (Folder_OnMessageCreated)

  Das Skript wird gestartet, wenn ein neues Element in diesem Ordner abgelegt wird. Damit können neue Nachrichten automatisch angepasst oder weitergeleitet werden.

- Ändern (Message_OnChange)

  Die Veränderung einer bestehenden Nachricht kann ebenfalls ein Skript starten.

- Löschen (Folder_OnMessageDeleted)

  Nach dem Löschen einer Nachricht wird das Skript gestartet. Allerdings kann damit kein Löschen verhindert werden, da die gelöschte Nachricht nicht mehr verfügbar ist.

Skripte werden jedoch immer nur pro Ordner eingerichtet. Soll vielen Ordnern das gleiche Skript zugewiesen werden, dann ist dieses jeweils einzeln einzurichten. Schlägt ein Skript fehl, so finden Sie einen Eintrag im Eventlog. Das Skript wird so lange nicht gestartet, bis der Fehler behoben ist. Besonders aufgrund der langsamen Verarbeitung der Skripte und der asynchronen Natur war die Einsatzmöglichkeit dieser Skripte beschränkt.

Event Sink

Mit Exchange 2000 wurde eine neue Möglichkeit geschaffen, eigene Skripte auf dem Exchange-Server zu installieren. Event Sinks sind Objekte, die an verschiedenen Stellen des Exchange-Servers registriert und in Echtzeit ausgeführt werden können. Es gibt drei verschiedene Sinks:

Aktiver Eingriff in den Ablauf

- Store Event Sink

  Abgelegte oder veränderte Nachrichten im Informationsspeicher können über diese Module verarbeitet werden. Im Gegensatz zu den Event-Skripten ist eine synchrone Ausführung möglich. Dies bedeutet, dass Sie mit Outlook eine Nachricht in einem Öffentlichen Ordner ablegen, ändern oder löschen können, der Event Sink indessen vorher gestartet und beendet sein muss, so lange blockiert der Prozess in Outlook mit einer Sanduhr. Damit wird erstmalig erreicht, das Löschen eines Events zu verhindern, obwohl Sie die Rechte dazu hätten. Die Event Sinks sollten als Programme auf dem Exchange-Server installiert und für den jeweiligen Ordner registriert werden.

- Transport Event Sink

  Neu seit Exchange 2003 sind die Sinks, die auf dem Transportweg eingebunden werden können. In der Exchange Routing Engine werden dazu an den verschiedensten Stellen eigene Module eingebunden, die Nachrichten während der Übertragung verarbeiten. Auch im virtuellen SMTP-Server sind diese Module nutzbar, zum Beispiel um eingehende

Nachrichten nach dem Empfang zu prüfen oder zu verändern und ausgehende Nachrichten mit einem „Disclaimer“ zu versehen.

- Protokoll Event Sink

  Diese Module erweitern den virtuellen SMTP-Server um weitere Befehle. Exchange 2003 selbst nutzt diese Sinks, um den Windows 2003 SMTP-Server um Exchange-spezifische Befehle, wie XLINKSTATE, zu erweitern. Über diese Option können Entwickler eigene Funktionen im SMTP-Server auf Protokollebene integrieren oder bestehende Funktionen ersetzen.

Die Exchange-Event Sinks sind damit um einiges leistungsfähiger als die Möglichkeiten des bislang mit Exchange 5.5 verfügbaren Exchange-Event-Service.

Ein einfaches Beispiel eines Sinks ist die „CatchAll“-Funktion, die Exchange von Hause aus nicht bietet. Ein Transport Event Sink auf dem virtuellen Exchange-Server leitet alle Nachrichten an eine Domäne in eine einzige Mailbox um. Den Sourcecode finden Sie im TechNet-Artikel 324021 „HOW TO: Create a "Catchall" Mailbox Sink for Exchange 2000“.

Auch auf http://msdn.microsoft.com/exchange finden sich viele Beispiele, Anleitungen und die entsprechenden SDKs.

Administrative Programme

Neben der Bearbeitung von Nachrichten bei der Erstellung mit Outlook und der Verarbeitung auf dem Mailserver ist die Exchange-Administration ein weiteres Gebiet, in dem durch eigene Programme eine Kostensenkung erreicht werden kann. Gerade größere Installationen und der Wunsch nach Automatisierung erfordern entsprechende Hilfsmittel zur Vereinfachung der Verwaltung von Objekten. Mit Exchange 2003 wurden auch hier weitere Schnittstellen offen gelegt, um eine effektive Administration zu ermöglichen:

- LDAP/ADSI

  Sehr viele Exchange-Informationen stehen im Active Directory, das über LDAP oder die ADSI-Schnittstelle sehr effizient zu administrieren ist. Diese Schnittstelle bietet sich an, um neue Benutzer anzulegen, Verteiler und Gruppen anzupassen oder Auswertungen und Berichte zu erstellen. Im Active Directory stehen unter anderem auch die E-Mail-Adressen der Anwender und die Grenzwerte für Postfächer und Protokolle, die sich so sehr einfach und schnell bearbeiten lassen.

- CDOEXM/CDO

  CDOEXM ist nach der Installation der Exchange-Management-Komponenten verfügbar, während CDO nur auf dem Exchange-Server selbst verfügbar ist. CDO wird unter anderem für die Verwaltung Öffentlicher Ordner benötigt. Die Verwaltung von Benutzern ist mit CDOEXM möglich.

  Einen Vergleich der beiden Methoden finden Sie im TechNet-Artikel 297390 INFO: Comparing Use of ADSI and CDO to Access CDOEXM Recipient-Related Methods.

- WMI

  Die Windows Management Instrumentation-Schnittstelle ist schon länger eine Schnittstelle zum Auslesen und Setzen diverser Systemeinstellungen. Seit Exchange 2003 sind über diesen Weg auch umfangreiche Änderungen an Exchange selbst über dokumentierte Funktionen möglich. So nutzt das Programm PFMIGRATE.WSH selbst die Exchange 2003-WMI-Erweiterung, um Replikate von Öffentlichen Ordnern zu ändern.

  Einen Einstieg in die Nutzung von WMI unter Exchange finden Sie auf http://msdn.microsoft.com/library/en-us/e2k3/e2k3/_e2k3_WMIIntro.asp.

Letztlich sind Sie für die Entwicklung von administrativen Hilfsprogrammen darauf angewiesen, alle Schnittstellen zu kennen und bei Bedarf einzusetzen, da bestimmte Aktionen nur mit der einen oder anderen Schnittstelle durchführbar sind. Umgekehrt gibt es überdies Aktionen, die mit verschiedenen Schnittstellen gleichermaßen ausgeführt werden können.

5

Internet-Grundlagen

5 Internet-Grundlagen

Nach den Konzepten zu Windows 2003, Active Directory und Exchange 2003 ist die Anbindung an das Internet ein weiterer großer Baustein bei der Integration von Exchange 2003. Gerade die Anbindung an das Internet ist der Teil einer Exchange-Einführung, der am schwierigsten umzusetzen ist und je nach Implementierung instabil oder nicht fehlerfrei funktioniert.

Daher ist dieses Kapitel um einiges umfangreicher geworden, um nicht nur die Sachverhalte und Zusammenhänge ausführlich zu beschreiben, sondern auch besonders auf die Situation in Deutschland einzugehen.

Im Installationsteil werden exemplarisch drei Anbindungen detaillierter beschrieben. Ungeachtet einer erfolgreichen Anbindung ans Internet anhand des praktischen Teils sollten Sie unter allen Umständen das Konzept zum Virenschutz vorab lesen und umsetzen.

5.1 Exchange und das Internet

Der Betrieb von Exchange im internen Netzwerk ermöglicht eine effektive Zusammenarbeit der Mitarbeiter. Aber erst durch die Anbindung an das Internet wird Exchange eine leistungsfähige Kommunikationsplattform.

Die Anbindung an das Internet bedeutet in der Regel auch eine Verbindung des gesamten Netzwerks, damit die Anwender Informationen suchen und erhalten können. Exchange nutzt das Internet überwiegend für die Übertragung von Nachrichten. Ein Internet-Anschluss nur für die Nutzung mit Exchange genügt nicht den zukünftigen Anforderungen im Unternehmen.

Folgende Dienste können von einer Internet-Verbindung mit Exchange profitieren:

Bereitstellung von Diensten über das Internet.

- Eingehende E-Mails

  E-Mails an die Postfächer werden vom Exchange-Server empfangen bzw. mit Hilfsprogrammen abgeholt

- Versand von Nachrichten per SMTP

  Die Nachrichten der Anwender werden an entfernte Systeme übermittelt.

- Lesen von Nachrichten über Internet-Protokolle

  Über den Zugriff per POP3 und IMAP4 können Anwender von unterwegs oder zu Hause Ihr Postfach öffnen. Allerdings nutzen beide Protokolle Klartext-Kennworte, so dass Sie eine Verschlüsselung mit SSL vorsehen

sollten. Zudem birgt gerade POP3 das Risiko, dass Anwender unabsichtlich die Nachrichten herunterladen und auf dem Server löschen.

- Lesen von Nachrichten per Browser

  Der Exchange 2003 Outlook Web Access (OWA) erlaubt einen einfachen Zugriff auf die Nachrichten im Postfach über einen beliebigen Browser. Auch hier ist die Verschlüsselung und Absicherung des Webservers zu beachten.

- Zugriff für mobile Geräte

  Exchange 2003 bietet mit Outlook Mobile Access (OMA) auch für PocketPCs und WAP-Systeme eine Möglichkeit, auf Nachrichten zuzugreifen. Aber auch andere Clients wie Blackberry etc. nutzen TCP/IP als Kommunikationsprotokoll und benötigen die Anbindung an das Internet.

- Zugriff per VPN

  Über eine VPN-Verbindung kann sich ein Mitarbeiter von unterwegs unter Nutzung von Verschlüsselung und Autorisierung in Ihrem Netzwerk anmelden und viele andere interne Dienste nutzen.

- Infrastrukturdienste

  Damit alle vorab genannten Zugriffsarten sicher funktionieren, ist die Einrichtung einiger unterstützender Dienste erforderlich. So muss der Server über DNS die Gegenstellen auflösen können. Nebenbei kann über die Internet-Verbindung auch gleich eine genaue Uhrzeit abgerufen werden, damit die Systemzeit korrekt gesetzt ist.

All dies ist Bestandteil dieses Kapitels.

5.2 E-Mail im Internet

Exchange 2003 ist aus Sicht des Internets primär ein E-Mail-Server, der Nachrichten sendet und empfängt. Um später die verschiedenen Varianten einer Anbindung zu verstehen und im Fehlerfall auf das notwendige Wissen zur Ursachenforschung zurückgreifen zu können, widmet sich dieser Abschnitt der Erklärung der Protokolle und Funktionsweise von SMTP, DNS und POP3.

Im ersten Teil wurde schon auf die Zusammenhänge zwischen E-Mail-Server, E-Mail-Client und MTA eingegangen. Ab hier beschäftigen wir uns nun mit der Verbindung zwischen den Message Transfer Agents (MTA) zweier Exchange-Server.

5.2.1 Die E-Mail im Detail

Aber ehe wir uns der Übertragung von Nachrichten widmen, ist ein kleiner Abstecher in die Begriffsdefinition erforderlich.

Was genau ist eigentlich eine E-Mail?

Aus technischer Sicht ist eine E-Mail eine Information, die als Datensatz in einer Datenbank oder als eine Datei auf einer Festplatte vorliegt. Die meisten E-Mail-Server arbeiten nach diesem Prinzip, damit die Nachricht nicht alleine im Hauptspeicher gehalten und bei einem Stromausfall verloren geht. Aus Sicht eines Anwenders besteht eine E-Mail aus den Bestandteilen der Adresse, dem Betreff und dem Textkörper, und optional sind noch Anlagen beigefügt. Aus der Computerperspektive wird die Nachricht in folgende drei Bestandteile aufgeteilt:

Teile einer Nachricht

- ENVELOPE

  Der Umschlag einer E-Mail enthält alle Auskünfte für die Computer, die für die Zustellung einer Nachricht notwendig sind. Der Umschlag selbst wird vom ersten E-Mail-Server oder dem Absender anhand der Empfängerliste erstellt und vom letzten E-Mail-Server wieder entfernt.

- HEADER

  Der eigentliche Kopf einer Nachricht enthält erneut die Liste der Empfänger, aber auch die Zwischenstationen, die die Nachricht bislang durchlaufen hat. Ferner finden sich hier die Zeit, das Datum und der Betreff sowie viele andere Attribute. Die Informationen im Header werden unterwegs und am Ziel nicht für die Zustellung der Nachricht verwendet, sondern helfen bei der Fehlersuche und werden von Ihrem E-Mail-Programm teilweise angezeigt.

- BODY

  Den Inhalt der E-Mail, den der Anwender als Nachricht sieht, ist im BODY untergebracht. Auch die Anlagen, die Sie als eigenständige Elemente der Nachrichten sehen, sind für den Computer auch nur einfach ein Teil des BODY.

Die Kenntnis dieser drei Bereiche ist wichtig für die spätere Erklärung von SMTP und POP3 und den damit verbundenen Problemen.

Eine E-Mail könnte folgenden Aufbau haben:

Die einfachste Form einer E-Mail

```
FROM: user1@msxfaq.de
TO: admin@msxfaq.de
BCC: frank@msxfaq.de
SUBJECT: Wichtige Nachricht

Nur für den Administrator!!
```

In dem Beispiel sendet der User1 eine Nachricht an den Administrator und trägt einen zweiten Empfänger als Blindkopie (BCC) ein. Dem normalen Empfänger (Administrator) bleiben die Empfänger unter „BCC:“ verborgen. Er wird später nicht sehen, dass „frank@msxfaq.de“ diese Nachricht ebenfalls erhalten hat. Viele Personen mögen „Blindkopien“ nicht, da Ihnen immer etwas Heimliches anhaftet. Schließlich erkennt der Empfänger nicht, wer noch eine Kopie erhalten hat. Exchange benötigt jedoch alle Empfängerinformationen, um die Nachrichten sowohl an die sichtbaren als auch an die Blindkopieempfänger richtig zuzustellen. Der erste E-Mail-Server erweitert diese Nachricht daher und überträgt:

Die E-Mail zwischen den Servern

```
MAIL FROM: user1@msxfaq.de
RCPT TO: admin@msxfaq.de
RCPT TO: frank@msxfaq.de
DATA
FROM: user1@msxfaq.de
TO: admin@msxfaq.de
SUBJECT: Wichtige Nachricht

Nur für den Administrator!!
.
```

Sie erkennen, dass der erste E-Mail-Server aus den Empfängerzeilen der eingelieferten E-Mail einen Umschlag (ENVELOPE) erstellt hat. In dem Envelope werden sowohl der Empfänger als auch der BCC-Empfänger gleichberechtigt hinter dem Feld „RCPT TO:“ aufgeführt.

Die eigentliche Nachricht beginnt nun nach dem Wort „DATA“ und enthält nicht mehr den BCC-Empfänger. Die E-Mail-Server leiten Nachrichten nur anhand der Adressierung im Envelope weiter. Die Daten, die der Anwender selbst als Empfänger und Absender sieht, sind für die E-Mail-Server nur Texte in der Nachricht selbst und werden nicht weiter ausgewertet.

Im Posteingang des Benutzers frank@msxfaq.de landet die folgende Nachricht. Der letzte E-Mail-Server hat den ENVELOPE wieder entfernt, und Frank erhält die E-Mail, obwohl seine E-Mailadresse überhaupt nicht in der „TO“-Zeile auftaucht.

Die E-Mail im Posteingang

```
FROM: user1@msxfaq.de
TO: admin@msxfaq.de
SUBJECT: Wichtige Nachricht

Nur für den Administrator!!
```

Nun wird auch klar, wie in Ihrem Postfach Werbenachrichten landen können, obwohl Sie überhaupt nicht in der Empfängerliste auftauchen. Auch wenn das Beispiel recht simpel erscheint, ist das Thema E-Mail doch sehr komplex.

Diese einfachen Nachrichten funktionieren, solange wir uns mit den ersten 127 Zeichen des ASCII-Zeichensatzes begnügen und auf Anlagen verzichten.

Wichtig ist, dass Sie den Unterschied zwischen den Empfängern und Sendern im ENVELOPE und den angegebenen Adressen in der ursprünglichen Nachricht unterscheiden können. Die Angaben im ENVELOPE sehen Sie als Absender und Empfänger nicht, sondern sie werden nur zwischen den E-Mail-Servern übermittelt. Im Postfach landet die E-Mail mit dem HEADER und dem BODY. Dies macht es für POP3-Abholprogramme ohne entsprechende Mitarbeit des Providers extrem schwer, Nachrichten aus einem Sammelpostfach wieder richtig zuzuordnen. Doch dazu später mehr.

5.2.2 MIME, UUENCODE und andere Codierungen

Heutzutage ist es selbstverständlich, in den Nachrichten auch Umlaute und Sonderzeichen zu verwenden, genauso wie Anlagen anzufügen. Spätestens dann holen uns die Folgen der Sparsamkeit früherer Jahrzehnte wieder ein.

Codierungs-methoden

Als Speicherplatz knapp und Bandbreite kostbar, zudem Englisch die einzige Sprache für digitalisierte Daten war, war der ASCII-Zeichensatz ausreichend. Mit der 7-Bit-Codierung wurde ein Zeichen mit Hilfe von sieben Informationseinheiten (Bit) beschrieben.

Der Buchstabe „A“ wurde auf einem PC im ASCII-Zeichensatz mit der Zahl „65 dezimal“, bzw. „1000001 binär“ dargestellt. Nur sind 127 Zeichen nicht mehr ausreichend, wenn die Sonderzeichen der verschiedenen Sprachen oder gar binäre Anlagen mit übertragen werden.

Infolgedessen entstanden Codierungsverfahren, damit diese erweiterten Informationen auch über bestehende E-Mail-Server übertragen werden konnten. Dabei gibt es drei grundsätzliche Verfahren:

- UUENCODE (Unix to Unix Encode)

ASCII-Zeichensatz

Dieses Verfahren konvertiert 8-Bit-Informationsinhalte in 7-Bit-Datenströme, indem es die Bits einfach anders aufteilt. Aus sieben Zeichen mit 8 Bit werden acht Zeichen mit 7 Bit generiert. Aus binären Dateien entstehen somit Textdateien, deren Inhalt nur aus dem originären ASCII-Zeichensatz besteht und problemlos in einer Nachricht übermittelt wird. Erhalten Sie einmal solch eine Datei, speichern Sie diese mit der Endung „UU“ ab. Die meisten Packprogramme wie WinZip, FilZip und andere konvertieren diese Inhalte direkt. Entsprechende Kommando-zeilenprogramme lassen sich im Internet problemlos auffinden.

- BINHEX

  Dieses Verfahren ist überwiegend in der Apple Macintosh-Umgebung bekannt und konvertiert ebenso jede Form von Daten in ASCII-Dateien zur problemlosen Übertragung. Diese Datei führt oft die Endung „.HQX“.

- MIME (Multipurpose Internet Mail Extensions)

  Dieses Format beschreibt die Übertragung von Nachrichten, die nicht nur als ASCII-Zeichen bestehen. MIME unterstützt dabei verschiedene Zeichensatztabellen, so dass die Konvertierung effektiver durchgeführt wird. Zusätzlich werden verschiedene Typen definiert, die bestimmte Inhalte kennzeichnen, z.B. GIF, PostScript etc. Heute werden die meisten Nachrichten als MIME-codierte Inhalte übertragen. Auch Webbrowser und andere Systeme nutzen diese Definition. Später wurde mit S/MIME auch die Unterstützung für verschlüsselte Inhalte ergänzt.

Standardmethode für E-Mail-konvertierung

Natürlich gibt es weit mehr Verfahren zum Konvertieren, und neben ASCII existieren auch EBCDIC UNICODE und andere Zeichensatztabellen. Der Vorteil einer Einigung auf ein bestimmtes Konvertierungsverfahren gestattet den Datenaustausch der unterschiedlichsten Systeme miteinander.

Etwas Aufmerksamkeit verdient die Thematik „Zeichensatz“ bei der Übertragung. Während BINHEX und UUENCODE alle Inhalte als ASCII-Zeichen konvertieren, legt MIME eine bestimmte Zeichensatztabelle als Quelle zugrunde und ist damit effektiver. Da in verschiedenen Sprachen bestimmte Zeichen nicht vorkommen, kann MIME effektiver codieren, wenn die Zeichensatztabelle die möglichen Zeichen vorgibt. Damit reduziert sich die Anzahl der zu codierenden Zeichen. Voraussetzung für die Funktion ist aber für Sender und Empfänger eine übereinstimmende Zeichensatztabelle. Nicht alle E-Mail-Server unterstützen alle Zeichensatztabellen.

Die verwendete Zeichensatztabelle steht in der Nachricht selbst. Hier ein Beispiel einer Quittung:

Eine Quittung mit Codierungen

```
Microsoft Mail Internet Headers Version 2.0
Received: from pc1.msxfaq.local ([192.168.0.9]) by
srv01.msxfaq.local with Microsoft SMTPSVC(5.0.2195.6713);  Wed,
24 Sep 2003 10:01:48 +0200
X-MimeOLE: Produced By Microsoft Exchange V6.0.6487.1
Subject: Gelesen: Testmail
Date: Wed, 24 Sep 2003 10:01:44 +0200
From: Testuser <test@msxfaq.de>
To: "Administrator" <admin@msxfaq.de>

------_=_NextPart_001_01C38272.1832B33F
Content-Type: text/plain;
   charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

------_=_NextPart_001_01C38272.1832B33F
Content-Type: message/disposition-notification
Content-Transfer-Encoding: 7bit

------_=_NextPart_001_01C38272.1832B33F–
```

Hier sehen Sie im Body gut die beiden Bestandteile einer Nachricht: neben den Angaben im Header wird zwischen zwei Zeichensätzen unterschieden. Die Quittung wurde zum einen als Textnachricht (text/plain) mit dem Zeichensatz „ISO-8895-1“ umgesetzt. Der zweite Teil enthält einen Content-Type, den Exchange viel vorteilhafter erkennt. Die eigentlichen codierten Texte wurden der Übersichtlichkeit wegen entfernt.

5.2.3 DNS und MX-Record

Ehe wir nun SMTP genauer untersuchen, stellt sich die Frage nach der Namensauflösung in Verbindung mit SMTP. Ein E-Mail-Server muss zum Versenden einer Nachricht eine Verbindung zum anderen E-Mail-Server herstellen. Zur Auflösung eines Namens zu einer IP-Adresse dient im Internet das Protokoll DNS (Domain Name Service). Jede Domäne ist in der weltweit verteilten DNS-Datenbank auflösbar. Suchen Sie nach einer Domain wie „www.msxfaq.de“, dann fragt Ihr TCP/IP-Stack beim konfigurierten DNS-Server nach einer IP-Adresse, die zu diesem Namen gehört. Hierbei spricht man auch von einem A-Record (A wie Adresse). Für die Suche von E-Mail-Servern wurde ein eigener Typ definiert. Hinter dem Typ „MX“ (MaileXchange) steht der Name und die Adresse des E-Mail-Servers. Prüfen Sie die Umsetzung des MX-Eintrages mit dem Programm NSLOOKUP.

Im folgenden Beispiel hat Frank eine Verbindung über die Telekom (DSL) hergestellt und frage gezielt die E-Mail-Server der Domäne „msxfaq.de“ ab. Nach der Meldung des DNS-Servers wird dazu der Anfragetyp auf „MX“ umgestellt und dann die Domäne eingegeben.

Suche nach dem E-Mail-Server über DNS

```
C:\>nslookup

Standardserver:  www-proxy.BI1.srv.t-online.de
Address:  212.185.248.180

> set q=MX
> msxfaq.de
Server:  www-proxy.BI1.srv.t-online.de
Address:  212.185.248.180

Nicht autorisierte Antwort:
msxfaq.de  MX preference = 10, mail exchanger = mx01.schlund.de
msxfaq.de  MX preference = 10, mail exchanger = mx00.schlund.de

msxfaq.de       nameserver = ns20.schlund.de
msxfaq.de       nameserver = ns19.schlund.de
mx00.schlund.de internet address = 212.227.126.163
mx00.schlund.de internet address = 212.227.126.210
mx01.schlund.de internet address = 212.227.126.146
mx01.schlund.de internet address = 212.227.126.148
```

```
ns19.schlund.de internet address = 195.20.224.101
ns20.schlund.de internet address = 212.227.123.15

> quit
```

Die erhaltenen Angaben zeigen die Antwort des DNS-Servers der Telekom (212.185.248.180), der zwei E-Mail-Server mit Namen kennt. Jedoch weist der DNS-Server darauf hin, dass er eine „nicht autorisierte Antwort“ liefert. Dies bedeutet lediglich, dass der Server die Daten selbst von einem anderen Server erhalten hat und nur stellvertretend weiter reicht (Stand September 2003).

Interessant wird es nun, da hinter den beiden Namen mx01.schlund.de und mx00.schlund.de mehrere IP-Adressen auftauchen. Offensichtlich betreibt der Provider mehrere E-Mail-Server, die alle Nachrichten an „msxfaq.de“ annehmen. Dies erlaubt auch beim Ausfall eines Servers, dass die Nachrichten über andere Server zugestellt werden. Einzig die Positionierung aller Server im gleichen IP-Subnetz ist vielleicht nicht optimal.

Über das Programm NSLOOKUP können Sie ganz einfach die E-Mail-Server der Empfängerdomäne ermitteln. Das gleiche Verfahren führt auch Ihr Exchange-Server durch. Daher ist es notwendig, dass auch der Exchange-Server in Ihrem Unternehmen die Namen und Adressen im Internet per DNS auflösen kann. Es sei denn, Sie setzen einen Smarthost ein.

5.2.4 SMTP

Simple Mail Transfer Protocol

Für die Übertragung von Nachrichten im Internet nutzt Exchange wie jeder andere E-Mail-Server das Protokoll SMTP. Der Anteil der Nachrichten, die noch mittels UUCP (Unix to Unix Copy) übertragen werden, ist mittlerweile so gering, dass nur noch vereinzelte Installationen in sehr bandbreitenarmen Gegenden existieren.

SMTP verstehen

Die Funktionsweise von SMTP möchten wir mit Ihnen anhand eines einfachen Terminalprogramms erschließen, indem wir „E-Mail-Server spielen“.

SMTP nutzt den ASCII-Zeichensatz und das Protokoll TCP/IP. Mit dem Programm HYPERTRM (Bestandteil jeder Windows 2000/XP/2003-Installation) oder dem zeichenbasierten TELNET können Sie die Verbindung zu einem SMTP-Server herstellen. Dabei ist der Port 25 (SMTP) einzutragen (Standardwert für TELNET = Port 23).

Nach der Verbindung meldet sich der E-Mail-Server auf der Gegenseite. Dies kann einige Sekunden dauern, da einige Server versuchen, die IP-Adresse unseres Systems aufzulösen.

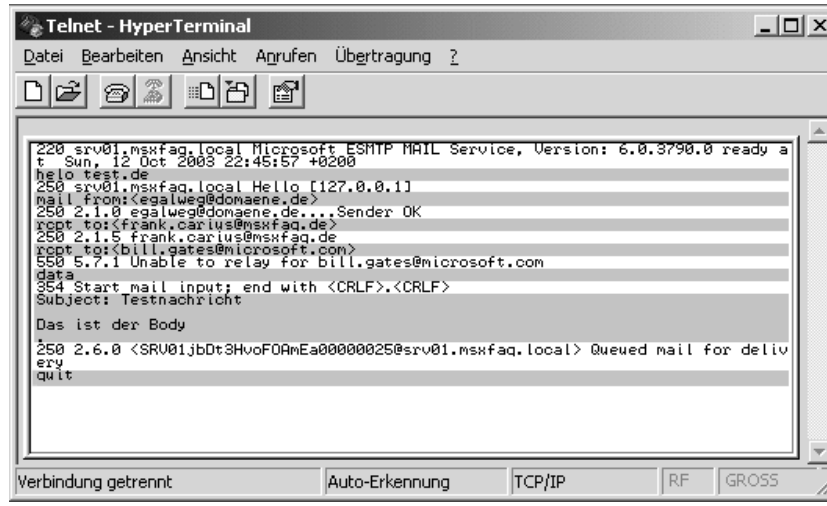


Abbildung 5.1
SMTP mit HyperTerminal

Der in der Abbildung dargestellte Dialog sendet eine Nachricht. Die grauen Zeilen sind die eigenen Eingaben (aktivieren Sie „local Echo“ in HyperTerminal, um diese zu sehen). Die Meldungen des Servers beginnen immer mit einem Nummerncode. Testen Sie das Beispiel mit Ihrer E-Mail-Adresse und Ihrem Server. Kurz darauf sollten Sie in hrem Posteingang eine entsprechende Nachricht vorfinden. Dieser einfache Test zeigt sehr schön, dass SMTP recht unspektakulär ist. Aber es handelt sich auch nur um eine einfache E-Mail.

Einige Jahre nach der ersten Definition von SMTP wurde offensichtlich, dass zusätzliche Funktionen wünschenswert sind. Folglich wurde ein erweiterter Standard (ESMTP) definiert, der zusätzliche Befehle wie die Überprüfung der maximal zulässigen Größe und die Übertragung von größeren Datenmengen ohne gesonderte Quittungen zulässt. Auch Exchange 2003 erweitert den SMTP-Befehlssatz um eigene Funktionen. Dies erkennen Sie, falls statt „HELO <Name des Systems>“ ein „EHLO <Name des Systems>“ übermittelt wird.

Meldet sich ein Server bei der Gegenseite mit EHLO, dann fordert er die SMTP-Erweiterungen an. Das andere System antwortet mit einer Liste der unterstützten Befehle. Anhand der beiden grau eingefärbten Zeilen können Sie z.B. einen Exchange 2003-Server erkennen. Ein Exchange 5.5-Server kennt zumindest noch die Erweiterung XEXCH50.

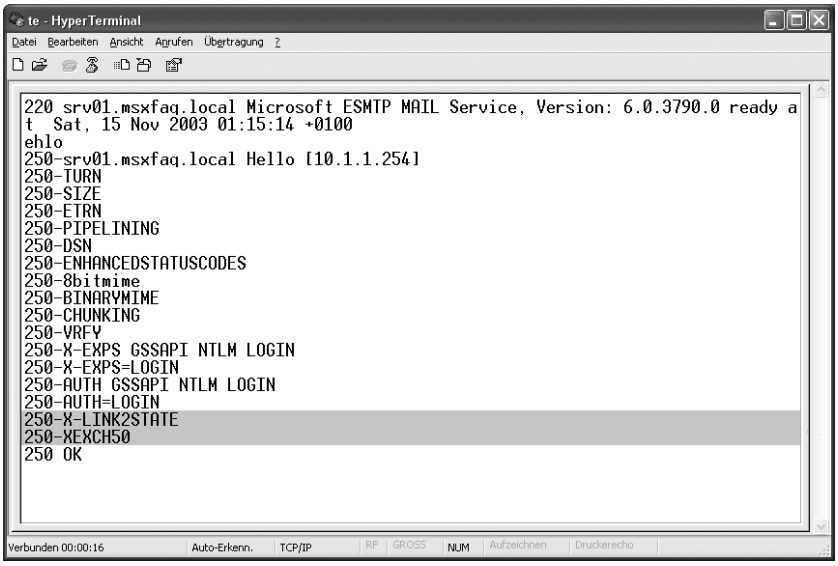


Abbildung 5.2 EHLO-Antwort des Exchange-Servers

Versteht der angesprochene Server hingegen kein ESMTP, wird er das EHLO-Kommando mit einem Fehler beantworten, und der Absender kehrt zum HELO zurück. Viele Firewalls können ebenfalls die SMTP-Befehle lesen, analysieren und gegebenenfalls bestimmte Funktionen blockieren.

Eine wichtige Erweiterung von ESMTP ist unter anderem die Übertragung von 8-Bit-Nachrichten. Auch die Übertragung binärer Informationen als Block ohne Quittierung sowie die Wiederaufnahme von Verbindungen zählen zu den bedeutsamen Neuerungen. Die Exchange 2003-Server in einer Organisation sprechen immer ESMTP miteinander, zumal über zusätzliche Steuerbefehle wie X-LINK2STATE auch die Leitwege bei der Verbindung mit übergeben werden.

SMTP und falsche E-Mail-Adressen

Ein großes Problem der Übertragung per SMTP ist die mangelnde Autorisierung und Überprüfung der Server. Zwar gibt es entsprechende Protokolle und Definitionen, wie sich ein E-Mail-Server ausweisen kann, aber mangels breiter Akzeptanz bedeutet der Einsatz von SMTP die Nutzung des kleinsten gemeinsamen Nenners. Dies bedeutet, dass weder der Absender in der E-Mail noch der versendende Server verifiziert sind. Ein Vergleich zu einer Postkarte verdeutlicht diese Situation.

Betrügerischer E-Mail-Versand

Niemand hindert Sie daran, eine Postkarte zu verfassen und an den Bürgermeister Ihrer Stadt zu senden und dabei bewusst Ihren unliebsamen Nachbarn als Absender einzutragen. Einige böse Worte machen die Sache brisanter. Der Empfänger sieht maximal den Poststempel auf der Briefmarke als einzige Möglichkeit, die Authentizität des Briefs zu prüfen. Der

vorgebliche Absender weiß hingegen nicht einmal etwas von seinem Glück. Besonders perfide wird dieser Vorgang, wenn Sie die Briefmarke einsparen und „Gebühr bezahlt Empfänger“ darauf schreiben. Nun wird sich der Empfänger doppelt ärgern. Nimmt er den Brief aber nicht an, dann hat der angebliche Absender den Ärger mit dem Postboten, der die Nachgebühr einfordern will. Diese Variante nutzen leider auch immer mehr Viren und Spam-Versender, um die Spuren zu verschleiern.

SMTP und Verschlüsselung

Neben der mangelnden Prüfung des Absenders werden alle Nachrichten als Klartext übertragen. Jeder, der Zugriff auf den Übertragungsweg hat, kann die Nachrichten mitlesen wie eine Postkarte. Die einzige Abhilfe bedeutet die Verschlüsselung der Übertragung. Hierzu gibt es mehrere Ansätze:

- Verschlüsselung der E-Mail

Mail Encryption

Durch den Einsatz von S/MIME, PGP oder auch durch einfaches Einpacken von Anlagen mit Kennwortschutz können Teile oder die gesamte E-Mail verschlüsselt werden. Dies ist aber für den Anwender ein sehr unangenehmer Prozess, da er entweder das Kennwort anderweitig dem Empfänger auf sicherem Wege mitteilen oder erst öffentliche Schlüssel mit dem Kommunikationspartner austauschen muss. Trotzdem ist dies der schnellste und aktuell praktikabelste Weg.

- Verschlüsselung der SMTP-Verbindung

SSL

Die zweite Möglichkeit bietet die Verschlüsselung von SMTP-Verbindungen mittels SSL. Ähnlich einem Webbrowser benötigen die SMTP-Server ein Zertifikat und die Anweisung, dass Sie die Verbindung verschlüsselt aufbauen. Dieses Verfahren würde auch das Problem der falschen Absender eingrenzen. Leider nutzen nur sehr wenige Unternehmen diese Variante. Primär findet dies für gezielt eingesetzte Verbindungen zu anderen Unternehmen und Partnern statt, aber nicht im freien E-Mail-Verkehr. Da die Verschlüsselung aber immer nur direkt zwischen den beiden Systemen erfolgt, ist beim Einsatz eines Relay auch dort die Verschlüsselung zu beiden Seiten zu konfigurieren.

- Verschlüsselung der TCP/IP-Verbindung

IPSec & VPN

Eine dritte Möglichkeit ist die Verschlüsselung auf der Ebene des TCP/IP-Protokolls. IPSec und VPN sind die Schlagwörter, um den Datenverkehr zwischen zwei Systemen zu verschlüsseln. Diese Methode wird oft genutzt, falls das Internet zwei interne Netzwerke verbindet. Der Einsatz im freien E-Mail-Austausch ist jedoch derzeit nicht praktikabel.

Exchange 2003 und Windows 2003 unterstützen alle drei Varianten. Windows 2003 verschlüsselt über IPSec oder die Einrichtung eines VPNs direkt den kompletten Datenstrom. Alternativ kann Exchange 2003 über TLS

(Transport Layer Security) mit einem SSL-Zertifikat verschlüsselte Verbindungen annehmen. Mit Exchange 2003 entfällt der Zertifikatsdienst der vorangegangenen Exchange-Versionen. Diese Funktion füllt nun die Windows 2003-CA komplett aus. So können auch Zertifikate für Outlook-Anwender erstellt werden.

Seit einiger Zeit gewähren spezielle Systeme eine Relay-Funktion. Ein Server wird in den Übertragungsweg eingefügt und regelt die Verschlüsselung, Signierung und Decodierung der Nachrichten zentral. Dazu muss freilich der private Schlüssel des Anwenders für diesen Server zugänglich sein. Mit dieser Handhabung erleichtern Sie dem Anwender den Umgang mit zu schützenden Daten (Konfiguration statt Kennwort) und geben ihm die Gewissheit, dass die Nachricht vom Empfänger stammt.

SMTP-Autorisierung

Bedingt durch die einfache Übermittlung der Nachrichten von einem x-beliebigen E-Mail-Server ist es verständlich, warum so viele Viren im Umlauf sind, die direkt per SMTP eine Nachricht senden.

Gegenwärtig ist es undenkbar, den Empfang von Nachrichten aus dem Internet über eine Anmeldung zu regeln. Der Versuch, anonyme Sender zu blockieren, bewirkt, dass Ihr E-Mail-System nicht mehr in der Lage ist, überhaupt Nachrichten aus dem Internet anzunehmen. Aber auch im internen Transfer kommt immer wieder SMTP zum Einsatz.

Grundsatz der Autorisierung

Exchange 2003 virtuellen SMTP-Server nehmen in der Standardkonfiguration alle Nachrichten an, aber verhindern die Weiterleitung an andere Systeme außerhalb der Exchange-Organisation. Gerade bei POP3/SMTP-Anwendern ist die Autorisierung eine Grundvoraussetzung, um Nachrichten per SMTP an den Exchange-Server zu übermitteln, der diese dann an den Empfänger weiterleitet.

Dieses Verfahren der SMTP-Autorisierung nutzen immer mehr E-Mail-Provider, die nicht über ein eigenes Netzwerk verfügen. Somit können Ihre Kunden, die über einen anderen ISP den Zugang zum Internet erhalten, nach der Anmeldung an dem E-Mail-Server Ihre Nachrichten versenden.

Verhindern Sie unbedingt, dass Ihr Server nicht als Relay für fremde Personen missbraucht werden kann, indem Sie das Weiterleiten der Nachrichten von nicht autorisierten Systemen ablehnen. Stellen Sie außerdem die Annahme der Nachrichten sicher, deren Empfänger in Ihrer Exchange-Organisation existieren. Aber prüfen Sie, ob Sie wirklich Nachrichten per SMTP aus dem Internet annehmen sollten, deren Absender vorgibt, ein interner Anwender zu sein. Normale Anwender können dies nicht unterscheiden.

5.2.5 Smarthost und Relay

Rückblickend ist Ihnen nun bekannt, dass die Namensauflösung der Empfängerdomäne per DNS erfolgt und der E-Mail-Server die Nachricht direkt an diesen Server sendet.

Dies ist in der Regel der direkte und schnellste Weg. Allerdings gibt es auch Einschränkungen, wenn Sie direkt die Nachrichten versenden, statt den *Smarthost* Ihres Providers zu nutzen. Wichtige Aspekte sind dabei:

Versand über Provider

- Versand von dynamischer Adresse wird blockiert

  Nicht jeder E-Mail-Server im Internet akzeptiert eine Verbindung von jedem anderen System. Gerade durch die Zunahme an Spam-Nachrichten wehren sich immer mehr Unternehmen mittels der Servereinstellung, keine Nachrichten von Systemen aus dynamischen Nummernkreisen anzunehmen.

  Diese haben sich sehr häufig als Spam-Versender erwiesen.

- Fehlender DNS-Eintrag

  Aus dem gleichen Grund lehnen einige E-Mail-Systeme eingehende Verbindungen ab, wenn die Adresse des Absenders nicht im DNS-System auflösbar ist. Dies ist in der Regel ein Zeichen für ein zweifelhaftes und schlecht gepflegtes System, als Nebeneffekt reduziert es unerwünschte Nachrichten. Der Smarthost eines Providers ist meist im DNS gepflegt.

- Mehrfachversand

  Gewiss versenden Sie auch eine Nachricht an mehrere Empfänger im Internet. Häufig sind das Marketing oder der Versand eines Newsletter die Quelle für solche Mehrfachversendungen bzw. Massenmailaktionen. Ohne Smarthost wird der E-Mail-Server die Nachrichten direkt an die verschiedenen Empfänger zustellen. Beim Einsatz eines Smarthost wird die Sammelnachricht nur einmal zum Smarthost übermittelt, und der Smarthost des Providers verteilt die E-Mail an die einzelnen Empfängersysteme. Dies entlastet Ihren E-Mail-Server.

- Instabile Verbindungen, langsame Übertragung

  Beim direkten Versand zum E-Mail-Server des Empfängers muss eine durchgängige Verbindung bestehen. Maßgeblich für die Geschwindigkeit ist aber die langsamste Teilstrecke. So kann es vorkommen, dass Sie selbst eine 64 KB-ISDN-Leitung nutzen, aber die Nachricht unterwegs einen Engpass passieren muss und mit wesentlich geringerer Geschwindigkeit übertragen wird. Das Ergebnis sind eine nur teilweise ausgelastete Leitung sowie höhere Kosten, wenn Ihre Leitung pro Zeiteinheit berechnet wird. Ärgerlich ist dann noch ein Verbindungsabbruch, weil die Gegenseite stockt oder die Verbindung abbricht. Der Server beginnt die Übertragung von vorne so lange, bis die

Nachricht zugestellt wurde oder der Server die E-Mail als unzustellbar erklärt.

Die Eintragung eines Smarthost beim Provider umgeht die oben genannten Probleme. Ihr Server sendet alle Nachrichten an das System des Providers, und dieser leitet die Nachrichten weiter. Nachteilig ist allenfalls, dass bei Problemen mit ausgehenden Nachrichten dies keine direkte Fehlersuche in den Warteschlangen des eigenen Exchange-Servers erlaubt, sondern die Nachrichten dann beim Provider zur Übermittlung anstehen.

Aus technischer Sicht kann jedes System mit einer gültigen IP-Adresse SMTP-Mails versenden, sofern das Empfängersystem erreichbar ist. Dabei ist es egal, ob die Adresse dynamisch oder statisch zugewiesen ist oder eine Firewall die Adresse umsetzt (Stichwort NAT).

Begriffe Relay und Smarthost

Die Begriffe des Relay und des Smarthost werden immer wieder vermischt und bedeuten in weiten Bereichen das Gleiche.

- Relay

  Ein Relay ist ein E-Mail-Server, der bestimmte Nachrichten annimmt und weiterleitet. Die Richtung ist dabei ebenso wenig festgeschrieben wie Einschränkungen der Domänen, IP-Adressen oder der Weg, wie andere Systeme diesen Server erreichen.

- Smarthost

  Der Begriff Smarthost steht für die Konfigurationseinstellung des E-Mail-Systems, durch die Exchange alle Nachrichten an ein Relay weiterleitet. Ein E-Mail-Server, der einen Smarthost nutzt, löst nicht selbst die Domänen des Empfängers per DNS auf.

Kontrolliertes „Relaying“

Relays sind ein wichtiger Baustein für die Zuverlässigkeit des E-Mail-Verkehrs im Internet. In den Anfangszeiten des Internets waren sehr viele Server bereit, Nachrichten anzunehmen und weiterzuleiten. Gerade bei sehr instabilen oder nur zeitweise verfügbaren Leitungen war dies ein Weg, eine Nachricht von Station zu Station näher an das Ziel zu bringen. Heute wird diese Freundlichkeit durch böswilligen Missbrauch bestraft. Viele unseriöse Absender missbrauchen ein offenes Relay zum massenhaften Versand unerwünschter Nachrichten auf fremde Kosten. Daher sind offene Relays heute eher ein Ärgernis und Zeichen einer falschen Konfiguration. Mittlerweile gibt es viele Datenbanken, in denen offene Relays gelistet werden, damit E-Mail-Server die Annahme verweigern.

Das einzige Relay, das von jedem System Nachrichten für Ihre Domäne annehmen sollte, ist Ihr E-Mail-Server selbst oder der Backup-Server Ihres Providers. Diese Backup-Server nehmen aber nur Nachrichten der Domänen

an, für die sie auch zuständig sind. Damit sind diese Server auch keine offenen Relay-Systeme.

Der richtige Smarthost

Welcher Smarthost?

Der Zugang zum Internet trennt sich in zwei verschiedene Zuständigkeiten:

- Zugangsprovider

  Dieses Unternehmen stellt Ihnen den Zugang zum Internet bereit. Sie erhalten eine IP-Adresse aus dem Bereich des Providers und bezahlen für die Nutzung der Leitung und der Datenübertragung. In Deutschland dürften die meisten kleineren Firmen hier mit der Telekom und einem DSL-Anschluss arbeiten.

- Domain-Provider

  Die zweite Firma bedient Ihre Internetdomäne und die entsprechenden E-Mail-Adressen. Dieser Provider betreibt in der Regel auch den DNS-Server und nimmt Nachrichten für Ihr System an. Bekannte Namen sind z.B. 1&1 Puretec und Strato.

Im Fall der Webseite „http://www.msxfaq.de“ baue ich selbst die Verbindung zum Internet über T-Online-DSL auf, um Nachrichten zu senden oder zu empfangen. Die Domäne selbst wird aber bei „1&1 Puretec“ gehostet.

In der Regel bieten beide Provider einen E-Mail-Server, an den Frank seine Nachrichten liefern kann. So kann er entscheiden, ob er in seinem Fall den E-Mail-Server von T-Online verwende, der Frank anhand der IP-Adresse als vertrauenswürdigen Absender einstuft, oder den E-Mail-Server von 1&1, bei welchem Frank sich zuvor mit Benutzername und Kennwort autorisieren muss. Sinnvoll ist die Nutzung eines Smarthost, der aus Netzwerksicht in der Nähe liegt, damit die Bandbreite optimal genutzt wird und möglichst wenige Stationen dazwischen liegen.

Allerdings gibt es Provider, wie T-Online, die bei der Weiterleitung die Absenderadresse verändern und dadurch zwar die Fälschung der Adressen von Privatanwendern erschweren, aber die Nutzung für Unternehmen uninteressant machen. Auf der anderen Seite wird ein kostenpflichtiges Relay angeboten, das genau diese Beschränkung nicht aufweist.

Prüfen Sie daher, welches Relay sich als Smarthost in Ihrer Umgebung eignet. Dabei sollten Sie zwar die Kosten mit beachten, wichtiger ist aber die Erreichbarkeit und die Stabilität der Lösung. Kann Exchange einen Smarthost nicht erreichen, dann bemerken Sie dies erst nach Stunden oder Tagen, da Exchange die Nachrichten zwischenspeichert und immer wieder eine Verbindung versucht und Sie nach längerer Zeit erst per E-Mail informiert, dass die Nachrichten nicht versendet werden können.

Smarthost und Firewall

Kein direkter Zugriff auf Exchange

Oftmals wird aus Sicherheitsaspekten im Netzwerk ein Smarthost eingesetzt. Immer dann, wenn eine direkte Verbindung von Exchange zum Internet oder zum Smarthost des Providers nicht möglich oder nicht erwünscht ist, setzen Unternehmen ein System zwischen Internet und Exchange. Dieses überbrückt alle eingehenden und ausgehenden Verbindungen. Damit ist der Exchange-Server nie direkt erreichbar, und bei einem Angriff kann das dazwischen geschaltete System einfach abgeschaltet oder entsprechend angepasst werden. Solch ein Relay eignet sich sehr gut auch als Virenscan oder Spam-Filter.

Smarthost bei Einzelanwendern

Übrigens nutzen Sie als Privatanwender auch den Smarthost Ihres E-Mail-Providers, nur wird er dort anders benannt.

Bei der Einrichtung Ihres POP3-Postfachs als Privatperson tragen Sie in Ihrem E-Mail-Programm auch einen SMTP-Server ein, der Ihre ausgehenden Nachrichten versendet. Das Mailprogramm (User-Agent) selbst stellt keine DNS-Anfragen und verfügt nicht über ausgeklügelte Warteschlangen, daher überlässt es diese Aufgabe dem SMTP-Server.

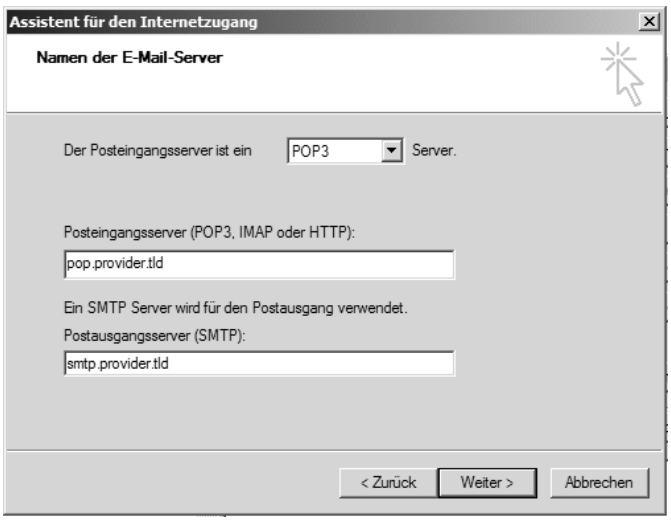


Abbildung 5.3 Outlook Express-Smarthost = Postausgangsserver

5.2.6 Dynamisches DNS

Ein großer Nachteil von SMTP ist der Verbindungsaufbau durch den Absender. Der Absender muss dazu über DNS die IP-Adresse des Empfängerservers erhalten, um die Verbindung aufzubauen. Ohne besondere Vorkehrungen bedeutet dies, dass der Empfänger eine statische IP-Adresse benötigt und empfangsbereit sein muss. Ein Abholen von Nachrichten über SMTP ist nicht definiert und nicht möglich.

Viele der in Deutschland verfügbaren DSL-Anschlüsse, mit einer Abrechnung nach Volumen oder pauschal, wechseln jedoch mindestens alle 24 Stunden die IP-Adresse, dazu gehört auch T-DSL der Telekom. Unter diesen Umständen scheidet ein statischer Eintrag im DNS auf die dynamische Adresse als Anbindung aus.

In dieser Situation kommen Dienste wie dns2go, dyndns und andere zum Einsatz. Diese Dienstleister betreiben Ihre Domäne und erlauben Ihnen, dynamisch die Einträge im DNS zu verändern. Hierbei gibt es zwei Modelle:

- Änderung des A-Records einer anderen Zone

  Ihr Provider betreibt die Zone Ihrer Domäne. Diese Informationen sind statisch und werden nicht geändert. Der MX-Eintrag in dieser Zone verweist auf einen Rechnernamen. Dieser Name muss nichts mit Ihrer Domäne zu tun haben. Die meisten dynamischen DNS-Provider bieten an, einen Namen wie „firmenname.dyndnsprovider.tld“ zu nutzen und die dort hinterlegte Adresse automatisch zu ändern. Ein E-Mail-Server wird nun über den MX-Eintrag Ihrer Domäne die Information erhalten, dass sich der Mail-Server hinter dem Namen „firmenname.dyndnsprovider.tld“ verbirgt. Der Name wird zu einer IP-Adresse aufgelöst und die Verbindung hergestellt.

- Direkte Zonenveränderung

  Eine andere Möglichkeit ist die direkte Aktualisierung der Einträge in der DNS-Zone selbst. So kann der MX-Eintrag zum Beispiel auf den Rechner „smtp.firma.de“ verweisen, und der Aktualisierungsprozess pflegt direkt die IP-Adresse in diese Zone ein.

DDNS

Dynamische DNS-Aktualisierung im Internet ist ein gängiges Verfahren, einen Rechner mit Namen zu erreichen, selbst wenn sich die IP-Adresse regelmäßig ändert.

Das Risiko dieser Anbindung ist die Gültigkeit des Namens im Internet auch noch nach dem Verbindungsabbruch. Viele DNS- und E-Mail-Server pflegen einen Cache mit den letzten Kommunikationspartnern, um die DNS-Abfragen zu minimieren. Schlimmstenfalls bedeutet es nach einem Wechsel der IP-Adresse, dass eingehenden Nachrichten noch eine Zeit lang an die alte Adresse gesendet werden und damit nicht bei Ihnen eingehen. Empfängt hinter der alten Adresse mittlerweile der E-Mail-Server einer anderen Firma Nachrichten, wird dieser die E-Mails bekommen und einfach verwerfen.

Eine Unterbrechung der Leitung sollte immer in Betracht gezogen werden. In diesem Fall ist die Relay-Eintragung beim Provider sinnvoll, damit die Nachrichten nicht beim Absender in der Warteschlange verbleiben, sondern beim Provider zwischengespeichert werden.

Selbst mit einer dynamischen IP-Adresse ist in Verbindung mit dem dynamischen DNS die gesamte Bandbreite der Internetfunktionalität nutzbar.

So können ein Outlook Web Access oder Outlook Mobile Access, WAP und VPN-Verbindungen genutzt werden. Sofern Sie eine Internetverbindung mit volumenbasierter oder pauschaler Abrechnung nutzen, ist die Anbindung per dynamischen DNS-Einträgem eine praktikable Lösung. Es gibt jedoch auch DSL-Anschlüsse mit festen IP-Adressen. Allein der Begriff DSL sagt nur etwas über die Übertragungstechnik aus, aber nicht über die logische Verbindung mit TCP/IP.

5.2.7 SMTP anstoßen

Abholen der SMTP-Mails

Nicht immer ist ein geeigneter Anschluss verfügbar, der nach Volumen abgerechnet wird, und oftmals sind Zeit und Bandbreite sehr teuer. Auch für diese Umgebungen gibt es Ansätze, um ohne feste IP-Adresse sowie ohne Standleitung die Nachrichten per SMTP an den Exchange-Server zu übermitteln.

Die nachfolgenden Verfahren informieren den E-Mail-Server des Providers darüber, dass Ihr Server empfangsbereit ist. Der Provider-Server sendet dann die zwischengespeicherten Nachrichten per SMTP direkt an Ihren Server.

- TURN/ETRN

  Diese auch von Exchange unterstützte Erweiterung signalisiert dem E-Mail-Server des Providers, dass Ihr Exchange-Server gerade online ist und der Provider die Nachrichten senden kann. Da hierbei keine Autorisierung oder sonstige Überprüfung stattfindet, sendet der E-Mail-Server die Daten immer nur an eine hinterlegte IP-Adresse. Damit eignet sich diese Methode eher für Wählverbindungen mit fest zugewiesenen IP-Adressen, aber nicht für dynamische Adressen.

- ATRN

  Diese Erweiterung des TURN-Befehls erlaubt eine Authentifizierung. Damit kann sich der auslösende E-Mail-Server mit Benutzernamen und Kennwort authentifizieren. Der Provider übermittelt dann die Nachrichten an die IP-Adresse, welche die ATRN-Anfrage gestellt hat. Exchange unterstützt ATRN nicht. Alternativ können Sie aber Drittprodukte mit dem Zeitplandienst einsetzen, die dieses Kommando absetzen.

- FINGER und andere

  Neben SMTP gibt es im Internet weitere Protokolle, die eine Verbindung vom Client zum Server aufbauen und sich dabei autorisieren. Viele Provider bauen auf solchen Programme auf, die eine Zustellung auf dem E-Mail-Server starten. Die Funktion ist vergleichbar zu ATRN, nur dass der Auslöser nicht über Port 25/TCP erfolgt. Exchange 2003 unterstützt auch diese Möglichkeit nicht direkt. Sie können mittels Drittprodukten und dem Zeitplandienst die Aktionen auslösen.

- UUCP

  Dieses recht antike Verfahren wurde früher genutzt, um Nachrichten ähnlich einem COPY-Befehl über langsame Verbindungen zu kopieren. Dabei wurden die Daten aus der Warteschlange eines E-Mail-Servers zum anderen E-Mail-Server verschoben. Heute hat das Verfahren kaum noch Bedeutung und wird von Exchange auch nicht unterstützt.

- Radius

  Einige Provider entwickelten eigene Lösungen, um Nachrichten zu senden. Wann immer Ihr Netzwerk mit dem Internet verbunden wird, muss sich der Router oder Server beim Provider autorisieren. Der Provider prüft die Daten über einen RADIUS-Server. Dieser Server erkennt die aktuelle IP-Adresse und die korrekte Anmeldung. Mit dieser Information wird der E-Mail-Server des Providers angestoßen, die wartenden Nachrichten zu senden.

Diese Verfahren zeigen nur einige Beispiele auf, die heute von Providern für die Übermittlung der wartenden SMTP-Nachrichten eingesetzt werden. Unabhängig von der wechselnden IP-Adresse und zeitweisen Erreichbarkeit kommen die Nachrichten richtig an. Sprechen Sie mit Ihrem Provider, welche Anbindung er für Ihren Exchange-Server empfiehlt. Er sollte Ihnen anhand bestehender Kunden eine Lösung unterbreiten können.

5.2.8 POP3-Sammeldienste

Post Office Protocol

Sehr viele Provider bieten Ihnen als Alternative ein POP3-Sammelkonto an, in dem alle Nachrichten für Ihre Mitarbeiter abgelegt werden. POP (Post Office Protocol, seit 1984) gestattet das Abrufen von E-Mails von Servern, auch wenn keine dauerhafte Verbindung zum E-Mail-Server besteht. Es gilt in Zusammenhang mit SMTP zum Senden von Nachrichten als Standardprotokoll für die meisten E-Mail-Programme im Internet.

POP3 ist somit ein Protokoll zum Abholen von Nachrichten eines einzelnen Postfachs und ist nicht zur Kommunikation zwischen E-Mail-Servern vorgesehen. Über POP3 können abgeholte Nachrichten auf dem Server gelöscht werden. Alle weiteren Funktionalitäten wie hierarchische Postfächer oder Filter können dagegen nur vom Client umgesetzt werden.

Um Kosten für echte SMTP-Verbindungen zu sparen, bieten Provider die Option an, dass alle Nachrichten für Ihre Domäne in einem POP3-Postfach abgelegt werden. Sie können diese Nachrichten dann mittels POP3 abholen.

Die Verwendung von POP3 als Übertragungsprotokoll ist realisierbar, wenn sowohl Provider als auch Ihre Übertragungssoftware zusammenspielen. Was beim POP-Client problemlos funktioniert, ist auf Serverebene nicht selbstverständlich. Mangels eines einheitlichen Standards gibt es keine

100 %ige Sicherheit, ob Ihr Provider mit der Konfiguration des Übermittlungsprogramms harmoniert und gleichfalls das Abholen Ihres POP3-Sammelkontos zulässt.

Die Kommunikation zwischen Ihrem Exchange-2003 Server und dem POP3-Sammelkonto erfolgt über spezielle Software von Drittanbietern, welche die Nachrichten per POP3 abholen und an den Exchange-Server mittels SMTP senden. Für den Exchange-Server ist kein Unterschied erkennbar dadurch, dass die Nachrichten nicht direkt aus dem Internet kommen.

Warum POP3?

Verbindungskosten in Deutschland

Der vermehrte Einsatz von POP3 in bestimmten Szenarien ist teilweise in einer Besonderheit des deutschen Gebührenmodells bei Telefonverbindungen zu suchen.

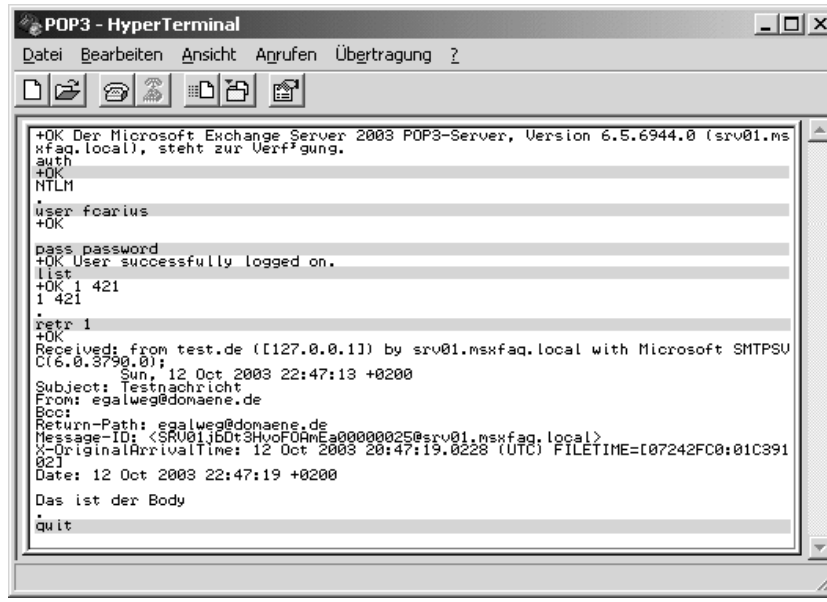
Für den Empfang von Nachrichten per SMTP muss Ihr E-Mail-Server aus dem Internet direkt erreichbar sein. Eine SMTP-Verbindung kann nie von dem Server aufgebaut werden, der die Nachrichten empfangen soll. Eine permanente Verbindung mit Hilfe einer Internet-Standleitung ist in Deutschland relativ teuer. Wählleitungen werden allerdings meist nach einem Zeittakt abgerechnet und sind damit als permanente Verbindung zu kostspielig. Demzufolge wird nach günstigen Lösungen gesucht, um die eingehenden Nachrichten beim Provider zwischenzuspeichern und diese zu bestimmten Zeiten abzuholen.

Wie funktioniert POP3?

Da es auch mit Exchange 2003 weiterhin Internet-Anbindungen mit POP3-Sammelkonten gibt und der E-Mail-Server selbst obendrein als POP3-Server fungiert, sollten Sie ein grundlegendes Verständnis des POP3-Protokolls besitzen. Ausgehend von der Frage, wie eine E-Mail per POP3 auf einen Einzelplatz-PC übertragen wird, können Sie Exchange mit POP3-Sammelkonten an Ihren Provider anbinden und Fehlersuche durchführen.

Ähnlich der Beschreibung zum Protokoll SMTP ist es gleichermaßen einfach, POP3 von Hand zu steuern. Die Verbindung zum POP3-Server wird erneut über Hyperterm oder ein anderes Terminal-Programm hergestellt. Diesmal ist der Port 110/TCP.

Abbildung 5.4 POP3-Nachricht lesen



Wird statt einer IP-Adresse der Rechnername verwendet, muss natürlich wie bei SMTP zuerst die Namensauflösung funktionieren.

POP3-Verbindung

Der POP3-Server meldet sich, und der erste Schritt ist die Authentifizierung am Server. Mittels der Eingabe eines Benutzers und eines Kennworts melden Sie sich am Server an. Sollte Ihr Exchange-Alias unterschiedlich zum Windows-Benutzerkonto sein, müssen Sie die Schreibweise „`ALIAS\DOMÄNE\USERNAME`“ bei der Anmeldung verwenden, damit Exchange den Benutzer zuordnen kann.

Nach der erfolgreichen Anmeldung zeigt der Server die Anzahl und Größe der Nachrichten an. Im Beispiel ist eine Nachricht mit 421 Byte im Postfach vorhanden. Mit dem Befehl „RETR 1“ wird die Nachricht 1 übertragen. Ihr E-Mailprogramm oder der POP3-Sammeldienst speichert die nun folgende Ausgabe in eine Datei oder einer Datenbank zur weiteren Verarbeitung. Mit dem Befehl „DELE 1“ wird diese Nachricht gelöscht. Mit „QUIT“ wird die Verbindung ordnungsgemäß beendet.

Sie können diesen Test mit Ihrem Exchange 2003-Server oder dem POP3-Server Ihres E-Mail-Providers fortwährend wiederholen. Solange Sie die Nachrichten nicht mit dem Befehl „DELE“ löschen, gehen keine Daten verloren.

POP3-Sammler und Exchange

Sammeldienst

Die Funktion des POP3-Sammeldienstes beruht darauf, nach einem bestimmten Zeitplan ein Sammelpostfach abzurufen und die Nachrichten an den Exchange-Server zu übermitteln. Der Versand an Exchange erfolgt per

SMTP. Der Exchange-Server erkennt keinen Unterschied zwischen den Nachrichten direkt aus dem Internet, von einem angeblichen E-Mail-Server im eigenen Netzwerk oder sogar auf dem gleichen System.

Das Problem einer POP3-Sammelsoftware ist nun, dass in der abgerufenen E-Mail nur der HEADER und der BODY vorhanden ist, aber nicht mehr die Informationen aus dem ENVELOPE vorliegen. Der POP3-Sammeldienst muss aber für die Weiterleitung an Exchange eben diese Information wieder aus den erhaltenen Daten regenerieren. Dies kann nur dann funktionieren, wenn der Provider und das Sammelprogramm sich auf ein Verfahren einigen. Einige Provider übermitteln die Zusatzinformationen aus dem ENVELOPE in besonderen Feldern des Headers. Ihr POP3-Sammelprogramm kann dann diese Felder auswerten. Es muss diese Daten aber aus der Originalnachricht löschen, da ansonsten die Empfänger auch die BCC-Empfänger erkennen können.

Eine Empfehlung für ein Produkt kann es aber aufgrund der Vielzahl der Provider und deren Feinheiten nicht geben. Die meisten Produkte lassen sich vorab testen, und die Hersteller bieten in der Regel eine passende Beschreibung der Installation, die auch auf Ihren Provider zutrifft. Eine Zusammenstellung von verbreiteten Produkten finden Sie auf:

http://www.msexchangefaq.de/internet/pop3smtp.htm.

Damit der Abruf regelmäßig funktioniert, nutzen viele POP3-Sammler den Zeitplandienst von Windows oder bringen einen eigenen Zeitplaner mit. Die Verbindung erfolgt entweder über das Windows-eigene DFÜ-Netzwerk oder einen Router.

Zur Erinnerung: Der POP3-Sammler ist jedoch nur für eingehende Nachrichten zuständig. Für den Versand in das Internet bleibt Exchange verantwortlich. Einige POP3-Sammler dienen aber zugleich auch als SMTP-Relay, so dass Exchange die ausgehenden Nachrichten nicht direkt in das Internet, sondern an diesen besonderen Smarthost sendet. Damit kann solch ein Programm auch Wählverbindungen managen. Zusatzfunktionen wie Spam-Filter oder Virenscanner lassen sich ebenfalls in vielen POP3-Sammeldiensten einbinden.

Folgende Probleme können beim Abruf über ein POP3-Sammelkonto auftreten.

POP3 — Unstimmigkeiten mit Quittungen

Beim Versand einer Nachricht fordert der Sender bei Bedarf eine Quittung für die Zustellung und beim Lesen ein. Während die „Gelesen"-Quittung durch das E-Mail-Programm auf Ihrem Arbeitsplatz erzeugt und gesendet wird, quittiert der E-Mail-Server die „Zugestellt"-Quittung in dem Moment, in dem die Nachricht in das Postfach abgelegt wird. Bei Nutzung eines

Sammelpostfachs kann dies dazu führen, dass die „Zugestellt“-Quittungen schon bei der Zustellung in dieses Sammelpostfach gesendet oder sogar doppelt erzeugt werden.

Bestätigung an Absender

Im ersten Fall hat der eigentliche Empfänger die Nachricht noch gar nicht erhalten, sondern bekommt diese erst, nachdem der POP3-Sammler die Nachricht abgeholt und in das Exchange-Postfach zugestellt hat. Dies führt zu Verwirrungen, wenn z.B. ein Kunde nach Eingang der Quittung telefonisch nachhakt, Ihre Anwender jedoch noch keine Nachricht finden können. Der zweite Fall tritt häufig auf, wenn auch der Exchange-Server die „Zugestellt“-Quittung erzeugt. Der Absender erhält zwei Quittungen.

Ein weiteres Problem im Hinblick auf Quittungen tritt auf, wenn Sie selbst eine Nachricht mit Einschreiben versenden. Die Quittungsnachricht hat nicht unbedingt einen Absender; dieses Feld ist oftmals leer. Ihr POP3-Sammler bekommt diese Nachricht und muss zum Versand per SMTP eine Absenderadresse erzeugen. Dies trifft umso mehr für „Unzustellbar“-Quittungen (NDR) zu, die ohne entsprechende Berücksichtigung zu einer Endlosschleife führen können.

POP3 — Probleme mit BCC

Als Blindkopien werden Empfänger einer Nachricht bezeichnet, die eine Kopie der Nachricht erhalten, aber für die anderen Personen nicht als Empfänger sichtbar sind. Sie stehen nicht im Adressfeld der Nachricht. Nur die E-Mail-Server kennen die eigentlichen Empfänger während der Übertragung. Ein E-Mail-Server sendet folgende Befehle an einen zweiten E-Mail-Server:

Testmail mit Blindkopien

```
MAIL FROM: USER1@FIRMA1.DE
RCPT TO: USER2@FIRMA2.DE
RCPT TO: USER3@FIRMA3.DE
RCPT TO: BCCUSER@FIRMA2.DE
DATA
TO: USER2@FIRMA2.DE
CC: USER3@FIRMA3.DE
Subject: Dies ist der Betreff

und dies der Body
.
```

Diese Nachricht besteht aus dem Umschlag (ENVELOPE), in dem alle drei Empfänger enthalten sind, und dem HEADER, der nur die zwei „sichtbaren“ Empfänger aufführt. Ohne Anpassungen wird der E-Mail-Server des Providers den ENVELOPE entfernen und die einfache Nachricht in das Sammelpostfach ablegen.

Die Nachricht stellt sich in Outlook wie folgt dar.

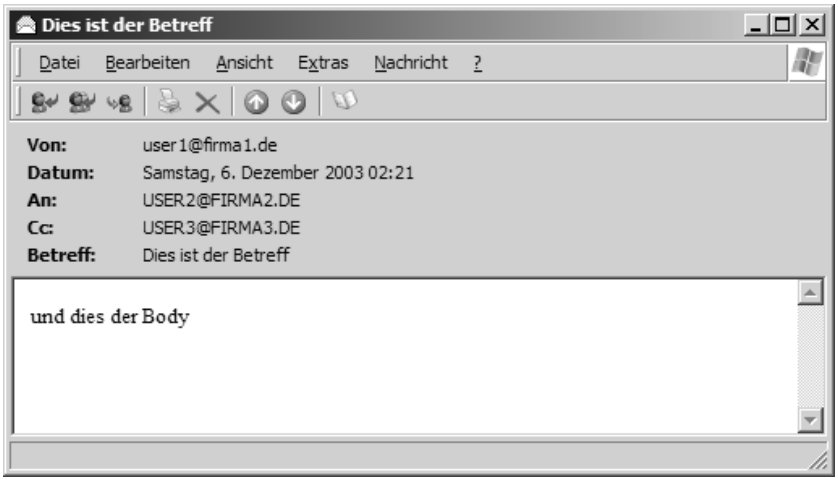


Abbildung 5.5
BCC-Problematik

Der POP3-Sammeldienst ist nicht in der Lage, aus dieser Nachricht den BCC-Empfänger zu ermitteln. Die Person erhält die Nachricht nicht.

Abhilfe ist nur möglich, indem der Provider die zusätzlichen Informationen des ENVELOPE der Nachricht zusätzlich in den HEADER der Nachricht einfügt, z.B. als zusätzliche Felder, vorausgesetzt der POP3-Sammeldienst wertet genau die gleichen Felder aus. Leider gibt es keinen allgemein gültigen Standard für dieses Vorgehen, so dass die verschiedenen Provider und POP3-Sammelprogramme nicht immer miteinander funktionieren.

POP3 — Probleme mit CC

Ein weiteres Problem lässt sich am gleichen Beispiel beschreiben. In der Nachricht ist die E-Mail-Adresse „USER3@FIRMA3.DE“ als Kopieempfänger aufgeführt. Diese Information erhält auch der POP3-Sammler. Ohne entsprechende Vorkehrungen sendet der POP3-Sammeldienst diese Nachricht direkt an den Exchange-Server. Der Exchange-Server besitzt kein lokales Postfach für die Nachricht, da der Empfänger zu einem anderen Unternehmen gehört.

Mehrfachübermittlung

Je nach Einstellung wird der Exchange-Server diese Nachricht als Relay wieder versenden oder mit der Fehlermeldung „Relay nicht erlaubt“ ablehnen. Im ersten Fall erhält der externe Empfänger die E-Mail mehrfach, einmal direkt vom Absender und des Weiteren vom Exchange-Server. Im anderen Fall muss der POP3-Sammler mit der Ablehnung umgehen können.

Auch hier muss der POP3-Sammler Vorkehrungen treffen, so dass E-Mail-Adressen von externen Personen, die als weitere Empfänger in der Nachricht enthalten sind, nicht in einen konstruierten ENVELOPE übernommen werden.

Stabilität einer POP3-Anbindung

Um mit einem POP3-Sammeldienst eine stabile Funktion zu erreichen, müssen Ihr Internet-Provider und das Programm zum Einsammeln der Nachrichten sowie Weiterleiten an Exchange miteinander harmonieren.

Monitoring POP3

Zusätzlich sollten Sie die Funktion regelmäßig überwachen, da beim Ausfall einer Komponente keine neuen Nachrichten mehr eintreffen. Dies wird besonders in kleineren Umgebungen mit wenig E-Mail-Aufkommen keineswegs sofort bemerkt. Die Nachrichten verweilen im Postfach des Providers, und die Ursache, warum der POP3-Sammler diese nicht abholt, ist kaum zu erkennen. Auch ein Update des E-Mail-Servers beim Provider kann das Abholen verhindern, wenn dabei das Format der Nachrichten im Sammelpostfach unabsichtlich verändert wird.

Die Anbindung des Exchange-Servers per POP3-Sammelkonto an das Internet ist ein gangbarer Weg, bei dem Sie entweder auf verschiedene kostenfreie Produkte (z.B. Pullmail) oder auf kommerzielle Lösungen zurückgreifen können, die allesamt im unteren Preissegment zu finden sind. Eine gute Quelle für Informationen ist Ihr Provider oder der Support der Hersteller der in Frage kommenden Produkte. Aber auch mit Wählverbindungen und kleinem Budget gibt es alternative Möglichkeiten, ein Unternehmen per SMTP an das Internet anzubinden und auf POP3-Sammler zu verzichten, z.B. mit ATRN oder dynamischen DNS-Einträgen in Verbindung mit einem leistungsfähigen Provider. Es ist verständlich, dass Zugänge für einzelne Computer von Privatpersonen nicht unbedingt auch für die Anbindung einer Firma geeignet sind, zumal hier auch nicht die entsprechenden Verfügbarkeiten gewährleistet werden müssen.

5.3 Die Kopplung an das Internet

Aufbauend auf den Kenntnissen zu Namensauflösung, SMTP und POP3 können Sie nun die möglichen Varianten einer Anbindung Ihres Netzwerks bestimmen. Für die Anbindung eines Exchange-Servers gibt es viele technisch denkbare Varianten, die unterschiedlich gut geeignet sind.

5.3.1 Die Verbindung

Zur Bestimmung der praktikablen Anbindungen ist es wichtig, die Art der Verbindung zu kennen. Hierbei zählt weniger die technische Realisierung, also die Übertragung von Bits und Bytes über ISDN-Leitungen, analoge Modems, DSL-Verbindungen oder sonstige Wege, sondern wie sich die Verbindung für das Netzwerk darstellt. Folgende vier Varianten können unterschieden werden:

- permanent

  Die Verbindung zum Internet besteht rund um die Uhr. In der Regel bedeutet dies eine Standleitung, bei der nach Volumen oder pauschal abgerechnet wird. Die Verbindung wird nicht explizit aufgebaut, sondern ist andauernd da.

- 24 h

  Auch bei dieser Variante besteht die Verbindung nahezu permanent. Im Gegensatz zu einer echten Standleitung erfolgt hier ein expliziter Verbindungsaufbau, und der Provider kann die Verbindung auch beenden. Dies trifft für die meisten T-DSL-Verbindungen zu, die nach Volumen oder pauschal abgerechnet werden. Einige City-Provider bieten auch ohne DSL entsprechende ISDN-Verträge an, die ebenfalls rund um die Uhr bestehen können, ohne den üblichen Telefontarif.

- DialUp Two-Way

  Diese Verbindung wird nur bei Bedarf aufgebaut. Dabei kann die Kommunikation von beiden Seiten initiiert werden und wird wieder abgebaut, wenn keine Daten mehr übertragen werden. Oftmals werden solche Verbindungen nach Zeit berechnet, so dass eine gesammelte Übertragung der E-Mails günstiger ist. Es ist auch möglich, dass der Provider die Kommunikationskosten beim Kunden über eine Rückruffunktion (Callback) auflaufen lässt. Diese Anbindung wurde früher oft mit ISDN-Wählverbindungen und Routern aufgebaut.

- DialUp ausgehend

  Die einfachste Anbindung ist die von Millionen Benutzern praktizierte Einwahl in das Internet über einen Provider bei Bedarf. Die Verbindung wird immer nur vom Kunden einseitig aufgebaut, wenn ausgehende Daten anstehen. Ein Provider hat keine Möglichkeit, den Server des Kunden zu erreichen, wenn die Verbindung nicht besteht.

Standleitung versus DialUp

Welche Anbindung Sie für sich umsetzen, ist eine Frage des Standortes und des Budgets. Eine Standverbindung ist im Hinblick auf einen Serverbetrieb die einfachste Lösung, bedeutet aber auch höhere Kosten für Installation, Betrieb und die korrekt konfigurierte Firewall. Die 24 h-Verbindung ist dank T-DSL und anderer Angebote günstiger, aber leider nicht überall verfügbar. Einige DSL-Verträge unterbinden zudem die Nutzung als Firmenzugang zum Schnäppchenpreis.

Wählverbindungen über ISDN und Modem sind seit vielen Jahren im Einsatz, aber kranken an der begrenzten Bandbreite. Der Trend zu größeren Nachrichten kann eine ISDN-Verbindung sehr schnell zu einer teuren Pseudostandleitung machen. Letztlich ist der Markt ständig in Bewegung, so dass eine regelmäßige Kontrolle der Anbindung notwendig ist.

5.3.2 Die IP-Adresse

Neben der eigentlichen Verbindung selbst ist die Vergabe der IP-Adresse das zweite Kriterium zur Auswahl der möglichen Anbindung Ihres Exchange-Servers. Bedeutend ist hierbei die IP-Adresse, die Ihr Netzwerk von Ihrem Provider erhält. Ein Router oder ein Server erhält diese IP-Adresse, wenn die Verbindung zum Internet hergestellt wurde. Es ist dabei nicht relevant, wie in Ihrem internen Netzwerk die IP-Adressen vergeben werden. Zwei unterschiedliche Ansätze gilt es zu betrachten:

IP-Adressvergabe

- Statisch

  Ihr System erhält von Ihrem Internet-Provider beim Verbindungsaufbau immer die gleiche IP-Adresse oder behält das gleiche Subnetz. Dies bedeutet nicht zwingend, eine Standverbindung zu besitzen. Auch Wählverbindungen und DSL-Verbindungen können mit einer statischen Adresse konfiguriert werden.

- Dynamisch

  Ihr System erhält bei jeder Verbindung eine andere IP-Adresse. Da niemand diese Adresse direkt kennt, ist eine Auflösung ohne Hilfsmittel wie dynamische DNS-Einträge nicht erreichbar. Auch semipermanente Standverbindungen wie T-DSL erhalten durch eine Zwangstrennung immer wieder eine andere IP-Adresse.

Mit beiden Varianten ist eine Anbindung des Servers an das Internet möglich. Allerdings sind unterschiedliche Anbindungsvarianten zu berücksichtigen.

5.3.3 Verbindungstabelle

Die folgende Tabelle zeigt auf, welche Alternativen sich Ihnen zum Versand und Empfang von Nachrichten bieten. Anhand der Verbindung und der Vergabe der IP-Adresse können Sie in der Tabelle die sinnvollen Möglichkeiten zur Übertragung der Nachrichten in die jeweilige Richtung ablesen.

In den Folgekapiteln werden die einzelnen Verbindungen kurz erläutert. Die favorisierte Methode ist fett gekennzeichnet.

Verbindung	IP-Adresse	Eingehend	Ausgehend	Produkte/Details
permanent	statisch	**Direkt** ETRN ATRN POP3	**SMTPDirekt** SMTPRelay	T-Interconnect T-Interconnect DSL
permanent	dynamisch	**ATRN** POP3 DynRelay **DynDNS**	**SMTPRelay** SMTPDirekt	Keine genaueren Informationen verfügbar. Sinnvolle Anwendungen und Produkte sind nicht bekannt.
24 h	statisch	**Direkt** ETRN ATRN POP3	**SMTPDirekt** SMTPRelay	Keine genaueren Informationen verfügbar.
24 h	dynamisch	**ATRN** POP3 DynRelay **DynDNS**	SMTPDirekt **SMTPRelay**	DSL-Flatrate DSL-Volumen T-DSL Business
DialUp TwoWay	statisch	**Direkt** ETRN ATRN POP3	SMTPDirekt **SMTPRelay**	ISDN-Wähl-verbindung mit fester IP-Adresse.
DialUp TwoWay	dynamisch	POP3 ATRN DynRelay	SMTPDirekt **SMTPRelay**	Keine Produkte bekannt.
DialUp ausgehend	statisch	Direkt ETRN ATRN POP3	SMTPDirekt **SMTPRelay**	Keine Produkte bekannt.
DialUp ausgehend	dynamisch	DynRelay POP3 ATRN	SMTPDirekt **SMTPRelay**	DSL-Zeittarif T-Online ISDN/analog Call by Call

Tabelle 5.1 Arten der Internet-Anbindung

5.3.4 Eingehender Verkehr

So können Nachrichten empfangen werden.

Viele verschiedene Anbindungen stehen für den Empfang der Nachrichten zur Verfügung. Wählen Sie die passende anhand der Tabelle für sich aus:

- Direkt

  Die eingehenden Nachrichten werden direkt auf Ihren E-Mail-Server zugestellt. Der MX-Eintrag im DNS verweist auf die offizielle IP-Adresse Ihres E-Mail- oder Relay-Servers. Schutzeinrichtungen wie Portfilter und

Firewall sind hierbei jedoch Pflicht. Dies ist aber zugleich die einfachste und direkte Methode, die bei Standleitungen mit fest zugewiesenen IP-Adressen genutzt werden sollte.

- ETRN

  Ihr Exchange-Server signalisiert dem Provider, dass er unter der vorgegebenen IP-Adresse erreichbar ist, und der E-Mail-Server des Providers sendet Ihnen die Nachrichten zu. Dies funktioniert nur, wenn Sie immer die gleiche IP-Adresse erhalten. Der Provider speichert jedoch die Nachrichten zwischen, bis Ihr Server seine Bereitschaft signalisiert.

- ATRN

  Wenn Sie nicht immer die gleiche IP-Adresse verwenden, kann ETRN nicht funktionieren. Dann muss Ihr Server Ihren Provider über ein sicheres Protokoll informieren, dass Sie unter der aktuellen IP-Adresse erreichbar sind. Der Provider erkennt die erfolgreiche Anmeldung und sendet daraufhin die E-Mails zu. Ähnliche Verfahren nutzen auch Programme wie FINGER, WHOIS etc.

- POP3

  Ihr Provider legt alle Nachrichten in einem Sammelpostfach ab, das Sie mit einem geeigneten Programm abholen und die E-Mails an Ihren Exchange-Server übergibt. Diese Möglichkeit ist mit allen Varianten der Anbindung nutzbar, beinhaltet aber auch die größten Kompatibilitätsrisiken. Trotzdem bieten viele Provider diesen Weg als die angeblich ideale Lösung an.

- DynDNS

  Server, die z.B. dank DSL-Flatrate immer erreichbar sind, aber keine fest zugewiesene IP-Adresse nutzen, können durch die Nutzung eines dynamischen DNS-Servers Ihre aktuelle IP-Adresse im Internet bekannt geben. Alle Server im Internet können Ihren Server unter dem registrierten Namen erreichen und Nachrichten zusenden.

- DynRELAY

  Hierbei speichert der Provider Nachrichten an Ihre Domäne auf seinem Server und sendet diese an eine angegebene IP-Adresse, sobald Sie online sind. Die Systeme des Providers erkennen Ihren erfolgreichen Verbindungsaufbau an der Einwahl in das Netzwerk des Providers. Ein gesonderter Aufruf mit ETRN/ATRN/FINGER etc. ist nicht erforderlich. Diese Methode funktioniert, wenn Ihr Zugangsprovider zugleich die Nachrichten für Sie puffert. Eine Sonderform dieser Anwendung ist die Verbindung zum Internet über einen beliebigen Provider und die Anmeldung bei Ihrem Mail-Provider über ein VPN. Auch dann kann der

Mail-Provider Ihre erfolgreiche Anmeldung erkennen und Ihnen die Nachrichten sogar verschlüsselt zusenden.

Dies sind nur die häufigsten Anbindungsarten. Natürlich gibt es weitere seltener genutzte Varianten und Lösungen. Ihr Provider sollte Ihnen dann weiterhelfen.

5.3.5 Ausgehender Verkehr

Der Versand von Nachrichten per SMTP gestaltet sich für Exchange relativ unkompliziert:

Nachrichten versenden per SMTP

- SMTP Direkt

  Exchange versucht, über DNS die Zielserver aufzulösen und direkt zu erreichen. Dies ist aber nur sinnvoll bei Festverbindungen oder volumenabhängigen Tarifen. Bei Zeittakttarifen entstehen häufig hohe Kosten durch langsame Strecken zwischen Ihrem Server und dem Zielsystem. Arbeitet Ihr E-Mail-System mit dynamischen Adressen, kann es vorkommen, dass diverse Empfänger die Annahme der Nachricht verweigern, um sich vor Spam zu schützen. Dann sollten Sie Ihre Nachrichten an Ihren Provider senden.

- SMTP Relay

  Die meisten Provider bieten Ihren Kunden einen Relay-Server an, an den sie Ihre Nachrichten per SMTP senden und der für sie die weitere Übermittlung and die Zielsysteme übernimmt. So kann Ihr Exchange-Server unter Ausnutzung der Bandbreite jede Nachricht einmal an den Provider senden, der diese an die einzelnen Empfänger verteilt. Sie sparen Bandbreite und umgehen das Problem, aufgrund dynamischer Adressen von Spam-Filtern blockiert zu werden. Der Provider erkennt Ihre Berechtigung zur Nutzung des Relays anhand der IP-Adresse aus dem Netzwerk des Providers oder durch eine SMTP-Anmeldung.

Für beide Varianten ist es natürlich erforderlich, dass Exchange entweder die E-Mail-Server direkt im Internet auflösen und erreichen oder zumindest die Verbindung zum Relay aufbauen kann. Sehr oft sendet Exchange seine Nachrichten an ein internes Relay in Ihrer Firma, um z.B. auch ausgehende Nachrichten auf Viren zu prüfen, zu archivieren oder einen Disclaimer anzuhängen. Dann muss dieses System die Nachricht nach einem der beiden Verfahren weitersenden.

5.4 Die Internet-Anbindung

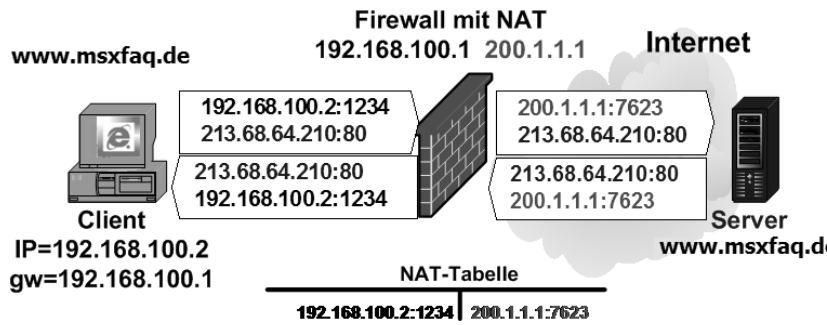
Damit Exchange 2003 Nachrichten über das Internet senden und empfangen kann, wird eine Verbindung zum Internet benötigt. Für die Anbindung gibt es ebenfalls eine Vielzahl von Verfahren. Exemplarisch werden drei häufig anzutreffende Verfahren erläutert.

5.4.1 Router mit Adressumsetzung

Die meisten kleinen Unternehmen setzen einen Router für die Verbindung zum Internet ein. Der Router ist auf einer Seite mit dem lokalen Netzwerk verbunden und auf der anderen Seite mit der entsprechenden Übertragungsleitung. Dies kann zum Beispiel ein DSL-Anschluss oder eine ISDN-Leitung sein.

Diesen Anbindungen ist gemeinsam, dass nur der Router eine offizielle IP-Adresse erhält und im internen Netzwerk private Adressen eingesetzt werden. Damit die internen Systeme mit dem Internet kommunizieren können, setzt der Router die IP-Adressen per NAT (Network Address Translation) um. Genau genommen müsste es PAT heißen, da nicht die Netzwerkadressen umgesetzt werden, sondern oft nur die einzelnen Ports.

Abbildung 5.6 Ausgehendes NAT



Zudem stellt sich die Frage der DNS-Auflösung. Nur der Router kennt durch den Verbindungsaufbau die aktuell gültigen DNS-Server. Die meisten Router bieten daher die Funktion eines DNS-Proxy an. Alle Systeme können den Router fragen, welcher die Anfrage an den Provider weiterleitet.

Unterstützt der Router diese Funktion nicht, dann muss Ihr DNS-Server im internen Netzwerk selbst die Anfragen an das Internet stellen. Dazu müssen Sie jedoch vom Provider die richtigen DNS-Server erfragen. Bei einer Änderung seitens des Providers müssen Sie ebenfalls diese Einträge aktualisieren.

Die meisten Router erlauben auch die Vergabe von IP-Adressen per DHCP. Diese Funktion sollten Sie nur aktivieren, wenn Sie selbst keinen DHCP-

Server betreiben. Einige Router erlauben sogar die Registrierung der zugewiesenen IP-Adresse bei einem dynamischen DNS-Service, so dass Sie sehr problemlos Nachrichten über dynamische DNS-Einträge empfangen können.

Um eingehende Verbindungen für SMTP und andere Dienste zu erlauben, muss der Router ein Verfahren zum Umleiten der eingehenden Verbindungen bieten. Diese Funktion wird oft als „Reverse NAT“ oder Portumleitung bezeichnet. Hierbei wird die eingehende Verbindung vom Router oder von der Firewall an einen bestimmten Port des internen Systems weitergegeben.

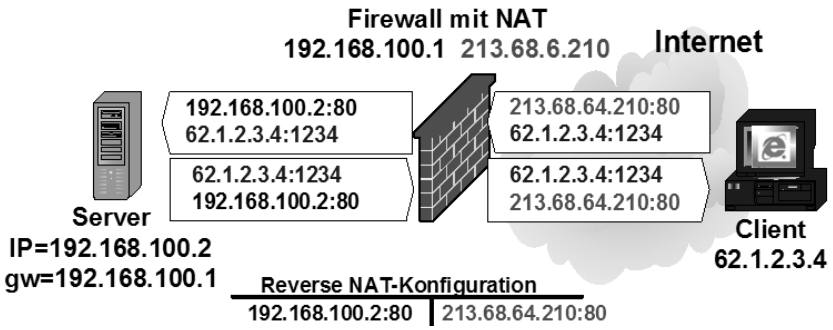


Abbildung 5.7 Eingehendes NAT

Die Schutzmechanismen sind beim Einsatz eines Routers prinzipiell gering. Der Schutz beschränkt sich meist darauf, bestimmte Protokolle anhand des TCP-Ports (Portfilter) zu erlauben oder zu verbieten. Einige Router analysieren zusätzlich die ansteigenden Sequenznummern der IP-Pakete und lehnen Pakete außer der Reihe ab. Zusätzlich wünschenswerte Funktionen wie die Überprüfung von E-Mail-Adressen, die Suche nach Viren etc. bleiben außen vor.

Zusammenfassung der Anbindung über einen Router mit NAT

- Ausgehende E-Mail

  Der Versand von Nachrichten ist für Exchange durch eine direkte Verbindung zum Internet sehr einfach. Exchange erreicht nach der erfolgreichen Auflösung per DNS direkt den Smarthost oder das Zielsystem.

- Eingehende E-Mail

  Der Router selbst holt keine eingehenden Nachrichten ab und speichert sie auch nicht. Diese Aufgabe muss ebenfalls Exchange über ETRN oder ein POP3-Sammler durchführen. Werden die Nachrichten per POP3 aus einem Sammelpostfach abgeholt, dann sind keine weiteren Vorkehrungen mehr zu treffen. Der POP3-Sammeldienst kann problemlos den Provider erreichen und die Nachrichten abholen.

  Über eine eingehende Portumleitung kann auch der Exchange-Server aus dem Internet erreicht werden. Damit ist der direkte Empfang über SMTP möglich. Ohne feste IP-Adresse sind jedoch dynamische DNS-Server

notwendig, bei denen sich der Router oder ein Programm meldet und die aktuelle IP-Adresse einträgt.

- Sonstige Funktionen

  Durch die Umleitung eingehender Verbindungen pro Port auf interne Systeme können auch HTTP (Outlook Web Access), POP3, IMAP4 und andere Protokolle genutzt werden. Der Einsatz von VPN ist je nach Produkt zu prüfen, da nicht alle Lösungen ein VPN über Adressumsetzungen aufbauen können. Aber auch hier muss bei wechselnder IP-Adresse über dynamische DNS-Server der Name im Internet bekannt gemacht werden.

- Eingehende Sicherheit

  Die Adressumsetzung durch den Router verhindert eingehende Pakete auf nicht explizit freigeschalteten Ports. Damit ist eine relativ hohe Sicherheit erreicht. Sobald jedoch interne Systeme von außen über eine Portumleitung verfügbar gemacht werden, sind diese Ports ungesichert zu erreichen. Die Absicherung muss direkt durch den Server durchgeführt werden. Zwar ist nicht der gesamte Server erreichbar, aber häufig sind gerade die aktiven Ports (z.B. 80 für IIS) die kritischen Dienste. Wer unter dieser Konstellation einen ungesicherten Webserver oder ein offenes Relay betreibt, wird nur kurze Zeit Freude an der Installation haben.

- Ausgehende Sicherheit

  Die Adressumsetzung verhindert zwar einen Zugriff auf das Netzwerk aus dem Internet, aber der Weg von intern nach extern ist ohne entsprechende Filterung freigegeben. Bei Verzicht auf weitere Konfiguration kann gewissermaßen jeder PC im internen Netzwerk Verbindungen zum Internet aufbauen. Damit sind Trojaner, aber auch Viren mit eigener SMTP-Funktion imstande, problemlos Nachrichten unter Umgehung Ihres E-Mail-Servers und Virenscanners zu versenden. Sie sollten den Router entsprechend konfigurieren, dass nur erwünschte Kommunikationen von innen nach außen erfolgen können. Leider erlauben die meisten Router im NAT-Betrieb alle ausgehenden Pakete. Die Probe können Sie sehr schnell mit dem Aufruf von

  ```
  TELNET mx00.schlund.de 25
  ```

  auf einem Arbeitsplatz durchführen. Meldet sich ein E-Mail-Server, dann kann jedes Programm auf dem PC E-Mails versenden.

- Kosten

Risikoabschätzung

  Die Anschaffungskosten solcher Router bewegen sich im dreistelligen Eurobereich, und auch die Betriebskosten sind relativ preiswert, vorausgesetzt die ISDN-Wählleitung wird nicht extrem oft aufgebaut. Der

Router kann Dienste und Verbindungen nur anhand der IP-Adresse und der Ports erkennen und filtern. Wählverbindungen baut der Router nur nach einer Leerlaufzeit ab, zu der eingehende Pakete aber nicht gezählt werden sollten. Das Risiko, dass sich aus einer Wählleitung eine teure Pseudostandleitung entwickelt, ist daher sehr groß. Bei der Anbindung mit DSL mit einem Volumentarif ist das Risiko gering, in eine Kostenfalle zu tappen.

Die Anbindung eines Exchange-Servers über einen einfachen Router an eine Stand- oder Wählleitung ist problemlos und erschwinglich. Die meisten Router erlauben in der Standardeinstellung alle ausgehenden Kommunikationswege. Dies ist jedoch für Unternehmen nicht sinnvoll. Entsprechende Filter sind aber nur auf Ebene der Ports und IP-Adressen möglich, so dass für weitere Funktionen zusätzliche interne Server und Dienste notwendig werden. Diese Methode stellt bei den meisten kleinen Unternehmen ohne eigenes IP-Subnetz die häufigste Anbindung dar.

5.4.2 Windows 2003 RAS-Service

Die Windows 2003-Server enthalten mit dem Routing- und RAS-Dienst (RRAS) eine sehr leistungsfähige Möglichkeit, direkt auf dem Server mit einer Netzwerkkarte, einer ISDN-Karte oder einem Modem eine Verbindung zum Internet aufzubauen und damit den Router einzusparen. Während Exchange 5.5 noch selbst eine Verbindung über RAS auf- und abbauen konnte, erwartet Exchange 2003 hingegen eine bestehende Verbindung. Das Betriebsystem muss nun eigenständig die Verbindung bei Bedarf aufbauen, sobald ausgehende Datenpakete anstehen und nach einer eingestellten Leerlaufzeit wieder abbauen. Diese Funktion bietet der Routing- und RAS-Service des Windows 2003-Servers bei entsprechender Konfiguration.

Sicherheitslücke

Die Praxis rät von solchen Konstellationen ab, da für die Zeit der Verbindung der Windows-Server mit einem Bein direkt im Internet steht. Eine solche Konfiguration ist nur ratsam, wenn zusätzliche Schutzvorrichtungen installiert werden. Dies könnte der Microsoft ISA-Server übernehmen.

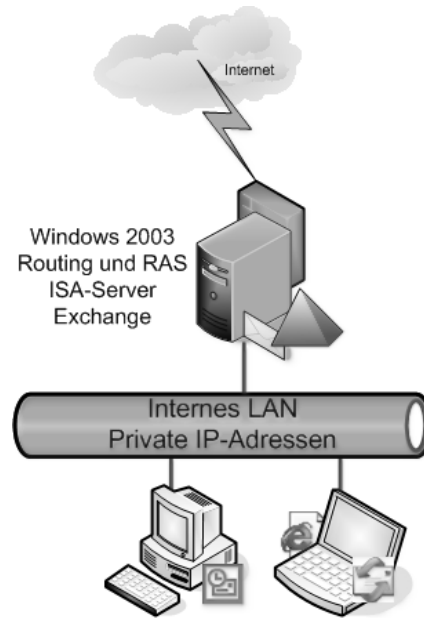
Ein zweites Problem kann auftreten, wenn Ihr Server zugleich Domänencontroller ist. Wenn die Verbindung zum Internet besteht, wird auch diese Adresse im DNS als gültige Adresse für den Domänencontroller registriert. Dies kann einige Clients etwas durcheinander bringen. Besonders wenn die Verbindung wieder abgebaut ist, dauert es einige Zeit, bis die nun ungültige IP-Adresse in diversen Caches veraltet ist. Zudem sollten Sie keinen Domänencontroller ungeschützt im Internet erreichbar machen.

Weiterhin erhält der Server durch die Verbindung zum Internet vom Provider die externen DNS-Server. Diese sollten Sie niemals nutzen, da ansonsten der

Server nicht mehr nur sich selbst oder andere interne DNS-Server befragt, sondern auch vom Provider eventuell Informationen über interne Systeme erbittet. Diese Anfragen schlagen sicher fehl. Die Fehlfunktion einiger Dienste auf dem Server ist damit vorprogrammiert.

Hier sollten die internen DNS-Server als Weiterleiter den Provider fragen, und alle Server inklusive des Servers mit der Internet-Anbindung sollten nur die internen DNS-Server befragen.

Abbildung 5.8
Anbindung RRAS



Dies kann jedoch bei geeigneter Konfiguration und dem Einsatz einer Firewall und Filtern auf dem Server unterbunden werden. Dann ist auch ein Windows 2003-Server mit Exchange als Verbindung zum Internet einsetzbar.

Die folgenden Aussagen gelten, wenn Exchange direkt auf dem gleichen Server installiert ist. Dies ist oft der Fall beim Einsatz des *Small Business Servers* oder des früher verfügbaren „Internet-Communication-Pakets“ von Microsoft, bei dem alle Dienste auf einem Server installiert werden.

Zusammenfassung der Windows 2003 RAS-Option:

- Ausgehende E-Mail

  Der Versand von Nachrichten ist für Exchange durch die direkte Verbindungsmöglichkeit zum Internet sehr einfach. Exchange erreicht nach der erfolgreichen Auflösung per DNS direkt den Smarthost oder das Zielsystem.

- Eingehende E-Mail

  Exchange ist ebenso direkt erreichbar, wenn keine zusätzlichen Schutzmaßnahmen eingebaut werden. Damit könnten eingehende Nachrichten direkt per SMTP zugestellt werden. Auch die Abholung per POP3 ist ohne weitere Vorkehrungen möglich.

- Sonstige Funktionen

  Durch die direkte offizielle IP-Adresse kann jeder Dienst auf dem Server ohne Einschränkung aus dem Internet erreicht oder beim Einsatz einer Schutzvorrichtung freigeschaltet werden.

- Eingehende Sicherheit

  Ohne zusätzliche Schutzmaßnahmen ist keine Sicherheit gegeben. Zwar können in den Bindungen der Netzwerkkarte die Arbeitsstationsdienste und Serverdienste entfernt werden, dagegen sind die LDAP-Schnittstellen des Active Directory und andere Dienste nicht ohne weiteres zu blockieren. Einzig über die etwas unübersichtlich zu konfigurierenden Portfilter von Windows 2003 pro Netzwerkkarte sind Einschränkungen erzielbar. Ein Betrieb einer solchen Konfiguration ohne Firewall ist daher nicht empfehlenswert.

- Ausgehende Sicherheit

  Ohne weitere Konfiguration können PCs aus dem internen Netzwerk nicht auf das Internet zugreifen. Erst die Installation zusätzlicher Dienste (z.B. Proxy-Server) oder das Aktivieren der Adressumsetzung im Routing- und RAS-Dienst gewähren den Zugriff. Der Versand von Mails über Exchange als Relay-Station oder über den Outlook-Client ist erlaubt.

- Kosten

  Die Verbindungskosten sind ähnlich der Routeranbindung zu bewerten. Den Einsparungen des Routers stehen die Kosten für eine ISDN-Karte oder DSL-Karte gegenüber sowie Kosten für zusätzliche Schutzmaßnahmen. Bei ISDN sind die Verbindungskosten zu berücksichtigen. Bei DSL sollte ein Volumentarif das Risiko hoher Kosten minimieren.

Der direkte Anschluss des Exchange-Servers an das Internet ist in bestimmten Situationen mit zusätzlich installierten Paketen möglich. Besonders der Small Business Server mit integriertem ISA-Server eignet sich für solche Konfigurationen. Allerdings ist die Einsparung eines eigenen Routers für die Verbindung zum Internet im Vergleich zur niedrigeren Sicherheit und höheren Komplexität der Serverinstallation zu sehen. In den meisten Fällen ist daher eine Trennung der Internet-Anbindung von den Serverdiensten ratsam. Eine Umstellung auf andere Übertragungsmöglichkeiten ist später problemlos umsetzbar, wenn nur der Router getauscht und die Konfiguration des Servers nicht verändert werden muss.

5.4.3 Firewall und DMZ

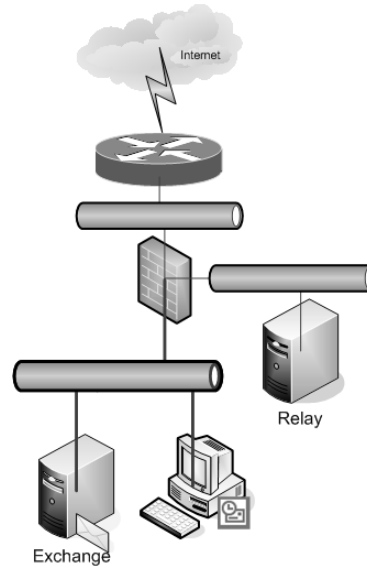
Die Anbindung mittels Router oder direkt über eine Schnittstellenkarte im Server sind für mittlere und kleinere Unternehmen oft die ersten Schritte der Verbindung ins Internet.

Erhöhte Anforderungen an die Sicherheit, Verfügbarkeit, Lastverteilung und zusätzliche Funktionen erfordern eine leistungsfähigere Internet-Anbindung. Eine solche Anbindung ist oft damit verbunden, dass der Provider die Verbindung inklusive Router stellt und der Kunde ein eigenes Subnetz mit einem Adressraum erhält. Erst ab der Ethernet-Schnittstelle des Routers baut die Firma selbst Ihre Infrastruktur auf.

Der Anschluss des Exchange-Servers direkt an dieses Subnetz ist nicht ratsam, da er ähnlich ungeschützt aus dem Internet erreichbar wäre wie bei einer RAS-Anbindung.

Der Router übernimmt in den seltensten Fällen eine Firewall-Funktion, so dass Sie selbst eine Schutzfunktion vorsehen müssen. Eine vollwertige Firewall verbindet dieses Netzwerk mit dem internen Netzwerk und erlaubt nur die gewünschten Pakete. Zusätzlich werden oft gesonderte Systeme installiert, die die Verbindungen aus dem Internet annehmen und nach einer Analyse der Daten an die internen Server weitergeben.

Abbildung 5.9
Firewall und DMZ



Um diesen Zwischenserver optimal zu schützen, wird die Kommunikation zu diesem System durch eine Firewall kontrolliert. Dieser besondere Bereich wird als demilitarisierte Zone (DMZ) oder auch Perimeternetzwerk bezeichnet, weil sowohl Verbindungen aus dem Internet als auch Verbindungen aus dem internen Netzwerk kontrolliert werden.

Für den Austausch von Nachrichten werden hierzu SMTP-Relays in der DMZ platziert, die zusätzlich auch eine Überprüfung nach Viren durchführen können. Für das sichere Surfen im Internet werden sehr häufig Proxy-Server eingesetzt. Abhängig von den individuellen Sicherheitsanforderungen werden eine oder mehrere unabhängige Firewalls installiert.

Zusammenfassung der Anbindung mit Firewall und DMZ:

- Ausgehende E-Mail

  Der Versand von Nachrichten von Exchange erfolgt am besten über ein Relay-System in der DMZ, das die E-Mails in das Internet weiter sendet. So besteht nie eine direkte Verbindung zwischen Exchange und einem fremden System.

- Eingehende E-Mail

  Auch eingehende Nachrichten werden nicht direkt von Exchange angenommen, sondern ein Relay in der DMZ nimmt die Nachrichten an und leitet diese an Exchange weiter.

- Sonstige Funktionen

  Das Relay-System in der DMZ kann eine ganze Reihe nützlicher Zusatzfunktionen erbringen, z.B. Virenscan, Spam-Filter, Disclaimer etc.

- Eingehende Sicherheit

  Durch die Trennung der Funktionen und Dienste ist die Sicherheit sehr hoch anzusetzen. Im Notfall kann die Verbindung unterbrochen werden, ohne die internen Abläufe zu stören. Das größere Risiko ist der Administrator oder eine unsaubere Konfiguration, die nicht ausreichend restriktiv oder nicht aktuell genug ist.

- Ausgehende Sicherheit

  Bei entsprechender Konfiguration ist ein Zugriff von intern nach außen nicht möglich. Auch Exchange hat keinen direkten Kontakt zu eventuell unsicheren Systemen.

- Kosten

  Relativ hoch aufgrund des Hardware- und Software-Einsatzes.

Die Anbindung mit einer Firewall und weiteren Servern, erlaubt eine sehr viel sicherere Verbindung von Exchange an das Internet. Allerdings sind die Kosten ebenfalls höher, so dass eine individuelle Risikoabschätzung notwendig ist.

5.5 Protokolle und deren Absicherung

In Verbindung mit Exchange sind weitere Protokolle und deren Umsetzung zu beachten. Für Funktionen, für die es keinen speziellen Proxy gibt, kann immer noch die Adressumsetzung angewendet werden. Dabei ist gleichwohl zu bedenken, dass diese Ports des Servers dann direkt aus dem Internet erreichbar sind. Die einzelnen Dienste des Proxy können auf einem eigenen Server realisiert werden. Ebenso ist es möglich, dass die Firewall selbst einen Teil oder alle Aufgaben übernimmt.

Folgende Protokolle sollten bei der Planung der Anbindung berücksichtigt werden:

Tabelle 5.2 Exchange-Protokolle

Protokoll	Port	Mögliche Umsetzungen
DNS Query	53/UDP	DNS-Forwarder oder Proxy in der DMZ/Firewall
SNTP	123/UDP 123/TCP	Zeitserver in der DMZ, der seine Uhrzeit aus dem Internet bezieht und von intern befragt werden kann. Alternativ eigene interne Zeitquelle mit Funkuhr.
SMTP	25/TCP	SMTP-Relay oder SMTP-Proxy
POP3	110/TCP	POP3-Proxy
IMAP4	143/TCP	IMAP4 Proxy
HTTP HTTPS	80/TCP 443/TCP	HTTP-Proxy/Reverse Proxy

Bei allen Schutzmechanismen darf der Mensch als schwächstes Glied in der Kette nicht ausgespart werden. Die Identifizierung des Benutzers am System erfolgt meist anhand des Benutzernamens und eines Kennwortes. Dieses Kennwort sollte ausreichend komplex sein und nach einer bestimmten Zeit ablaufen. Ebenso sollte das Konto nach mehreren Fehlversuchen für einige Zeit gesperrt bleiben und eine entsprechende Informationsnachricht erstellt werden. Kennworte, die sehr kurz sind oder sehr lange unverändert bleiben, ind genauso eine Einladung für mögliche Saboteure und Angreifer wie Konten, die nicht gesperrt werden. Eine höhere Sicherheit ist durch den Einsatz von Zertifikaten, Smartcards oder andere eindeutige Schlüssel gegeben.

5.5.1 DNS- und NTP-Anbindung

Namensauflösung, DNS und Uhrzeit

Für die Auflösung von externen Adressen sollte der Exchange-Server, wie bisher auch, immer die internen DNS-Server fragen. Falsch wäre es, wenn der Exchange-Server externe DNS-Server befragen würde. Damit ist zwar der Versand von Nachrichten in das Internet möglich, aber die interne Auflösung gestört. Daher ist es besser, wenn der interne DNS-Server auch Anfragen nach externen Adressen auflösen kann. Dazu kann der interne DNS-Server u.a. die DNS-Server des Providers als Weiterleiter verwenden.

Zur Absicherung könnte dies auch über die DNS-Proxy-Funktion eines Routers oder ein weiteres DNS-Relay in einer DMZ erfolgen.

Nicht verschwiegen werden sollte, dass auch in Exchange der virtuelle SMTP-Server angewiesen werden kann, abweichend von der Systemeinstellung einen anderen DNS-Server zu fragen. Allerdings kann dies später auch die Kommunikation zwischen Exchange-Servern stören, so dass diese Konfiguration nur in Verbindung mit der Einrichtung eines weiteren virtuellen SMTP-Servers sinnvoll ist.

Zeit-Server einrichten

Das gleiche Prinzip kann angewendet werden, um die aktuelle Uhrzeit aus dem Internet anzufordern. Die Physikalisch Technische Bundesanstalt in Braunschweig betreibt dazu einige NTP-Server, die über das Internet unter dem Namen „ptbtime1.ptb.de“ und „ptbtime2.ptb.de“ zu erreichen sind (siehe http://www.ptb.de/de/org/q/q4/q42/ntp/ntp_main.htm). Ein NTP-Server in der DMZ oder auf der Firewall holt die amtliche Uhrzeit aus dem Internet. Der interne Domänencontroller wiederum bezieht die Uhrzeit von diesem NTP-Server oder direkt. In Windows richten Sie mit dem Befehl

```
NET TIME /SETSNT:ipadresse
```

den Zeitserver ein. Die internen Systeme fragen weiter wie bisher die Windows 2003-Domänencontroller. Damit ist sichergestellt, dass alle Server die korrekte Uhrzeit nutzen und damit alle Nachrichten korrekt gekennzeichnet werden. Auch Windows 2000- und Windows XP-Clients beziehen die aktuelle Uhrzeit von den Domänencontrollern. Andere Clients können mit Hilfsprogrammen ebenfalls per NTP die Uhrzeit beziehen. Dies ist nicht nur ein schöner Nebeneffekt. Eine korrekte Uhrzeit und Zeitzone bewirken nebenbei auch eine korrekte Kennzeichnung von Nachrichten und Terminen und ermöglichen erst die zuverlässige Anmeldung über Kerberos.

5.5.2 SMTP-Relay oder SMTP-Proxy

SMTP sicher mit Relay übertragen

Schon bei der Internet-Anbindung wurde das Thema SMTP-Relay ausgiebig im Hinblick auf die Funktion, Einsatz und Stabilität behandelt. Allerdings lag der Schwerpunkt dort bei dem Einsatz des Relays auf der Seite des Providers.

Auch im eigenen Netzwerk ist der Einsatz eines SMTP-Relays zu prüfen, das zwischen Exchange und dem Internet geschaltet wird und eine direkte Verbindung zum Exchange-Server unterbindet.

Durch die Reduzierung der Funktion auf dem Relay in der DMZ sind diese Systeme sehr viel robuster gegen Angriffe. Selbst bei einem Ausfall oder einer notwendigen Abschaltung bleibt das interne Nachrichtensystem funktionsfähig.

Ein SMTP-Relay wird für den ausgehenden Nachrichtentransfer eingesetzt, so dass Exchange alle E-Mails nur an das Relay übermittelt. Das SMTP-Relay selbst sendet die Nachrichten entweder an den Smarthost des Providers oder direkt an die Empfängerserver im Internet.

Ein eingehendes SMTP-Relay ist nur dann zweckmäßig, wenn eingehende Nachrichten per SMTP an die Firma gesendet werden. Ein Unternehmen, das seine Nachrichten per POP3 abholt, benötigt kein eingehendes SMTP-Relay zum Schutz des Exchange-Servers gegen externe Angriffe. Die Nachrichten befinden sich schon intern und werden vom POP3-Sammler per SMTP an den Server gesendet. In diese Verbindung kann jedoch ein SMTP-Relay sehr gut als Virenscanner eingeschaltet werden, sofern der POP3-Sammeldienst keine entsprechende Funktion unterstützt.

5.5.3 POP3 und IMAP4

Zugriff per POP3

Der Zugriff auf den Exchange-2003 Server per POP3 oder IMAP4 aus dem Internet ist ebenfalls ein beliebter Weg, um den E-Mail-Server anzugreifen.

Bislang sind kaum Fehler in der Implementierung des POP3- oder IMAP4-Dienstes bekannt. Trotzdem ist es im Interesse des sicheren Betriebs, eine direkte Verbindung von außen zum Server durchaus nicht zuzulassen und ein Vermittlersystem dazwischen zu schalten. Ein solcher POP3-Reverse-Proxy kann unter anderem den „DELETE“-Befehl verhindern und somit das irrtümliche Löschen des Anwenders von Nachrichten aus dem Posteingang verhindern.

Auch bei der Verbindung über POP3 und IMAP4 ist eine Verschlüsselung der Daten mittels SSL wünschenswert. Eine unverschlüsselte Verbindung erlaubt ein einfaches Abhören der Kennworte und ist aus Sicherheitsgründen zu vermeiden.

Wird POP3 als Protokoll zur Abholung neuer Nachrichten genutzt, ist ein POP3-Proxy in die ausgehende Richtung denkbar, um das Abholprogramm zu schützen. Dies ist in der Regel nicht der Grund für den Einsatz von POP3-Proxies, sondern der Vorteil liegt in der zusätzlichen Funktion solcher Proxy-Server als Spam-Schutz und Virenscanner.

5.5.4 HTTP/HTTPS Proxy

Sicheres Surfen im Internet

Exchange 2003 nutzt selbst nicht das Protokoll http, um Informationen aus dem Internet anzufordern. Der Client auf den Arbeitsstationen versucht jedoch über dieses Protokoll, in Nachrichten eingebettete Bilder oder Links zu öffnen, und benötigt allein dazu schon den Zugriff auf das Internet. In diesem Fall kann ein HTTP-Proxy diesen Zugriff erlauben und gleichzeitig als Filter gegen Viren, Werbebanner und anderes dienen. Zudem ermöglicht ein HTTP-Proxy die Protokollierung der Zugriffe und eine spätere Abrechnung des Übertragungsvolumens. Der Zugriff auf das Internet über einen Proxy ist sehr viel leistungsfähiger, sicherer und durch einen Cache oftmals auch schneller als der direkte Zugriff über eine Adressumsetzung.

Viel wichtiger ist indessen der umgekehrte Weg, also das Lesen der Nachrichten auf Ihrem Exchange-Server aus dem Internet. Exchange 2003 bietet mit OWA eine sehr einfache und leistungsfähige Methode an, die aber entsprechend zu schützen ist. Es ist heute gerade zu unverantwortlich, einen Exchange-Server direkt am Internet zu betreiben. Aus diesem Grund steht der E-Mail-Server meist im internen Netzwerk, und der Zugriff von außen erfolgt über einen anderen Server, der die eingehenden Anfragen annimmt und an den internen Server weiterleitet. Hierzu kennt Exchange 2003 zwei grundlegende Verfahren:

Proxy- versus Front-End-Server?

- Reverse HTTP-Proxy

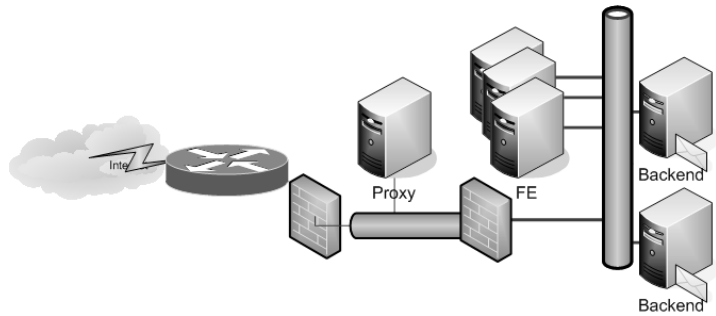
  Ein entsprechender Proxy-Server nimmt die externen Anfragen an und leitet sie nach innen weiter. Diese Funktion unterstützt unter anderem der Microsoft ISA-Server sowie Checkpoint und andere Firewalls. Die Einschränkung dieser Lösung ist die Beschränkung der Weiterleitung an genau einen bestimmten internen Exchange 2003-Server. Gibt es mehrere Postfachserver, deren Daten abgerufen werden, benötigen Sie auch mehrere Umleitungen.

- Front-End-Server

  Diese Einschränkung umgeht Microsoft mit dem Exchange 2003-Front-End-Server. Dieser Exchange-Server betreibt keine eigenen Datenbanken, sondern wird als Front-End-Server konfiguriert und leitet dann ähnlich einem Reverse-Proxy die Anfrage intern weiter. Hierbei greift der Front-End-Server auf die Informationen des Active Directory zu, um für jede Verbindung den passenden Backend-Server anzusprechen. So wird nach außen nur genau ein Server sichtbar. Diese Flexibilität kostet Sie eine weitere Exchange-Lizenz sowie Hardware-Ressourcen. Trotzdem entfällt nicht die Schutzmaßnahme des Front-End-Server gegen Angriffe von außen, für die ein vorangestellter Reverse-Proxy sorgt.

Für den Zugriff mittels Outlook Web Access greift ein Client nur auf die virtuellen Verzeichnisse „\EXCHANGE“, „\EXWEB“ und „\PUBLIC“ zu. So ist es möglich, mit URLSCAN oder der Firewall nur diese URLs zuzulassen und alle anderen Pfade zu blockieren.

Abbildung 5.10 Front-End-Backup mit Reverse-Proxy



Ein wichtiger Faktor bei der Nutzung des Browsers ist die Verschlüsselung der Informationen. Erst durch den Einsatz von SSL ist sichergestellt, dass die Benutzerdaten und Kennwörter nicht in Klartext übermittelt werden und die übertragenen Inhalte nicht in einem Proxy oder der lokalen Festplatte des Clients im Cache liegen.

Die Einrichtung von SSL ist dabei auf dem vordersten Server, der als Gegenstelle für den Client auftritt, erforderlich. Die Verbindung vom Reverse-Proxy zum Exchange-Server oder Front-End-Server sollte ebenfalls per SSL oder IPSec verschlüsselt werden.

„RPC over HTTP“

Die Nutzung von HTTP als Verbindungsprotokoll nimmt mit dem Einsatz von Outlook 2003 vermehrt zu, da der Client hier eine Kommunikation mit dem Exchange-Server über „RPC over HTTP“ herstellen kann. Die Daten, die bisher per RPC direkt übertragen wurden und aufwändig mit einem VPN zu sichern waren, sind über HTTPS sehr viel problemloser auszutauschen. Auch hierbei sind die Firewall und der Proxy gefragt, um ungültige Daten abzulehnen.

5.6 SMTP-Connector

Die Konfiguration der Exchange 2003-Installation erfordert hinsichtlich des Versands von Nachrichten eigentlich keine besonderen Anpassungen, vorausgesetzt der Server ist direkt aus dem Internet erreichbar und sendet seinerseits per SMTP direkt ins Internet. Der virtuelle SMTP-Server des Exchange-Servers nimmt per Default jede Nachricht per SMTP an, solange die Domäne in einer Empfängerrichtlinie eingetragen ist. Ebenso sendet er die Nachrichten direkt an die Zielsysteme, solange diese per DNS auflösbar und per TCP/IP erreichbar sind. Dies ist aber in den meisten Fällen nicht möglich und nicht erwünscht.

Die Exchange 2003-Server in einer Organisation pflegen eine Tabelle mit Leitwegen, ähnlich wie sich Router miteinander abgleichen, um den kürzesten und günstigsten intakten Pfad zum Ziel zu finden. In dieser Tabelle sind alle Connectoren für die Erreichbarkeit der Exchange-Server untereinander aufgeführt. Auch der Weg zum Internet wird in dieser Tabelle gepflegt. Durch die Konfiguration eines SMTP-Connectors wird in der Exchange-Organisation bekannt gegeben, welche Server Nachrichten in das Internet übertragen können und welche Beschränkungen für diesen Zugang gelten. Ohne SMTP-Connector versucht jeder Server selbst die Nachrichten zuzustellen. In Exchange 5.5 musste hingegen immer erst ein SMTP-Connector installiert werden, damit Nachrichten an das Internet überhaupt gesendet und aus dem Internet empfangen werden konnten.

Ein Exchange-2003 Server hingegen nimmt immer Nachrichten über den virtuellen SMTP-Server an und benötigt auch keinen weiteren Dienst zum Versenden von Nachrichten. Der SMTP-Connector ist nur eine Konfigurationseinstellung und kein eigener Dienst oder ein eigenes Programm.

5.6.1 Der Assistent zur Einrichtung

Die Installation des SMTP-Connectors kann über einen Assistenten erfolgen oder manuell in der Routinggruppe definiert werden. Der Assistent versucht anhand der gewählten Optionen die korrekten Angaben beim virtuellen SMTP-Server und beim SMTP-Connector einzurichten. Allerdings gestaltet sich der Assistent nur in sehr wenigen Fällen wirklich hilfreich.

Der Assistent geht davon aus, dass der Exchange-Server direkt oder über einen Smarthost die Nachrichten versendet und eingehende Nachrichten auf die IP-Adresse des Servers zugestellt werden.

Abbildung 5.11 Exchange 2003-SMTP-Assistent zur Installation

Spezifische Anpassungen wie dynamisches DNS, POP3-Abholen oder ein- und ausgehende Smarthosts als Virenschutz und Firewalls werden nicht berücksichtigt.

Folgende Einstellungen führt der Assistent durch:

- Versand von SMTP ein- oder abschalten

  Aktivieren Sie den Versand nicht, dann richtet der Assistent keinen SMTP-Connector ein, sondern erlaubt nur die Anpassung der Empfängerrichtlinien.

- Empfang von SMTP ein- oder ausschalten

  Sie können über den Assistenten zwar den Empfang abschalten, bewirken freilich nur, dass die Empfängerrichtlinien nicht abgefragt und entsprechend gesetzt werden. Es werden keine Konfigurationen durchgeführt, die den Empfang von Nachrichten durch den Server verhindern. Um den Zugriff wirklich zu blockieren, müssen Sie später manuell die Beschränkungen im virtuellen SMTP-Server setzen.

- Empfängerrichtlinien anpassen

  Exchange 2003 nimmt alle Nachrichten an, sofern es entsprechende Empfängerrichtlinien gibt. Der Assistent erfragt alle SMTP-Adressen des Betriebes und passt die Standardempfängerrichtlinie entsprechend an.

- Smarthost oder direkte Verbindung

  Falls ein Smarthost für den Versand genutzt wird, findet dieser sich später im SMTP-Connector wieder. Der Eintrag im virtuellen SMTP-Server hierzu bleibt unverändert. Er sollte leer sein.

- DNS-Auflösung

  Diese Einstellungen werden im virtuellen SMTP-Server eingetragen. Wird hier abweichend vom Betriebssystem ein externer DNS-Server eingetragen, ist ein Versand in das Internet möglich, aber der interne Versand zu anderen Exchange-Servern kann gestört sein. Dieser Fall kann dann nur mit zusätzlichen virtuellen SMTP-Servern und entsprechend konfigurierten Routinggruppen-Connectoren gelöst werden. Die Kopplung an den internen DNS-Server und die Auflösung externer Adressen über diesen Server ist daher die bessere und einfachere Alternative.

- Zustelldomänen

  Diese Einstellung steuert die Nachrichtenübermittlung an bestimmte Zieldomänen. Diese Information wird in dem Adressraum des SMTP-Connectors hinterlegt. So können Sie mit dem Assistenten gesonderte Leitwege zu bestimmten Adressräumen einrichten, z.B. zu Partnerfirmen.

Trotz Assistent wird die Anbindung des Exchange 2003-Servers an das Internet nicht einfacher. Der Assistent reicht nur aus, wenn Ihr Exchange-Server direkt mit einer offiziellen IP-Adresse mit dem Internet verbunden ist. Aber selbst dann sollten Sie nicht allein auf den Assistenten vertrauen.

5.6.2 Einstellungen des virtuellen SMTP-Servers

Die Einstellungen des SMTP-Connectors wirken sich auf alle Server aus, die als lokale Bridgeheads aufgeführt werden. Folgende Einstellungen können jedoch nur im virtuellen SMTP-Server durchgeführt werden und sind daher je Server anzupassen:

- IP-Adresse des virtuellen Servers

  Besitzt Ihr Exchange-Server mehrere IP-Adressen, können Sie steuern, ob alle oder nur eine bestimmte Adresse für den Internet-Anschluss genutzt wird. Die Antwortpakete werden jedoch immer mit der ersten IP-Adresse der Netzwerkkarte versendet. Dies ist wichtig im Hinblick auf Einstellungen in Firewall- und Filtereinstellungen. Sie sollten nicht ohne Grund hier feste IP-Adressen zuweisen. Wenn Sie später die IP-Adresse des Servers umstellen, müssen Sie ansonsten auch diese Änderung anpassen.

- Exchange TCP/IP-Port

  Nachrichten über SMTP werden auf dem Port 25 empfangen. Nur wenn Sie auf dem gleichen Server eine Zusatzsoftware installieren, die ihrerseits die Nachrichten zuerst annehmen muss, sollten Sie Exchange auf einem anderen Port konfigurieren. Ihre Anwendung muss die eingehenden Nachrichten dann an diesen alternativen Port weitergeben.

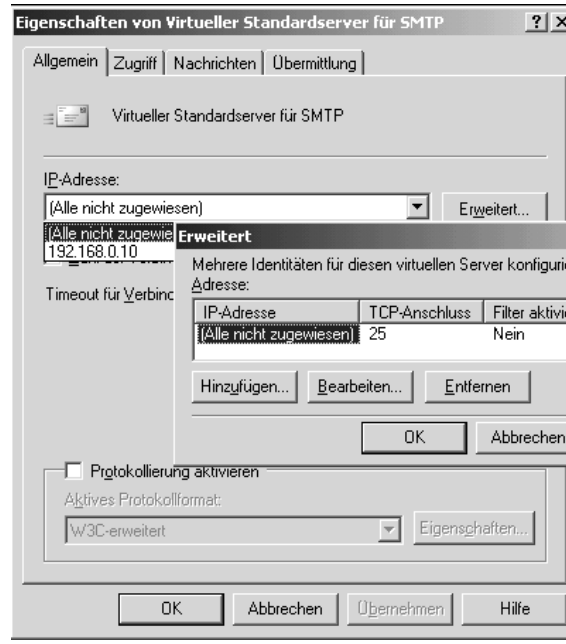


Abbildung 5.12 Einstellungen des virtuellen SMTP-Servers

Unter der Einstellung „Erweitert“ verbirgt sich auch die Möglichkeit, die Verbindungsfilter zu aktivieren. Bedenken Sie, dass auch die interne Kommunikation zwischen Exchange-Servern von solchen Einstellungen betroffen ist. Die Filter müssen aktiviert werden, wenn die RBL-Funktion von Exchange genutzt werden soll. Zur Fehlersuche bietet es sich an, die Protokollierung zu aktivieren. Achten Sie jedoch auf Ihre freie Festplattenkapazität, da die Protokolldateien sehr groß werden können.

- Zugriffsbeschränkungen

  Damit können Sie steuern, welche Systeme überhaupt den Exchange-Server per SMTP erreichen dürfen. Somit können Sie die Sichtbarkeit und Erreichbarkeit des Servers beschränken, damit nur vertrauenswürdige Systeme Ihren Exchange-Server über SMTP erreichen. Wenn intern alle Mitarbeiter über Outlook arbeiten, könnten Sie damit verhindern, dass Personen mit Outlook Express Nachrichten einliefern.

- Relay-Einschränkungen

  Wenn interne Systeme per SMTP über Exchange Nachrichten an das Internet versenden wollen, dann müssen diese für diese Relay-Funktion zugelassen werden. Exchange 2003 erlaubt per Default nur autorisierten Anwendern diese Funktion. Nicht alle Systeme können jedoch eine Autorisierung durchführen. Dann ist es hier möglich, ausgewählten IP-Adressen auch ohne Anmeldung den Versand zu erlauben.

SMTP-Connector oder Virtual SMTP-Server?

Im virtuellen SMTP-Server sind sehr viele weitere Parameter einstellbar, z.B. die Anzahl der gleichzeitigen Verbindungen, die maximale Anzahl an Empfängern etc. Hier sollten jedoch nur mit Bedacht Änderungen an den Standardwerten vorgenommen werden. Auf keinen Fall sollten Sie hier die Größe der Nachrichten oder einen Smarthost eintragen. Diese Einstellungen wirken sich auf alle SMTP-Nachrichten aus und behindern später auch die Kommunikation zwischen Exchange-Servern oder Active Directory-Replikationen über SMTP. Für die Konfiguration eines Smarthosts ist der SMTP-Connector der bessere Ort.

5.6.3 Einstellungen SMTP-Connector

Der SMTP-Connector erlaubt primär die Konfiguration ausgehender Verbindungen. Zusätzlich kann der SMTP-Connector auch auf der Gegenseite wartende Nachrichten mittels ETRN abfordern.

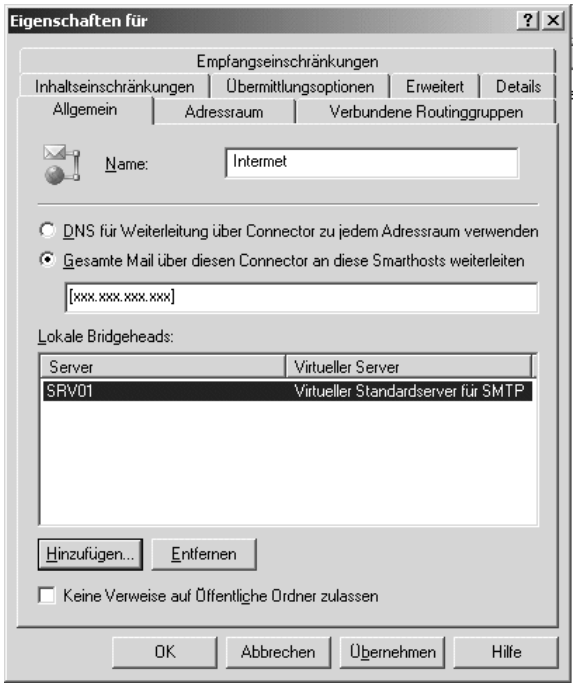


Abbildung 5.13 Smarthost beim virtuellen SMTP-Server

Die einzelnen Einstellungen bedeuten:

- Allgemein: Zustellungsoptionen

  Hier legen Sie fest, ob ausgehende Nachrichten an einen per DNS aufgelösten Server oder über einen Smarthost zugestellt werden. Beim Smarthost ist der Name oder die IP-Adresse in eckigen Klammern zulässig. Bevorzugt sollten Sie Namen verwenden, da Provider oft

mehrere Relay-Server betreiben oder auch die IP-Adressen sich manchmal ändern. Dies erfordert jedoch eine funktionierende Namensauflösung.

Mit den lokalen Bridgeheads sind die Server gemeint, welche diese Konfiguration anwenden. Im Gegensatz zu Exchange 5.5 können die Einstellungen eines einzigen SMTP-Connectors für viele Server gelten.

- Adressraum

Provider-Limits als Basis für E-Mail-Größe

Diese Einstellungen steuern, für welche Domänen dieser Connector zuständig ist. Wenn Sie für eine Partnerfirma einen eigenen Weg definieren möchten oder für Empfänger bei T-Online und anderen Providern besondere Beschränkungen für die Größe festlegen wollen, dann sind mehrere SMTP-Connectoren zu konfigurieren. Dies ist ebenfalls ein Unterschied zu Exchange 5.5, wo nur ein einziger Connector pro Server möglich war und je Server beim Connector unterschiedliche Leitwege für Domänen gepflegt werden mussten.

Wenn Sie Ihren Exchange-Server als zentrale Verteilstelle für andere E-Mail-Server mit eigener SMTP-Domäne in Ihrem Unternehmen nutzen, dann können Sie hier die Option „Weitergabe als Relay“ aktivieren. Exchange wird dann Nachrichten an diese Domänen annehmen und weiterleiten. Ansonsten würde Exchange die Nachrichten zwar annehmen, aber als unzustellbar ablehnen, wenn es keine internen Empfänger hierfür gibt.

Aktivieren Sie diese Option niemals auf einem Connector mit einem Adressraum wie „SMTP:*“, da Ihr Exchange-Server dann als offenes Relay missbraucht werden kann.

- Verbundene Routinggruppen

Diese Einstellungen erlauben die Verbindung mehrerer Standorte über SMTP. Die Exchange-Nachrichten werden dazu in einer Systemnachricht eingeschlossen. Damit ist auch über das Internet eine Kopplung von Exchange-Routinggruppen möglich, auch wenn die Server keine direkte Verbindung miteinander aufnehmen können. Bei direkter Verbindung Ihrer Exchange-Server sollten Sie mit Routinggruppen-Connectoren arbeiten. Auch Exchange 5.5 konnte Standorte mit dem SMTP-Connector auf diese Weise verbinden.

- Übermittlungsoptionen

Sie können bestimmen, wie oft und wann Exchange ausgehende Nachrichten übermittelt. Somit nehmen Sie Rücksicht auf Wählverbindungen oder erlauben anderen Systemen das Abholen Ihrer Nachrichten per TURN/ATURN von Ihrem Server. Interessant ist die Option, Nachrichten ab einer bestimmten Größe zu verzögern und so z.B. nur nachts zu senden.

- Erweiterte Einstellungen

  Über diese Einstellungen bestimmen Sie selbst, ob bei der Verbindung zur Gegenseite nur ein „HELO“ anstelle eines EHLO gesendet wird. Wichtig ist die Option, dass Exchange 2003 sich bei der Gegenseite authentifizieren kann. Dies ist bei vielen Smarthosts von Providern notwendig.

- Empfangsbeschränkungen

  Wer darf raussenden?

  Dieser unglücklich übersetzte Begriff bedeutet nicht die Einstellung, von wem der SMTP-Connector Nachrichten aus dem Internet annimmt, sondern welche internen Absender über diesen Connector Ihre Nachrichten nach außen senden können. So kann kontrolliert werden, welche Personen Nachrichten in das Internet senden dürfen. Der Empfang von Nachrichten kann hierüber nicht kontrolliert werden. Sollen einige Anwender keine Nachrichten erhalten, dann dürfen Sie diesen keine gültige SMTP-Adresse geben oder müssen über Empfangsbeschränkungen beim Anwender die Zustellung blockieren.

- Inhaltseinschränkungen

  Die eingestellte Größenbeschränkung verhindert allzu große Nachrichten und ist eine globale Einstellung. Ebenso lassen sich Nachrichten anhand ihrer Priorität filtern.

5.6.4 Empfängerrichtlinien und Nachrichtenformate

Der SMTP-Connector und die virtuellen SMTP-Server sind jedoch nicht die einzigen Punkte, an denen Einstellungen im Bezug auf die Internet-Anbindung vorgenommen werden. Zwei weitere Konfigurationsbereiche steuern direkt das Verhalten des SMTP-Connectors.

- Empfängerrichtlinien

  Anhand der in der Summe aller Empfängerrichtlinien verwendeten SMTP-Domänen liest der Exchange-Server die Domänen aus, für die es Empfänger innerhalb der Exchange-Organisation geben kann. Dies ist zugleich ein Teil der Liste, für die Exchange Nachrichten annimmt. Zu dieser Liste hinzu kommen alle Domänen, die im SMTP-Connector unter Adressraum aufgeführt und mit der Option „WEITERGABE VON NACHRICHTEN AN DIESE DOMÄNEN PER RELAY ERLAUBEN“ versehen sind.

- Nachrichtenformate

  Die zweite Einstellung im Bezug auf das Internet ist die Konfiguration der Nachrichtenformate im Exchange System-Manager. Abweichend von der Standardeinstellung können für weitere Domänen Konfigurationen

bezüglich der Codierung der Nachrichten und die Behandlung von automatisch generierten Nachrichten gesteuert werden.

Halten wir fest:

- Die Einrichtung eines SMTP-Connectors ist notwendig, um erweiterte Funktionen für die Zustellung von Nachrichten zu nutzen, z.B. Versand über einen Smarthost oder Beschränkungen nach Größe oder Absender.
- Ein SMTP-Connector ist erforderlich, wenn mehrere Exchange-Server nur über bestimmte Server die Nachrichten versenden sollen. Erst der SMTP-Connector mit Adressräumen informiert alle Server in der Organisation über mögliche Leitwege und verhindert den direkten Versand über die virtuellen SMTP-Server.
- Mehrere SMTP-Connectoren sind zwangsläufig notwendig, wenn ausgehende Nachrichten abhängig von der Empfängerdomäne, Größe oder Absender unterschiedliche Wege nehmen sollen.
- Ein SMTP-Connector steuert nicht, welche Systeme den Exchange-Server als Relay benutzen oder welche Systeme sich mit dem Exchange-Server verbinden dürfen. Dies ist eine Einstellung der virtuellen SMTP-Server.

6

Weitere Konzepte

6 Weitere Konzepte

Konzepte zu Windows 2003, Active Directory, Exchange und der Internet-Anbindung sind für eine fachmännische Installation wichtig. Aber damit ist es noch nicht getan. Für den Betrieb eines Exchange-Servers sind weitere Details zu definieren und umzusetzen. Dazu gehören die nachfolgend näher erläuterten Themen. Sie sind nicht direkt mit Exchange in Verbindung zu bringen, aber ohne diese sollten Sie keinen Exchange-Server betreiben. Wir haben dazu vier der wichtigen Konzepte herausgegriffen, die auf keinen Fall unberücksichtigt bleiben sollten.

6.1 Serverkonzeption und Dimensionierung

Auf der Webseite von Microsoft gibt es Hinweise zur Mindestausstattung eines Exchange-Servers. Faktisch ist jeder PC, den Sie heute kaufen können, leistungsfähig genug, um Exchange 2003 zu betreiben. Ob Sie jedoch eine neue Installation von Exchange 2003 auf einer älteren Hardware durchführen, sollten Sie sich genau überlegen. Ein einmal installierter Exchange-Server wird sehr schnell zu einer Schlüsselkomponente in Ihrem Netzwerk, und ein Administrator kommt prompt in Erklärungsnot, wenn er nach kurzer Zeit den Server schon wieder umbauen oder ersetzen muss.

6.1.1 Grundvoraussetzungen

Auf jeden Fall sollte der Server einige Mindestvoraussetzungen erfüllen, damit er seiner Aufgabe gerecht wird:

Umgebung und Komponenten des Servers

- Zuverlässige Hardware

  Es gibt durchaus Unterschiede in der Hardware zwischen Servern und Desktops. Ein Server muss 24 h durchlaufen und, wenn er nicht in einem klimatisierten Raum steht, auch bei höheren Umgebungstemperaturen ausreichend belüftet sein. Besonders weil ein Server oft mehrere Festplatten enthält, muss das Netzteil eine entsprechende Dauerleistung und Kühlleistung bereitstellen. Eine Möglichkeit der Überwachung sollte ebenfalls gegeben sein, um den Ausfall oder Leistungsverlust eines Lüfters oder Netzteils rechtzeitig zu erfahren.

- ECC-RAM

  Die Speicherchips sind wichtige Bausteine in Ihrem Server, und kleinste Fehler führen unweigerlich zum Ausfall des Servers. Achten Sie auf Qualität und auf die doppelten Parity-Bits „ECC“ (Error Correction Code). So werden einzelne Defekte erkannt UND korrigiert. Normale Speicher mit einfachem Parity-Bit erkennen zwar Fehler, aber Ihr Server fällt trotzdem aus. Sie wissen nur im Nachhinein, dass ein Speicherfehler die Ursache ist. Allerdings kostet diese zusätzliche Sicherheit etwas mehr.

- Redundante Festplatten

  Festplatten sind mechanische Komponenten, die einem erhöhten Verschleiß unterliegen und sicher ausfallen. Es ist nur die Frage, wann dies passiert. Die Angaben zu Haltbarkeit (MTBF) sind theoretischer Natur, und der Ausfall einer Festplatte ohne entsprechende Absicherung bedeutet immer einen Serverausfall und hohe Folgekosten. Bei den heutigen Festplattengrößen ist ein RAID 1 in der Regel die beste Wahl, da die Geschwindigkeit höher als bei einem RAID 5 ist und meist der gesparte Einbauplatz für spätere Erweiterungen genutzt werden kann.

- Unterbrechungsfreie Stromversorgung

  Deutschland ist ein Land mit einer sehr guten Stromversorgung. Dennoch kann schon ein kleiner Fehler von einem Bruchteil einer Sekunde einen Server „abstürzen“ lassen. Sie sollten Ihrem Server eine USV spendieren. Und wundern Sie sich nicht, wie oft Sie im Laufe eines Jahres auch aktiv wird. So mancher Einschaltvorgang eines Fotokopierers auf der gleichen Phase ist für eine USV ein Grund anzuspringen.

- Datensicherung

  „Online“-Backup

  Ihre Exchange-Daten gehören schneller, als Sie vielleicht heute vermuten, zu den wichtigsten Daten Ihrer Firma. Eine ganze Reihe von Faktoren wie Fehler, unabsichtliches Löschen, Viren und andere Dinge kann diese Daten verändern oder zerstören. Ohne Datensicherung sollten Sie keine Exchange-Installation betreiben. Erst die Datensicherung setzt die Transaktionsprotokolle zurück, damit Ihre Festplatte nicht voll läuft. Sie können Ntbackup oder eine kommerzielle Software nutzen. Sie sollten aber Exchange 2003 immer „online“ sichern. Dazu später mehr.

Entscheiden Sie sich für einen Server Marke „Eigenbau“, dann sollten Sie das System einem längeren Dauertest unterziehen und die Leistung mit einem ähnlichen Server vergleichen. Es wäre nicht das erste Mal, dass eine 100 MBit-Netzwerkkarte am falschen Switch oder im falschen PCI-Slot nur so schnell ist wie eine 10 MBit-Karte.

6.1.2 CPU — Speicher — Festplatte

Exchange beansprucht alle Komponenten eines Servers. Allerdings haben die Bereiche Hauptspeicher und CPU-Leistung in den letzten Jahren stetig zugenommen, so dass die mechanischen Festplatten immer mehr der begrenzende Faktor werden.

CPU

Exchange 2003 unterstützt den Betrieb mit mehreren Prozessoren. Allerdings ist die Zunahme der Leistung begrenzt, da auch mehrere CPUs in der Regel auf eine Information der Festplatten warten. Interessant werden mehrere Prozessoren, wenn zusätzliche Dienste auf dem Exchange-Server ablaufen, z.B. ein Virenscanner, Skripte oder Event Sinks, da dann ein Prozess nicht alle anderen über Gebühr behindert.

Speicher

RAM > 3 GB aktivieren

Exchange war lange Jahre als wahrer Speicherfresser verschrien, weil ein Server nach kurzer Zeit im Task-Manager mehr benutzten Speicher angezeigt hat, als physikalisch vorhanden war. Exchange hatte dabei einen großen Anteil, weil manchmal bis zu 1 GByte und mehr verwendet wurde. Dies müssen Sie aber vor dem Hintergrund sehen, dass es für einen Server keinen Sinn macht, kostbaren Speicher brachliegen zu lassen, und Exchange daher diesen als Cache nutzte. Exchange hat die Eigenschaft, den Speicher sofort wieder freizugeben, sobald eine andere Anwendung diesen benötigt. Allerdings hat Exchange 5.5 selten die 1 GByte-Grenze überschritten. In der Regel hat sich der Bedarf bei ca. 850 MB eingependelt, selbst wenn der Server viel mehr Hauptspeicher hatte. Exchange 2003 nutzt nun mehr Speicher, was aber auch von der Anzahl der Speichergruppen abhängt. Viel zusätzlichen Speicher kann Exchange erst durch den Einsatz der Enterprise Edition mit mehreren Speichergruppen nutzen. Dazu muss aber auch die Windows 2000 Advanced Edition oder Windows 2003 installiert sein, damit Sie die „/3 GB“-Option des Betriebssystems einsetzen können. Auch heute können Sie die meisten Server mit 1 bis 2 GByte ausstatten und damit auskommen.

Festplatten

Aufgrund der Nutzung von Transaktionsdateien ist die Exchange-Leistung sehr stark von diesen Komponenten abhängig. Dies gilt nicht nur für die Datensicherung, sondern auch bei Wartungsarbeiten mit ESEUTIL ist ein schneller Massenspeicher schon sehr hilfreich. Für die meisten Unternehmen zählen bei den Massenspeichern weitere Faktoren:

- Größe

  Volumen auf Basis erwarteter Daten kalkulieren

  Die Nettogröße der Speicherkapazität lässt sich anhand des Platzbedarfs für das Betriebssystem, die zu installierenden Anwendungen und deren erwarteten Nutzdaten ermitteln. Zusätzlich sollte eine Reserve eingeplant werden, damit ein plötzliches Wachstum Ihre Handlungsfähigkeit nicht einschränkt und ausreichend Platz für Recovery, Sicherheitskopien etc. vorhanden ist. Mittlerweile lassen sich Server mit 146 GB-Festplatten bestücken. Dies ist schon viel Platz für einen normalen Exchange-Server, aber noch lange nicht Kapazitätsgrenze. In Anbetracht, dass die Exchange 2003 Standard Edition ein Limit von maximal 75 GB hat, ist in diesem Fall ausreichend Reserve vorhanden.

- Ausfallsicherheit

  Verfügbarkeit mit RAID steigern

  Festplatten sind mechanische Komponenten, deren Lebensdauer begrenzt ist und bei denen ein Ausfall nur eine Frage der Zeit ist. Zwar erlauben Datensicherungen eine Wiederherstellung, dagegen ist der Ausfall und die zusätzliche Arbeit nicht zu vernachlässigen. Schon sehr lange werden daher Techniken angewandt, um den Ausfall einzelner Festplatten abzusichern. Mittels entsprechender RAID-Controller oder der Software-Funktion von Windows 2003 werden Daten auf mehreren Festplatten derart verteilt, dass der Ausfall einer Festplatte keine Unterbrechung bedeutet. Bei entsprechender Hardware kann die defekte Festplatte im laufenden Betrieb getauscht werden (Hot Plug). Ein RAID 5 bietet zwar eine höhere Kapazität, dagegen erkaufen Sie den Speicherplatz mit einer langsamen Performance.

- Verfügbarkeit durch Unabhängigkeit

  Trennung der Daten

  Ein weiterer wichtiger Aspekt ist die Unabhängigkeit der verschiedenen Datenbereiche. Dabei sollten Sie die beiden Risiken beachten, dass Sie entweder durch Defekt oder durch ein Vollschreiben der Partition nicht mehr mit einer Partition arbeiten können.

  Ein Risiko sind hier die Transaktionsprotokolle, die Sie möglichst von der Datenbank trennen sollten. Dies bringt nicht nur eine bessere Performance mit sich, sondern erlaubt die Wiederherstellung bis zum Moment des Ausfalls, wenn nur einer der beiden Datenträger ausfällt. Wenn Ihre Online-Sicherung einige Tage nicht funktioniert, werden die Transaktionsdateien immer weiter geschrieben und füllen die Partition auf. Ein fataler Prozess, wenn dies die Systempartition füllt und letztlich nicht einmal mehr das Betriebssystem weiter funktioniert.

Sie können so langsam einschätzen, wie schwer die Dimensionierung eines Servers fällt, ohne aussagekräftige Informationen über die zu erwartete Nutzung zu besitzen. Daher werden die meisten Server nach dem Motto „Das Beste, was der Geldbeutel hergibt“ dimensioniert, in der Hoffnung, es reicht

aus. Das Ergebnis sind teilweise Server, die nach einigen Monaten schon wieder erweitert oder ersetzt werden müssen, oder Server, die hoffnungslos überdimensioniert und damit ebenfalls sehr teuer für das Unternehmen sind.

6.1.3 Dimensionierung von Exchange

Die richtige Dimensionierung eines Exchange-Servers ist eine der schwierigsten Aufgaben, da die vorausgesetzten Informationen in der Regel nicht bekannt sind.

Zwei Dinge interessieren die Anwender:

- Schnelle Antwortzeiten

  Ein Server muss die Anfragen der Anwender in sehr kurzer Zeit beantworten. Reagiert Outlook träge, dann ist der Ärger vorprogrammiert. Der Server, aber auch das Netzwerk, muss hier in die Betrachtung mit einbezogen werden.

- Ausreichend Platz

  Exchange-Server haben die Eigenschaft, sehr beständig und schnell zu wachsen, da die Anwender immer mehr Informationen in Outlook ablegen und immer mehr Daten als E-Mail versendet werden. Der Server muss auch die entsprechende Kapazität bereitstellen und erweiterungsfähig sein.

Das Problem hierbei ist, dass die Antwortzeit eines Exchange-Servers nicht einfach mit einem PING im TCP/IP zu vergleichen ist, sondern je nach Nutzungsverhalten des Benutzers andere Anforderungen an das System stellt. Das Problem fängt schon damit an, dass in den meisten Unternehmen nicht bekannt ist, wie die Anwender mit der Software arbeiten und welche Antwortzeiten heute akzeptiert werden. Die Hersteller und Microsoft haben entsprechende Simulationen (LOADSIM, MEDUSA, MAILTEST, MMB2) entwickelt, die ein bestimmtes Nutzerverhalten annehmen, um damit einen installierten Server testen zu können. Interessant ist hierbei der Herstellertest eines Servers, der mit verschiedenen Ausbaustufen (CPU, RAM, Festplatten) wiederholt wird und so die Auswirkungen sichtbar macht.

Die namhaften Hersteller publizieren solche White Papers im Internet. Trotzdem ist es schwer, für den eigenen Bedarf ohne entsprechende Vorerhebungen eine qualitative Aussage zu machen. Es bleibt daher meist beim „Viel hilft viel“.

Entwicklung der Daten notieren

Die vermeintlich leichtere Frage ist die Dimensionierung der Festplattenkapazität. Auch hier hat sich schon so mancher Administrator verschätzt. Wenn Sie schon heute Exchange-Server einsetzen und in der glücklichen Lage sind, über regelmäßige Aufzeichnungen der Datenbankgröße der letzten

drei Jahren zu verfügen, dann könnten Sie eine recht zuverlässige Schätzung über die nächsten Monate abgeben.

Die Vergangenheit und Projekte haben indes gezeigt, dass eine zuverlässige Abschätzung in der Regel nicht möglich ist. So wächst eine Datenbank bei der Migration von einem Fremdsystem auch gerne um das Doppelte. Hinzu kommt, dass die Anwender mit Outlook 2003 sehr viel intensiver arbeiten und damit die Datenmenge weiter zunimmt. Insofern gilt auch bei der Planung der Festplattenkapazität, immer die größeren Festplatten zu wählen und Platz für die nächste Erweiterung vorzusehen. Freier Platz ist bei Exchange auch erforderlich, um entsprechende Reserven für Defragmentierungen, Wiederherstellungen und Protokolldateien zu haben. Das 18 GB-Limit der Exchange Standard Edition mit SP2 können Sie bei Bedarf auf 75 GB anheben (siehe TechNet-Artikel 912375). Bei Erreichung des Limits sollten Sie jedoch umgehend Maßnahmen ergreifen, um den Server wieder langfristig betriebsbereit zu stellen. Als Alternative stehen das Archivieren der alten Informationen und damit das Reduzieren der Datenbank zur Verfügung sowie auch das Update auf die Exchange Enterprise Edition mit allen Service-Packs.

6.1.4 Funktionstrennung

Aufgaben des Exchange-Servers

Als weiterer Punkt bei der Planung eines Servers ist die Trennung der Funktionen zu nennen. Auf Basis der Exchange-Organisationsstruktur können Sie weitere Server installieren, die bestimmte Funktionen übernehmen. Neben den Kosten für zusätzliche Hardware und Lizenzen gewinnen Sie jedoch durch einfachere Server mit weniger Belastung und geringerer Fehleranfälligkeit. Beim Bedarf neuer Hardware haben Sie die Wahl, diesen komplett zu ersetzen oder durch einen zweiten Server zu ergänzen, der die arbeitsintensiven Aufgaben erledigt. Zwei kleinere Server sind oftmals stabiler und leistungsfähiger als ein Gigant, der aufgrund der Kombination aller Funktionen auf einem System weniger verfügbar ist.

Trennen nach Aufgaben

Die Aufgabentrennung hat auch aus Sicherheitsaspekten einiges für sich. Mit Exchange 2003 können Sie die folgenden Funktionen unterscheiden und entsprechend trennen:

- Postfachserver

  Server, die Postfächer der Mitarbeiter halten und den Zugriff darauf gewähren (Mailbox-Server). Diese Daten sind leider nicht replizierbar, so dass dieser Server entsprechend verfügbar sein sollte. Eine höhere Verfügbarkeit ist mittels *Microsoft Cluster Services* möglich.

- Öffentliche Ordner-Server

  Diese Serverfunktion erlaubt den Zugriff auf Öffentliche Ordner. Schon allein die Trennung vom Postfachserver erlaubt eine Skalierung. Hinzu kommt, dass Öffentliche Ordner auf mehrere Server repliziert werden können und damit auch ohne Cluster eine Ausfallsicherheit bieten. Exchange-Server mit mehreren Gigabyte Daten in einem Ordner und mehrere hundert Gigabyte in der Gesamtstruktur sind bestätigt.

- Routing- und Connector-Server

  Sie können eigene Server vorsehen, die nur für die Übermittlung von Nachrichten zuständig sind. Der Vorteil hierbei ist, dass diese Server in einem Notfall auch problemlos heruntergefahren werden können, bis z.B. der Virenscanner das aktuelle Pattern-File hat. In der ganzen Zeit können die Mitarbeiter intern weiterarbeiten. Durch mehrere Server ist auch hier einfach eine Ausfallsicherheit realisierbar. Oftmals werden in einer Exchange-Organisation weitere Dienste wie Fax, SMS etc. integriert. Solche Server werden zusätzlich mit Fax- und ISDN-Karten sowie zusätzlicher Software ausgestattet. Auch für solche Dienste bietet sich ein eigener Server an, um bei Updates und Problemen nicht die komplette interne Kommunikation lahm zu legen.

- Front-End-Server

  Eine Besonderheit der Exchange 2003-Server ist die Funktion als Front-End-Server. Diese nehmen die Verbindungen von Internet-Clients (OWA/OMA/POP3/IMAP/RPC over HTTP) an und leiten sie zum richtigen Postfachserver weiter. Dabei können diese Server nicht nur die Autorisierung, sondern auch die Verschlüsselung per SSL und die Lieferung statischer Inhalte (Icons und Java-Klassen bei OWA) übernehmen und damit den Postfach-server im Hintergrund entlasten. Zusätzlich erhöht solch eine Konfiguration die Sicherheit der Postfachserver, die nicht mehr direkt erreichbar sind. Auch für den Anwender wird der Zugriff leichter, da sie sich immer mit dem gleichen Front-End-Server verbinden und der eigentliche Postfachserver nicht offensichtlich ist.

- Active Directory

  Exchange-Server müssen keine Domänencontroller und Globale Katalog-Server sein. Je größer und komplexer eine Umgebung wird, desto eher ist es anzuraten, die Funktion des DC auf eigene Systeme zu verlagern. Somit wird der Exchange-Server entlastet und kann seiner Kernaufgabe viel besser gerecht werden. Ein fälliger Neustart eines Exchange-Servers beeinträchtigt dann nicht auch alle anderen Dienste, die vom Active Directory abhängig sind. Eine nachträgliche Änderung der Rolle (DCPROMO) des Exchange-Servers wird von Microsoft nicht unterstützt.

Durch die Trennung von Funktionen vereinfacht sich die Konfiguration jedes einzelnen Servers, und die Ausfälle durch Update, Inkompatibilitäten und zu hohe Belastungen reduzieren sich. Demgegenüber steht natürlich der Aufwand für zusätzliche Hardware und Lizenzen.

6.1.5 Beispiel: Serverkonfiguration

Auf die Frage „Welche Hardware brauche ich für Exchange?“ gibt es daher keine pauschale Antwort. Mittlerweile sind die meisten modernen Server so schnell, dass für mittlere und kleine Unternehmen mit normalen Anforderungen fast jeder Server prinzipiell geeignet ist. Sofern Sie keine vorhandene Exchange-Umgebung besitzen, die als Vergleich herhält, und auch die Zeit und die Mittel für eine Analyse nicht vorhanden sind, dann werden Sie wohl oder übel mit einem Restrisiko einen Server konfigurieren und installieren. Unter Umständen bauen Sie den Server in einem halben Jahr schon wieder um. Dieser Prozess ist gerade im Bereich Messaging oft nicht zu verhindern, da neue Möglichkeiten der Software von Mitarbeitern entdeckt und genutzt werden, die wesentlich mehr Volumen produzieren.

Berechnung der Kapazität

Die folgenden Überlegungen können als Muster für einen Serverentwurf eines kleinen Unternehmens mit einem Standort dienen:

Vorgaben

20—100 Benutzer

ca. 20—50 MB durchschnittlich pro Postfach/User

ca. 5 GB in Public Folder

ca. 100 MB E-Mailtransfer insgesamt je Monat

Mit diesen Vorgaben ist ein Postfachspeicher von bis zu 5 Gigabyte zu erwarten. Selbst wenn die Postfächer im Mittel auf 100 Megabyte anwachsen, sind Sie mit 100 Anwendern schon bei 10 Gigabyte. Aber auch dies ist für heutige Systeme keine „gefährliche“ Datenmenge mehr.

Auch bei den Prozessoren ist die 2 GHz-Grenze schon länger überschritten, so dass der Engpass eines Servers heute eher bei den Festplatten zu suchen ist. Diese haben mit der rasanten Entwicklung der Prozessoren, Hauptspeicher und Netzwerke nicht richtig Schritt gehalten. Viele Server sind aber auch nur deshalb langsam, weil die Clients aufgrund fehlerhafter Namensauflösung den Server nicht sofort auflösen können.

Die Festplatten

Wichtig bei Festplatten ist daher die Leistung und Verfügbarkeit. Im Hinblick auf die Verfügbarkeit ist der freie Platz auf den Partitionen am wichtigsten, da Exchange sich sonst selbstständig herunterfährt. Damit

zumindest das Betriebssystem weiter funktioniert, sollten die variablen Nutzdaten vom Betriebssystem getrennt sein, z.B. in eine eigene Partition.

Natürlich ist es optimal, wenn für die Datenbereiche System, Programme, Swap-File, Exchange-Datenbank und Transaktionsprotokolle eigene Speichersysteme bereitstehen. Aber im Extremfall würde dies bis zu fünf eigenständige logische Festplatten bedeuten, die durch den Einsatz von RAID zu einer Vielzahl von physikalischen Festplatten führen. Solche Designs mit SAN und externen Speichern sind für große Installationen gang und gäbe, aber für unseren Musterserver, der uns in den nachfolgenden Kapiteln begleitet, müssen Kompromisse geschlossen werden.

RAID

Durch die heute verfügbaren Festplattengrößen ist der Einsatz von RAID 5 nicht mehr zwingend erforderlich. Zwar kosten drei Festplatten weniger als zwei doppelt so große Festplatten, allerdings sparen wir einen Einbauplatz und haben die für RAID 1 höhere Performance.

Sie könnten Ihren Server mit zwei 72 GB-Festplatten oder größer ausstatten, welche als RAID 1 verschaltet sind. Nur extrem sparsame Naturen verbauen zwei IDE-Festplatten, die mit Windows gespiegelt werden. Dies ist in der Anschaffung die preiswerteste Variante, nicht jedoch im Betrieb. Ein RAID-Controller, der dem Betriebssystem die Arbeit abnimmt und beim Ausfall der ersten Festplatte trotzdem noch bootet, sollte der absolute Mindeststandard für einen Exchange-Server sein. Größere Festplatten sind natürlich sinnvoll, wenn Sie ein hohes Datenvolumen erwarten oder zusätzliche Dienste auf dem gleichen Server betreiben möchten. In der Regel sind größere Festplatten durch die höhere Datendichte auch schneller, und Sie erhalten länger Ersatz.

Es macht jedoch keinen Sinn, in einem RAID-Verbund mehrere logische Festplatten zu konfigurieren, da diese weder im Hinblick auf die Ausfallsicherheit noch die Zugriffe getrennt sind. Sie könnten daher aus zwei Festplatten ein RAID 5-Pack definieren, indem eine große logische Festplatte à 72 GB eingerichtet wird. Diese kann unter Windows dann in Partitionen aufgeteilt werden.

Partitionierung

Die Partitionierung von Servern hängt vom geplanten Einsatz ab und ist immer ein Spagat zwischen der Abtrennung von Datenbereichen und dem Risiko, dass bei vielen Partitionen eine Partition zu klein geplant wird, während andere Partitionen viel ungenutzten Platz besitzen. Nutzen Sie daher so wenige Partitionen wie möglich, aber so viel wie notwendig.

Sinnvolle Einteilung

Unbestritten ist eine eigene Partition für das Betriebssystem sinnvoll, damit variable Bestandteile der Benutzer und Anwendungsdaten nicht überraschend Ihr System außer Funktion setzen.

Eine eigene Partition für die Auslagerungsdatei wie bei Unix-Systemen üblich ist bei Windows nicht zwingend. Wenn Sie gleich am Anfang eine entsprechend große unveränderliche Auslagerungsdatei anlegen, dann ist auch die Fragmentierung kein Thema mehr. Allerdings kann die Auslagerungsdatei nur bis zu 4096 MB groß werden. Sehr große Server mit noch größeren Speicheranforderungen müssen daher die Auslagerungsdatei auf mehrere Partitionen verteilen.

Da der Musterserver für die nächsten Kapitel nur eine logische Festplatte hat, macht eine Trennung der Exchange-Datenbank und der Transaktionsprotokolle in verschiedene Partitionen wenig Sinn. Eine zweite Partition wird angelegt, in der später alle Daten abgelegt werden.

Hauptspeicher und CPU

Heute sind Server mit zwei und mehr Gigabyte Hauptspeicher keine Seltenheit mehr. Lange Zeit mussten Sie die Kombination Windows 2000 Advanced Edtion und Exchange 2000 Enterprise Edition kaufen, um den Speicher effektiv nutzen zu können. Erst Windows 2003 erlaubt auch in der Standardversion die sinnvolle Nutzung größerer Speichermengen. Aber selbst dann ist erst der Exchange Enterprise-Server mit mehreren Speichergruppen dazu geeignet, den Speicher effektiv zu nutzen.

Der Musterserver bekommt jedoch nur eine Speichergruppe mit zwei Datenbanken, und in der Regel nutzt Exchange in diesem Betrieb selten mehr als ein Gigabyte Hauptspeicher. Wenn Sie noch etwas Reserve für Virenscanner, Datensicherung, Betriebssystem etc. einplanen, dann sollten Sie mit 1,5 Gigabyte problemlos hinkommen. Achten Sie bei der Bestellung darauf, dass noch Speicherbänke für eine Nachrüstung frei sind, d.h. nicht alle Bänke sollten durch kleine Module belegt sein, die bei einer späteren Erweiterung dann ausgetauscht werden müssten.

Die CPU ist zwar wichtig, jedoch sind alle neuen Server mittlerweile so gut ausgestattet, dass die Unterschiede nur noch minimal sind. Anhand eines vorhandenen Servers können Sie die aktuelle Belastung abschätzen. Wenn Sie nicht gerade den Volltextindex von Exchange aktivieren, sollten heutige CPUs keine Probleme mit den gemachten Annahmen haben.

Netzwerk

Die Anbindung an das Netzwerk ist für einen Exchange-Server im Vergleich zu einem Dateiserver oder Datensicherungsserver nicht so kritisch zu sehen. Startet nicht gerade ein Outlook 2003-Anwender seine erste Replikation für den Offline-Betrieb oder Cached Mode, dürfte für die Vorgaben jede 100 MBit-Karte ausreichend sein. Wird der Exchange-Server jedoch auch für andere Dienste genutzt oder über das LAN gesichert, dann ist dies zu berücksichtigen. Prüfen Sie aber auf jeden Fall, dass die Netzwerkkarte auch

wie erwartet funktioniert und nicht durch eine Inkompatibilität zwischen Karte und Switch oder falschen Treiber sowie fehlerhafte Konfiguration die nutzbare Übertragungsrate reduziert wird. Programme wie NETIO und TTCP oder auch einfach nur ein einfacher COPY-Befehl über das Netzwerk eignen sich als Kontrollmittel.

6.2 Datensicherung

Es ist ein schönes Gefühl, wenn Ihr Exchange-Server endlich installiert ist und wie gewünscht funktioniert. Und ein zuverlässiger Server mit redundanten Festplatten erlaubt einen längeren stabilen Betrieb, bei dem selbst der Ausfall einer Festplatte oder eines Netzteils nicht gleich den Administrator und die Anwender verzweifeln lassen. Trotzdem sind redundante Festplatten, Lüfter und weitere Komponenten kein Ersatz für eine Datensicherung. Das Backup ist keine Kür, sondern eine notwendige Pflicht, und der Einsatz muss gut überlegt und geplant sein.

6.2.1 Anforderungen an die Datensicherung

Die Sicherung der Daten auf Computersystemen verfolgt mehrere Ziele:

Backup & Restore

- Schnelle Wiederherstellung des letzten Standes

  Nach dem Ausfall einer Festplatte oder eines kompletten Servers müssen die Daten möglichst aktuell wieder hergestellt werden. Dieser Fall ist aufgrund der Datenmenge auch der umfangreichste Prozess.

- Rollback einer Installation

  Durch die Installation von Updates und Service-Packs kann ein nicht funktionsfähiger Zustand entstehen. Eine Wiederherstellung des vorherigen Standes ist erforderlich.

- Wiederherstellung gelöschter Elemente

  Oft werden unabsichtlich oder vorsätzlich bestimmte Informationen gelöscht. Dies kann eine Datei sein, ein Benutzer im Active Directory, aber auch eine E-Mail oder ein Öffentlicher Ordner. Eine Sicherung muss auch diese Wiederherstellung ermöglichen. Das Restore ist oft auch der einzige Weg, durch Virenbefall veränderte Daten zu restaurieren.

- Wiederherstellung älterer Versionen

  Dateien verändern sich im Laufe der Zeit. Ohne Archivsystem ist es fast unmöglich, eine frühere Version zu behalten, da die meisten Anwender neuere Versionen mit dem gleichen Namen wieder ablegen. Dies ist aber rechtlich nicht ganz unproblematisch. Die Wiederherstellung älterer Versionen ist daher auch eine Aufgabe der Sicherung. Hier ist es natürlich

notwendig, entsprechende Generationen zu führen und auch langfristig vorzuhalten. Besonders bei Viren, die erst lange Zeit nach der Infizierung aktiv werden, sind mehrere Versionsstände der betroffenen Daten für die Wiederherstellung erforderlich.

- Sonderfälle

  Die Kapazität eines Bandlaufwerks kann auch dazu genutzt werden, große Datenbestände zwischen Standorten auszutauschen oder beim Austausch eines Servers die Daten zu übernehmen.

Dabei ist natürlich zu beachten, dass eine Datensicherung immer nur eine Momentaufnahme zu einem bestimmten Zeitpunkt sein kann und zwischen dem Vorfall und der letzten Sicherung eine Lücke klafft, die nur sehr kostenintensiv minimiert werden kann. Lösungsansätze sind hier Archivsysteme oder häufige zusätzliche inkrementelle Sicherungen.

6.2.2 Datenbeständigkeit und Sicherungsverfahren

Um den Bedarf an Bändern und Wechselaktionen als auch die Laufzeit der Sicherung und die Größe des Wechslers zu bestimmen, sind bestimmte Faktoren zu definieren:

- Datenmenge und Wachstumsprognose

  Die Abschätzung der Kapazität ist eine Erfassung der aktuellen Datenmenge und der zukünftigen Entwicklung. Eine sorgfältige Analyse ist hier besonders wichtig, da Bandlaufwerke in der Regel auf einen längeren Zeitraum als der Server selbst angeschafft werden. Eine Datensicherungslösung sollte einige Jahre nutzbar oder zumindest einfach erweiterbar sein. Die Menge ist auch in Hinblick auf den Einsatz eines Wechslers oder SANs und für die Bestellung ausreichender Bänder wichtig.

- Die maximal verfügbare Zeit für die Wiederherstellung der Daten SLA

  Ermitteln Sie den Wert für die maximal erlaubte Zeit einer Wiederherstellung der Daten und Funktion (SLA). Ziehen Sie die Zeit für die Reparatur der Hardware ab. In der verbliebenen Zeit müssen Sie den Server wieder restaurieren können. Diese Dauer ist maßgeblich für die Auswahl der Übertragungswege und Bandtechniken, aber auch für die Entscheidung zu alternativen zusätzlichen Sicherungsmethoden (Backup-to-Disk, Schattenkopie, Spiegelung). In Zeiten von Servern mit über 100 Gigabyte und Bandlaufwerken mit Durchsätzen von 20 GB/h wird hier schon deutlich, dass ein Laufwerk in dieser Konstellation nicht mehr ausreicht oder das SLA weiter gefasst werden muss.

- Das Zeitfenster für die Sicherung der Daten

  Zwar ist die Wiederherstellung der kritischere Bestandteil, aber auch die Sicherung selbst sollte regelmäßig in bestimmten Zeitfenstern ablaufen. Eine Sicherung zur Betriebszeit beeinträchtigt die Nutzung der Daten, teilweise durch die Verringerung der Performance, aber auch durch die Nichtverfügbarkeit, wenn zur Sicherung einige Dienste beendet werden. Exchange sollte ebenfalls nicht gerade dann gesichert werden, wenn die Online-Defragmentierung läuft oder ein Volltextindex aktualisiert wird.

- Die Anzahl der Generationen bzw. Versionen

Großvater-Vater-Sohn-Prinzip

  Die Wiederherstellung der letzten Version benötigter Informationen ist nicht allein ausschlaggebend. Oftmals ist auch ein Rückgriff auf frühere Versionen erforderlich. Ebenso sollten Sie den Fall einkalkulieren, dass das letzte Backup vielleicht fehlgeschlagen oder das Speichermedium nicht mehr lesbar ist.

- Größte Verlustzeit

  Auch bei regelmäßiger Sicherung existieren Daten, die nicht mehr wiederhergestellt werden können. Dies betrifft alle Daten, die nach der letzten Sicherung bis zum Moment des Ausfalls erstellt oder verändert wurden. Diese Daten sind nicht in der aktuellsten Version gesichert. Auf Basis einer täglichen Sicherung betrifft dies in der Regel alle zwischen Arbeitsbeginn und Ende der Sicherung oder zum Ausfall angefallenen Daten. Der Verlust kann bis zu einem kompletten Arbeitstag reichen. Diese Menge kann z.B. durch inkrementelle Sicherungen während des laufenden Tages reduziert werden.

Aufgrund der täglich zunehmenden Datenmenge wird es immer schwerer, die Daten als Komplettsicherung täglich auf Bänder zu sichern. Solange alle Daten auf ein Band passten, wurde früher einfach täglich eine Vollsicherung durchgeführt. Der Prozess war zugleich einfach zu handhaben und erlaubte eine schnelle Wiederherstellung.

Limitierung unterstützt Backup/Restore

Exchange 2003 Service Pack 2 bietet nun die Möglichkeit, die Datenbanken zu begrenzen. Dies stellt einen interessanten Ansatz für das Backup- und Restore-Verfahren dar. Somit kann zum Beispiel die Wiederherstellung einer Exchange-Datenbank innerhalb einer vorgegebenen Zeit gewährleistet werden sowie die Größe der Backup-Tapes für eine Storage Group ausreichen.

Bei den heutigen Datenmengen ist eine tägliche Komplettsicherung nicht mehr die Regel, da die dabei anzusetzenden Bandlaufzeiten und die Belastung der Infrastruktur ebenfalls Kosten darstellen. Aus diesem Grunde werden immer mehr angepasste Sicherungen geplant, bei denen häufig nur die Veränderungen gesichert werden. Hier gibt es zwei Ansätze:

- Sicherung nach Zeit/Änderung

  Differenzen sichern

  Die meisten Desktop und Serverprodukte wie ARCserve, BackupExec, Tapeware und andere sichern in vorgegebenen Zeitintervallen. Bei einem Voll-Backup werden alle unveränderten Dateien immer wieder mitgesichert. In Umgebungen ohne Wechsler oder begrenztes Bandvolumen erweist sich dies auch als sinnvoll. Schwerpunkt ist hierbei die Wiederherstellung des letzten Standes und einiger vorheriger Versionen. Durch die mehrfache Sicherung gleicher Daten werden die Bänder nicht optimal genutzt im Sinne der Platzökonomie. Die Wiederherstellung erfolgt allerdings sehr schnell. Ändern sich Dateien jedoch täglich, dann wird auch bei jeder inkrementellen Sicherung die gleiche Datei nochmals gesichert.

- Sicherung nach Version

  Programme wie TSM (Tivoli) erlauben eine Sicherung von Versionen und Änderungen und sparen die Vollsicherungen und damit auch den Bandbedarf ein. Warum sollte ein Sicherungsserver die gleiche Datei eine Woche später erneut sichern, wenn diese schon zuvor gesichert wurde? Über die Speicherung von Versionen ist ebenfalls ein Zugriff auf frühere Informationen möglich. Dateien, die selten geändert werden, sind dabei sehr viel länger wieder herstellbar.

Beide Ansätze haben Ihre Vor- und Nachteile und sind entsprechend den Anforderungen zu prüfen. Kleinere und mittlere Umgebungen sichern meist die Daten auf Bänder und nutzen den Zeitfaktor als Schlüssel. Große Installationen nutzen eher die Version der Daten als Kriterium.

6.2.3 Sicherungsvarianten

Nachdem sowohl die Menge, der Zeitbedarf und die Software diskutiert wurden, steht nun die Überlegung an, wie die Datenmenge zu sichern ist.

Sehr schnell wird klar, dass ab einem bestimmten Datenvolumen eine tägliche Vollsicherung nicht mehr praktikabel ist. Zum einen wird der Bedarf an Bandmaterial sehr hoch, und sowohl die Betriebszeiten der Bandlaufwerke als auch die Last der Systeme lassen hiervon Abstand nehmen. Somit wird es auf eine Mischform der drei Basisroutinen hinauslaufen.

- Voll-Backup

  Prinzip der Verfahren

  Der komplette Server wird zu einem bestimmten Zeitpunkt gesichert. Für ein Restore wird nur der letzte Bandsatz und wenig Zeit benötigt. Allerdings werden recht viele Bänder gebraucht, und das Voll-Backup bedeutet lange Sicherungslaufzeiten. Das erste Backup nach einer Installation ist immer eine Vollsicherung.

- Differenzielles Backup

  Basierend auf der letzten Vollsicherung (z.B. vom Samstag) werden die Veränderungen seit diesem Zeitpunkt gesichert. Damit ist die Datenmenge am Montag meist gering und wird bis zum Donnerstag immer größer. Mit verschiedenen Bändern für jeden Wochentag wird für das Restore immer das letzte Voll-Backup und das letzte Band des differenziellen Backups benötigt. Dies spart Bänder und Laufzeit, aber die Wiederherstellung ist etwas aufwändiger.

- Inkrementelles Backup

  Hierbei werden einfach die Änderungen zum letzten vollen oder inkrementellen Backup gesichert. Die Sicherung geht sehr schnell und spart Ressourcen. Aber zur Wiederherstellung sind neben dem letzten Voll-Backup auch alle Zwischenschritte hintereinander einzuspielen. Dies benötigt wesentlich mehr Zeit, und alle Bänder müssen intakt sein.

Online-/Offline-Backup

Für die Sicherung von Dateien sind diese Verfahren einfach zu verstehen. Aufwändiger wird es bei der Sicherung von Datenbanken, wie sie auch von Exchange verwendet werden. Eine Differenzsicherung bei einem Offline-Backup entspricht der Vollsicherung, da die Datenbank eine physische Datei ist und selbst die kleinste Änderung immer eine Sicherung der gesamten Datei bedeutet. Beim Online-Sicherungsverfahren ist die Differenz meist geringer, da nur die seit der letzten Vollsicherung angelegten Protokolldateien der Datenbank gesichert werden.

Arbeitet die Datenbank mit Protokolldateien, die weiter geschrieben werden, dann enthalten diese Protokolldateien alle Änderungen seit dem letzten Voll-Backup. Beim Restore kann die Datenbank dann anhand dieser Protokolldateien wieder einen „Roll-Forward“ durchführen. Dies gilt auch für Exchange-Server. Interessant ist hier, dass die Datenbanken bei der richtigen Produktwahl auch „online“ gesichert werden können, das heißt, die Datenbanken müssen zur Sicherung nicht vom Netz genommen werden.

Letztlich ist die Konzeption der Sicherung immer ein Kompromiss zwischen Laufzeit, Bandverbrauch sowie dem Aufwand und damit eine individuelle Entscheidung.

Unter dem Zeitdruck einer Wiederherstellung sollten Sie einen fertigen Plan mit Handlungsanweisungen bereitliegen haben. Besonders wenn Sie eher selten etwas restaurieren müssen. Der erste Punkt auf der Liste sollte lauten:

Aktivieren Sie den Schreibschutz an der Bandkassette!

Es bietet sich an, mindestens einmal im Jahr die Funktion der Datensicherung in einem Testfeld zu überprüfen oder dies überprüfen zu lassen.

6.2.4 Serverklassen für Datensicherung

Um die Kosten und den Aufwand für Datensicherung und Recovery zu ermitteln, werden die Server in bestimmte Funktionen und Datenmengen aufgeteilt. Die Kombination von bestimmten Aufgaben auf einem Server ist möglich, wenn Kostenaspekte und geringere Anforderungen an Verfügbarkeit und Unabhängigkeit toleriert werden können. Dies ist in der Regel bei kleinen Standorten möglich. Die wesentliche Unterscheidung der Server kann anhand der Größe erfolgen. Hierbei können drei Klassen unterschieden werden:

Datenvolumen definiert Restore-Zeit.

- Kleine Server bis 40 GB

  Diese Server sind klein genug, um über das LAN auf einem Backup-Server gesichert zu werden. Die Zeiten der Wiederherstellung betragen wenige Stunden. Weder der Einbau lokaler Bandlaufwerke noch der Anschluss an SAN-Systeme ist erforderlich und rentabel.

  Je nach Leistung der Bandlaufwerke oder der Netzwerkverbindung erfolgt die Sicherung direkt auf die Bandlaufwerke oder zuerst auf eine Festplatte, um die Bandlaufwerke besser auszulasten.

  Diese Datenmengen sind in ca. zwei bis vier Stunden restauriert, bei einem Netzwerk-Restore (100 MBit).

- Mittlere Server 40–200 GB

  Diese Server sind zu groß, um sie in akzeptabler Zeit über das Netzwerk zu sichern. Daher ist in der Regel eine lokale Sicherung über ein lokales Bandlaufwerk oder eine Tape-Library im SAN anzuraten.

  Diese Datenmengen können mit aktuellen LTO- oder SDLT-Laufwerken in bis zu fünf Stunden wieder hergestellt werden.

- Große Server > 200 GB

  Diese Server sind zu groß, um sie über klassische Medien in ausreichender Zeit nach einem Ausfall wiederherzustellen. Hier sind andere Wege zur Bereitstellung gefordert. Zum Tragen kommen hier SAN-Systeme, die über Snapshots und andere Techniken eine schnelle Wiederherstellung erlauben. Eine Dateisicherung ist trotzdem notwendig, um auch einzelne Daten und ältere Versionen wiederherzustellen. Die Sicherung erfolgt z.B. über im SAN verfügbaren Bandspeicher.

Folgende Größen sind für bestimmte Server zu erwarten:

Tabelle 6.1 Server und ihre Sicherungsverfahren

Datengröße	bis 40 GB	40–200 GB	Über 200 GB
Infrastrukturserver: Diese DC-, DNS-, WINS-, DHCP-Server sind klein, und teilweise ist eine Sicherung durch die Redundanz nicht relevant.	Remote über LAN oder auf Backup-Server		
Backup-Server: Diese Serverfunktion sichert andere kleine Server mit und dient zur Synchronisation für SAN-Laufwerke. Der Server hat in der Regel größere lokale Festplatten, um temporär Backup-Daten über das LAN anzunehmen und später auf Band zu verlagern. Teilweise ist ein SAN-Anschluss notwendig, um Bandlaufwerke im SAN zu nutzen oder SAN-Festplatten zu sichern.		Lokales Bandlaufwerk oder SAN-Tape	Lokales Bandlaufwerk oder SAN-Tape
Dateiserver: Je nach Niederlassung sind die Dateiserver unterschiedlich groß. Entsprechend sind die Sicherungen zu planen und zu installieren.		Lokales Bandlaufwerk oder SAN-Tape	SAN-Festplatten mit erweitertem Schutz
Druckserver: Neben der Betriebssysteminstallation und den Druckertreibern befinden sich hier nur temporäre Daten der Spool-Dateien. Diese sind kaum zu sichern. Denkbar ist sogar, nur mittels PRINTMIG die Konfiguration zu sichern und statt einer Wiederherstellung eine Neuinstallation mit dem Einspielen der letzten Konfiguration durchzuführen.	Remote über LAN oder auf Backup-Server		
Messaging-Server: Exchange- und Notes-Server sind meist unter 200 GB, da üblicherweise dann eine Verteilung auf mehrere Systeme durchgeführt wird. Kleine Server können über den Backup-Server gesichert werden, mittlere auf Band.	Remote über LAN oder auf Backup-Server	Lokales Bandlaufwerk oder SAN-Tape	

Datengröße	bis 40 GB	40–200 GB	Über 200 GB
Connector-Server: Diese Server halten in der Regel keine Nutzdaten, sondern sind nur Durchgangsserver. Klassisch sind dies Exchange-Connector-Server, Fax-Server, SMS-Server etc.	Remote über LAN oder auf Backup-Server		
Anwendungsserver: Hierunter fallen verschiedene andere Server: Datenbankserver, Virenverteilserver, Multicash und andere. In der Regel sind die Datenmengen klein oder mittel.	Remote über LAN oder auf Backup-Server	Lokales Bandlaufwerk oder SAN-Tape	
Terminalserver: Als Anhäufung vieler Workstations in einem System sind die lokalen Datenmengen eher gering. Es handelt sich um das Betriebssystem, installierte Anwendungen und temporäre Profile der Anwender. Oft werden mehrere Server als Redundanz bereitgestellt, so dass die Recovery-Zeit nicht im Bereich von Stunden sein muss.	Remote über LAN oder auf Backup-Server		

6.2.5 Sicherungsplanung

Für die Planung der Sicherung sind eine Betrachtung der Daten, die Haltbarkeit und das Sicherungsverfahren (= Laufzeit) von Belang.

Tabelle 6.2 Sicherungsplanung und Generationen

Auswahl	Alter/Detail ODER Generationen	Sicherungstag	Sicherungsverfahren
Alle Daten	14 Tage/Tag, 5 Generationen	Montag bis Donnerstag	Dateien: DIFF* SQL: FULL* Exchange: FULL*
Alle Daten	3 Monate/Woche, 12 Generationen	Freitag	FULL*
Alle Daten	2 Jahre/Monat, 24 Generationen	Freitag	FULL*
Wichtige Daten	2 Stunden, 5-6 Generationen	Mehrfach am Tag	DIFF*

Auswahl	Alter/Detail ODER Generationen	Sicherungs-tag	Sicherungs-verfahren
Mailboxen	1 Jahr/Monat, 12 Generationen	1. des Monats	Single Instance Backup
Statische Daten (Bilder, Archiv, Quellen)	Nach Bedarf	Manuell	FULL*
Betriebssystem (*System State*)		Täglich	FULL*

```
* FULL = Voll-Backup, DIFF = Differenz-Backup
```

6.2.6 Voraussetzungen für ein erfolgreiches Backup

Exchange 2003 speichert alle Informationen in einer transaktionsorientierten Datenbank ab. Gemäß der Vorgabe, dass Exchange rund um die Uhr betriebsfähig ist, muss die Datenbank auch zu sichern sein, während Exchange darin aktiv Änderungen vornimmt. Die Dateien sind permanent geöffnet, und nur über entsprechende Schnittstellen kann der Exchange-Server gesichert werden. Diese Schnittstelle sorgt auch dafür, dass Exchange nach dem erfolgreichen Backup die Transaktionsdateien löscht und den Festplattenplatz freigibt.

Um eine komplette Sicherung des Servers zu haben, müssen Sie folgende Bereiche sichern:

- Dateisystem

  Sie sollten alle lokalen Platten (C:, D:, E: etc.) sichern, damit Sie im Falle eines Defektes auch die Programme auf dem Server wieder restaurieren können. Das Laufwerk M: dürfen Sie aber NICHT sichern!!!

Keine „Open File"-Sicherung

  Ebenso können Sie mit dem Datei-Backup einige Dateien nicht sichern, da sie permanent offen sind. Diese werden meist über spezielle Schnittstellen trotzdem gesichert. Um die Anzahl der späteren Fehlermeldungen zu reduzieren, können Sie die gesperrten Dateien (WINS, DHCP, temporäres Verzeichnis und alles in MDBDATA) ausschließen. Nach dem ersten Voll-Backup finden Sie diese Dateien im Fehlerprotokoll der Sicherungssoftware.

- Windows 2003-Systemstatus

System State

  Damit werden das Betriebssystem, die SAM, die Registrierung, COM-Objekte und alles Weitere gesichert, das nicht über ein Datei-Backup der Betriebssystempartition gesichert werden kann. Hier befindet sich auch die Active Directory-Datenbank der Domänencontroller.

- Exchange-Informationsspeicher

  Hiermit wird „online“ der Exchange-Speicher gesichert. Dies können durchaus mehrere Speichergruppen und Datenbanken sein als auch Zusatzdienste wie der SRS.

  Private & Public Store's

- Einzelinstanzsicherung der Mailboxen und Öffentlicher Ordner

  Hierbei handelt es sich nur um eine optionale zusätzliche Sicherung, die jedoch eher als Export zu bewerten ist, da nur die Mailbox-Inhalte gesichert werden. Diese Variante bietet keinerlei Ersatz zur Sicherung des Informationsspeichers und ist immer nur zusätzlich zu sehen.

Eigentlich ist es doch ganz einfach, ein Backup zu fahren, doch weit gefehlt. Sie sollten nicht nur täglich ein erfolgreiches Backup durchführen, sondern dies regelmäßig kontrollieren. Weiterhin sollten Sie ab und an den Restore des Backups auf einem Testsystem verifizieren.

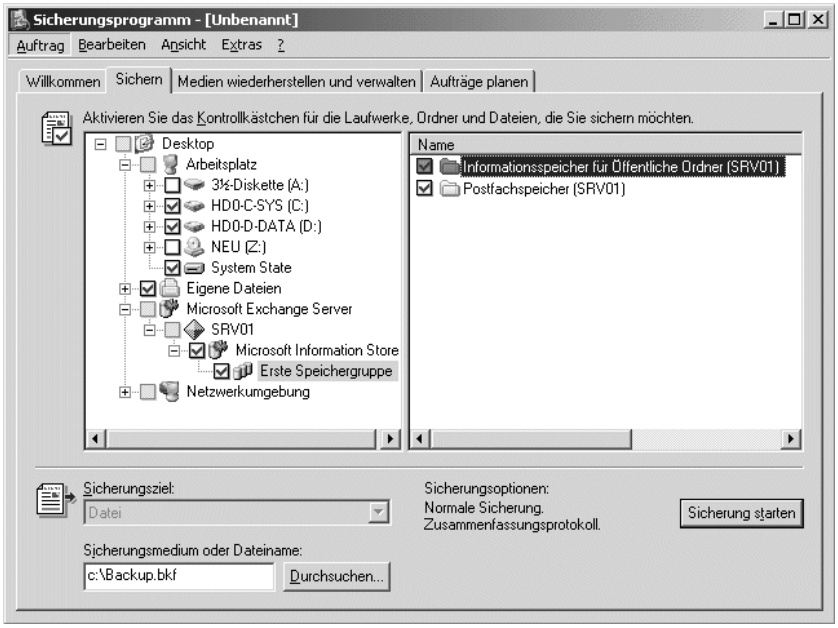


Abbildung 6.1 NTBackup-Auswahl

Sie können die Funktion der Sicherung auch teilweise prüfen, indem Sie zum Beispiel eine Wiederherstellung des Dateisystems in ein temporäres Verzeichnis umleiten. Denn selbst ein Bandlaufwerk und ein Band „altern“ und bedürfen der Kontrolle, ob alle Daten auch lesbar geschrieben wurden.

Mit Exchange 2003 können Sie auch die Speichergruppe zur Wiederherstellung nutzen, um Ihre Exchange-Online-Sicherung auf dem Server in diese gesonderte Speichergruppe (Recovery Storage Group) zurückzuspielen. Die produktive Datenbank wird dabei nicht gestört. Sie müssen nur für ausreichend Platz auf der Festplatte sorgen.

Überwachung Sicherungsmedien

Zum Schluss sollten Sie eine Rotation für die Bänder einplanen. Es bietet sich an, auch dem Server ein besonderes „Weihnachtsgeschenk" zu machen. Tauschen Sie Ihre Bänder regelmäßig aus, da auch diese dem Verschleiß unterliegen. Einige Backup-Programme (z.B. BackupExec) liefern Ihnen genaue Bandberichte, unter anderem auch über die Zuverlässigkeit des Bandes. Sie werden hier nach einigen Durchläufen immer wieder feststellen, dass die Anzahl der „behebbaren Fehler“ ansteigt. Dafür haben Bandlaufwerke umfangreiche Sicherungstechniken mit Prüfsummen (CRC). Allerdings sind irgendwann auch diese Reserven verbraucht. Je nach Bandtechnik ist ein Band nach ca. 10—20 Durchläufen (z.B. DAT) nicht mehr vertrauenswürdig. Das neue Jahr ist eine gute Zeit, Bänder mit zu vielen Fehlern auszusondern und einen Satz neuer Bänder in Umlauf zu bringen.

6.2.7 Voraussetzungen für ein erfolgreiches Restore

Allein das Backup eines Exchange-Servers ist noch keine Garantie für ein erfolgreiches Restore. Ehe wir uns daher um die einzelnen Wege eines Backups kümmern, sollten Sie folgende Voraussetzungen kennen, damit Ihr Backup und Restore überhaupt funktionieren.

Diese Vorbedingungen sind Pflicht, um eine Datenbank wieder starten zu können. Nach dem Restore müssen Sie überhaupt wieder an die Daten herankommen, um diese u.a. zu extrahieren. Weitere Punkte sollten ebenfalls stimmen, um ein komplettes funktionsfähiges Restore des Exchange-Servers zu erreichen.

Exchange 2003 arbeitet anders als Exchange 5.5. Daher sind andere Voraussetzungen gegeben. Diese gestalten sich sogar um einiges „einfacher“, da einige Bedingungen entfallen und andere ausgelagert wurden.

Organisation

- Der Name der Organisation muss gleich sein.

  Hier zählt nicht der „Displayname“, sondern der interne Name, welcher bei der Installation eingegeben und hoffentlich dokumentiert wurde. Fehlt diese Information, kann Exchange zwar restauriert, aber nicht gestartet werden. Beim ersten Startversuch finden Sie im Eventlog eine Meldung, die den Namen der Organisation enthält. Sie dürfen den Restore-Prozess dann noch einmal starten. Ein Problem hierbei ist jedoch, dass diese falsche Information im Active Directory steht und der Neuinstallation erst eine saubere Exchange-Deinstallation der kompletten Organisation vorangehen muss (`Setup /removeorg`).

Administrative Gruppe

- Der Name der Administrativen Gruppe muss gleich sein.

  Erinnern Sie sich auch hier nicht mehr an den Namen, gilt das gleiche Vorgehen wie bei der falschen Organisation. Sofern keine Exchange 5.5-

Server in Ihrer Exchange 2003-Organisation sind, können Sie die Administrativen Gruppen umbenennen.

- Name des Servers muss nicht gleich sein.

  Servername

  Diese Neuerung bindet die Datenbank nicht mehr fest an den Server und eröffnet daher einige alternative Restaurierungswege. So kann beispielsweise über SAN und Ersatzserver eine Datenbank an einem anderen Server geladen werden.

- SID des Exchange-Dienstkontos

  Dienstkonto

  Exchange 2003 im Native Mode benötigt kein Dienstkonto mehr. Nur wenn Exchange 5.5-Server in einer „Mixed AG“ vorhanden sind, wird das Dienstkonto zur Verbindung mit diesem Server in der AG mit hinterlegt, damit die Server miteinander kommunizieren können. Daher ist die SID dieses Kontos nur bedingt wichtig. Stattdessen muss aber das Computerkonto das Recht besitzen, die Einträge im Active Directory zu lesen. Dies ist bereits durch die Exchange-Installation sichergestellt worden.

- Das Backup muss erfolgreich eine Datenbank gesichert haben.

  Zuletzt benötigen Sie natürlich eine erfolgreiche Sicherung der Exchange-Datenbank. Das mit der Exchange-Installation aktualisierte *NTBackup* kann Exchange bereits online sichern und restaurieren. Für Drittprodukte müssen Sie oft einen gesonderten Agenten oder eine Lizenz installieren. Dann sollte die Rücksicherung natürlich auch noch funktionieren.

Mit diesem Wissen können Sie nicht nur Ihren produktiven Server wieder reaktivieren, sondern auch jede existierende konsistente Datenbank an einem Notfallserver wieder anbinden und starten. Allerdings müssen Sie je nach Zustand des Active Directory dann die Postfächer erneut mit den Benutzern verbinden und andere Konfigurationen von Hand nachpflegen.

6.2.8 Recovery Storage Group

Exchange 2003 erweitert die Möglichkeiten des Exchange-Administrators im Hinblick auf die Wiederherstellung einzelner Postfächer. Bis zur Version Exchange 2000 war die Wiederherstellung einzelner Postfächer nur möglich, wenn dazu ein eigener Server zur Wiederherstellung installiert wurde.

Alternate Server Data Recovery

Der zusätzliche Restore-Server bedeutete einen recht hohen Aufwand. Sehr viele Sicherungslösungen schafften daher eine Möglichkeit, zusätzlich zur Sicherung der Datenbank auch einzelne Nachrichten, Postfächer und Ordner zu sichern und später wiederherzustellen.

Nachteile dieser Lösungen sind die sehr lange Laufzeit solcher Sicherungen und ständig auftretende Probleme mit einigen Nachrichten und

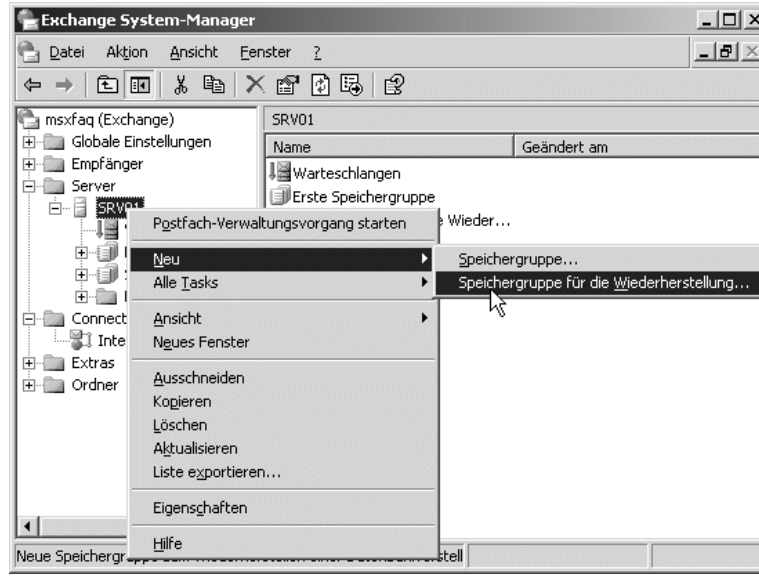
Berechtigungen. Es soll sogar Administratoren geben, die allein auf die Sicherung der einzelnen Inhalte vertrauen und auf die Datenbanksicherung verzichten. Hiervon ist dringend abzuraten.

Recovery Storage Group

Exchange 2003 erlaubt die Anlage einer besonderen *Speichergruppe zur Wiederherstellung*, in der auch NTBackup eine Sicherung restaurieren kann. Die produktiven Speichergruppen müssen in der Zwischenzeit nicht abgeschaltet werden.

Die Einrichtung der „Speichergruppe für die Wiederherstellung“ erfolgt auf einem beliebigen Server mit ausreichendem Speicherplatz. Nun können Sie die „wiederherzustellende Datenbank hinzufügen“, die nicht gestartet wird und den Überschreibmodus erhält. Die Wiederherstellung der Daten in den ursprünglichen Bereich wird vom System in die Recovery Storage Group umgeleitet.

Abbildung 6.2 Speichergruppe für die Wiederherstellung einrichten



Nach der Wiederherstellung über die Datensicherung und dem Bereitstellen der „Recovery“-Datenbank behandelt Exchange 2003 diese Datenbank genauso wie eine normale Postfachdatenbank. Die Postfächer und deren Größe sind im Exchange System-Manager sichtbar. Allerdings sind die Postfächer mit einem kleinen roten „x“ versehen und können nicht mit Active Directory-Benutzern verbunden werden.

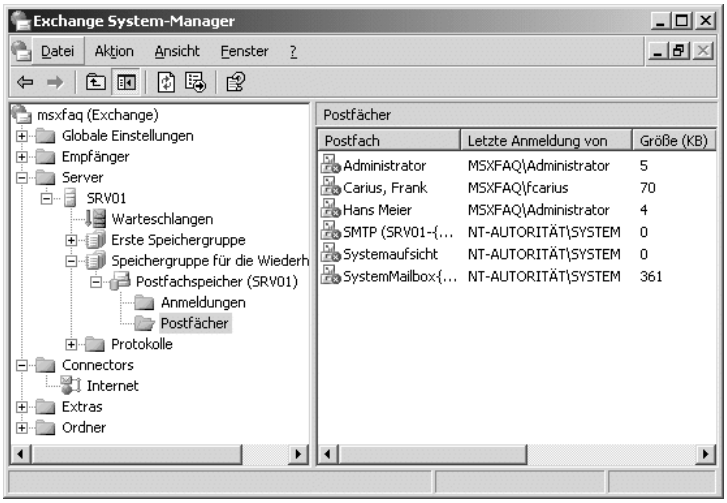


Abbildung 6.3 Postfächer in der „Recovery Storage Group“

Wurde bislang das Programm EXMERGE zum Übertragen der Daten in das aktuelle Postfach benutzt, erlaubt Service Pack 1 nun die direkte Übernahme der Objekte im Exchange System Manager. Über das Kontextmenü EXCHANGE-AUFGABEN können Sie die Postfachinhalte in das aktuelle Postfach kopieren oder mit diesem zusammenführen.

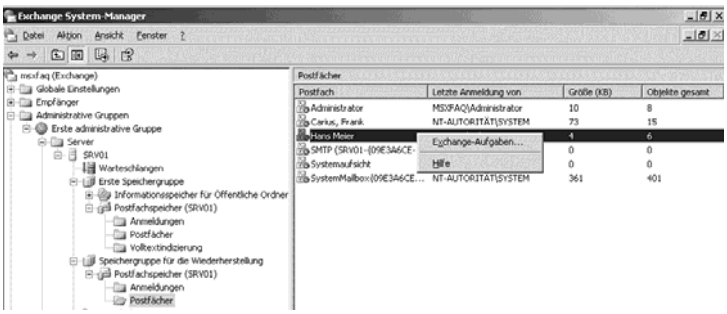


Abbildung 6.4 Exchange-Aufgaben zur Wiederherstellung

Sie können nun zwischen zwei Arten der Wiederherstellung wählen:

Neue Wiederherstellungsoptionen mit SP1

- Zusammenführen

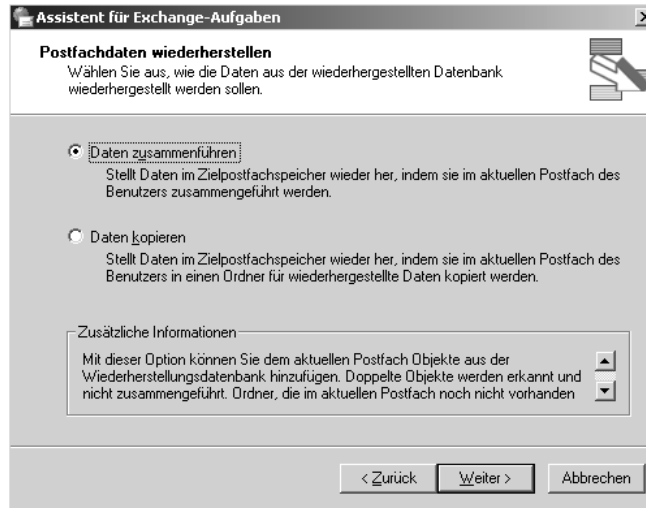
  Bei dieser Methode werden nur die Elemente aus dem Quellpostfach kopiert, die im Zielpostfach nicht vorhanden sind. Somit werden alle gelöschten E-Mails wiederhergestellt. Soll jedoch ein irrtümlich veränderter Eintrag wieder auf den alten Stand gebracht werden, muss das fragliche Element vorher gelöscht werden. Elemente im Postfach, die aktueller oder gleich sind, werden nicht überschrieben.

- Kopieren

Der Assistent kopiert alle Daten des wiederhergestellten Postfachs in einen Unterordner des aktuellen Postfachs. Prüfen Sie vorab die Grenzwerte für die Postfachgröße, damit diese bei Verdopplung der Postfachdaten nicht überschritten werden. Der Anwender kann danach selbst bestimmen, welche

Inhalte des Unterordners er in die originalen Positionen verschiebt oder löscht. Stellen Sie als Administrator sicher, dass dieser Zweig im Postfach anschließend wieder gelöscht wird, und setzen Sie ggf. die Limits wieder zurück.

Abbildung 6.5 Zusammenführen oder Kopieren der Inhalte



Einsatz von EXMERGE

Der Assistent lässt sich für jedes weitere Postfach anwenden und bietet zudem eine zeitgesteuerte Funktionsweise an. Jedoch gibt es immer wieder Situationen, die den Einsatz von EXMERGE erfordern. Die neue Option in Service Pack 1 bietet keine Wiederherstellung von Regeln und Berechtigungen an. EXMERGE ermöglicht zudem eine Filterung nach Betreff, Datum und weiteren Kriterien. Dabei stellt das Programm eine Verbindung zu dieser Datenbank her und exportiert selektiv den Inhalt einzelner Postfächer in PST-Dateien oder importiert diese direkt in die produktive Datenbank.

Unter http://www.microsoft.com/exchange finden Sie eine aktuelle Version von EXMERGE.

Abbildung 6.6 Exmerge aus der restaurierten Datenbank

Beide Programme funktioniert sogar über mehrere Server hinweg. Sie können auf einem Exchange 2003-Server auch problemlos die Online-Sicherung eines anderen Exchange-Servers zurücksichern. Auch ein Backup von Exchange 2000 mit Service-Pack 3 kann so restauriert werden.

Zusammenführen mit EXMERGE

Beim Einsatz von EXMERGE sind wie bisher auch die Besonderheiten gemischter Sprachinstallationen zu beachten. EXMERGE wird über die Datei „Exmerge.ini“ gesteuert, welche auch die Namen der Ordner und Spracheinstellungen der Dienste beinhaltet. Sollten diese nicht den Einstellungen in der Datei MAPISVC.INF im System32-Verzeichnis übereinstimmen, kann EXMERGE keine entsprechenden Profile anlegen. Die Fehlermeldungen im Protokoll EXMERGE.LOG helfen bei der Eingrenzung des Problems. Für die Funktion von EXMERGE ist es nicht erforderlich, Outlook auf dem Server zu installieren. Outlook auf einem Exchange-Server ist sogar schädlich, da Konflikte von DLLs vorprogrammiert sind. Weiterhin müssen Sie beachten, dass der Administrator als auch alle Konten, die in den Gruppen „Domänen-Admins“ oder „Organisations-Admins“ sind, ein Verbot auf die Postfächer haben. Sie können daher nicht auf Informationen in Postfächern zugreifen.

Server „aufräumen“

Über die Speichergruppe zur Wiederherstellung ist es damit einfach möglich, eine bestehende Online-Sicherung auf dem produktiven Exchange-Server zurückzuspielen und die Inhalte einzelner Postfächer zu migrieren. Zu berücksichtigen ist dabei aber, dass immer die komplette Datenbank zurückgespielt wird und damit auf dem Server zumindest temporär für die Datenbank und die zusätzlichen Daten ausreichend Speicherplatz bereitstehen muss. Löschen Sie die Wiederherstellungsdatenbank anschließend, um den Festplattenplatz wieder freizugeben. Denken Sie daran, dass bei Vorhandensein einer Recovery Storage Group die Wiederherstellung einer Datenbank an den originalen Platz immer fehlschlägt. Sollten Sie nach einem Defekt der Datenbank diese wieder restaurieren, darf auf dem Server keine Recovery Storage Group existieren. Die Wiederherstellung eignet sich leider nur für Postfachspeicher und nicht für Öffentliche Ordner.

3rd-Party-Produkte

Diese Schwäche und das Fehlen der „Recovery Storage Group“ in Exchange 2000 und Exchange 5.5 haben Hersteller wie Kroll Ontrack erkannt und bieten Produkte (PowerControls) an, die direkt eine Exchange-Datenbank von einem Backup zurückholen, öffnen und die Inhalte auslesen. Dies funktioniert teilweise sogar mit defekten Datenbanken und Öffentlichen Ordnern (http://www.msexchangefaq.de/produkte/pc2.htm).

6.2.9 NTBackup und die Grenzen

Durch die Installation von Exchange 2003 wird auch das Windows-Sicherungsprogramm Ntbackup, um die Funktion der Exchange-Sicherung

erweitert. Mit Ntbackup können Sie daher sofort einen Exchange 2003-Server online sichern und wieder herstellen. Allerdings ist die Funktion des Windows-Sicherungsprogramms in vielerlei Hinsicht eingeschränkt, so dass die Anschaffung einer kommerziellen Sicherungssoftware überlegt werden muss. Die Grenzen von Ntbackup sind unter anderem:

- Keine Band- und Medienverwaltung

  Vollwertige Produkte führen eine Datenbank zur Inventarverwaltung der Bänder und der gesicherten Informationen. Sie können somit ohne das Band einzulegen schnell den Inhalt sehen und die passende Datei für die Wiederherstellung finden. Zudem können Sie Bänder entsprechend schützen, damit diese bei einer Fehlbestückung nicht zu früh überschrieben werden.

- Begrenzte Überwachung, Administration und Benachrichtigung

  Ntbackup schreibt eine Protokolldatei mit dem Ergebnis der Sicherung. Nur mit eigenen Skripten können Sie diese Datei z.B. per E-Mail weitersenden oder bei Fehlern einen SNMP-Trap auslösen. Auch eine Remote-Überwachung eines Jobs ist nicht möglich. Ntbackup informiert Sie nicht, wenn das falsche Band eingelegt ist.

- Wechslerunterstützung nur über RSM

  Wenn Sie einen automatischen Wechsler betreiben, dann unterstützt Ntbackup dies nur so weit, wie der RSM-Dienst des Betriebssystems den Wechsler nutzen kann.

- Zeitplandienst

  Als Zeitplaner wird der Windows-Zeitplandienst („at“, geplante Tasks) genutzt. Das ist für viele Zwecke ausreichend, aber angenehmer ist schon, wenn die Datensicherung z.B. Feiertage überspringt.

- Keine SAN-Unterstützung

  Sobald Sie gemeinsam genutzte Bandlaufwerke in einem SAN verwenden, kommen Sie mit dem Windows-Sicherungsprogramm nicht weiter, da Ntbackup von lokal angeschlossenen und exklusiv nutzbaren Laufwerken ausgeht.

- Keine Agenten (OpenFiles/Notes/Oracle)

  Ntbackup kann im Wesentlichen das Betriebssystem und nun auch Exchange sichern. Aber viele andere zu sichernden Daten sind während des Betriebs geöffnet. Die Schattenkopien erlauben seit Windows 2003 auch die Sicherung solcher Daten, aber im Hinblick auf Datenbanken ist dies in den meisten Fällen keine adäquate Sicherung. Für Exchange ist solch eine Schattenkopie mit Ntbackup nicht einsetzbar.

- Kein „Desaster Recovery“

  Einige Produkte erlauben es, eine CD zu brennen, mit der im Notfall der Server sehr schnell wieder hergestellt werden kann. Mit Ntbackup müssen Sie immer erst ein Windows installieren, damit Sie das komplette System restaurieren können. Erst die ASR-Funktion in Windows 2003 bietet eine ähnliche Funktion, einen Server schnell wieder reparieren zu können, wenn alle anderen Alternativen versagen.

- Keine optimale Bandtreiberunterstützung

  Es werden nur Bandlaufwerke unterstützt, die vom Betriebssystem erkannt werden. Einige Backup-Produkte bringen eigene Laufwerkstreiber mit. Diese sind teilweise sehr viel schneller im Datendurchsatz und erkennen zusätzliche Meldungen der Bandlaufwerke, z.B. dass eine Reinigung erforderlich ist.

- Keine Prüfung auf Viren

  Kommerzielle Produkte erlauben meist das zusätzliche Scannen auf Viren während des Backups. Für Exchange ist diese Funktion zwar nicht relevant, aber da eine Sicherung auch immer die Dateien mitsichert, ist dies eine zusätzliche Möglichkeit, die Qualität des Backups zu verbessern.

- Begrenzte Exchange-Unterstützung

  Neben dem Exchange-Backup ist es oft auch gewünscht, einzelne Nachrichten oder Ordner zu sichern und zu restaurieren, Auch die Umleitung eines Restore auf einen anderen Server (Remote) ist mit Ntbackup nicht möglich.

Ntbackup ist übrigens eine vereinfachte Version von Veritas Backup Exec. Trotz der vielen Einschränkungen ist Ntbackup ein sehr nützliches Programm, um schnell eine Sicherung des Servers vor größeren Umbaumaßnahmen zu machen. Ntbackup ist auf jedem Server immer betriebsbereit und muss nicht erst installiert werden.

6.3 Virenschutz

Durch die immer weiter zunehmende Vernetzung der Systeme nimmt auch die Gefahr durch unerwünschte Programme in Ihrem Netzwerk zu. Dies betrifft nicht nur den E-Mailaustausch mit Exchange, sondern jede Art von Dateiaustausch. Dazu gehören neben Disketten und CD-ROMs auch immer mehr Wechselfestplatten, USB-Speichersticks und natürlich das Surfen im Internet. Trotzdem ist auch jedes E-Mail-System durch die einfache und effektive Funktion nicht nur dazu geeignet, sondern regelmäßig die Basis für die Verbreitung von Viren.

Aus heutiger Sicht ist es unverantwortlich, ein System ohne aktuellen Virenschutz zu betreiben. In diesem Zusammenhang müssen Sie nicht nur im Hinblick auf Exchange wissen, welche Viren es gibt, wie Viren funktionieren und wo Sie diese abwehren können.

Viren und andere Schädlinge

Sehr häufig werden Viren einfach mit Schadprogrammen gleichgesetzt, ohne eine Unterscheidung zu treffen. Die Zusammenfassung von unerwarteten Reaktionen und Missbrauch als „Virenverseuchung“ ist einer Fehlersuche eher abträglich. Schadprogramme gibt es in verschiedenen Ausprägungen:

- Klassische Viren

  Viren sind Programme, die sich eigenständig vervielfältigen und verbreiten. Während früher oft eine infizierte Bootdiskette oder eine infizierte Installationsquelle der Auslöser für einen Virenbefall war, sind es mittlerweile unsichere Downloads aus dem Internet oder die Verteilung als Anlage einer Nachricht. Viele Viren verteilen sich mittlerweile schon selbstständig per SMTP. Die Intention der Autoren dürfte eher darin liegen, zweifelhafte Berühmtheit zu erlangen, als einen Hersteller auf einen Fehler hinzuweisen oder Ruf schädigend zu sein.

- Trojaner

  Trojaner unterscheiden sich von klassischen Viren derart, dass der Schadanteil nicht direkt destruktiv ist, sondern dass Informationen nach außen veruntreut werden oder Ihr System aus der Ferne kontrolliert werden kann. Mit der Zunahme der Standleitungen ist für mögliche Angreifer auch eine Verteilung ähnlich der Viren interessant, wenn der Trojaner eigenständig nach Hause telefoniert. Trojaner sind besonders tückisch, da sie lange untätig bleiben können, bis ein Signal alle Systeme aktiviert, und damit ein weiteres System, z.B. eine Webseite, angreifen (Denial of Service, Distributed Denial of Service).

- Angreifer

  Viele Programme, die eine Schwachstelle in einem Betriebssystem angreifen (Ping of Death, Rootkits etc.) sind eigentlich keine Viren. Diese Programme werden meist entwickelt, um eine Schwachstelle in einem System zu nutzen und das System zu übernehmen oder den Betrieb zu stören.

- Funny Joke

  Der Sinn dieser meist auf E-Mails beschränkten Programme oder Meldungen ist es, möglichst oft vervielfältigt und verteilt zu werden. Meist sind es Falschmeldungen, die andere Personen dazu verleiten sollten, diese wieder zu verteilen oder an den vermeintlichen Absender oder Dritte zu antworten. Bestes Beispiel ist die Falschmeldung über Bonsaikatzen (www.bonsaikitten.com), welche aber diverse Tierschutz-

organisationen und staatliche Stellen mit Anfragen und Beschwerden beschäftigt. Bestes Mittel: ignorieren.

- Spam/Virenmails

  Die unerwünschte Zusendung von Nachrichten jeder Art ist zwar ein Ärgernis, aber erst durch eine virenrelevante Anlage wird daraus ein Virus, den entsprechende Programme erkennen können. Während Spam über andere Wege reduziert werden kann, haben viele Viren einen Schadanteil, sich per E-Mail an viele andere Personen zu versenden.

- Relay

  Wenn Ihr Exchange-Server ein offenes Relay ist, d.h., unautorisierte SMTP-Verbindungen zulässt und die Nachrichten weiterleitet, dann wird Ihr System sehr bald als Versender verschiedenster Nachrichten missbraucht. Dies sollten Sie vermeiden, ist aber kein Virus. Allerdings suchen viele Viren ein SMTP-Relay, um sich weiter verbreiten zu können. Insofern sollten Sie auch internen Systemen nicht blind vertrauen.

Nicht alle Viren haben auch immer einen Schadanteil, d.h., zerstören Daten oder stören die Funktion aktiv. Die meisten kosten aber Speicherplatz, Bandbreite, Rechenleistung und primär auch Arbeitskraft. Nicht alle Hersteller von Virenschutzsoftware behandeln alle Ausprägungen von Schadprogrammen gleich.

6.3.1 Wo kann Exchange „gescannt“ werden?

In einem Umfeld mit Exchange 2003 gibt es verschiedene Stellen, um Viren und anderen Schädlingen die Verbreitung zu erschweren oder unmöglich zu machen. Einige Ansätze lassen sich ohne zusätzliche Software realisieren. Für die meisten Lösungen ist eine käuflich zu erwerbende Software erforderlich.

Schnittstellen für Scan-Programme

Wir betrachten die komplette Bandbreite vom Internet über die Server bis zum Anwender, um alle Schnittstellen für den Einsatz eines Virenscanners zu erläutern. Exchange 2003 bietet selbst sehr viele Schnittstellen für Virenprogramme an. Aber allein ein Exchange-Virenscanner ist in Ihrer IT-Infrastruktur nicht immer ausreichend.

Speziell wenn Anwender Ihre Nachrichten digital signieren oder verschlüsseln und Anlagen mit Kennworten schützen, kann ein Virenscanner zwischen Absender und Empfänger nur eingeschränkt die Schädlinge erkennen. An folgenden Stellen kann ein Virenscanner eingreifen:

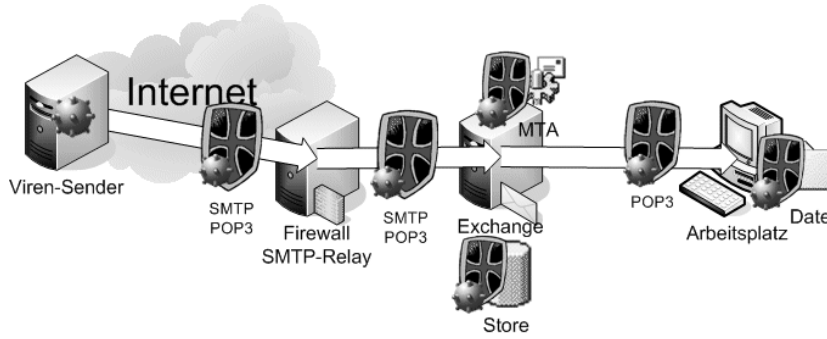


Abbildung 6.7
Hier kann auf Viren geprüft werden.

Auf dem Transportweg

Beim Transfer von Dateien über das Internet besteht immer die Gefahr, unerwünschte Inhalte und korrupte Dateien zu erhalten. Hier helfen Scanner, die den Datenverkehr auf dem Weg zum Server scannen und damit von vorneherein verhindern, dass solche Inhalte bis zum Client oder Server gelangen.

- SMTP-Scanner

  SMTP-Scanner kontrollieren die Nachrichten im SMTP-Protokoll. Alle Nachrichten, die per SMTP gesendet oder empfangen werden, können so kontrolliert und verändert werden. Dazu arbeiten die Virenscanner in der Regel als SMTP-Relay und werden zwischen das Internet und Exchange geschaltet. So ist sichergestellt, dass jede Nachricht aus dem Internet geprüft wird. Zusätzlich kann durch eine Prüfung für ausgehende Nachrichten verhindert werden, dass Ihre Firma selbst Viren versendet. Dies ist insbesondere gegen Viren interessant, die selbst per SMTP versuchen, eine Nachricht zu versenden.

  Die Platzierung dieser Scanner erfolgt meist in der DMZ einer Firewall. In kleineren Installationen wird der Virenscanner auch auf dem Exchange-Server installiert und der Port 25 entsprechend umgeleitet.

- POP3-Scanner

  Über das Protokoll POP3 holen Anwender ihre Nachrichten von einem Server ab. Durch die Realisierung als POP3-Proxy können somit Nachrichten, die vom Anwender abgeholt werden, schon beim Empfang geprüft und entfernt werden.

  Die Funktion eines POP3-Scanners ist auch für alle Administratoren interessant, die Ihre Nachrichten per POP3 aus einem Sammelpostfach abholen und an Exchange weiterleiten. Allerdings bieten die meisten POP3-Sammeldienste bereits eine eigene Schnittstelle für Virenscanner an, so dass diese Funktion in Verbindung mit der Anbindung eines Exchange-Servers an das Internet selten genutzt wird.

Der Scanner auf dem Transportweg hat den Vorteil, dass er weder allzu tief in den eigentlichen E-Mailserver eingreift und sehr viel einfacher und schneller aktualisiert werden kann als alle Clients eines Unternehmens. Oftmals erlauben eigene Regeln und Erweiterungen eigene angepasste Filter, z.B. um bestimmte Schlüsselwörter zu verhindern.

Im Store

Exchange-Datenbank scannen

Selbst wenn auf dem Empfangsweg nach Viren gesucht wird, können trotzdem Nachrichten in Ihrem Posteingang landen. Sie können nicht sicher sein, dass ein Scanner auf dem Transportweg alle Viren entdeckt. Wenn Ihnen ein Anwender per Outlook Web Access eine Nachricht sendet, dann landet diese direkt im Informationsspeicher. Daher ist ein Schutz auch auf der Exchange-Datenbank wichtig.

- MAPI

  Eine Möglichkeit der Virensuche ist der Zugriff per MAPI. Ein Virenscanner erhält die Rechte, alle Postfächer zu lesen, und baut eine Verbindung zu allen Postfächern auf. Jede neue Nachricht wird nicht nur dem Anwender gemeldet, sondern auch der Virenscanner erkennt den Eingang und kann die Nachricht prüfen und behandeln.

  Die Probleme dieser Methode sind, dass Sie die Berechtigung sicherstellen müssen und es eine kleine Lücke zwischen Zustellung der E-Mail in das Postfach und dem Entfernen durch den Virenscanner gibt. Wenn der Server oder der Virenscanner stark beschäftigt ist, kann ein Anwender theoretisch eine Nachricht öffnen, ehe diese vom Scanner bearbeitet wurde. Dies ist ein prinzipielles Problem von MAPI. Aber früher war es der einzige Weg, in Exchange nach Viren zu suchen.

- AVAPI/VSAPI-Scanner

  Aus all den Erfahrungen mit MAPI hat Microsoft seit dem Exchange 5.5 SP3 eine neue Schnittstelle AVAPI bereitgestellt. Mit Exchange 2003 liegt diese API in der Version 2.5 vor, über die zertifizierte Softwarehersteller sich direkt in die Exchange-Datenbank einbinden können. Registriert sich eine Antivirus-Software, dann präsentiert Exchange die Nachrichten vor der Zustellung dem Virenscanner, welcher diese prüft und gegebenenfalls behandelt. Erst dann erhält der Anwender die E-Mail. Die AVAPI/VSAPI-Schnittstelle selbst ist nicht öffentlich dokumentiert und wird nur an „vertrauenswürdige“ Antiviren-Hersteller abgegeben. Seit Exchange 2003 ist es zudem möglich, auch über AVAPI Informationen über das Postfach und die Nachricht zu erhalten. Damit entfällt die Beschränkungen früherer Versionen im Vergleich zu MAPI.

- Event Sink-Scanner (Exchange 2003)

  Seit Exchange 2000 ist es möglich, auch an verschiedenen Stellen der Zustellung und der Speicherung entsprechende Event Sinks einzubauen, die auch „synchron“ arbeiten, d.h., die Nachrichten werden erst nach der Verarbeitung durch den Sink weitergeleitet. Diverse Beispiele zeigen, wie mit Sinks z.B. an jede E-Mail ein Trailer angehängt werden kann. Ebenso gut kann hiermit jede eingehende E-Mail abgefangen und auf Viren geprüft werden. Microsoft liefert mittlerweile einen SMTP-Transport-Event Sink für Windows 2000/2003, um Anlagen zu blockieren.

- ESE.DLL

  Aufgrund der früheren Einschränkungen bzw. dem Fehlen der AVAPI-Schnittstelle hatte die Firma Sybari begonnen, einen eigenen Weg zu gehen und vor die ESE.DLL ein eigenes Programm zu schalten. Alle Aufrufe an die ESE-Schnittstelle landen beim Virenscanner, der die Aufrufe dann an die originale ESE-Engine durchreicht. Dabei kann die Routine die Daten abfangen und beliebige Scanner einbinden. Diese Methode wird mittlerweile auch von anderen Herstellern unterstützt.

  Nachteilig an dieser Methode ist die enge Verzahnung mit der ESE-Engine und die damit verbundene Problematik mit Updates. Für jedes Update von Exchange ist in der Regel auch ein Update der Antivirus-Software erforderlich.

- MTA-Scanner

  Eine der wesentlichen Funktionen in Exchange 5.5 ist der MTA, der für die Zustellung und Weiterleitung von Nachrichten notwendig ist. Mit Exchange 2000 ist der MTA nur noch Informationsdrehscheibe für alte Connectoren und X.400-Verbindungen. Auf Ebene des MTA könnte theoretisch auch ein Virusscan erfolgen, aber uns sind keine Produkte bekannt.

Dateibasierter Virenscan auf dem Client und Server

Selbst beim Einsatz aller Virenscanner auf dem Transportweg und dem Server selbst werden immer noch schädliche Anlagen bis zum Arbeitsplatz gelangen.

- Scanner auf dem Arbeitsplatz

  Spätestens wenn der Benutzer eine E-Mail öffnet, wird diese von Outlook vom Exchange-Server geladen und in einem temporären Verzeichnis auf der Festplatte gespeichert. Sobald der Anwender eine Anlage speichert oder ein bestimmtes virulentes Verhalten auf dem PC durch den Virenscanner festgestellt wird, hat der Scanner auf dem Arbeitsplatz die Aufgabe, dieses zu unterbinden. Dies funktioniert auch wunderbar bei gepackten Anlagen (auch mit Kennwort) und verschlüsselten Nach-

richten. Damit ist der Scanner auf der Workstation die letzte Bastion, ehe ein Virus aktiv werden kann, und wird zu einer Pflichtkomponente.

Tücken beim Workstation-Scan

Leider ist ein Scanner auf dem Arbeitsplatz keine zentrale Lösung und bedeutet für den Administrator die Herausforderung, diese Komponenten immer aktuell zu halten und natürlich auch eine Rückmeldung über Aktivitäten zu erhalten. Besonders bei Notebooks mit temporärer Netzwerkanbindung muss die Software pfiffig sein, ein Update zu verzögern, eine Verbindung zu erkennen und die Benachrichtigungen an einer zentralen Stelle zu puffern. Dank der Möglichkeit, heutige PCs einfach in den Ruhezustand zu versetzen, ist auch ein Anmeldeskript nicht mehr zuverlässig genug. Viele Anwender melden sich nicht mehr täglich an, sondern setzen Ihre Arbeit dort fort, wo sie zuletzt aufgehört haben.

Den Inhalt von PST- oder OST-Dateien kann ein Scanner auf dem Arbeitsplatz nicht prüfen, da die Nachrichten dort nicht als Datei, sondern als Datenbankseiten abgelegt werden. Wenn ein Virenscanner ein Bitmuster als „auffällig“ deklariert, wird er den Zugriff auf die Datei verhindern. Damit ist die Datei in der Regel nicht mehr zu gebrauchen. Daher gehört *.OST und *.PST auf die Ausschlussliste für dateibasierte Scanner.

- Scanner auf einem Dateiserver

  Durch einen Einsatz von Exchange 2003 sollten Sie generell auf (PST-) Dateiablagen auf einem Dateiserver verzichten. Es gibt zwar immer wieder Firmen, die durch Postfachbegrenzungen indirekt dafür sorgen, dass Mitarbeiter ihre älteren Nachrichten in PST-Dateien exportieren oder mit Outlook archivieren und diese Dateien dann auf einem Dateiserver ablegen. Neben dem Platzbedarf, dem erhöhten Backup-Volumen und der Netzwerkbelastung sollten Sie im Hinblick auf einen Virenscanner auch auf einem Dateiserver abgelegte Archiv- und PST-Dateien aus dem Scanprozess ausschließen.

- Dateiscanner und Exchange

  Wenn Sie auf dem Exchange-Server selbst einen dateibasierten Virenscanner installieren möchten, dann sollten Sie mehrfach kontrollieren, dass der Zugriff auf das Laufwerk M: unterbleibt. Exchange 2003 richtet das Laufwerk M: per Default nicht mehr ein, aber für bestimmte Programme kann es notwendig sein, diesen Zugriff zu aktivieren. Ein Virenscanner auf Laufwerk M: zerstört in der Regel die Zugriffsrechte, kostet Performance und kann die Protokolldateien stark anwachsen lassen. Siehe dazu auch den TechNet-Artikel „328841 XADM: Exchange and Antivirus Software“.

Sonstige Schnittstellen

Neben dem Virenscanner auf Dateiservern, der Exchange-Datenbank, den Transportwegen und Arbeitsplätzen gibt es weitere Möglichkeiten, nach Viren zu suchen und diese zu blockieren:

- HTTP-Scanner

  Jeder, der im Internet surft, kann sich Viren als Download, ActiveX- oder als JavaScript-Programme einfangen. Meist verhindert ein Scanner auf dem Arbeitsplatz Schlimmeres, aber beim Einsatz eines Proxy-Servers kann in Verbindung mit einem Virenscanner hier Schlimmeres zentral verhindert werden. Dies ist insbesondere dann wichtig, wenn Mitarbeiter immer mehr per Browser auf ihre Mailbox zugreifen. So mancher Virus ist durch die Nutzung eines kostenfreien Webmailers in Firmen gelangt.

- Scannen beim Backup

  Sehr viele Datensicherungsprogramme bieten mittlerweile auch die Möglichkeit an, während der Sicherung die Daten auf Viren zu prüfen. Das funktioniert mit Dateien, aber nicht mit einer Exchange-Sicherung. Weder bei einer Online-Sicherung, noch einer Offline-Sicherung von Exchange liegen die Nachrichten in einer Form vor, dass ein Virenscanner der Sicherungssoftware darin sinnvoll nach Viren suchen kann.

6.3.2 Kriterien bei der Auswahl einer Schutzlösung

Die Entscheidung, welcher Virenscanner in Ihrer Umgebung am besten integriert werden kann, müssen Sie leider selbst evaluieren. Beim Studium von Newsgroups und Webseiten werden Sie aber sehr einfach die Favoriten der Exchange-Administratoren herausfinden. Sie sollten bei der Bewertung folgende Faktoren mit berücksichtigen:

- Installation

  Nicht alle Virenschutzlösungen lassen sich automatisch verteilen. Das mag für kleinere Firmen nicht wichtig sein, aber wenn Sie mehrere Exchange-Server an verschiedenen Standorten haben, dann ist eine Installation vom Arbeitsplatz über das LAN eine schöne Sache. TrendMicro „ScanMail“ löst dies derart, dass die Installation auf dem Arbeitsplatz eines Administrators gestartet wird und über das Netzwerk auf den ausgewählten Servern die Dateien und Dienste installiert. Andere Hersteller nutzen ähnliche Methoden, damit der Administrator nicht auf jedem Server manuell die Installation starten muss.

- Konfiguration

  Ebenso wichtig ist eine zentrale Konfiguration, damit mehrere Server gut unter Kontrolle gehalten werden können. Praktisch ist eine

Administration, die Richtlinien vorgibt, nach denen sich alle richten. Das müssen keine NT-Policies oder Windows 2003-Gruppenrichtlinien sein, eine einfache INI-Datei auf einer Dateifreigabe tut es auch, welche von den Clients regelmäßig kopiert wird. Hauptsache, die zeit- und kostenaufwändige individuelle Konfiguration pro Arbeitsplatz entfällt.

- Update

  Wichtig ist auch, wie „stabil“ das Update bei einem Virenansturm ist. Bekommen Sie noch die Pattern-Dateien vom Hersteller, wenn tausend Kunden das Gleiche tun? Auch mehrmalige Updates pro Tag sind heute an der Tagesordnung, um zeitnah auf neue Viren zu reagieren. Sie sollten aber beim Einsatz von Scannern auf jedem Arbeitsplatz auch hier eine schnelle Verteilung über einen zentralen Server ermöglichen können und vor allem eine Übersicht erhalten, welche Clients noch nicht aktualisiert wurden. Die notwendige Bandbreite ist ebenfalls ein Kriterium bei der Entscheidung.

- Erfahrungen und Geschäftsmodell

  Schauen Sie sich den Hersteller selbst an. Lebt der Hersteller von der Software, wie dies z.B. bei Trend Micro, Kaspersky Labs, H+B EDV und anderen der Fall ist, oder ist der Virenscanner ein Produkt unter vielen, um eine Suite zu komplettieren? Die meisten Programme sind gleichwertig in ihrer Leistung und allemal besser als der Verzicht auf einen Virenscanner. Daher nehmen Support, Handbücher, aber auch Fachhändler eine immer bedeutendere Rolle ein.

- Alarmierung und Management

  Natürlich gehört es zum guten Ton, dass ein Scanner einen Virus meldet. Die meisten Programme melden dies per Netzwerk-Popup oder E-Mail. Unterschiede gibt es auch hier: Sendet die Software die Nachricht E-Mail per SMTP, oder benötigt die Software eigens ein Postfach, um per MAPI die Nachricht zu senden? Leider integrieren sich nicht alle Virenscanner in das Eventlog, in Performance Counter oder SNMP, für die häufig schon Überwachungslösungen existieren.

- Lizenzierung und Preis

  Kosten entstehen nicht nur durch den Produktpreis.

  Das Geld ist ein wichtiger Faktor, aber steht unserer Meinung nach sehr weit hinten an. Die aktuelle Marktsituation regelt die Preise auf einem normalen Niveau. Ein Produkt wird erst richtig teuer, wenn es nicht wie erwartet funktioniert oder ein hoher Arbeitsaufwand für die Pflege verbunden ist.

- Besonderheiten

  Beachten Sie auch die Kleinigkeiten, die am Ende aber eine große Wirkung haben. Kann der Scanner auch komprimierte Dateien verar-

beiten und, wenn ja, wie weit rekursiv. Was macht er, wenn eine Datei mit Kennwort verschlüsselt ist? Gerade SMTP-Scanner sind genau zu prüfen, da es verschiedene MIME-Zeichensätze etc. gibt, sonst fehlen vielleicht plötzlich Umlaute. Es ist nicht ungewöhnlich, dass eine Nachricht eines asiatischen Kunden über Ihren Server weiter transportiert werden muss.

6.3.3 Minimalschutz

Ideal wäre der Einsatz aller möglichen Virenscanner an allen Schnittstellen. Dies reduziert die Wahrscheinlichkeit eines Schadens, bedeutet aber auch eine Investition in entsprechende Lizenzen, eine Pflege aller Virenscanner und entsprechende zusätzliche Verringerung der Leistung.

Unbedingt erforderlich!

Aus der praktischen Erfahrung hat sich im Einsatz von Exchange daher gezeigt, dass zwei Virenscanner unbedingt notwendig sind und weitere Scanner je nach individuellen Anforderungen installiert werden können.

- Dateibasierte Scanner

  Es ist unverantwortlich, ein Netzwerk ohne einen Virenscanner auf den Systemen selbst zu betreiben. Dies bedeutet, dass alle Arbeitsplatzsysteme immer mit einem aktuellen Virenscanner ausgestattetet werden müssen und alle Server als zentrale Datenablage ebenso einen Virenscanner erhalten. Sofern die Aktualisierung der Systeme gesichert ist, ist dieser Minimalschutz gewährleistet. Dieser Schutz sollte auch alle intern verwendeten Wechselmedien und gemeinsame Datenbereiche ausreichend schützen und das Risiko eines Schadens minimieren.

  Zudem ist der Schutz auf dem Arbeitsplatz in vielen Fällen die einzige Möglichkeit, bestimmte Viren zu finden und zu blockieren, z.B. in verschlüsselten Nachrichten.

- Content-Scanner im Transportweg

  Der zweite Ansatz ist ein Virenscanner auf den Übertragungswegen. Hier ist sehr einfach und effektiv eine zentrale Blockade von Viren für die gesamte Firma möglich. Das Internet ist leider zu dem primären Transportmittel für Viren und andere Schädlinge geworden. Da Sie nie sicher sein können, dass alle Systeme in Ihrem Netzwerk mit einem aktiven Virenscanner ausgestattet sind und diese zudem nicht immer aktuell sind, ist eine zweite Absicherung notwendig.

  Oftmals sind solche Produkte auch zugleich Relay und verhindern damit die direkte Erreichbarkeit des Exchange-Servers und bieten zusätzliche Inhaltsfilter an, z.B. gegen Spam oder die Filterung nach Schlüsselwörtern, bestimmten Anlagen etc.

Diese beiden Scanner sind für den Betrieb eines Netzwerks und die Anbindung an das Internet sehr empfehlenswert. Leider zeigen viele Viren, die aus Firmen versendet werden, dass zumindest auf dem Transportweg noch nicht alle Unternehmen entsprechend vorgesorgt haben. Ein Scanner im Transportweg sollte natürlich so gestaltet sein, dass er nicht von einem Virus umgangen werden kann. Der direkte Zugriff eines Arbeitsplatzes in das Internet über das SMTP-Protokoll Port 25/TCP ohne entsprechende Autorisierung muss natürlich blockiert werden.

Trotzdem haben auch andere Optionen ihre Daseinsberechtigung. Wenn ein sehr neuer Virus beim Empfang noch nicht erkannt wurde, dann landet diese Nachricht schon in der Exchange-Datenbank. Liest der Anwender diese Nachricht etwas später, dann kann der Virus immer noch aktiv werden, zumindest wenn der Scanner auf dem Arbeitsplatz nicht aktuell ist. Daher ist ein zusätzlicher zentraler Scanner ein hilfreiches Werkzeug, der z.B. am Wochenende immer mal wieder einen kompletten Scan startet. Solange Sie nicht sicher sind, dass alle Arbeitsstationen einen aktiven aktuellen Virenscanner besitzen, sollten Sie überlegen, auf dem Exchange-Server selbst einen Virenscanner für Exchange einzusetzen.

6.4 Spam-Schutz und UCE

Der Versand von Nachrichten per SMTP ist wesentlich günstiger als der Versand von Postbriefen oder Massenwurfsendungen. Diese Vorteile hat auch die Werbeindustrie erkannt und betreibt immer intensiver die Vermarktung ihrer Produkte per E-Mail. Dagegen ist nichts einzuwenden, solange die Anbieter seriös arbeiten und nur interessierte Personen mit entsprechenden Informationen versorgen.

Werbung und unerwünschte E-Mails

Aber es gibt auch jede Menge schwarzer Schafe, die das Internet als Transportmittel für verschiedenste Nachrichten verwenden. Meist handelt es sich um zweifelhafte Gewinnspiele, angeblich sichere Tipps und vorgeblich günstige Angebote. Die meisten dieser Anpreisungen werden jedoch von der überwiegenden Anzahl der erfahrenen Empfänger gelöscht oder gefiltert. Durch das immense Wachstum des Internets gibt es immer noch sehr viele Neueinsteiger, die diese Masche noch nicht durchschaut haben und den Trickbetrügern auf den Leim gehen. Um diese Opfer zu erreichen, fahnden diese Anbieter mit automatischen Programmen nach E-Mail-Adressen auf Webseiten, in Newsgroups und anderen elektronisch auswertbaren Quellen. Es gibt sogar einen großen Markt für den Handel von qualifizierten E-Mail-Adressen.

Diese Nachrichten werden als Spam bezeichnet. Dieser Begriff basiert auf einem Spot der Komiker-Truppe um *Monty Python*, in dem einige Personen

eine Konversation immer stärker durch den Zwischenruf von „Spam“ zum Erliegen gebracht haben. Auch der Begriff UCE (Unsolicited Comercial E-Mail = unerwünschte kommerzielle Nachricht) wird häufig benutzt.

6.4.1 Risiken von Spam-Nachrichten

Selbst wenn Sie nicht auf die Werbung hereinfallen, gibt es wichtige Gründe warum Sie eine Abwehr gegen diese Nachrichten einplanen sollten:

Risiken in Ihrem Unternehmen

- Kosten der technischen Ressourcen

  Diese Nachrichten kosten sowohl Übertragungsvolumen wie auch Zeit. Sogar mit einer pauschalen Berechnung des Internet-Verkehrs reduzieren solche Nachrichten die verfügbare Bandbreite und bremsen damit den gewünschten Verkehr.

- Kosten des Personals

  Mitarbeiter müssen diese Nachrichten lesen oder zumindest ihr Postfach davon bereinigen. Das Risiko, dabei eine wichtige Nachricht zu löschen, ist ebenso gegeben wie das Öffnen einer Werbenachricht. Enthält Ihr Postfach mehrere dieser Spam-Nachrichten, die zum Beispiel per SMS an das Handy weitergeleitet oder von unterwegs mit Outlook repliziert werden, ist der Ärger vorprogrammiert.

- Integrität

  Viele dieser Werbenachrichten enthalten ausführbare Anlagen oder auch klassische Viren, die die Unversehrtheit Ihrer Daten gefährden. Virenscanner helfen auch hier. Aber nicht alles ist immer als Virus erkannt. Und ein Hyperlink in einer E-Mail, der einen Dialer nachlädt, ist kein Virus im klassischen Sinn.

- Verlust von Nachrichten

  Aufgrund einer eingestellten Postfachbeschränkung können viele Werbenachrichten Ihre Mailbox-Grenzen überschreiten, und auch erwünschte Nachrichten, auf die Sie warten, können nicht zugestellt werden. Der Absender erhält die wenig schmeichelhafte Information, dass Ihr Postfach voll ist.

- Datenschutz

  Immer mehr dieser „Spam“-Nachrichten enthalten HTML-Texte, die beim Öffnen weitere Bilder aus dem Internet herunterladen. Der Absender erhält die Chance der Nachverfolgung, da Sie ihm signalisieren, die E-Mail-Adresse ist gültig und wird gelesen. Damit ist die Adresse viel kostbarer bezogen auf den Wiederverkauf an andere Werbefirmen.

- Rechtliche Aspekte

  Nachrichten können Anlagen enthalten, die in einigen Ländern gesetzwidrig sind. Anhand der Empfängeradresse ist nicht zu erkennen, ob ein Kind oder ein Erwachsener dieses Postfach liest. Dies ist aber eher ein Aspekt für Internet-Provider. Aber durch den Empfang liegen solche Nachrichten schon auf dem Unternehmensserver, und nicht jeder Richter wird dafür Verständnis zeigen. Selbst in einer Quarantäne sind solche Inhalte gefährlich.

Letztlich stellt es einfach ein Ärgernis dar, wenn der Missbrauch ein höchst effizientes Kommunikationsmittel wie E-Mail extrem beeinträchtigt.

Nie auf Spam reagieren!

Sie können den Absender um Unterlassung bitten oder auch drohen, werden allerdings schnell feststellen, dass dies Ihre E-Mail-Adresse nur noch wertvoller für den Verkauf macht. Oftmals sind die Absenderadressen ebenfalls gefälscht, so dass Sie dann eventuell einen unbeteiligten Dritten zusätzlich ärgern, dessen E-Mailbox vermutlich schon lange von erbosten Antworten überläuft.

Solange solche Anbieter auf diesem Wege auch nur wenige Opfer finden, die die angebotenen Waren oder Dienstleistungen kaufen, wird weiterhin eine zunehmende Anzahl von Spam oder UCE-Nachrichten verbreitet.

6.4.2 Wo und wie kann geblockt werden?

Einsatzbereiche für Spam-Filter

Der erste Schritt zur Abwehr der unerwünschten Werbenachrichten ist ein Regelwerk, das möglichst viele dieser Nachrichten erkennt, ohne dabei erwünschte Nachrichten zu treffen. Diese Regeln basieren zumeist auf Listen vertrauenswürdiger Empfänger oder berüchtigter Spam-Versender. Sie enthalten auch offene Relays sowie bekannte IP-Adressen von Spam-Sendern und die Analyse der HEADER und des BODY von Nachrichten nach immer aktuelleren Vorgaben (z.B. Viagra).

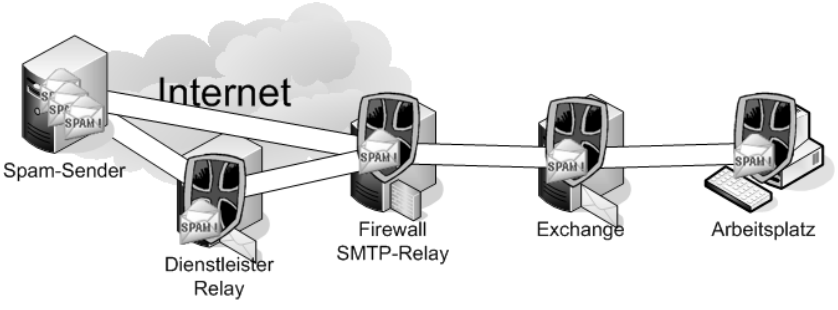


Abbildung 6.8 Stellen für Spam-Filter

Damit beginnt für Sie die Suche nach ausreichenden Lösungen. Entsprechende Filterprogramme werden an mehreren Stellen eingesetzt:

- Client

Junk-E-Mail-Filter in Outlook 2003

Bei der Übertragung der Nachricht in den lokalen Posteingang beziehungsweise nach dem Empfang auf dem Client kann eine Filterung nur noch vom E-Mail-Programm selbst oder einer entsprechenden Zusatzsoftware stattfinden. Die neue Nachricht wird geprüft und bei berechtigtem Verdacht verschoben oder gelöscht. In Verbindung mit Exchange ist diese Variante weniger geeignet, da die Nachrichten bereits empfangen wurden und beim alternativen Zugriff per Outlook Web Access oder anderen Geräten/Clients die Filterfunktion nicht gegeben ist.

- E-Mailserver

  Empfehlenswerter ist der Einsatz einer Software, die auf dem Server zentral alle eingehenden Nachrichten durchleuchtet und bei Bedarf diese als „Spam“ kennzeichnet, verschiebt oder löscht. Aber auch in diesem Fall ist die Nachricht bereits empfangen worden.

- DMZ

  Eine weitere Stelle zur Überprüfung ist der Übertragungsweg aus dem Internet zum Exchange-Server. Eine entsprechende Software kann während des Empfangs die Nachrichten bewerten und gegebenenfalls den Empfang verhindern, die Nachrichten kennzeichnen, verschieben oder löschen.

- Dienstleister

  Die Abwehr von Spam kann auch extern vergeben werden. Dabei zeigt der MX-Eintrag Ihrer Domäne auf den Server des Dienstanbieters. Dieser prüft die Nachrichten und leitet sie an Ihren E-Mail-Server weiter, dessen IP-Adresse ansonsten niemandem im Internet bekannt ist. Viele Spam-Versender umgehen dies aber, indem sie gleich den Backup MX-Eintrag nutzen, der in der Regel auf Ihren richtigen Server verweist, um bei einem Ausfall des Providers weiter ungefiltert Nachrichten zu erhalten.

Für Ihr Unternehmen mit einem Exchange-Server ist der Einsatz einer entsprechenden Software auf oder vor dem Server der Vorzug zu geben. Eine clientbasierte Schutzlösung eignet sich eher für den Privatanwender und Einzelplatzbenutzer.

6.4.3 Entscheidungskriterien

Egal, wo welches Produkte versucht, der Werbeflut Einhalt zu gebieten, so müssen alle Produkte die Nachrichten analysieren und anhand von Filtern und Regeln Entscheidungen treffen. In der Praxis hat sich die Kombination mehrerer Kriterien durchgesetzt, wobei diese Regeln einer permanenten Anpassung unterliegen. Einige davon sind:

Regeln zur Spam-Erkennung

- Whitelist/Blacklist

  Absolute Einträge in Listen blockieren oder erlauben Nachrichten von bestimmten Absender- oder Empfängeradressen oder Servern. Diese Listen werden oft manuell gepflegt oder anhand ausgehender Nachrichten (z.B. Empfänger werden zu erlaubten Absendern) ergänzt. Nach der Erfahrung mit Viren wie „SVEN“ und anderen Schädlingen ist aber allein eine gültige Absenderadresse noch keine Garantie für einen werbefreien Posteingang.

- RBL-Listen und DNS-Prüfungen

  Viele Spammer nutzen offene Relays, dynamische IP-Adressen oder spam-freundliche Provider. Daher gibt es auch Dienste im Internet mit Datenbanken, in denen solche Adressen vermerkt sind. Nachrichten von diesen Systemen könnten mit hoher Wahrscheinlichkeit als Werbung angesehen werden. Allerdings würde dies auch erwünschte Nachrichten betreffen, wenn der Provider oder Absender sein System nicht ordentlich konfiguriert hat, dynamische DSL-Zugänge nutzt oder den Smarthost des Providers umgeht. Auch die Einträge in den Datenbanken sind nicht immer zuverlässig. Zudem hat jeder Anbieter sein eigenes System, um offene Relays zu erkennen, die auch nicht immer fehlerfrei arbeiten.

  Ihr E-Mailserver könnte auch prüfen, ob der Absenderserver überhaupt selbst ein E-Mailserver und über DNS auflösbar ist. Allerdings gibt es hierzu keine Pflicht, so dass auch diese Kriterien nicht allein entscheidend sein können.

- Statische Regeln auf Inhalte

  Nachrichten können z.B. anhand von bestimmten Worten im Betreff oder Nachrichtentext oder bei ungültigen E-Mail-Adressen, exotischen Zeichensätzen etc. als unerwünscht klassifiziert werden.

- Bayes-Filter

  Selbst lernende Filter mit ausgeklügelten Wortlisten können ebenfalls Nachrichten anhand von Wortlisten in erwünscht und unerwünscht unterscheiden. Ähnlich der heuristischen Suche von Virenscannern wird hier versucht, anhand von Wahrscheinlichkeiten und Worten diese Entscheidung zu fällen und damit die Erkennungsrate im Gegensatz zu statischen Wortlisten zu erhöhen.

Die meisten Produkte setzen auf eine Kombination mehrerer Regeln mit einer Gewichtung der Einzelergebnisse. In der Zukunft wird es sicher weitere ausgeklügelte Regeln geben, und ähnlich zu den Aktualisierungen für Virenscanner werden auch bei der Behandlung unerwünschter Nachrichten immer wieder Aktualisierungen notwendig sein.

Das Problem jeder Erkennungssoftware ist die Wahrscheinlichkeit, dass gute Nachrichten irrtümlich blockiert werden. Folgende Tabelle zeigt die möglichen Entscheidungen:

Tabelle 6.3 Entscheidungen bei Spam

Verbindung	Zugestellt	Blockiert
Gute Nachricht	o.k.	„False Positive“
Unerwünschte Nachricht	Störend, aber tolerierbar	o.k.

Hierbei werden zwei mögliche Fehlentscheidungen einer Software sichtbar. Solange gute Nachrichten zugestellt und unerwünschte Nachrichten blockiert werden, ist die Welt in Ordnung. Werden einige unerwünschte Nachrichten fälschlicherweise auch zugestellt, dann ist dies zwar ärgerlich, aber bis zu einem bestimmten Grad tolerierbar. Was möglichst nicht passieren sollte, ist die Blockade erwünschter Nachrichten. Diese so genannten „False Positive“ werden sich aber nie ganz vermeiden lassen, aber die Anzahl sollte möglichst gering sein. Leider sind beide Fehlentscheidungen eng miteinander verbunden. Je weniger „False Positive“ erreicht werden sollen, desto schlechter wird auch die Erkennungsrate, so dass automatisch mehr unerwünschte Nachrichten den Filter ungeblockt passieren.

Hinzu kommt, dass es keine allgemein gültigen Grundsätze für „Erwünscht“ und „Unerwünscht“ gibt. Eine Nachricht kann je nach Empfänger unterschiedliche Reaktionen hervorrufen. Insofern müssen Filter entweder personalisierbar werden oder keine Entweder-oder-Entscheidungen treffen, sondern gewichten.

Das Problem bei allen blockierten Nachrichten ist, dass der angebliche Absender nicht informiert werden sollte. Die meisten Absenderadressen sind gefälscht, so dass Sie selbst zum Versender unerwünschter Nachrichten werden. Damit werden natürlich auch keine Absender informiert, deren Nachricht fälschlicherweise aussortiert wurde.

6.4.4 Behandlung von Spam

Wird eine Nachricht als unerwünscht klassifiziert, gibt es gleich mehrere Varianten, diese Nachricht zu behandeln:

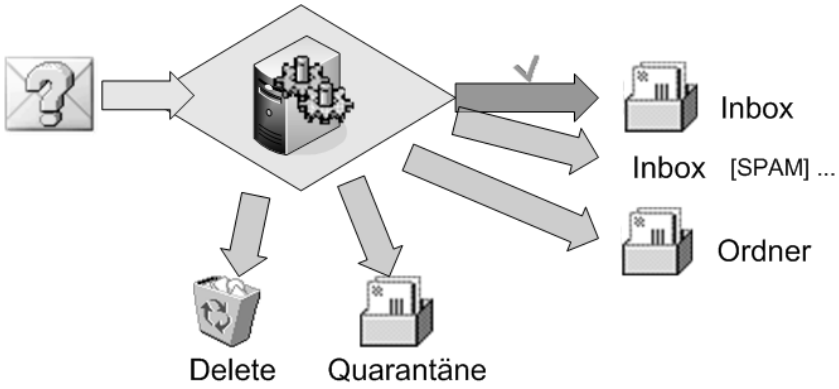


Abbildung 6.9 Spam-Verarbeitung

Nachdem eine Nachricht als Spam klassifiziert wurde, gibt es mehrere Varianten, mit der Nachricht zu verfahren.

Ist die Filtersoftware zugleich das erste System, welches eine Nachricht aus dem Internet erreicht, dann kann die Annahme der Nachricht abgelehnt werden.

- Beim Empfang die Verbindung beenden.

  Spam-Eingang abwenden

  Bei einer Prüfung während des Empfangs ist eine direkte Unterbrechung der Verbindung denkbar, so dass die Gegenseite die Nachricht erst gar nicht komplett übertragen kann. Die Gegenseite erzeugt die Unzustellbarkeitsnachricht, und Ihr Übertragungsvolumen wird eingespart. Da die Nachricht nie empfangen wurde, kann Ihnen niemand vorwerfen, Sie hätten eine Nachricht gelöscht.

Diese Alternative steht Ihnen aber nur dann zur Auswahl, wenn die Schutzsoftware am Eingang Ihres Netzwerks steht und die Nachrichten zuerst erhält. Prüft Ihre Spam-Software die Daten jedoch erst nach dem Empfang, findet eine Verarbeitung der E-Mails statt, für die folgende Alternativen zur Auswahl stehen:

- Globale Quarantäne

  Spam-Verarbeitung

  Eine als Spam erkannte Nachricht wird auf dem Server in einem gesonderten Bereich festgehalten. Der Anwender erhält diese Nachrichten nicht. Problematisch ist hier die irrtümliche Quarantäne von „guten“ Nachrichten zu sehen. Kein Administrator wird regelmäßig alle Nachrichten nach Falschklassifizierungen durchstöbern, um Irrläufer zu entdecken, sondern nur wenn ein Anwender eine Nachricht erwartet und diese vermisst.

- Quarantäne beim Benutzer

  Serverbasierte Produkte legen im Postfach des Anwenders einen neuen Ordner „Junk-Mail“ oder Ähnliches an und sortieren dort die Nachrichten ein. Damit bleibt der eigentliche Posteingang verschont, trotzdem kann der Anwender bei Bedarf in diesem Ordner nachschauen. Diese Variante kostet allerdings wieder Speicherplatz und Arbeitszeit.

- Kennzeichnen

  Systeme, die keine Ordnerstruktur anbieten (z.B. reine POP3-Server), markieren oft die erkannten Nachrichten mit Kennzeichnung, oft im Betreff. Der Anwender kann basierend hierauf eigene Regeln und Filter in der E-Mail-Software einstellen, um diese Nachrichten automatisch zu verarbeiten.

- Löschen

  Das direkte Löschen von vermeintlich erkannten Nachrichten belastet den Empfänger und das E-Mail-System am wenigsten. Da die Bewertung der Filter aber nicht fehlerfrei sein kann, kann dadurch auch eine erwünschte Nachricht gelöscht werden. Aufgrund der gesetzlichen Forderung nach Nachvollziehbarkeit in bestimmten Geschäftsbereichen ist dieser Ansatz nur sehr selten realisierbar.

Alle Methoden haben individuelle Vor- und Nachteile. Es wird immer die Unsicherheit bestehen, eine gute Nachricht irrtümlich als Werbung zu klassifizieren. In dieser Hinsicht sollte der Absender nach einiger Zeit die Daten erneut senden, auch wenn laut Sendeprotokoll diese Nachricht erfolgreich zugestellt wurde. Hier hilft die Funktion des Einschreibens nur indirekt. „Anti-Spam“-Produkte, die die Nachricht erst nach dem Empfang im Postfach prüfen, können die Quittung des E-Mailservers nicht mehr aufhalten. Nur die „Gelesen“-Quittung garantiert dem Absender, dass die Nachricht wirklich angekommen ist.

Rechtliche Aspekte

Unabhängig von dem technischen Aspekt ist die rechtliche Seite. So verbietet §303a StGB zur Datenveränderung, dass Nachrichten ohne Zustimmung des Empfängers unterdrückt werden dürfen. Ein Postbote darf auch nicht einfach einen Brief nicht zustellen.

Der §206 Abs. 2 StGB (Verletzung des Post- oder Fernmeldegeheimnisses) hingegen verbietet es, dass die Nachricht als solche einer Inspektion unterzogen wird. Dies ist aber zur Erkennung von Spam, aber auch von Viren notwendig.

Als Quintessenz sollten Sie auf jeden Fall bei dem Einsatz einer Lösung die Erlaubnis der Anwender einholen und aktiv über die Funktion und die Folgen informieren.

Eine Empfehlung für ein Produkt oder eine Auswahl kann dieses Buch nicht erlauben, denn dieses Gebiet ist gerade sehr im Umbruch. Bewerten Sie selbst die verschiedenen Schutzmodelle und Verfahren, und vergleichen Sie die in Frage kommenden Produkte. Das Thema Spam-Nachrichten wird sich ähnlich wie bei den Virenscannern entwickeln. Die Versender von Spam und die Anbieter von Schutzsoftware werden immer wieder ihre Produkte anpassen.

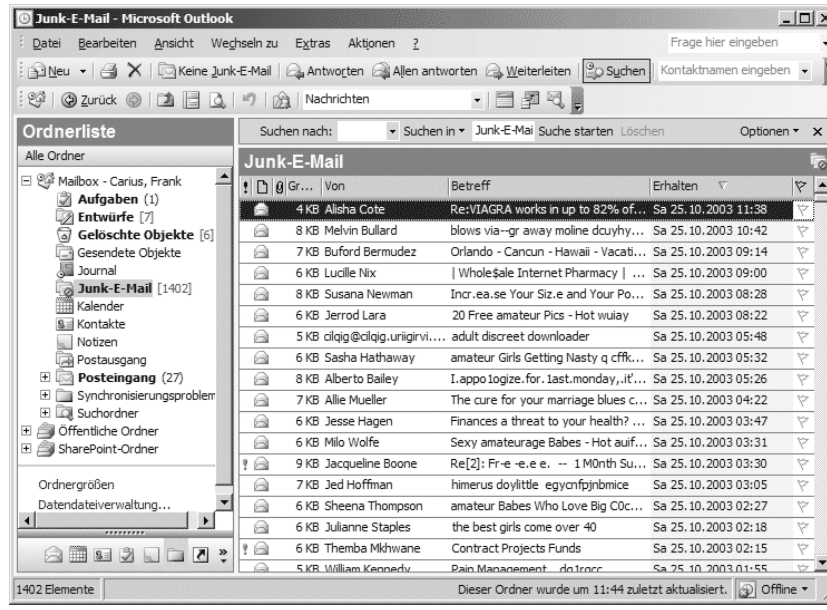
6.4.5 Outlook 2003-Junk-E-Mail

Microsoft ist im Bereich der Spam-Bekämpfung ebenfalls nicht untätig und hat Outlook 2003 mit einer Junk-Mail-Funktion ausgestattet, die verdächtige Nachrichten in einen eigenen Ordner „Junk-E-Mail“ verschiebt. Dazu nutzt Outlook vom Anwender zu pflegende Adresslisten und einen eigenen statischen Wortfilter. Die vom Benutzer in Outlook 2003 gepflegten Listen werden auf den Exchange 2003-Server hochgeladen und dort verarbeitet. Zusätzlich ist für Exchange 2003 eine serverbasierte Lösung angekündigt, die direkt auf dem Server die Nachrichten in den Junk-E-Mail-Ordner des Anwenders einsortiert.

Exchange 2003 selbst kann heute schon Verbindungen von Systemen ablehnen, die in den verschiedenen Datenbanken (RBL, ORDB etc.) geführt werden. Aber auch diese Verfahren können nur ein Teil einer Strategie sein und funktionieren nur, wenn Ihr Exchange 2003-Server direkt die Nachrichten aus dem Internet empfängt.

Auch wenn der Spam-Filter in Outlook 2003 nur statisch ist, so war die Erfolgsrate in den ersten Wochen beeindruckend. Outlook hat in Franks persönlichem Postfach in zwanzig Tagen über 1400 Werbenachrichten aussortiert und dabei keine einzige falsche Nachricht verschoben. Aber ebenso ist erkennbar, dass die Versender sich darauf einstellen, denn die Anzahl an nicht erkannten Nachrichten wird von Tag zu Tag größer.

Abbildung 6.10
Outlook
Junk-E-Mail



Insgesamt haben sich in den letzten drei Jahren fast 20.000 Nachrichten allein in Franks Postfach gesammelt.

Es ist zu erwarten, dass die Menge an unerwünschten Nachrichten stärker zunehmen wird, je mehr Filter in Firmen eingesetzt werden, da die Absender immer mehr Nachrichten aussenden müssen, um für ihre Geschäfte ausreichend Opfer zu finden. Damit ähnelt diese Thematik stark dem Wettstreit zwischen Grippeviren und modernen Medikamenten, bei denen sich die Viren immer wieder verändern müssen, um überhaupt noch Opfer zu finden. Letztlich muss es sich zeigen, ob nicht vielleicht das Medium E-Mail als offene Plattform zum Austausch von Nachrichten in einiger Zeit sogar unbrauchbar wird und andere Ansätze gefunden werden müssen. Ein Lösungsansatz könnte darauf hinauslaufen, dass irgendwann entweder die Absender und Empfänger selbst oder die E-Mailserver untereinander auf einer Autorisierung durch Zertifikate bestehen und damit die Anonymität heutiger Absender wegfällt. Im Moment ist dies noch nicht durchsetzbar. Damit bekommt das Thema S/MIME, PGP und SMTP über SSL (TLS) eine ganz neue Bedeutung. Aber selbst dann bleibt noch die Frage der gesetzlichen Rahmenbedingungen beim Versand solcher Nachrichten. Was hilft Ihnen die Gewissheit, wer der Absender ist, wenn Sie nicht dagegen vorgehen können. Dann beginnt das Spiel erneut mit Listen vertrauenswürdiger und nicht erwünschter Absender anhand der Zertifikate.

6.5 Intelligent Message Filter und Sender-ID

IMF klassifiziert SMTP-Mails

Seit Sommer 2004 bietet Microsoft allen Unternehmen mit eingesetzten Exchange 2003-Servern das kostenfreie Zusatzmodul „Intelligent Message Filter (IMF)“ zur Installation an. IMF erweitert ihren Exchange 2003-Server um die Analyse von per SMTP eingehender E-Mails und versieht sie mit einer Bewertung. Abhängig von dieser Bewertung kann der SMTP-Server die E-Mail ablehnen, in ein Archiv verschieben oder durchlassen. Der Postfachserver kann anhand dieser Bewertung die E-Mail auf dem Server in den besonderen Ordner „Junk-E-Mail“ einsortieren. Service Pack 2 enthält das neue IMF Version 2 sowie auch einen Absendererkennungsfilter (Sender-ID). In den folgenden Abschnitten lesen Sie etwas mehr zu den Funktionen, der Installation und Konfiguration sowie den bisherigen Erfahrungen.

6.5.1 Was ist SCL?

Spam Confidence Level zeigt Spam-Wahrscheinlichkeit an.

SCL ist die Kurzform von „Spam Confidence Level“ und beschreibt mit einer Zahl zwischen -1 und 9 die Wahrscheinlichkeit, dass eine Nachricht wirklich Spam ist. Microsoft nutzt zur Ermittlung des Wertes eine „SmartScreen“ genannte Technologie, die bei Microsoft Research zusammen mit Hotmail/MSN entwickelt wurde. Mit Exchange Service Pack 2 kommen weitere Verbesserungen bei der Nachrichtenreinhaltung hinzu.. Leider sind die internen Methoden nicht veröffentlicht. Auf http://go.microsoft.com/fwlink/?LinkId=25910 wird aber allgemein erklärt, dass der Filter mit Wahrscheinlichkeiten arbeitet und mit vielen Nachrichten für den Einsatz trainiert wurde. Microsoft wird zukünftig auch immer wieder Aktualisierungen veröffentlichen, um die Aktualität des Filters zu gewährleisten.

Das Ergebnis dieser Bewertung wird in einem gesonderten Feld jeder Nachricht mit abgespeichert und kann in Outlook mit etwas Bastelei auch sichtbar gemacht werden.

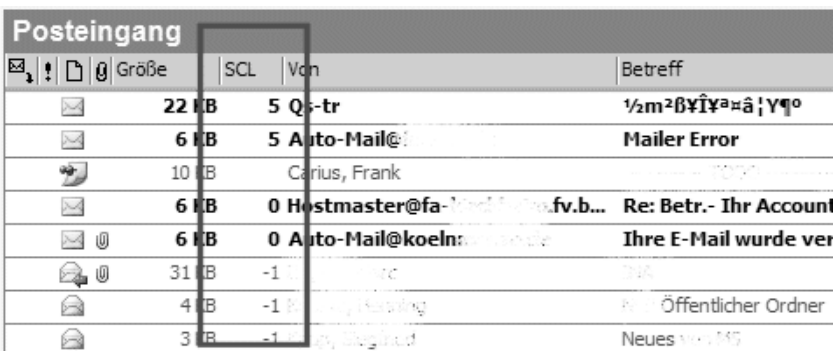


Abbildung 6.11 SCL in Outlook anzeigen

6.5.2 Funktionsweise

Eine Exchange-Organisation besteht aus einem oder mehreren Exchange-Servern, die zusammengeschaltet für die Weiterleitung von Nachrichten zuständig sind. IMF besteht aus zwei Komponenten, die gemeinsam die Verarbeitung übernehmen:

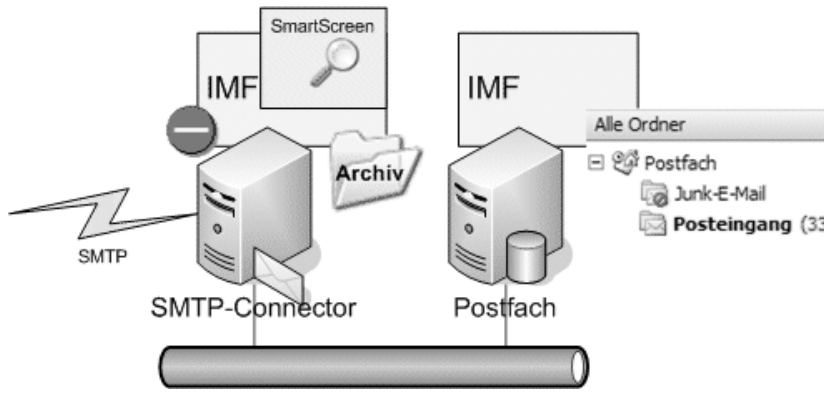
- SMTP-Erweiterung

  Der virtuelle SMTP-Server wird durch IMF derart erweitert, dass eingehende Nachrichten mittels SmartScreen analysiert und klassifiziert werden. Abhängig von der Höhe der Klassifizierung kann diese Komponente E-Mails direkt ablehnen, in ein Archiv verschieben oder an den Postfachspeicher übergeben.

- Informationsspeicher

  Die Installation von IMF auf dem Postfachspeicher übernimmt die Funktion, Nachrichten ab einem eingestellten SCL-Wert direkt in den Ordner „Junk-E-Mail“ des Postfachs umzuleiten und nicht dem Posteingang zuzustellen.

Abbildung 6.12 Funktionsweise des IMF



Damit IMF eine eingehende Nachricht überhaupt bewertet, muss die SMTP-Verbindung „Anonym“ sein, d.h. SMTP darf nicht mit einer Anmeldung arbeiten. IMF kontrolliert nur anonym zugestellt E-Mails. Dadurch wird verhindert, dass bei der Zustellung zwischen mehreren Exchange-Servern mittels SMTP die Überprüfung immer wieder durchgeführt wird, und zudem erlaubt es den vertrauenswürdigen Kommunikationspartnern die Blockade über eine SMTP-Anmeldung zu umgehen. Bei der Übertragung über das Internet werden die Nachrichten fast immer anonym übertragen. Dieses Verhalten stellt für das E-Mail-System keine Gefahr dar, solange Sie das Konto „Gast“ in ihrer Domäne deaktiviert haben.

Selbst beim Verzicht auf die SmartScreen-Funktion des IMF bietet dieser eine zusätzliche, aber wesentliche Erweiterung der Exchange 2003-Server. Der Zugang auf die SCL-Ergebnisse ist für Entwickler möglich, und so

können Sie selbst mittels Skripte diesen Wert jederzeit setzen. Dies eröffnet unter anderem auch die Möglichkeit, Lösungen eines Drittherstellers oder OpenSource-Programme wie SpamAssasin und andere einzusetzen, die normalerweise eine E-Mail im Betreff oder über besondere Felder im Header der Nachricht kennzeichnen. Ein Exchange-Transport-EventSink könnte nun diese E-Mail auswerten und die Ergebnisse der vorgelagerten Spamschutzlösung in das Feld für den SCL-Wert eintragen. IMF auf dem Postfachspeicher verschiebt dann diese E-Mail weiterhin nach Junk-E-Mail.

Es ist jedoch nicht möglich, den SCL-Wert über eine anonyme SMTP-Verbindung direkt in einer Nachricht mit zu übergeben. Dies würde es einem Spammer doch zu einfach machen.

6.5.3 IMF aktivieren

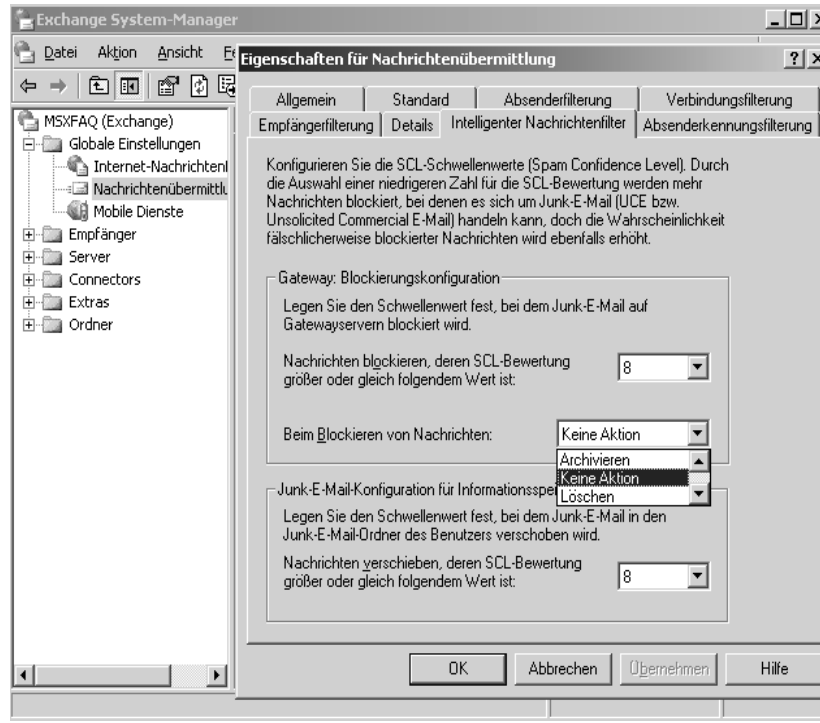
Im Gegensatz zur ersten Version des Intelligent Message Filters wird der IMF Version 2 mit dem Update von Exchange Service Pack 2 installiert. Anschliessend muss der IMF noch aktiviert werden. Dazu gibt es im Exchange System Manager zusätzliche Eigenschaften:

- Globale Einstellungen der Nachrichtenübermittlung (Aktion, SCL-Level)
- Aktivierung auf dem virtuellen SMTP-Server

Die Installation des IMF erweitert die Eigenschaften der Nachrichtenübermittlung um die Register INTELLIGENTER NACHRICHTENFILTER und ABSENDERKENNUNGSFILTERUNG. Ebenso sollten Sie beim Einsatz von IMF die IP-Adressen der SMTP-Server Ihres Netzwerks sowie Ihrer DMZ hinzufügen, um die Annahme des internen Nachrichtenverkehrs zu gewährleisten.

Unter INTELLIGENTER NACHRICHTENFILTER können Sie den SCL-Schwellenwert festlegen und was mit den Nachrichten geschehen soll. Da es sich bei der Nachrichtenübermittlung um eine „Globale Einstellung“ handelt, ist die Konfiguration des IMF für die komplette Organisation gültig. Eine Steuerung auf Basis von Servern, Postfachspeichern oder SMTP-Domänen ist nicht möglich.

Abbildung 6.13 Intelligenter Nachrichtenfilter



Logisch befindet sich diese Einstellung an der gleichen Stelle, an der auch Empfangsbeschränkungen, basierend auf der E-Mail-Adresse oder die Nutzung von RBL-Servern konfiguriert wird. Diese Funktionen liefert Exchange 2003 von Hause aus schon mit.

Damit per SMTP eingehende Nachrichten auch durch IMF mit einem SCL-Wert versehen werden, müssen Sie die Funktion auf dem jeweiligen virtuellen SMTP-Server aktivieren. In einigen Fällen macht es Sinn, einen weiteren virtuellen SMTP-Server zu konfigurieren, der die Nachrichten ohne Filter übermittelt. Dies ist hilfreich, wenn Sie Partner über ein VPN angebunden haben oder andere interne Systeme z.B. Benachrichtigungen an ein Exchange-Postfach senden und Sie die Zustellung sicherstellen müssen. Alternativ könnten die Absender sich natürlich auch per SMTP anmelden, um den Filter zu umgehen.

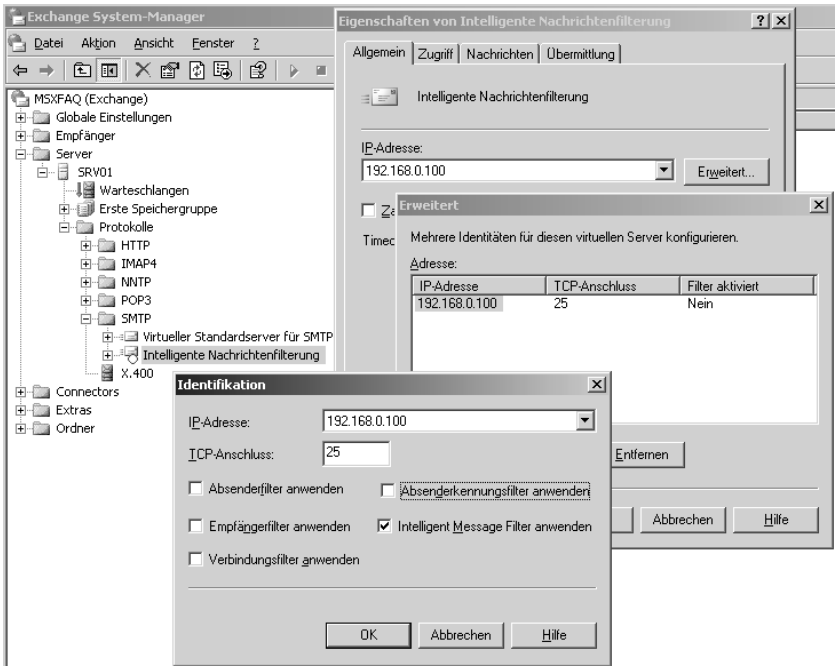


Abbildung 6.14 SMTP-Server mit Intelligenter Nachrichten-filterung

Erst nach dem Setzen der Checkbox in den SMTP-Eigenschaften des Servers werden eingehende Nachrichten an IMF übergeben und durch den SmartScreen-Filter geschleust. Weitere Konfigurationen wie die Nutzung eigener Schlüsselwörter sind nur auf mühsamen Wege ohne Benutzer-oberfläche möglich.

Damit die Nachrichten bei Anwendern in den Ordner Junk-E-Mail verschoben werden, müssen Sie IMF auf jedem Postfachserver installieren. Beachten Sie hierzu auch die von Microsoft bereitgestellten weiterführenden Informationen für größere Umgebungen und Installation auf einem Cluster.

6.5.4 Absenderkennung und Anti-Pishing

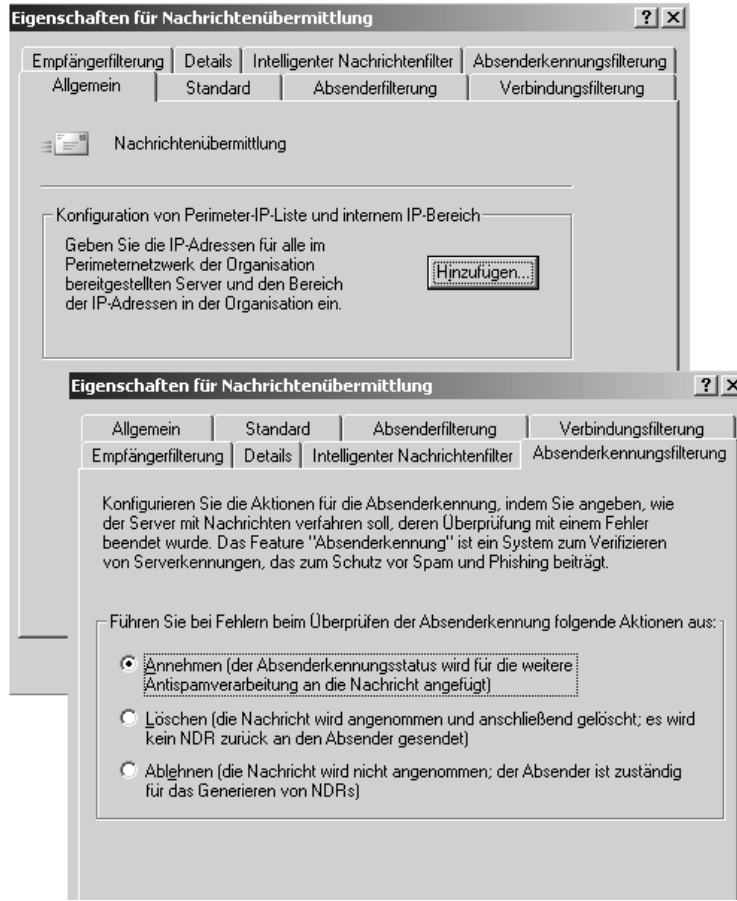
Sender-ID im Aufbau

Häufig verwenden Spammer falsche Domänen, um so E-Mails zustellen zu können und über Pishing an Benutzerdaten zu gelangen. Ein weiteres Feature von Exchange SP2 soll diese Spam-Lücke schließen, indem der Domänenname überprüft wird, von dem die E-Mail gesendet wurde. Dabei wird die Absender-IP mit den offiziell im DNS verzeichneten SMTP-Servern der Domäne verglichen. Vorausetzung für dieses Verfahren ist jedoch, dass jeder Inhaber einer E-Mail-Domäne neben dem MX-Record auch alle ausgehenden Mailserver im DNS veröffentlicht.

In den Eigenschaften der Nachrichtenübermittlung definieren Sie über ABSENDERKENNUNGSFILTERUNG, wie der Server mit den als fehlerhaft gekennzeichneten Nachrichten verfahren soll. Zuvor müssen Sie die

Absenderkennungsfilterung in den Eigenschaften des virtuellen SMTP-Servers genau wie das IMF aktivieren.

Abbildung 6.15 Aktion bei Sender-ID-Erkennung



6.5.5 IMF-Praxis

Obwohl die Einrichtung und Konfiguration des IMF so einfach erscheint, ist das Programm jedoch so wirkungsvoll, dass viele Firmen erstmal auf den Einsatz von Zusatzprodukten verzichten können. Es ist damit zu rechnen, dass Microsoft auch für den IMF aktualisierte Datenbanken bereitstellt (ähnlich dem OfficeUpdate für Outlook 2003), damit dieser auch zukünftig sehr effektiv und vor allem kostengünstig die Anzahl der Werbemails gering hält.

SCL-Wert richtig setzen

Allerdings müssen Sie als Administrator die richtigen SCL-Grenzwerte für ihr Unternehmen bestimmen. Bestimmen Sie einen zu hohen Wert, werden zu viele Nachrichten in den Postfächern der Mitarbeiter landen. Setzen Sie hingegen den Wert tiefer an, steigt die Wahrscheinlichkeit, dass auch gute

Nachrichten in den Ordner „Junk-E-Mail“ landen. Um dieses Risiko gering zu halten, könnten Sie den IMF anweisen, Nachrichten ab einem bestimmten Schwellenwert einfach abzulehnen und auf den Junk-E-Mail-Ordner zu verzichten. Ein guter Absender wird sich aufgrund der Unzustellbarkeitsmeldung seines eigenen E-Mail-Servers sicher melden.

Abhängig vom Unternehmen und eigener Richtlinien zur Bearbeitung von Nachrichten müssen Sie einen Kompromiss finden, diese E-Mails zu filtern. Dazu zählt die Ablehnung von Nachrichten, die Einsortierung in den Ordner „Junk-E-Mail“ und das Risiko der irrtümlich abgelehnten oder in Junk-E-Mail einsortierten Nachrichten. So bietet es sich an, IMF zuerst einmal ohne aktiven Eingriff zu konfigurieren und die individuelle Verteilung der Werbemails in Ihrem Unternehmen anhand der verfügbaren Performancecounter sowie einer angepassten Ansicht in Outlook zu analysieren.

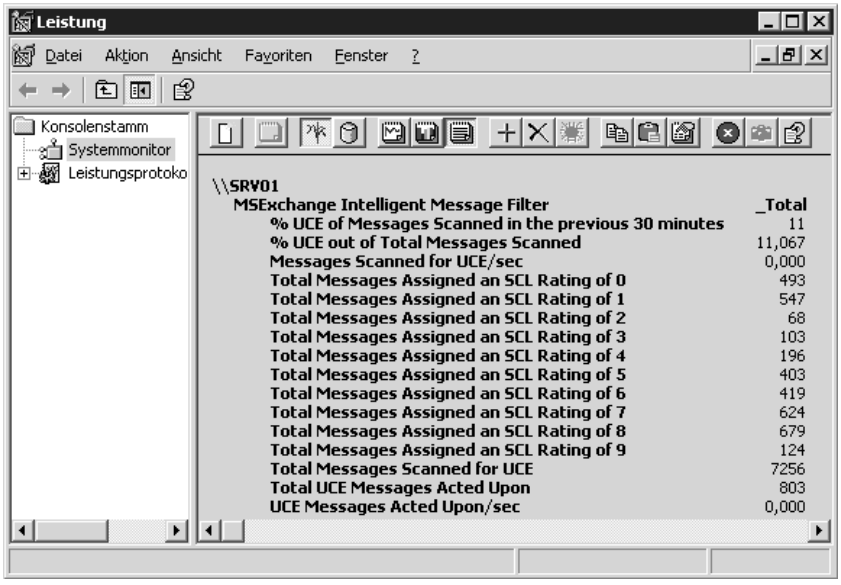
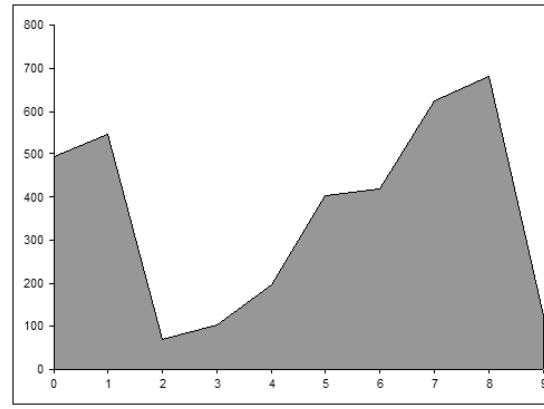


Abbildung 6.16 Performance-Monitor

Eine grafische Aufarbeitung der Zahlen lässt die Verteilung besser erkennen.

Abbildung 6.17 SCL-Rate eingehender E-Mails



Sie können deutlich erkennen, dass viele Nachrichten eindeutig als gut eingestuft werden, dass jedoch weit mehr Nachrichten mit einem hohen SCL-Wert als Spam klassifiziert werden. Eine kleinere, aber nicht unbedeutende Zahl an E-Mails finden sich mit einem SCL-Wert zwischen zwei und vier im Mittelfeld. Bei solch einer Verteilung könnte es sinnvoll sein, Nachrichten mit einem SCL von fünf bzw. sechs oder höher bereits auf dem SMTP-Server zu blocken und Nachrichten mit einem SCL von drei bzw. vier und höher auf dem Informationsspeicher in den Junk-E-Mail-Ordner zu verschieben. Damit wäre ein Großteil der Spam-Nachrichten schon vor der Zustellung blockiert und die Menge der vom Anwender zu kontrollierenden Nachrichten im Ordner Junk-E-Mail überschaubar.

6.5.6 Grenzen des IMF

Einschränkungen für den Einsatz von IMF

Ehe Sie nun tatkräftig den IMF installieren, sollten Sie noch einmal die Randbedingungen und Einschränkungen kontrollieren. Eventuell ist IMF wegen einem oder mehrerer dieser Punkt nicht für Sie geeignet, so dass Sie nach Drittprodukten Ausschau halten müssen.

- Kein Virenscanner

  Die Filterfunktion von SmartScreen ersetzt keinen Virenscanner. Hierfür müssen Sie weiterhin ein Produkt einsetzen. Wird der Virenscanner als vorgeschaltetes Relay eingesetzt, ist es nicht mehr möglich, die entsprechenden Spam-Nachrichten über den IMF abzulehnen.

- Ablehnen nur bei direkter Verbindung

  Viele Unternehmen erhalten Ihre E-Mails trotz Exchange-Server nicht direkt aus dem Internet, sondern über ein Relay oder einem Provider. In diesem Fall dürfen Sie die Nachrichten nicht ablehnen, da sonst Ihr Relay mit Unzustellbarkeitsmeldungen selbst zum Störfaktor wird. Nur das erste System, welches die E-Mail empfängt, kann die Verbindung mit einer Fehlermeldung vorzeitig beenden.

- Wenig transparente Wirkungsweise, keine eigenen Anpassungen

  Die Funktion des SmartScreen-Filters ist nicht offen gelegt und nicht modifizierbar. Insofern können Sie keine abweichenden Regeln für bestimmte Empfänger oder Gruppen einrichten. Alle Empfänger unterliegen der gleichen Einstufung.

- „False Positive“

  Blockieren Sie die Nachrichten nicht direkt durch den ersten SMTP-Server, können auch wichtige Nachrichten im Ordner „Junk-E-Mail“ landen und damit dem Benutzer verborgen bleiben. Die Praxis hat gezeigt, dass die wenigsten Anwender sich die Mühe machen, diesen Ordner regelmäßig zu sichten.

- Keine Whitelist durch den Anwender

  Häufig müssen E-Mails, die irrtümlicherweise als Spam klassifiziert wurden, vom Anwender aus dem Junk-E-Mail-Ordner herausgenommen werden. Jedoch ist es dem Anwender nur bedingt möglich, den IMF durch individuelle Regeln zu umgehen, sodass bei erneuter Zustellung besagter E-Mail diese als „gut“ eingestuft wird. Besonders schwierig zu konfigurieren sind Nachrichten, die bereits am SMTP-Server abgelehnt werden. Faktisch ist es dem Absender nicht möglich, in solch einem Fall eine Zustellung zu erreichen, ohne dass die E-Mail geändert wird und somit die Hoffnung auf eine freundlichere Einstufung durch SmartScreen besteht.

- Keine eigenen bzw. zusätzlichen Filter

  Neben dem SmartScreen-Filter bietet Exchange 2003 noch die Möglichkeit nach weiteren Kriterien zu filtern, wie dem Empfänger, dem angeblichen Absender und der IP-Adresse. Weitergehende Filter sind aktuell nicht möglich und im IMF nicht einfach zu integrieren. Auch wenn die SmartScreen-Funktion für viele Firmen ausreichend erscheint, ist es nur eine Frage der Zeit, bis Spammer ihre Nachrichten entsprechend umgestalten. Aktualisierungen können später durch Microsoft erfolgen, aber werden sicher nur mit einem zeitlichen Verzug verfügbar sein. So haben Sie nicht die Möglichkeit, unter anderem mit einfachen Wortlisten oder Textbausteinen aktuelle Spam-Nachrichten etwas abzumildern. Sie können zwar wie bisher mit eigenen Transport-EventSinks arbeiten, diese greifen jedoch erst nach der Annahme der E-Mails. Eine Ablehnung ist damit nicht mehr möglich.

Diese Aufzählungen könnten den Anschein erwecken, dass IMF noch nicht ausgereift wäre. Dem ist freilich nicht so. IMF ist nach der einfachen Installation auf dem Exchange 2003-Server ein wesentlicher Beitrag von Microsoft zur Eindämmung der Flut unerwünschter Nachrichten und kann in

vielen Installationen den Einsatz von kostenpflichtigen Drittprodukten ersparen.

6.5.7 Postfach-Verwaltung

Anstieg des Datenbank-volumens durch alte Junk-E-Mails.

Viele Anwender beachten den Ordner „Junk-E-Mail“ nicht weiter und löschen auch den Inhalt dort nicht. Für einen Administrator stellt sich daher die Frage, wie er alte Nachrichten im Junk-E-Mail-Ordner nach einiger Zeit möglichst automatisch entfernen kann. Zwar können viele Nachrichten schon bei der Übertragung abgelehnt werden, aber auch die Nachrichten im Ordner „Junk-E-Mail“ können nach und nach den Server füllen. Gerade die Exchange Standard-Server mit einer Datenbanklimitierung auf 16 GB sind hier gefährdet. Schon seit längerer Zeit gibt es von Microsoft die Postfach-Verwaltung, die ferner eine automatische Entfernung von Elementen aus Ordnern ermöglicht. Dieses Hilfsmittel ist gerade für die Wartung des Ordners „Junk-E-Mail“ sehr gut geeignet, um Nachrichten nach Ablauf einer bestimmten Frist zu löschen.

In der Regel tauschen die Kommunikationspartner häufig E-Mails aus oder melden sich anderweitig, wenn eine Antwort ausbleibt. Wird vom IMF irrtümlich eine E-Mail nach „Junk-E-Mail“ verschoben und dies vom Anwender nicht erkannt, wird in den meisten Fällen der Absender nachfragen. Der Anwender kann dann die E-Mail immer noch zurückholen. Damit dieser Ordner aber nicht zu groß wird, sollten die Spam-Nachrichten nach einiger Zeit gelöscht werden. Die Anwender erledigen dies nur sehr unregelmäßig oder gar nicht. Daher macht es Sinn, die Postfach-Verwaltung auf dem Server mit dem Löschen zu beauftragen. Ehe Sie diese Funktion nun aktivieren, sollten Sie auf jeden Fall die Zustimmung der Mitarbeiter und Firmenleitung einholen, denn die Gefahr besteht, dass eine wichtige E-Mail, die lange unerkannt im Junk-E-Mail-Ordner liegt, endgültig gelöscht wird. Zudem sind rechtliche Aspekte zu beachten.

Junk-E-Mails über Richtlinie löschen

Die Postfach-Verwaltung wird über die Empfängerrichtlinien gesteuert. Beim Anlegen einer neuen Richtlinie legen Sie die Art der Richtlinie fest. Neben den E-Mailadressen können ebenfalls die Postfachinhalte kontrolliert werden.

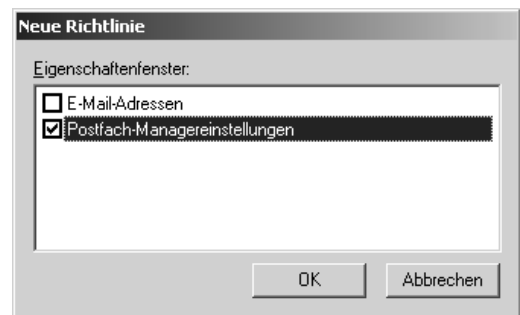


Abbildung 6.18 Neue Empfänger-richtlinie

Sie können ebenso eine bestehende Richtlinie um die Einstellungen für den Mailbox Manager ergänzen.

Nachdem Sie einen Namen für die Richtlinie gewählt haben, können Sie über die LDAP-Filterregel die Zielpostfächer bestimmen. Auf der Karteikarte POSTFACH-MANAGEREINSTELLUNGEN (RICHTLINIE) legen Sie den Ordner sowie die durchzuführende Aktion fest.

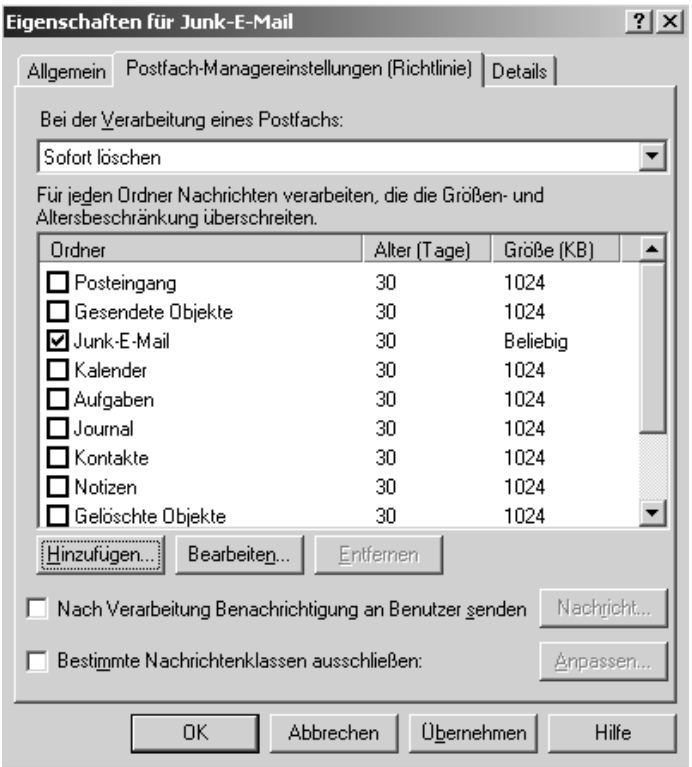
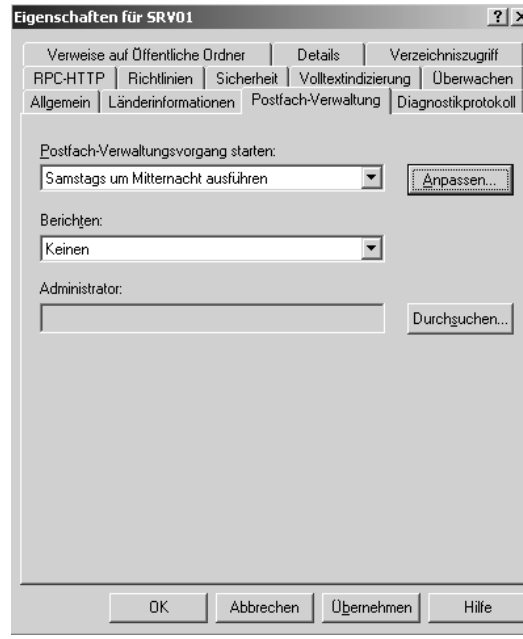


Abbildung 6.19 Richtlinie zum Löschen von Junk-E-Mails

Hier müssen Sie für die Steuerung des Inhalts des Ordners „Junk-E-Mail“ erst alle anderen Standardordner deaktivieren und dann den Junk-E-Mail-Ordner hinzufügen. Im gezeigten Beispiel löscht der Mailbox-Manager in allen Postfächern, für die diese Richtlinie gilt, alle Junk-E-Mails, die älter als 30 Tage sind. Sie können die Postfach-Verwaltung ferner so konfigurieren, dass nur ein Bericht erstellt und versendet wird. Ändern Sie dazu die Einstellung von „Sofort löschen“ auf „Nur Bericht erstellen“ und tragen Sie einen Empfänger für den Bericht ein.

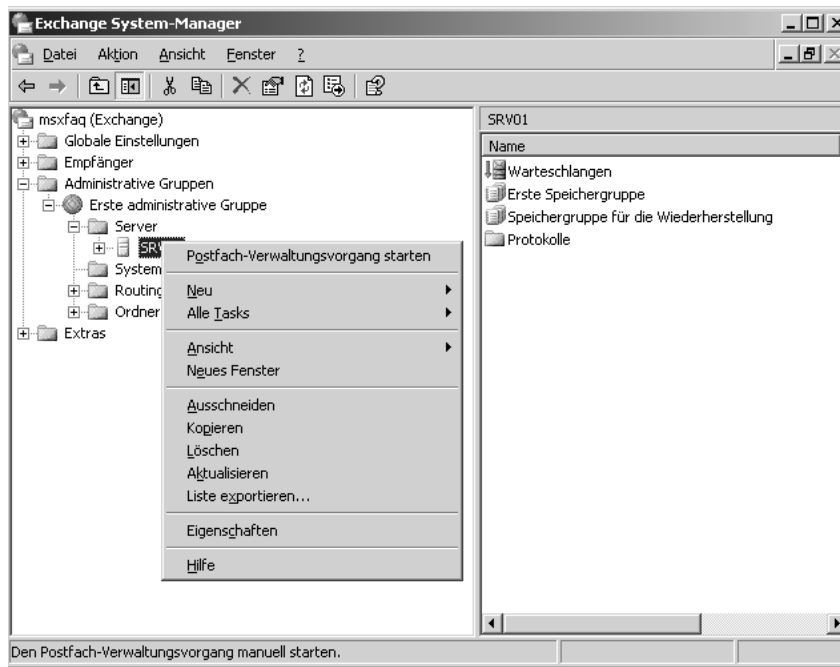
Damit die Postfach-Verwaltung aktiv wird, müssen Sie im Exchange System Manager in den Eigenschaften des jeweiligen Servers die Postfach-Verwaltung starten. In der Voreinstellung wird die Postfachverwaltung nicht ausgeführt.

Abbildung 6.20 Postfach-Verwaltung des Servers starten



Da die Postfach-Verwaltung eine größere Belastung für den Server darstellt, sollten Sie den Aufruf während einer lastarmen Zeit und nicht zeitgleich zum Backup einplanen. Sie können die Postfach-Verwaltung aber auch über das Kontextmenü sofort starten:

Abbildung 6.21 Postfach-Verwaltungsvorgang



Teil III

Der folgende Teil führt Sie
durch eine Musterinstallation,
von Windows bis hin zur Internetanbindung.

7

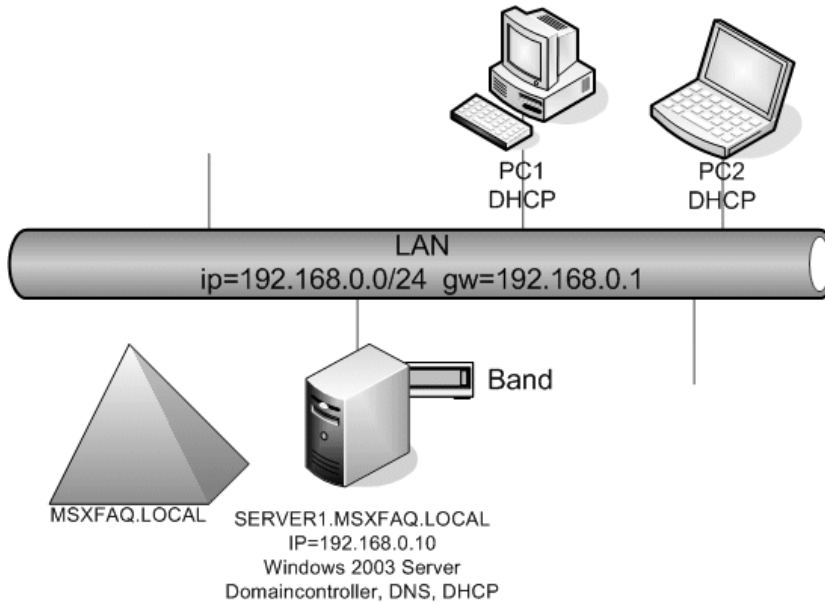
Aufbau der Infrastruktur

7 Aufbau der Infrastruktur

Die nun folgenden Kapitel widmen sich der Installation von Anfang an, um an Beispielen die Installation und Konfiguration eines Netzwerks mit Windows 2003 und Exchange 2003 zu erläutern.

Dieses Kapitel wird Sie dabei begleiten, die Infrastruktur für die Exchange 2003-Installation bereitzustellen. Sie müssen dazu nicht unbedingt die Konzepte des vorherigen Kapitels gelesen haben. Für das Verständnis des Aufbaus und der Installation ist dies jedoch zu empfehlen.

Abbildung 7.1 Installation Schritt 1



Muster-Installation

Nach diesem Kapitel sollten Sie einen Windows 2003-Server als Domänencontroller in einem Netzwerk installiert und alle Vorbereitungen für die Installation eines Exchange 2003-Servers getroffen haben. Alle Clients können per DHCP eine IP-Adresse erhalten, und die interne Namensauflösung ist ebenfalls sichergestellt.

7.1 Netzwerk-Einstellungen

Vor der Installation sind einige Parameter zu definieren. Dieser Schritt wird in den folgenden Kapiteln ebenfalls am Anfang erforderlich sein. Sie finden eine Vorlage zum Eintragen der Werte am Ende des Buches und auf der Webseite zum Buch.

N1 — Netzwerkadresse

Private IP-Adressen: 192.168.0.0/24

Jedes Netzwerk hat einen IP-Adressraum mit einer Subnetzmaske. Dieser ist für die Installation von Windows und allen anderen Geräten im gleichen Segment wichtig. Selbst wenn Sie einen offiziellen Adressraum erhalten haben, sollten Sie sich zweimal überlegen, ob Sie Ihre Server und PCs mit eben diesen offiziellen Adressen ausstatten wollen. Für den Einsatz in privaten Netzwerken eignen sich Adressen aus dem Raum 10.0.0.0/8, 172.16/16—172.16.31.0/16 und 192.168.0.0/24—192.168.255.0/24. Diese Adressen werden nirgendwo im Internet verwendet und sind damit per Definition nicht direkt zu erreichen, selbst wenn Sie keine Firewall hätten. Eine höhere Sicherheit haben Sie zudem damit gewonnen, dass alle Datenzugriffe aktiv umgesetzt werden müssen. Sie müssen aktiv etwas konfigurieren, um Systeme erreichbar zu machen. In unserem Beispiel nutzen wir 192.168.0.0/24 als Netzwerk. Für Ihre eigene Planung sollten Sie sich ein IP-Nummernkonzept überlegen. Speziell wenn Sie schon IP-Adressen verwenden und diese nicht aus dem privaten Bereich sind, dann ist eine Umstellung auf diese privaten Adressen vor der Installation ratsam. Nutzen Sie nämlich Adressen, die im offiziellen Internet einer anderen Firma gehören, dann ist zumindest dieser Bereich für Sie nicht erreichbar.

N2 — Default Gateway

Router: 192.168.0.1

Alle Systeme innerhalb des gleichen Subnetzes können direkt miteinander kommunizieren. Sobald jedoch ein System außerhalb des eigenen Netzwerks erreicht werden muss, benötigt der Absender die Information über die nächste Station auf dem Weg dorthin. In unserem Fall ist dies der Router zum Internet, welcher später installiert wird. Dieser erhält später die IP-Adresse 192.168.0.1. Dieser Eintrag ist das „Default Gateway“, an das alle Pakete an entfernte Systeme gesendet werden.

N3 — IP-Bereich der Clients

DHCP-Adresse-Bereich: 192.168.0.100—192.168.0.254

Ein Teil der Adressen im Netzwerk wird für Arbeitsplätze reserviert. Es ist praktisch, diese Adressen samt der dazugehörigen Konfiguration per DHCP an diese Systeme zu vergeben. Nur Dienstanbieter wie Server, Netzwerkdrucker, Router und Ähnliches benötigen feste IP-Adressen. Wir reservieren die Adressen 192.168.0.100 bis 192.168.0.254 für die Arbeitsplätze.

N4 — DNS-Server für interne Systeme

Interner DNS-Server: 192.168.0.10

In einem Netzwerk besteht zudem der Bedarf, dass ein System ein anderes System anhand eines Namens auffinden kann. Dazu dient ein interner Adressbuchdienst, welcher die Namen in IP-Adressen umsetzt. Dieser interne DNS-Server ist auch für die Funktion des Active Directory zwingend notwendig. Wenn Sie eine Namensauflösung über das Internet nutzen

können, sollten Sie trotzdem verhindern, dass die PCs direkt im Internet nach Namen fragen können. Zum einen können lokale Systeme dort nie gefunden werden, und zum anderen kostet es Zeit, Übertragungsvolumen und führt zu Fehlern. Sie können bei Systemen mehrere DNS-Server eintragen. Diese Funktion ist zur Redundanz gegen Ausfälle eines Servers gedacht. Dabei müssen aber alle Server die gleiche Information liefern können. Die Konfiguration eines internen Servers und eines externen Servers bedeutet nicht, dass beide Welten zuverlässig aufgelöst werden, sondern dass mal der eine und mal der andere DNS-Server gefragt wird. Liefert ein Server eine negative Antwort, wird der andere Server nicht erneut befragt. Umgekehrt muss verhindert werden, dass aus dem Internet die internen Namen auflösbar sind. Nur Firmen, die ihren eigenen DNS-Server im eigenen Netzwerk betreiben, können diese Funktion gezielt aktivieren. Im Beispiel installieren wir einen DNS-Server im eigenen Netzwerk, welcher für die Auflösung aller internen Namen zuständig ist. Dies ist der Server 192.168.0.10 und wird nicht von außen erreichbar sein.

N5 — DNS-Server für die Internet-Auflösung

DNS-Proxy: 192.168.0.1

Damit Exchange seine Nachrichten später in das Internet senden kann und natürlich auch damit Sie selbst im Internet surfen können, müssen Hostnamen im Internet wie z.B. www.msexchangefaq.de zu gültigen IP-Adressen aufgelöst werden. Auch wenn Sie später vielleicht die Nachrichten über einen Smarthost zustellen werden, ist es von Vorteil, logische Namen statt physikalische Adressen zu verwenden. Ansonsten bedeutet eine Änderung der Adresse beim Provider auch eine Änderung der Konfiguration am Exchange-Server. Generell sollten so weit wie möglich Namen statt Adressen verwendet werden, auch wenn dies eine starke Abhängigkeit von der Funktion „DNS“ bedeutet. Die einzigen Systeme, die nicht mit einem Namen ausgelöst werden können sind der DNS-Server selbst und das *Default Gateway*. Diese werden statisch oder per DHCP zugewiesen. Wenn Sie eine Standleitung haben, sollte Ihnen Ihr Provider die korrekten DNS-Server nennen. Bei Wähl- und DSL-Verbindungen erhält der Router oder Computer bei der Einwahl diese Adressen. Dann ist dies das einzige System in Ihrem Netzwerk, welches externe Adressen auflösen kann. Die meisten Router agieren als DNS-Proxy, d.h., eine Anfrage an den Router wird von diesem an den DNS-Server gestellt und die Antwort intern weitergegeben. Als letzte Möglichkeit können Sie direkt die „Root-Server“ des Internets fragen. Dies ist aber nicht sinnvoll, da die DNS-Server Ihres Providers viel schneller antworten können. In unserem Beispiel dient der Router als DNS-Proxy, so dass die Adresse 192.168.0.1 später für die externe Auflösung zuständig ist.

7.2 Windows Server 2003-Einstellungen

Auch für den Server sind vorab die Parameter zu definieren, die bei der späteren Installation genutzt werden. Die Dokumentation dieser Einstellungen ist später für Wiederherstellungen und die Pflege sehr wichtig und in wenigen Minuten erledigt.

S1 — Name des Servers

Server: srv01.msxfaq.local

Jedes System benötigt einen Namen. Sie sind in der Wahl relativ frei, wobei aus Gründen der Kompatibilität und Handhabung sich eine Beschränkung auf Buchstaben und Zahlen und eine Länge von maximal 15 Zeichen bewährt hat. Die genauen Hinweise für erlaubte Namen finden Sie in der Windows 2003-Dokumentation. Verbotene Namen werden auch bei der Installation abgewiesen. Sofern Sie noch kein Namenskonzept haben, sollten Sie sich spätestens jetzt überlegen, wie Sie zukünftig Server, Arbeitsplätze, Drucker und viele andere Objekte benennen wollen. Ob Sie dabei Comic-Figuren, Planeten, orientalische Götternamen oder eine Zusammensetzung aus Ländercode, Kfz-Kennzeichen, Postleitzahl und Nummern verwenden, bleibt Ihnen überlassen. Zusätzlich muss ein DNS-Domänenname definiert werden. Der Server für die Beispielinstallation heißt SRV01. Der Domänenname wird auf msxfaq.local gesetzt. Damit lautet der komplette Rechnername srv01.msxfaq.local. Der Domänenname ist später mit dem Namen des Active Directory identisch.

S2 — Hardware-Beschreibung

Hardware-Daten

Dieses Feld ist groß genug, um die aktuelle Hardware zu dokumentieren. Die detaillierte Auflistung und Konfiguration des Motherboards, der Netzwerkkarte, Festplattencontroller und anderer Komponenten erleichtert später die Installation der Treiber. Spätere Fragen zur Erweiterung der Hardware und Aktualisierung von BIOS und sonstigen Komponenten können später auch ohne Neustart, Öffnen des Server oder Suchen in Datenblättern und Lieferscheinen geklärt werden. Auch im Falle eines späteren Defekts ist die Ersatzbeschaffung und Wiederherstellung einfacher möglich. Moderne Server sind mit der Fähigkeit zur Remote-Steuerung ausgestattet. Diese Konfiguration ist ebenfalls wichtig für spätere Zugriffe. Die Beschreibung des Musterservers finden Sie in der Vorlage.

S3 — Festplattenkonfiguration

Partitionen: Betriebssystems und Nutzdaten

Fast alle Server werden heute mit redundanten Festplattensystemen aufgebaut. Die Ausfallwahrscheinlichkeit mechanischer Komponenten ist zu hoch, um wichtige Daten einer einzelnen ungesicherten Festplatte anzuvertrauen. Bei der Einrichtung des RAID-Systems sind die Parameter für die Stripe-

Größe, den Cache, die zugewiesenen Festplatten und anderes wichtig zu dokumentieren. Heute haben Server meist 36 GB und mehr Speicherplatz, und es ist nur selten sinnvoll, daraus eine große Partition zu machen. Wir nutzen für unseren Server eine Partition für das System und eine zweite Partition für die Nutzdaten. Wir trennen bei unserem Beispiel nicht zwischen Benutzerdaten, Exchange-Datenbank und Exchange-Transaktionsprotokollen. Durch die Trennung des Betriebssystems verhindern wir, dass dieser Bereich durch die Exchange-Datenbank oder Transaktionsprotokolle gefüllt wird und den Server unbrauchbar macht. Eine weitere Aufteilung der Daten birgt aber das Risiko, dass ein Bereich der Festplatte sich im Nachhinein als zu klein darstellt und dies dann aufwändig korrigiert werden müsste. Die Musterinstallation erfolgt in eine 7,9 GB große Betriebssystempartition und eine große Partition für die Nutzdaten.

S4 — Netzwerkkonfiguration

Active Directory-DNS nutzen

Auch wenn im Netzwerkplan bereits die Eckpunkte der Konfiguration festgehalten sind, muss auch für den Server die Konfiguration dokumentiert werden. Dies ist umso wichtiger, da heutige Server mehrere Netzwerkkarten besitzen, die als Team verschaltet werden oder weitere Netzwerkkarten für ein Remote-Management genutzt werden können. Der Server erhält die IP-Adresse 192.168.0.10 und befragt sich selbst als DNS-Server. Tragen Sie hier nicht einen Internet-DNS-Server ein, da Windows 2003 dort sicher keine dynamischen Einträge für das Active Directory vornehmen kann. Das Default Gateway wird der später vorhandene Router mit der Adresse 192.168.0.1 werden.

S5 — Windows-Installationsumfang

Dienste: IIS, SMTP, NNTP und ASP.NET

Eine der wichtigsten Entscheidungen ist die Bestimmung des Windows-Installationsumfangs. Windows 2003 ist in dieser Hinsicht sehr viel restriktiver als Windows 2000 und installiert als Standard nur ein minimales System. Der Administrator muss die erforderlichen Dienste manuell nachinstallieren. Exchange 2003 benötigt neben dem Active Directory noch die Dienste IIS, SMTP, NNTP und ASP.NET. Zur Fehlersuche und Überwachung ist die Installation von SNMP und dem Netzwerkmonitor hilfreich. Die hier gemachten Angaben gelten für die Musterinstallation. Wenn Ihr Server andere Aufgaben zusätzlich übernimmt, sind eventuelle Anpassungen notwendig. Nehmen Sie diese Überlegungen zum Anlass, eine Serverrichtlinie in Ihrem Unternehmen zu entwerfen. Dokumentieren Sie unbedingt Ihren Installationsumfang in der Anlage, und vergessen Sie nicht die Dokumentation der Lizenznummer.

S6 — DHCP-Einstellungen

Client-Netzwerk-Konfiguration

Für Exchange ist der Einsatz von DHCP nicht zwingend notwendig, aber damit Ihre Anwender auch problemlos den Server finden und erreichen können, müssen Sie dessen korrekte Konfiguration sicherstellen. Dies ist mit einem DHCP-Server am einfachsten möglich. Wir vergeben später mittels DHCP-Server den Arbeitsplätzen eine IP-Adresse zwischen 192.168.0.100 und 192.168.0.254 mit der 192.168.0.1 als Default Gateway, 192.168.0.10 als DNS-Server und msxfaq.local als DNS-Suffix.

S7 — DNS-Server-Einstellungen

Forwarder und Reverse-Lookup

Der Server muss ebenso wie die Arbeitsstationen die Namen im Netzwerk auflösen können. Daher wird Windows 2003 im Beispiel so konfiguriert, dass der Server sich selbst befragt. Die Auflösung der Adressen im Internet übernimmt der DNS-Server über die Forwarder-Funktion. Dazu befragt der DNS-Server im Beispiel den Router. Prüfen Sie, welche Systeme Sie als Forwarder nutzen können. Die Pflege einer Reverse-Zone zur Auflösung von IP-Adressen zu Namen ist nicht zwingend, aber zeugt von gutem Design.

7.3 Active Directory-Einstellungen

Der dritte Aufgabenblock zur Installation des Servers ist das Active Directory. Auch hierzu sind einige Angaben zu machen, die nachträglich allerdings nur sehr schwer zu ändern sind. Daher sollten Sie sich die Einstellungen gut überlegen.

A1/A2 — Name des Forests und der Domäne

AD-Domäne: msxfaq.local

Wir installieren den ersten Domänencontroller überhaupt und bauen damit eine neue Gesamtdomänenstruktur (Forest) und eine neue Domänenstruktur auf. Wir halten uns an die Vorgabe und nennen die Active Directory-Domäne „msxfaq.local“. Dies ist gleichzeitig der Namen des Forests. Der erste Teil des Namens „MSXFAQ“ ist der NetBIOS-Name für Systeme, die nicht mit dem Active Directory umgehen können. Zur Erinnerung: Dieser Name hat nichts mit der SMTP-Empfängerdomäne für Exchange zu tun.

A3 — Name der Active Directory-Site

AD-Site: Bellheim

Wie gewissenhaft ein Administrator arbeitet, ist auch daran zu erkennen, ob die Standorte (Site) im Active Directory mit Ihren IP-Adressen gepflegt sind. Solange nur ein Standort existiert, ist diese Pflege eher als Kür zu verstehen, aber sobald mehrere Standorte bestehen, ist die Pflege der Standorte und Subnetze für die Funktion des Active Directory extrem wichtig. Hierbei unterstützt Sie kein Assistent von Windows. Die Installation des Active

Directory richtet einen Standort mit den Namen „Name des ersten Standorts“ ohne IP-Adressen ein. Der Standort sollte das physikalische Netzwerk beschreiben und ist bei den meisten Firmen daher der Ortsname, das Kfz-Kennzeichen oder ein anderes Kürzel für den Standort. Die Musterinstallation nutzt einfach „Bellheim“ als Name. Wählen Sie einen Namen, der den Standort Ihres Subnetzes am besten beschreibt.

A4 — Active Directory-Rollen und -Funktionen

FSMO und Global Catalog

Nur zu Ihrer Information ist die Dokumentation der verschiedenen Active Directory-Funktionen und FSMO-Rollen gedacht. Bei der Installation mit nur einem Server ist die Zuweisung der Rollen klar verteilt. Sobald sie mehrere Domänencontroller haben, können Sie diese Funktionen auf mehrere Server verteilen. Sie sollten auf eine Redundanz bei den GC-Servern achten, aber auch die Unverträglichkeit von Infrastrukturmaster und Globalem Katalog in bestimmten Umgebungen beachten. In unserem Umfeld ist dies jedoch nicht notwendig, da es zunächst nur einen Server gibt, der auch alle Rollen trägt.

Damit sind die wesentlichen Daten zum Active Directory definiert, und die Installation kann gestartet werden.

7.4 Installation des Netzwerks

Für die Funktion von Exchange ist die Existenz eines Netzwerks notwendig, welches alle Server, Computer und Router miteinander verbindet. Wir ersparen uns die Beschreibung, wie ein Netzwerk physikalisch installiert wird. Solche Anleitungen sind heute schon jedem Hub und Switch beigelegt, und die Zeiten, als ein Administrator noch selbst Hand angelegt hat, um Koaxialkabel auf BNC-Stecker zu crimpen, sind schon länger vorbei. Für die weiteren Schritte gehen wir davon aus, dass der Server, der Router und die Arbeitsplätze korrekt verkabelt sind.

Netzanbindung testen

Kontrollieren Sie bitte, dass alle Systeme bei der Verwendung eines Netzwerks auch einen „Link“ haben, da sonst später die Installation des Active Directory fehlschlägt.

7.5 Serveraufbau

Der nächste Schritt ist der Aufbau und die Konfiguration des Servers, damit Sie Windows Server 2003 installieren können. Neben dem Anschluss an das Stromnetz und das Netzwerk müssen Sie in der Regel die RAID-Systeme konfigurieren. Verlassen Sie sich hier auf keinen Fall auf die Vorinstallation des Herstellers. Oft sind die Vorinstallationen nur Überbleibsel des Endtests

und für die Produktion ungeeignet. Solche Konfigurationen können durchaus aus einem RAID 0-Verbund bestehen oder mit verzögerten Schreibzugriffen arbeiten, ohne die notwendige Sicherungsbatterie zu besitzen.

Standards versus individuelle Konfiguration

Einige Hersteller liefern ihre Server schon vorinstalliert aus, so dass nach dem ersten Einschalten nur noch eine kurze Konfiguration notwendig ist und Sie sofort einen Windows-Server haben. Dies beschleunigt die Installation, aber Sie wissen später nicht wirklich, wie der Server installiert wurde und welche Programme zusätzlich eingerichtet wurden. Auch die Partitionierung kann für den Einsatzzweck als Exchange 2003-Server unpassend sein. Sie können auf Basis eines vorinstallierten Servers durchaus starten, aber nur eine eigene Installation gibt Ihnen die Gewissheit, auch im Fehlerfall alle Hilfsmittel und Schritte zu kennen.

Schalten Sie den Server ein, und nutzen Sie die Möglichkeiten des BIOS oder spezieller Service-CDs, um die Festplatten zu konfigurieren und sonstige Funktionen des Servers einzurichten, z.B. das Verhalten beim Ausfall eines Speicherbausteins, Lüfters oder Netzteils. Erstellen Sie eine Checkliste für die ersten Schritte beim Aufbau des Servers, um später die Qualitätskontrollen zu erleichtern:

- Hardware-Aufbau:
  - ☑ System sicher aufstellen bzw. ins Rack einschrauben
  - ☑ System mit weiteren Komponenten komplettieren
  - ☑ Stromversorgung an USV
  - ☑ Netzwerkkabel an Server anschließen
  - ☑ Optional: Netzwerkkabel an Monitoring-Board anschließen
  - ☑ Optional: Anschluss an SAN
  - ☑ Tastatur/Maus an Konsolen-Umschalter
- Software-Konfiguration:
  - ☑ Service-CD booten
  - ☑ Server konfigurieren
  - ☑ Einstellen der Uhrzeit im BIOS
  - ☑ Konfiguration des RAID-Systems
  - ☑ Konfiguration eines vorhandenen Monitoring-Boards

Nach dieser Vorbereitung kann die eigentliche Betriebssysteminstallation beginnen.

7.6 Windows Server 2003-Installation

Exchange 2003 kann auf Windows 2000 oder Windows 2003 installiert werden. Allerdings erlaubt erst die Installation auf Windows 2003 die Nutzung vieler erweiterter Funktionen wie z.B. RPC over HTTP. Die Musterinstallation basiert auf Windows 2003.

Installation automatisieren

Die Installation von Windows 2003 ist gegenüber Windows 2000 sehr stark vereinfacht. Der Server bootet von der CD und installiert mit wenigen Angaben ein minimales Betriebssystem. Unternehmen, die mehrere Server installieren, können sich in der Windows 2003-Hilfe und den Deployment-Tools auf der CD über die Automatisierung der folgenden Eingaben und Anpassungen informieren. Mit einem Windows 2003-RIS-Server ist eine sehr schnelle Installation von Servern und Arbeitsstationen möglich. Die Installation der Musterumgebung erfolgt allerdings von Hand. Die Installation erfolgt überwiegend mittels eines Assistenten (Wizard), der Sie mit vielen hilfreiche Informationen sowie Warnungen begleitet. Folgende Schritte werden für die Muster-Installation durchlaufen:

Ablauf Muster-Installation

- Der Server bootet die Betriebssystem-Installation von der CD

  Sofern Windows 2003 Ihren Festplatten-Controller nicht unterstützt, müssen Sie mit F6 und einer Treiberdiskette des Herstellers eigene Treiber einbinden.

- Partitionierung der Festplatte

  Legen Sie eine Partition für das System und auch die Partition für die späteren Daten an, und formatieren Sie diese mit NTFS.

Nach dem Abschluss der textbasierten Installation startet der Server neu, und im grafischen Teil werden die weiteren Einstellungen durchgeführt.

- Sprache und Tastatur

  Wählen Sie die Sprache (Deutsch) und das Tastaturlayout aus. Aufgrund der Installation in internationalen Unternehmen, und der schnellere Verfügbarkeit von Service-Packs und Updates installieren einige Firmen grundsätzlich nur „englische“ Server. Bei der Installation eines englischen Servers sollten Sie zusätzlich die deutsche Tastatur einrichten.

- Benutzerinformationen

  Geben Sie Ihren Benutzernamen und Firmennamen ein. Es macht Sinn, hier den Namen einer Abteilung, wie IT-Service, zu wählen, anstatt eines personifizierten Benutzernamens, der letztlich wechseln kann.

- Product Key

  Hier müssen Sie Ihren Produktschlüssel (25 Stellen) eingeben.

- Lizenzierungsmodus

  Als Lizenzierungsmodus in der Musterinstallation kommt die „Pro Arbeitsplatz“-Variante zum Zuge. Dies bedeutet, dass später für jede Arbeitsstation oder Benutzer eine CAL vorhanden und eingetragen werden müsste. Allerdings ist der zur Verwaltung notwendige Lizenzdienst seit Windows 2003 deaktiviert.

- Servername und Kennwort

  Tragen Sie den gewählten Servernamen und ein Kennwort ein. Die Musterinstallation verwendet SRV01 und als Kennwort „Password!“. Windows 2003 aktiviert als Standard ein komplexes Kennwort. Wenn Sie ein nicht ausreichend sicheres Kennwort verwenden, werden Sie entsprechend darauf hingewiesen.

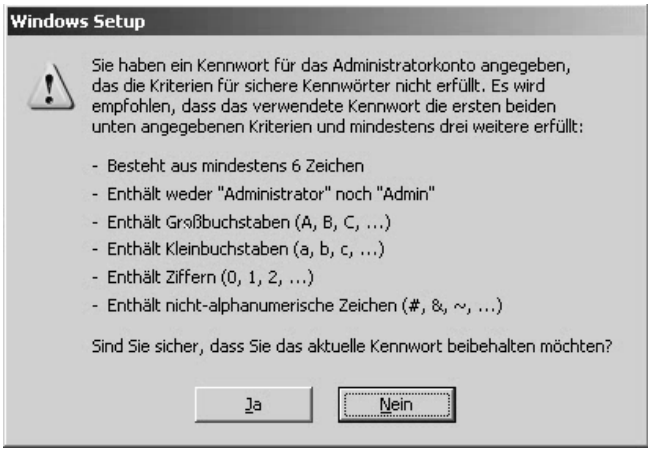


Abbildung 7.2 Kennwort-richtlinien

  Sie können den Ratschlag auch ignorieren und ein unsicheres Kennwort verwenden. Sie sollten es aber möglichen Angreifern nicht so einfach machen.

- Datum, Zeit und Zeitzone

  Die korrekte Angabe dieser Parameter ist wichtig, da Exchange hiervon auch die Zeitinformation für Nachrichten ableitet. Besonders die aktive Einstellung der automatischen Sommerzeit-/Winterzeit-Umstellung ist wichtig, damit später Termine auch korrekt eingetragen werden.

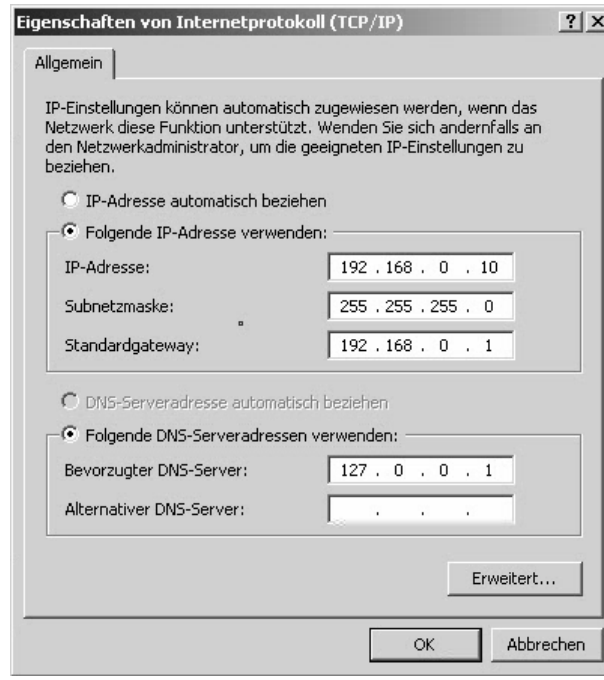
Zeitzone: GTM +01:00 Berlin

- Konfiguration der Netzwerkkarte

  Bei der Konfiguration der Netzwerkverbindung ist die benutzerdefinierte Installation zu wählen, da ansonsten der Server eine IP-Adresse per DHCP beziehen möchte. Geben Sie die vorher festgelegten Informationen ein. Nur wenn Sie mehrere Netzwerkkarten haben, die später als Team genutzt werden sollen, dann können Sie hier die Standardeinstellung (DHCP) nutzen und später die Konfiguration anpassen. Die Bindungen bleiben in der Musterinstallation unverändert.

Feste IP-Adresse

Abbildung 7.3 Netzwerk-einstellungen



Das Windows 2003-Setup installiert die restlichen Dateien und Einstellungen und startet neu.

7.7 Windows-Anpassung und -Konfiguration

Nach dem Neustart und der Anmeldung begrüßt Windows 2003 Sie mit einem Assistenten und einer Auflösung von 640 x 480 Pixel. In der Musterinstallation wird der Assistent über die Checkbox am linken unteren Rand abgeschaltet, und die einzelnen Schritte werden über das Startmenü aufgerufen. Die Auslösung wurde auf 800 x 600 Pixel eingestellt. Wählen Sie eine für Ihren Bildschirm und Ihre Arbeit angemessene Einstellung.

Mit der erforderlichen Aktivierung von Windows 2003 können Sie bis zu 60 Tage warten. Sinnvoll ist die Aktivierung nach der Installation aller Treiber, Dienste und Software am Ende der Installation, damit bei einem Fehler auch wieder eine neue Installation gestartet werden kann. Vergessen Sie aber nicht die Aktivierung am Ende, da Sie sich nach dem Ablauf dieser Zeit nicht mehr interaktiv am Server anmelden können.

Gerätemanager

Nach der Installation des Betriebssystems sollten Sie umgehend in den Gerätemanager des Servers schauen, um eventuell nicht korrekt erkannte Geräte zu finden und die entsprechenden Treiber zu installieren. Ein einwandfrei installierter Server sollte keine gelben Ausrufezeichen im Gerätemanager aufweisen.

Der Umfang der Windows 2003-Installation ist für Exchange entsprechend anzupassen. Hierzu gehört die Nachinstallation notwendiger Dienste und Einstellungen bestimmter Parameter. Über START — SYSTEMSTEUERUNG — SOFTWARE — WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN werden folgende Komponenten hinzugefügt, die für den Betrieb des Active Directory und Exchange erforderlich sind:

Dienste für AD und Exchange

- ASP.NET

  Die Unterstützung von ASP.NET ist notwendig, um in Verbindung mit dem IIS6 die Funktion „ActiveSync“ bereitzustellen. Damit können später PocketPCs direkt Inhalte synchronisieren.

- SMTP-Dienst

  Ohne diesen Dienst kann Exchange 2003 keine Nachrichten aus dem Internet empfangen oder selbst senden. Auch für die Kommunikation zwischen Exchange-Servern ist SMTP erforderlich und somit ein notwendiger Dienst. Exchange 2003 erweitert den Windows SMTP-Dienst um eigene Funktionen.

- NNTP-Dienst

  Auch der NNTP-Dienst ist für Exchange 2003 notwendig, um den Zugriff auf Öffentliche Ordner über das Protokoll NNTP zu erlauben. Wenn NNTP nicht genutzt wird, können Sie den Start des Dienstes später immer noch deaktivieren.

- DNS-Server

  Für die Funktion des Active Directory ist ein DNS-Server erforderlich. Nur wenn andere Server in Ihrem Netzwerk für die Namensauflösung zuständig sind, können Sie hierauf verzichten. In der Musterinstallation gibt es jedoch nur einen Server, der alle Funktionen übernimmt.

- DHCP-Server

  Weder Exchange noch das Active Directory benötigen einen DHCP-Server. Die Vergabe von IP-Adressen an die Clients wird damit jedoch sehr vereinfacht.

- Web-Dienste

  Unter diesem Namen verbirgt sich der Internet Information Server 6 (IIS6). Die Installation der Web-Dienste (WWW) ist Voraussetzung für Exchange 2003, da hierüber nicht nur der Zugriff für OWA, sondern später auch die Administration der Öffentlichen Ordner erfolgt.

- RPC over HTTP-Proxy

  Wenn Sie später den Zugriff von Outlook 2003 über HTTP ermöglichen wollen, müssen Sie diese Komponente mit installieren.

- WINS

  Die NETBIOS-Namensauflösung funktioniert nur im gleichen Subnetz mit Broadcast. Wenn Sie mehrere Subnetze betreiben, dann ist für eine effiziente Namensauflösung der Einsatz von WINS-Servern erforderlich.

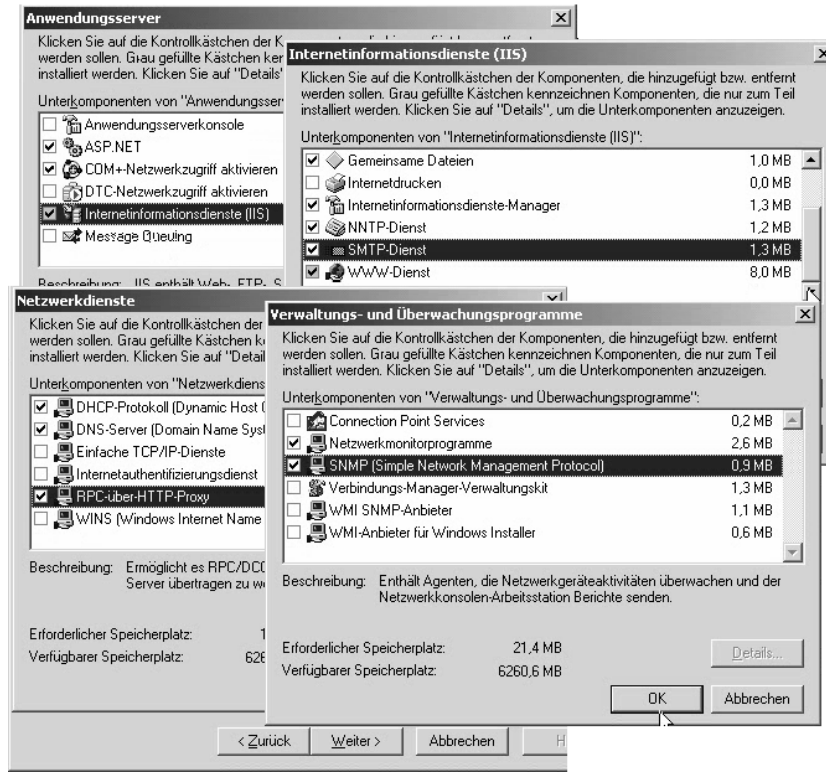
- SNMP

  Die Installation von SNMP ist nicht für Exchange notwendig. Aber SNMP ist eine der Grundlagen, um später den Server mit entsprechenden Hilfsmitteln zu überwachen. Sehr viele Hilfsprogramme der Hersteller zur Hardware-Überwachung erfordern ebenfalls die Installation von SNMP.

- Netzwerk-Monitor

  Für die spätere Fehlersuche ist der Netzwerkmonitor sehr hilfreich. Zwar kann die im Server verfügbare Version nur Pakete mitschneiden, die den Server selbst betreffen, aber dies reicht für die meisten Suchen aus. Die Installation kostet nur einige Megabyte.

Abbildung 7.4 Windows 2003-Dienste



Netzwerk-einstellungen

Sofern Sie nicht schon bei der Installation die richtige Netzwerkkarten-Einstellung vorgenommen haben, können Sie dies nun nachholen. Für den Einsatz von Adapter-Teaming benötigen Sie eine Zusatz-Software des Netzwerkkartenherstellers.

Weitere Konfigurationseinstellungen haben sich in der Praxis bewährt. Stimmen Sie diese mit Ihren eigenen Bedürfnissen ab.

Serverbeschreibung

In der Netzwerkumgebung ist später die Beschreibung des Servers sichtbar. In der Musterumgebung lautet diese „Exchange 2003-Server“.

Erfahrungswerte nutzen

- Auslagerungsdatei

  Die Auslagerungsdatei für den virtuellen Speicher ist dynamisch. Es kann sinnvoll sein, sie von Anfang an ausreichend groß zu setzen und eine dynamische Änderung der Größe zu unterbinden, um eine spätere Fragmentierung zu verhindern. Leider gibt es keine pauschalen Aussagen, wie groß die Datei sein sollte. Frühere Angaben vom 1,5-fachen des Hauptspeichers sind zu allgemein.

- Start Timeout

  Normalerweise wartet Windows ca. 30 Sekunden im Startmenü auf eine Bestätigung. Windows 2003 startet sofort die einzige vorhandene Konfiguration. Wenn Sie später mehrere Konfigurationen eingerichtet haben, können Sie den Wert verringern, um das Hochfahren etwas zu beschleunigen.

- DUMP

  Wenn Ihr Server mit einem so genannten „Blue Screen“ stehen bleibt, dann wird er den kompletten Hauptspeicher beim nächsten Start herausschreiben. Heutige Server mit 1 GByte Speicher sind damit einige Zeit beschäftigt, und der Festplattenplatz kann schnell knapp werden. Oftmals reicht für eine Analyse des Fehlers hier ein „Minidump“, welcher auch noch ausreichend Informationen für die Ursache liefert, aber mit 64 KB Platzbedarf sehr viel schneller erfolgt.

- Größe des Eventlog

  Bei Windows 2003 ist die Größe der Ereignisanzeige je Protokoll auf 64 KByte eingestellt. Dies ist für die meisten Umgebungen zu wenig, um auch langfristig Fehler verfolgen zu können. Eine Größe von 4 Megabyte pro Eventlog ist vorteilhaft. Diese Einstellung kann später auch mittels Gruppenrichtlinien vorgenommen werden.

- Grafikkarte

  Passen Sie bitte die Auflösung des Servers an den Monitor und Ihre Wünsche an. Beachten Sie beim Betrieb an einem Monitorumschalter oder mit einem LCD-Display die maximalen Grenzwerte.

- SNMP-Konfiguration

  Die Installation des SNMP-Dienstes erlaubt das Management des Servers für entsprechende Programme, Windows 2003 stellt die Sicherheit sehr hoch ein, indem nur der Server selbst diese Schnittstelle nutzen darf.

Wenn Sie eine Management-Software auf einem anderen System betreiben, müssen Sie die Konfiguration anpassen.

- Umgebungsvariablen

  Speziell auf Servern mit der Möglichkeit zum Wechseln von PCI-Geräten im laufenden Betrieb (Hot Plug-PCI-Schnittstellen) sollten Sie die Umgebungsvariable DEVMGR_SHOW_NONPRESENT_DEVICES=1 setzen, damit Sie später im Gerätemanager auch die Geräte sehen und entfernen können, die sich nicht mehr in Ihrem System befinden. Dies gilt besonders, wenn Sie später z.B. eine Netzwerkkarte ungeplant entfernen und vermeiden möchten, dass die Ersatzkarte nicht die gleiche IP-Adresse erhalten kann.

- Fernsteuerung

Remotesteuerung mit MSTSC

  Wenn Sie den Windows 2003-Server über die Terminal-Dienste fernsteuern möchten, müssen Sie dies in den Eigenschaften des Arbeitsplatzes freischalten. Die Verbindung können Sie dann mit dem Terminal-Services-Client aufbauen, wenn Sie „/CONSOLE“ beim Aufruf als Parameter übergeben.

```
MSTSC /console
```

- Wiederherstellungskonsole (Recovery Console)

  Für die Behebung von Fehlern ist die Wiederherstellungskonsole bei Windows 2003 sehr gut geeignet. Diese kann von der Installations-CD gestartet werden. Allerdings kostet es wertvolle Zeit, die CD in diesem Fall erst wieder zu suchen und dann die Bootreihenfolge entsprechend einzustellen. Daher bietet sich die Installation auf der Festplatte mit folgendem Aufruf an:

```
<CDLaufwerk:>\I386\WINNT32.EXE /CMDCONS
```

- Partitionierung und Labels

  Bei der Installation wird häufig nur die Systempartition formatiert und installiert. Die sonstigen Festplatten sind ebenfalls einzurichten und zu formatieren. Dabei sollten auch die Labels der Festplatten vergeben werden. Dies ist umso wichtiger, wenn bei einem späteren Defekt die Buchstaben verwürfelt sind und anhand der Labels schneller die korrekte Festplatte zugeordnet werden kann. Die Musterinstallation benennt die beiden Partitionen auf der logischen Festplatte als HD0-C-SYS (Systemdaten) und HD0-D-DATA (Nutzdaten). Zusätzlich kann das CD-ROM-Laufwerk auf den Buchstaben Z: verschoben werden.

Dies soll für den Anfang ausreichend sein. Überlegen Sie selbst, wie Sie gerade mit mehreren Servern für eine sinnvolle Standardisierung in Ihrem Unternehmen sorgen können.

7.8 Windows-Support und Management Tools

Heutige Server sind nicht nur einfache PCs, sondern enthalten erweiterte Funktionen, wie z.B. austauschbare Lüfter und Netzteile, Überwachung kritischer Systemparameter und redundante Speicherbausteine. Die Funktion und den Ausfall solcher Komponenten muss eine gesondert zu installierende Management-Software melden. Beispiele hierfür sind HP Insight Manager, IBM IT-Directory, Fujitsu-Siemens ServerView, Dell OpenManage und andere Programme. Alle dienen dazu, dass Sie frühzeitig über einen Defekt oder eine Verschlechterung informiert werden, ehe der Fehler einen echten Ausfall verursacht. Auch für die USV und für den RAID-Controller gibt es Zusatzprogramme, deren Installation notwendig ist. Bitte informieren Sie sich bei dem jeweiligen Hersteller, wie diese Produkte installiert und konfiguriert werden.

Für die Unterstützung der Fehlersuche und korrekten Funktion liefert Microsoft die Support-Tools mit, die manuell zu installieren sind. Die Installation dieser Hilfsprogramme ist wichtig um recht einfach eine Qualitätskontrolle und Diagnose durchführen zu können. Zu den Support-Tools gehören folgende nützliche Programme:

Windows-Support-Tools

- NETDIAG
  Überprüft alle Netzwerkfunktionen und gibt diese detailliert aus. Dieses Programm sollten Sie auf jedem Server nach der Installation einmal ausgeführt haben. Einige Administratoren führen dieses Programm sogar regelmäßig als Kontrolle aus.
- DCDIAG
  Überprüft die Funktion des Domänencontrollers im Netzwerk.
- REPLMON
  Erlaubt die Anzeige und Kontrolle der Replikation zwischen Domänencontrollern. Mit diesem Tool ist auch ein Anstoßen der Replikation möglich.

Die komplette Liste aller Tools und deren Funktion ist nach der Installation über die dazugehörige Hilfe im Startmenü einsehbar. Die Installation wird durch den Aufruf der Installation aus dem Verzeichnis Support\Tools\ der Installations-CD gestartet.

7.9 Kontrolle der Server-Installation

QS-Maßnahmen

Ehe der Server weiter für seine eigentliche Aufgabe angepasst wird, sollte er einige Tests und Prüfungen bestehen. Diese Qualitätssicherungstests (QS) sind an dieser Stelle notwendig, da bei einem Versagen des Servers noch

keine Gefahr für Daten oder Netzwerk besteht. Nach dem darauf folgenden Schritt ist der Server produktiv. Wenn bei der Installation und Konfiguration oder den Tests ein Fehler auftritt, ist im schlimmsten Falle eine Neuinstallation erforderlich, und auch zu empfehlen. Daher werden sowohl Tests bezüglich der Performance als auch bezüglich der Zuverlässigkeit erfolgen.

7.9.1 Zuverlässigkeit

Die erste Testfunktion bezieht sich auf die Zuverlässigkeit der eingesetzten Komponenten. Hierzu gehören folgende Maßnahmen, die bei entsprechend ausgestatteten Servern durchgeführt werden können:

Test der USV

Trennen Sie das System vom Stromnetz. Läuft der Server weiter, oder haben Sie beim Verkabeln die falsche Steckdose genutzt? Wie lange läuft der Server mit der Batterie? Stimmen die geschätzten Zeiten der USV-Steuerungssoftware mit den tatsächlichen Belastungen überein, und wird der Server rechtzeitig sauber heruntergefahren? Haben Sie auch daran gedacht, den Netzwerk-Switch und den Tastaturumschalter mit an die USV anzuschließen? Ein Windows-Server, besonders mit einem Active Directory ohne Netzwerkverbindung, verhält sich manchmal etwas seltsam.

Test Netzteile

Wenn Ihr Server mehrere redundante Netzteile besitzt, dann sollten Sie diese einzeln vom Stromnetz trennen und kontrollieren, ob der Server noch läuft und die Überwachungssoftware korrekt den Ausfall erkennt und meldet. Hängen Sie redundante Netzteile nicht an die gleiche Phase, sondern an getrennte Stromkreise oder sogar getrennte USV-Anlagen.

Test Netzwerkredundanz und Netzwerkkartentausch

Wenn Ihr Server mehrere Netzwerkkarten im Teaming betreibt, dann können Sie diese Funktion jetzt gefahrlos testen. Simulieren Sie die zu vermeidenden Ausfallszenarien, und prüfen Sie die Funktion und Alarmierung. Bei Servern mit „Hot Plug-PCI“ können Sie z.B. den Austausch der Netzwerkkarte üben.

Test Festplattenredundanz

Server mit RAID-Controllern und entsprechender Konfiguration sollten den Ausfall einer Festplatte problemlos überstehen. Wenn die Festplatten „Hot Plug“-tauglich sind, dann ist auch das Entfernen unter Last kein Problem. Auch hier sollte die Management-Software den Ausfall erkennen und melden. Wenn Sie die Festplatte wieder einschieben, sehen Sie zudem, ob der Controller den Verbund eigenständig wieder herstellt oder ob Sie

manuell eingreifen müssen. Nutzen Sie die Chance, sich mit der Anwendung vertraut zu machen. Protokollieren Sie die Zeitspanne, bis alle Systeme wieder „grün“ sind, und auch, wie stark der Server dadurch ausgebremst wird. Diese Zahlen sind später wichtig für die Garantie von SLAs.

Ausfall simulieren

Viele moderne Server erlauben auch den Wechsel von Steckkarten, Lüftern und andere Komponenten im laufenden Betrieb. Wenn Sie über einen entsprechenden Server verfügen, dann sollten Sie dies jetzt testen. Brauchen Sie diese Funktion später einmal, dann wissen Sie schon jetzt, wie es funktioniert oder welche manuellen Schritte zusätzlich notwendig sind.

7.9.2 Performance

Eine zweite wichtige Testfunktion ist die Kontrolle der versprochenen Leistung. Bei einem Server interessieren primär die Performance der Festplatte und der Netzwerkkarte. Zwar sind die folgenden Tests sehr einfach gestrickt und nur bedingt vergleichbar, aber grobe Fehlkonfigurationen und Ausfälle bei Belastung lassen sich mit so wenig Aufwand durchaus erkennen.

Netzwerkkarte

Die stabile Anbindung des Servers an das Netzwerk sowie dessen Performance ist für den späteren Betrieb außerordentlich wichtig. Häufig sind aber veraltete Treiber, falsche Einstellungen am Netzwerk-Switch oder der falsche PCI-Slot im Server eine oft unerkannte Bremse. Neu installierte Server, die trotzdem weniger als 10 % der möglichen Nettoleistung bringen, sind Realität!

Für die Messung der Netzwerkleistung benötigen Sie einen zweiten Computer mit einer entsprechend gleichwertigen Anschlusstechnik und etwas Zeit. Mit Programmen wie NETIO oder auch einem einfachen COPY-Befehl über Netzwerk können Sie ermitteln, wie schnell die Daten übertragen werden. Fragen Sie Ihren Lieferanten, ob er Ihnen entsprechende Vergleichswerte anderer Server bereitstellen kann, oder nutzen Sie selbst einen anderen ähnlichen Server.

Ein moderner Server sollte auf einer 100 MBit-Karte in einem unbelasteten Netzwerk mit NETIO durchaus die physikalische Obergrenze erreichen. Beim Einsatz von Gigabit können Werte über 200 MBit erwartet werden.

Festplatte

Für einen Server noch wichtiger ist die Leistung des Festplattensubsystems. Gerade Exchange arbeitet mit den Transaktionsdateien und Datenbanken sehr intensiv auf den Datenträgern. Auch bei der Datensicherung oder später

eventuell notwendigen Einsätzen von ESEUTIL ist ein schnelles Subsystem wichtig.

Die einfachen Qualitätsmaßnahmen ersetzen keinen umfangreichen End-Test und sind auch nur bedingt mit anderen Servern vergleichbar, aber Sie sollten damit grobe Konfigurationsfehler erkennen:

- COPY

  Einfacher Test ist das Kopieren einer großen Datei (z.B. das ISO-Image einer CD) von einer Festplatte auf die andere. Messen Sie die Zeit, und vergleichen Sie dies mit einem anderen ähnlichen Server. Natürlich gibt es Ungenauigkeiten durch die Fragmentierung und sonstige Aktivitäten der Festplatte, aber die sollten bei einem neuen Server keine extremen Abweichungen ergeben.

- DT

  Ein weiteres Testprogramm ist DT von Robin Miller (http://www.bitnet.com/~rmiller/dt.html), das mit einfachen Mitteln große Datenmengen auf Festplatten schreibt und liest. Verschiedene Zugriffsmuster und Blockgrößen lassen hierbei eine gute Analyse des Festplattensubsystems zu. Weitere Informationen und den Link dazu finden Sie auf http://www.msexchangefaq.de/produkte/dt.htm.

- JETSTRESS

  Für die besonderen Anforderungen von Exchange-Datenbanken bietet Microsoft auch das Programm JETSTRESS an, das im Exchange-Resource-Kit enthalten und bei Microsoft auf der Webseite zu finden ist. Es simuliert die typische Belastung eines Servers durch eine Exchange-Datenbank.

- LOADSIM 2003

  LOADSIM ist eine Testanwendung, die auf einem bestehenden Exchange-Server sehr viele Postfächer und Verteiler anlegt und entsprechende Tests mit simulierten Clients durchführt. Dies ist letztlich der finale Test, wie leistungsfähig Ihr Server sein kann. Allerdings sollten Sie LOADSIM nicht in der Produktivumgebung durchführen.

Ihnen fallen sicher noch weitere Tests ein. Nutzen Sie die Chance jetzt, alle im Betrieb austauschbaren Teile auch im Betrieb zu wechseln. Sie werden diese Praxis später gut brauchen können. Und auf jeden Fall sollte die Management- bzw. Monitoring-Software Sie rechtzeitig über einen Defekt informieren. Was hilft Ihnen eine redundante Festplatte, wenn nach dem Ausfall des ersten Datenträgers der zweite einige Wochen später folgt und Sie haben den ersten Ausfall noch nicht bemerkt?

Wenn Sie davon überzeugt sind, dass Ihr Server für den Einsatz vorbereitet ist und die Spuren der Tests komplett entfernt sind, dann kann der nächste Schritt gestartet werden.

7.10 Installation des Active Directory

Der nächste Schritt ist die Einrichtung des Active Directory. Die Hintergrundinformationen zur Installation und Planung finden Sie im Kapitel 3. Die daraufhin ermittelten Installationsparameter sind am Anfang dieses Kapitels dokumentiert.

7.10.1 Installation

Die Installation des Active Directory wird durch das Programm DCPROMO gestartet. Der Assistent führt Sie durch die Installation, und mit den im vorherigen Kapitel gemachten Angaben gelingt die Installation sehr einfach.

- Windows-Sicherheit

  Der Assistent weist darauf hin, dass die Windows 2003-Voreinstellungen eine Verbindung mit älteren Clients aufgrund höherer Sicherheitseinstellungen nicht mehr zulassen. Sie können diese Einstellungen aber nachträglich lockern.

- Die Installation baut eine neue Domäne in einer neuen Gesamtstruktur mit dem Namen „msxfaq.local“ auf. Der NetBIOS-Name wird „MSXFAQ“ lauten.

  Neuer Forest — neue Domäne

- Datenbankpfade

  Die Verzeichnisse zur Ablage der Active Directory-Datenbank belassen wir auf den Standardwerten. Wenn Sie andere Pfade eingeben, sollten Sie diese in der Dokumentation ergänzen. Die Verlagerung macht nur in sehr großen Umgebungen Sinn, wenn das Active Directory viele Objekte verwalten muss und eine entsprechende Anzahl an Änderungen erfolgt.

- DNS-Prüfung

  Die Überprüfung des DNS durch DCPROMO findet keinen DNS-Server mit entsprechenden Zonen und schlägt die lokale DNS-Installation vor. Aufgrund der Vorteile des AD-integrierten DNS wird die Option gewählt und DCPROMO richtet den Server entsprechend ein.

- Kennwörter

  Der Domänen-Administrators übernimmt beim ersten DC das Kennwort des lokalen Administrators. Für die Wiederherstellung wird ein eigenes Kennwort benötigt, das einzugeben und zu dokumentieren ist. Im Fall

einer Wiederherstellung des AD-Servers vom Band wird das Password benötigt. Ebenso ist es für die lokale Anmeldung in der Recovery-Console erforderlich, wenn das AD nicht zur Verfügung steht.

- Zusammenfassung

  Der Assistent zeigt eine Zusammenfassung der gewählten Schritte an. Diese Zusammenfassung kann problemlos in die Zwischenablage übernommen und mit einem Texteditor als Datei abgespeichert und später zur Dokumentation hinzugefügt werden.

- Einrichtung und Neustart

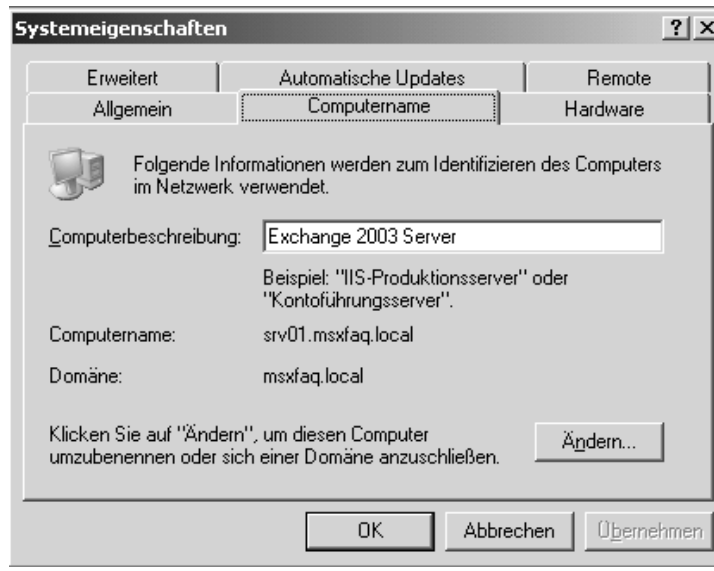
  Der Assistent installiert das Active Directory und fordert Sie danach zum Neustart des Servers auf.

Damit ist die grundlegende Installation des Active Directory abgeschlossen.

7.10.2 Kontrolle

Nach der Installation steht zuerst die Kontrolle der Funktion an. Der Server wurde durch die Hochstufung zum Domänencontroller zugleich Mitglied der Domäne, und der DNS-Namenszusatz wurde geändert. Dies kann in den Eigenschaften des Arbeitsplatzes kontrolliert werden.

Abbildung 7.5 Computer-Eigenschaften



Eine weitere Prüfung gilt dem Eventlog. Neben den Anzeigen für Anwendung, System und Sicherheit, hat die AD-Installation nun drei weitere Ereignisanzeigen hinzugefügt: Verzeichnisdienst, DNS-Server und Datei-

replikationsdienst. Hier ist besonders das Eventlog des Verzeichnisdienstes zu kontrollieren.

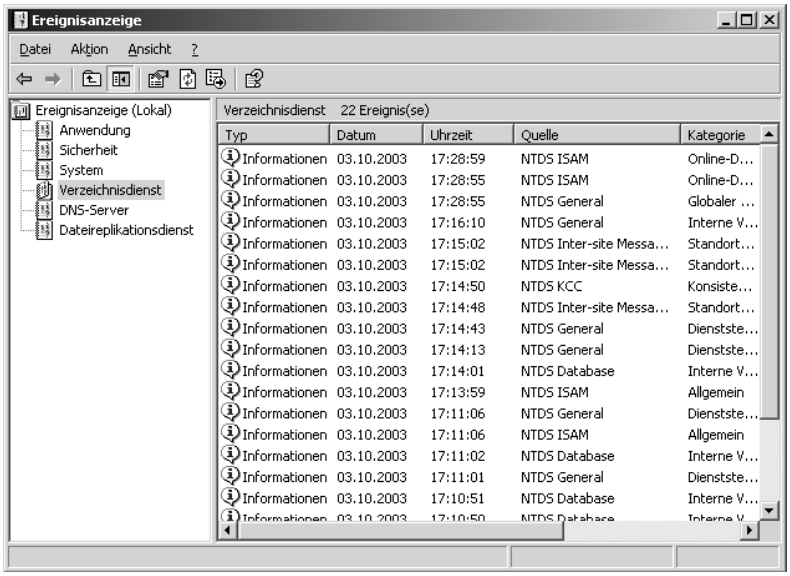


Abbildung 7.6 Eventlog

Das Eventlog zeigt keine Fehler des Verzeichnisdienstes. Auch die anderen Bereiche im Eventlog sollten keine Fehler aufführen, die Sie nicht kennen oder nicht erklären sowie als irrelevant abhaken können.

Die nächste Kontrolle gilt den Einträgen im DNS-Server. Windows 2003 sollte sich selbst und die bereitgestellten Dienste im DNS eingetragen haben.

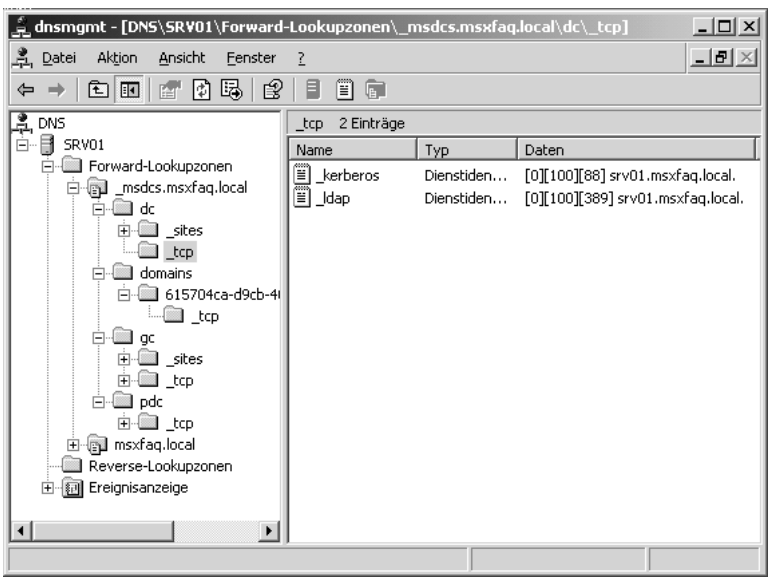
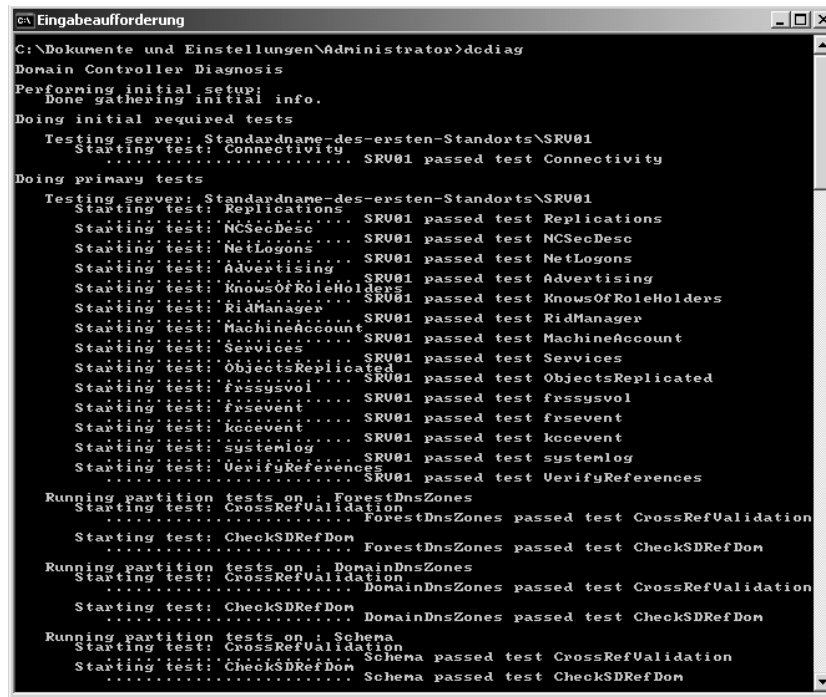


Abbildung 7.7 DNS-Informationen

Die DNS-Zone enthält die Informationen über den Server im Bereich „_MSDCS“. Hier sollten Sie die Einträge für _LDAP und _KERBEROS prüfen. Der Eintrag „srv01.msxfaq.local“ sollte auf die lokale IP-Adresse des Servers, hier 192.168.0.10, weisen.

Eine weitere Kontrolle ist die Funktion mittels DCDIAG, welches durch die Installation der Support-Tools verfügbar ist. Hierbei sollten alle wesentlichen Tests „*passed*“ sein. DCDIAG überprüft auch das Eventlog und meldet Fehler dort. Kontrollieren Sie diese Fehlermeldungen im Eventlog auf Ihren Zusammenhang mit dem Active Directory.

Abbildung 7.8
DCDiag-Ausgabe



7.10.3 Domäne in den Native Mode schalten

Für die Nutzung von universellen Sicherheitsgruppen (USG) ist der Betrieb der Domäne im einheitlichen Modus erforderlich. Dies ist auch notwendig, um später aus einer bestehenden NT4-Domäne die Benutzer mit dem Hilfsprogramm ADMT und der Beibehaltung der SIDs (SID-History) zu übernehmen. Die Aktivierung des einheitlichen Modus erfolgt mit der Management-Konsole *Active Directory-Domänen und -Vertrauensstellungen.*

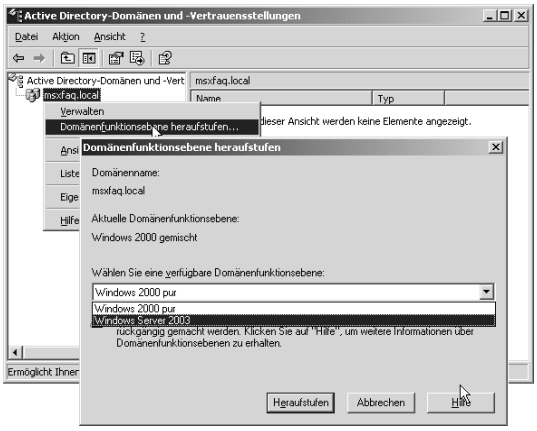


Abbildung 7.9 Domain in Native Mode bringen

Die universellen Sicherheitsgruppen sind für den Einsatz von Exchange besonders in Umfeldern mit mehreren Domänen wichtig. Wenn Sie nur eine einzelne Domäne betreiben und keine Benutzer mittels ADMT migrieren müssen, dann können Sie auch im gemischten Mode verbleiben.

Wenn alle Domänencontroller mit Windows 2003 betrieben werden, dann kann auch der Betriebsmodus des Forests geändert werden. Im Hinblick auf Exchange ist diese Änderung allerdings nicht weiter zu betrachten.

7.10.4 Standorte und Subnetze pflegen

Active Directory und viele andere Dienste nutzen das Wissen über die Netzwerkstandorte (Sites), um die Verzeichnisserver zu erreichen, die aus Netzwerksicht in der Nähe liegen. Solange Sie nur genau einen Standort betreiben, ist die Pflege der *Active Directory-Standorte und -Dienste* nicht nebensächlich. Aber sobald Sie mehrere Standorte haben, ist diese Konfiguration zwingend erforderlich, um die Zugriffe auf lokale Domänencontroller zu optimieren.

In der Musterinstallation wird der aktuelle Standort umbenannt und das IP-Subnetz entsprechend eingetragen.

Abbildung 7.10 Active Directory-Sites und -Subnetze

Mit dem Hilfsprogramm NLTEST ist auf dem Server und angeschlossenen Clients die Funktion der Eintragungen zu überprüfen.

Abbildung 7.11 NLTEST-Kontrolle

Auch bei Ihrem Server muss der Standort richtig erkannt werden. Ansonsten müssen Sie Ihre Einstellungen erneut prüfen.

7.10.5 OUs und Dienstkonten anlegen

Entsprechend Ihrem Konzept für Organisationseinheiten (OU) können Sie die Organisationseinheiten anlegen. Dies ist im Hinblick auf die Installation weiterer Programme und Computer sinnvoll, da z.B. auch für die Datensicherung und den Virenscanner eigene Benutzerkonten angelegt werden sollten. Auch Anwender und Gruppen können bereits erstellt werden.

In der Musterinstallation wird das Beispielkonzept umgesetzt, und die entsprechenden Organisationseinheiten und Dienstbenutzer werden angelegt.

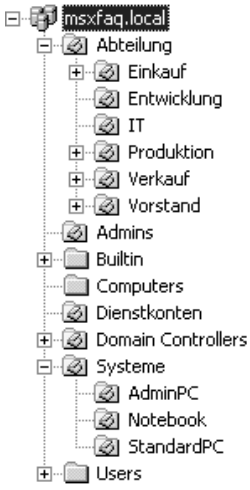


Abbildung 7.12 OU-Struktur der Musterinstallation

Sie sollten natürlich gemäß Ihrer eigenen OU-Konzeption die Organisationseinheiten anlegen, wenn Sie einen produktiven Server installieren. Exchange 2003 selbst benötigt keine Dienstkonten, sofern es keinen Exchange 5.5-Server in der gleichen Administrativen Gruppe gibt.

7.11 DHCP autorisieren und konfigurieren

Die Funktion des DHCP-Servers ist für den Exchange-Server zwar nicht notwendig, aber für die spätere Anbindung der Clients eine nützliche Einrichtung. Es gibt nur sehr wenige Gründe, warum Sie keinen DHCP-Server in Ihrem Netzwerk einsetzen sollten.

DHCP-Server autorisieren

AD erfordert Autorisierung

Der DHCP-Server erkennt automatisch die Existenz des Active Directorys. Bervor der Server nun seine Arbeit aufnimmt und Adressen vergibt, müssen Sie den Server im AD autorisieren. Ändern Sie später die IP-Adresse des Servers, muss auch die Autorisierung erneuert werden. Dies erfolgt im Kontextmenü AUTORISIEREN bei den Eigenschaften des Servers.

Bereich anlegen

Im zweiten Schritt legen wir einen Bereich für die Freigabe der IP-Adressen von 192.168.0.1 bis 192.168.0.254 an. Hier schließen wir die Adressen von 1 bis 99 aus der Verteilung aus, um diese als statische Adressen zu nutzen.

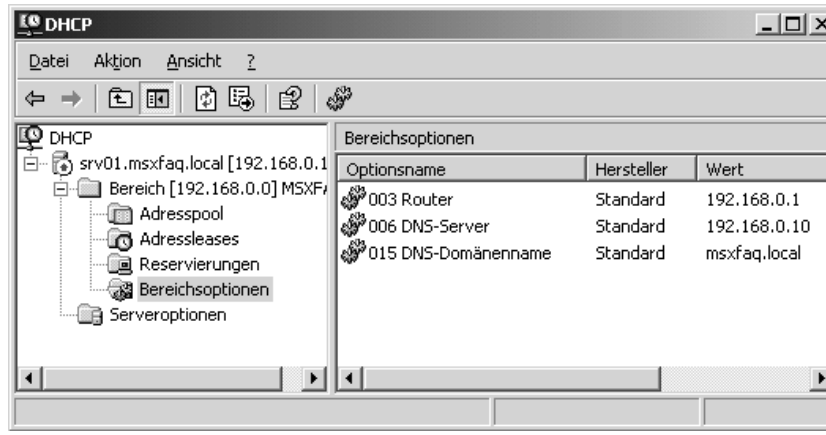


Abbildung 7.13 DHCP-Einstellungen

Bei den globalen Eigenschaften tragen wir entsprechend der Dokumentation das Gateway 192.168.0.1 und den DNS-Server 192.168.0.10 ein. Die DNS-Domäne erhält in unserem Beispiel den Wert „msxfaq.local“.

7.12 DNS konfigurieren und kontrollieren

Die Installation des Active Directory mittels DCPROMO hat für die Einrichtung der Namensauflösung schon ganze Arbeit geleistet. Der lokale DNS-Server ist bereits installiert und konfiguriert und bedient die Zone „msxfaq.local“.

In der Zone „msxfaq.local“ müssen die Einträge für den Domänencontroller richtig registriert sein. Prüfen Sie, ob alle IP-Adressen korrekt sind und nicht in die Irre weisen. Besonders Server mit DFÜ-Netzwerk oder anderen Steckkarten, die eine Netzwerkkarte simulieren (z.B. Dell RMA-Adapter), sind hier anfällig. Diese nicht permanent erreichbaren Adressen sollten nicht im DNS-Server auftauchen.

Auch wenn Windows die meisten Einträge selbst durchführt, so kann das System nicht alle Einstellungen selbstständig ermitteln und eintragen. Folgende Dinge müssen wir daher selbst anpassen:

Reverse-Zone einrichten

Ein DNS-Server sorgt nicht nur dafür, dass logische Namen auf IP-Adressen umgesetzt werden, sondern auch, dass aus IP-Adressen entsprechende Namen ableitbar sind. Diese Funktion erfüllt die Reverse-Zone für das Subnetz 192.168.0.0/24. Zwar ist dies nicht unbedingt für die Funktion notwendig, beschleunigt aber Programme wie Tracert und Pathping, die neben der IP-Adresse auch den Namen anzeigen möchten. Dies ist besonders bei der Fehlersuche sehr nützlich.

Eintrag für Router

Im Windows DNS-Server können sich alle Systeme selbst dynamisch eintragen, die entsprechend autorisiert sind. Dies ist die Standardeinstellung in der DNS-Zone (dynamische sichere Updates). Im Musternetzwerk gibt es weitere Geräte, die sich nicht selbst eintragen und daher im DNS gepflegt werden sollten. Somit wird der DNS-Server zur aktuellen Datenbank Ihrer Geräte. In unserem Fall ist der Router 192.168.0.1 als Host einzutragen. Weitere Geräte wie Drucker, der Switch und andere Systeme können Sie ebenfalls eintragen. Durch die Aktivierung der Checkbox für den PTR-Eintrag erfolgt automatisch auch der Reverse-Eintrag.

Forwarder einrichten

DNS-Anfragen weiterleiten

Damit der DNS-Server auch externe Adressen auflösen kann, muss er mitgeteilt bekommen, welche externen Server er hierzu befragen kann. Der Eintrag eines Forwarders wird erst möglich, nachdem Sie die Root-Zone „.“ entfernt haben. Warten Sie danach einige Minuten und starten den DNS-Dienst neu, damit dieser die neuen Einstellungen übernimmt. Sie können nun in den Eigenschaften des Servers einen DNS-Forwarder eintragen. In der Musterinstallation ist dies der Router, der als DNS-Proxy arbeitet. Bei einer Standleitung sollten Sie die DNS-Server nutzen, die Ihnen Ihr Provider nennt. Wenn Sie eine Firewall einsetzen, nutzen Sie eventuell auch ein eigenes DNS-Relay in der DMZ. Nur wenn all das nicht funktioniert, sollte Ihr DNS-Server die „Root-Server“ des Internets fragen.

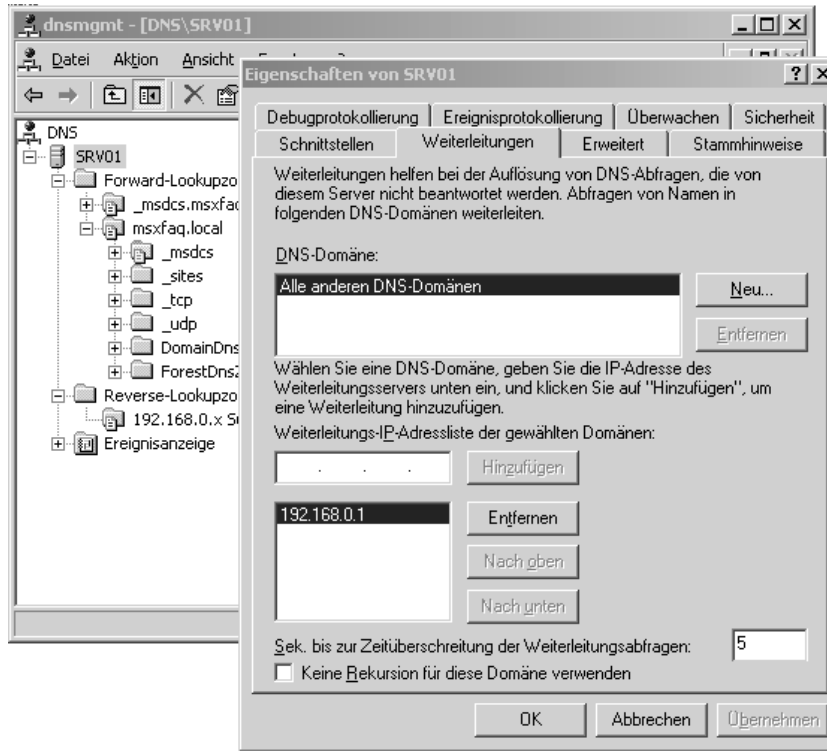


Abbildung 7.14 DNS-Weiterleitung

Nach diesen Einstellungen kann der DNS-Server alle lokalen Anfragen zur Domäne „msxfaq.local“ und die IP-Adressen von 192.168.0.x auflösen. Alle weiteren Anfragen leitet er an die Adresse 192.168.0.1 weiter, die später dem Internet-Router zugewiesen wird.

7.13 Aktualisierung

Nachdem Sie denWindows 2003 Server installiert haben, sollten Sie prüfen, ob es bereits erforderliche Updates gibt. Dazu zählen Service Packs und Hotfixe, die unter anderem auch als sicherheitskritisch eingestuft sind.

Unter http://windowsupdate.microsoft.com/ können Sie den Server prüfen, nach wichtigen Updates suchen und diese installieren lassen. Beim Einsatz mehrerer Server sollten Sie sich die Einführung des *Windows Software Update Service* (WSUS) überlegen.

Microsoft empfiehlt die Installation des Windows 2003 Server Service Pack 1 für den Einsatz von Exchange 2003 Server SP2.

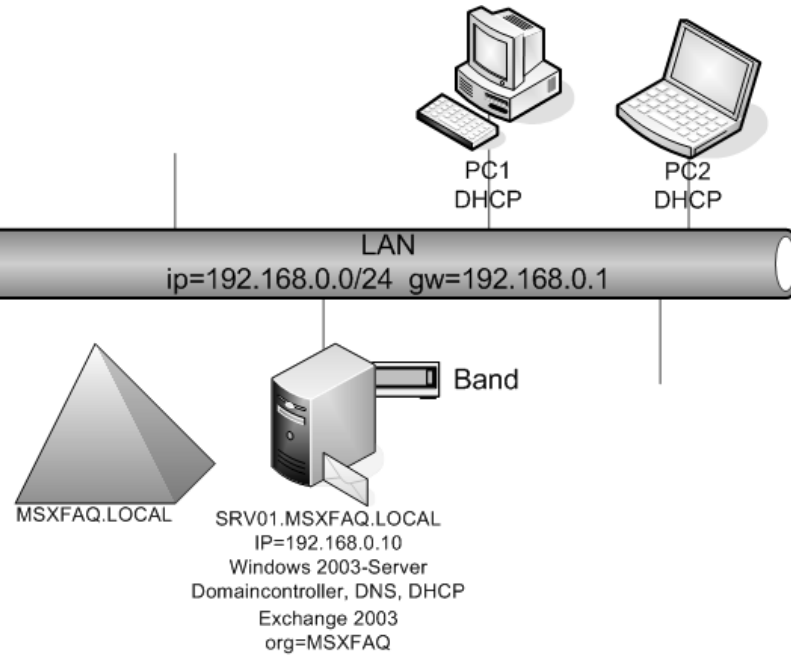
8

Exchange 2003 installieren

8 Exchange 2003 installieren

Nach der Installation des Windows 2003-Servers samt Active Directory und Namensauflösung folgen Installation und Konfiguration des Exchange 2003-Servers. Aufbauend auf der bisherigen Musterinstallation wird der bestehende Server auch zum Exchange 2003-Server.

Abbildung 8.1 Installation Schritt 2



Es ist natürlich ebenso möglich, einen zweiten Server in das Netzwerk aufzunehmen und darauf Exchange 2003 zu installieren.

8.1 Exchange-Konfigurationsdaten

Für die Installation von Exchange sind Vorgaben zu definieren. Einige dieser Parameter sind nachträglich nur sehr schwer wieder änderbar. Wenn Sie von Exchange 5.5 in der gleichen Organisation migrieren, sind Sie an die dort vorgegebenen Einstellungen wie den Namen der Organisation-Namen und der Standorte gebunden.

Exchange organisiert seine Dienste in Organisationen, Administrativen Gruppen und Routinggruppen. Zumindest die Exchange-Organisation (ORG) ist bei der ersten Installation anzugeben. Die beiden anderen Parameter werden durch das Setup vorgegeben.

E1 — Name der Organisation

Organisation: MSXFAQ

In einem Active Directory kann es immer nur genau eine Exchange-Organisation geben. Speziell wenn mehrere Firmen in einem Active Directory zusammenarbeiten, ist die Wahl dieses Namens immer auch eine politische Angelegenheit und nicht unbedingt einfach zu klären. Der Name der Organisation kann nachträglich nur durch eine Neuinstallation geändert werden. Zwar sieht ein Anwender den Namen der Organisation in der Regel nie, aber es ist bei einer Umfirmierung natürlich auf Dauer störend, den alten Firmenname immer noch an diversen Stellen zu sehen. Wird eine Firma übernommen oder ein Teil abverkauft, sind in der Regel die Veränderungen schon aus Sicht des Active Directory so gravierend, dass hier der Name nicht mehr kritisch ist. Wir wählen für das Beispiel einfach „MSXFAQ“. Vermeiden Sie bitte auch hier Leerzeichen, Umlaute und Sonderzeichen, da dieser Name ein Teil des LDAP-Pfades wird.

E2 — Name der Administrativen Gruppe (AG)

AG: Erste administrative Gruppe

Den Namen der „Ersten administrativen Gruppe“ können Sie bei der Installation nicht bestimmen, da das Exchange-Setup nicht nachfragt, sondern je nach Sprache automatisch eine „First Administrative Group“ oder „Erste administrative Gruppe“ anlegt. Dies können Sie im Nachhinein ändern. Erst bei weiteren administrativen Gruppen sollten Sie eine Namensvergabe definieren.

E3 — Default SMTP-Domäne

SMTP-Domäne: msxfaq.de

Wichtig ist hingegen die Definition der SMTP-Domäne, unter deren Namen die Nutzer Ihres Exchange-Servers später die Nachrichten senden und empfangen. Das Setup übernimmt hier die DNS-Domäne des Active Directory. Mit `frank.carius@msxfaq.local` wird Frank sicher keine Nachricht empfangen können. In der Musterinstallation wird daher „msxfaq.de“ genutzt. Bitte tragen Sie Ihre SMTP-Domäne als Standard ein. Domänen wie t-online.de oder aol.com sind allerdings nur bedingt geeignet. Sie sollten einen eigenen Domänennamen besitzen. Erst dann bekommt der Aufwand für einen eigenen E-Mail-Server auch einen Sinn.

E4 — Nachrichtenverfolgung

Tracking aktivieren

Exchange kann alle Übertragungen von Nachrichten protokollieren. Wenn Sie daher den Weg einzelner Nachrichten in Exchange verfolgen (tracking) möchten, müssen Sie die Protokollierung in den Server-Eigenschaften aktivieren und die Verfallszeit entsprechend einstellen. In der Musterinstallation werden die Protokolle nach sieben Tagen gelöscht.

E5 — Postfachrichtlinien

Postfach-Limit: max. 150 MB

Weiterhin sollten Sie die maximale Größe eines Postfachs definieren, also ab wann keine Nachrichten im Postfach empfangen und gesendet werden können. Ein zu kleiner Grenzwert behindert die E-Mail-Anwender oder verführt zur Ablage von Dateien in lokalen PST-Dateien. Ein zu großer oder gar kein Grenzwert kann bei einem Virus, einem Fehler oder anderem Missbrauch den gesamten Server außer Betrieb setzen. In der Musterumgebung nutzen wir 100 MB, 120 MB und 150 MB als Grenzen für Warnung, Senden verbieten und komplette Sperre auf dem Postfachspeicher. Individuelle Regelungen pro Anwender sind weiterhin möglich.

E6 — Richtlinien für Öffentliche Ordner

Public Folder-Limit: 300 MB

Für öffentliche Ordner können Verfallszeiten und eine Warngrenze festgelegt werden. Natürlich ist es besser, diese Einstellungen je Ordner individuell vorzunehmen. Globale Grenzen sorgen jedoch für die Einhaltung der Maximalwerte, die Sie als Administrator vorgeben, und sichern damit die Betriebsbereitschaft Ihres Servers. In der Musterinstallation wird die Verfallszeit auf „nie“ gesetzt, während die Warnung für die Größe eines Ordners auf 300 MB eingestellt wird. So löscht Exchange selbst nie eine Nachricht, sendet jedoch eine Warnung an den Ordnerbesitzer, wenn dessen Ordner über 300 MB wächst. Es ist kein Problem, später dieses Limit pro Ordner oder global höher zu setzen, wenn die Nutzung dies erfordert. Aber Sie unterbinden so ein ungeplantes und vor allem unbemerktes Volumenwachstum.

E7 — Datenbankpfad

Pfad festlegen für *.edb und *.stm

Entsprechend Ihrer Server-Dimensionierung und Festplattenkonfiguration werden Sie nach der Exchange-Installation die Datenbanken in die gewünschten Zielpartitionen verschieben. Dokumentieren Sie die Einstellungen, damit Sie im Falle der Wiederherstellung auch die richtigen Datenbanken nutzen. Sehr oft finden sich im Fehlerfall auf einem Exchange-Server mehrere Datenbanken früherer Kopien, Reparaturversuche etc., so dass Sie den Pfad der produktiven Datenbank kennen sollten.

Dies sind bei weitem nicht alle Exchange-Einstellungen, die Sie vornehmen können. Dokumentieren Sie auf jeden Fall alle Einstellungen und Änderungen, damit bei einem späteren Neuaufbau oder einer Erweiterung diese geprüft werden können. Allzu oft werden die individuellen Einstellungen bei einer Änderung der Installation wieder auf die Standardwerte zurückgesetzt.

8.2 Exchange-Software-Installation

Mit diesen Vorbereitungen kann die Installation von der CD gestartet werden. Das Exchange-Setup startet zuerst einen Assistenten (Wizard), bei dem auf den ersten Blick nicht sofort erkenntlich ist, wie das eigentliche Exchange-Setup nun gestartet wird.

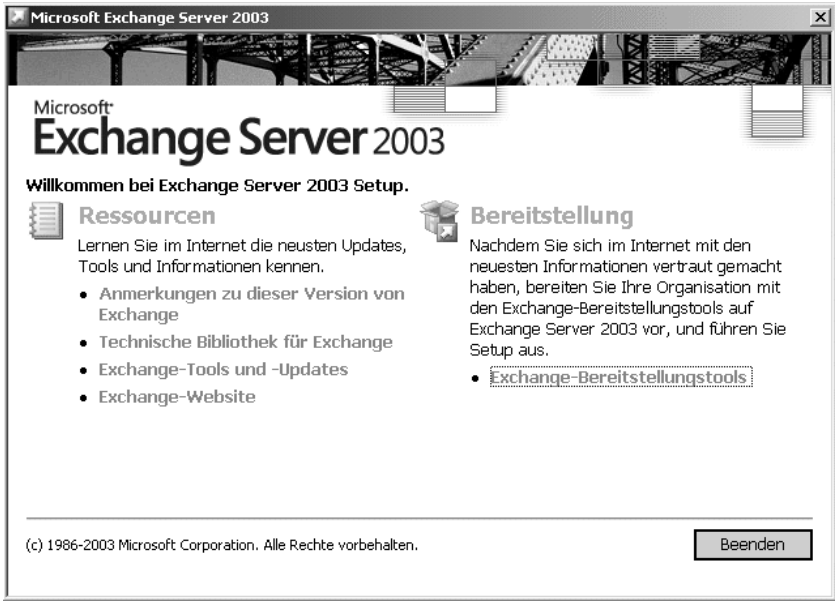


Abbildung 8.2 Exchange-Installations-Assistent

Auf der rechten Seite finden Sie den Punkt „Exchange-Bereitstellungstools“. Diese starten den Assistenten für den Installationsprozess. Alle anderen Punkte führen Sie auf die Microsoft-Webseite oder zu der mitgelieferten Dokumentation.

Wizard reduziert Installationsfehler und -probleme

Microsoft hat sich nach einer Analyse der Support-Anrufe und der häufigsten Problem- und Fragestellungen für die Integration eines ausführlichen Assistenten entschieden. Der Assistent führt Sie sehr genau an die Installation eines Exchange 2003-Servers heran und hilft Ihnen, die meisten Fehler bei der Exchange-Installation zu vermeiden. Der Assistent ersetzt aber kein grundlegendes Know-how über die Zusammenhänge und eine ordentliche Konzeption. Speziell bei Migrationen ist eine vorbereitende Schulung, Informationsbeschaffung und Planung notwendig.

Sie können weiterhin das eigentliche Exchange Setup-direkt von der CD aus dem Verzeichnis „<CD:>\SETUP\I386\SETUP.EXE“ starten und damit den Assistenten komplett umgehen. Das Setup unterstützt auch die vollautomatische Installation von Exchange 2003 mittels einer vorbereiteten Antwortdatei (Unattended Setup).

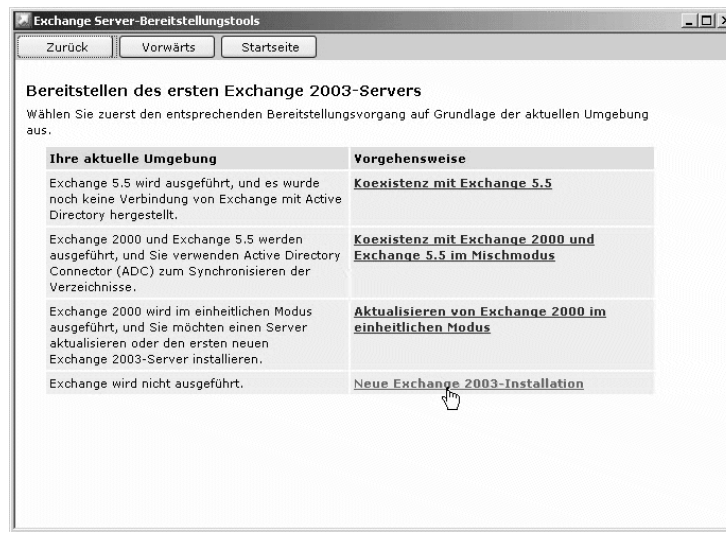
Trotzdem ist es auch für erfahrene Administratoren ratsam, den Assistenten zu nutzen, um frühzeitig Probleme zu erkennen. Auch wenn Sie sicher sind, all die Schritte sowieso zu kennen und alles richtig gemacht zu haben, sollten Sie nicht auf den Wizard verzichten. Selbst ein Flugzeugpilot arbeitet eine Checkliste vor dem Start ab.

Allen Lesern, die schon mit einer Exchange 2003-Beta-Version experimentiert haben, ist dieser Assistent ebenso neu wie für alle Exchange 2000-Administratoren.

Abbildung 8.3 Exchange 2003-Installation

Für die Musterinstallation ist der erste Vorgang zutreffend, da dieser Server der erste und einzige Exchange 2003-Server ist. Abhängig von der hier getroffenen Entscheidung geleitet Sie der Assistent durch weitere Schritte.

Abbildung 8.4 Exchange 2003 Schritt 3



Erst jetzt wird die Entscheidung gefällt, ob Sie eine neue Exchange-Organisation installieren oder einer bestehenden beitreten wollen.

Die Musterinstallation bezieht sich auf eine neue Exchange 2003-Installation, da keine Exchange 5.5- oder Exchange 2000-Server existieren.

8.2.1 Vorbereitung

QS für Windows- und AD-Installation

Der Assistenten fordert Sie nun dazu auf, diverse Prüfungen vor der eigentlichen Installation durchzuführen. Dazu gehören Selbstverständlichkeiten wie die Installation des passenden Windows-Servers und der notwendigen Dienste. Auch die Installation der Support-Tools und die Nutzung von DCDIAG und NETDIAG werden angemahnt. Diese Prüfungen sind wichtig, da sehr viele Installationen fehlschlagen, da die Basis nicht korrekt funktioniert. Die ordnungsgemäße Funktion des Servers wurde in der Musterinstallation schon durch entsprechende Prüfungen bei der Windows- und Active Directory-Installation sichergestellt.

Ehe Sie aber die Installation fortsetzen, sollten Sie kontrollieren, dass keine anderen Dienste die Installation behindern könnten. Kandidaten für solche Störungen sind:

SNMP und PERFMON

Diese Dienste und Programme blockieren die Performance Counter und verhindern, dass das Exchange-Setup die eigenen Werte hinzufügt. Dies gilt auch für Systeme, die über das Netzwerk solche Parameter auslesen und überwachen.

Programme zur Überwachung

Monitoring deaktivieren

Das Exchange-Setup stoppt und startet sehr viele Dienste. Es gibt Programme, die die Funktion eines Dienstes oder Servers überwachen. Wird der Server aus Sicht des überwachenden Programms ungeplant gestoppt, startet das Monitoring den Dienst neu. Diese Funktion bietet sogar Windows 2003 selbst, sie muss nur noch vom Administrator entsprechend konfiguriert werden. Während der Installation von Exchange sollte kein anderes Programm Dienste stoppen und starten.

Virenscanner

Bei der Installation von den Exchange 2003-Originalmedien sollte kein Virenscanner anschlagen. Trotzdem kommt es immer wieder vor, dass ein Virenscanner die Installation auch ohne Meldung vereitelt. Manchmal ist daher die kurzzeitige Deaktivierung notwendig.

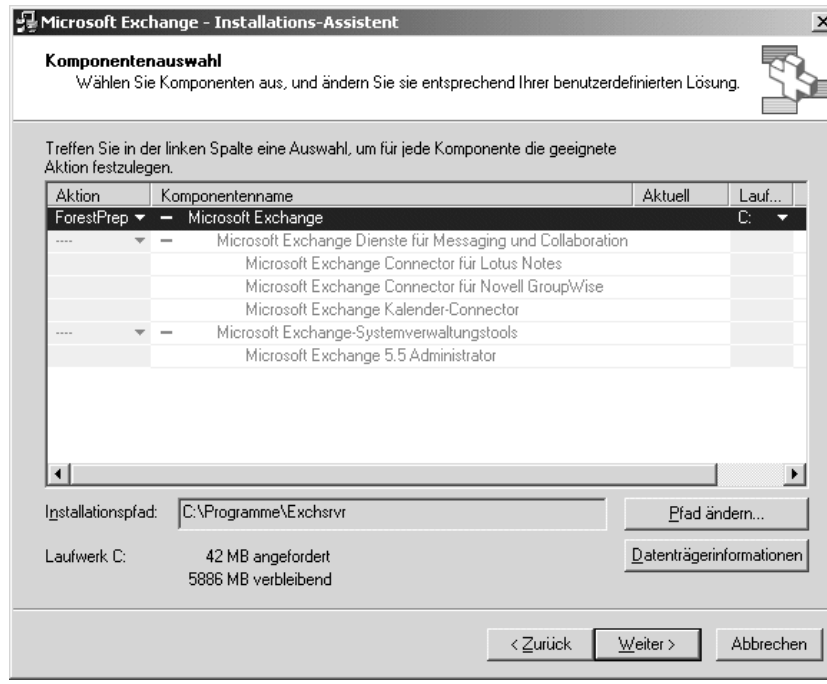
Fehlgeschlagene Installation

Bei einer fehlerhaften Installation hilft auch die Datensicherung nicht mehr den Server in die Ursprungszustand zu setzen. Ein abgebrochenes Exchange-Setup führt an verschiedenen Stellen Änderungen durch, die eine Wiederherstellung des Servers nur dann ermöglicht, wenn dies der einzige Server für AD und Exchange war. Sobald mehrere Exchange-Server und Domänencontroller existieren, werden die Änderungen des Setups auch auf alle anderen Server repliziert. In diesem Fall ist es besser, die Ursache für den Fehler zu finden und die Installation erneut zu starten. Dazu schreibt Exchange eine Protokolldatei C:\Exchange Server Setup Progress.Log, anhand dieser der Fehler für einen Abbruch genauer analysiert werden kann.

8.2.2 ForestPrep

Die eigentliche Exchange-Installation startet mit der Durchführung der Active Directory-Vorbereitung. Durch den Aufruf von ForestPrep werden das Schema und die ersten Konfigurationseinstellungen im Active Directory durchgeführt. Der Assistent startet das Exchange-Setup mit der Option „/FORESTPREP“ und erweitert das Schema.

Abbildung 8.5 Aufruf von ForestPrep



Die eigentliche Schema-Erweiterung besteht aus zehn einzelnen Dateien, die nacheinander importiert werden. Der Vorgang dauert einige Minuten.

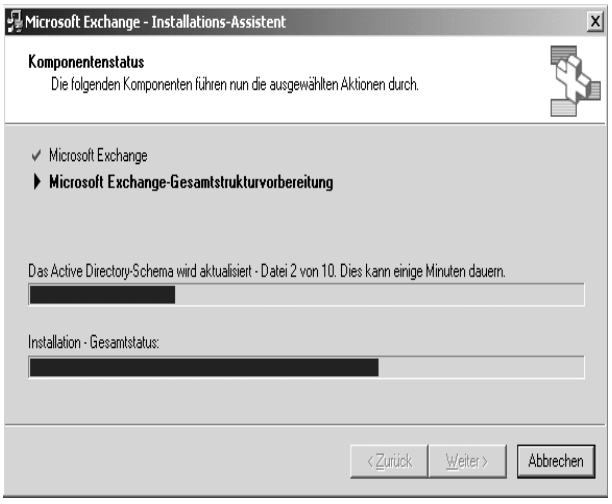


Abbildung 8.6 Schema wird erweitert.

Der eigenständige Aufruf von ForestPrep ist notwendig, wenn die Rolle des Schema- und Organisations-Administrators nicht gleichzeitig dem Exchange-Administrator zugewiesen wird. Das Setup prüft auch später immer wieder ab, ob der Forest bereits erweitert wurde. Vergessen Sie diesen Schritt, führt das Setup den ForestPrep später automatisch durch, sofern der installierende Benutzer die Berechtigungen dazu hat.

ForestPrep erweitert auch die AD-Konfiguration um den Bereich „Microsoft Exchange“, in dem alle weiteren Exchange-Einstellungen abgelegt werden.

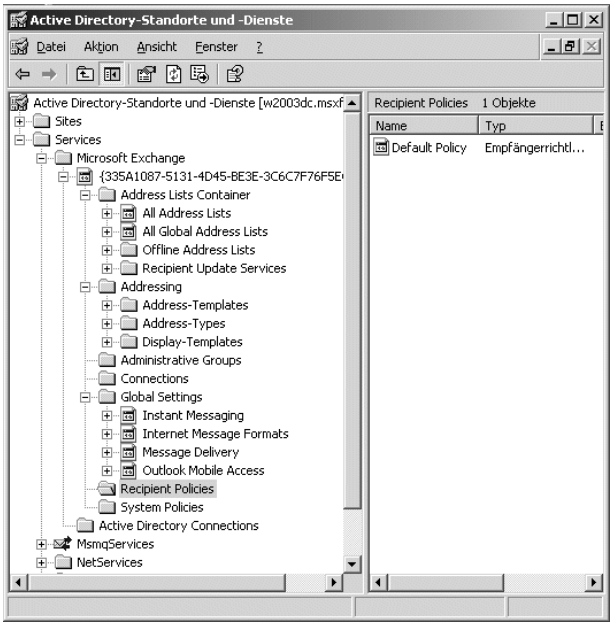


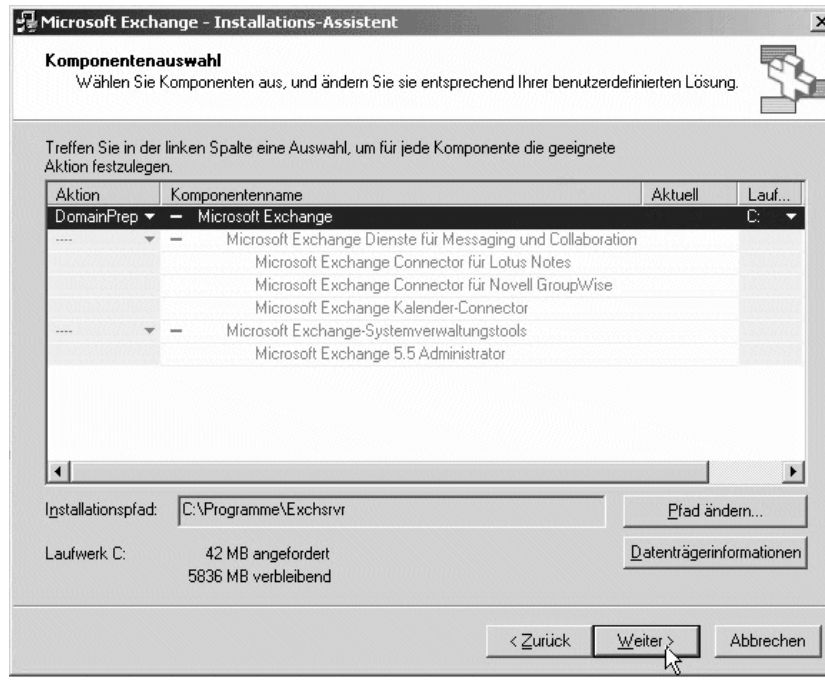
Abbildung 8.7 ADSI Edit nach dem ForestPrep

Der Name der Organisation ist jedoch noch nicht vergeben. Ebenso wurden noch keine administrativen Gruppen angelegt.

8.2.3 DomainPrep

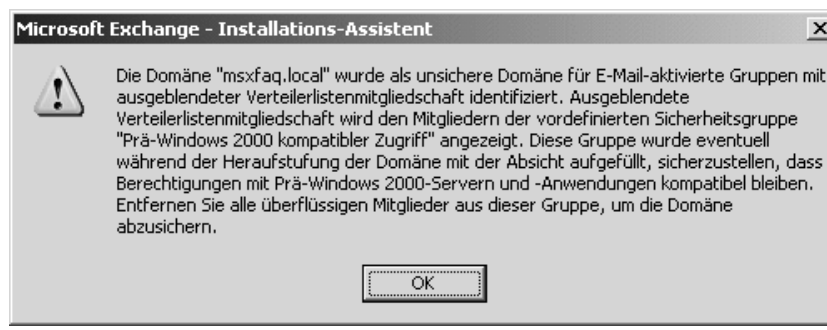
Der nächste Schritt vor der Exchange 2003-Installation ist die Vorbereitung der Domäne. Hierbei werden unter anderem die versteckte OU „*Microsoft Exchange System Objects*“ sowie Sicherheitsgruppen angelegt und Berechtigungen gesetzt. Der Assistent startet für Sie das Exchange-Setup mit der Option „/DOMAINPREP“. Diese Vorbereitung der Domäne muss später für jede Domänen im Forest einmalig durchgeführt werden, in der Sie Exchange-Objekte anlegen.

Abbildung 8.8 Auswahl von DomainPrep



Durch WEITER wird die Domänenerweiterung gestartet. Hierbei wird gegebenenfalls folgende Warnung ausgegeben:

Abbildung 8.9 Warnung unsichere Domäne



Bei der Installation des Active Directory wird eine Gruppe „Prä-Windows 2000 kompatibler Zugriff“ eingerichtet. Aus der Windows NT 4-Zeit gibt es Programme und Dienste, die als anonyme Benutzer bestimmte Einstellungen aus der Domänendatenbank lesen. Dazu gehört z.B. der Windows NT 4-RAS-Dienst. Dies bedeutet aber auch, dass Mitglieder dieser Gruppe auch die Informationen der Verteilerlisten lesen können. Um auszuschließen, dass die Berechtigungen dieser Gruppe von Anwendungen oder Diensten in Ihrem Netzwerk verwendet werden, können Sie die Mitglieder aus dieser Gruppe entfernen. Bitte löschen Sie die Gruppe nicht sofort, Sie können, bei einem Irrtum, diese Aktion nicht rückgängig machen. Bestätigen Sie diese Meldung, damit das Exchange 2003-Setup die Vorbereitung der Domäne durchführt.

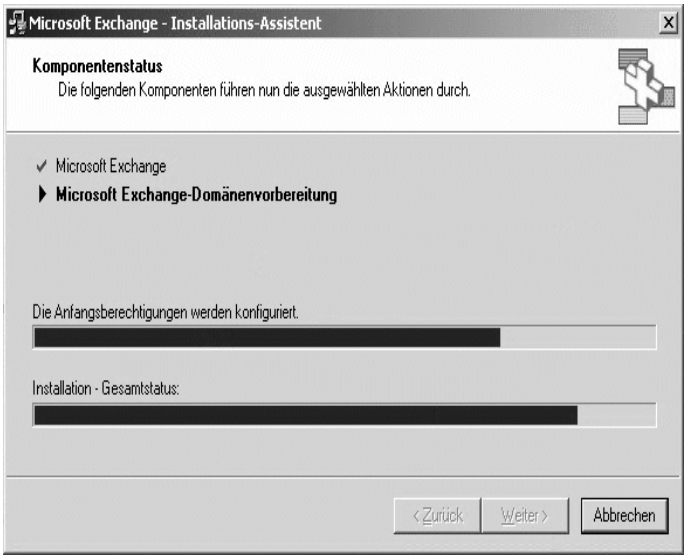


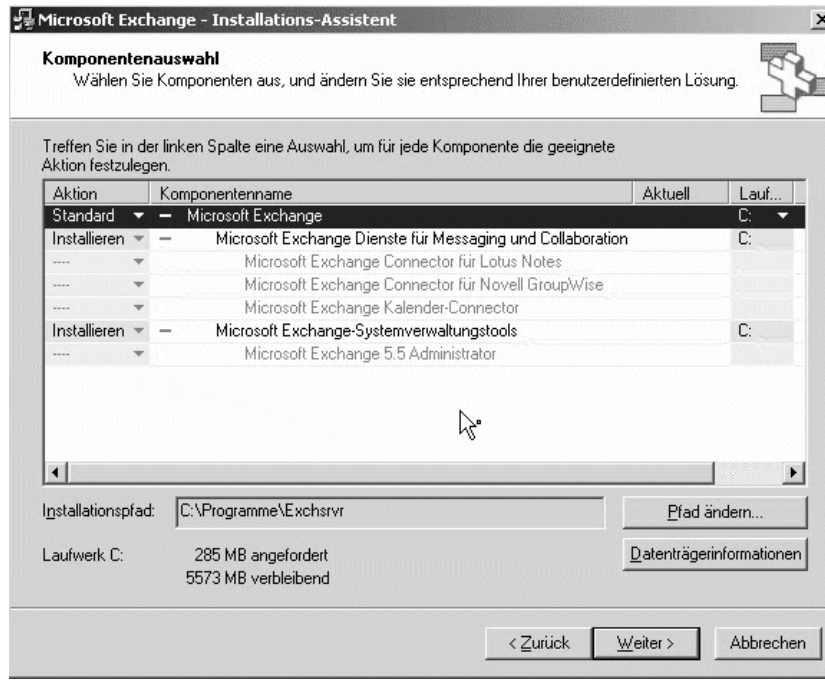
Abbildung 8.10 DomainPrep wird ausgeführt.

Die Trennung von DomainPrep und ForestPrep von der eigentlichen Exchange-Installation erlaubt es größeren Firmen, die Durchführung zeitlich und personell zu trennen. Werden diese Schritte nicht durchgeführt, dann versucht das Exchange-Setup bei der Installation des eigentlichen Servers, dies erneut durchzuführen.

8.2.4 Serverinstallation

Erst jetzt kann die eigentliche Exchange 2003-Server-Installation erfolgen. Der Assistent startet dazu die Installationsroutine und erlaubt die Auswahl der gewünschten Komponenten.

Abbildung 8.11 Exchange-Setup-Hauptauswahl



Der Standardumfang ist für die Musterinstallation ausreichend. Die Connectoren zu Notes und GroupWise sowie der Kalender-Connector für diese Systeme sind ebenso wenig erforderlich wie der Exchange 5.5-Administrator, der nur bei Migrationen von Exchange 5.5 mit installiert werden sollte. An dieser Stelle ist auch die Änderung des Zielpfades möglich, der bei der Musterinstallation auf „C:\Programme\exchsrvr“ belassen wird.

Die Frage nach der Organisation ist eine entscheidende Gabelung bei der Installation von Exchange 2003. Bei der Musterinstallation wird eine neue Exchange-Organisation angelegt. Obwohl bei der bisherigen Nutzung des Assistenten immer eine Neuinstallation statt einer Migration ausgewählt wurde, bietet das Exchange 2003-Setup hier trotzdem den Beitritt in eine bestehende Exchange 5.5-Organisation an.

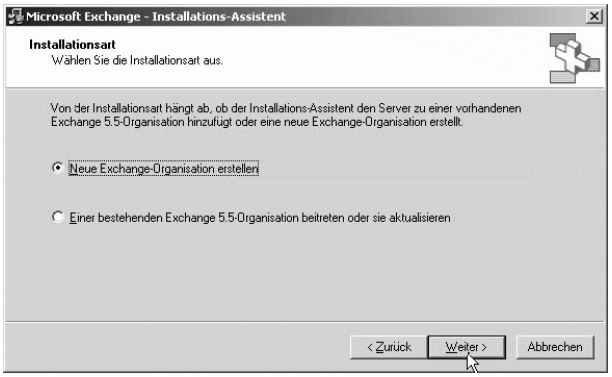


Abbildung 8.12 Neue oder bestehende Organisation?

Wenn Sie tatsächlich schon Exchange 5.5-Server betreiben, dann sollten Sie hier abbrechen und den Assistenten für die Migration nutzen. Bei einer Migration von Exchange 5.5 nach Exchange 2003 ist die Installation von Exchange 2003 niemals der erste Schritt. Vorab sind weitere Vorbereitungen zu treffen (siehe Kapitel „Migration“).

Der Name der Exchange-Organisation in der Musterinstallation lautet MSXFAQ.

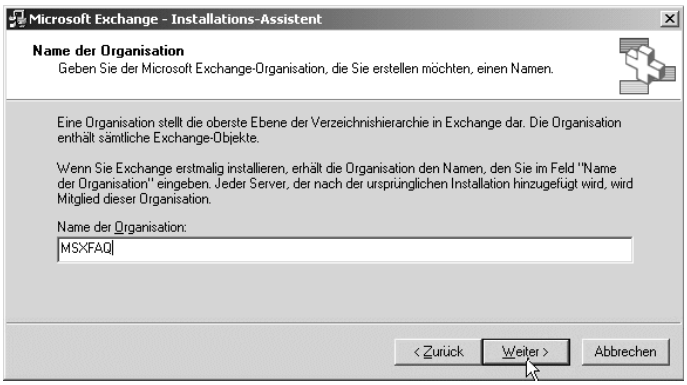
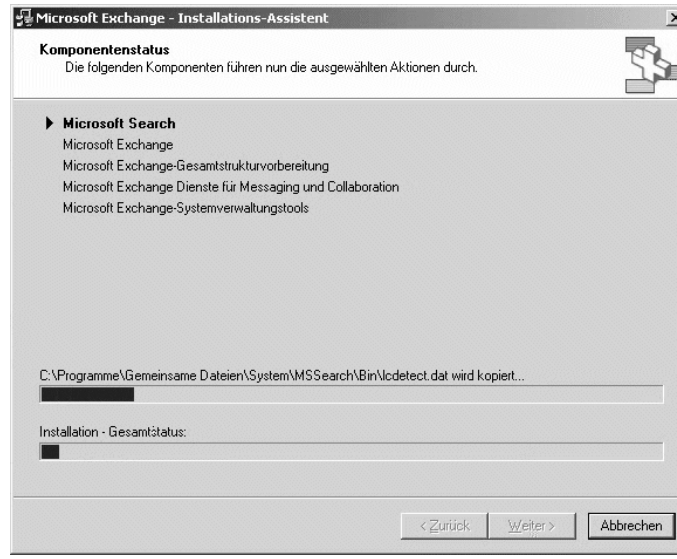


Abbildung 8.13 Eingabe der Organisation

Nach der Bestätigung und der Annahme der Lizenzbedingungen startet nun die eigentliche Exchange 2003-Installation, die einige Minuten in Anspruch nimmt. Dabei werden mehrfach Dienste gestoppt, gestartet und Dateien kopiert. Sie können Sie Status der Komponenten beobachten.

Abbildung 8.14 Installation wird durchgeführt.



Nach der Installation sind die Exchange 2003-Dienste gestartet und der Server ist meist ohne Neustart betriebsfähig. Ein Neustart ist nur dann notwendig, wenn das Setup einige Dateien nicht kopieren konnte, da diese gesperrt waren. Dieses Verhalten weist nachträglich auf nicht beendete Dienste und Funktionen hin, die Exchange bei der Installation behindern.

Interessant ist auch die Information, die Sie vom Exchange-Setup mit dem Parameter „/?“ erhalten. Für Unternehmen mit vielen Exchange-Servern kann die Vorbereitung einer automatischen Installation sehr nützlich sein.

Abbildung 8.15 Setup-Kommando-zeilen

Die Option „/DISASTERRECOVERY“ dient zur Exchange-Installation unter Beibehaltung der bisherigen Datenbanken und Einstellungen im Active Directory und ist hilfreich, wenn die Exchange-Installation auf dem Server defekt ist, aber die Datenbanken noch vorhanden sind.

Vorsicht, Datenverlust möglich!

Allerdings fehlt die Option „/REMOVEORG“ in der Auflistung, mit der Sie die komplette Konfiguration im Active Directory ohne Rückfrage löschen können. Dies benötigen Sie für einen Exchange-Neuanfang, um die Organisation anders zu benennen. Durch diese Option verlieren Sie allerdings den Zugriff auf alle Informationen in den Exchange-Datenbanken Ihres gesamten Forests. Die Option funktioniert nur, wenn Sie auch entsprechende Berechtigungen besitzen.

8.2.5 Abschließende Schritte

Nach der Installation des ersten Servers bietet der Assistent die Hilfe zur Installation weiterer Server an. Diese Auflistung entspricht im Wesentlichen der ersten Liste bis auf den Punkt „ForestPrep“. Dieser ist bei weiteren Servern nicht mehr notwendig. „DomainPrep“ benötigen Sie nur bei einer weiteren Domäne, unabhängig vom Exchange-Server.

Ebenso weist der Assistent Sie darauf hin, dass Sie bestehende Postfächer von anderen Servern auf diesen Server verschieben und Öffentliche Ordner replizieren können. Bei dem hierbei beschriebenen „*Exchange Public Folder Migration Tool*“ handelt es sich um das Skript „*pfmigrate.wsh*“ zum Ändern der Replikate. Dieses Skript ist bei Migrationen sehr hilfreich. Obwohl es nur auf einem Exchange 2003-Server ausgeführt wird, kann es von dort indirekt die Einstellungen der Exchange 5.5- und Exchange 2000-Systeme anpassen. Im Fall der Musterinstallation ist beides nicht notwendig.

8.2.6 Hauptspeicheroptimierung

Windows 2000 und Windows 2003 reservieren in der Standardeinstellung zwei Gigabyte für die Anwendungen. Dies war vor einigen Jahren noch sehr viel Speicher. Mittlerweile besitzen die meisten neuen Server bereits mehr Hauptspeicher. Exchange 2003 nutzt diesen zusätzlichen Speicher nur, wenn es entsprechend konfiguriert wird.

Wichtig ist eine Grenze von ca. 1 GB Hauptspeicher. Bis dahin passt Exchange 2003 die Einstellungen selbst dynamisch an die Anforderungen an. Sobald ein Server mehr als 1 GBHauptspeicher bereitstellt, sind zusätzliche Konfigurationen erforderlich.

Mehr Hauptspeicher nutzen

Bei den Betriebssystemen Windows 2003-Server oder Windows 2000 Edition „Advanced“ und „Datacenter“ kann mit der Option „/3GB“ in der BOOT.INI eine alternative Speicherzuteilung aktiviert werden. Auf einem Windows 2003-Server ist zusätzlich der Eintrag „/USERVA“ in der BOOT.INI möglich. Allerdings ist die Optimierung von Exchange für große Speichermengen damit alleine nicht getan. Ob Ihr Exchange 2003-Server korrekt konfiguriert ist, können Sie im Eventlog nachlesen. Der Informationsspeicher prüft die Werte und meldet im Eventlog die „EventID 9665“, wenn die Voraussetzungen nicht erfüllt sind. Entsprechende White Papers von Microsoft liefern weitergehende Konfigurationshinweise für große Server.

Hauptspeicher – anpassung SP1

Nach dem Update auf Service Pack 1 sollten Sie noch weitere Konfigurationen vornehmen. Der Wert der Option /userva sollte zwischen 2970 und 3030 liegen. Zudem sollten folgende Werte der Registrierungsschlüssel angepasst werden:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Session Manager\HeapDeCommitFreeBlockThreshold = 0x00040000

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Session Manager\Memory Management\SystemPages = 0
```

8.2.7 Service Packs und Updates

Aktueller Stand schützt das System

Nach der Installation sollten Sie sofort kontrollieren, ob alle Komponenten auf Ihrem Server aktuell sind. Besonders die Funktion „*Windows Update*“ sollten Sie regelmäßig ausführen, um das Betriebssystem Ihres Servers aktuell zu halten. Obwohl die wenigsten Server direkt aus dem Internet erreichbar sind, haben Viren wie MSBLAST und andere gezeigt, dass auch von intern eine erhebliche Gefahr für Server besteht. Prüfen Sie die aktuellen Updates für Exchange 2003. Die Installation des Service Pack 1 sowie Konfigurationsanpassungen werden ab Kapitel 8.8 beschrieben. Bitte lesen Sie die „Release Notes“ des Service Packs, um Abhängigkeiten zu erkennen und zu beachten.

8.3 Exchange-Basiskonfiguration

Exchange 2003 ist zwar von Hause aus sicherer konfiguriert als Exchange 2000, dennoch sind einige Einstellungen notwendig, ehe Sie die ersten Postfächer anlegen können. Zur Konfiguration wird der ESM aus dem Startmenü aufgerufen.

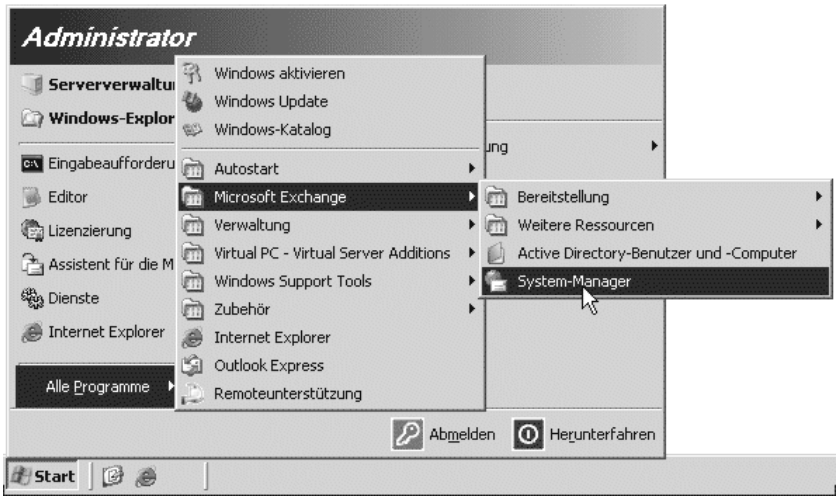


Abbildung 8.16 Startmenü der Exchange-Programme

Alle folgenden Tätigkeiten werden im Exchange System-Manager (ESM) ausgeführt. Sie können den ESM in einen erweiterten Modus schalten, in dem auch die Administrativen Gruppen und Routinggruppen sichtbar werden. Diese Ansicht ist erst im Kapitel „Enterprise“ notwendig.

8.3.1 Kontrolle der GC/DC-Nutzung

Jeder Exchange-Server greift auf die Domänencontroller und Globalen Kataloge zu. Eine Fehlkonfiguration im Active Directory lässt sich über die Eigenschaften des Exchange-Servers sehr schnell ausfindig machen.

Der Exchange-Server sollte die DCs fragen, die aus Netzwerksicht nahe und schnell angebunden sind. Beim Einsatz mehrerer Domänencontroller und Globale Katalog-Server zeigt die Ansicht im Exchange System-Manager dies entsprechend an, sofern diese in der gleichen AD-Site sind.

Das DSProxy-Verhalten wurde mit SP2 insofern optimiert, dass der Server erkennt, ob ein GC aus einer anderen Domäne kontaktiert werden muss, um beispielsweise die Anpassung von Stellvertreterberechtigungen sowie Gruppenmitgliedschaften domänenübergreifend sicherzustellen.

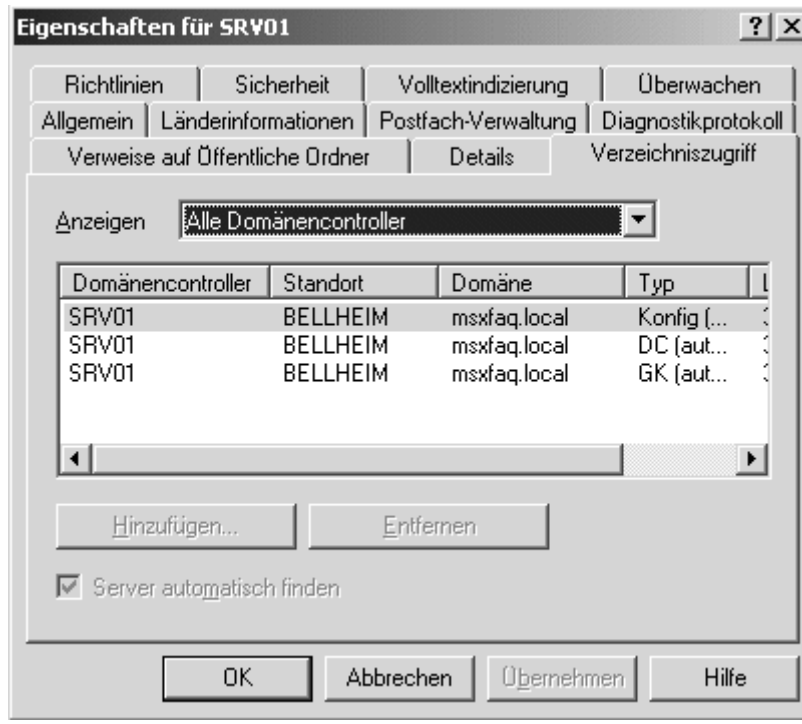


Abbildung 8.17 Verzeichniszugriff des Servers

Stimmt die Anzeige nicht mit Ihren Erwartungen überein, sollten Sie die Einträge im DNS-Server und in *Active Directory-Standorte und -Dienste* kontrollieren.

8.3.2 Empfängerrichtlinien

Gültige SMTP-Standardadresse

Die Empfängerrichtlinien sind in Kombination mit dem Dienst zur Empfängeraktualisierung (RUS) wichtig, damit alle Benutzer und sonstigen Exchange-Objekte eine gültige E-Mail-Adresse erhalten. Exchange 2003 übernimmt bei der Neuinstallation den Domänennamen des Active Directory für die SMTP-Standardadresse. Unsere Musterinstallation mit „msxfaq.local“ als E-Mail-Adresse ist denkbar ungeeignet für einen späteren Betrieb mit einer Internet-Anbindung. Daher ist der nächste Schritt die Anpassung dieser Empfängerrichtlinie „Default Policy“ im ESM unter EMPFÄNGER – EMPFÄNGERRICHTLINIEN.

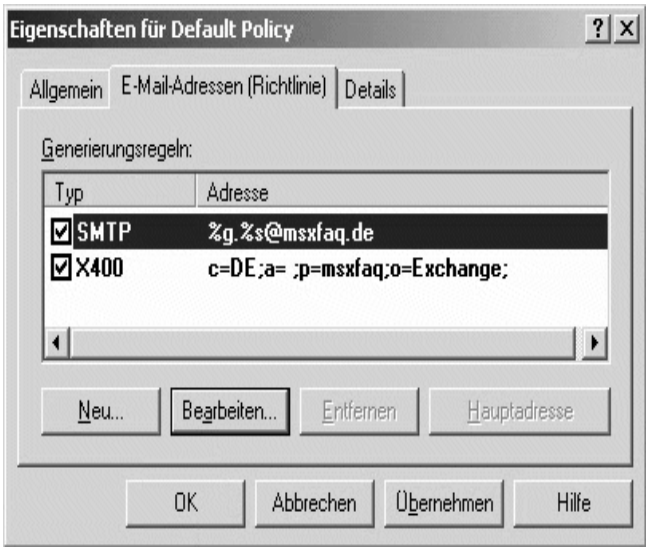


Abbildung 8.18 Empfänger-richtlinien

Denken Sie daran, dass die primäre SMTP-Domäne der „Default Policy" immer *autoritativ* sein muss. Dies darf auch durch keine andere Richtlinie ausgehebelt werden.

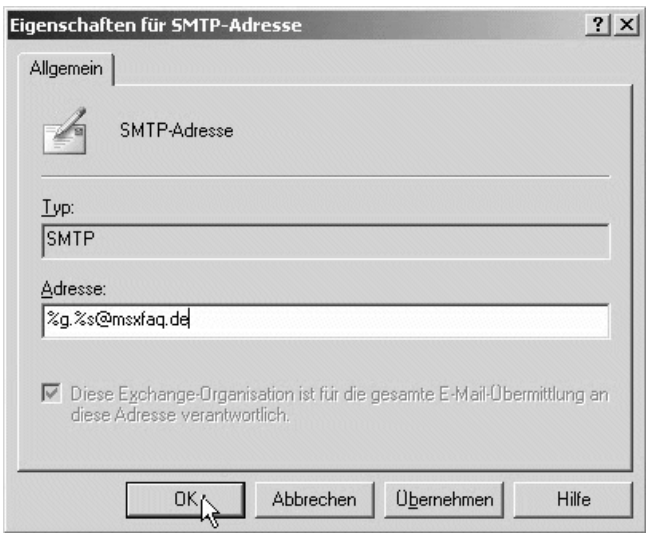


Abbildung 8.19 Einstellung der SMTP-Adresse

Möchten Sie den Adressraum von Exchange mit einem fremden E-Mail-Server nutzen, dann müssen Sie eine andere Einstellung vornehmen (siehe Kapitel „Enterprise"). In der Musterinstallation wird „%g.%s@msxfaq.de" als SMTP-Richtlinie eingetragen, damit die SMTP-Adressen das Format „Vorname.Nachname@msxfaq.de" erhalten. Folgende Variablen sind hierbei einsetzbar:

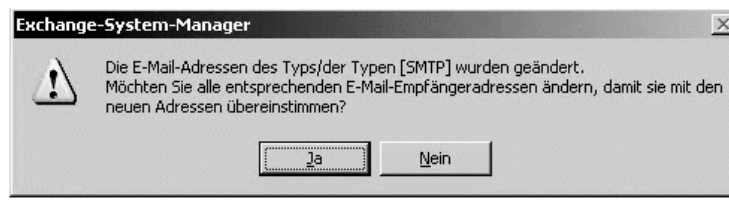
Tabelle 8.1 Variablen für Empfänger-richtlinien

Variable	Bedeutung
%s	Nachname (Surname)
%g	Vorname (Given Name)
%i	Initiale
%d	Angezeigter Name (DisplayName)
%m	Exchange Alias (mailNickname)

Siehe auch TechNet: "Q285136 XADM: How to Customize the SMTP E-Mail Address Generators Through Recipient Policies".

Eine Ziffer direkt nach dem %-Zeichen bestimmt die Anzahl der genutzten Zeichen. Aus dem Vornamen „Frank" und Nachnamen „Carius" wird mit %1g%7s@msxfaq.de ein „fcarius@msxfaq.de". Damit die neuen Einstellungen aktiv werden, muss der Dienst zur Empfängeraktualisierung angetriggert werden. Die Abfrage hierzu erhalten Sie beim Abspeichern der geänderten Einstellungen.

Abbildung 8.20 RUS antriggern



Update SMTP-Adressen

Exchange 2003 übernimmt das Update nach der Bestätigung. In größeren Installationen kann solch eine Änderung mehrere Stunden dauern. Da zudem auch die E-Mail-Adressen der Server und anderer Systemelemente entsprechend angepasst werden, sind die Auswirkungen entsprechend umfangreich. Den Erfolg dieser Änderung sehen Sie bei den E-Mail-Adressen der Anwender erst etwas später.

8.3.3 Öffentliche Ordner-Rechte

Exchange 2003 bietet die gemeinsame Nutzung von Informationen in Öffentlichen Ordnern an. Allerdings konnte bei Exchange 2000 ohne entsprechende Konfiguration jeder Anwender selbst Ordner auf der obersten Ebene anlegen (TLF). Ohne Einschränkungen entstand nach kurzer Zeit eine planlose Ordner-Struktur. Sinnvoll ist eine Begrenzung der Anlage von Basisordnern im ESM für wenige Personen, und die Berechtigung für das Erstellen von Unterordnern kann an weitere Personen vergeben werden. Mit Exchange 2003 hat erstmals nur der Administrator das Recht, entsprechende „Top Level Foldern" anzulegen. Im Gegensatz zu den Unterordnern können die TLF-Rechte nur Exchange System-Manager konfiguriert werden.

Nun gehört es zu den Grundlagen eines sicheren Netzwerks, dass einfache Tätigkeiten nicht mit dem Administrator-Konto durchgeführt werden. Einer der nächsten Schritte ist daher die Delegierung der Berechtigung „CREATE TOP LEVEL PUBLIC FOLDER“.

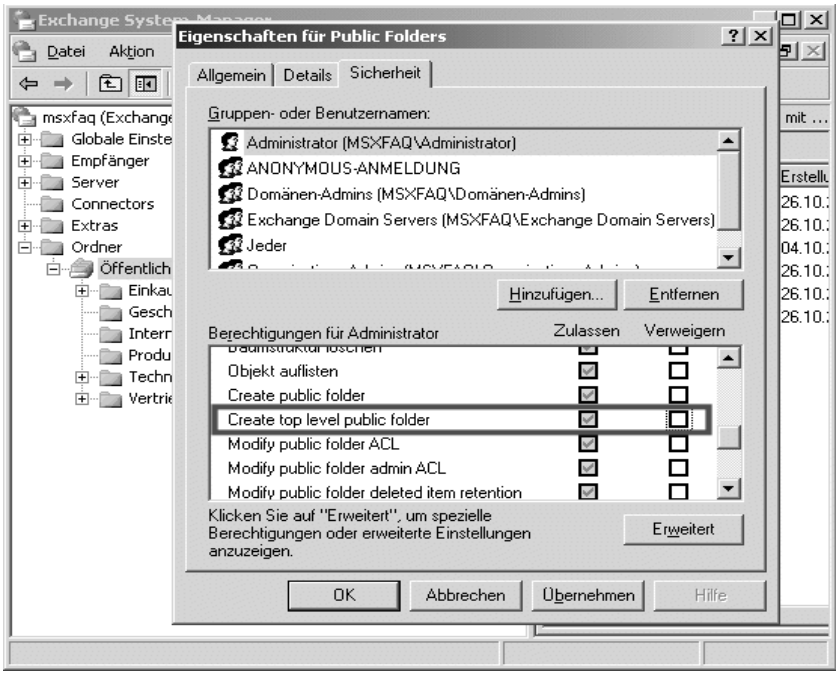


Abbildung 8.21 Rechte für Basisordner einstellen

Das Recht „CREATE TOP LEVEL PUBLIC FOLDER“ sollten Sie nur ausgewählten Personen oder besser noch einer Gruppe geben. Diese Mitarbeiter können dann selbstständig in Outlook entsprechende Ordner anlegen, ohne Domänen-Administrator oder Exchange-Administrator zu sein.

8.3.4 Datenbankpfade optimieren

Datenbank (*.edb und *.stm) auf andere Partition verschieben

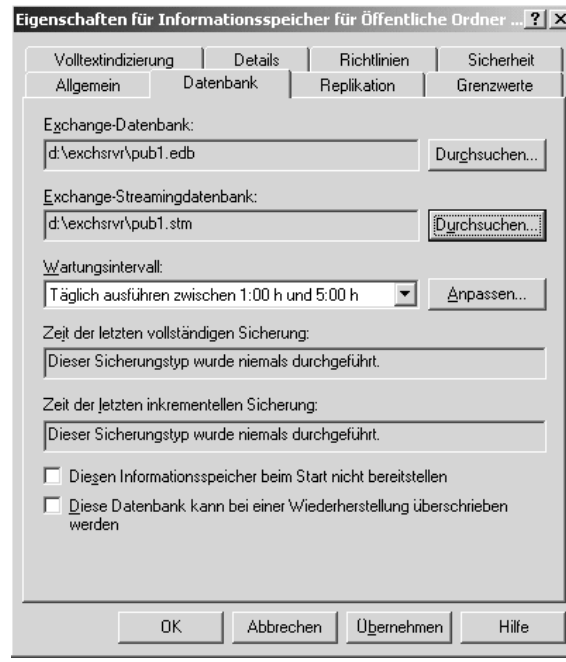
Bei der Installation von Exchange in der Musterumgebung wurde Exchange in die gleiche Partition wie das Betriebssystem installiert. Ohne weitere Anpassungen liegen nun auch die Exchange-Datenbanken und die SMTP-Warteschlange in dieser Partition. Sie sollten diese Pfade über den ESM verändern und die Inhalte verschieben. In der Musterinstallation wurde für die Exchange-Datenbanken und andere Nutzdaten eine eigene Partition D: vorgesehen, die bei der Windows-Installation bereits formatiert und mit einem Label versehen wurde.

Insgesamt sind vier Änderungen erforderlich, um die Datenbanken von der Systempartition auf die Datenpartition zu verschieben:

Verlagern der öffentlichen Ordner Datenbank

In den Eigenschaften des Informationsspeichers wird dazu der Pfad geändert, und Exchange verschiebt die Inhalte. Sie sollten immer beide Datenbanken – die EDB- und die STM-Datenbank – auf die dafür vorgesehene Partition verschieben, da diese direkt zusammengehören.

Abbildung 8.22 Speicherplatz für Public Folder verschieben



Der Exchange System-Manager beendet, verschiebt und startet die Datenbank selbstständig.

Verlagern der Postfachdatenbank

Die Verlagerung der Postfachdatenbank erfolgt in den Eigenschaften der Postfachdatenbank. Auch hier werden wieder die Exchange-Datenbank sowie die Exchange-Streamingdatenbank auf das Laufwerk D: verschoben. Ebenso beendet (dismount) der Exchange System-Manager die Datenbank, verschiebt sie selbstständig auf das andere Laufwerk und startet die Datenbank nach diesem Vorgang wieder.

Bitte beachten Sie, dass diese Aktion nicht im produktiven Betrieb durchgeführt werden sollte, da die Benutzer die Verbindung zur Datenbank verlieren.

In der Praxis wird für das D:-Laufwerk oft ein eigenes RAID-Array, bestehend aus RAID 1 oder RAID 5, eingesetzt, auf dem dann nur die Exchange-Datenbanken verschoben werden.

Abbildung 8.23 Speicherplatz der Postfachdatenbank ändern

Verlagern der Transaktionsprotokolle

Move Log-Files

Auch die Transaktionsprotokolle werden auf die zweite Partition verschoben. Dies ist im Hinblick auf die Verfügbarkeit und Performance zwar nicht optimal, aber immer noch besser, als wenn sehr viele Protokolldateien die Systempartition voll schreiben.

Beim Einsatz eines physikalischen Arrays für Laufwerk C: wird dieses oft in zwei Partitionen, C: für System und E: für Logfiles, aufgeteilt.

Die Einstellung erfolgt in den Eigenschaften der Speichergruppe.

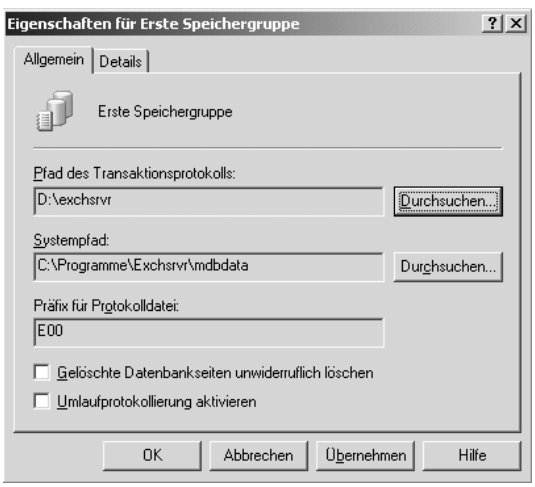


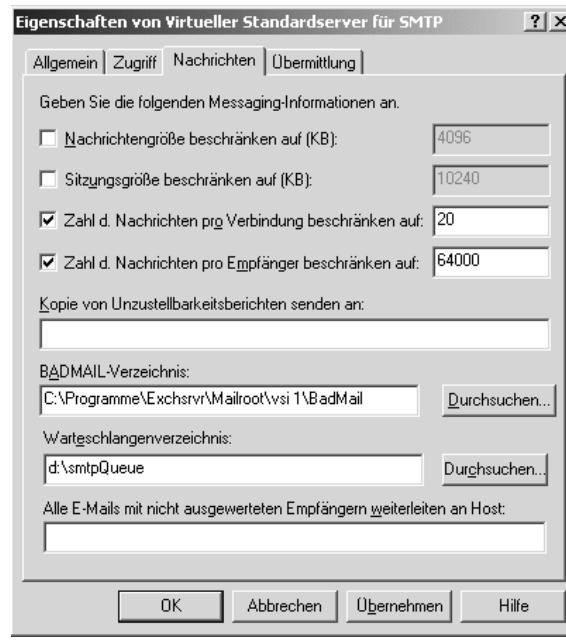
Abbildung 8.24 Pfad für Transaktionsprotokolle anpassen

Durch die Änderungen der Transaktionsprotokolle werden alle Datenbanken in der Speichergruppe kurz beendet und neu gestartet.

Verlagern der SMTP-Warteschlange

Um die Warteschlange des virtuellen SMTP-Servers zu verschieben, muss dieser zuerst beendet werden. In den Eigenschaften des virtuellen Servers kann dann unter Nachrichten der Pfad angepasst werden.

Abbildung 8.25 Pfad des SMTP-Queue-Verzeichnis verschieben



Diese Anpassung ist in Exchange 2003 möglich, da alle Nachrichten in diesem Verzeichnis temporär gespeichert werden und damit eine schnelle Festplatte in größeren Installationen sinnvoll ist. Mit Exchange 2000 war diese Änderung nur direkt über einen Eintrag in der Registrierung denkbar.

Logging schreibt Protokoll-Dateien

Damit sind die größten Datenbereiche von Exchange verschoben. Aber mit dem Einsatz von Exchange bekommen auch der Web- und der SMTP-Server mehr zu tun. Beide Server können ebenfalls ihre Aktivität protokollieren. Der SMTP-Server protokolliert in der Standardeinstellung keine Zugriffe. Sie können das Logging jedoch aktivieren und dabei den Pfad von der Systempartition auf die Datenpartition verlagern.

Der Internet Information Server hingegen protokolliert alle Zugriffe in das Verzeichnis „C:\Windows\system32\logfiles“. Diese Einstellung ist im Internet-Dienstmanager zu ändern, damit diese Protokolldateien nicht nach einiger Zeit die Systemfestplatte voll schreiben. Bei den heutigen Partitionsgrößen dauert dies im normalen Betrieb zwar einige Monate, allerdings könnte jemand durch massenhaft vorgetäuschte Seitenabrufe diese Dateien auch schneller wachsen lassen. Wichtig ist später auf jeden Fall eine

Überwachung des Servers, hier speziell der Festplattenkapazität, um nicht unerwartet vor einer gefüllten Festplatte zu stehen.

8.3.5 Grenzwerte und Systemrichtlinien

Der nächste Schritt sieht Einstellungen der im Konzept vorgesehenen Grenzwerte für Postfächer und Öffentliche Ordner vor.

Maximale interne Nachrichtengröße

Das wichtige Limit ist die Begrenzung der maximalen Nachrichtengröße auf dem Transportweg. Hier kann in Exchange sowohl auf dem Transportagent als auch auf dem Connector zum Internet ein Grenzwert eingestellt werden.

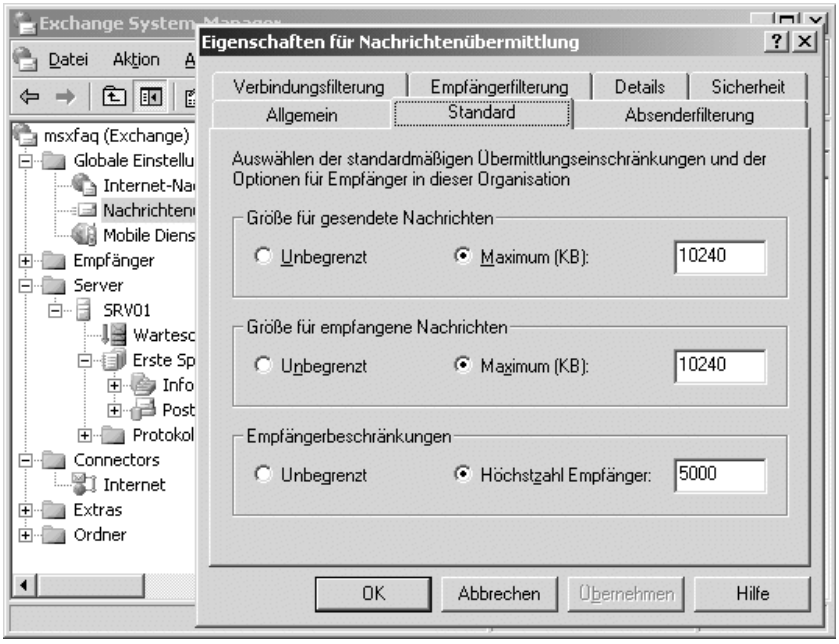


Abbildung 8.26 Globales Nachrichten-Limit

Für die Musterumgebung ist der Standardwert von 10240 KByte ausreichend. Grenzwerte für Connectoren sollten Sie ebenfalls einstellen.

Postfachrichtlinien

In der Musterinstallation werden für alle Anwender die folgenden Standardwerte definiert. Davon abweichend können später je Anwender andere Werte eingestellt werden:

Limit für Postfächer

- Warnen: 100 MByte

  Prüfen Sie, ob in Ihrer Umgebung diese Größe ausreichend ist. Beim Überschreiten dieser Grenze erhält der Anwender regelmäßig eine Nachricht, dass sein Postfach diese Grenze überschritten hat.

- Senden verbieten: 120 MByte

  Beim Erreichen dieser Grenze ist es dem Anwender nicht mehr möglich, Nachrichten über Exchange zu senden. Der Empfang von E-Mails ist weiterhin möglich.

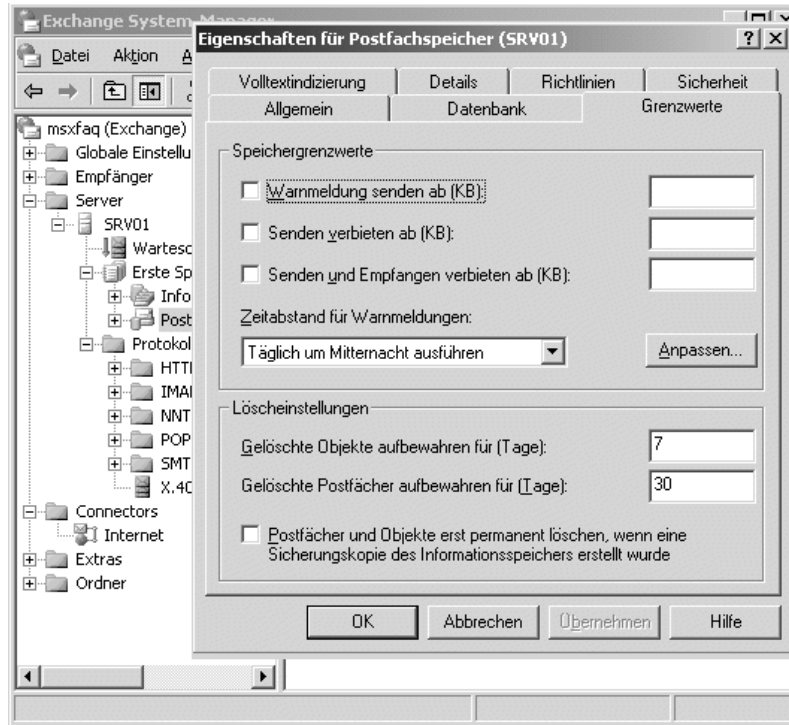
- Senden und Empfangen verbieten: 150 MByte

  Bei Erreichen dieser Grenze verweigert der Exchange-Server die Annahme weiterer Nachrichten. Der Absender wird hierüber informiert. Spätestens dann sollte der Anwender um eine höhere Grenze nachfragen oder alte Nachrichten löschen.

Der Anwender kann immer auf das Postfach zugreifen und alte Nachrichten löschen. Bestimmen Sie für Ihre Produktionsumgebung geeignete Grenzen.

Bei dieser Konfiguration sind gleich die Werte für die Haltezeit gelöschter Postfächer (30 Tage) und gelöschter Nachrichten (7 Tage) zu prüfen und gegebenenfalls anzupassen. Exchange 2000 hatte als Haltezeit für gelöschte Nachrichten noch 0 Tage vorgesehen. In unserer Musterumgebung stellen wir den Wert auf 30 Tage.

Abbildung 8.27 Limits auf dem Postfachspeicher



Es ist sinnvoll, nach einiger Zeit die aktuellen Größen der Postfächer auszuwerten und ggf. die Standardwerte anzuheben oder über die Archivierung von Nachrichten nachzudenken.

Grenzwerte für Öffentliche Ordner

Analog zu den globalen Postfacheinstellungen sind auf den Öffentlichen Ordnern entsprechende Parameter einstellbar.

Limit für Public Folder

- Warnmeldung

  Tragen Sie hier einen sinnvollen Standardwert ein, damit alle Ordner ohne explizite Definition nicht unbemerkt anwachsen können. Diese Grenze wird in der Musterumgebung auf 300 MB eingestellt.

- Bereitstellen

  Dieser Wert bestimmt, wie groß maximal eine Nachricht sein darf, die als E-Mail in diesen Ordner eingestellt wird. Aufgrund des globalen Limits von 10 MB sind nur kleinere Werte sinnvoll.

- Maximale Objektgröße

  Ein Anwender kann auch direkt ein Objekt im Öffentlichen Ordner ablegen. Hier ist die maximale Größe von 10240 KB in den meisten Fällen angemessen.

- Gelöschte Objekte

  Eventuell möchten Sie gelöschte Ordner-Objekte länger aufbewahren. Der Platz in der Datenbank wird dabei jedoch nicht sofort freigegeben. Beim Löschen der Information durch den Anwender erst einigen Wochen, ist der Speicherbedarf ebenfalls vorhanden. In unserer Musterumgebung setzen wir diesen Wert auf 30 Tage, damit Anwender problemlos gelöschte Elemente zurückholen können.

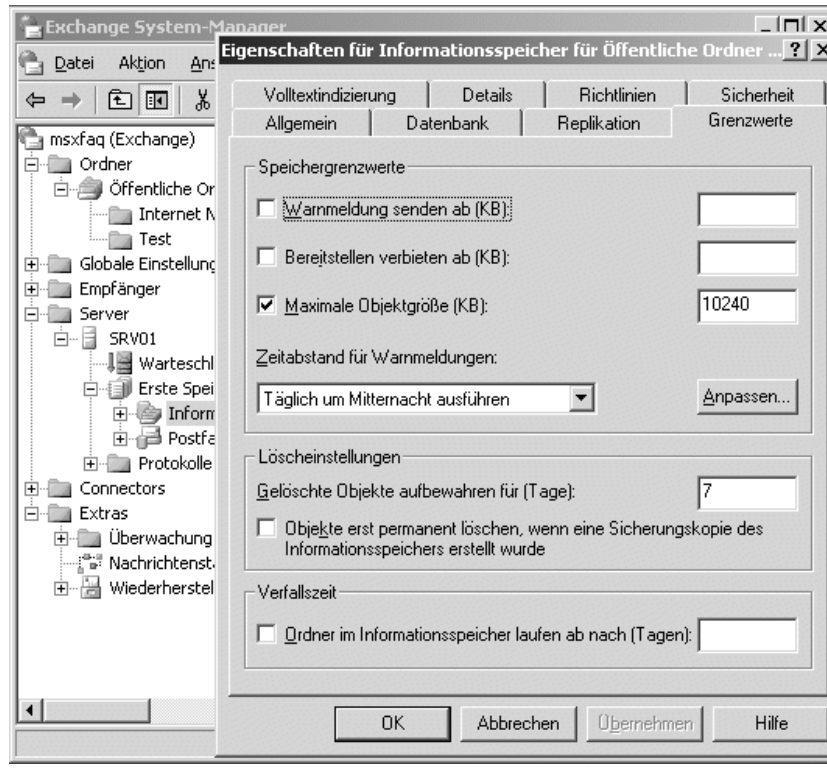


Abbildung 8.28 Grenzwerte auf dem Öffentlichen Ordner-Speicher

Vorsicht ist jedoch beim Eintragen einer Verfallszeit geboten. Nach Ablauf dieser Zeit im Speicher werden ältere Nachrichten unwiderruflich gelöscht. Diese globale Einstellung ist daher nur dann angebracht, wenn in allen Öffentlichen Ordnern Daten nur kurze Zeit gehalten werden müssen. Dies ist z.B. bei Newsservern der Fall. Sie können diese Einstellung später auch für entsprechende Ordner getrennt aktivieren.

Systemrichtlinien

Richtlinie zuordnen

In Unternehmen, die mehrere Postfachserver einsetzen, ist es mühselig, alle Grenzwerte manuell zu pflegen. Exchange bietet nun die Möglichkeit, Systemrichtlinien einzurichten. Der Systemrichtlinien-Container wird in der AG angelegt. Hier können Sie Richtlinien für Server, Öffentliche Ordner und Postfachspeicher definieren und entsprechend zuordnen.

Datenbank-Grenzwerte

Datenbank-Limit anpassen

Neu mit SP2 ist die individuelle Limitierung der Datenbankgröße. Beim Exchange Standard Server wird die Datenbank nach dem Update nicht größer als 18 Gigabyte, während beim Enterprise Server das Limit bei 8000 GB bestehen bleibt. Unter Verwendung eines Registrierungseintrags können Sie den Grenzwert des Standard Servers bis maximal 75 GB setzen. Beim

Enterprise Server können Sie mit dem gleichen Eintrag ein unkontrolliertes Wachstum hard begrenzen. Mittels einem geeigneten Monitoring sollten Sie die Größe der Datenbanken überwachen. Sie finden die Beschreibung zur Einstellung der Datenbankgrenzen bei der Installation des Service Packs.

8.3.6 Nachrichtenverfolgung

Message Tracking ist unverzichtbar!

Gerade am Anfang ist es wichtig, eine Diagnosemöglichkeit zu haben, wenn Nachrichten angeblich nicht ankommen. Exchange 2003 erlaubt eine Buchführung über jede übertragene Nachricht. So kann zweifelsfrei geklärt werden, wann ein Anwender eine Nachricht zum Versand eingeliefert hat und wann diese Nachricht die Exchange-Organisation verlassen hat oder intern zugestellt wurde.

Diese Protokollfunktion muss jedoch erst pro Server aktiviert werden. Im Exchange System-Manager werden bei den Eigenschaften des Servers die entsprechenden Einträge eingestellt.

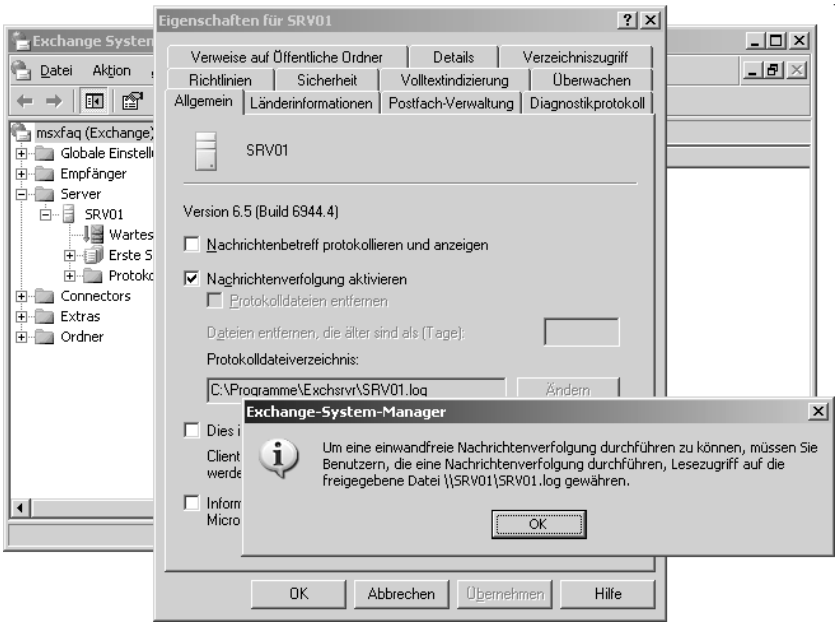


Abbildung 8.29 Nachrichten-Tracking aktivieren

Rechte auf Log-Files delegieren

Nun protokolliert Exchange 2003 die Übertragung der Nachrichten in einer täglich neu angelegten Textdatei mit. Im Gegensatz zu früheren Versionen ist die Freigabe „\\SRV01\SRV01.LOG“ mit den Protokollen jedoch nicht mehr für jedermann lesbar. Sie müssen dem Personenkreis zumindest Leserechte auf die Freigabe gewähren.

Im gleichen Fenster können Sie die Verfallszeit und den Pfad der Log-Dateien bestimmen.

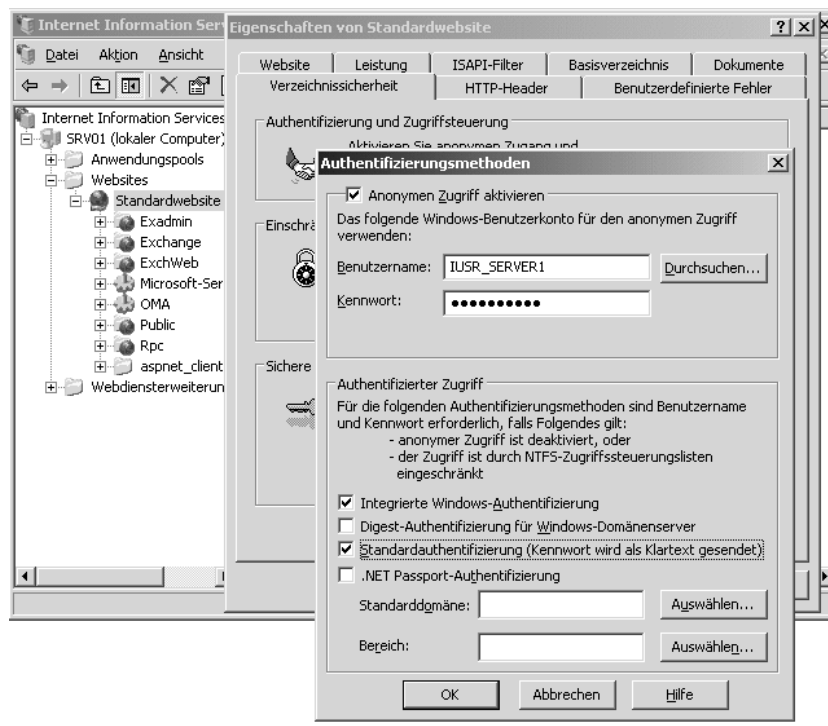
Die Auswertung der Log-Dateien erfolgt später im ESM über den NACHRICHTENSTATUS im Bereich „Extras“. Das Format der Protokolldateien ist sehr einfach dokumentiert, Sie können auch mit eigenen Anwendungen ausführlichere Analysen starten. Im Backoffice Resource Kit gibt es z.B. vorgefertigte RPT-Dateien für den Einsatz mit der *Crystal Reports Runtime*.

8.3.7 Outlook Web Access

Der Zugriff auf die Postfächer mit einem Webbrowser ist bei Exchange 2003 immer aktiviert. Der IIS ist für Exchange eine sehr wichtige Funktion, weil darüber nicht nur der Zugriff für Anwender auf ihr Postfach möglich ist, sondern auch der Exchange System-Manager die Öffentlichen Ordner verwaltet oder der Zugriff mobiler Geräte erfolgt. Sie können bei den Eigenschaften des Anwenders bei Bedarf die OWA-Nutzung deaktivieren.

Beim Zugriff auf OWA werden in den meisten Fällen die Kennwörter unverschlüsselt übertragen. Auch beim Zugriff mit dem Internet Explorer kann die NTLM-Authentifizierung nur genutzt werden, wenn kein Proxy-Server dazwischen die Daten umsetzt. Die meisten Browser nutzen die „Basic-Authentication“. Diese Autorisierung sollten Sie daher im IIS aktivieren.

Abbildung 8.30 Basic-Authentifizierung einschalten



Nun werden die Kennwörter aber unverschlüsselt übertragen. Daher ist es dringend notwendig, die Daten mittels SSL zu verschlüsseln. Über den Assistenten im Internetinformationsdienste-Manager muss eine entsprechende Zertifikatsanforderung erstellt werden. Der private Schlüssel verbleibt auf dem Server, während der öffentliche Schlüssel als „CER-Datei" zur Signierung an eine Zertifikatsstelle gesendet werden muss. Für den Einsatz im Internet sollten Sie eine offizielle Zertifikatsstelle beauftragen, die Ihnen diese Dienstleistung in Rechnung stellt. Wenn Sie sich später mit einem Browser verbinden, wird die Anmeldung ohne weitere Rückfragen erfolgen, da der Name des Rechners, die Gültigkeit und die ausstellende Zertifikatsstelle dem Browser schon bekannt ist.

Für den primären Einsatz der Verschlüsselung, ohne offizielles Zertifikat, können Sie auch die Zertifikatsstelle (CA) von Windows 2003 installieren und sich Ihre eigenen Zertifikate ausstellen. Im *Internet Information Server Resource Kit* gibt es zudem das Programm SELFSSL.EXE, mit dem Sie auch ein Selbstzertifikat ausstellen können.

Erfolgt später eine Verbindung aus dem Internet, erhält der Anwender allerdings eine Warnung, dass der Name und das Datum zwar gültig sind, aber die ausstellende CA nicht vertrauenswürdig ist.

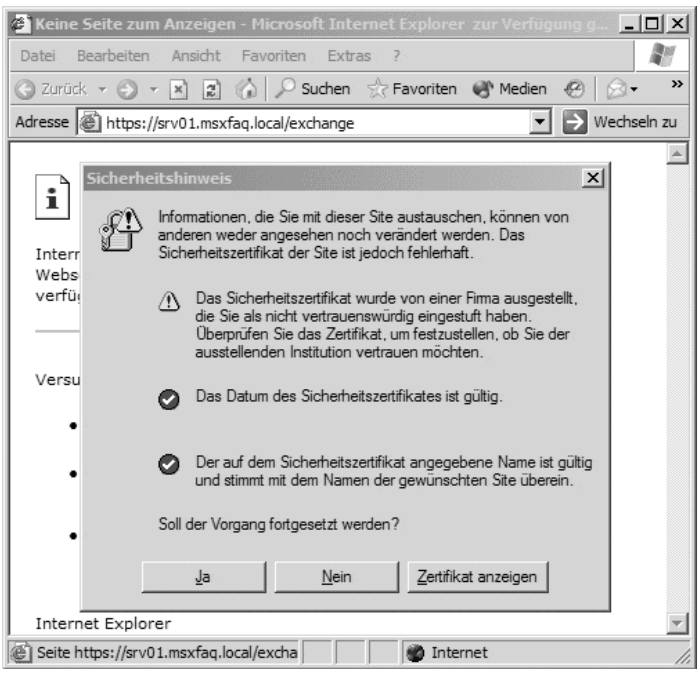


Abbildung 8.31 SSL mit nicht-vertrauens-würdigem Zertifikat

Wird diese Meldung bestätigt, ist die weitere Verbindung ebenso verschlüsselt wie mit einem offiziellen Zertifikat. Allerdings kann jeder ein solches Selbstzertifikat erstellen, und Sie können damit nicht sicher sein, dass

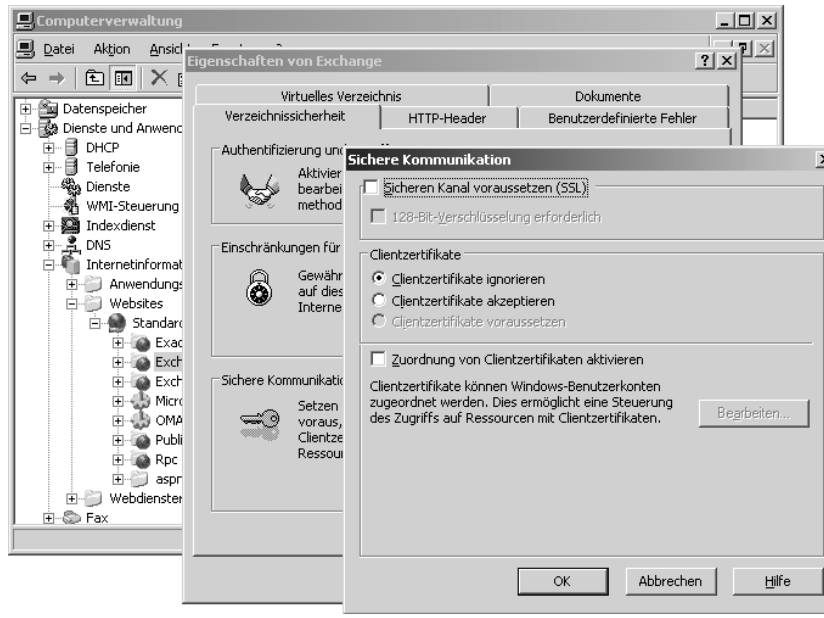
Sie beim Zugriff aus dem Internet wirklich auf dem richtigen Server gelandet sind.

Musterzertifikat begrenzt gültig

Für die Musterinstallation finden Sie auf der CD ein Musterzertifikat für den Server „srv01.msxfaq.local“. Nach dem Import können Sie alle weiteren Tests und Funktionen auch mit SSL durchführen, ohne in der Musterumgebung eine eigene Zertifikatsstelle installieren zu müssen. Achtung: Dieses Zertifikat ist nur begrenzt gültig.

Nach der Installation des Zertifikats muss auf den IIS-Verzeichnissen „/exchange“ und „/public“ die Verwendung von SSL aktiviert werden. Sie können zwar SSL erzwingen, allerdings dürfen Sie nicht diesen SSL-Zwang auf die ganze Webseite ausdehnen, da Sie sonst keine Öffentlichen Ordner mehr mit dem Exchange System-Manager administrieren können. Die Aktivierung von SSL erfolgt im IIS-Dienste-Manager.

Abbildung 8.32 SSL im IIS-Dienste-Manager aktivieren



Nur SSL-Zugriff erlaubt

Wenn SSL für den Zugriff verpflichtend vorgeschrieben ist, dann erhalten Benutzer, die ohne HTTPS auf den Server zugreifen wollen, die Fehlermeldung „*403.4 Forbidden: SSL is required*“. Dies kann elegant abgefangen werden, indem die entsprechende Fehlerseite des IIS durch eine eigene Seite ersetzt wird, die den Benutzer auf die SSL-Verbindung hinweist oder sofort weiterleitet. Eine entsprechende Seite könnte so aussehen:

```
<html>
<head>
<meta http-equiv="refresh" content="0;
URL=https://serv01.msxfaq.local/exchange">
```

```
<title> Startseite SSL Outlook Web Access</title>
</head>
<body>
Moment bitte ... Sie werden verbunden zu
https://serv01.msxfaq.local/exchange
</body>
</html>
```

Die Einstellung für diese Fehlerseiten können Sie im IIS-Manager konfigurieren.

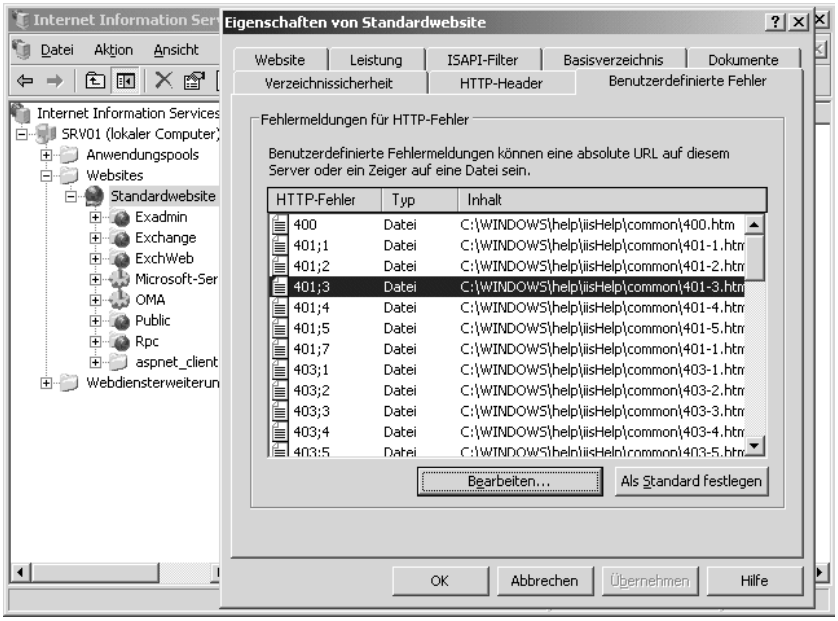


Abbildung 8.33 SSL-Fehlerseite umstellen

Über diesen Kniff können Sie auch bisherige Anwender auf SSL umstellen, die bislang immer nur http://servername/exchange eingegeben haben.

8.3.8 POP3 und IMAP4

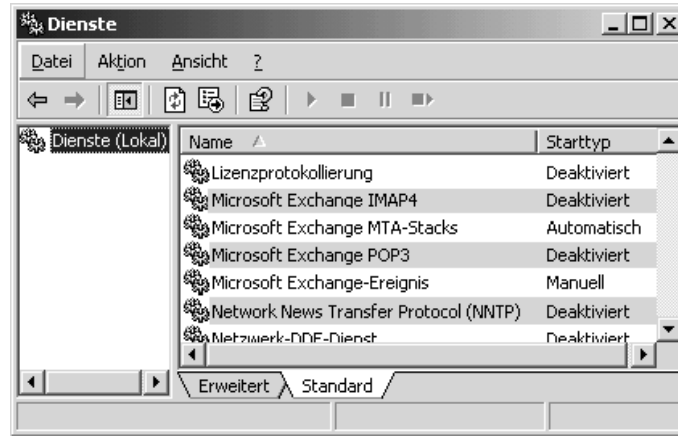
Dienste starten

Exchange 2003 unterstützt nicht nur den Outlook-Client und den Webzugriff über Outlook Web Access, sondern auch POP3 und das besser geeignete IMAP4 zur Kommunikation mit Clients. Über diesen Weg können Arbeitsplätze (z.B. Linux), die kein Outlook betreiben können, an Exchange 2003 angebunden werden.

POP3 wird oft bei einer Anbindung von Gateways zu anderen Diensten genutzt. So gibt es Faxserver, die Ihre Aufträge per POP3 von einem Exchange-Server abholen, oder Drucker, die ebenfalls per POP3 die Druckaufträge erhalten. Allerdings sind beide Dienste standardmäßig

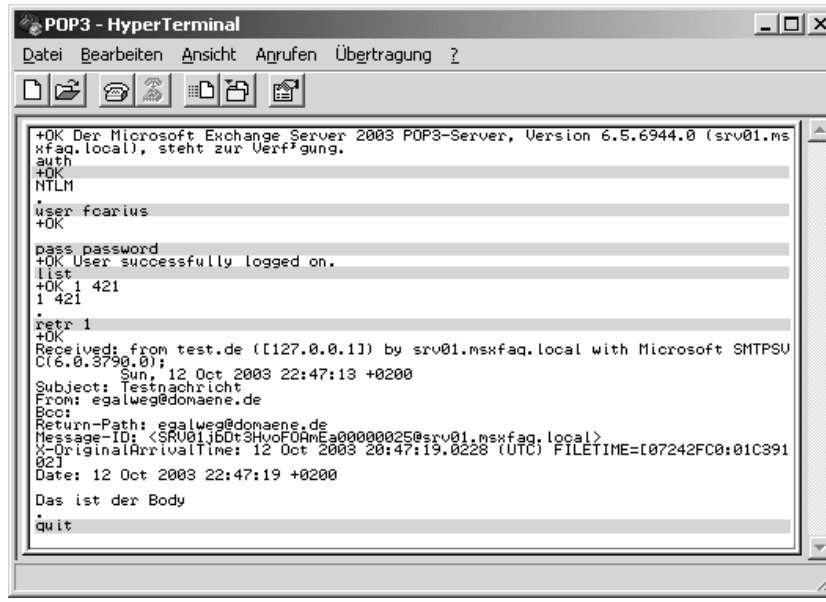
deaktiviert und müssen in der Systemsteuerung unter VERWALTUNG — DIENSTE erst gestartet werden.

Abbildung 8.34 POP3, IMAP4 und NNTP aktivieren



Mehr ist zur Einrichtung nicht zu tun, da ab sofort die Arbeitsstationen auf den Server zugreifen können. Voraussetzung ist, dass der Client über das Protokoll TCP/IP mit dem Server in Kontakt treten kann und der Server vom Client gefunden wird. Der Test der Funktion ist mit dem Programm HyperTerminal und einer Verbindung auf den Port 110 über TCP/IP möglich. Exchange muss mit einer Willkommensmeldung antworten.

Abbildung 8.35 POP3-Funktionstest mit HyperTerminal



Da sowohl bei POP3 als auch bei IMAP4 das Kennwort in Klartext übertragen wird, sollten Sie zumindest beim Zugriff aus dem Internet auch

hier den Einsatz von SSL erwägen. Dies müssen natürlich alle Anwendungen entsprechend unterstützen.

Der Zugriff auf den POP3-Server kann pro Anwender in den EXCHANGE-FEATURES deaktiviert werden. Im virtuellen POP3-Server ist ebenso eine Begrenzung auf bestimmte IP-Adressen oder Subnetze möglich. Hiervon sollten Sie auf jeden Fall Gebrauch machen, um den Zugriff nur auf besondere Arbeitsstationen zuzulassen. Die Gefahr, dass ein POP3-Client aus Unachtsamkeit das Postfach leert, ist doch sehr groß.

8.3.9 Outlook Mobile Access (OMA)

Die letzte Einstellung der Musterumgebung betrifft die Konfiguration des mobilen Zugriffs. Damit der Zugriff von mobilen Geräten überhaupt möglich ist, muss dieser aktiviert werden. Dies erfolgt im Exchange System-Manager unter „GLOBALE EINSTELLUNGEN – MOBILE DIENSTE“.

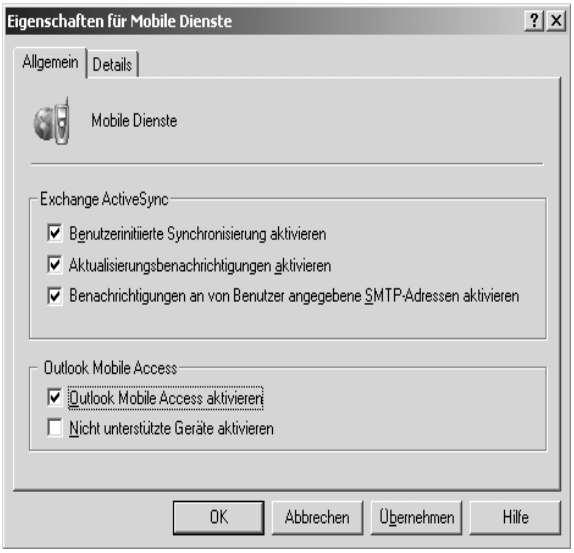


Abbildung 8.36 Aktivierung von Mobile Access

Outlook-Daten auf Handy und PDA

Der Zugriff über ActiveSync ist standardmäßig aktiv, während der Zugriff per WAP und anderen mobilen Geräten erst aktiviert werden muss. Anhand der Anfragen des Clients erkennt Exchange, um welches Endgerät es sich handelt, und passt die Oberfläche entsprechend an. Aktivieren Sie die Nutzung durch nicht unterstützte Geräte, können Geräte, die nicht in der ASP.NET Device-Datenbank hinterlegt sind, auf den OMA-Dienst zugreifen. Allerdings steht dann nur eine beschränkte generische Funktionalität zur Verfügung.

Nach diesen Einstellungen können die Anwender per WAP oder PocketPC mit dem Exchange-Server in Kontakt treten. Der Zugriff über WAP erfordert

allerdings die Möglichkeit der Funktelefone, eine IP-Verbindung zum Server aufzubauen. Dies ist kein Problem, wenn Ihr Exchange-Server aus dem Internet erreichbar ist. Zu Testzwecken reicht aber auch ein WAP-Emulator auf einem PC. Auch der Internet Explorer 6 kann WML-Seiten anzeigen. Der Zugriff erfolgt über die URL „`http://<servername>/OMA`".

Die Möglichkeit, mit mobilen Endgeräten auf Exchange zuzugreifen, gab es bereits unter Exchange 2000 und Exchange 5.5. Dazu musste das Standalone-Produkt „*Mobile Information Server*" lizenziert und installiert werden. Diese Funktion ist mittlerweile in Exchange 2003 integriert. Der Zugriff auf ein Postfach eines Exchange 2000- oder Exchange 5.5-Servers über einen installierten Exchange 2003-Server ist jedoch nicht möglich.

8.4 Datensicherung

Der nächste Schritt nach der Installation des Exchange-Servers ist die Einrichtung einer Datensicherung. Wie in den Konzepten schon erläutert, gibt es mehrere Möglichkeiten, einen Exchange-Server zu sichern.

Der beste Weg einer Sicherung ist die „Online-Backup" der Exchange-Datenbanken und aller sonstigen relevanten Informationen. Dies bedeutet, dass neben den Datenbanken natürlich auch das Betriebssystem, das Active Directory und die Einstellungen in der Registrierung, der Metadatenbank des IIS und SMTP-Servers sowie die entsprechenden Programmdateien zu sichern sind.

Online-Sicherung mit Ntbackup vs. 3rd-Party-Produkte

Mit der Installation von Exchange 2003 wird das Backup-Programm von Windows 2003 aktualisiert, so dass auch eine Sicherung von Exchange möglich ist. Das mitgelieferte *Ntbackup* ist für die Sicherung von Exchange und Windows 2003 vollkommen ausreichend.

Dies bedeutet aber nicht, dass damit alle kommerziellen Programme überflüssig wären. Oftmals ist die Sicherung von Exchange bei diesen Lösungen jedoch eine kostenpflichtige Zusatzoption. Sie sollten beim Einsatz anderer Sicherungsprodukte aber keinesfalls auf die Vorteile dieser Option verzichten oder gar einer „*Open File Option*" die Aufgabe der Sicherung Ihres Exchange-Servers überlassen.

Bis zur Installation einer alternativen Sicherungssoftware können Sie manuell mit Ntbackup sowohl den Windows 2003-Server als auch die Exchange-Datenbanken sichern. Wenn Sie neben Exchange 2003 auch die Exchange 5.5-Verwaltungswerkzeuge mit installiert haben, dann zeigt Ntbackup allerdings zwei Exchange-Einträge an. Ntbackup kann sowohl Exchange 5.5- als auch Exchange 2000- und Exchange 2003-Server sichern.

Allerdings befindet sich nur unter „MICROSOFT EXCHANGE SERVER“ die Speichergruppe mit Ihren Datenbanken.

Bei der Musterumgebung werden neben beiden Partitionen auch der Systemstatus und die Exchange-Informationsspeicher gesichert.

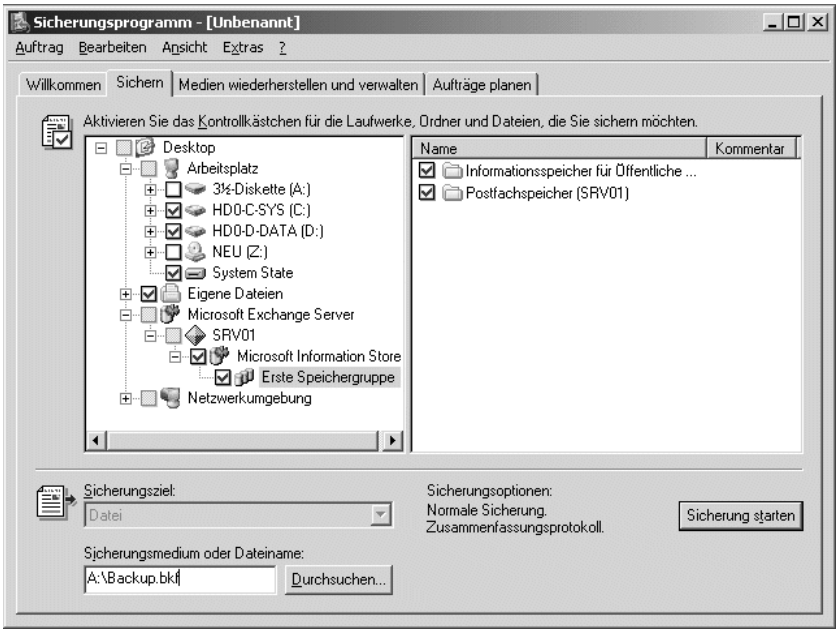


Abbildung 8.37 Ntbackup-Auswahl der Quellen

Wichtig ist auf jeden Fall die regelmäßige Sicherung, damit die Transaktionsprotokolle gelöscht werden. Nebenbei überprüft eine Online-Sicherung über die Prüfsumme die Konsistenz der Datenbank, deren Bedeutung Sie nicht unterschätzen sollten.

8.5 Virenschutz

Für den Betrieb eines Exchange-Servers ist ein Schutz gegen Viren notwendig. Diese Software sollte schon vor der Einrichtung der ersten Anwender und dem Empfang der ersten Nachrichten durchgeführt werden. Jetzt ist der richtige Zeitpunkt, eine solche Software zu installieren.

Virenscanner für Produktivbetrieb erforderlich

Im Konzeptteil sind die verschiedenen Möglichkeiten zur Installation eines Virenscanners erläutert. Sehr viele Firmen bieten ihre Virenscanner als Testversion für 30 oder mehr Tage an, die später nur durch einen Lizenzschlüssel freigeschaltet werden. Wenn Sie schon ein Produkt ausgewählt, aber noch nicht gekauft oder erhalten haben, sollten Sie prüfen, ob Sie die Testversion installieren und später einfach die Lizenz einspielen können. Ohne Virenscanner sollten Sie keine Systeme produktiv betreiben.

8.6 Überwachung und Monitoring

Probleme erkennen und beheben

In diesem Kapitel wurde der Windows 2003-Server um die Funktionen Exchange 2003, Datensicherung und Virenscanner erweitert. Für den stabilen und zuverlässigen Betrieb des Servers ist es unerlässlich, bestimmte Systemparameter zu überwachen und langfristig aufzuzeichnen. Einige dieser Überwachungen können automatisiert werden, andere erfordern eine regelmäßige manuelle Kontrolle. Die nachfolgend genannten Tools geben Ihnen einen guten Überblick, um auch Ihre Exchange-Umgebung optimal zu überwachen, und schnellstmöglich bei Problemen reagieren zu können.

8.6.1 Eventlog

Sie sollten es sich zur Gewohnheit machen, regelmäßig das Ereignisprotokoll der Server zu kontrollieren. Nahezu alle Programme melden dort zumindest schwerwiegende Fehler. Mit entsprechenden Hilfsprogrammen ist es sogar möglich, diese Überwachung zu automatisieren und Fehler weiter zu melden. Entsprechende Beispielskripte sind bei Microsoft im *Scripting Center* (http://www.microsoft.com/technet/scriptcenter/default.asp) verfügbar, um das Eventlog über WMI auszulesen und Aktionen zu starten. Andere kostenfreie Tools wie NTSYSLOG (http://www.msexchangefaq.de/Produkte/ntsyslog.htm) erlauben es, Meldungen an andere Systeme zu übermitteln oder einzusammeln. Dabei sollte diese Überwachung auch unabhängig von der Funktion des Exchange 2003-Servers arbeiten, damit ein Ausfall oder Defekt auch gemeldet wird, wenn Exchange auf ein Problem gestoßen ist.

Sie können auch kommerzielle Produkte wie den *Microsoft Operation Manager* (MOM) nutzen, die sehr umfangreiche Auswertungen und Regeln mitliefern. Exchange 2003 bringt das entsprechende Management Pack bereits mit.

8.6.2 Performance-Monitor

Trendanalyse mittels Perfmon

Für die Analyse von Trends bei der Nutzung des Servers sind die Performance-Counter von Windows 2003 sehr aufschlussreich. Für nahezu jeden Dienst und Prozess gibt es entsprechende Zähler, die genaue Informationen zu dessen Verwendung und Belastung aufzeigen. Ohne gesonderte Konfiguration zeigt der Windows Performance Monitor jedoch nur Momentanwerte. Der Performance-Monitor (Perfmon) kann auch dazu eingesetzt werden, von bestimmten Werten regelmäßig einen Schnappschuss in eine Datenbank zu schreiben. Dies erlaubt eine langfristige Auswertung, z.B. der Abnahme der freien Festplattenkapazität oder die Anzahl der

übertragenen Nachrichten. Zusätzlich erlaubt die Leistungsmessung auch den Start beliebiger Programme, wenn bestimmte Grenzwerte über- oder unterschritten werden. Damit ist die Leistungsüberwachung eine von Exchange unabhängige Instanz zur Überwachung des Servers.

Das folgende Bild zeigt die aktivierte Überwachung von CPU-Belastung und Hauptspeicher.

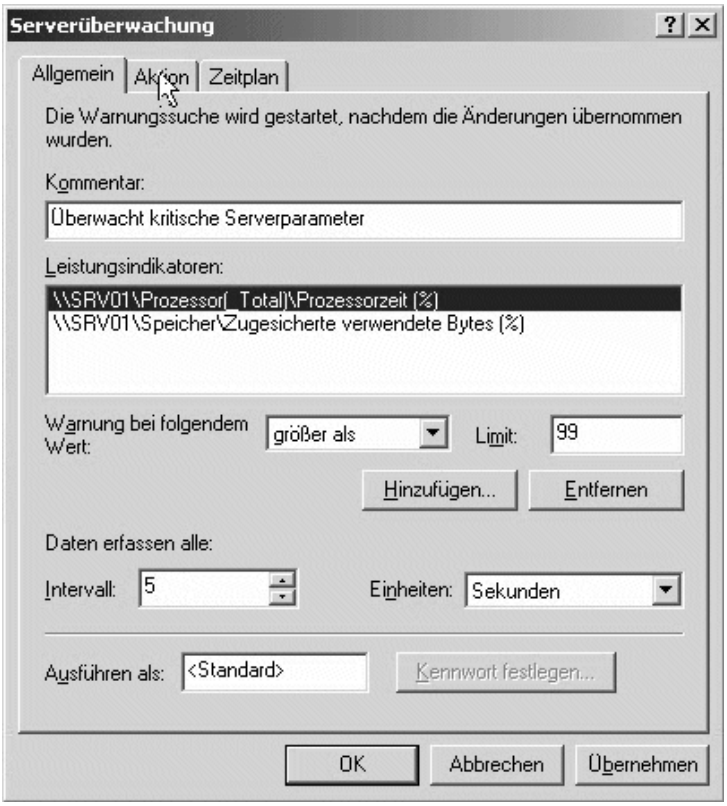
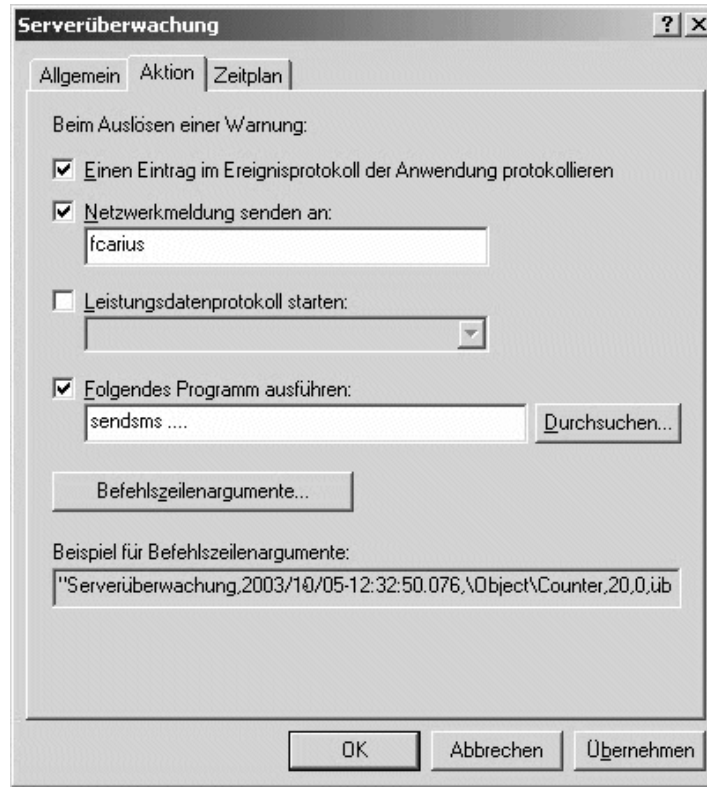


Abbildung 8.38 Überwachung von CPU und Speicher

In der Karteikarte „Aktion“ können Sie entsprechende Befehle wie SENDMSM anstoßen, wenn die Warnschwellen erreicht sind.

Abbildung 8.39 Aktionen bei Alarmen



Im Beispiel wird eine Netzwerkmeldung gesendet, wenn die CPU-Belastung über 99 % angestiegen ist. Ist der Benutzer jedoch nicht angemeldet, dann geht die Windows-Meldung verloren. Über ein Skript könnte zusätzlich z.B. eine E-Mail gesendet, ein Anruf auf einem Telefon über ein angeschlossenes Modem sowie eine SMS abgesetzt werden.

Eine weitere Funktion des Performance-Monitors ist die Langzeitüberwachung bestimmter Parameter des Servers. Windows 2003 liefert eine Standardeinstellung mit, die bestimmte Parameter alle 15 Minuten in eine Datei schreibt. Diese Protokollierung ist nicht änderbar und wird nicht automatisch gestartet.

Sie können eigene Überwachungsprotokolle anlegen, die Ihrer Meinung nach für das System wichtige Parameter regelmäßig aufzeichnen. Eine Auswertung der Daten ist später mit Perfmon auch nach einem Absturz des Servers möglich. Für die Testumgebung wird keine Überwachung aktiviert.

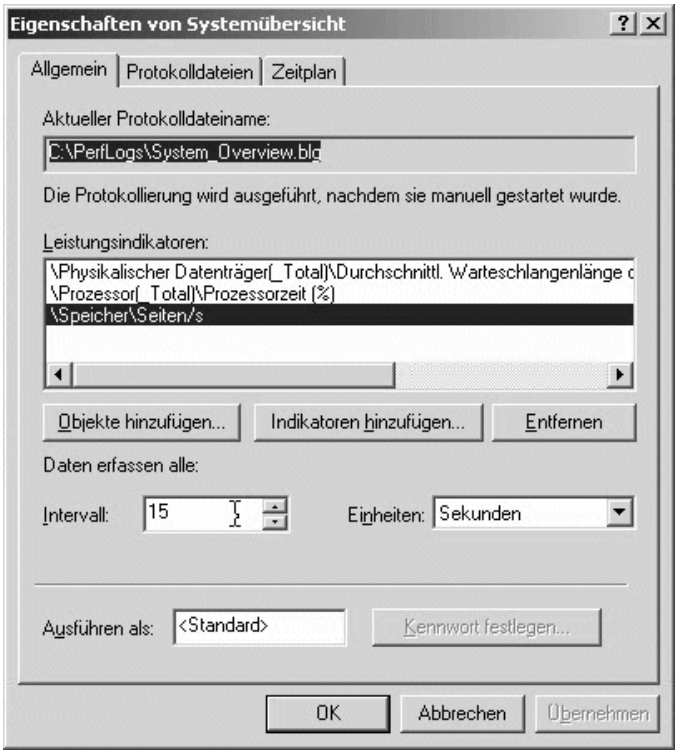


Abbildung 8.40 Langzeitprotokolle mit Perfmon

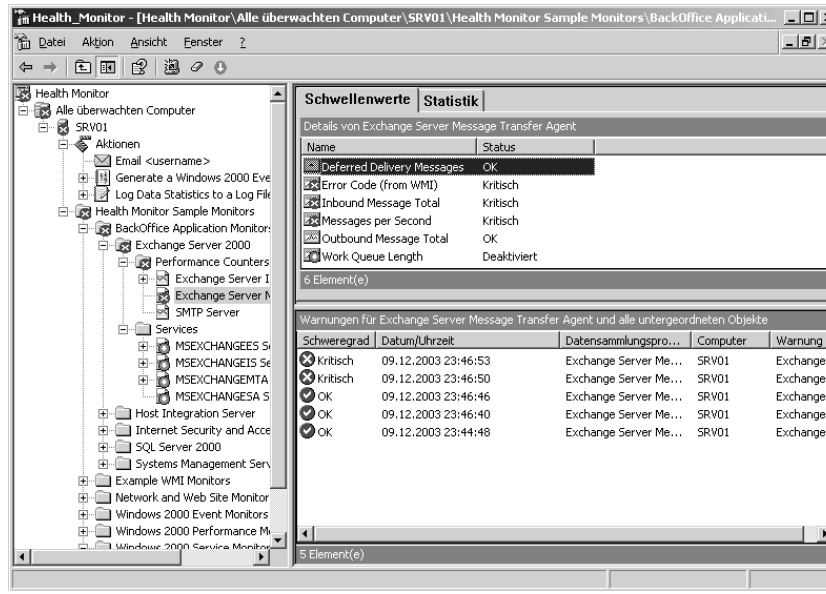
Natürlich ersetzt der Performance-Monitor weder den Microsoft Operation Manager noch andere kommerzielle Überwachungsprogramme, aber es ist ein Einstieg zur Fehlersuche und Trendanalyse. Interessante Werte sind hierbei immer die freie Festplattenkapazität, der Speicherbedarf, die Netzwerkauslastung und die CPU-Belastung.

8.6.3 Healthmon

Einen Vorteil haben die Firmen, die den Small Business Server nutzen. Auf der CD 3 des Small Business Servers 2003 ist der *Microsoft Healthmon 2.1* enthalten.

Ein entsprechender Agent kann den lokalen Server und andere Systeme im Netzwerk überwachen und statistische Daten aufzeichnen, Schwellenwerte prüfen und Alarme versenden.

Abbildung 8.41 Healthmon im Einsatz



Leider ist der Healthmon nicht im normalen Windows-Server-Paket enthalten, sondern nur im Rahmen des Small Business Servers, SMS 2.0 oder dem Windows Application Center Server.

8.6.4 Windows Update

Für die Aktualisierung des Betriebssystems kann der *Windows Update-Dienst* regelmäßig den Server überprüfen und notwendige Updates herunterladen. Die wenigsten Administratoren werden jedoch gestatten, dass der Dienst selbstständig die Updates installiert und gegebenenfalls den Server neu startet. Windows Update erkennt leider keine fehlenden Exchange 2003-Aktualisierungen. Sie müssen als Administrator regelmäßig auf dem Server nachschauen, ob über Windows Update neue Updates für MS-Produkte zur Installation bereitstehen. Leider gibt es noch keine einfache Möglichkeit, dies über Performance-Counter oder Eventlog-Meldungen zu erkennen.

Sobald mehrere Server und Arbeitsstationen im Netzwerk sind, sollten Sie über die Einführung des *Windows Software Update Service* (WSUS) oder eine kommerzielle Patch-Management-Lösung nachdenken.

8.6.5 Exchange-Überwachung

Exchange 2003 bietet selbst ebenfalls eine Überwachung der Funktion an. Im Exchange System-Manager sind die Ergebnisse der Überwachung sichtbar und eigene Anpassungen möglich. Exchange 2003 überwacht die

Standarddienste und Connectoren und zeigt Ausfälle und Fehler im System-Manager an. Unter dem Punkt EXTRAS – ÜBERWACHUNG UND STATUS sind die beiden Bereiche STATUS und BENACHRICHTIGUNG erreichbar.

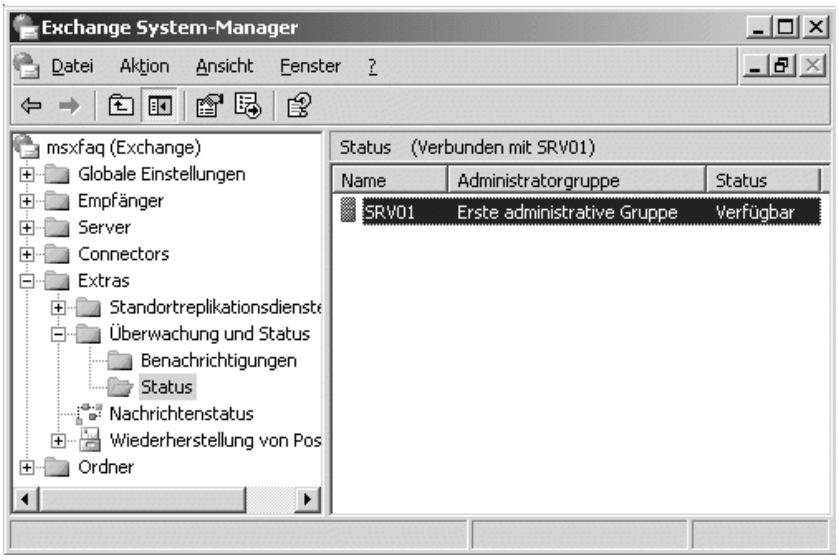


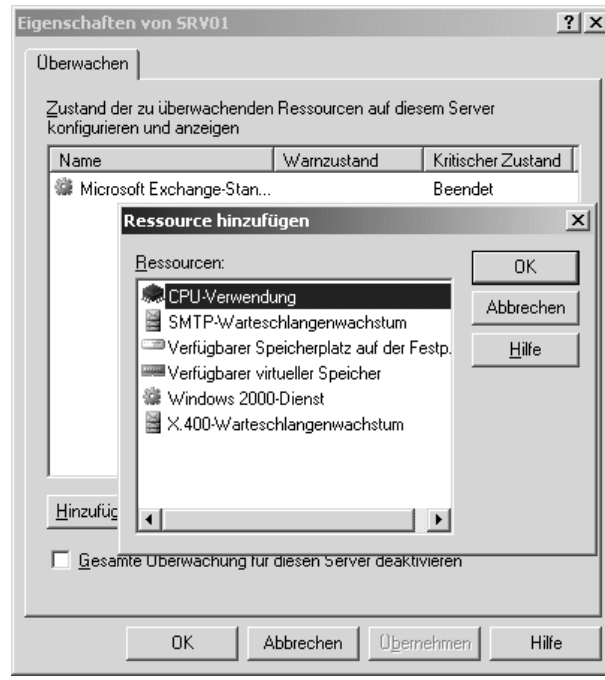
Abbildung 8.42 Statusanzeige der Exchange-Server

Je Server kann definiert werden, welche Dienste und Komponenten überwacht werden sollen und bei welchen Änderungen der Status auf „Kritisch“ oder „Warnung“ gesetzt werden soll.

Allerdings können diese Funktionen nur Exchange-Server überwachen. Andere Server im Active Directory, die keine Exchange-Server sind, können nicht mit überwacht werden.

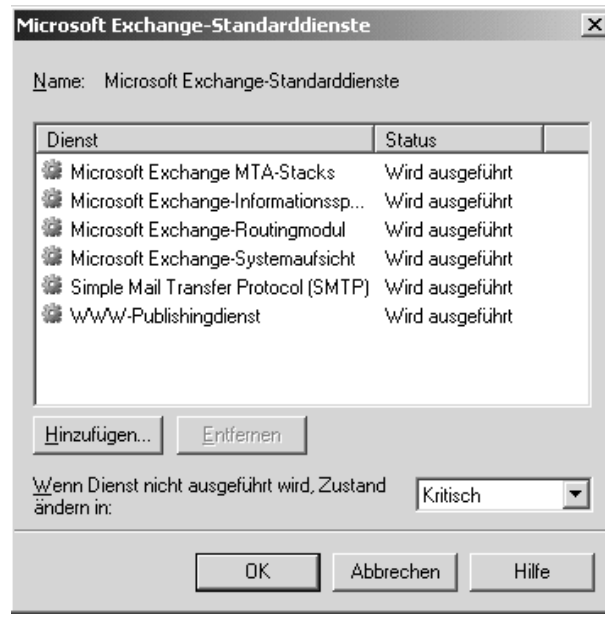
Neben den eigentlichen Exchange-Standarddiensten wie der Informationsspeicher, das SMTP-Protokoll und die Systemaufsicht, kann hier auch die Überwachung der Warteschlangen und der virtuelle Speicher sowie auch der Ressourcen wie CPU und Festplatte hinzugefügt werden.

Abbildung 8.43 Ressourcen zur Überwachung addieren



Die Standardeinstellung überwacht die Dienste des Servers und setzt den Status auf kritisch, sobald einer der Dienste nicht mehr gestartet ist.

Abbildung 8.44 Überwachte Dienste im Detail



Die Exchange 2003-Systemaufsicht (SA) kann aber auch jeden anderen Dienst auf diesem Server überwachen. Um auch über Ausfälle oder Probleme

informiert zu werden, erlaubt die Exchange 2003-Systemüberwachung die Definition von E-Mail- und Skriptbenachrichtigungen. Bei E-Mail-Benachrichtigungen wird eine entsprechend formatierbare Nachricht an ein Postfach gesendet, das sich natürlich nicht auf dem überwachten Exchange-Server befinden sollte.

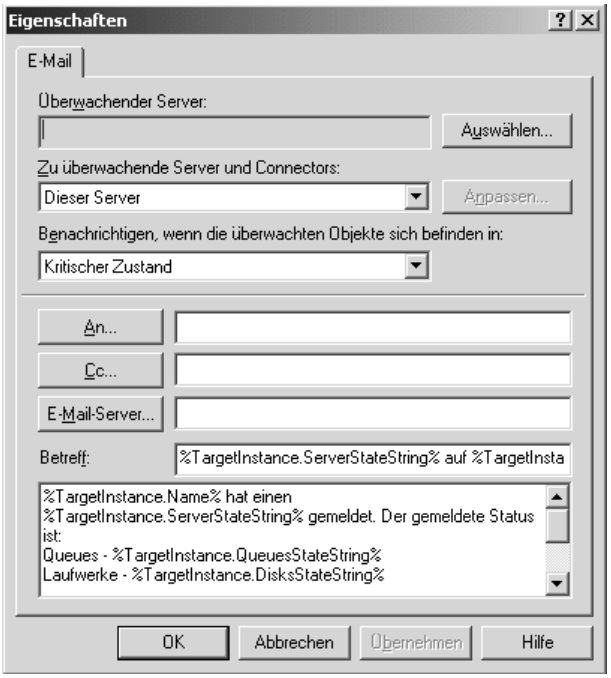


Abbildung 8.45 Einstellen der Benachrichtigung

Zusätzlich sind über die Skriptbenachrichtigung beliebige Programme ausführbar, die sonstige Prozesse in Gang setzen. In der Musterinstallation wird diese Funktion nicht eingesetzt.

8.6.6 Exchange Best Practice Analyzer

Health Check und Problemdiagnose

Seit September 2004 stellt Microsoft Ihnen ein neues Tool zur Verfügung: *Exchange Server Best Practice Analyzer* (ExBPA). Der ExBPA führt einen so genannten „Gesundheitscheck“ Ihres Servers durch und prüft die Systemkonfiguration. ExBPA ist über die kurze URL www.exbpa.com zum Download verfügbar. Es sammelt alle Daten der Konfiguration jedes Servers in der Exchange-Struktur und analysiert diese. Unter anderem werden die Werte und Konfigurationen aus dem Active Directory, der Registry, der Metabase und die Leistungsindikatoren (Performancecounter) berücksichtigt. Als Ergebnis erhalten Sie eine detaillierte Auflistung aller kritischen Konfigurationen, potenzieller Problemen und Einstellungen, die nicht der Standardkonfiguration entsprechen. Zusätzlich wird Ihnen zu jedem Punkt

eine Empfehlung angezeigt, wie Sie das Problem beheben können. ExBPA hilft Ihnen dabei, die häufigsten Konfigurationsfehler und Unstimmigkeiten zu erkennen und darauf angemessen zu reagieren. Dies kommt letztlich auch der Funktionssicherheit und Verfügbarkeit für Exchange zugute.

Positive Erfahrungen

Unsere Erfahrung mit ExBPA hat gezeigt, dass dieses Tool mittlerweile besonders in großen Exchange-Umgebungen unverzichtbar ist. Über eine automatische Updatefunktion bezieht ExBPA von Microsoft bei jedem Start eine aktuelle Datenbank, die den neuesten Wissensstand des Exchange Support Teams enthält. Laut Microsoft gehen mittels ExBPA die Supportanfragen für Standardprobleme zurück.

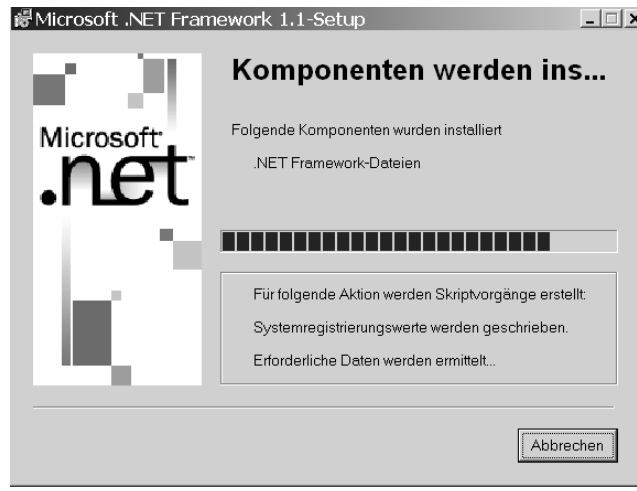
.NET-Framework

Die Installation des ExBPA auf einer Workstation setzt Microsoft .NET 1.1 voraus (http://www.microsoft.com/germany/ms/entwicklerprodukte/). Sie benötigen die .NET-Version für alle Programme, die auf Basis des .NET-Framework geschrieben wurden. Beachten Sie jedoch, in welcher Sprache Sie .NET installieren und welche Plattformen unterstützt werden.

„Best Practice Analyser“ wird ständig von MS aktualisiert

Nach dem Download von www.exbpa.com müssen Sie die EXE-Datei starten, um das darin erhaltene MSI-Paket zu entpacken. Dieses rufen Sie dann für die eigentliche Installation auf. Sie können das Tool sowohl auf dem Server als auch auf einer Workstation installieren. Erst dann haben Sie im Startmenü den Eintrag "Microsoft Exchange - Best Practice Analyzer Tool". Eventuell wird ExBPA Sie direkt auf ein Update hinweisen. Dazu prüft das Tool bei Microsoft nach, ob die installiert Version des Programms und die „Best Practice“-Datenbank aktuell sind. Diesen Prozess sollten Sie nach einiger Zeit wiederholen, um sicherzustellen, dass Ihr Exchange-System immer auf dem neuesten Stand ist. Ein Update des ExBPA finden Sie auch unter dem Link „Web Update Pack“ auf www.exbpa.com, die auch weitere Informationen über das Tool enthält.

Abbildung 8.46 Microsoft .NET für ExBPA



Auf einem Windows 2003 Server sind die .NET-Komponenten bereits vorinstalliert, sodass Sie direkt mit der Installation des ExBPA fortfahren können. Auf Windows 2000 und Windows XP müssen Sie das .NET Framework erst installieren.

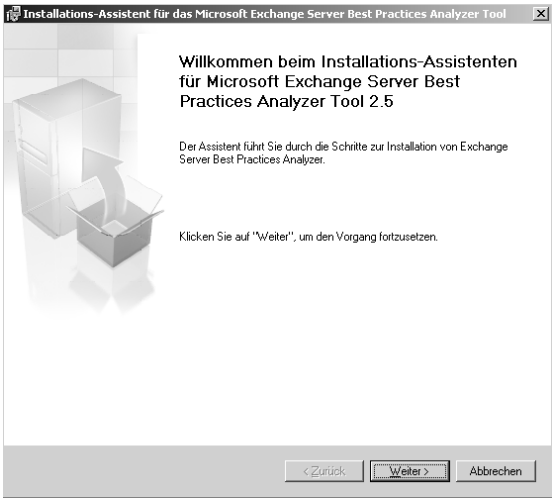


Abbildung 8.47 Installation ExBPA

Nach dem Start beginnt der Analyser sofort mit der Prüfung auf ein neues „Best Practice"-Update, das gegebenenfalls ein Neustart des Tools erfordert.

ExBPAUpdate.exe

Sofern Ihr Server keine Verbindung zum Internet aufbauen kann, müssen Sie auf einem anderen System das Web Update Pack herunterladen und in das Programmverzeichnis extrahieren (ExBPA.Config.xml und ExBPA.chm).

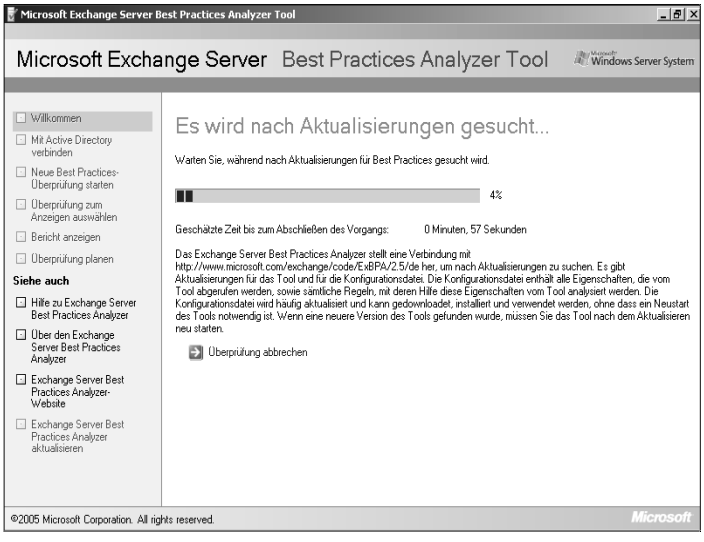


Abbildung 8.48 Auf Update prüfen

Gleichzeitig mit der Konfiguration wird beim Update auch die Hilfedatei erneuert. Diese beschreibt nicht nur die Anwendung des ExBPA, sondern

Hilfe beachten

enthält auch wertvolle Informationen über die zu prüfenden Daten, das Lesen des Berichtes und wie Sie bei der Fehlerbehebung vorgehen.

„New-Scan„ nach Update

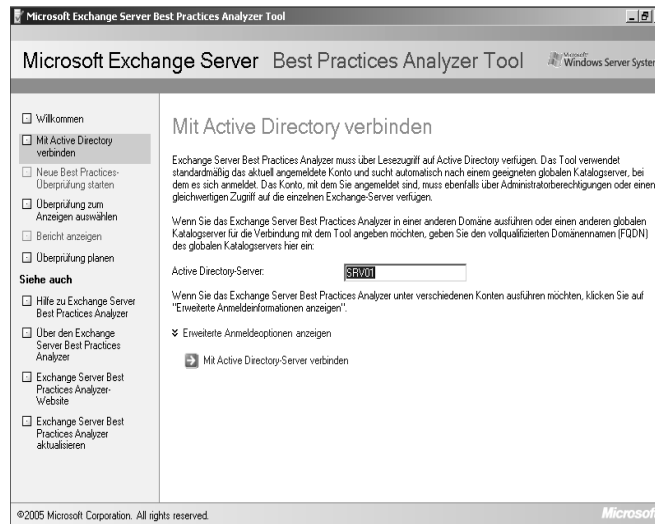
Für ExBPA gibt es immer wieder aktualisierte Know-How-Datenbanken. Beachten Sie, dass Sie bei der Auswertung einer früher aufgezeichneten Installation mit einer neueren Datenbank nur die Fehler finden, die auch mit der damals genutzten Datenbank schon aufgezeichnet wurden. Im Zweifelsfalle sollten Sie nach der Installation eines Updates Ihre Organisation neu analysieren. In der Regel ist die englische Version aktueller, daher sollten Sie diese bei akuten Problemen vorziehen.

8.6.6.1 Exchange-Überprüfung starten

Berechtigung zum Auslesen der Daten

Der erste Dialog nach dem Starten des ExBPA erwartet die Verbindung mit dem Aktive Directory. Hier wird ein Servername angezeigt oder Sie entscheiden sich für einen anderen Server und geben hier den Full Qualified Domain Name (FQDN) des Servers ein. Für die Verbindung mit dem AD benötigen Sie die Rechte eines Domänenbenutzers aller Domänen des Forest sowie die Exchange-Administrator-Rechte „Nur Ansicht“. Unter den erweiterten Anmeldeoptionen können Sie diese Benutzer angeben, ohne sich speziell mit einem Administratorkonto zum Starten des Tools anzumelden. Es ist zu empfehlen, generell nicht mit einem Administratorkonto zu arbeiten, sondern nur im Bedarfsfall die erweiterten Rechte zu nutzen.

Abbildung 8.49 Connect to AD



Der ExBPA lädt sich aus dem Active Directory die Daten der Exchange Organisation. Sie können dann alle oder nur einen Teil der Server analysieren lassen. In unserer Musterinstallation sind ebenfalls nur ein Domänencontroller sowie ein Exchange-Server vorhanden. Nun können Sie mit dem

Scannen der Server beginnen. In der Fußzeile wird Ihnen dabei der aktuelle Prozessstatus angezeigt. Bei entfernten Standorten sollten Sie die Angaben des Netzwerkes noch überprüfen. Überweigend werden die Daten über die WMI-Schnittstelle ausgelesen. Der „Health Check“ zeigt mit Symbolen und einem sogenannten „Ampelsystem“ den Erfolg des Scannens an.

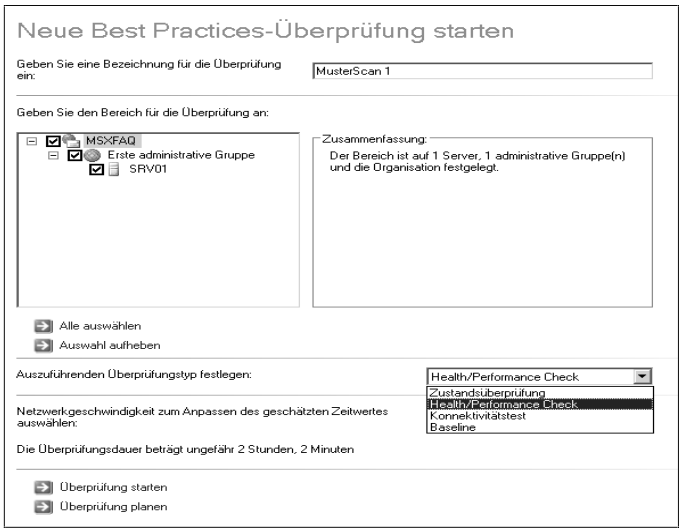


Abbildung 8.50 Exchange Scan

Im Anschluss daran erhalten Sie einen detaillierten Report Ihres Servers, von der AD-Installation bis hin zur Exchange-Konfiguration und erforderlichen Updates. In großen Umgebungen kann das Einlesen aller Informationen abhängig von der Netzwerkverbindung mehrere Stunden dauern. Hier sollten Sie im Bedarfsfall nur die gewünschten Standorte oder Server auswählen. Am Ende sehen Sie auf einen Blick den Status der Überprüfung. Hier zeigt ein COMPLETED mit grünem Häckchen an, dass alle Daten ermittelt werden konnten und keine Firewall oder fehlende Berechtigungen den Zugriff verhindert.

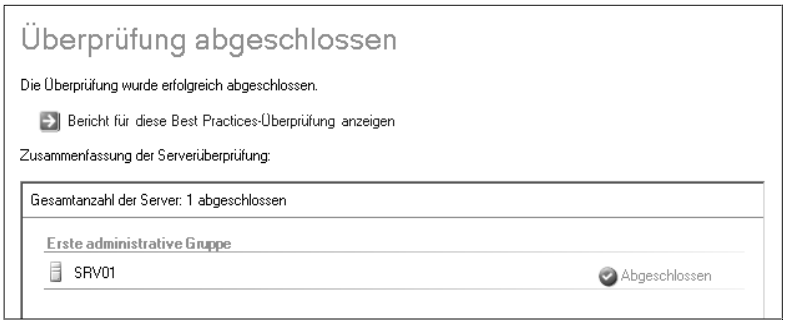


Abbildung 8.51 Erfolg des Scanvorgangs

Symbole zeigen Erfolg an

Symbol	Beschreibung
	Der Server wurde erfolgreich geprüft (Grün).
	Der Server wurde geprüft, jedoch wurde wärend der Datensammlung ein Fehlergrenzwert erreicht (Gelb).
	Der Server wurde nicht geprüft, da er nicht mehr antwortete oder nicht erreichbar ist (Rot).

8.6.6.2 Ergebnisübersicht

Über den Link "View this Best Practices Report" können Sie das Ergebnis aufbereiten lassen. In verschiedenen Ansichten und Filtern können Sie sich nun die schwerwiegenden oder leichteren Fehler und Warnungen anzeigen lassen und Hinweise für die Korrektur erhalten. Teilweise sind Einstellungen von Ihnen ja sogar erwünscht, z.B. abweichende Nachrichtengrößen oder Relay-Einstellungen. Sie sollten jedoch sehr genau die Zusammenhänge der Standardabweichungen verstehen und begründen können, warum Sie diese nicht korrigieren wollen.

Der ExBPA Report zeigt sechs verschiedenen Datentypen an. Dies sind Fehler, Warnungen, nicht vorgegebene Werte (Standardabweichungen), neueste Änderungen, fehlerhafte Basisdaten sowie allgemeine Informationen. Die verschiedenen Ansichten des Reports listen diese Daten in übersichtlicher Art und Weise auf:

- Liste schwerwiegender Probleme (CRITICAL ERRORS LIST)

  zeigt alle kritischen Fehler an, die Sie sofort beheben oder untersuchen sollten. Diese sind mit einem roten X-Symbol gekennzeichnet.

- Vollständige Liste der Probleme (FULL ISSUES LIST)

  zeigt kritische Fehler, Warnungen und Standard-abweichungen an. Eine Warnung ist mit einem gelben Warnschild gekennzeichnet und deutet auf eventuelle Probleme sowie Abweichungen von der „Best Practice“-Konfiguration hin.

- DETAILED VIEW – FULL ISSUE LIST

  gibt alle wichtigen Werte aus. Hier sehen Sie die gesamte Konfiguration des Servers sowie der Exchange- und AD-Infrastruktur.

- Dataillierte Ansicht (DETAILED VIEW)

  greift dabei auf Attributebene sowie auf die Registry-Inforamtionen zu.

- DISABLED ISSUE LIST

  enthält alle Daten, die Sie aus dem Serverreport herausgenommen haben. Dies kann z.B. eine Warnung aufgrund einer gewünschten Einstellung

sein, die nicht dem MS-Standard entspricht, wie etwa das Senden von Informationen im Fehlerfall an Microsoft.

ExBPA-Technet-Artikel helfen weiter

Zur Problembehebung befassen wir uns hier nur mit den ersten beiden Ansichten. Klicken Sie auf eines der angezeigten Probleme um weitere Informationen zu erhalten. ExBPA zeigt Ihnen eine Kurzbeschreibung des Problems an und über den Link „Tell me more about this issue and how to resolve it“ werden Sie auf die entsprechende Hilfe-Seite geleitet. Sofern von dem Rechner aus eine Internet-Verbindung vorhanden ist, wird Ihnen der aktuelle ExBPA-Technet-Artikel zu diesem Punkt angezeigt, anderenfalls greift das Tool auf die mitgelieferte Hilfe zurück, die jedoch nicht unbedingt dem aktuellen Stand entspricht.

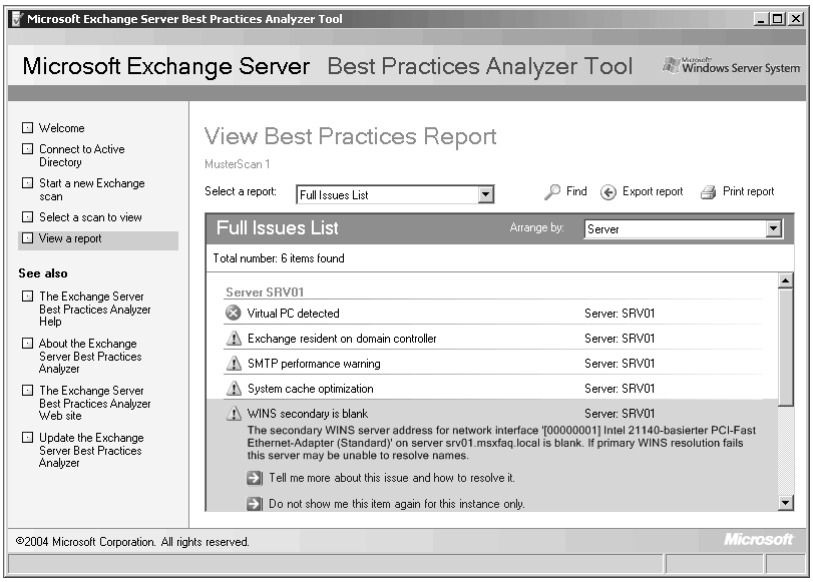


Abbildung 8.52 Ergebnisliste des Reports

Auch in unserer Musterinstallation, bereits auf SP1 aktualisiert, findet der ExBPA noch einige Konfigurationen, die Warnungen und kritische Fehler hervorrufen. Sie sollten auf keinen Fall einen produktiven Exchange-Server auf einem Virtuellen PC installieren, da dies nicht „supported“ wird. Auch die Installation des ADC wird in der Musterinstallation nicht benötig, da keine Exchange 5.5-Server vorhanden sind. Deinstallieren Sie deshalb den ADC. Viele Firmen verhindern das automatische Senden von Fehlern an Microsoft, Sie können diese Funktion im ESM aktivieren.

Exchange und DC trennen

ExBPA warnt Sie, wenn der Exchange Server als Domänencontroller fungiert. Dies ist zwar unterstützt, aber nicht empfohlen. Speziell in kleineren Umgebungen ist dies die Regel und kann in diesem Fall ignoriert werden. Sie dürfen einen bereits installierten Exchange-Server jedoch nicht mit

DCPROMO hinauf oder herunter stufen – dies ist ein nicht unterstütztes Vorgehen. Sie haben nur die Wahl über einen neuen Server oder einer Neuinstallation den Status zu ändern.

Exchange braucht WINS

ExBPA macht Sie darauf aufmerksam, wenn keine WINS-Server eingetragen wurde. Entgegen vieler früherer Verlautbarungen ist eine korrekte NETBIOS-Namensauflösung mit WINS weiterhin erforderlich. Ohne WINS-Server werden vermehrt Broadcasts genutzt und in verzweigten Netzwerken sind Folgefehler zu erwarten. Installieren Sie daher einen WINS, und tragen Sie die IP-Adresse bei Servern und PCs ein.

Sie können über den Punkt "Select a Report to View" auch andere Reports importieren. Dies ist eine gute Möglichkeit, einen Report zum Beispiel an einen Dienstleister zur Auswertung und Unterstützung bei der Fehlersuche zu geben. Der ExBPA verfügt auch über eine Kommandozeilen-Option, um die Funktion auch in eine Batchdatei einbinden zu können (ExBPACmd.exe).

Zu allen Warnungen und Fehlern finden Sie einen speziellen ExBPA-Artikel auf den Microsoft Technet-Seiten und in der Hilfe, der das Problem beschreibt und einen Lösungsansatz bietet. Aus unseren Erfahrungen heraus können wir dieses Tool wirklich nur empfehlen.

8.7 Abschlussdokumentation

Mit diesen Schritten ist die Installation des Windows 2003- und Exchange 2003-Servers abgeschlossen. Wenn Sie am Anfang bei der Festlegung der Begriffe, Namen und anderen Parametern diese Dinge auch dokumentiert haben, dann ist es jetzt an der Zeit zu prüfen, ob Ihre Dokumentation noch aktuell und vollständig ist.

Wichtige Maßnahme für den Notfall!

Eine gute Idee ist es, auch im Zeitalter der elektronischen Dokumente, für jeden Server einen klassischen DIN A4-Heftordner anzulegen und dort alles abzulegen, was zu diesem Server gehört. Dazu zählen unter anderem:

- Eine Kopie des Lieferscheins und der Rechnung
- Eine Liste der Ansprechpartner sowie Support-Verträge, Garantieurkunden und Lizenznummern
- Die Installationsquellen

  Legen Sie die CDs, mit denen die Installation durchgeführt wurde, mit in den Ordner, und bewahren Sie dieses Vorgehen auch später bei einer Änderung der Konfiguration, Nachinstallation und Anpassung. Werden später Service-Packs und andere Produkte installiert, werden auch diese CDs (evtl. in Kopie) mit eingeheftet. So haben Sie immer den direkten Zugriff auf alle Medien, wenn Komponenten verändert oder nachinstalliert werden müssen. Gerade in Notfällen kostet die Suche nach der

richtigen CD kostbare Zeit, zumal es durch die Unterscheidung nach Evaluierungs- und Vollversion, Standard und Enterprise Edition und der Sprachen sehr viele Varianten gibt.

- Notfalldisketten und erste Sicherung

  Mit dem Programm Ntbackup können Sie seit Windows 2003 eine Diskette für eine automatische Wiederherstellung erzeugen. Nebenbei erzeugt dieser Schritt auch eine Kopie der Systemeinstellungen im Verzeichnis „C:\windows\repair“. Bei der Erzeugung der Diskette wird zudem gleich das erste Backup ausgeführt, um das System wiederherstellen zu können. Beide Medien kommen mit in die Archivbox.

- Die Dokumentation

  Neben der Anlage mit den Einstellungen sollten Sie auch alle dokumentierten Installationsschritte und andere relevanten Unterlagen mit ablegen. Dazu kann auch ein Ausdruck des Gerätemanagers, der RAID-Konfiguration und anderer Einstellungen gehören. Wenn irgendwann Ihr Server nicht mehr funktioniert, kann jede Information den entscheidenden Hinweis für die Wiederherstellung geben.

- Protokoll der Änderungen

  Auch nach der Installation werden Sie immer wieder Änderungen am Server vornehmen. Um diese nachvollziehbar zu machen, reicht eine einfache Textdatei im Basisverzeichnis, in die jeder Administrator neben einem Zeitstempel (in „Notepad“ die F5-Taste!), den Namen und die Tätigkeiten festhält. Sie können aber auch klassisch ein „Server-Tagebuch“ in Papierform führen. Windows 2003 fordert Sie mittlerweile beim Neustart eines Systems zur Eingabe eines Grundes an. Leider muss man Windows 2003 nur noch sehr selten neu starten, so dass diese Angaben nur lückenhaft sind.

So vorbereitet können Sie sehr viel beruhigter schlafen, und es ist sichergestellt, dass bei einem Fehler die richtigen Datenträger und alle Informationen vorhanden sind.

8.8 Exchange Service Pack

Nachdem Sie Exchange installiert haben, sollten Sie jetzt mit dem Update auf das aktuelle Service Pack (derzeit SP2) fortfahren. Die Installation des Service Pack ändert keine bisher durchgeführten Einstellungen. Sie können die Basiskonfiguration daher vor oder nach dem Update auf SP2 durchführen.

Bevor Sie jedoch mit der Installation des SP2 beginnen, sollten Sie folgende Punkte bei jedem Update beachten:

Wichtige Punkte für jedes Update!

- Sichern Sie Ihr System vor und nach dem Update, um im Bedarfsfall auf eine gültige Sicherung des Servers zurückgreifen zu können.
- Planen Sie einen Wartungszeitraum ein, der groß genug ist, um das System im Problemfall ohne große Beeinträchtigung der Clients wieder herzustellen.
- Installieren Sie das Update zuerst auf einem Testsystem, um alle erforderlichen Schritte wie etwa Updates, Hotfixe oder mögliche Probleme in einer speziellen Umgebung einplanen zu können.
- Schließen Sie alle geöffneten Programme und beenden Sie Virenscanner und sonstige Programme, die auf Exchange zugreifen.
- Stellen Sie mittels einer Information (Stichwort: Change-Management) sicher, dass weder die Mitarbeiter noch ein Kollege auf den Server zugreifen.
- Stellen Sie sicher, dass im Problemfall eine kompetente Unterstützung von intern oder extern zur Verfügung steht.
- Beenden bzw. stoppen Sie alle Programme, die das System überwachen und die Dienste bei Ausfall wieder neu starten.
- Beenden Sie den SNMP-Dienst, da dieser nicht automatisch beim Update gestoppt wird, aber eventuell eine Aktualisierung der Performancecounter verhindert.
- Prüfen Sie, welche Updates nach dem Service Pack zusätzlich erforderlich sind (Hotfix, Patch).
- Prüfen Sie, ob eingesetzte Drittprodukte wie Virenscanner, Antispam-software und weitere kompatibel mit dem neuen Update sind.

Das aktuelle SP2 für Exchange können Sie auf der Microsoft Webseite herunterladen oder als CD bestellen: http://www.microsoft.com/downloads.

8.8.1 Server auf SP2 vorbereiten

Betriebssystem-Update

Bevor Sie mit der Installation beginnen können, sollten Sie das Betriebssystem und die erforderlichen Service Packs bzw. Hotfixe prüfen. Microsoft empfiehlt Windows 2003 Server SP1, bei Windows 2000 benötigen Sie auf jeden Fall SP4. Ebenso müssen Sie einen weiteren Hotfix auf Ihrem Server installieren, der im Knowlegde-Base-Artikel 898060 beschrieben wird. Dabei handelt es sich um einen Routingfehler in Kombination mit Windows 2003 Server SP1 oder dem Sicherheitsupdate MS05019, der die Netzwerkverbindung des Exchange Servers zum AD oder

IIS blockieren sowie auch AD-Replikationsfehler verursachen kann. Der Hotfix erfordert einen Neustart.

Sender ID Filtering verwenden

Beim Einsatz der „Sender-ID“-Filterung auf einem virtuellen SMTP Server kann es vorkommen, dass der Windows Server nicht mehr reagiert. Dann benötigen Sie einen weiteren Hotfix von Microsoft (http://support.microsoft.com/?id=905214), den Sie auch nur dann beim Microsoft Product Support Services anfordern sollten..

Entfernen von IMF 1

Sofern Sie bereits Exchange Service Pack 1 installiert haben und den Intelligent Message Filter einsetzen, müssen Sie diese Version vor dem Update auf SP2 deinstallieren. IMF Version 2 ersetzt vorherige Version.

8.8.2 SP2 installieren

Rufen Sie nun die Update.exe aus dem Service Pack auf. Exchange startet den Installationsassistenten, der Sie durch das Update führt. Dieser erkennt auch sofort, welche Komponenten in welcher Version installiert sind und ob das System aktualisiert werden kann oder noch ein Hotfix fehlt. Ohne Windows Server 2003 SP1 müssen Sie den Hotfix 831464 installieren, bevor Sie mit dem Exchange SP2-Update fortfahren können.

Während des Update-Prozesses werden die Exchange-Dienste beendet und anschließend wieder gestartet. Beachten Sie auch hier, dass Sie alle Programme, die die Funktion eines Dienstes oder Servers überwachen, vorher deaktivieren.

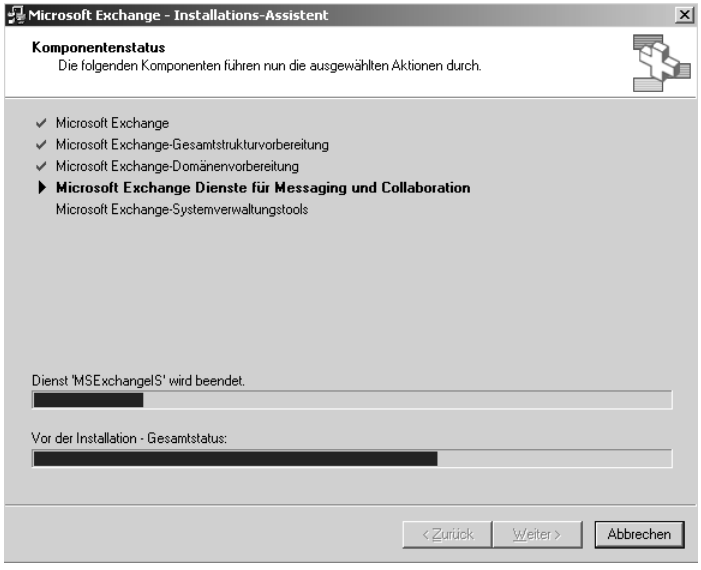


Abbildung 8.53 Installation SP1

Um nun sicherzustellen, dass alle notwendigen Hotfixe und Patches, die nach dem Service Pack 1 erschienen sind, installiert werden, sollten Sie den ExBPA (Exchange Best Practice Analyser) ausführen.

8.8.3 Update-Reihenfolge

In großen Umgebungen werden die Dienste der Exchange-Umgebung häufig auf verschiedenen Servern getrennt installiert. Somit unterscheiden wir hier zwischen Front-End- und Back-End-Servern. Bei solch einer Infrastruktur müssen Sie die Update-Reihenfolge der verschiedenen Services beachten.

ADC SP1 installieren

Für die Migration von Exchange 5.5 auf Exchange 200x ist zudem ein Active Directory Connector installiert, den Sie auf jeden Fall vor dem Update der Exchange Server auf SP1 aktualisieren sollten. Dazu starten Sie aus dem Verzeichnis „<LAUFWERK>:\E3SP1DEU\ADC\I386“ die SETUP.EXE und wählen die Option NEU INSTALLIEREN.

Front-End-Server vor Back-End-Server

Nun erfolgt das Update aller dedizierten Front-End-Server, dazu gehören die Dienste OWA, POP3, IMAP, SMTP, ActivSync und OMA. Erst danach erlaubt das System erst das Update der Back-End-Server, also der Postfach- und Öffentlichen Ordner-Server.

Im Anschluß daran sollten Sie das Exchange SP2 auf allen Computern ausführen, auf denen Exchange-Komponenten installiert sind. Dazu zählen sowohl Administrations-PC’s, auf denen der Exchange System-Manager installiert ist, sowie Anwendungsinstallationen, die auf Exchange basieren (z.B. selbst entwickelte Administrationstools, Datensicherungsserver oder Archivierungslösungen).

Voraussetzung für ein erfolgreiches Update der Exchange-Infrastruktur bei einem Mehrserverbetrieb ist auch hier eine präzise Planung, die die Zeiten für Problembehebung und der Nichtverfügbarkeit beachtet.

8.8.4 Nachbereitung

Beim Update eines Exchange Standard Servers wird automatisch der Grenzwert von 16 GB auf 18 GB hochgesetzt. Verfügt Ihr Server über ausreichend Festplattenplatz, können Sie den Grenzwert weiter erhöhen.

Rufen Sie das Registrierungstool REGEDIT auf und wechseln Sie zum Pfad `HKEY_LOCAL_MASCHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS` wählen Sie den Serverpfad. Hier befinden Sie jeweils eine Privat- und eine Public-Datenbank. Setzen Sie in dem Ordner der Privat-Datenbank den DWORD-Wert „Database Size Limit in GB“ mit der erforderlichen Zahl als Dezimalwert.

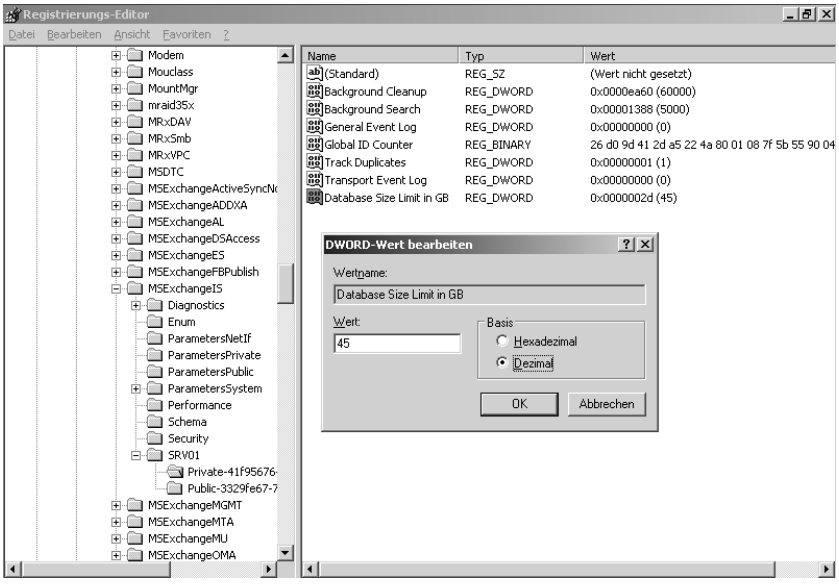


Abbildung 8.54 Datenbanklimit setzen

Das Setzen der Grenzwerte bei einem Enterprise Server sollte gut durchdacht sein. Hier muss dann für jeden neue Postfachspeicher der Grenzwert gesetzt und aktualisiert werden.

Bedenken Sie, dass größere Datenbanken nicht nur von den Festplatten abhängen, sondern Sie diese Datenmenge auch sichern und restaurieren müssen. Oft erfordern Service Level Agreements, dass die Datenbank eine gewisse Dateigröße nicht überschreiten.

Hilfe wurde aktualisiert

Das Update aktualisiert die folgenden Hilfedateien:

- ExAdmin.CHM zeigt die „Gewusst wie“-Themen im ESM an
- ExHelp.CHM enthält das kontextbezogene Hilfethema für ESM-Dialoge
- ContentFilterHELP.CHM enthält die Hilfen für Absendererkennungsfilterung und IMF
- ExSMTPui.CHM unterstützt SMTP-Fragen in einer Exchange Server-Umgebung mittelt „Gewusst wie“-Themen

Wir empfehlen Ihnen diese wichtigen Hilfestellungen bei Ihrer tägliche Arbeit mit Exchange 2003.

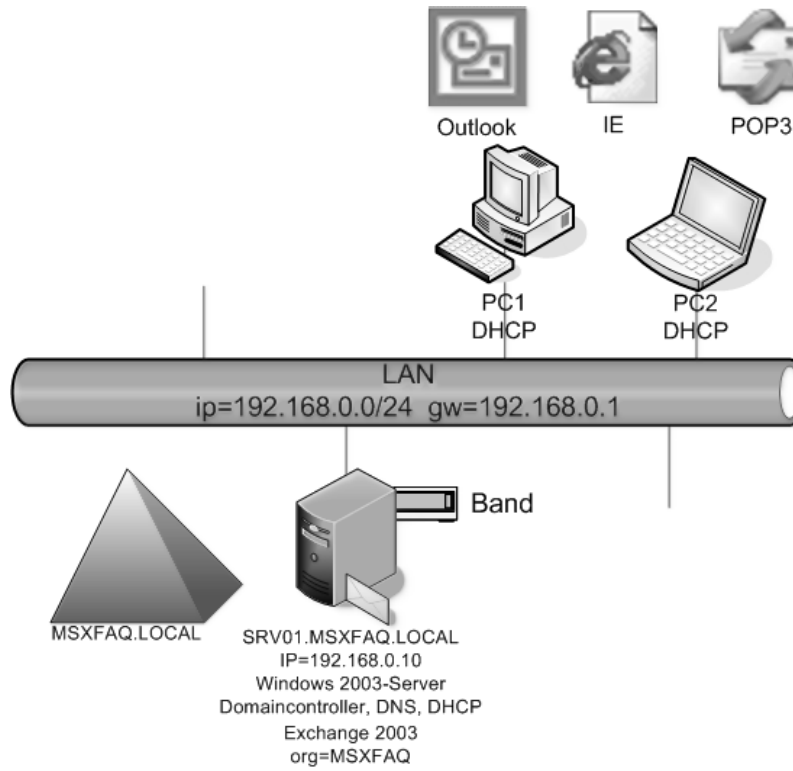
9

Exchange-Clients einrichten

9 Exchange-Clients einrichten

Im vorigen Kapitel wurde der Exchange-Server für den Betrieb installiert und konfiguriert. Ehe dieser Server nun an das Internet angeschlossen wird, sollte die Funktion des Servers erst anhand interner Anwender kontrolliert werden. Solange noch nicht alle Anwender eingerichtet sind, besteht zudem die Gefahr, dass eingehende Nachrichten als unzustellbar abgewiesen werden.

Abbildung 9.1 Installation Schritt 3



In diesem Kapitel werden die Benutzer und Verteiler für Exchange aktiviert und die Funktion von Exchange anhand verschiedener Clients demonstriert und kontrolliert.

9.1 Benutzer für Exchange aktivieren

Ehe die Anwender sich mit dem Exchange-Server verbinden können, müssen entsprechende Postfächer angelegt werden. Hierzu dient diesmal nicht der Exchange System-Manager, wie dies bei Exchange 5.5 der Fall war, sondern die Management-Konsole für Benutzer und Gruppen. Die gesamte Ad-

ministration der Anwender erfolgt dort, wo Sie auch sonst die Anwender anlegen, verschieben, Kennwörter zurücksetzen etc.

Sie können die Management-Konsole wie gewohnt über START – PROGRAMME – VERWALTUNG aufrufen. Durch die Installation des Exchange-Servers wurde die MMC ADUC um zusätzliche Funktionen erweitert. Möchten Sie auch auf Ihrem Arbeitsplatz oder einem anderen Server die Exchange-Eigenschaften von Benutzern verwalten, müssen Sie auf diesen Systemen das Exchange-Setup ausführen und bei der Installation nur die Exchange-Verwaltungswerkzeuge auswählen.

Damit der Benutzer ein Postfach erhält, muss das bestehendes Active Directory-Benutzerkonto über das Kontextmenü EXCHANGE-AUFGABEN erst für Exchange aktiviert werden.

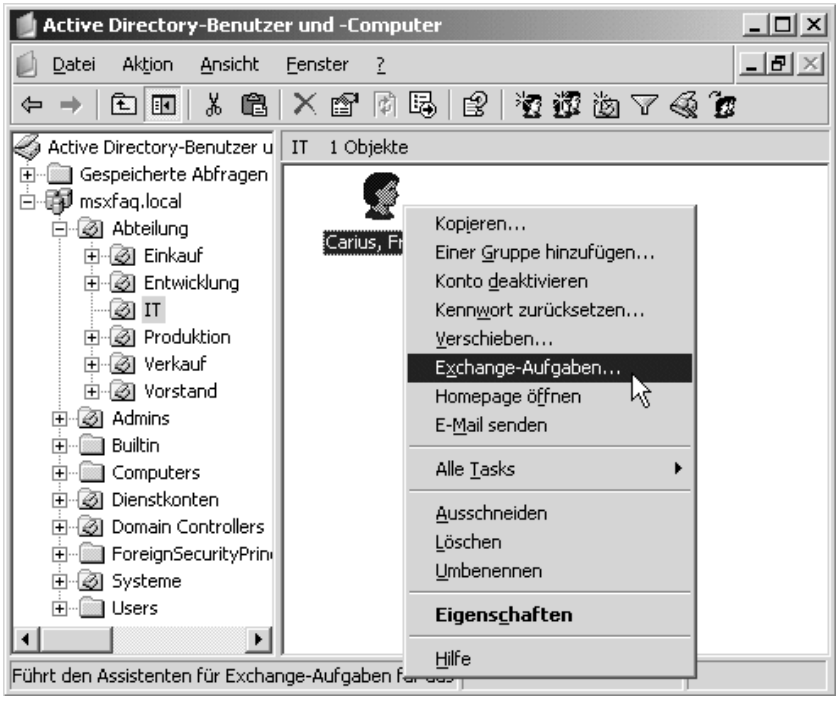
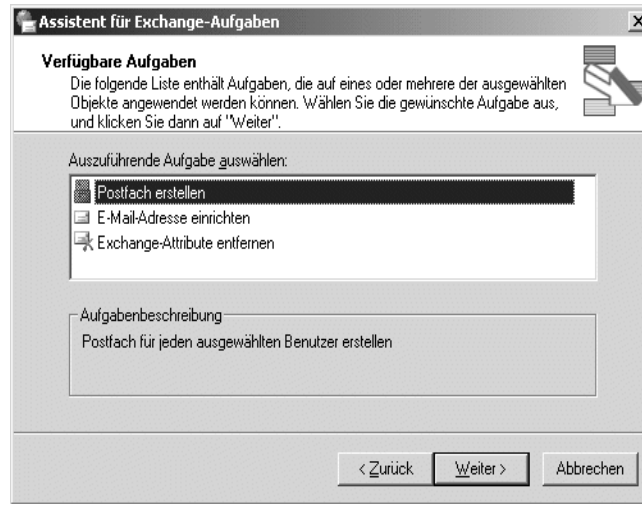


Abbildung 9.2 Exchange-Aufgaben für Benutzer

Benutzer, für die es noch kein Konto im Active Directory gibt, müssen wie gewohnt erst angelegt werden. Allerdings erlaubt die Management-Konsole nun auch gleich die Aktivierung der Exchange-Funktionen.

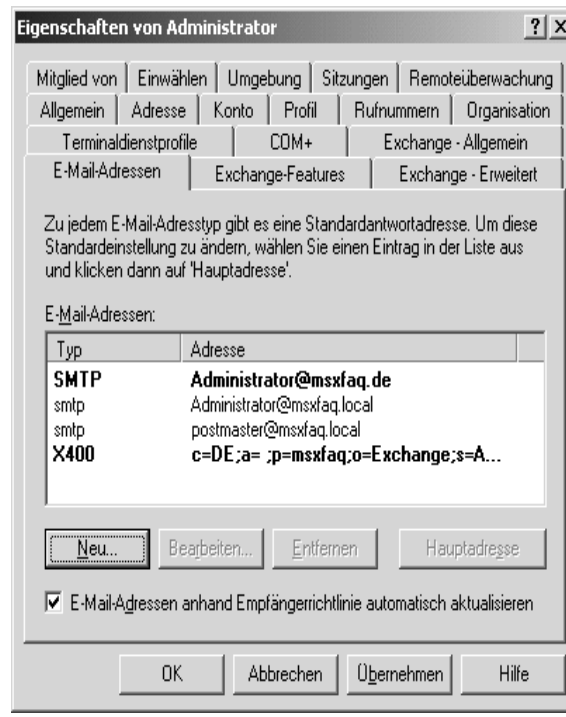
Der Assistent erlaubt Ihnen die Auswahl, ob der Anwender ein Postfach auf einem Server (mailbox-enabled) erhält oder nur eine E-Mail-Adresse (mail-enabled), die in Exchange als Kontakt erscheint.

Abbildung 9.3 Exchange-Aufgaben für Benutzer



Nach der Auswahl des Servers und des Postfachspeichers im darauf folgenden Fenster ist der Benutzer „Exchange-aktiviert“. Allerdings können nach der Aktivierung einige Minuten vergehen, da nun erst der Empfängeraktualisierungsdienst diesen neuen Benutzer erkennen und mit den entsprechenden Maildressen versehen muss. Erst wenn der RUS die E-Mail-Adressen eingetragen hat, ist das Postfach auch für den Anwender nutzbar.

Abbildung 9.4 Exchange-E-Mail-Adressen beim Benutzer



RUS setzt E-Mail-Adressen

Sollten die E-Mail-Adressen nach einigen Minuten immer noch nicht sichtbar sein, dann gilt es, die Funktion des RUS im Eventlog zu überprüfen. In größeren Umgebungen ist auch die Replikation des Active Directory zu berücksichtigen, da hier Verzögerungen durch die Replikation eingeplant werden müssen.

Individuelle Benutzer-einstellungen

Sobald ein bestehender Benutzer den neuen Anwender in Outlook als Empfänger auswählen kann, ist das Postfach fertig angelegt. Erst dann kann der Benutzer sich mit Outlook verbinden und Nachrichten senden und empfangen. Abweichend von den Standardeinstellungen des Servers und Informationsspeichers können Sie auf den weiteren Exchange-Karteikarten des Benutzers z.B. Empfangsbeschränkungen, Postfachgrenzwerte und die nutzbaren Protokolle einstellen.

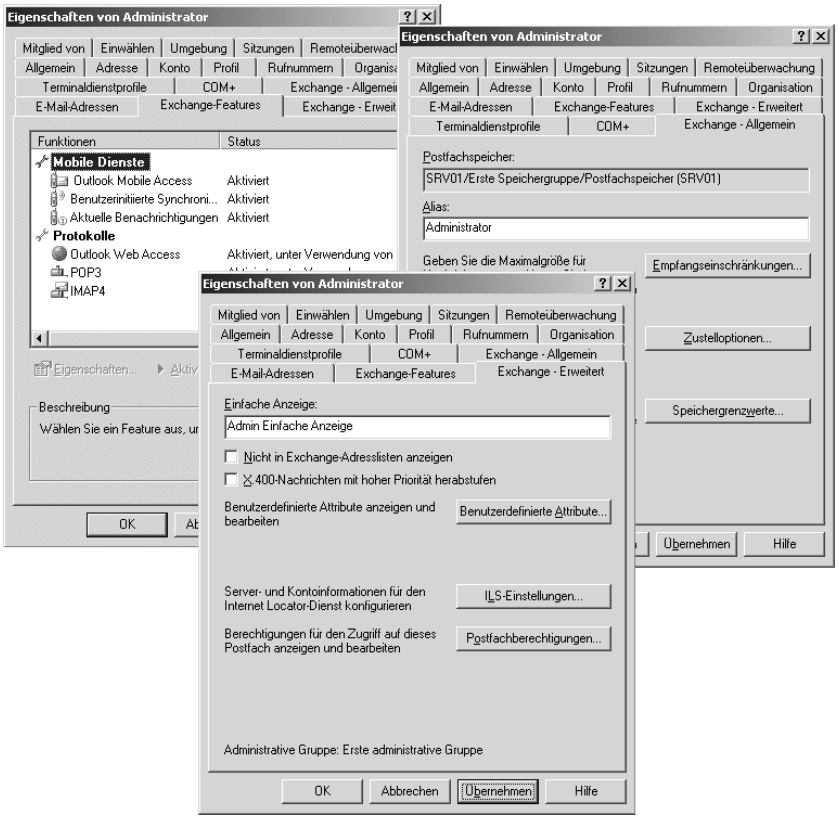
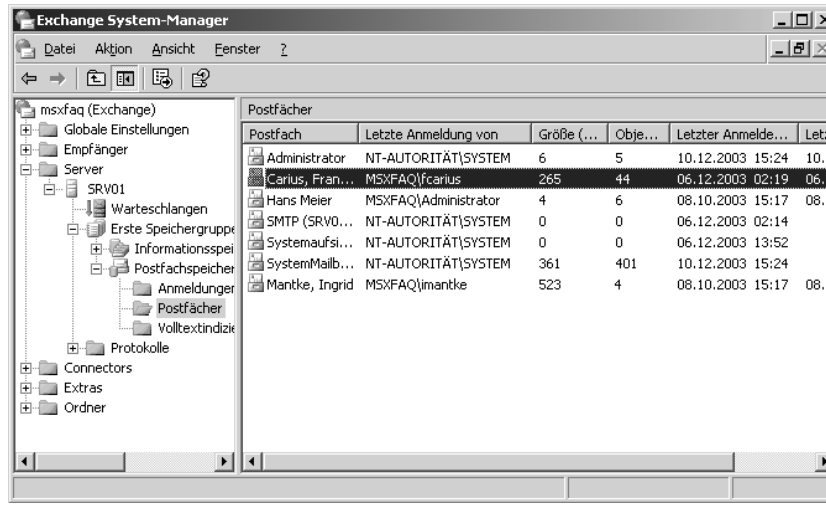


Abbildung 9.5 Weitere Exchange-Eigenschaften

Beim Blick in die Exchange-Datenbank-Ressourcen (POSTFACHSPEICHER — POSTFÄCHER) wird das Postfach allerdings erst sichtbar, wenn der Benutzer sich erstmalig angemeldet hat oder eine Nachricht an dieses Postfach zugestellt wurde.

Abbildung 9.6 Postfächer im Informationsspeicher

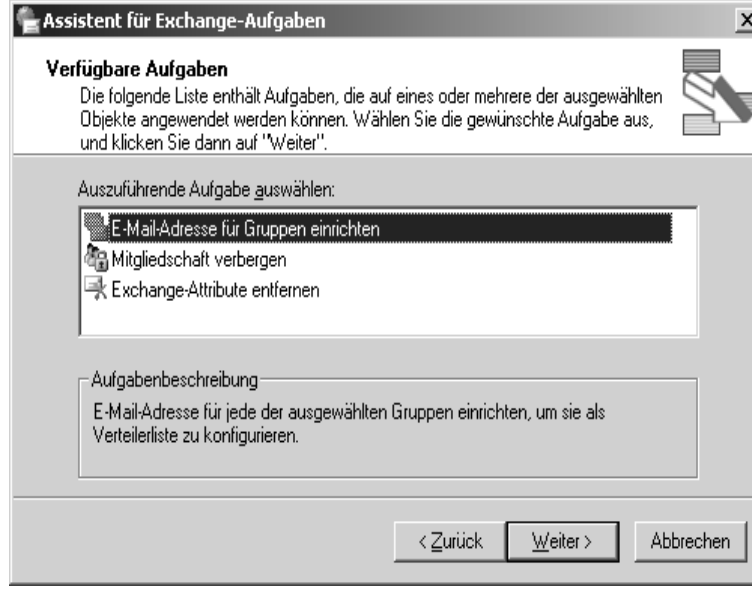


Für die Musterinstallation sollten Sie nun einige Benutzer anlegen.

9.2 Gruppen für Exchange aktivieren

Analog zu den Anwendern müssen auch die Gruppen erst für Exchange aktiviert werden, wenn Sie diese als Verteiler für Nachrichten oder zur Vergabe von Berechtigungen auf Öffentliche Ordner nutzen möchten. Bestehende Sicherheitsgruppen können über das Kontextmenü für Exchange aktiviert werden. Bei der Anlage von neuen Gruppen bietet der Assistent direkt die Aktivierung für Exchange mit an.

Abbildung 9.7 Exchange-Tasks für Gruppen



Nach der Aktivierung der Gruppe für Exchange muss ebenfalls der Empfängeraktualisierungsdienst diese Gruppe finden und entsprechend der Empfängerrichtlinien mit einer E-Mail-Adresse versehen. Das Ergebnis ist etwas später in den Eigenschaften der Gruppe zu sehen:

Abbildung 9.8 E-Mail-Adressen einer Gruppe in Exchange

USG als Verteiler

In der Musterinstallation wird eine Gruppe Vertrieb angelegt, die die Mitarbeiter des Vertriebs enthält und durch die Aktivierung für Exchange die E-Mail-Adresse „Vertrieb@msxfaq.de“ bekommt. Weitere Gruppen können Sie jederzeit anlegen. Jede Gruppe verfügt über weitere Karteikarten, in denen Sie unter anderem einstellen können, ob die Gruppe in Exchange als Verteiler sichtbar ist, wer diese Gruppe nutzen darf und wie groß Nachrichten an diese Gruppe sein dürfen.

Denken Sie daran, dass für Exchange die universellen Sicherheitsgruppen (USG) am besten geeignet sind, da diese auch in anderen Domänen aufgelöst werden können.

9.3 Ordner für Exchange aktivieren

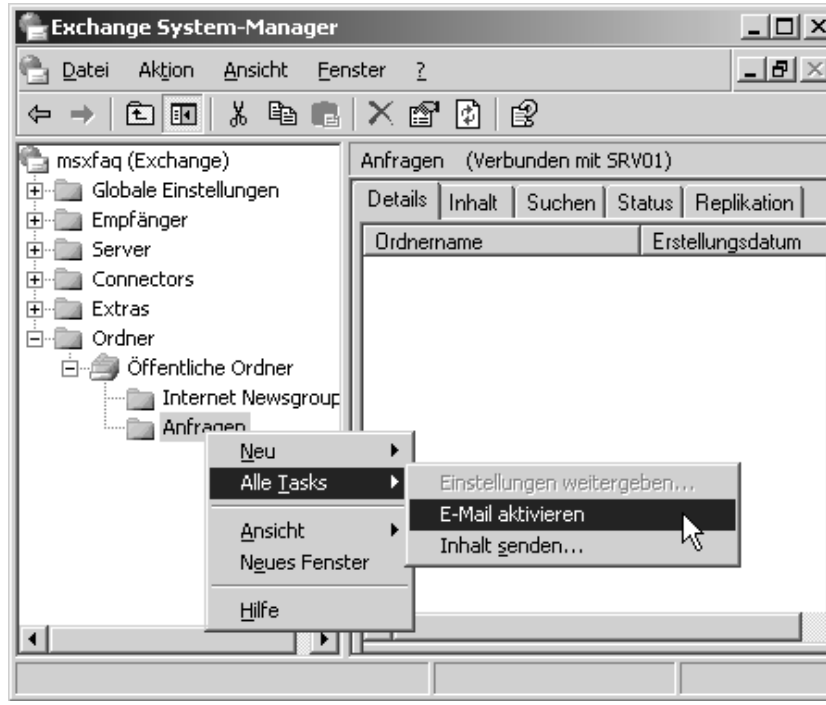
Alternative für Team-Bearbeitung von E-Mails

Auch Öffentliche Ordner (PF) können als Empfänger für Nachrichten mit einer E-Mail-Adresse ausgestattet werden. Zwar sind Verteiler sehr häufig die einfachere Möglichkeit, eine Nachricht an mehrere Personen zu senden, aber damit erhalten auch alle Personen eine Kopie dieser Nachricht. Dieses Verfahren ist nicht optimal, wenn eine Nachricht nur von einer Person der Gruppe bearbeitet werden soll. Hierfür eignen sich Öffentliche Ordner

eventuell besser, da eine Mehrfachbearbeitung vermieden werden kann. Der Einsatz Öffentlicher Ordner ist im Konzeptteil dieses Buches ausführlich beschrieben. Für die Musterinstallation wird ein Ordner „Anfragen“ angelegt, der über die E-Mail-Adresse „Anfragen@msxfaq.de“ erreichbar sein soll.

Die Aktivierung der E-Mail-Funktion eines Ordners erfolgt abweichend von den Benutzern und Gruppen über den Exchange System-Manager. Hier kann der Ordner auch angelegt und verwaltet werden, sofern dies noch nicht durch einen Anwender über Outlook erfolgt ist. Im Kontextmenü des PF wird der Ordner für den Empfang von Nachrichten aktiviert.

Abbildung 9.9 Ordner für E-Mail aktivieren



Durch die Aktivierung wird für diesen Ordner ein Objekt im Active Directory angelegt. Nach der Replikation dieser Information im Active Directory können alle Exchange 2003-Server die E-Mail-Adresse auflösen und die Nachrichten weiterleiten. Das Objekt selbst liegt im versteckten Ordner „Microsoft Exchange System Objects“ in der Domäne.

Wie bei den Anwendern und den Gruppen muss auch hier der Dienst zur Empfängeraktualisierung dieses Objekt mit einer E-Mail-Adresse gemäß den Richtlinien versehen. In den Eigenschaften des öffentlichen Ordners können Sie etwas später den Erfolg des RUS kontrollieren.

Abbildung 9.10 Public Folder-E-Mail-Adressen

Ehe Sie diesen Ordner nun nutzen können, müssen Sie die Berechtigungen auf dem Ordner anpassen. Dies kann im Exchange System-Manager oder mit Outlook erfolgen. Hierzu wird die bereits eingerichtete Gruppe „Vertrieb“ als Editor für diesen Ordner bestimmt, und der Eintrag „Anonym“ muss auf „Mitarbeiter“ gesetzt werden, damit auch externe Absender überhaupt eine Nachricht zusenden können. Auch den Eintrag „Standard“ sollten Sie auf „Mitarbeiter“ setzen, damit interne Personen, die nicht zum Vertrieb gehören, ebenfalls eine Nachricht an diesen Ordner senden können.

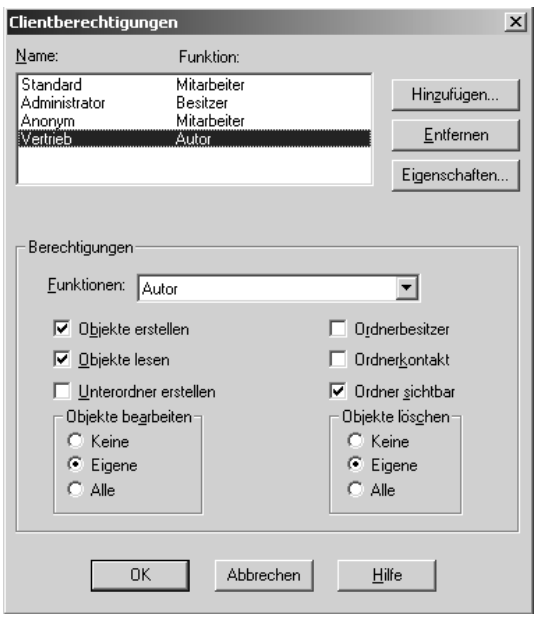


Abbildung 9.11 Rechte auf Öffentliche Ordner

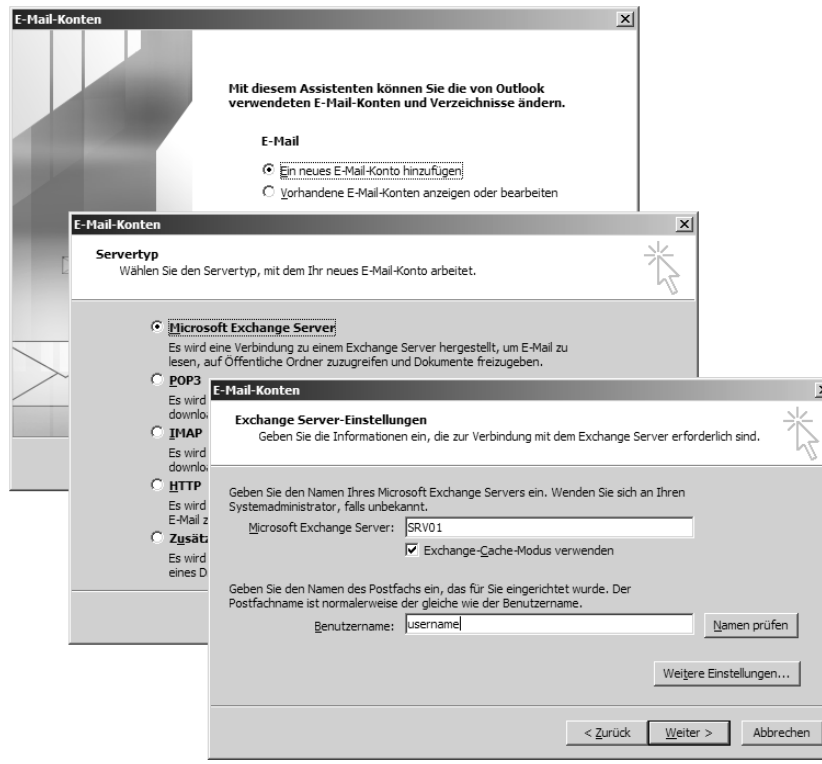
Mit diesen Einstellungen kann der Ordner von allen internen und externen Absendern erreicht werden, und die Mitarbeiter aus dem Vertrieb können in dem Ordner die Nachrichten einsehen und mit dem Hilfsmittel des KENNZEICHNUNGSSTATUS und der Überarbeiten-Funktion bearbeiten.

9.4 Outlook 2003

Die primäre Anwendung zur Arbeit mit Exchange ist natürlich Outlook. Durch die Installation der Arbeitsstationen in das Netzwerk und die Aufnahme derer in die Domäne können sich die Anwender an diesem PC mit ihrem Domänenkonto anmelden und die installierten Anwendungen starten.

Damit der Anwender mit Outlook 2003 arbeiten kann, muss Outlook für den Einsatz mit dem Exchange-Server konfiguriert werden. Der Assistent von Outlook unterstützt beim ersten Start diese Konfiguration, so dass es ein Leichtes ist, die Verbindung herzustellen.

Abbildung 9.12 Outlook-Profil-Assistent



Auch später ist die Konfiguration der Profile über SYSTEMSTEUERUNG – MAIL jederzeit wieder erreichbar. Da ein Exchange-Server für den Outlook-Client alle drei Funktionen (Transport, Ablage, Adressbuch) bereitstellt, ist es normalerweise nicht notwendig, zusätzliche PST-Dateien für die Ablage von

Nachrichten, PAB-Dateien als Adressbuch oder sonstige Transportdienste für die Übermittlung von Nachrichten zu installieren.

Cached Mode

Bitte prüfen Sie bei der Einrichtung des Profils, ob Aktivierung der Option Exchange-Cache-Modus sinnvoll ist. Outlook synchronisiert den kompletten Inhalt in eine lokale OST-Datei. Beim häufigen Wechsel der Arbeitsplatzen sollten Sie die Option bei den Anwendern deaktivieren.

Für den Einsatz mit Exchange sind die zwei folgenden Dienste ausreichend:

- Exchange Server-Dienst

  Mit diesem Dienst kann Outlook auf die Informationen in der Exchange-Datenbank zugreifen, eingehende Nachrichten anzeigen und zum Versand anstehende Nachrichten an Exchange übergeben. Auch die Ablage der eigenen Nachrichten in Ordnern und der Zugriff auf Öffentliche Ordner erfolgt über diesen einen Dienst.

- Outlook Adressbuch-Dienst

  Dieser zusätzliche Dienst erlaubt es, die Postfach-Kontakte und Kontakte in beliebigen Öffentlichen Ordnern als Adressbuch für den Versand von Nachrichten zu verwenden.

Nach dem Start präsentiert sich Outlook 2003 im gewohnten Bild und fertig zur Verwendung. Damit die Anbindung problemlos funktioniert, sind jedoch einige Randbedingungen zu beachten:

- Netzwerkverbindung

  Namensauflösung prüfen

  Der Arbeitsplatz muss den Exchange-Server und den Global Catalog-Server auflösen und erreichen können. Dies ist in der Musterinstallation dank geeigneter DHCP- und DNS-Einstellungen gewährleistet. Allerdings können lokale Filter, manuell konfigurierte TCP/IP-Einstellungen und aktive DFÜ-Netzwerke dies trotzdem verhindern. Mit NETDIAG aus den Support-Tools, NSLOOKUP und PING ist eine erste Kontrolle möglich.

- Windows als Mitglied der Domäne

  Domänen-Computer-Konto für Single Login

  Die Arbeitsstation sollte Mitglied in einer Domäne des Active Directory sein oder einer vertrauenden Domäne. Dann kann der Anwender sich als Domänen-Benutzer anmelden und ohne weitere Autorisierung auf sein Postfach zugreifen. Erfragt Outlook beim Start jedoch erneut Anmeldeinformationen, dann ist der lokale Anwender nicht berechtigt, das konfigurierte Postfach zu lesen. Dies ist oft ein Zeichen für eine fehlerhafte Vertrauensstellung zwischen dem Arbeitsplatz und der Domäne. Auch hier können Sie mit NETDIAG schnell die Ursache finden. Sind Vertrauensstellungen zwischen Domänen beteiligt, kann mit dem Programm DOMMON (Windows 2000 Resource Kit) die Ursache eingekreist werden.

- Anmeldung an der Domäne

  Der Benutzer sollte mit seinem Domänen-Konto angemeldet sein. Bei der Verbindung übermittelt Outlook neben dem im Profil eingestellten Benutzer auch die Anmeldeinformationen des an Windows angemeldeten Benutzers. Hat sich ein lokaler Anwender oder ein Konto aus einer nicht vertrauten Domäne angemeldet, dann können die Berechtigungen nicht geprüft werden. In diesem Fall muss der Anwender explizit den Windows-Benutzernamen (Domäne\Anmeldekonto) des Exchange-Postfachs sowie das Kennwort angeben.

- Exchange 2003 RUS funktionstüchtig

  Ohne den Empfängeraktualisierungsdienst werden neu angelegte Benutzer nicht für Exchange 2003 nutzbar, und der Anwender bekommt bei der Verbindung die Fehlermeldung, dass der Benutzer-Name nicht aufgelöst werden könnte. Die Kollegen können diese neuen Benutzer nicht im Adressbuch finden. Kontrollieren Sie die Funktion des RUS und die Replikation des Active Directory, wenn ein neu angelegter Benutzer nach einiger Zeit nicht im Adressbuch auftaucht und auch keine E-Mail-Adresse erhält.

Client-Test über OWA

Sollte die Kommunikation mit Outlook nicht möglich sein, dann ist ein Zugriff über den Webbrowser auf den Servernamen der nächste Test zur Eingrenzung des Problems. Funktioniert der Zugriff über einen Browser, dann ist das Postfach und der Server funktionstüchtig, und Netzwerkeinstellungen oder die lokale Outlook-Installation verhindern die Funktion des Clients. In einigen Fällen hilft die erneute Installation des TCP/IP-Protokolls auf dem Client. Prüfen Sie auch die Bindungen und eine eventuell installierte Firewall auf dem Arbeitsplatz.

Seit Outlook 2003 gibt es einen Kniff, um den aktuellen Verbindungsstatus anzuzeigen. Beim Klick auf das Outlook-Icon in der Taskleiste mit gedrückter [STRG]-Taste wird ein weiteres Kontextmenü VERBINDUNGSSTATUS sichtbar, das ein Fenster mit den aktuellen Verbindungen und statistische Daten öffnet.

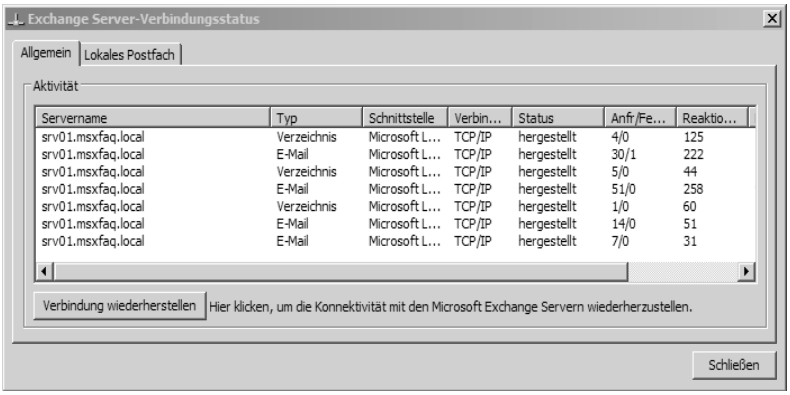


Abbildung 9.13 Outlook 2003-Statusfenster

Interner E-Mail-Test

Nachdem Outlook nun ebenfalls funktioniert, sollten Sie einfach als Test eine Nachricht an die bereits angelegten Verteiler, Öffentlichen Ordner und andere Postfächer senden. Vorerst beschränken wir uns auf die interne Kommunikation. Die Internet-Anbindung ist Thema im nächsten Kapitel.

RPC over HTTP

Outlook 2003 ermöglicht erstmalig eine Verbindung zum Exchange 2003-Server über das Protokoll HTTP. Dazu wird auf dem Windows 2003 Server der „RPC over HTTP-Proxy“ installiert, damit Outlook von nahezu überall auf den Exchange-Server zugreifen und Nachrichten abgleichen kann.

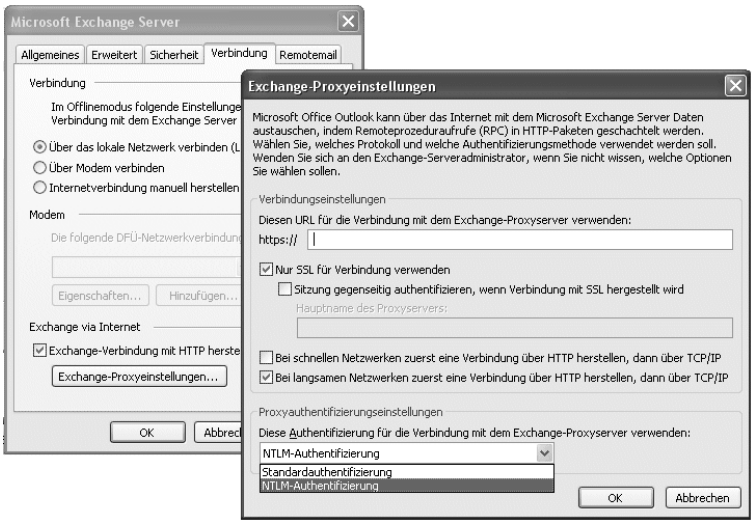


Abbildung 9.14 Outlook für RPC over HTTP einrichten

Damit der Zugriff entsprechend sicher möglich ist, sollten Sie über eine Firewall und den Einsatz einer Verschlüsselung mit SSL nachdenken. Wenn Sie bei einer Verbindung aus dem Internet zusätzlich auch noch Zugriff auf Ihre Dateiserver, Terminalserver und andere Dienste benötigen, ist eine Verbindung mit einem VPN die leistungsfähigere Wahl.

9.5 Outlook Web Access

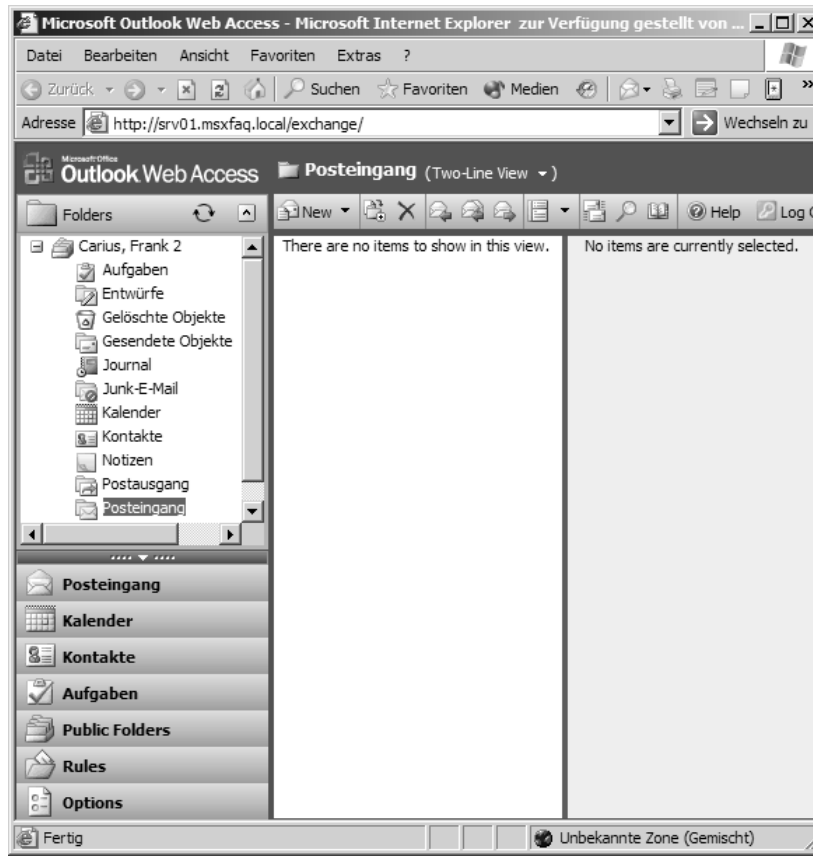
Sie können aber nicht immer davon ausgehen, dass auf allen Computern Outlook installiert ist. Vielleicht möchten Sie auch nur auf einem fremden Arbeitsplatz mal eben schnell in Ihren Posteingang schauen, ohne den aktiven Anwender abzumelden oder ein Profil für Outlook zu erstellen. Dann ist der Zugriff über einen Webbrowser eine einfache Möglichkeit, auf Informationen in Exchange zuzugreifen. Jeder Exchange 2003-Server erlaubt den Zugriff auf diese Informationen über das HTTP-Protokoll.

Im internen Netzwerk erfolgt der Zugriff einfach über die Eingabe der URL:

```
http://serv01.msxfaq.local/exchange
```

Wird der Browser nicht direkt auf einem Computer in der gleichen Domäne gestartet oder die „NTLM-integrierte Autorisierung“ abgeschaltet, erfragt der Browser die Anmeldeinformationen. Danach sehen Sie Ihren Posteingang:

Abbildung 9.15 Outlook Web Access 2003



Neues „Look&Feel“ mit aktuellem Internet-Explorer

Aber selbst beim Zugriff per Webbrowser kann es Probleme geben. Nicht alle Webbrowser unterstützen die neuen Erweiterungen, so dass ältere Browser eine etwas eingeschränkte Oberfläche erhalten. Wird zwischen dem Browser und dem Exchange-Server ein Proxy-Server oder eine Firewall installiert, welche nicht alle http-Befehle übersetzt, dann ist manchmal nur die Navigation und kein Inhalt sichtbar. Dies lässt sich meist durch den Einsatz der SSL-Verschlüsselung lösen.

HTTPS

Mit dem vorbereiteten SSL-Zertifikat in der Musterumgebung können Sie auch mit `https://srv01.msxfaq.local/exchange` auf den Posteingang verschlüsselt zugreifen. Die Warnungen des Browsers können Sie ignorieren. Im späteren Produktivnetz sollten Sie jedoch offizielle Zertifikate nutzen oder die Stammzertifikate der ausstellenden Stelle auf die Arbeitsplätze verteilen.

9.6 POP3-Zugriff mit Outlook Express

Natürlich erlaubt Exchange 2003 auch den Zugriff mit anderen Programmen außer Outlook und einem Webbrowser. Im Internet sind die Protokolle POP3 und IMAP4 hierfür geläufig, die auch von Exchange 2003 unterstützt werden. Im Gegensatz zu Exchange 2000 und früheren Versionen sind diese beiden Protokolle in der Exchange-Standardinstallation abgeschaltet. Die beiden dazu notwendigen Dienste müssen erst aktiviert und gestartet werden. Im jeweiligen virtuellen Server können weitere Konfigurationen erfolgen wie die Einrichtung von SSL oder Zugriffsbeschränkungen auf bestimmte Teilnetzwerke und auch das Beschränken von Systemen.

Nach der Aktivierung haben alle Benutzer die Möglichkeit, per POP3 oder IMAP4 auf ihre Nachrichten zuzugreifen. Für den Zugriff sind in der Musterumgebung folgende Daten wichtig.

Tabelle 9.1 POP3-, IMAP4- und SMTP-Einstellungen

Parameter	Einstellung
Postausgangsserver	Name: SRV01.MSXFAQ.LOCAL Port 25 Anmeldung erforderlich!
Posteingangsserver POP3	SRV01.MSXFAQ.LOCAL unverschlüsselt: Port 110/tcp SSL: spop3 Port 995/tcp Anmeldung erforderlich!
Posteingangsserver IMAP4	SRV01.MSXFAQ.LOCAL unverschlüsselt: Port 143/tcp SSL: simap4 Port 993/tcp Anmeldung erforderlich!
Anmeldung	ExchangeAlias\Domäne\Benutzername oder der UPN-Name: fcarius@msxfaq.local

Für den Versand ist es ebenfalls notwendig, dass der Anwender sich am Postausgangsserver autorisiert. Ein Versand über Exchange in das Internet wird ohne Anmeldung als Relay-Versuch abgelehnt. Unterstützt das Client-Programm keine Authentifizierung, können Sie auf dem virtuellen SMTP-Server entsprechende IP-Adressen oder Subnetze ohne Anmeldung zulassen. Dies sollten Sie aber nur in Ausnahmesituationen einrichten.

In Outlook Express ist daher Folgendes einzutragen:

Abbildung 9.16 Outlook Express: POP3-Einstellungen

Serverportnummer für SSL und Zustelloptionen modifizieren

Die gesicherte Kennwortauthentifizierung ist nicht mit SSL zu verwechseln. Dies ist nur ein Verfahren das Kennwort unverschlüsselt zu übertragen. Die Nutzdaten werden nur dann verschlüsselt, wenn in der Karteikarte ERWEITERT die sichere Verbindung aktiviert wird und Sie ein Zertifikat auf dem Server installiert haben. Beim gelegentlichen Einsatz von POP3 ist auf jeden Fall sicherzustellen, dass Ihre Anwendungen die Nachrichten nicht vom Server herunterladen und dort löschen, da diese dann nicht mehr auf dem Server für Outlook und andere Zugriffe zur Verfügung stehen. Leider ist dies bei vielen Programmen die Standardeinstellung.

9.7 PocketPC und ActiveSync

Exchange 2003 erlaubt von Hause aus die Synchronisation mit einem PocketPC. Ein mobiles Endgerät mit Pocket Windows kann dazu über das

Protokoll HTTP eine Verbindung zum Exchange-Server aufbauen und ein Postfach mit Pocket Outlook synchronisieren. Dies bedeutet, dass ein echter Abgleich stattfindet und eine Löschaktion auf dem PocketPC auch auf den Exchange-Server repliziert wird. Aufgrund der begrenzten Speicherkapazität werden allerdings nur Teile des Postfachs repliziert.

Synchronisation der Postfach-Inhalte

Die Verbindung vom PocketPC zum Exchange-Server kann über verschiedene Wege erfolgen:

- Craddle

  Wird der PocketPC in der Halterung aufbewahrt, erfolgt eine Synchronisierung in der Regel über die Software ActiveSync auf dem PC und dem lokal installierten Outlook. Die Verbindung wird über ein Kabel mit dem USB oder seriellem Anschluss des Arbeitsplatzcomputers aufgebaut. Neuere Geräte nutzen eine serielle Verbindung über Bluetooth-Geräte. Die gleiche Verbindung erlaubt dem PocketPC auch eine direkte Verbindung zum Netzwerk. Dann kann auch über diesen Weg eine direkte Synchronisierung mit dem Exchange 2003-Server stattfinden.

- Wireless LAN

  Der PocketPC ist nicht auf eine Netzwerkverbindung über den Arbeitsplatz angewiesen. Viele neue PocketPC-Systeme sind mit eigenen Funknetzwerkkarten ausgestattet, so dass auch ohne Basisstation eine Verbindung zum Hausnetzwerk und damit zum Exchange-Server möglich ist. Dank der Nutzung von HTTP kann ein Mitarbeiter auch von den immer mehr verbreiteten drahtlosen Zugängen auf Flughäfen und anderen Orten auf das Postfach zugreifen.

- Funktelefon/Modem

  Für all diejenigen, die immer „online“ sein wollen, ist die Verbindung über GSM und andere großräumig verfügbare Netze möglich. Der PocketPC verbindet sich über Ihr Funktelefon mit dem Internet oder direkt mit Ihrem privaten Netzwerk und greift auf den Exchange-Server zu. Mittlerweile gibt es schon PocketPC-Systeme mit *Windows Phone Edition*, die das Funktelefon schon enthalten. Interessant wird diese Anbindung in Verbindung mit volumenbasierten Abrechnungsmodellen.

Um die Sicherheit für ActiveSync zu verbessern, sollte die Synchronisation zwischen Exchange und dem PocketPC über SSL mit offiziellen Zertifikaten erfolgen. Für eine Erprobungsphase ist es möglich, mit einem eigenen SSL-Zertifikat zu arbeiten. Dazu muss auf dem PocketPC aber die Überprüfung der Stammzertifikate mit `DisableCertChk.exe` abgeschaltet oder das Stammzertifikat der ausstellenden CA auf dem PocketPC installiert werden: Hierzu enthalten die Exchange 2003-Tools das Programm „AddRootCert“, das auf dem PocketPC gestartet werden muss, um das Zertifikat der

ausstellenden CA zu installieren. Erst dann kann Ihr Pocket Windows eine Verbindung zu Ihrem Exchange-Server aufnehmen.

Abbildung 9.17 ActiveSync auf IPAQ

Die meisten Probleme bei der Anbindung eines PocketPC ist die Namensauflösung und die teilweise umständliche Konfiguration von Pocket Windows 2002. Dies hat sich mit Pocket Windows 2003 schon verbessert.

9.8 Mobilitätsverbesserungen mit SP2

Das Service Pack 2 verfügt über neue Mobilitäts-Features, die jedoch nur mit einem Gerät verwendet werden können, auf dem *Windows Mobile 5.0* und das *Messaging and Security Feature Pack für Windows Mobile 5.0* installiert ist. Ohne dem Feature Pack funktioniert lediglich das Synchronisieren von Aufgaben.

Für den Benutzer stellen die folgenden Features eine wichtige Neuerung dar:

- Direct Push

  Mit dieser neuen Exchange-Technologie wird die Verbindung zwischen Server und dem mobilen Gerät beibehalten. Neue Informationen werden daher direkt an das mobile Gerät weitergegeben.

- Adresslist-Suche

  Neu ist auch die Suche nach Kontaktinformationen in der Globalen Adressliste anhand des Namens, der Firma und anderen Suchkriterien.

- Zertifikatbasierte Authentifizierung

  Eine große Sicherheitslücke stellte bislang die Speicherung des Windows-Kennworts auf dem mobilen Gerät dar. Alternativ war der Benutzer gezwungen, jede Verbindung mit seinem Kennwort zu bestätigen. Mit SP 2 kann der Benutzer ein Zertifikat auf seinem mobilen Gerät hinterlegen, dessen Funktion nur die E-Mail-Synchronisation umfasst. Das Kennwort wird dann nicht mehr auf dem mobilen Endgerät hinterlegt.

- Nachrichten signieren und verschlüsseln

  Unter Verwendung von S/MIME zum Signieren und Verschlüsseln von Nachrichten ist auch hier eine Sicherheitslücke geschlossen worden.

- Sychronisierung von Aufgaben

  Mit Windows Mobile 5.0 kann der mobile Endgerätnutzer jetzt auch Aufgaben serverbasiert synchronisieren. Somit steht dem Benutzer eine weiterere Outlook-Komponente auch mobil zur Verfügung.

War dem Administrator bislang die Steuerung des mobilen Zugriffs sowie ein Eingreifen bei Verlust des Gerätes nicht möglich, ändert sich dies mit Service Pack 2.

- Remote Wipe

  Mit SP2 kann der Administrator aus der Ferne die Daten auf dem Endgerät löschen. Vertrauliche Daten gelangen infolgedessen bei einem Diebstahl oder Verlust nicht in fremde Hände. Nachdem die Daten auf dem mobilen Gerät gelöscht wurden, erhält der Administrator eine Bestätigung.

- Richtlinienbereitstellung

  Mittels Richtlinien können zum Beispiel sichere Gerätekennwörter erzwungen werden. Dazu gehören unter anderem die Zulassung der Synchronisierung aller Geräte (inkl. älterer Geräte) oder die Einschränkung nur sicherheitsrelevanter Geräte, die Windows Mobile 5.0 mit dem MS Feature Pack nutzen.

Microsoft hat mit dem SP2 hier jede Menge wichtige Funktionen bereitgestellt, die jedoch nur durch aktualisierte Endgeräte genutzt werden können. Erst seit April 2006, also viele Monate nach dem Release von SP2, kommen die ersten Geräte mit aktueller Firmware in den Handel.

9.9 Mobile Access und WAP

Eine weitere Möglichkeit, mit mobilen Geräten auf einen Exchange 2003-Server zuzugreifen, ist die Nutzung von „Outlook Mobile Access“. Dieser

Zugriff erlaubt es WML-kompatiblen Endgeräten, auf Informationen im Posteingang und in Kontakten zuzugreifen.

Nach der Aktivierung des Outlook Mobile Access-Servers ist allen Anwendern der Zugriff möglich, sofern in den Eigenschaften des Benutzers der mobile Dienst nicht deaktiviert ist. Der Zugriff erfolgt über die Eingabe der URL auf dem mobilen Gerät.

Die meisten Telefone bedienen sich dabei einem WAP-Gateway des Mobilfunkanbieters, das die Verbindung zwischen dem Telefon und Ihrem Server über das Protokoll TCP/IP herstellt. Dies funktioniert mit dem Exchange 2003-Server der Musterinstallation natürlich nur, wenn der Server im Internet erreichbar ist. Für die ersten Tests der Funktion hilft ein WAP-Browser für PCs weiter.

Abbildung 9.18 WAP-Zugriff mit Nokia 6210 Emulator

Verschiedene Hersteller bieten entsprechende Produkte als kostenfreie Versionen, Testversionen oder kommerzielle Produkte an. Das „Wireless Companion“ (http://www.yourwap.com, Buch CD) simuliert verschiedene Mobilfunktelefone.

Aber auch der Internet Explorer 6 kann WML-Seiten anzeigen. So können Sie den WAP-Zugang Ihres Exchange-Servers im internen Netzwerk testen und bewerten, ob Sie später den Zugang aus dem Internet freischalten. Mit

der Entwicklung leistungsfähigerer Geräte mit größeren Bildschirmen wird WAP auch besser nutzbar.

Die Menüstruktur des WAP-Zugangs ist sehr übersichtlich und stellt den einfachen, aber trotzdem eindrucksvollen Zugang zum Exchange-Postfach dar:

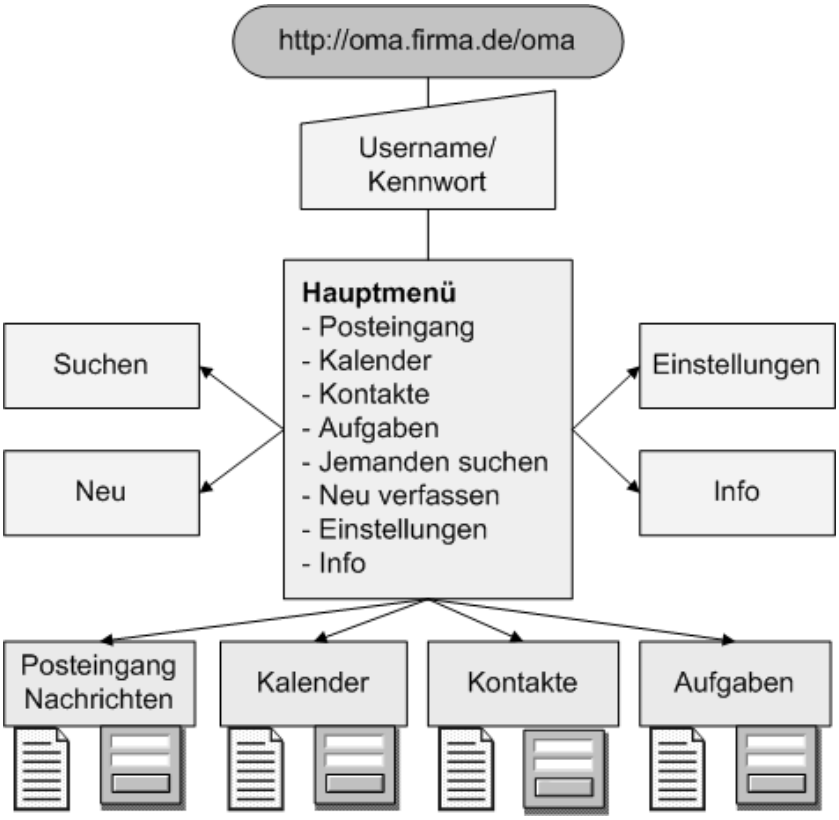


Abbildung 9.19 WAP-Menüstruktur

10

Die Internet-Anbindung

10 Die Internet-Anbindung

Thema dieses Kapitels ist die praktische Anbindung der bisherigen Musterinstallation an das Internet. In den Konzeptkapiteln des Buches sind die technischen Grundlagen für die Anbindung und die Funktionsweise von SMTP, DNS und POP3 beschrieben. Anhand der dort aufgestellten Tabelle mit den möglichen Internet-Anbindungen sollten Sie auch für Ihr Netzwerk eine passende Anbindung definieren können. Eine Auswahl der vermutlich häufigsten Konstellationen muss getroffen werden, da wir hier nicht alle Konstellationen darstellen können. Folgende drei Szenarien werden exemplarisch erläutert:

- Anbindung mittels einer festen Standleitung mit fester IP

Feste IP

Eine Anbindung, die immer mehr Firmen wählen, da heute entsprechende Leitungen zu einem akzeptablen Preis verfügbar sind. Sie entspricht einer normalen Anbindung eines E-Mail-Servers an das Internet mit fester IP-Adresse und direkter Zustellung der Nachrichten.

- Anbindung per DSL mit dynamischer IP und DynDNS

Dynamische IP

Das zweite Beispiel geht ebenfalls von einer permanent verfügbaren Verbindung aus (z.B. DSL), berücksichtigt jedoch dynamische IP-Adressen und damit verbundene DNS-Veränderungen. Zudem muss ein Router eingehende Pakete umsetzen.

- Anbindung mit einem POP3-Sammler

POP3-Sammler

Das letzte Beispiel berücksichtigt alle Umgebungen, in denen keine permanente Verbindung möglich ist und der Zugang zum Internet nur zu bestimmten Zeiten aktiviert wird. Ein Hilfsprogramm holt die wartenden Nachrichten aus einem POP3-Sammelpostfach ab.

Versuchen Sie anhand der Beispiele und der möglichen Umsetzungen zu prüfen, ob Sie es ebenso konfiguriert hätten. Für alle Beispiele werden die folgenden Fragen beantwortet:

Tabelle 10.1 Bewertungskriterien

Funktion	Konfiguration
Namensauflösung intern	Wie wird sichergestellt, dass alle internen Systeme auch die Server finden und nicht irrtümlich im Internet nachfragen?

Funktion	Konfiguration
Namensauflösung nach extern	Wie lösen die Systeme in Ihrem Netzwerk die Adressen der Server im Internet auf? In den Beispielen ist immer eine externe Auflösung möglich. Firmen, die dies nicht wünschen, verhindern damit nur, dass ein Arbeitsplatz anhand eines Namens ein anderes externes System findet. Der Zugriff nach außen anhand einer IP-Adresse wird damit nicht verhindert. Potenzielle Angreifer kommen auch ohne DNS aus.
Namensauflösung von extern	Wie ist die eigene Domäne im Internet bekannt gemacht? Wer pflegt diese Einträge? Hier sind die notwendigen MX-Einträge zu klären, damit Nachrichten überhaupt an einem Mailserver zugestellt werden.
Versand von Nachrichten	Hier stehen die entsprechenden Einstellungen für den Versand von Nachrichten mit Exchange per SMTP.
Empfang von Nachrichten	Dieser Abschnitt beantwortet die Frage: Wie werden Nachrichten an die Postfächer auf dem EMail-Server übermittelt?
Zugriff per OWA/OMA	Können die Anwender auch aus dem Internet z.B. mit einem Webbrowser einen Zugriff erhalten? Wie erfolgt der Zugriff?
Outlook über VPN	Können mobile Anwender mit einem VPN-Client eine Verbindung aufbauen?
Outlook über RPC over HTTP	Kann in dieser Konstellation der Outlook-Client auch über RPC over HTTP synchronisieren?
Virenschutz/ Spam-Schutz	Wie werden Viren und Werbemails in dieser Konfiguration blockiert?
Zugriffe nach außen	Wie gut ist die Firma gegen unerwünschte Verbindungen nach außen geschützt?

Die folgenden Konfigurationen haben ihre Tauglichkeit mehrfach bewiesen, aber sind natürlich nicht die einzigen Möglichkeiten zur Anbindung eines Exchange-Systems an das Internet.

Transparente Darstellung mit getrennten Dienst-Servern

Zur Vereinfachung wurde die Funktion des Exchange-Servers sowie der Domänencontroller und DNS-Server voneinander getrennt dargestellt. Der Betrieb der Dienste auf einem Server ist natürlich trotzdem möglich. Die Beispiele beziehen sich speziell auf kleine und mittlere Umgebungen. Je höher die Anforderungen an Sicherheit und Skalierbarkeit werden, desto umfangreicher kann eine Anbindung mit mehreren Firewalls und abgetrennten Relay- und Proxy-Diensten sein.

10.1 Beispiel 1: Standleitung und ISA-Server

Das erste Beispiel zeigt die einfache klassische Anbindung eines Firmen-Netzwerkes an das Internet. Die permanente Verbindung zum Internet (Standleitung) wird mittels eines Routers des Providers hergestellt. Die Firma erhält ein eigenes Teilnetzwerk mit offiziellen IP-Adressen. Alle anderen Systeme ab diesem Übergabepunkt liegen im Aufgabenbereich des Kunden, also bei Ihnen. Meist erhält der Kunde ein Subnetz mit der Netzwerkmaske „255.255.255.248“, woraus sich insgesamt acht IP-Adressen ergeben. Die Netzadresse ist ebenso wie die Broadcast-Adresse und die IP-Adresse des Routers nicht nutzbar, so dass die Firma letztlich über fünf unterschiedliche offizielle IP-Adressen verfügt. Natürlich sind auch größere Subnetze möglich, wenn dies begründet wird.

Angenommen Ihr Provider gibt Ihnen ein Subnetz mit den Daten „217.7.121.32/29“, dann bedeutet dies:

Tabelle 10.2 IP Nummernplan

IP-Adresse	Nutzung
217.7.121.32/28	Netzwerkadresse
217.7.121.33	Router des Providers
217.7.121.34	System 1
217.7.121.35	System 2
217.7.121.36	System 3
217.7.121.37	System 4
217.7.121.38	System 5
217.7.121.39	Broadcast-Adresse des Netzwerks

Sie können fünf Adressen effektiv nutzen. Dieses offizielle Netzwerk ist in keiner Weise gegen Zugriffe aus dem Internet gesichert, so dass in diesem Netzwerkbereich nur besonders geschützte Systeme installiert werden sollten.

NAT

Die begrenzte Anzahl an IP-Adressen macht es erforderlich, entsprechende Hilfsprogramme einzusetzen, damit eine größere Anzahl an Anwendern im Internet surfen kann. Nicht jeder interne PC kann in dieser Konstellation eine „eigene“ offizielle Adresse erhalten.

In diesem Beispiel kommt ein ISA-Server mit zwei Netzwerkkarten zum Einsatz, der das interne Netzwerk vom Internet abkoppelt und nur die explizit freigegebenen Verbindungen durchlässt. Sie können auch ein anderes Firewall-System einsetzen oder eine vorhandene DMZ nutzen.

In der nachfolgenden Grafik wird der Schwerpunkt der Kommunikation anhand einer einfachen Firewall-Konfiguration verdeutlicht. Somit weicht die

Darstellung von den sonst üblichen Internet-Anbindungs-Grafiken ab, die in Kapitel 5 erläutert wurden.

Die Anordnung in Abbildung 10.1 zeigt, dass sowohl der Exchange 2003-Server als auch der Domänencontroller im internen Netzwerk geschützt stehen. Auch alle Arbeitsplätze stehen im internen LAN. Nur die Firewall (ISA-Server) ist aus dem Internet erreichbar und besonders zu schützen.

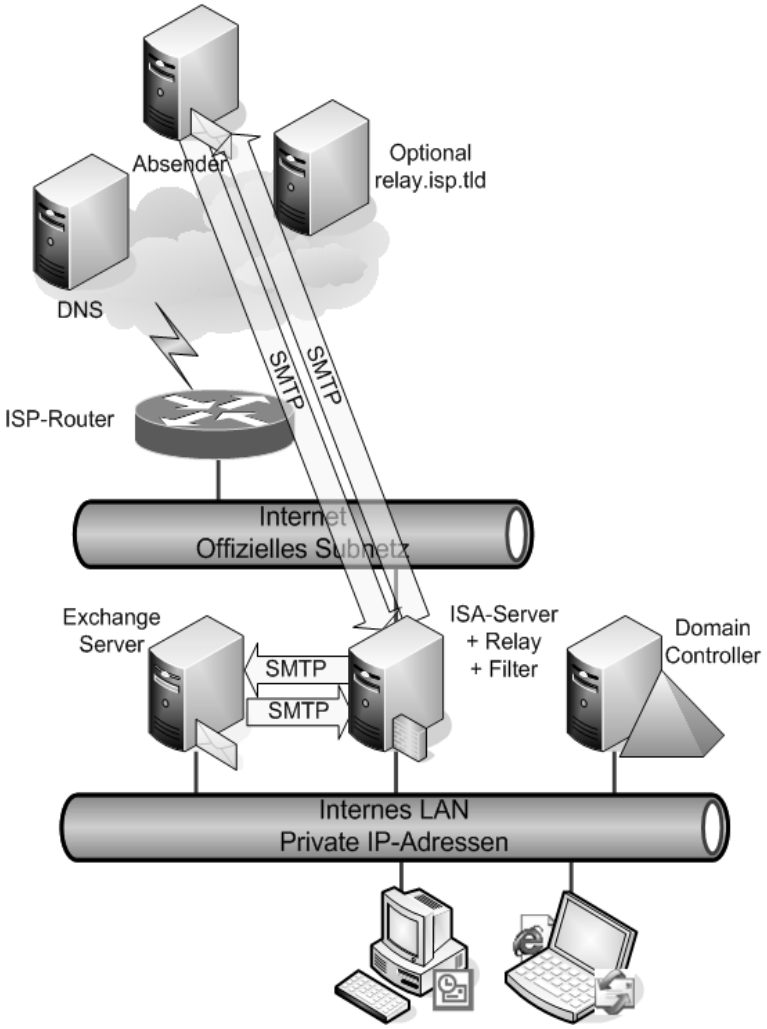


Abbildung 10.1 Internet-Anbindung: Beispiel 1: Standleitung

Für die Umsetzung der notwendigen Kommunikationswege gilt:

Funktion	Konfiguration
Namensauflösung intern	Der interne DNS-Server auf den Domänencontroller bedient die interne Active Directory-Zone. Alle internen Systeme inklusive des ISA-Servers fragen immer nur die internen Domänencontroller. Damit ist die interne Auflösung sichergestellt.

Tabelle 10.3 Bewertung der Standleitung

Funktion	Konfiguration
Namensauflösung nach extern	Auf dem ISA-Server sollte ein DNS-Server als Forwarder arbeiten und seinerseits die Root-Server oder einen DNS-Server des Providers fragen. Der interne DNS-Server nutzt den DNS-Server auf dem ISA-Server als Forwarder. So können alle internen Systeme auch externe Namen auflösen. Alternativ kann der interne DNS-Server direkt über eine Adressumsetzung (NAT) die DNS-Server im Internet fragen.
Namensauflösung von extern	Ihr Provider betreibt den DNS-Server für Ihre offizielle SMTP-Domäne. Denkbar ist natürlich auch, dass der ISA-Server selbst primärer DNS-Server und Ihr Provider nur Secondary DNS-Server ist. Dies ist aber nur sinnvoll, wenn häufig Änderungen durchgeführt werden. In der Regel sind diese Einträge sehr statisch, so dass Sie diese Aufgabe auch Ihrem Provider überlassen können.
Versand von Nachrichten	Eine statische IP-Adresse erleichtert den direkten Versand in das Internet per SMTP. Exchange 2003 kann über einen SMTP-Connector direkt per DNS die Nachrichten senden. Allerdings sollte dazu der ISA-Server den Zugriff für den Exchange 2003-Server nach außen freigeben und die IP-Adressen umsetzen. Die bessere Alternative ist die Konfiguration des ISA-Servers als SMTP-Relay mit dem Windows SMTP-Dienst. Der Exchange-Server sendet die Nachrichten an dieses Relay, und das Relay leitet die Nachrichten entweder direkt oder über einen E-Mail-Server beim Provider in das Internet weiter. Diese Variante trennt die Exchange 2003-SMTP-Funktion vom Internet. Statt des Windows 2003-SMTP-Servers können Sie auf dem ISA-Server natürlich auch ein Relay mit einem Virenscanner einsetzen.
Empfang von Nachrichten	Mit Hilfe der festen IP-Adresse kann der MX-Eintrag im Internet auf eine Ihrer offiziellen IP-Adressen verweisen. Über eine Serververöffentlichungsregel des ISA-Servers können alle Zugriffe auf diese IP-Adresse Port 25 direkt auf den Exchange-Server im internen Netzwerk weitergereicht werden. Besser ist es aber, die SMTP-Verbindung auf dem ISA-Server mit einem SMTP-Relay zu beenden und die Nachrichten dann an Exchange weiterzuleiten. Neben den SMTP-Filter-Funktionen des ISA-Servers können hierbei ebenfalls Virenscanner und andere Zusatzdienste zum Einsatz kommen.

Funktion	Konfiguration
Zugriff per OWA/OMA	Sofern in der Internet-DNS-Zone ein geeigneter Eintrag existiert, können Anwender aus dem Internet mit einem Browser eine Verbindung zum ISA-Server herstellen. Um nun auch einen Zugriff auf die Postfächer zu erhalten, ist eine entsprechende Webveröffentlichungsregel notwendig. Ab dem ISA-Server SP1 gibt es eigens einen Assistenten zur Einrichtung einer OWA-Veröffentlichungsregel. Ein SSL-Zertifikat auf dem ISA-Server rundet diese Lösung ab. Der Einsatz eines Front-End-Servers ist erst notwendig, wenn intern mehrere Exchange-Postfachserver stehen.
Outlook über VPN	Auch der Zugriff über VPN ist denkbar. Der ISA-Server kann dabei der VPN-Endpunkt sein. Über den Routing- und RAS-Dienst können mehrere Benutzer gleichzeitig aus dem Internet eine Verbindung aufbauen und so arbeiten, als wären sie direkt mit dem internen Netzwerk verbunden. So ist ein sicherer Zugriff über Outlook und RPC möglich.
Outlook über RPC over HTTP	Auch der Zugriff mit Outlook 2003 und RPC over HTTP ist möglich, wenn der interne Exchange 2003-Server dies unterstützt. Der ISA-Server muss dazu nur die entsprechenden URLs nach intern über eine Webveröffentlichung durchleiten.
Virenschutz/ Spam-Schutz	Eingehende Nachrichten können ohne zusätzliche Software durch den ISA-Server nicht überprüft werden. Der SMTP-Filter erlaubt aber die generelle Blockade bestimmter Anlagen. Es ist problemlos möglich, Drittprodukte hierzu zu integrieren. Ein Virenscanner auf dem Exchange-Informationsspeicher und dem Client ist trotzdem sinnvoll, da Anwender mit Outlook über VPN oder OWA auf Exchange zugreifen und dabei den SMTP-Scanner umgehen.
Zugriffe nach außen	Durch den ISA-Server können ohne gesonderte Konfiguration keine Anwender von intern eine Verbindung in das Internet aufbauen. Dies erschwert zum einen das Umgehen der E-Mail-Funktion, als auch den direkten Versand von Nachrichten durch SVEN und andere Viren. Achten Sie bei der Konfiguration darauf, dass nur erwünschte Verbindungen ermöglicht werden.

Die Anbindung einer Firma mit einer Standleitung und einer entsprechenden Firewall erlaubt eine sehr umfangreiche Kontrolle und Sicherung der Kommunikation. Allerdings sind die Kosten für die Anschaffung und Installation höher als bei einfacheren Lösungen. Die hier vorgestellte Lösung ist eine eher kleine Lösung. Größere Firmen installieren in der Regel zwei Firewall-Systeme, um in der dazwischen liegenden demilitarisierten Zone (DMZ) die Dienste mit Relays, Proxy-Server und anderen Systemen getrennt abzusichern. In dem vorgestellten Beispiel ist der ISA-Server gegen Angriffe von innen relativ ungeschützt.

10.2 Beispiel 2: DSL mit dynamischem DNS

Das zweite Beispiel nutzen viele Firmen, die mit einem günstigen DSL-Anschluss ihr Netzwerk an das Internet anbinden, aber keine statischen IP-Adressen zugewiesen bekommen. Bei jeder Einwahl erhält das System eine neue IP-Adresse. In diesem Beispiel ist die Verbindung zum Internet rund um die Uhr vorhanden und wird nach einer Trennung immer wieder neu aufgebaut. Es erfolgt keine Abrechnung nach einem Zeittakt.

Dieses Beispiel eignet sich daher nicht für Wählverbindungen, bei denen die Internet-Anbindung nur zu bestimmten Zeiten aufgebaut wird.

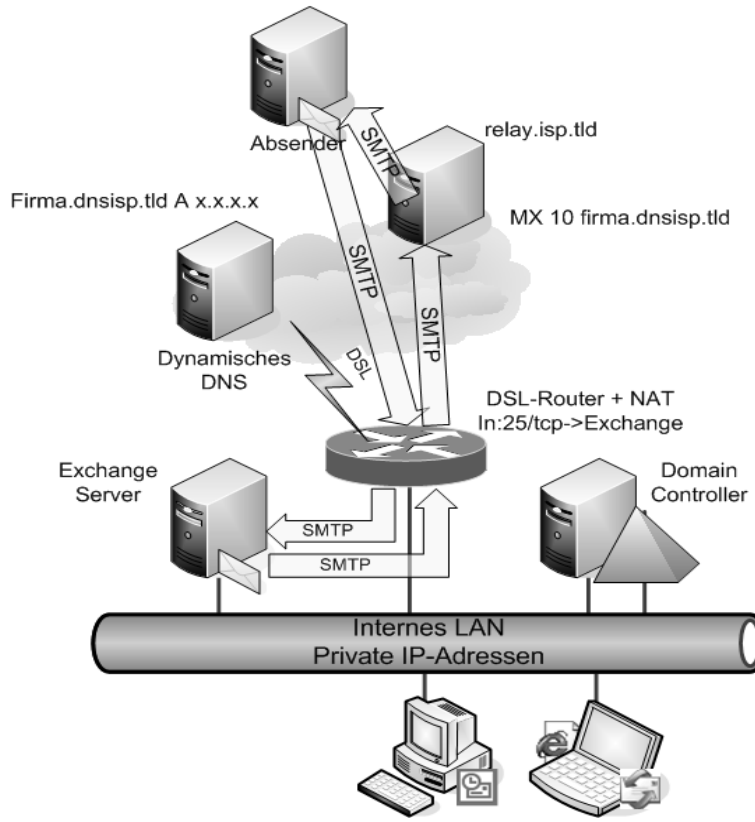


Abbildung 10.2 Internet-Anbindung Beispiel 2: dynamisches DNS

Auch hier stehen alle Server im internen Netzwerk und sind mit einer privaten IP-Adresse versehen. Der Router ist das einzige System, das auf der DSL-Schnittstelle eine offizielle dynamische IP-Adresse erhält. Alle Zugriffe von intern nach außen werden durch den Router über eine Adressumsetzung (NAT) ermöglicht.

Tabelle 10.4 Bewertung: dynamisches DNS

Funktion	Konfiguration
Namensauflösung intern	Alle Systeme nutzen zur Auflösung den internen DNS-Server des Domänencontrollers.
Namensauflösung nach extern	Damit Exchange und andere Dienste externe Namen auflösen können, leitet der interne DNS-Server die Anfragen entweder direkt an einen festen DNS-Server des Providers, die Root-Server oder an den Router (DNS-Proxy-Funktion) weiter. Die Nutzung des Routers als DNS-Proxy ist die beste Wahl, da dieser immer die aktuellen DAS-Server des DSL-Providers fragt.
Namensauflösung von extern	Die externe Namensauflösung ist bei dieser Lösung etwas umfangreicher, da der Zugangsprovider oft nur den Internet-Zugang günstig anbietet. Es ist aber kein Problem, Ihre DNS-Zone bei einem anderen Provider zu betreiben. Dies kann der Provider sein, der auch heute schon die Webpräsenz betreibt. Die aktuelle IP-Adresse des Routers wird über die Funktion des dynamischen DNS-Dienstes im Internet mit einem Hostnamen veröffentlicht. An diese Adresse werden später alle Nachrichten zugestellt. Der Provider kann nun alle Nachrichten für Ihre Domäne auf den Hostnamen weiterleiten oder der MX-Eintrag verweist direkt auf den dynamischen Hostnamen Leider bieten nicht alle Webhosting-Provider diese Lösung an, so dass Sie alternativ die DNS-Zone komplett beim DNS-Provider betreiben und von dort die Zugriffe auf eine Webseite umleiten müssen.
Versand von Nachrichten	Mangels entsprechender Relay-Funktion des Routers muss der Exchange 2003-Server die Nachrichten selbst per SMTP versenden. Auch wenn ein direkter Versand in das Internet möglich ist, sollte möglichst der Smarthost des Providers genutzt werden. Im SMTP-Connector von Exchange ist der Smarthost und eine optional notwendige Authentifizierung einzutragen. Beim direkten Versand können diverse Gegenstellen, z.B. aufgrund von Spam-Filtern, nicht immer erreicht werden. Mit einer dynamischen IP-Adresse sind Sie für einige Empfänger nicht vertrauenswürdig genug.

Funktion	Konfiguration
Empfang von Nachrichten	Der Empfang von Nachrichten erfolgt direkt über das Protokoll SMTP. Der absendende E-Mail-Server ermittelt über den MX-Eintrag in der Domäne den zuständigen E-Mail-Server. Verweist dieser Eintrag direkt auf die dynamische IP-Adresse, werden die Nachrichten über eine Verbindung an den Router zugestellt. Oft bietet der Provider aber auch ein Relay an, damit alle Nachrichten an Ihre Firma bei einer unterbrochenen Verbindung bereits bis zum Provider kommen. In dem Fall zielt der MX-Eintrag auf den Provider, der seinerseits eine feste Weiterleitung in seinem E-Mail-Server auf Ihre dynamische Adresse einrichtet. Damit überhaupt eingehende Verbindungen an Exchange durchgereicht werden, muss auf dem Router eine eingehende Regel eingetragen werden. Somit werden die Verbindungen auf den Port 25/TCP vom Router auf den Port 25 des Exchange-Servers weitergeleitet (eingehendes NAT).
Zugriff per OWA/OMA	Ähnlich der eingehenden Umleitung für SMTP können auch die Ports 80/TCP (HTTP) und 443/TCP (HTTPS) auf den Exchange-Server umgeleitet werden. Achtung: Hierbei sind eingehend alle URLs möglich. Im Gegensatz zur Webveröffentlichung bestimmter URLs des ISA-Servers im ersten Beispiel ist es hier notwendig, dass der interne IIS entsprechend sicher konfiguriert wird. So kann die Erreichbarkeit des virtuellen Verzeichnisses /EXADMIN und anderer URLs auf das lokale private Netzwerk beschränkt werden. Noch besser wird der Schutz, wenn eigens ein zweiter virtueller HTTP-Server mit einer eigenen IP-Adresse für den Zugriff aus dem Internet konfiguriert wird. Dann bleibt die „Standard-Webseite“ unerreichbar für externe Systeme. Auch der Einsatz von „IISLOCKDOWN“ und die Konfiguration von „URLSCAN“ gehören zum Pflichtprogramm des Administrators, der einen IIS derart am Internet betreibt.
Outlook über VPN	Der Aufbau einer VPN-Verbindung kann über zwei Alternativen erfolgen: a) Der Router selbst ist VPN-Gegenstelle und verschlüsselt die Daten. Die Authentifizierung erfolgt am Router. Für die Systeme im Netzwerk gibt es keine Veränderungen. b) Der Router leitet die eingehenden Verbindungen auf einen Windows 2003-Server weiter, der als Routing- und RAS-Server die VPN-Verbindungen annimmt. Hierbei ist zu beachten, dass nur wenige VPN-Protokolle über eingehende Adressumsetzungen (NAT) betrieben werden können. Die Dokumentation des Routers liefert hier entsprechende Hinweise.

Funktion	Konfiguration
Outlook über RPC over HTTP	Dieser Zugriff nutzt wie OWA das Protokoll http/https und ist durch die gleiche eingehende Umleitung der Ports 80/443 im Router nutzbar. Allerdings fehlt auch hier jeder Schutz mangels Filtermöglichkeiten oder vorhergehender Autorisierung.
Virenschutz/ Spam-Schutz	Der Einsatz eines Virenscanners für SMTP ist hier nicht auf dem Router möglich. Allerdings kann der Router die eingehenden Verbindungen problemlos auf eine vor Exchange geschaltete Software leiten, die die Nachrichten erst nach der Kontrolle an Exchange weiterleitet.
Zugriffe nach außen	Die meisten Router erlauben in der Standardeinstellung jedem System einen transparenten Zugriff von intern nach außen. Dieser Ansatz ist für ein Firmen-Netzwerk nicht akzeptabel, da auf diese Weise auch Trojaner und Viren wie SVEN ohne Blockade aktiv werden können. Um dies zu verhindern, konfigurieren Sie den Router so, dass nur vertrauenswürdige Endsysteme auf bestimmte Internet- Dienste zugreifen können. Mit dem Einsatz eines Exchange 2003-Server benötigen die Anwender keinen direkten Internet-Zugriff über SMTP, POP3 oder IMAP. Sie sollten diese Protokolle aus Sicherheitsgründen sperren und für den Webzugriff einen HTTP-Proxy-Server zur Verfügung stellen. Leider erlauben die meisten DSL-Router keine oder nur sehr wenige ausgehende Filter.

Durch die breite Verfügbarkeit verhältnismäßig günstiger DSL-Anschlüsse wird diese Anbindungsvariante sehr gerne umgesetzt. Allerdings ist für die Zustellung der Nachrichten ein Provider für dynamische DNS-Einträge notwendig, der jedoch auch den Fall berücksichtigen muss, dass Sie Ihre Webseite vielleicht bei einem anderen Internet Provider betreiben.

Die Nutzung von DSL-Anschlüssen erscheint auf den ersten Blick günstig, auch wenn Sie zusätzliche Kosten für DNS-Provider und Webspace-Provider einplanen müssen.

Geeigneten DSL-Anschluss auswählen

Aber auch bei den DSL-Anschlüssen gibt es einige Unterschiede. DSL-Anschlüsse für Unternehmen erlauben auch in den AGBs die Nutzung durch mehrere Computer. Nicht alle DSL-Anschlüsse dürfen für die Anbindung eines kompletten Firmen-Netzwerks genutzt werden. Ein weiterer Aspekt ist die Verfügbarkeit der Leitung. Gerade bei DSL-Anschlüssen für Privatkunden und Einzelpersonen werden in der Regel niedrigere Verfügbarkeitsgarantien gegeben. Ein Ausfall der Leistung für mehrere Stunden oder gar Tage ist nicht auszuschließen. Dies ist bei der Wahl des richtigen DSL-Anschlusses zu berücksichtigen.

So unterscheidet z.B. die Telekom zwischen T-DSL und T-DSL Business. Die Business-Variante ist teurer, aber erlaubt die Nutzung mit mehreren

Systemen. Als Verfügbarkeit werden 97 % angegeben. Das entspricht immer noch einer erlaubten Ausfallzeit von über 262 Stunden bzw. über zehn Tage im Jahr. DSL beschreibt jedoch nur eine Übertragungstechnik. Bei der Wahl des richtigen Providers und des richtigen Vertrags wird auch über DSL eine höhere Verfügbarkeit versprochen.

Erlaubt Ihr heutiger Webseiten-Provider keine Weiterleitung der Nachrichten an eine dynamische Adresse, können Sie über ein POP3-Sammelpostfach Ihre Nachrichten abholen.

10.3 Beispielkonfiguration „POP3 abholen“

Das dritte Beispiel beschreibt eine Lösung für Firmen, denen eine Standleitung aus verschiedenen Gründen zu teuer ist, die Verbindung zum Internet nur zu bestimmten Zeiten aufgebaut werden kann oder die direkte Zustellung per SMTP aus anderen Gründen nicht möglich ist. In diesem Fall müssen die Nachrichten beim Provider zwischengespeichert und regelmäßig abgeholt werden. Da SMTP nur ein Protokoll für den Versand von Nachrichten ist, wird häufig POP3 zweckentfremdet, um die Nachrichten beim Provider abzuholen. Der Versand von Nachrichten erfolgt weiterhin über SMTP.

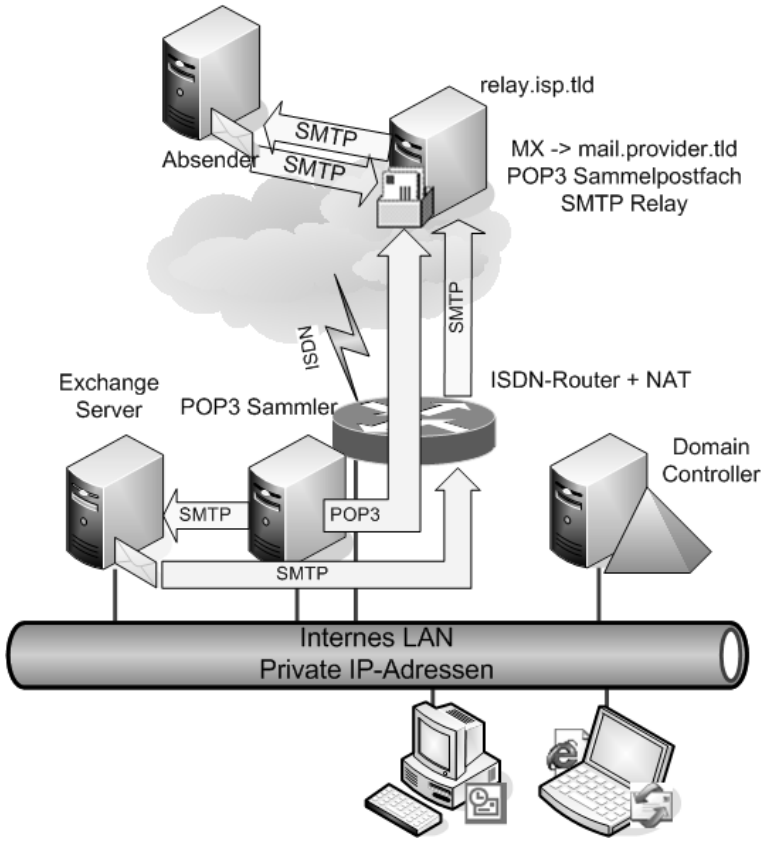


Abbildung 10.3 Internet-Anbindung Beispiel 3: POP3-Abholung

Die Verbindung zum Internet selbst kann dabei vom Exchange Server mit einem Modem oder einer ISDN-Karte hergestellt werden. Allerdings ist hiervon abzuraten, da während der Verbindung der Server ohne weitere Vorkehrungen ungeschützt aus dem Internet erreichbar wäre.

Auch bei einer Anbindung über Wählleitungen und den Abruf über ein POP3-Sammmelpostfach darf der Faktor „Sicherheit“ nicht unberücksichtigt bleiben. Aus diesem Grunde ist die Anbindung mit einem Router auf jeden Fall vorzuziehen. Wird trotzdem der Windows 2003 Routing- und RAS-Dienst eingesetzt, so sollten Sie unbedingt darauf achten, dass die Verbindung zum Provider von Windows selbstständig aufgebaut und wieder abgebaut wird. Im Gegensatz zu Exchange 5.5 ist es mit Exchange 2003 nicht mehr möglich, den Verbindungsaufbau und -abbau zu steuern.

Funktion	Konfiguration
Namensauflösung intern	Wie bereits bei den beiden vorherigen Beispielen fragen die Systeme im lokalen Netzwerk den lokalen DNS-Server auf dem Domänencontroller.

Tabelle 10.5 Bewertung POP3-Abholung

Funktion	Konfiguration
Namensauflösung nach extern	Ähnlich wie bei den bisherigen Anbindungen kann der interne DNS-Server als Forwarder den Router (DNS-Proxy), einen DNS-Server des Providers oder die Root-Server fragen. Bei dieser Anbindung sollten Sie auf eine externe Auflösung verzichten, um häufige Verbindungen aufgrund von versuchten Namensauflösungen interner Systeme zu ersparen. Der Windows 2003-DNS-Server muss selbst zum „Stammserver“ mit einer „.“-Zone konfiguriert werden, da er sonst eigenständig die Root-Server des Internets befragt. Ein entsprechender Filter auf dem Router sollte dies zusätzlich unterbinden. Für den Versand von Nachrichten und dem Zugriff auf das Internet sind die entsprechenden IP-Adressen zu verwenden.
Namensauflösung von extern	Die komplette DNS-Zone, die Webseite und der E-Mail-Server werden beim Provider betrieben. Das Firmennetzwerk ist nicht zu erreichen.
Versand von Nachrichten	Um die ausgehenden Nachrichten möglichst schnell und damit günstig abzusetzen, sendet der Exchange 2003-Server alle Nachrichten an den Smarthost des Providers. Ein entsprechend einzurichtender SMTP-Connector erhält die IP-Adresse des Providers und optional notwendige Anmelde-Informationen. Der Router übernimmt dabei die Umsetzung der IP-Adressen (NAT).
Empfang von Nachrichten	Die eingehenden Nachrichten werden alle in einem POP3-Sammelkonto oder einzelnen Postfächern beim Provider abgelegt. Ein zusätzliches Programm holt die Nachrichten zu bestimmten Zeiten ab und leitet diese per SMTP an den Exchange-Server weiter. Dieses Programm kann sowohl auf dem Exchange-Server selbst als auch jedem anderen Server gestartet werden. Der Router übernimmt auch hier die Umsetzung der IP-Adressen. Die Besonderheiten und Einschränkungen von POP3 (siehe 5.2.8, POP3-Sammeldienste) sind zu berücksichtigen.
Zugriff per OWA/OMA	Ein Zugriff von außen auf die Postfächer ist praktisch nicht möglich. Selbst die Anbindung mit dynamischen DNS-Einträgen scheitert daran, dass die Verbindung nicht permanent vorhanden ist. Der einzig sinnvoll erscheinende Zugriff ist die direkte Einwahl in das Netzwerk über den RAS-Dienst und ein Modem bzw. ISDN-Karte.
Outlook über VPN	Die Verbindung zum Firmennetzwerk mit einem VPN über das Internet ist aufgrund der nur kurzfristig bestehenden Verbindung nicht sinnvoll möglich.
Outlook über RPC over HTTP	Auch dieser Zugriff ist nur über eine direkte Einwahl sinnvoll nutzbar.

Funktion	Konfiguration
Virenschutz/ Spam-Schutz	Der Transfer vom POP3-Sammeldienst zum Exchange-Server erfolgt per SMTP. Damit können in diesen Übertragungsweg entsprechende Scanner eingebunden werden. Sehr viele kommerzielle POP3-Sammeldienste erlauben auch die Einbindung eines Virenscanners direkt beim Abrufen der E-Mails. Alternativ kann der Virenscanner selbst als POP3-Proxy zwischen dem Sammelprogramm und Ihrem Internet-Provider scannen.
Zugriffe nach außen	Da die internen Systeme die externen Namen im Internet nicht auflösen können, ist es für die Anwender sehr schwer, Dienste im Internet zu erreichen. Die Anwender kann dazu die IP-Adressen nutzen und der Router müsste die Pakete weiterleiten. Um Missbrauch durch Anwender oder Schad-programmen definitiv auszuschließen, sollten Sie trotzdem auf dem Router mit entsprechenden Filtern nicht erwünschte Zugriffe blockieren. Dies spart zudem unerwünschte Verbindungsversuche und Kosten ein. Müssen Ihre Anwender trotzdem über die Wählverbindung im Internet surfen, so ist die Einrichtung eines HTTP-Proxys ratsam, der die Anfragen der Anwender annimmt und an den Proxy des Providers weiterleitet. Ansonsten sind zusätzliche Einstellungen für die externe Namensauflösung notwendig. Der Cache des Proxy-Servers reduziert die Kosten. Diese Anbindung kann dann allerdings sehr schnell zu einer Kostenfalle werden, da viele Programme auch im Hintergrund eigenständig Zugriffe auf das Internet durchführen.

Alternativen abwägen

Die Anbindung über eine unidirektional aufgebaute Wählverbindung zum Internet stellt sicher die kleinste Lösung dar, mit der eine Internet-Anbindung realisiert wird. Gleichwohl sind Alternativen wie DSL nicht flächendeckend verfügbar, und für kleine Firmen ist diese Anbindung oft der einzige Weg, mehrere E-Mail-Anwender mit einem eigenen Exchange-Server zu bedienen.

Die Anbindung mit POP3-Sammelkonten wird teils auch von Firmen eingesetzt, die eine DSL-Verbindung mit einer Abrechnung nach Verbindungszeit nutzen und damit nicht rund um die Uhr online sein können oder deren aktueller Provider keine dynamischen DNS-Einträge unterstützt.

Mit Ausnahme der Small Business Edition ist in Exchange keine Funktion enthalten, um Nachrichten über POP3 abzuholen. Damit gibt es einen sehr großen Markt unterschiedlichster Programme. So gibt es kostenfreie Programme wie PULLMAIL, einfache Connectoren für wenig Geld und komplette Pakete, die zusätzlich die Wählverbindung effektiv managen, eine CAPI-Schnittstelle im Netzwerk bereit stellen, als HTTP-Proxy arbeiten und nebenbei auch Nachrichten per POP3 abholen und an den internen Exchange-Server weiterleiten. Die leistungsfähigeren Produkte können auch als

ausgehendes Relay genutzt werden und die komplette Steuerung, Optimierung und Kontrolle der Verbindungskosten übernehmen.

Um kurze Übertragungszeiten zu erreichen, sollten alle ausgehenden Nachrichten zum Provider und nicht direkt an die Empfänger in alle Welt gesendet werden. Allerdings erheben einige Provider für diese Funktion eine Gebühr. So erlaubt z.B. die Telekom einen Versand mit beliebigen Absenderadressen nur über ein kostenpflichtiges Relay. Wird das normale Relay für Privatanwender genutzt, dann ersetzt das System Ihre Absenderadresse durch die Zugangsadresse des Anschlussinhabers. Dies ist für Unternehmen natürlich nicht geeignet. Prüfen Sie daher, inwieweit Ihr ausgewählter Provider eine Begrenzungen bezüglich der Anzahl der Nachrichten, der Größe oder der Adressen aktiviert hat.

Die Anbindung einer kompletten Firma über POP3-Sammeldienste ist möglich, aber sollte nur die letzte Option darstellen. Die Funktionalität ist eingeschränkt und macht immer wieder Anpassungen notwendig, die von den eigenen Mitarbeitern oft problemlos und unbemerkt durchgeführt werden. Als Dienstleister müssen Sie Ihrem Kunden jedoch erklären, dass bei einer Änderung seitens des Providers eine Nachkonfiguration nicht als Nachbesserung kostenfrei erfolgen kann. Zudem kann der Dienstleister die Funktionsstörung nicht vorhersehen und es betrifft dann sehr viele Kunden zur gleichen Zeit.

Die POP3-Sammelkonten sind ein Tribut an Umgebungen, in denen eine direkte Zustellung per SMTP nicht möglich ist und andere Alternativen meist vom Provider nicht angeboten werden.

Teil IV

Dieser Teil widmet sich den weiterführenden Konzepten wie Migration und „Mehr-Server“-Betrieb.

11

Enterprise-Umgebung

11 Enterprise-Umgebung

Das Buch widmete sich bislang den Konzepten und der Installation eines einzigen Servers sowie der Anbindung an das Internet. Diese Umgebung ist für viele Firmen zutreffend. Exchange 2003 eignet sich ebenfalls sehr gut für umfangreichere Installationen. Dieses Kapitel beschreibt die möglichen Erweiterungen einer Exchange-Installation.

11.1 Der zweite Server

In der Musterinstallation wird zugunsten der Übersichtlichkeit von einem Exchange 2003-Server ausgegangen. Exchange ist optimal dafür ausgelegt, auch im Verbund mit mehreren Servern zu arbeiten. Für die Installation eines weiteren Servers kann es unterschiedliche Gründe geben:

- Verteilung der Anwender auf mehrere Server

  Erhöhte Verfügbarkeit

  Exchange 2003 skaliert sehr gut durch die Möglichkeit, mehrere Datenbanken anzulegen. Die Verbesserungen durch den Cached Mode von Outlook 2003 entlasten ebenfalls den Server. Sie können problemlos mehrere tausend Anwender auf einem entsprechend ausgelegten Server betreiben. Aber wenn Verfügbarkeit gefragt ist und ein Cluster nicht zur Auswahl steht, stellen weitere Server zur gleichmäßigen Verteilung der Postfächer und Öffentlichen Ordner eine Möglichkeit dar, die Verfügbarkeit zu erhöhen. Beim Ausfall eines Servers können die Benutzer mit Postfächern auf anderen Servern weiter arbeiten.

- Connector-Server

  Verteilung von Aufgaben

  Oftmals wird zugunsten der Stabilität des Postfachservers die Aufgabe der Nachrichtenübermittlung an das Internet, aber auch zu Faxservern etc. auf andere Systeme verlagert. Die Trennung erlaubt Ihnen viel flexibler zu reagieren, z.B. beim Neustart des Servers für Connectoren oder der Aktualisierung von Drittsoftware. Sie haben auch die Chance, den Server z.B. bei einem Virenangriff temporär außer Betrieb zu nehmen, ohne den internen E-Mail-Transfer zu beeinflussen. Da die Anwender auf dem Postfachserver arbeiten, ist in der gesamten Zeit die interne Kommunikation nicht beeinträchtigt.

- Front-End-Server

  OWA-Zugriff steuern

  Sobald Sie mehrere Postfachserver betreiben und die Anwender nur einen Namen in der URL für den Outlook Web-Zugriff eingeben sollen, benötigen Sie einen Front-End-Server. Der Front-End-Server nimmt die Anfragen an und verteilt sie an die Postfachserver.

Dies erlaubt dem Administrator die Flexibilität bei der Ablage der Postfächer, und Sie müssen nicht jeden Postfachserver im Internet verfügbar machen Ein Front-End-Server ist ein normaler Exchange 2003-Server, auf dem sich keine Postfächer befinden und der explizit in den Servereigenschaften als „Front-End“ aktiviert ist.

- Migration

  Über die Installation eines zweiten Servers ist auch die Migration eines alten Servers möglich. Die Inhalte des bisherigen Servers können über Tage und Wochen hinweg schrittweise auf den neuen Server verschoben werden, und nach einiger Zeit kann der alte Server deinstalliert werden.

Erweiterung der vorhandenen Konfiguration

Die Installation des zweiten Exchange 2003-Servers ist sehr einfach. Nach der entsprechenden Dimensionierung des Servers und der Installation von Windows-Server können Sie direkt das Exchange-Setup starten. Die Vorbereitungen der Domäne und das Schema-Update entfallen, da diese schon bei der Installation des ersten Servers erfolgt sind. Die Installationsroutine erkennt die bestehende Exchange-Konfiguration und fügt den Server in die Umgebung hinzu. Sie müssen nur die entsprechende Administrative Gruppe während der Installation auswählen.

Im Exchange System-Manager wird der zweite Server sichtbar und übernimmt sofort die globalen Einstellungen bezüglich der Empfängerrichtlinien, Connectoren und Beschränkungen.

Einzig die serverspezifischen Einstellungen sind manuell nachzuholen oder über eine Serverrichtlinie einzustellen. Dies sind unter anderem:

- Grenzwerte auf Informationsspeicher

  Diese Einstellungen sind je Server oder mittels einer Systemrichtlinie durchzuführen, damit die Anwender auf dem zweiten Server nicht unbeschränkt über die Kapazität verfügen können.

- Nachrichten-Tracking

  Die Protokollierung aller Nachrichtenübertragungen ist pro Exchange-Server oder über eine Serverrichtlinie zu aktivieren. Erst dann können Sie auch serverübergreifend die Wege der Nachrichten verfolgen.

- Einstellungen der virtuellen Server

  Eventuell durchgeführte Einstellungen bezüglich Relay- und Zugriffsbeschränkungen auf den virtuellen Servern für SMTP, POP3, IMAP4, NNTP und HTTP sind nachzuführen.

- Connectoren

  Ist der neue Server ebenfalls für Verbindungen zu anderen Standorten oder zum Internet vorgesehen, sind die bestehenden Connectoren anzupassen. Der neue Server muss als lokaler Bridgehead-Server in den Einstellungen des Connectors hinzugefügt werden. Ohne diese Konfigu-

ration leitet der Server alle Nachrichten an die vorhandenen Exchange-Server zur Übermittlung weiter.

Über die Management-Konsole für Benutzer und Computer können Sie die bestehenden Benutzer sehr einfach auf den neuen Server verschieben. Bei der Neuanlage von Benutzern stehen die Postfachspeicher des neuen Servers ebenfalls zur Auswahl. Die E-Mail-Adressen der Anwender auf diesem Server werden über die Empfängerrichtlinien unabhängig vom Exchange-Server vergeben. Öffentliche Ordner können über den Exchange System-Manager auf den zweiten Server repliziert werden.

Swing-Server

Nur wenn der Server zur Migration des ersten Servers vorgesehen ist, sind bei der Deinstallation des ersten Servers einige Besonderheiten zu beachten. Die Deinstallationsroutine von Exchange 2003 prüft sehr viele Abhängigkeiten und warnt vor Fehlern. Sie müssen u.a. dafür sorgen, dass der Routinggruppenmaster sowie die Systemordner verschoben und der RUS auf den neuen Server umgestellt wurde.

Ist der alte Server zugleich Domänencontroller, dann müssen Sie auch diese Funktionen korrekt auf die verbliebenen Server übertragen. Dies betrifft die FSMO-Rollen ebenso wie die Funktion als Globaler Katalog- und DNS-Server. Auch in Exchange muss bei Bedarf ein anderer Domänencontroller im Empfängeraktualisierungsdienst eingetragen werden. Auf keinen Fall sollten Sie einen Server einfach abschalten und versuchen, von Hand die Konfiguration zu bereinigen.

11.2 Der zweite Standort

Die Verbindung von Exchange 2003 mit Outlook 2003 erlaubt dank des „Cached Mode“ die Kompression der Daten und ermöglicht somit über langsame Leitungen eine effektive Arbeit. Trotzdem kommt irgendwann der Moment, an dem ein weiterer Standort größer wird und die Mitarbeiter nicht mehr direkt mit Outlook über die WAN-Leitung arbeiten sollen. Häufig ist eine Anbindung über Terminaldienste ebenfalls nicht möglich oder erwünscht. Dann ist es an der Zeit, einen zweiten Standort einzurichten.

Exchange-Organisation basiert auf AD-Forest

Exchange 2003 baut auf dem Active Directory auf und benötigt zum Betrieb eines Exchange-Servers an diesem neuen Standort auch die Verfügbarkeit des Active Directorys. Verfügt der zweite Standort über einen eigenen Forest, dann bedeutet dies für Exchange den Aufbau einer komplett eigenen Organisation. In dem Fall entspricht die Verbindung zwischen den beiden Standorten eher der Verbindung zweier unabhängiger Unternehmen über das Internet.

Sofern am zweiten Standort auch ein Domänencontroller des gleichen Forests verfügbar ist, können Sie Exchange 2003 in die vorhandene Organisation

installieren. Dabei sind vor der Exchange-Installation die Voraussetzungen zu schaffen:

- IP-Verbindung zum zweiten Standort

  Nicht nur Exchange nutzt SMTP über TCP/IP, auch die Domänencontroller benötigen zur Kommunikation eine TCP/IP-Verbindung Diese kann dabei problemlos eine Standleitung oder eine VPN-Verbindung über das Internet darstellen. Eine Wählverbindungen ist jedoch nicht ratsam.

- Active Directory

  Vor Ort sollte ein Domänencontroller stehen, der zudem auch Globaler Katalog-Server ist. Exchange 2003 wird später diesen Server zur Auflösung der Adressen nutzen. Damit die Server und Arbeitsplätze die benötigten Dienste finden, ist die Namensauflösung entsprechend zu konfigurieren. Da Exchange zudem auf einer funktionierenden Namensauflösung aufbaut, sollten Sie prüfen, ob im Standort die Erreichbarkeit eines WINS und DNS-Servers sichergestellt ist. In kleinen Standorten kann der Exchange Server auch diese Funktion mit übernehmen.

- Active Directory-Standorte und -Dienste

  Durch den Aufbau eines neuen Standorts mit einem eigenen IP-Subnetz sollten Sie dieses IP-Subnetz auch im Active Directory pflegen. Ohne diese Informationen können weder die Clients, noch die Server erkennen, in welchem Standort sie sich befinden und welcher Domänencontroller gut zu erreichen ist.

Zur Vereinfachung gehen wir für die weiteren Schritte von einer Domäne aus. Durch die effektive Replikation des Active Directory ist es heute kaum mehr notwendig, dass jeder Standort eine eigene Domäne betreibt. Für die Installation einer weiteren Domäne gibt es nur wenige administrative Gründe, weniger die Belastung des Netzwerks durch Replikation und Zugriffe.

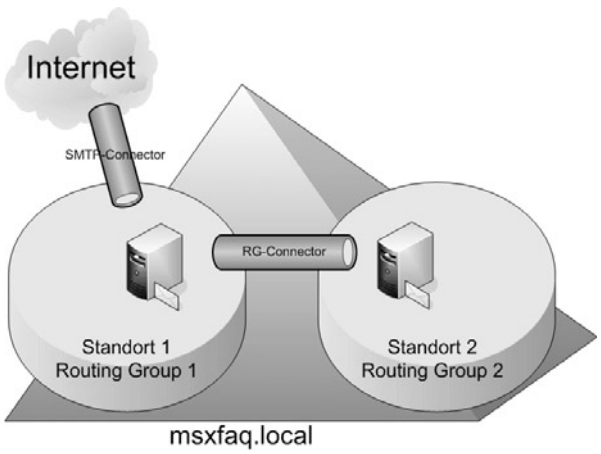


Abbildung 11.1 Der zweite Standort

Ähnlich der Installation eines zweiten Servers wird der neue Exchange 2003-Server in die gleiche Administrative Gruppe (AG) wie die bestehenden Server installiert. Nach der Installation erkennt der Server, dass er im Hinblick auf das Active Directory den Domänencontroller vor Ort fragen muss. Hinsichtlich der Kommunikation der Exchange Server untereinander geht der Server davon aus, dass er in einem Netzwerk mit allen Exchange-Server steht und mit jedem dieser Server ohne weitere Steuerung per SMTP kommunizieren kann. Dies ist natürlich nicht wünschenswert.

Routinggruppen und Connectoren

Ähnlich den Standorten im Active Directory können auch im Exchange System-Manager Standorte gepflegt werden. Diese Zusammenfassung von Servern an einem Standort bezeichnet Exchange als Routinggruppe (RG). Die Zuordnung der Server zu Routinggruppen erfolgt jedoch nicht anhand der IP-Adressen, sondern manuell durch den Exchange-Administrator. Alle Server innerhalb einer Routinggruppe kommunizieren direkt miteinander per SMTP. Damit die Server zwischen den Routinggruppen kommunizieren können, wird ein entsprechender Connector eingerichtet. Für die Installation des Exchange-Servers in einem anderen Standort bedeutet dies:

- Kontrolle des Active Directory

  Kontrollieren Sie die Active Directory-Installation, -Replikation und DNS-Funktion mit dem Aufruf von „`NLTEST /DsGetSite`“, ob der Server vor Ort den richtigen Standort nutzt. Nutzen Sie zusätzlich die Programme DCDIAG, NETDIAG und REPLMON aus den Windows Support Tools, um die einwandfreie Funktion zu prüfen.

- Installation des Exchange 2003-Servers im neuen Standort

  Kontrollieren Sie nach der Installation im Exchange System-Manager in den Server-Eigenschaften die Karteikarte VERZEICHNISZUGRIFF, ob der Server wirklich den Domänencontroller vor Ort nutzt. Nutzt Exchange einen Domänencontroller in einem anderen Standort, dann sind die DNS-Einträge noch nicht korrekt erfolgt und repliziert.

- Einrichten einer weiteren Routinggruppe

  Starten Sie den Exchange System-Manager, und aktivieren Sie in den Eigenschaften der Organisation die Ansicht der Routinggruppen.

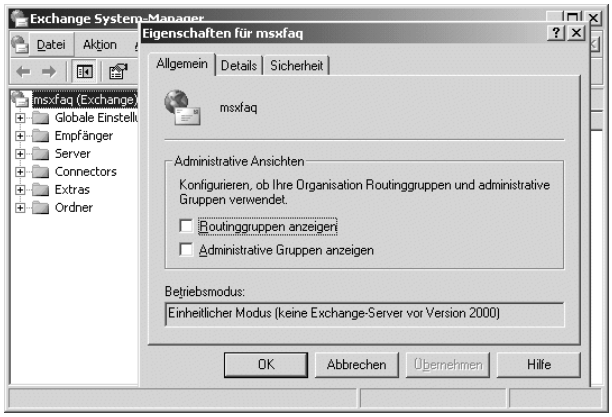


Abbildung 11.2 Anzeigen der Routinggruppen und Administrativen Gruppen

Erst dann wird der neue Eintrag für die Verwaltung der Routinggruppen sichtbar. Fügen Sie hier eine weitere Routinggruppe hinzu.

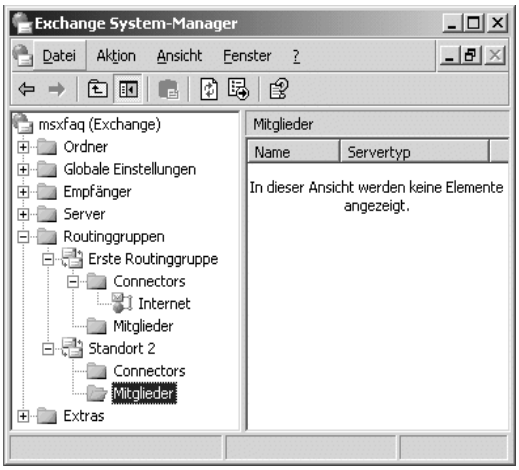


Abbildung 11.3 Anlegen der zweiten Routinggruppe „Standort 2“

Die neue Routinggruppe sollte einen Namen haben, der eine einfache Zuordnung zum Standort zulässt (siehe „Namenskonzept“).

- Verschieben des Servers in die neue Routinggruppe

  Der neu installierte Server wird einfach per „Drag and Drop“ aus der bisherigen Routinggruppe zu den Mitgliedern der neuen Routinggruppe verschoben. Diese Information wird im Active Directory eingetragen. Je nach Einstellung der Active Directory-Replikation kann es bis zu 180 Minuten dauern, bis diese Information auch den entfernten Standort und den dortigen Exchange-Server erreicht hat.

- Connector einrichten

  Routinggruppen verbinden

  Für den Austausch der Nachrichten zwischen zwei Routinggruppen muss immer ein Connector eingerichtet werden. Der Routinggruppenconnector ist für diese Aufgabe am besten geeignet. Alternativ können Sie die

Routinggruppen mit dem X.400-Connector oder einem SMTP-Connector verbinden. Allerdings nutzt der Routinggruppenconnector von Exchange 2003 das erweiterte SMTP-Protokoll zum Wiederaufsetzen von Verbindungen, so dass der X.400-Connector aus diesem Aspekt nicht mehr notwendig ist. Auch dies ist nur eine Konfigurationseinstellung im Active Directory und wird nach einiger Zeit allen Servern bekannt.

Nach diesen Tätigkeiten ist der zweite Exchange Server in der neuen Routinggruppen installiert, und die beiden Routinggruppen sind mit einem Connector verbunden. Wenn Sie später weitere Standorte mit Routing-gruppen aufbauen, sollten Sie die Connectoren immer entlang der physikalischen Netzwerkverbindungen einrichten.

Alle Anwender können nun wieder untereinander Nachrichten über Standorte hinweg austauschen. Die Mitarbeiter des entfernten Standortes können über den SMTP-Connector, der von der Anbindung an das Internet noch in der ersten Routinggruppe vorhanden ist, Nachrichten in das Internet versenden. Exchange leitet die Nachrichten entsprechend der internen Leitwegetabelle durch die Organisation.

Public Folder-Replikation und -Referrals

Nun ist zu prüfen, welche Informationen der Öffentlichen Ordner in beiden Standorten benötigt werden. Es ist für Outlook problemlos möglich, auch auf diese Informationen in einem entfernten Standort zuzugreifen (PF-Referral). Mit Rücksicht auf das Datenvolumen auf der Weitverkehrsleitung sollten Sie die erforderlichen Öffentlichen Ordner und Systemordner auf den neuen Server replizieren. Zwar bedeutet auch die Replikation der Inhalte ein entsprechendes Nachrichtenaufkommen, aber ist in der Summe oft günstiger, als wenn die Mitarbeiter über die WAN-Leitung auf die Ordner des ersten Standorts zugreifen. Der lokale Zugriff erfolgt wesentlich schneller, so dass die Mitarbeiter flüssiger mit Outlook arbeiten können.

Die Replikation der Inhalte ist je Ordner einzustellen und kann auf die Unterordner übertragen werden. Vergessen Sie nicht die entsprechenden Systemordner (Frei-/Belegt-Zeiten, Offline-Adressbücher) zu replizieren, damit auch bei der Terminplanung ein Zugriff auf die lokalen Replikate erfolgen kann.

In den Eigenschaften des Connectors können Sie über die Einstellung „Verweise auf Öffentliche Ordner zulassen“ den Zugriff der Anwender über die WAN-Verbindung auf entfernte Server unterbinden. Allerdings können die Anwender dann nur noch auf die Ordnerinhalte zugreifen, die auch auf den Servern in der gleichen Routinggruppe vorliegen.

11.3 Weitere Domäne im Forest

Die Musterinstallation beschränkt sich bislang auf ein Active Directory mit genau einer Domäne. Dies trifft sicher für die meisten Firmen zu, aber auch in Umgebungen mit mehreren Domänen kann Exchange 2003 problemlos integriert werden. Faktoren für die Installation weiterer Domäne sind z.B.:

- Administration

  In einer Domäne gibt es genau eine Gruppe „Domänen-Admins“, die sehr weit reichende Rechte hat. Es muss nicht immer Misstrauen sein, die eine Trennung verschiedener Abteilungen oder Firmenteile in mehrere Domänen erforderlich macht.

- Migration

  Bei der Migration einer NT4-Domäne können die Benutzer mittels ADMT in das Active Directory migriert werden. Sehr oft wird aber die bestehende Windows NT4-Domäne als neue eigenständige Domäne in das Active Directory integriert.

- Rechtliche Eigenständigkeit/Namensraum

  Einige Unternehmen sehen es ungern, dass alle Töchter unter dem gleichen Namensraum arbeiten. Durch die Einrichtung mehrerer Domänen kann jede Firma ihren eigenen DNS-Namensraum verwalten.

- Sicherheit

  Speziell in größeren Firmen werden häufig Ressourcen-Domänen angelegt, um bestimmte Dienste besonders abzusichern. Dies kann die Root-Domäne sein, in der die Gruppen der Schema- und Organisations-Administratoren liegen, aber auch Anwendungen wie SAP oder Systeme mit Internet-Verbindung werden oft in eigenen Domänen betrieben. Dies gilt auch für sensible Systeme wie z.B. Server der Personalabteilung oder Systeme in der Produktion.

Für die Exchange-Administration gibt es im Hinblick auf weitere Domänen zwei wichtige Punkte zu prüfen:

- Benutzer mit Postfach in der neuen Domäne

  Rechte delegieren

  Sollen in der weiteren Domäne auch Benutzer mit einem Exchange-Postfach angelegt werden, muss die Domäne zuerst mit `Setup /DOMAINPREP` vorbereitet werden. Zusätzlich muss ein neuer Empfänger-aktualisierungsdienst eingerichtet werden, der auf einen Domänen-controller der neuen Domäne verweist. Die Benutzer sind dann wie gewohnt mit der Management-Konsole für Benutzer und Computer zu aktivieren. Damit der Administrator vor Ort den Benutzern ein Postfach zuweisen kann, muss er die Exchange-Administrationswerkzeuge installieren und zudem die Leserechte auf die entsprechende

Administrative Gruppe in Exchange erhalten. Erst dann kann er die Benutzer „Exchange aktivieren“ und eine Speichergruppe aus der Liste auswählen. Der RUS vergibt entsprechend der Empfängerrichtlinien die E-Mail-Adressen für die neuen Postfächer.

- Exchange-Server in der neuen Domäne

  Der zweite Aspekt ist die Installation weiterer Exchange-Server in der neuen Domäne. Eine Domäne bedeutet oft auch eine administrative Trennung, und die Neuanlage einer entsprechenden administrativen Gruppe im Exchange System-Manager erscheint sinnvoll. Auf diese administrative Gruppe können ausgewählte Personen oder Gruppen der neuen Domäne Berechtigungen erhalten. Damit ist nicht nur die Active Directory-Domäne aus administrativer Sicht eigenständig, sondern auch die Exchange-Server sind bis zu einem bestimmten Grad eigenständig verwaltbar. Allerdings sollten Sie genau prüfen, ob eine verteilte Administration innerhalb von Exchange sinnvoll ist. Viele Dinge wie Empfängerrichtlinien, globale Nachrichtenbeschränkungen etc. werden organisationsweit geregelt, so dass eine Zusammenarbeit auf jeden Fall erforderlich ist. Dies war bei Exchange 5.5 nicht so streng vorgegeben.

Nach der Installation der neuen Domäne sollten Sie auf jeden Fall erneut die Funktion des Active Directory prüfen. Dabei gilt es, besonders auf die Funktion der DNS-Auflösung zu achten sowie die Konzeption und Konfiguration der Globalen Katalog-Server überprüfen. Erst dann sollten Sie einen Exchange Server installieren oder administrative Tätigkeiten durchführen. Hierbei unterstützt Sie wieder der Installationsassistent, der die meisten Routinetätigkeiten und Prüfungen für Sie durchführt. Die damit verbundenen Tätigkeiten sind:

Neue Umgebung für Exchange einrichten

- Vorbereiten der Domäne mit DomainPrep

  Jede Domäne muss mit SETUP /DOMAINPREP vorbereitet werden. Installieren Sie einen Exchange-Server in einer noch nicht vorbereiteten Domäne, führt das Setup dies eigenständig durch.

- Einrichten von Empfängerrichtlinien

  Oftmals erhalten Benutzer einer neuen Domäne durch ihre Firmenzugehörigkeit eigene SMTP-Adressen. Ehe diese Benutzer ein Exchange-Postfach erhalten, sollten Sie eine entsprechende Empfängerrichtlinie einrichten, damit sofort die korrekte E-Mail-Adresse zugewiesen wird.

- Einrichten eines Empfängeraktualisierungsdienstes

  In der Exchange-Organisation ist für jede Domäne ein Empfängeraktualisierungsdienst einzurichten. Diese Aufgabe ist manuell durchzuführen, nachdem die Exchange-Server dank der Domänen-Vorbereitung die notwendigen Rechte erhalten haben. Nur so bekommen

die Benutzer und Gruppen die für den Betrieb notwendigen Exchange-Attribute zugewiesen.

- Administrative Gruppe einrichten

  Richten Sie eine neue Administrative Gruppe ein, um die Exchange-Administration in der neuen Domäne an den Administrator vor Ort zu delegieren. Die Administrative Gruppe muss vor der Installation des Exchange-Servers eingerichtet werden, weil dieser nach der Installation nicht mehr in eine andere Administrative Gruppe verschoben werden kann. Auf diese Administrative Gruppe können dann entsprechende Berechtigungen vergeben werden. Delegieren Sie bitte keine Rechte an einzelne Benutzer. Besser ist hier die Vergabe von Berechtigungen über Gruppen, da die Mitgliedschaft und damit die verbundenen Berechtigungen dieser Gruppe sehr viel einfacher zu pflegen sind. Auch administrative Zuständigkeiten ändern sich im Laufe des Betriebs.

- Routinggruppen und Connectoren

  Sofern die Domäne zugleich einen neuen Standort in Ihrem Netzwerk darstellt, sollten Sie die Einrichtung einer Routinggruppe vorsehen. Befindet sich Ihre Exchange-Organisation im Mixed Mode, erfolgt dies automatisch mit der Einrichtung einer neuen Administrativen Gruppe. Im Native Mode sind Sie selbst für die Zuordnung zu der Routinggruppe verantwortlich. Entsprechende Connectoren zur Verbindung der neuen Routinggruppe sind ebenfalls einzurichten.

- Exchange-Administratorwerkzeuge und Berechtigungen

  Für die Verwaltung der Benutzer in der Domäne ist die Installation der Exchange-Administrationskomponenten auf den Systemen notwendig, an denen ein Administrator die Benutzer pflegt. Zusätzlich benötigt diese Person oder die Gruppe die Berechtigung auf die entsprechenden Organisationseinheiten.

Zur Erinnerung: Es ist nicht möglich, in einer zusätzlichen Active Directory-Domäne einen Exchange-Server zu installieren und dabei eine neue Exchange-Organisation aufzubauen. In einem Active Directory-Forest kann nur genau eine einzige Exchange-Organisation existieren.

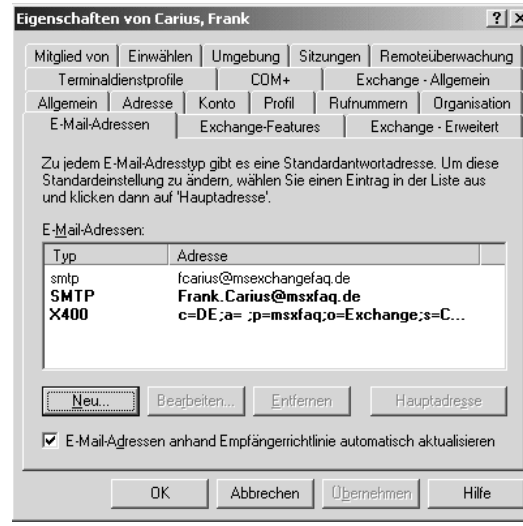
11.4 Advanced SMTP-Domain

Eine weitere Beschränkung der bisherigen Musterumgebung war die Nutzung einer einzigen SMTP-Domäne für den Versand und Empfang von Nachrichten in das Internet. Dies ist aber selbst in kleinen Firmen eher selten, da immer mehr Unternehmen zwei oder mehr Domänennamen im Internet reserviert haben und auch nutzen möchten. Daher muss Exchange

entsprechend konfiguriert werden, um ebenfalls Nachrichten an die weiteren SMTP-Domänen anzunehmen und zuzustellen.

Damit ein Postfach auch Nachrichten anderer E-Mail-Adressen annimmt, müssen diese Adressen bei dem Benutzer eingetragen werden. Sie können diese Adresse von Hand hinzufügen. Diese Aufgabe kann aber auch der Empfängeraktualisierungsdienst in Verbindung mit einer entsprechend konfigurierten Empfängerrichtlinie übernehmen.

Abbildung 11.4 Mehrere SMTP-Adressen eines Benutzers



Primary SMTP-Adresse = Reply-Adresse

Verfügt ein Benutzer über mehrere SMTP-Adressen, so ist eine der Adressen immer die primäre Adresse, mit der alle ausgehenden Nachrichten versendet werden. Ist dies nicht gewünscht, müssen Sie den Umweg über ein zweites Active Directory-Benutzerkonto mit Exchange-Postfach gehen. Dieses Postfach erhält die zweite E-Mail-Adresse, und der erste Benutzer bekommt das Recht, dieses Postfach zu nutzen und Nachrichten zu senden (FULL MAILBOX ACCESS und SEND AS).

Damit Exchange überhaupt die neue SMTP-Domäne akzeptiert, muss diese unbedingt in den Empfängerrichtlinien eingetragen werden. Alle Exchange 2003-Server in der Organisation erkennen anhand der Richtlinien, welche SMTP-Domänen für den Empfang von E-Mails akzeptiert werden. Über die Empfängerrichtlinien kann die Verwaltung der E-Mail-Adressen sehr viel besser gesteuert werden als die manuelle Vergabe. Bei der Konfiguration der Empfängerrichtlinie können Sie zwischen drei Varianten wählen:

SMTP-Domäne in Empfängerrichtlinie eintragen

- Erweitern einer bestehenden Richtlinie

  Eine zusätzliche SMTP-Adresse für eine bestehende Empfängergruppe, weisen Sie am besten über die bestehende Richtlinie zu. Fügen Sie einfach die weitere SMTP-Adresse in der betreffenden Richtlinie hinzu.

Alle Benutzer bekommen die neue Adresse zusätzlich zu der bisherigen Adresse. Kleine Firmen mit einer Empfängerrichtlinie für alle Personen werden in der Regel die Standardrichtlinie erweitern.

- Anlegen einer neuen Richtlinie mit Anwendern

  Soll eine weitere Personengruppe, unabhängig von den anderen Benutzern, diese eine SMTP-Adresse erhalten, ist eine neue Empfängerrichtlinie sinnvoll. Richten Sie eine neue Richtlinie ein, die die SMTP-Domäne den per LDAP-Filter ausgewählten Benutzern zuweist. Hierbei ist es hilfreich, wenn diese Anwender ein gemeinsames Suchkriterium, z.B. den Firmennamen, in den Eigenschaften enthalten, so dass Sie mühelos einen entsprechenden Filter erstellen können.

- Anlegen einer Platzhalterrichtlinie

  Für Exchange 2003 ist es nicht relevant, ob für die eingerichtete SMTP-Domäne auch ein Empfänger mit der E-Mail-Adresse existiert. Erfolgt die Weiterverarbeitung der E-Mails z.B. über Regeln, Connectoren oder eigene Transport Event Sinks, oder pflegen Sie die Empfänger-Adressen von Hand, erscheint eine Richtlinie im ersten Moment nicht sinnvoll. Sie müssen jedoch sicherstellen, dass Exchange die Nachrichten überhaupt annimmt. Hierzu benötigen Sie eine Richtlinie, die zwar die SMTP-Domäne enthält, aber mit einem geeigneten Filter diese Adressen niemals einem Objekt zuweist. Nun können Sie komplett von Hand die SMTP-Adressen bei den gewünschten Objekten hinzufügen.

Die Änderungen werden im Active Directory eingetragen und nach der Replikation und der damit verbundenen Wartezeit (ohne Neustart der Dienste) aktiv. Ob Ihr Exchange-Server die neue Domäne bereits akzeptiert, lässt sich z.B. mit Outlook Express oder TELNET prüfen. Versuchen Sie einfach eine Nachricht per SMTP für die neue Adresse an den Exchange-Server zu senden. Sobald die Richtlinie aktiv ist, nimmt der Server die Nachricht an, anstatt sie mit einem „Unable to Relay“ abzulehnen.

Damit die Nachrichten aus dem Internet bis zum Server gelangen, sind auch im Internet die entsprechenden Einträge in der DNS-Zone (Stichwort MX-Record) notwendig. Weitere Systeme zwischen dem Internet und Exchange (z.B. Virenscanner, Firewall, POP3-Sammler) erfordern eventuell eine entsprechende Konfiguration.

11.5 Advanced SMTP-Routing

Exchange 2003 ist ein sehr leistungsfähiger E-Mail-Server, der vielerorts auch als zentrale Station für die Verteilung von Nachrichten an andere Systeme übernimmt. Dabei kann Exchange sowohl Nachrichten für

komplette Domänen annehmen und weiterleiten, als auch mit anderen E-Mail-Systemen den gleichen Adressraum gemeinsam nutzen und Nachrichten je nach Empfänger individuell weiterleiten.

Gerade bei der Migration oder wenn mehrere E-Mail-Server parallel betrieben werden, stellt sich die Aufgabe, der Nutzung des gleichen Adressraums für mehrere Systeme. Allerdings bietet weder das Internet noch DNS eine Lösung für dieses Problem. Alle Nachrichten an eine SMTP-Domäne werden an die eingetragenen E-Mail-Server zugestellt. Eine Unterscheidung Der Zielserver nach Postfächern wird nicht durchgeführt, selbst wenn es entsprechende Standards sogar gibt.

E-Mail-Zustellung für verschiedene Systeme splitten

Einige Firmen lösen dieses Problem durch Subdomains in der Adresse. E-Mail-Adressen wie user1@exchange.firma.de und user2@notes.firma.de zeigen auch nach außen, dass das E-Mail-System keine globalen Adressen nutzt. Dies macht nicht nur einen unprofessionellen Eindruck, sondern erschwert auch die Migration der Anwender, da sich bei einem Umzug auf ein anderes System auch die E-Mail-Adresse ändert. Einige Unternehmen nutzen das Länderkennzeichen in der E-Mail-Adresse, um ein Routing innerhalb der Firma auf den richtigen E-Mail-Server zu erreichen (user@de.firma.com).

Dieser Aufwand ist mit Exchange nicht notwendig, da das System anhand des Globalen Katalogs problemlos alle Personen mit ihren Postfächern zuordnen und Sie als Adresse einfach username@firma.de verwenden können. Wo sich das Postfach physikalisch befindet, ist nicht entscheidend.

Hinter den Kulissen ist jedoch etwas Vorbereitung und Konfiguration notwendig. Damit mehrere E-Mail-Systeme eine gemeinsame Adresse nutzen können, bietet Exchange dazu mehrere Möglichkeiten:

- Exchange leitet eine komplette Domäne weiter

  Weiterleitung der Kunden- E-Mails

  Sofern das andere E-Mail-System eine komplett eigene Domäne bedient, kann Exchange 2003 für diese Domäne ein Relay spielen. Dieser Einsatz ist häufig bei Providern gewünscht, die E-Mails für ihre Kunden annehmen und für sie bereithalten. Dies wird dadurch erreicht, indem für jede dieser Domänen ein eigener SMTP-Connector eingerichtet wird, der den Adressraum des Kunden enthält und als Relay freigeschaltet wird.

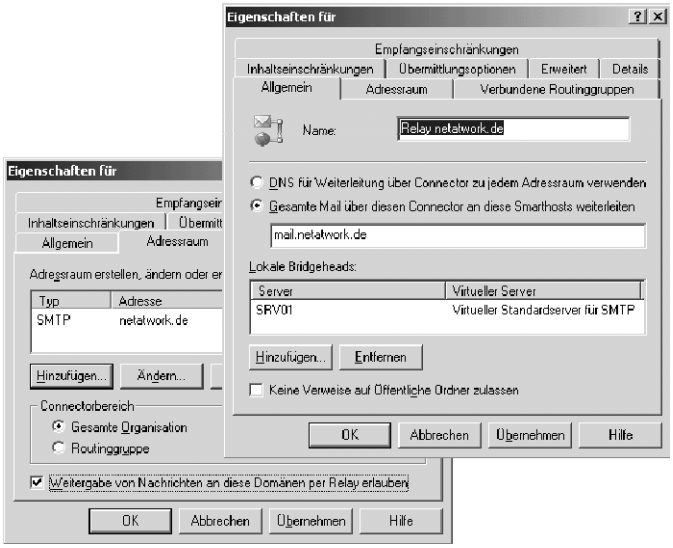


Abbildung 11.5 SMTP als Relay weiterleiten

Ein Eintrag in den Empfängerrichtlinien ist hierzu nicht notwendig. In der erweiterten Konfiguration des Connectors wird dazu die IP-Adresse oder ein Hostname des Kunden eingetragen, an den die Nachrichten weitergeleitet werden sollen (Smarthost). Die Zustellung über DNS ist meist ungeeignet, da der MX-Record auf den Exchange-Server selbst verweist. Die dynamischen Verbindungen eines Kunden sind über dynamische DNS-Einträge, VPN und ATRN möglich.

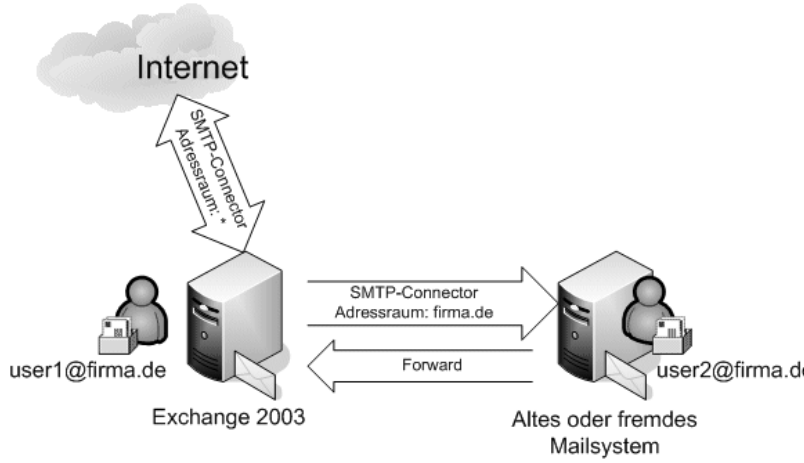
Die gleichen Einstellungen eignen sich auch, wenn ein Konzern alle Nachrichten für eine Tochter mit Exchange 2003 annimmt und an den unabhängigen E-Mail-Server der Firmentochter weiterleitet.

- Exchange leitet E-Mails an unbekannte Empfänger weiter

Interne Weiterleitung an gleiche SMTP-Domäne

Die zweite Art der Anbindung berücksichtigt, dass es sowohl in Exchange als auch in dem anderen E-Mail-System Empfänger gibt, die die gleiche SMTP-Domäne nutzen. In diesem Fall muss diese SMTP-Domäne für Exchange 2003 in einer Empfängerrichtlinie aufgeführt, aber nicht autoritativ sein. Achtung: Die primäre SMTP-Adresse der *Standard-Richtlinie* darf nie in einer anderen Richtlinie als „nicht autoritativ“ außer Kraft gesetzt werden (siehe Konzepte „RUS und Empfängerrichtlinien“). Zusätzlich wird Exchange mit einem SMTP-Connector der Weg zu dem alternativen E-Mail-System mitgeteilt, da die MX-Einträge im DNS in der Regel auf den Exchange 2003-Server selbst verweisen und damit eine Schleife entstehen würde. Hierfür eignet sich ein SMTP-Connector, in dem die E-Mail-Weiterleitung über den Adressraum und den Smarthost gesteuert wird.

Abbildung 11.6 Unbekannte Empfänger weiterleiten



Das fremde E-Mail-System sollte die ausgehenden Nachrichten für die eigene SMTP-Domäne, zu der es keine lokalen Benutzer findet, an Exchange senden. Somit sind die Exchange 2003-Postfächer mit der gleichen SMTP-Domäne erreichbar. Sendet dieser E-Mail-Server alle Nachrichten an Exchange 2003, muss Exchange dieses System als Relay zulassen. Die Relay-Einstellung kann über die IP-Adresse des fremden E-Mail-Servers oder eine Authentifizierung erfolgen.

Diese Konfiguration ist häufig auch bei der Exchange 2003-Migration von einem anderen E-Mail-Server ohne Connector notwendig.

- Fremde Personen sind Exchange Kontakte im Active Directory

Weiterleitung an Kontakte

Personen auf einem anderen E-Mail-System lassen sich in Exchange 2003 als Kontakte im Active Directory eintragen. Werden diese Kontakte auch für Exchange „enabled“ sind, ist der Empfang von E-Mails für sie sichergestellt. Beim Kontakt selbst ist eine E-Mail-Adresse zu pflegen, an die die Nachrichten weitergeleitet werden. Dieser Ablauf stellt eine praktikable Lösung dar, um Benutzer auf anderen E-Mail-Systemen mit deren eigener SMTP-Domäne zu erreichen.

In dieser Konstellation ist ein SMTP-Connector nicht zwingend erforderlich, vorausgesetzt Exchange kann diese andere Domäne über DNS auflösen (MX-Eintrag). Der Einsatz eines SMTP-Connectors ist sinnvoll, um Exchange 2003 einen direkten Leitweg über einen Smarthost aufzuzeigen. Bei internen Systemen findet somit kein Versand über das Internet statt.

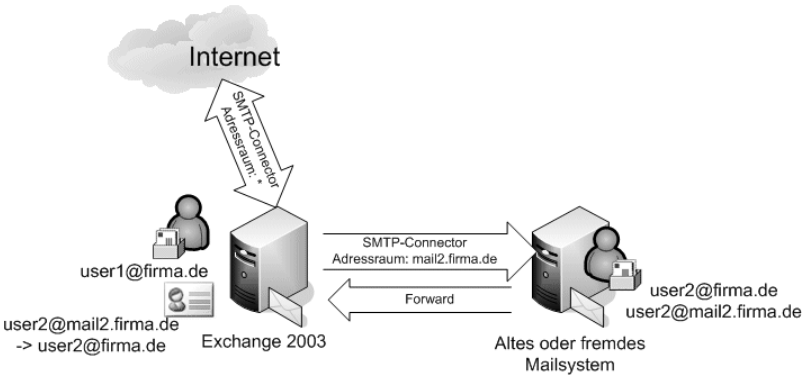


Abbildung 11.7 Adressraum mit Kontakten verbinden

Reply-Adresse anpassen

Allerdings sollte der Anwender auf dem weiteren E-Mail-System seine Antwortadresse entsprechend anpassen, damit ausgehende Nachrichten korrekt beantwortet werden können. Sofern das andere E-Mail-System eine Möglichkeit bietet, die Adressen der Postfächer über LDAP auszulesen, sollten Sie eine Verbindung mit dem Active Directory Connector prüfen, so dass die Adressen automatisch abgeglichen werden (Inter-Org-Verbindungsvereinbarungen).

- Kopplung per Connector

  Spezielle Connectoren verbinden E-Mail-Systeme

  Die Anbindung mit einem Connector ist eine Sonderform der Anbindung mit Kontakten. Statt des SMTP-Connectors kann mit den Exchange 2003-Connectoren für Notes und GroupWise eine enge Anbindung dieser beiden fremden E-Mail-Systeme erreicht werden. Bestandteil des Connectors ist ein Verzeichnisabgleich der Adressen, so dass jedes Postfach in Notes oder Groupwise im Active Directory korrekt als Kontakt mit der jeweiligen E-Mail-Adresse eingetragen wird. Über diese Anbindung können Sie die Postfächer der Fremd-Systeme ebenfalls per E-Mail aus dem Internet sowie von den Exchange-Benutzern erreichen. Einen wesentlichen Vorteil bietet hierbei die optimale Konvertierung der E-Mail-Formate über die Connectoren. Zudem sind alle Empfänger der Organisation im Adressbuch sichtbar, können in Verteiler aufgenommen werden und Nachrichten an ungültige Empfänger werden sehr früh als unzustellbar zurückgewiesen. Der Aufwand für die manuelle Pflege und Anpassung der Kontakte entfällt.

Diese verschiedenen Varianten werden bei der Verbindung von Exchange mit anderen E-Mail-Systemen häufig eingesetzt und erlauben bei einer Migration von Fremdsystemen die notwendige Flexibilität.

Exchange-Postfach stellt Active Directory-Benutzer dar

In allen Fällen ist Exchange das primäre Nachrichten-System, welches ähnlich einem Stellwerk die Nachrichten an das richtige System verteilt. Vergleichbare Lösungen sind natürlich auch mit anderen E-Mail-Systemen möglich. Allerdings bietet Exchange den Vorteil, dass die Einträge im Active

Directory zugleich für die Anmeldung an Arbeitsstationen und Server genutzt werden können. Die Anwender der fremden E-Mail-Systeme verfügen gleichzeitig auch über Benutzerkonto im Active Directory. Somit bietet es sich gerade zu an, Exchange als zentralen Routing-Server im Unternehmen einzusetzen.

11.6 Administrative Gruppen

Administrative Gruppen erlauben es, mehrere Server logisch zu gruppieren, so dass bestimmte Personenkreise diese eigenverantwortlich verwalten können. Bei einer Migration von Exchange 5.5 in der gleichen Organisation wird aus jedem Exchange 5.5-Standort eine Administrative Gruppe. Dies entspricht am ehesten den Berechtigungskonzepten der Exchange 5.5-Umgebung.

In Exchange 2003 bedeuten die Administrative Gruppen (AG) ebenfalls die Grenze für bestimmte administrative Tätigkeiten und Zugriffe auf Konfigurationen und Datenspeichern. Die Konfiguration von Empfängerrichtlinien und Nachrichteneinstellungen werden global definiert und erfordern erweiterte Berechtigungen.

AG erstellen

Die meisten Unternehmen kommen beim Neuaufbau einer Exchange-Organisation mit einer Administrativen Gruppe aus. Weitere Administrative Gruppen werden erst eingerichtet, wenn der tatsächliche Bedarf und ein entsprechendes Berechtigungskonzept hierfür bestehen. Die Anlage einer weiteren Administrativen Gruppe ist im Exchange System-Manager in wenigen Sekunden erledigt (NEU — ADMINISTRATIVE GRUPPE).

Im gemischten Betriebsmodus können die Routinggruppen nur Server der gleichen Administrativen Gruppe beinhalten. Erst im Exchange-Native Mode können Routiggruppen auch die Server aus verschiedenen Administrativen Gruppen enthalten.

Besonderheit: Migrations-umgebungen

Falls Ihre Administrativen Gruppen aus einer Exchange 5.5-Migration stammen, sollten Sie später die Zusammenführung in eine Administrative Gruppe überlegen. Im Exchange 2003-Native Mode ist es problemlos möglich, Postfächer von einem Server einer Administrativen Gruppe auf den anderen Server in einer anderen Administrativen Gruppe zu verschieben. Sie können über diesen Umweg einen Server leeren und diesen letztlich deinstallieren. Allerdings ist es nicht möglich, nachträglich einen Server in eine andere Administrative Gruppe zu verschieben. In dieser Situation können Sie die Leap-Frog-Methode anwenden. Dazu installieren einen temporären Exchange 2003-Server und verschieben die Inhalte und Funktionen. In einem zweiten Schritt entfernen Sie den alten Server und installieren ihn neu in der gewünschten Administrativen Gruppe. Dann

verschieben Sie alle Inhalte und Funktionen vom temporären Server wieder auf den neu installierten Server zurück.

11.7 Externe NT4-Domäne oder anderer Forest

Solange alle Exchange 2003-Anwender im gleichen Active Directory-Forest als Benutzer existieren, ist die Zuordnung eines Exchange-Postfachs problemlos möglich. Allerdings gibt es auch Situationen, in denen die Anwender ein Postfach in Ihrer Exchange 2003-Organisation erhalten sollen, aber kein aktives Konto im gleichen Active Directory-Forest besitzen. Dieser Fall tritt auf, wenn die Anwender noch mit einer Windows NT 4-Domäne arbeiten oder ein Domänenkonto in einem anderen Forest nutzen.

Placeholder-Account

Exchange 2003 benötigt zwingend ein Benutzerkonto im gleichen Active Directory-Forest, um die E-Mail-Adresse und die Verbindung zum Postfach in der Datenbank zu speichern. Exchange 2003 trägt dieser Konstellation dadurch Rechnung, dass ein entsprechender Active Directory-Benutzer angelegt, aber nicht für eine interaktive Anmeldung freigeschaltet wird. Diese deaktivierten Konten sind Platzhalter für die Exchange-Informationen und unterscheiden sich ansonsten nicht von den „normalen“ Postfach-Benutzern, die auch zur Anmeldung an Windows genutzt werden.

Trust einrichten

Exchange 2003 behandelt alle deaktivieren (mailbox-enabled) Konten als Platzhalter für Anwender in vertrauten NT4-Domänen oder anderen Forests mit Vertrauensstellungen. Voraussetzung ist eine gültige SID, anhand Exchange die Berechtigung ausliest und zuordnen kann. Bei einem deaktivierten AD-Konto liest Exchange nicht die SID des Objekts, sondern nutzt die SID, welche in dem Feld „msExchMasterAccountSID“ beim Benutzer hinterlegt ist. Zusätzlich wird dem externen Konto der vertrauten Domäne das Recht gegeben, das Postfach des deaktivieren Active Directory-Kontos zu nutzen Über die Vertrauensstellung (Trust) kann auf die SID des Benutzers-Anmeldekontos zugegriffen werden.

Diese Einstellungen sind in den Eigenschaften des Benutzers unter den Postfachberechtigungen einzusehen.

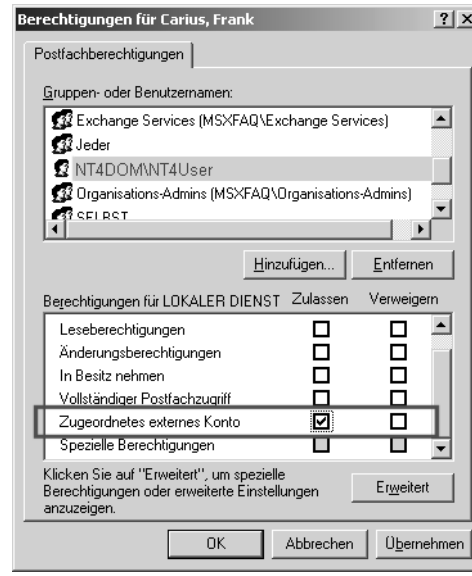


Abbildung 11.8 Associated External Account

Postfach-Besitzer zuordnen

Mit der Option ASSOCIATED EXTERNAL ACCOUNT wird in dem zusätzlichen Attribut „msExchMasterAccountSID“ des deaktivierten Benutzers die SID des eigentlichen NT4-Kontos der vertrauten Domäne hinterlegt. Dieses Feld ist ebenfalls Bestandteil des Globalen Katalogs. Sobald ein Client mit seinem externen Anmeldekonto eine Anfrage an Exchange stellt, kann der Exchange-Server diesen Benutzer dem deaktivieren AD-Konto zuordnen und den Zugriff anhand der Berechtigungen gewähren. In der Microsoft TechNet wird diese Vorgehen erläutert (Artikel 278888 „How to associate an Exchange 2000 Mailbox with a Windows NT 4.0 Account“.)

ADC weist externes Konto zu

Eine wichtige Rolle bei der Anlage solcher Konten spielt der Active Directory Connector. Wird in einer Exchange 5.5-Umgebung mit NT4-Domänen zuerst das Postfach nach Exchange 2003 migriert, ehe die Benutzer in das Active Directory übernommen wurden, legt der ADC genau diese deaktivieren Konten mit dem zugeordneten externen Konto an.

Werden die NT4-Domänenkonten erst später, z.B. mit dem Programm ADMT, in das Active Directory überführt, können Sie mit dem Programm „Assistent für die Active Directory Kontenbereinigung“ (ADCleanUp) die Exchange Eigenschaften der deaktivierten Benutzer den migrierten Anmeldekonten zuweisen. Beachten Sie dabei auch die 1:1-Beziehung von Postfach zu AD-Konto, die in Exchange 5.5 durch das *Primäre Windows NT-Konto* dargestellt wird.

Diese Sonderbehandlung der deaktivieren Konten hat natürlich auch Auswirkungen auf den normalen Betrieb. Sobald ein Active Directory-Konto aus anderen Gründen deaktiviert wird, versucht Exchange die SID des „Associated External Accounts“ zu lesen, die jedoch dann nicht existiert. Die

E-Mails an dieses Postfach werden als unzustellbar abgewiesen. Als Lösung können Sie den Self-Account „SELBST“ als externes Konto eintragen.

Wird umgekehrt versehentlich ein deaktivierter Exchange-Benutzer mit einem solchen externen Konto aktiviert, entfernt die Management-Konsole die Einträge und Berechtigungen in Exchange. Ein einfaches erneutes Deaktivieren korrigiert dies nicht. Sie müssen manuell die Einträge korrigieren. Exchange 2003 bietet auch hierbei eine Unterstützung durch den Exchange Assistent.

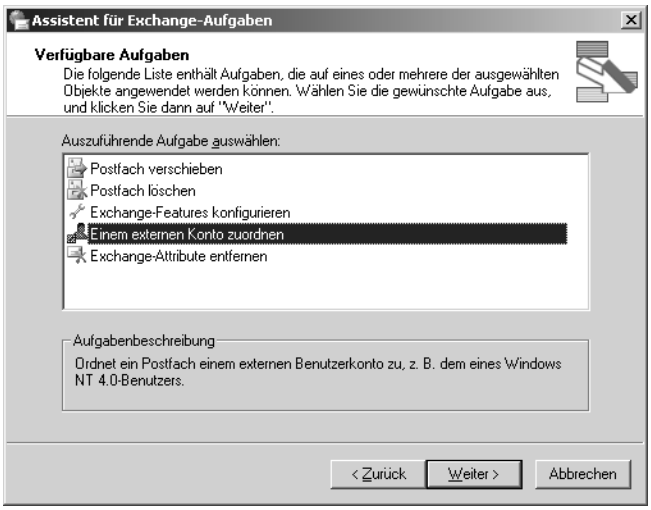


Abbildung 11.9 Externes Konto zuweisen

Single-Logon erfordert Trust

Gibt es zwischen der NT4-Domäne und dem Active Directory keine Vertrauensstellung, dann kann das Active Directory-Konto nur als aktivierter Benutzer eingerichtet werden. Der NT4-Anwender erhält den Zugriff auf sein Postfach nur über einen weiteren Benutzernamen mit Kennwort. Dies entspricht natürlich nicht dem Ansatz eines „Ein Benutzer = ein Konto“-Konzepts und wird in Firmen nicht gerne angewendet. Anbieter von Exchange-Hosting-Umgebungen nutzen diesen Weg jedoch für ihre Kunden.

11.8 Fax-Versand und -Empfang

Exchange 2003 beinhaltet, wie alle vorherigen Exchange-Versionen, keinen eigenen Faxserver. Wenn eine Ihrer Anforderungen lautet, eingehende Faxe in Exchange zuzustellen und aus Outlook ebenfalls Faxe zu versenden, müssen Sie die Anschaffung einer zusätzlichen Software vorsehen.

Die Einbindung der verschiedenen Faxlösungen ist je nach Programm unterschiedlich gelöst. In den meisten Fällen ist der Faxserver ein eigenständiges Produkt, das auch ohne Exchange-Anbindung funktioniert. Dies ist wichtig, da es neben Exchange und Outlook auch andere Prozesse gibt, die von einem

Faxserver profitieren, z.B. Anwender, die über einen Druckertreiber ein Fax versenden.

Fax-Connector

Die Anbindung an Exchange erfolgt häufig über einen Connector, der Exchange um den Adressraum „FAX“ erweitert. Outlook erkennt die Fax-Verarbeitung in Exchange und bietet Ihnen automatisch alle Fax-Adressen der Kontakte als gültige Empfänger an. Der Faxserver selbst ist für die formatgetreue Konvertierung der Nachrichten verantwortlich. Spätestens, wenn Anlagen an einer E-Mail über diesen Weg versendet werden, sind die Konvertierungsleistungen des Faxservers gefragt.

Umgekehrt kann jedes Postfach in Exchange eine Adresse vom Typ „FAX“ erhalten. Viele Faxserver lesen diese Information aus, um eingehende Faxe anhand dieser Durchwahlziffern einem Postfach zuzustellen.

Fax an SMTP-Adresse

Andere Anbieter nutzen die SMTP-Funktion von Exchange um über diesen Weg die Fax-Nachrichten zuzustellen und abzuholen. Bei dieser Methode können Nachrichten an Faxgeräte z.B. mit „Rufnummer@fax“ erstellt werden. Ein passender Connector sendet diese E-Mails per SMTP an einen Fax-Server, der die Domäne „fax“ bedient.

Fax-Datenbank versus AD-Einträge

Die zweite Komponente einer Anbindung ist der Abgleich mit den Verzeichniseinträgen im Active Directory. Die meisten Faxserver pflegen eine eigene Datenbank mit den Benutzern und den Zuordnungen zur Faxnummer, die oft auf einer Telefon-Lösung basieren. Allerdings ist es von Vorteil, wenn der Faxserver diese Einträge auch mit dem Active Directory abgleichen kann. Die Pflege der Fax-Durchwahl und -optionen im Active Directory wird mittels eigener Karteikarten oder vorhandenen Feldern erleichtert Einige Faxserver verzichten sogar komplett auf eine eigene Datenbank und halten alle Konfigurationen im Active Directory. Dies ist jedoch oft mit einer Schemaerweiterung verbunden.

Der Übertragungsweg zum Telefonnetz wird heutzutage mit ISDN-Karten oder speziellen Faxkarten realisiert. Die wenigsten Firmen arbeiten mit analogen Modems, und der Versand über das Internet zu einem Fax-Dienstleister steht erst am Anfang. Die früheren Diskussionen über das Pro und Kontra der verschiedenen Faxkarten sind aufgrund der stark gestiegenen Rechnerleistung nahezu hinfällig. Spezialisierte Faxkarten haben immer noch den Ruf der besseren Kompatibilität zu den verschiedenen Gegenstellen, aber auch einfache günstigere ISDN -Karten sind überwiegend problemlos im Einsatz.

Windows 2003-Fax-Dienst

Windows 2003 selbst bringt auch einen einfachen Faxserver mit, der eingehende Faxe sogar per SMTP versenden kann. Damit können Sie, ohne zusätzliche Kosten, in kleinen Umgebungen den Empfang von Faxen an eine E-Mail-Adresse ermöglichen. Das Ziel könnte z.B. ein Öffentlicher Ordner sein.

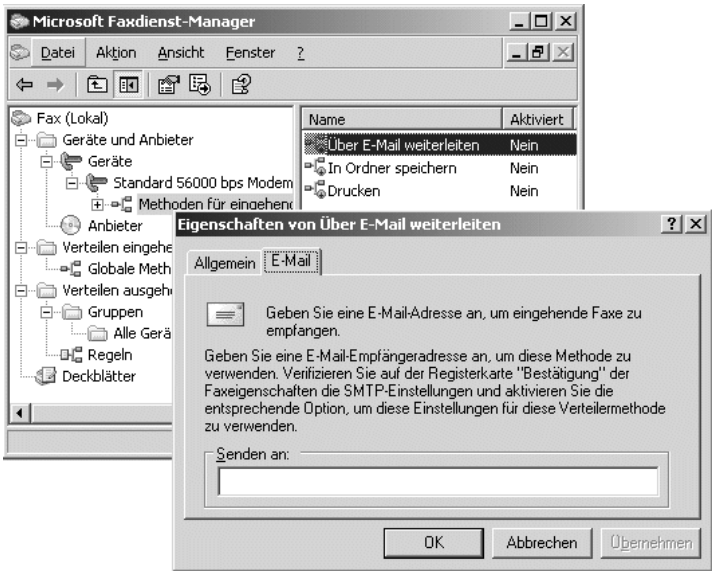


Abbildung 11.10 Eingehende Faxe an eine E-Mail-Adresse senden

Das Zustellen von Faxen anhand von Durchwahlen und anderen Kriterien leistet dieser Server jedoch nicht. Die Anbindung beschränkt sich darauf, eingehende Faxe optional per SMTP an einen Empfänger in Exchange zu senden, und ausgehende Faxe ebenfalls per E-Mail zu quittieren. In der Musterumgebung wurde kein Faxserver installiert. Der Windows 2003-Faxdienst nutzt einfache Modems. Andere Fax-Produkte für Einzelplatzsysteme können ebenfalls eingehende Faxe per SMTP an einen Server senden, oder Skripte ausführen, die das Fax an Exchange weiterleiten. Die Windows-Lösung stellt keinen Einsatz für einen vollwertigen Fax-Server dar.

11.9 SMS-Versand

Short Message Services (SMS) und zusätzlich die neu verfügbaren Multimedia Messaging Service (MMS) bieten die Möglichkeit, schnell und einfach kurze Nachrichten auf ein Mobiltelefon zu senden. Aber SMS und MMS sind nicht nur dazu da, Bilder und Texte zu übertragen, sondern auch, um Programme und Dienste zu informieren. So nutzt der Outlook Mobile Server (OMA) von Exchange 2003 diese Möglichkeit, Endgeräte über neue Nachrichten zu informieren. Diese können dann eine Synchronisation über ActiveSync durchführen.

Exchange 2003 enthält, wie alle vorhergehenden Exchange-Versionen, keinen Dienst zum Versand von SMS Nachrichten. Möchten Sie über neue eingehende Nachrichten per SMS informiert werden, oder selbst SMS Nachrichten aus Outlook an andere Personen senden, dann benötigen Sie ein

Drittprodukt und eine entsprechende technische Anbindung an ein SMS Message Center (SMSC). Auch für die Integration in Exchange gibt es mehrere verschiedene Varianten, die je nach dem zu erwartenden SMS-Aufkommen und dem Nutzung auszuwählen sind.

Individueller SMS-Empfang

Als Inhaber eines Mobiltelefons haben Sie mehrere Wege zur Auswahl, um anderen Personen Ihre Erreichbarkeit per SMS zu erlauben:

SMS an spezielle Rufnummer

- SMS über Mobilfunkanbieter

  Die meisten Anbieter erlauben den Versand einer E-Mail an die SMTP-Adresse „Rufnummer@smsdomäne.tld“. Der Mobilfunk-Provider empfängt die Nachricht und sendet diese an den Teilnehmer. Die Kosten trägt hier der Empfänger. Diese einfache Möglichkeit muss daher vom Empfänger erst freigeschaltet werden, und ist aufgrund der Zunahme von Spam-Nachrichten nicht ganz ungefährlich, im Hinblick auf Kosten und Störungspotenzial. Es bietet jedoch eine einfache Lösung, einem Kunden die SMS-Erreichbarkeit des Mobilfunkteilnehmers zur Verfügung zu stellen. Alle großen deutschen Mobilfunk-Provider bieten Ihnen diese Möglichkeit an.

- SMS über Internet Provider

  Die kommerziellen Ableger der E-Mailboxen von GMX, WEB.DE und anderen Anbietern erlauben die Weiterleitung von Nachrichten per SMS an eine Mobilrufnummer. Sie können bei diesen Providern ein Postfach anmelden und dessen SMS-Benachrichtigungsfunktion nutzen. Dieser Weg eignet sich eher für einzelne Personen, die so eine SMS Funktion für einzelne Telefone einrichten.

Alle bisher vorgestellten Wege dienen dazu, dass lediglich eine Person per SMS erreichbar ist.

Einzelplatz SMS

Programm am Client

Möchten Sie eine Vielzahl von SMS-Empfängern erreichen, sind andere Wege gefragt. Sofern nur wenige Benutzer eine Nachricht per SMS versenden, ist eine Installation einer entsprechenden Software auf dem PC vielleicht schon ausreichend. Ein geeignetes Programm ist oft beim Funktelefon enthalten. Auch Microsoft bietet eine Software an (http://go.microsoft.com/?linkid=247348).

Ebenso könnte dieser Anwender über eine Weboberfläche bei einem der vielen Dienstleister im Internet die SMS versenden. Mit einer Exchange Anbindung hat dies noch nichts zu tun.

Server SMS

SMS-Versand über E-Mail-Server

In Verbindung mit Exchange 2003 ist es für Sie interessante, möglichst alle Mobilfunkteilnehmer über SMS zu erreichen, ohne dass diese entsprechende Vorkehrungen treffen müssen. Folgende Wege sind hier nutzbar:

- SMS Gateway und Handy

  Eine Software wird auf dem Exchange-Server als Gateway eingerichtet und kommuniziert auf der anderen Seite mit einem angeschlossenen Mobiltelefon. Das Gateway nimmt alle Exchange-Nachrichten vom Typ „SMS“ an, und leitet diese als SMS an die angegebene Rufnummer weiter. Das genutzte Protokoll zwischen Handy und PC ist sehr einfach, es reichen einige AT-Befehle hierzu aus. Der Nachteil dieser Lösung beruht auf die relativ hohen Kosten per SMS und die Notwendigkeit eines Mobilfunkvertrages. Zudem gibt es Vorbehalte gegen den Betrieb eines Mobilfunksenders in einem Rechenzentrum.

- SMS über SMSC

  Verfügbare SMS-Gateways für Exchange nutzen daher die Möglichkeit, die Nachricht direkt beim Short Messaging Center des Providers einzuliefern. Eine ISDN-Karte oder X.25-Verbindung, und immer häufiger auch Internet-Verbindungen, erlauben die Übermittlung von SMS-Nachrichten, ohne ein lokal angeschlossenes Handy. Der erhöhte Aufwand ist durch geringere Kosten pro SMS gerechtfertigt. Dies rechnet sich erst ab einer großen Menge an SMS Nachrichten.

- SMS über Provider

  Da nun nicht jede Firma in Kommunikations-Hardware und -leitungen investiert, bieten Dienstleister diese Übertragung an. Ihr Exchange-Server sendet dabei die Nachrichten primär per SMTP an das Internet-System des Dienstleisters, das die Nachrichte als SMS weiterleitet. Neben einem Internet-Anschluss benötigen Sie keine weiteren Einrichtungen. Der Provider autorisiert ihren Server z.B. anhand der IP-Adresse, oder durch eine Anmeldung mit Kennwort und Benutzername. Einige Provider nutzen die Absenderadresse als Schlüssel, was in Zeiten von Viren jedoch nicht mehr zuverlässig ist.

Bevor Sie daher ein Budget für Software, Hardware und Betrieb einplanen, sollten Sie die voraussichtliche Anzahl der SMS-Nachrichten pro Monat ermitteln, und prüfen, ob dies dem Gegenwert für Installationskosten entspricht. Gerade für Administratoren bedeutet die Benachrichtigung per SMS bei Systemfehlern eine interessante Handhabe, frühzeitig über Probleme informiert zu werden.

Gerade der Versand über das Internet an einen Serviceprovider in Verbindung mit einem Outlook-Formular ist oftmals ein günstiger und schnell zu realisierender Weg.

SMS Empfangen

Zuletzt ist noch die Frage zu klären, wie Sie einen SMS-Empfang realisieren können. Falls Sie eine SMS versenden, kann der Empfänger ohne weiteres darauf antworten. Abhängig von der entsprechenden Lösung kommt diese Antwort sogar wieder bei Ihnen an. Prüfen Sie auch hier den Bedarf und dann die Möglichkeiten anhand verschiedener Kriterien wie Kosten, Anforderungen und Alternativen.

In der Praxis ist der Empfang meist weniger wichtig. Die meisten Mobilfunkanbieter erlauben mittlerweile, dass Mobilfunkteilnehmer per SMS auch eine E-Mail erstellen und versenden können. Infolgedessen ist jeder Benutzer mit einer Internet-Adresse ohne weitere Installationen auch von mobilen Geräten aus erreichbar. Die Kosten fallen hierbei beim Absender der SMS an.

11.10 OWA und OMA aus dem Internet

In der Musterumgebung wurde Outlook Web Access bereits so konfiguriert, dass eine Verbindung mit SSL-Verschlüsselung möglich ist, und auch eine Anmeldung mit Klartextkennworten erlaubt ist. Für den Zugriff aus dem Internet sind weitere Schritte notwendig.

Namensauflösung

Alias einrichten

Sie sollten Ihren Anwendern nicht zumuten, sich kryptische IP-Adressen zu merken, um OWA aus dem Internet-Cafe zu nutzen. Daher ist die Registrierung eines passenden Namens im Internet für den Server ratsam, wie z.B. „owa.firma.de“. Der Name ist entscheidend für ein später auszustellendes Zertifikat. Dieser Name wird aus dem Internet zu einer offiziellen IP-Adresse aufgelöst, unter der Ihr Exchange 2003-Server direkt oder indirekt zu erreichen ist. Besitzt Ihr Netzwerk keine festen IP-Adressen besitzt, ist der Umweg über dynamische DNS-Einträge ein möglicher Lösungsweg, um trotzdem OWA zu nutzen.

Die Sicherheit

Filter einsetzen

Zwischen dem Internet und Ihrem Exchange Server sind weitere Systeme für die OWA/OMA-Nutzung zu konfigurieren. Eine direkte Internetanbindung des Exchange-Servers oder die Weitergabe der Pakete über die Adressumsetzung eines Routers (Port 80/443) bedeuten einen vollständigen und unsicheren Webzugriff auf alle Web-Verzeichnisse des Servers. Auch die Absicherung des IIS bedeutet keinen dauerhaften Schutz. Ergänzen Sie den Exchange-Server um weitere Webdienste wie Windows 2003 Share Point Team Services, sind diese Dienste ebenfalls von extern erreichbar. Ihr

Ziel muss daher die Filterung der eingehenden Anfragen sein, damit nur Zugriffe über die gewünschten URLs möglich sind. Mit dem IIS6 ist das Modul „URLSCAN“ ein mögliches Hilfsmittel, um die eingehenden HTTP-Requests zu filtern. Auch für den IIS5 gibt es URLSCAN als Bestandteil des Programms IISLOCKD.

Zweiter virtueller Server

Ein solcher Filter kann aber auch wichtige interne Verwaltungsfunktionen und eigene Webseiten des IIS stören. Sie sollten daher einen weiteren virtuellen HTTP-Server mit einer eigenen IP-Adresse aufsetzen, und dort explizit die Exchange Funktion aktivieren. Eingehende Anfragen müssen dann auf diese IP-Adresse umgeleitet werden. Die Standardwebseite ist dann nicht mehr aus dem Internet erreichbar. Der Einsatz von URLSCAN ist trotzdem ratsam. Diese Vorgehensweise ist jedoch nur für sehr kleine Firmen, mit geringen Anforderungen an die Sicherheit, ausreichend.

ISA-Server oder anderer Reverse-Proxy

Bei höheren Anforderungen an die Sicherheit sollten Sie vor dem eigentlichen Exchange-Server einen weiteren Dienst schalten. Dieser Dienst-Server nimmt die Anfragen der Clients an und leitet sie, nach einer entsprechenden Überprüfung, an den Exchange Server weiter. Diese Funktion kann z.B. der *Microsoft ISA-Server* Übernehmen. Alle externen Anfragen werden vom ISA-Server angenommen und analysiert. Dieser Reverse-Proxy prüft die URLs auf die Verzeichnisse /EXCHANGE, /EXCHWEB, /PUBLIC, /OMA oder /Microsoft-Server-ActiveSync, deren Daten durch den ISA-Server vom internen Server angefordert werden. Nebenbei kann der ISA-Server dank des Caches den Exchange Server von der Arbeit der SSL-Verschlüsselung sowie der Lieferung statischer Inhalte (Bilder, StyleSheets etc.) entlasten.

Oftmals ist solch ein Server bereits vorhanden, da er die Zugriffe von innen in das Internet kontrolliert und Anfragen mit einem Cache beschleunigt.

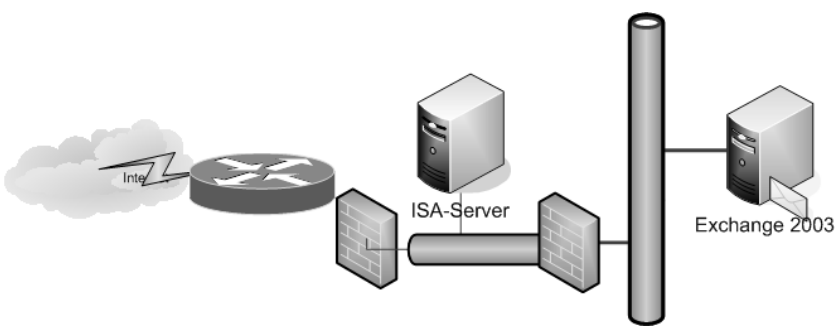


Abbildung 11.11 ISA veröffentlicht einen Exchange-Server

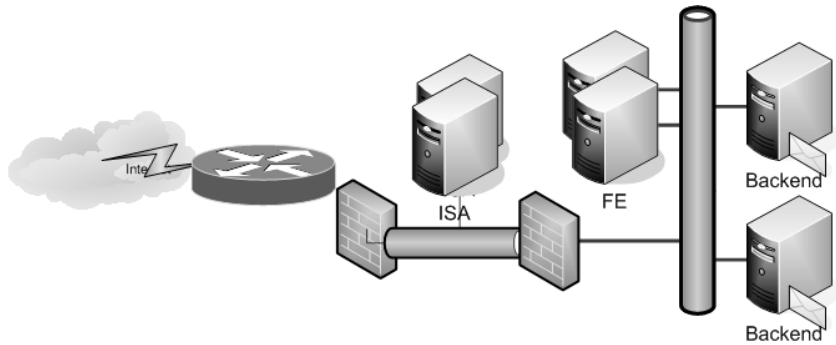
Diese Art der Anbindung ist für die meisten Firmen der erste und einfache Weg, einen Exchange 2003-OWA abgesichert zu betreiben.

Wer braucht einen Front-End-Server?

Nutzen Sie bereits ISA-Server für eine sichere Veröffentlichung, dann stellt sich Ihnen die Frage: Wozu ist ein Front-End-Server notwendig?

Der Microsoft ISA-Server kann, wie jeder anderer Reverse-Proxy, nicht ermitteln, auf welchem der vielen internen Exchange-Server sich das Postfach des Benutzers befindet. Die Weiterleitung mittels Proxy erfolgt immer nur auf genau einen Server. Betreiben Sie nun mehrere Postfachserver (Back-End-Server) im internen Netzwerk, würde dies bedeutet, dass Sie für jeden internen Server eine eigene externe Umleitung schalten müssten.

Abbildung 11.12 ISA mit Front-End-Server



Hier kommt der Front-End-Server ins Spiel! Dieser nimmt wie ein Proxy alle Anfragen an und leitet sie an den zuständigen Postfachserver weiter. Der Front-End-Server ähnelt in der Funktion ebenfalls einem Reverse-Proxy Server, mit dem Unterschied, dass dieser Server die Benutzer-abhängige Weiterleitungen zum richtigen Back-End-Server durchführt.

Load-Balancing

In größeren Installationen werden zur Skalierung und Ausfallsicherheit mehrere Front-End-Server nebeneinander aufgestellt, und z.B. mit NLBS zusammengeschaltet. Auch ISA-Server lassen sich zur Ausfallsicherheit und zur Skalierung als Gruppe betreiben. Nur das Postfach liegt immer auf genau einem Exchange 2003-Back-End-Server.

Administratoren, die in einer Migrationsumgebung mehrere Exchange-Versionen einsetzen, sollten die Zusammenarbeit der verschiedenen Exchange- und OWA-Versionen kennen. Ein Exchange 5.5-OWA-Server ermöglicht aufgrund der MAPI-Schnittstelle ebenfalls einen Zugriff auf Exchange 2000/2003-Back-End-Server. Aufgrund von Inkompatibilitäten von Outlook 2003 mit Exchange 5.5 sollten Sie jedoch die aktuellsten Updates und Fixes für Exchange 5.5 installieren.

Front-End-Server	Back-End-Server	Version OWA
Exchange 2000	Exchange 2000	Exchange 2000
Exchange Server 2003	Exchange 2000	Exchange 2000
Exchange 2000	Exchange Server 2003	nicht supported
Exchange Server 2003	Exchange Server 2003	Exchange Server 2003
Exchange 5.5	Exchange 2000	Exchange 5.5
Exchange 5.5	Exchange 2003	Exchange 5.5

Tabelle 11.1 Zusammenspiel Front-End-/Back-End-Server

Allerdings ist der Einsatz eines Exchange 5.5 Servers als OWA-Server mit starken Einschränkungen in der Funktion verbunden, so dass Sie einen Exchange 2003 Front-End-Server vorziehen sollten.

11.11 Verbindung zu „vertrauten“ Firmen

Das Internet erlaubt einen schnellen und unkomplizierten Nachrichtenaustausch beliebiger Firmen und Personen untereinander. Die offene Funktion des Internets stellt zugleich auch die größte Schwäche dar. Jede Person kann an jedes andere Postfach eine Nachricht versenden, und diese wird ohne besondere Schutzvorkehrungen, ähnlich einer Postkarte, übertragen.

Geschützte Nachrichten-Übertragung

In der Realität pflegen einige Unternehmen eine sehr enge Beziehungen, und der Nachrichtenaustausch mit diesen Partnern, Töchtern, Lieferanten oder Abnehmern sollte optimiert werden. Dies betrifft sowohl die Möglichkeit, eigene besondere Transportwege zu nutzen, als auch die Übertragung durch eine Verschlüsselung etc. zu sichern.

Eigene Verbindungen oder VPN

Zwischen zwei Unternehmen kann eine direkte Kopplung der Netzwerke erfolgen. So bauen viele Firmen eigene WAN-Verbindung zu festen Lieferanten und Kunden auf. Diese Verbindungen sind entsprechend abgesichert, verfügbar und vom Internet unabhängig. Die verfügbare Bandbreite ist somit planbar und eine mögliche Verschlüsselung der Daten erhöht die Sicherheit.

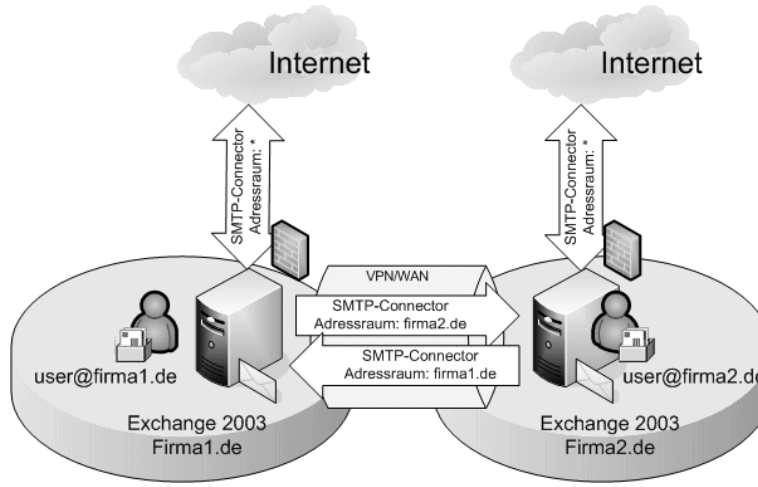
Ohne entsprechende Konfiguration nutzt Exchange 2003 diese Verbindungen nicht. Entsprechend der Internetanbindung werden die E-Mails immer über das Internet zur Partnerfirma übermittelt.

Die direkte Nachrichtenübertragung an Partnerfirmen können Sie mittels akrobatischen Konfigurationen auf dem DNS-Server einrichten, oder Sie legen dafür einen SMTP-Connectors in Exchange 2003 an. Über den

Adressraum können Sie steuern, für welche SMTP-Domänen dieser Connector zuständig ist und an welches Zielsystem die Nachrichten übermittelt werden.

Diese logische Verbindung zwischen den Partnerfirmen muss nicht unbedingt eine eigene physikalische Leitung darstellen. Auch eine VPN-Verbindung über das Internet ist möglich, solange die beiden E-Mail-Server sich über TCP/IP erreichen.

Abbildung 11.13 Verbindung von Partnern mit einem privaten SMTP-Link



Sicheres SMTP/TLS

Selbst über das Internet sind ohne VPN verschlüsselte Verbindungen zu Partnerfirmen möglich, vorausgesetzt beide E-Mail-Server erreichen sich via TCP/IP. Über die Aktivierung der SSL-Verschlüsselung für SMTP, mittels Transport Layer Security (TLS), können die Verbindungen gesichert werden. Allerdings sind diese Methoden etwas aufwändiger, da entsprechende Zertifikate zu beantragen und einzutragen sind.

Exchange 2003 unterstützt die Verschlüsselung von Nachrichten auf dem SMTP-Transportweg. Ähnlich einer sicheren Verbindung mit dem Webbrowser, können Sie auch E-Mail-Server mit Zertifikaten ausstatten, und die Daten werden per SSL übertragen.

Für die sichere Übertragung zu einem Partner sind, neben der direkten Kommunikation der beiden E-Mail-Server, vertrauenswürdige Zertifikate sowie die SSL-Aktivierung erforderlich. Mit Exchange 2003 richten Sie entsprechend einen SMTP-Connector ein, der auf der Gegenseite die SSL-Verbindung anfordert.

Die Nutzung von SSL für die eingehende Sicherheit ist auf dem virtuellen SMTP-Server einzurichten. Allerdings gelten diese Einstellungen für alle

eingehenden Verbindungen über diesen virtuellen SMTP-Server. Wenn Sie daher SSL erzwingen, um eine Verschlüsselung sicher zu stellen, werden Sie die Mehrheit der Absender aussperren. Im schlimmsten Fall wird sogar die Kommunikation zwischen Exchange 2003-Servern innerhalb ihrer eigenen Organisation sowie die Active Directory-Replikation über SMTP lahm gelegt.

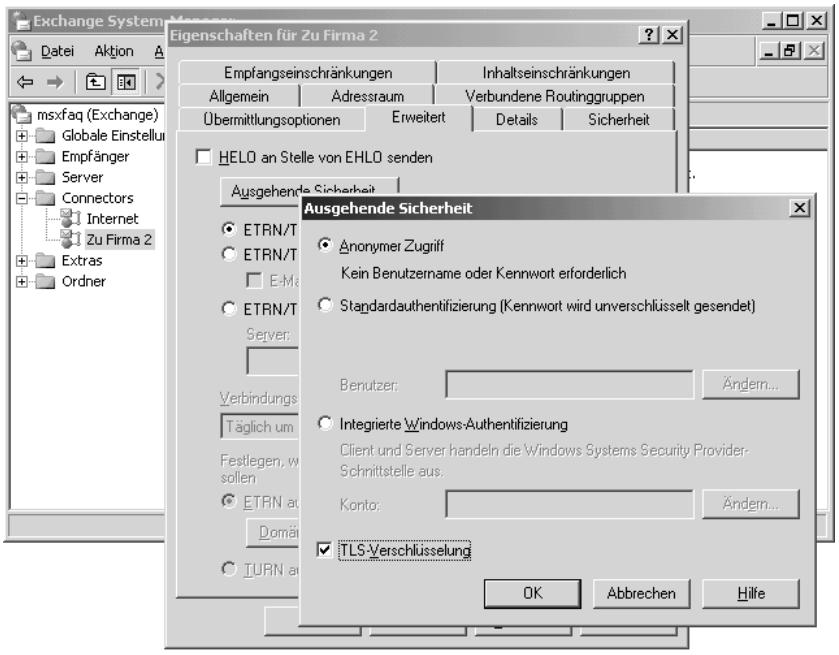


Abbildung 11.14 TLS für ausgehende Verbindungen nutzen

Um eine eingehende SSL-Verbindungen zu erzwingen, sollten Sie einen eigenen virtuelle SMTP-Server hierfür mit einer eigenen IP-Adresse einrichten und den Kommunikationspartnern diesen Server nennen.

Der virtuelle Server, der für den Empfang von allen anderen Nachrichten aus dem Internet zuständig ist, muss weiterhin auch ohne SSL erreichbar bleiben.

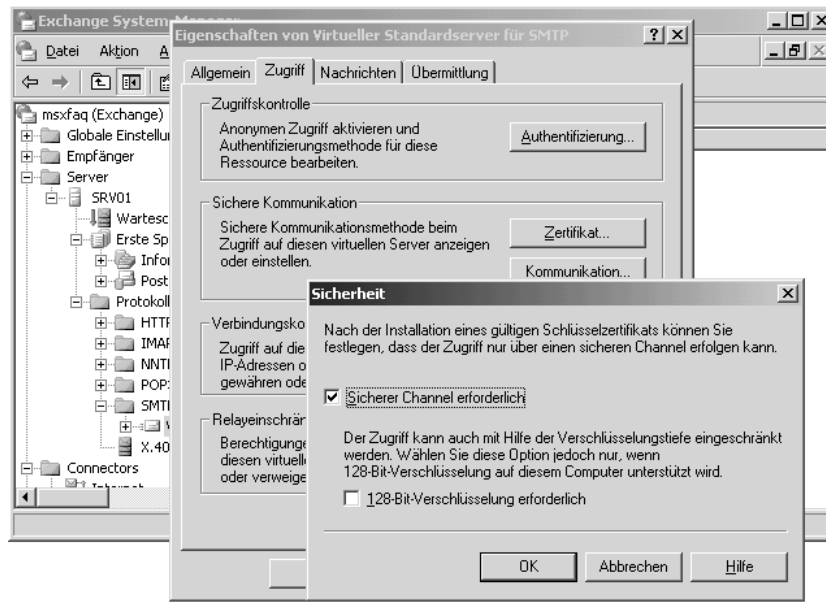


Abbildung 11.15
SSL für eingehende Verbindungen erzwingen

Die Verschlüsselung erfolgt allerdings immer nur auf dem Übertragungsweg zwischen den direkt beteiligten E-Mail-Systemen. Die Nachricht selbst ist nicht verschlüsselt. Sie können daher nicht sicher sein, dass auf dem gesamten Weg über Zwischenstationen die Sicherheit gewährleistet ist.

Outlook und S/MIME

Erst die Verschlüsselung der Nachricht durch das Absender-System oder den Absender selbst, stellt einen Schutz der Nachricht bis zum Empfänger sicher. Im Gegenzug können Programme wie Virenscanner, Spam-Filter, Archiv-System, Eventskripte oder anderen Prozessen diese Nachricht dann nicht mehr analysieren und bearbeiten. Entsprechend wichtig sind lokale Virenscanner in solch einem Umfeld.

Die beiden gebräuchlichen Standards, S/MIME und PGP, verschlüsseln die Nachrichten beim Versand bereits auf dem Arbeitsplatz des Benutzers mit dem öffentlichen Schlüssel des Empfängers. Der Empfänger ist die einzige Person, die solche Nachrichten wieder decodieren und lesen kann. Beide Verfahren bedienen sich einer symmetrischen Verschlüsselung, bei der die Nachricht mit einem zufällig gewählten Schlüssel codiert wird. Dieser Schlüssel wird dann über asymmetrische Verfahren (*Public Key, Private Key*) sicher zum Empfänger übermittelt. Der sichere Austausch dieser öffentlichen Schlüssel sowie der zusätzliche Aufwand beim Anwender erschweren aktuell den Einsatz auf jedem Arbeitsplatz. Nur wenige Personen benutzen ein persönliches Zertifikat, das von einer der bekannten Stamm-zertifizierungsstellen (CA) signiert wurde. Dies scheitert teilweise an den

Kosten, aber auch an der notwendigen Sensibilität für die Sicherheit und der Bereitschaft den zusätzlichen Aufwand zu betreiben.

Zudem fehlen einfache Strukturen, um problemlos an die öffentlichen Schlüssel (Public Key) der Empfänger zu kommen. Insofern nutzen nur die Benutzer diese Technik, die entsprechend sensibilisiert und im Umgang damit geschult sind.

Einen neuen Ansatz gehen Produkte, die als Gateway zwischen Exchange und Internet geschaltet werden, und auf dem Server die Verschlüsselung nach S/MIME oder PGP durchführen. Die E-Mail wird vom System bei der Übertragung in das Internet mit dem hinterlegten Public Key des Empfängers verschlüsselt. Alternativ können Sie einen allgemeinen Firmenschlüssel einsetzen. Damit kann zumindest gewährleistet werden, dass die Nachrichten bei der Übertragung über das Internet verschlüsselt und signiert werden. Folglich stellen Sie sicher, dass der Absender aus Ihrem Unternehmen kommt und nur die Empfängerfirma die Nachricht decodieren kann. Hier wird sich in den nächsten Jahren sicher noch einiges bewegen.

11.12 Öffentliche Ordner-Konzept

Bei mehreren Standorten und Server stellt sich die Frage, wie das Konzept für Öffentliche Ordner aussehen sollte. Gerade in großen Umgebungen werden diese gerne zwischen verschiedenen Standorten und Servern repliziert. Leider führt dies häufig zu einem unerwünscht hohen Replikationsaufkommen, im schlimmsten Fall sogar bis hin zur Inkonsistenz der Ordnerinhalte. Eine Planung der Öffentlichen Ordner-Struktur und deren Verteilung ist unbedingt erforderlich. Dabei ist die Replikation der Public Folder in zwei Bereiche zu unterteilen: die Replikation der Inhalte sowie die Replikation der Hierarchie.

Public Folder Server reduzieren

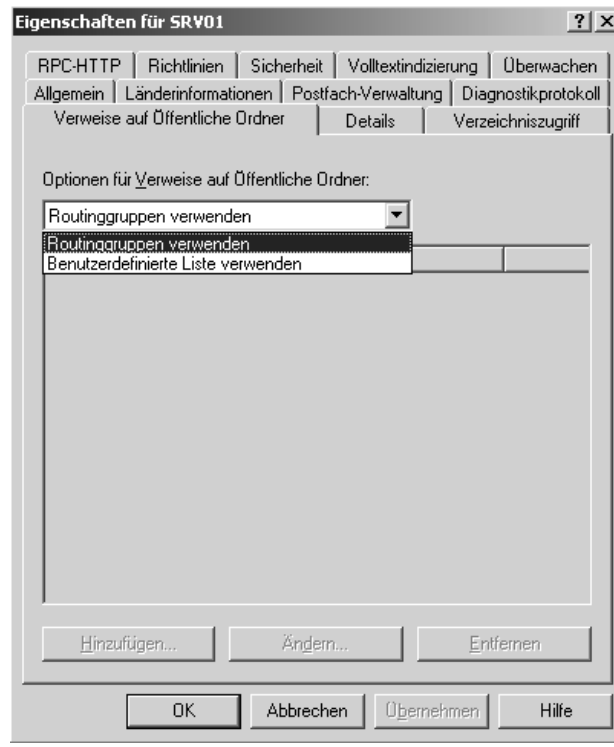
Im Gegensatz zu Exchange 5.5 bietet Exchange 2003 nun die Möglichkeit, das bisherige Konzept zu überdenken bzw. ein ganz neues Konzept einzuführen. Microsoft empfiehlt, die Anzahl der Server mit einem Öffentlichen Ordner-Speicher zu reduzieren. Sie können in größeren Umgebungen daher die Anzahl der Öffentlichen Informationsspeicher je Administrativer Gruppe reduzieren und trotzdem die Erreichbarkeit und Ausfallsicherheit gewährleisten. Dies entlastet die Postfachserver von der Öffentlichen Ordner-Replikation und den Zugriffen. Sie sollten aber mindestens einen Informationsspeicher je Administrativer Gruppe bestehen lassen, damit z.B Offline-Adressbuch, Frei/Belegt-Zeiten und die gewünschten Öffentlichen Ordner lokal erreichbar sind.

Referrals nutzen

Mittels Verweise auf Öffentliche Ordner (Public Folder Referrals) können Sie nun definieren, auf welche Öffentlichen Ordner-Server die Postfächer des

betroffenen Servers zugreifen dürfen. Bitte geben Sie hier auch immer die Server mit den Systemordnern an. Sofern der Zugriff nicht innerhalb der Routinggruppe gewährleistet ist, können Sie auch eine Benutzerdefinierte Liste nutzen.

Abbildung 11.16 Verweise auf Öffentliche Ordner



Die Erfahrung hat gezeigt, dass die Replikation auf ein Minimum zurückgeschraubt werden sollte. Interessant ist die Tatsache, dass jede Änderung der Hierarchie auf allen Servern der Organisation repliziert wird, die einen Öffentlichen Ordner-Speicher besitzen. Dazu gehören auch die Anpassungen der Ordnerrechte und Speichergrenzen sowie die E-Mail-Aktivierung. Diese Hierarchie-Replikation kann neben der Replikation der Ordnerinhalte bei großen Public Folder-Umgebungen eine sehr hohe Belastung für das System darstellen und gerade in Migrationsumgebungen zu Komplikationen führen.

12

Migration

12 Migration

Bisher haben Sie nur etwas über die Einrichtung von Exchange, die Anbindung an das Internet und die Installation der Clients gelesen. In den meisten Fällen ist heute bereits ein bestehendes Nachrichtensystem vorhanden, so dass dieses bei der Einführung von *Microsoft Exchange Server 2003* berücksichtigt werden muss.

Eine Migration gestaltet sich bei weitem aufwändiger und komplexer als die einfache Neuinstallation eines Systems. Insofern stellt sich die Frage, ob die Beschreibung einer Migration in diesem Buch im Grunde vollständig sein kann. Bedauerlicherweise ist keine Migration wie die andere, so dass dieses Ziel vermutlich nie in einem Buch erreicht werden kann. Der Schwerpunkt dieses Kapitels bezieht sich daher auf die Erläuterung der Zusammenhänge und Migrationswege, und weniger auf eine passende Handlungsanweisung. Aufbauend auf das entsprechenden Wissen um die Zusammenhänge und die möglichen Vorgehensweisen sowie einiger Beispiele, lässt sich das Thema anhand der Microsoft-Unterlagen, speziell für Ihr Unternehmen, leichter erschließen.

Schon bei der Installation Ihres Exchange 2003-Servers werden Sie durch den leistungsfähigen Assistenten an die Hand genommen und auch bei einem Update nicht alleine gelassen. Aber ohne das Grundverständnis der Migration werden Sie auch mit dem Assistenten nicht problemlos das Ziel erreichen.

Migrations-Szenarien

Nach der Erläuterung der Grundlagen wird an einigen konkreten Beispielen die Migration nach Exchange erläutert. Die ersten Beispiele nutzen dabei eine bestehende Exchange 5.5-Organisation. Die weiteren Beispiele bauen auf einer neuen Exchange-Organisation auf. Die Beispiele in Kürze:

- Beispiel 1: Exchange 2000 nach Exchange 2003

  Die erste Migration ist zugleich die einfachste Art der Umstellung auf Exchange 2003. Sie betrifft die Aktualisierung einer Exchange 2000-Organisation nach Exchange 2003.

- Beispiel 2: Ein Exchange 5.5-Standort nach Exchange 2003

  Dieses Szenario beschreibt die einfache Migration einer einzelnen Exchange 5.5-Installation mit einem Server in einer NT 4-Domäne nach Windows 2003 und Exchange 2003 in einer Administrativen Gruppe.

- Beispiel 3: Exchange 5.5 Multi Site in eine Exchange 2003-AG

  Die Bildung einer administrativen Gruppe mit mehreren Routinggruppen und die Zusammenfassung mehrerer Windows NT 4-Domänen in eine Active Directory-Domäne ist der Ausgangspunkt für diese Migration. Hier werden zwei Exchange-Standorte und zwei NT 4-Domänen in eine

Exchange 2003-Administrativen Gruppe und einer Active Directory-Domäne migriert.

- Beispiel 4: Erweiterung und Migration einer Exchange 5.5-Umgebung

  Ausgehend von einer bestehenden Exchange 5.5-Umgebung, die gegenwärtig nach Exchange 2003 migriert wird, sollen weitere Exchange 2003-Systeme in einer neuen Administrativen Gruppe installiert werden. Dieser Fall ist bei größeren Unternehmen recht häufig, die auch während der Migration erweitern und infolgedessen eine native Exchange 2003 Administrative Gruppe integrieren müssen.

- Beispiel 5: Fremdsystem ohne Connector

  Ein vorhandenes Nachrichtensystem wird nach Exchange 2003 migriert. Es gibt keinen Connector zu Exchange 2003, oder der Parallelbetrieb ist zu kompliziert. Der Exchange-Assistent zur Migration bietet in diesem Fall eine Übernahme der Daten aus dem Fremdsystem an. Für die Phase des Parallelbetriebs erfolgt die Zustellung von Nachrichten häufig für beide Systeme, für das alte und neue Postfach.

- Beispiel 6: Fremdsystem mit Connector migrieren

  Arbeiten Sie bisher mit Lotus Notes oder GroupWise, hilft Ihnen dieses Beispiel für das Verständnis der Migration. Hierbei wird Exchange mit dem Altsystem über einen Connector verbunden, der zusätzlich die Adressbücher abgleicht. Dieser Betrieb erlaubt eine längere Koexistenz und eine langsame Migration.

Die beiden letzten Beispiele eignen sich dazu, bei einem Firmenzusammenschluss die Systeme ebenfalls zusammenzuführen. Ehe Sie jedoch zur Tat schreiten, sollten Sie die Zusammenhänge verstehen.

12.1 Migrationswege

Die wenigsten Firmen arbeiten bislang ohne ein E-Mail-System. Sehr oft ist eine bestehende Exchange 5.5-Installation die Ausgangssituation für die Migration nach Exchange 2003. Manchmal sind aber auch ein fremdes Nachrichtensystem wie Notes, GroupWise oder einfache E-Mail-Server auf POP3-Basis bereits vorhanden. Bei der Migration können Sie grundsätzlich drei Modelle unterscheiden:

- Neuaufbau

  Sie installieren Exchange 2003 ohne Rücksicht oder Verbindung zu einem bestehenden E-Mail-System. Sobald Sie sicher sind, dass Exchange 2003 funktioniert und alle Benutzer mit Postfach angelegt sind, stellen Sie die Anwender auf das neue System um. Dazu stoppen Sie den Zugriff auf das alte System und lenken die eingehenden Nachrichten auf

den Exchange 2003-Server um. Die alten E-Mails werden hier mit dem Exchange-*Assistent für die Migration* übernommen.

- Aktualisierung des Servers (In-Place Update)

  Sofern möglich, installieren Sie Exchange 2003 auf dem vorhandenen Server und aktualisieren somit die bisherige Version des E-Mail-Systems.

- Langsame Migration (Swing Server)

  Das neue Nachrichtensystem wird parallel zum bestehenden System installiert, und beide E-Mail-Systeme werden miteinander verbunden. Ein geeigneter Connector gewährleistet die Nachrichtenübertragung. Der Verzeichnisabgleich sorgt für einen Abgleich der Adressbücher. Die Inhalte werden schrittweise auf die neuen Server verlagert.

Die Methode, die am meisten Zeit und Aufwand bedeutet, ist die langsame Migration. Sehr viele kleinere Firmen schließen Ihre Umstellung mit einem Neuaufbau oder sogar mit einem In-Place Update sehr schnell ab. Für große Unternehmen ist gerade die langsamen Migrationen, ohne Unterbrechung der E-Mail-Funktionalität, der einzige Weg, auf Exchange 2003 umzustellen. Um nun den für Ihre Umgebung passenden Weg zu ermitteln, benötigen Sie mehr Informationen zu den einzelnen Migrationsarten.

12.1.1 Neuinstallation

Einer der realisierbaren Migrationswege ist die Neuinstallation von Exchange 2003 auf der grünen Wiese. Besonders wenn das bisherige E-Mail-System nicht fehlerfrei oder passend konfiguriert ist, stellt ein Neuanfang oft eine wünschenswerte Alternative zu einem „Update“ dar.

System wird „frisch“ aufgesetzt

Eine bestehende Exchange-Umgebung oder andere E-Mail-Server werden bei der Installation nicht berücksichtigt. Dies erleichtert den Aufbau der neuen Umgebung, da weder das Know-how für den Parallelbetrieb, noch eine komplizierte Migration aufzubauen ist. Zudem entfallen einige Beschränkungen, die bei einer direkten Migration des Altsystems zwangsläufig vorhanden sind.

Ausgehend von den bisherigen Erkenntnissen zur Nutzung des alten E-Mail-Systems können Sie die neuen Server dimensionieren, installieren und verbinden. Umfangreiche Tests und die Integration in Datensicherung und Virenschutz sind möglich, ohne den Produktivbetrieb der bisherigen Umgebung zu stören. Auch die Migration der Altdaten kann mehrfach geprobt werden.

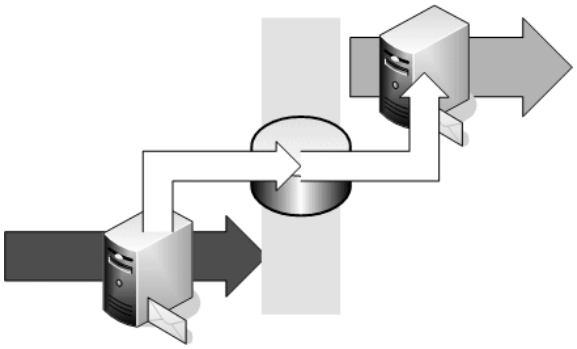


Abbildung 12.1 Neuinstallation mit Zwischenspeicherung der Daten

Irgendwann kommt der Moment, an dem die neue Umgebung in Betrieb genommen wird. Dazu wird das alte Nachrichtensystem zu einem bestimmten Zeitpunkt angehalten, so dass die Anwender keine Veränderungen mehr vornehmen und keine neuen Nachrichten aus dem Internet eintreffen können. Ab diesem Moment ist die Firma ohne ein E-Mail-System.

Inhalte übernehmen

Die Inhalte aus dem alten E-Mail-System können abhängig vom System exportiert und in Exchange 2003 importiert werden. Hierbei unterstützt Sie der Exchange-Assistent für die Migration, der für Sie die Nachrichten aus fremden Systemen exportiert und in Exchange importiert. Parallel dazu müssen die Arbeitsplätze der Anwender auf den Einsatz von Exchange 2003 umgestellt werden. Zuletzt werden die Verbindungen zum Internet für Exchange 2003 aktiviert und die Freigabe für die Anwender erteilt.

Wichtige Aspekte dieser Methode:

- Es gibt einen Zeitraum, in dem das alte Nachrichtensystem nicht mehr zur Verfügung steht, aber das neue System noch nicht betriebsbereit ist. Das Mail-System ist in der Regel für einige Stunden oder gar Tage „offline“.
- Diese Migration funktioniert nicht, wenn das Altsystem Exchange 2000 im gleichen Active Directory ist und Sie über diesen Weg eine neue Organisation installieren möchten. Dann müssen Sie die Daten der vorhandenen Organisation in PST-Dateien temporär zwischenspeichern, Exchange 2000 deinstallieren, und dann Exchange 2003 neu installieren.
- Diese Migration funktioniert ebenfalls nicht, wenn Sie als Altsystem Exchange 5.5 einsetzen und mit dem Active Directory Connector eine Verbindung zum bestehenden Active Directory konfiguriert haben. Im Active Directory sind bereits alle Informationen über die alte Organisation hinterlegt und müssen vor der Migration entfernt werden.
- Alle Anwender müssen zeitgleich umgestellt werden. Dies ist ab einer bestimmten Anzahl oder räumlichen Verteilung nicht mehr realisierbar. Denken Sie auch an die notwendige Anwenderschulung beim Umstieg auf Outlook 2003.

- Können die Daten des bisherigen E-Mail-Servers nicht zentral übernommen werden, sind aufwändige Importtätigkeiten auf den Clients erforderlich. Auch dies ist ein Grund, bei größeren Installationen eine andere Migrationsart zu wählen.
- Point of no Return: Es ist kaum möglich, bei einem später erkannten Fehler wieder zum alten E-Mail-System zurückzukehren. Die Vorbereitung muss sehr sorgfältig sein, da Sie bei einem Fehler oder einer übersehenen Abhängigkeit nicht mitten in der Migration eine Pause einlegen können. Entweder wird migriert oder der alte Stand wieder hergestellt. Durch die möglichst schnelle parallele Anpassung aller Clients ist der Weg zurück jedoch sehr schnell verbaut.
- Alle Clients müssen in kurzer Zeit angepasst werden. Bei vielen Systemen ist dies nur mit einer Software-Verteilung und einem guten Systemmanagement möglich.
- Die Hotline muss für den ersten Support-Ansturm ausreichend besetzt sein und das notwendige Know-how besitzen. Das ist besonders schwierig, wenn der Umstieg von einem anderen System erfolgt und Outlook 2003 eine neue Anwendung für die Benutzer ist.
- Alle sonstigen Anwendungen wie Datensicherung, Virenschutz, Faxserver und andere müssen ebenfalls zeitgleich umgestellt werden.
- Auch die Administratoren müssen von einem auf den anderen Tag produktiv das neue System betreuen können. Entsprechende Schulungen sollten vorab besucht werden. Die notwendige Betriebserfahrung während der ersten Tage kann durch externe Hilfe gewährleistet werden.

Nur in sehr kleinen Umgebungen mit entsprechender Absicherung ist es denkbar, die Server-Daten auf einen temporären Speicher zu exportieren und den gleichen Server mit Exchange 2003 neu zu installieren. Die damit verbundene Ausfallzeit und der verbaute Rückweg im Fehlerfall sprechen allerdings gegen solch ein Vorgehen.

Diese Migration eignet sich weniger für größere Firmen mit mehreren Standorten, sondern ist meist eine mögliche Migrationsart für kleine Firmen, in denen die Ausfallzeit und der Aufwand für die Client-Umstellung überschaubar bleibt. Es gibt sehr viele Unwägbarkeiten. Eine langsame Migration Postfach für Postfach ist nicht möglich.

Auf der anderen Seite ist diese Migration oft der Weg, eine Teilfirma aus der bestehenden Exchange-Organisation auszugliedern, wenn diese selbstständig geworden ist. Bei diesem Verfahren kann der Name der Organisation neu bestimmt werden. Auch eine Trennung des Active Directory ist möglich.

12.1.2 Serveraktualisierung (In-Place Update)

Eine weitere Möglichkeit, einen Server auf Exchange 2003 zu aktualisieren, ist das Update eines bestehenden Exchange-Servers. Bei der Installation von Exchange 2003 werden die bestehenden Konfigurationsinformationen und E-Mail-Datenbanken übernommen und weiter verwendet.

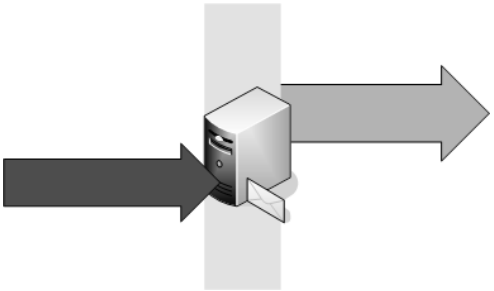


Abbildung 12.2
In-Place-Update

In-Place-Update:
Exchange 5.5 →
Exchange 2000 →
Exchange 2003 ✓

Allerdings beschränkt sich diese Möglichkeit der Aktualisierung mit Exchange 2003 auf einen Exchange 2000-Ausgangsserver mit SP 3. Ein In-Place-Update von Exchange 5.5 direkt auf Exchange 2003 ist nicht mehr möglich. Möchten Sie trotzdem einen bestehenden Exchange 5.5-Server auf Exchange 2003 aktualisieren, kann der Umweg über eine Migration auf Exchange 2000 und dann auf Exchange 2003 gegangen werden. Die Aktualisierung erfolgt dann in zwei getrennten Schritten, in Abhängigkeit der erforderlichen Service Packs.

Für den ersten Schritt ist die Installation des Active Directory Connectors (ADC) erforderlich, ehe das Update auf Exchange 2000 erfolgen kann. Der zweite Schritt zur Aktualisierung von Exchange 2000 auf Exchange 2003 ist dagegen unspektakulär.

Das In-Place-Update von Exchange 2000 auf Exchange 2003 ist auch der einzige Weg, um ein Update des Server-Betriebssystems auf Windows 2003 durchzuführen. Da Exchange 2000 nicht auf Windows 2003 funktioniert, erfolgt zuerst das Update auf Exchange 2003, und erst im zweiten Schritt kann Windows 2000 auf Windows 2003 aktualisiert werden.

Folgende Aspekte sind für das Update von Exchange 2000 auf Exchange 2003 zu berücksichtigen:

- Während des Updates sind die Exchange-Dienste für einige Zeit nicht verfügbar.
- Eventuell sind Aktualisierungen von Drittkomponenten (Faxserver, Datensicherung, Virenscanner) notwendig.
- Bei einem Fehler während des Updates sind Änderungen nur schwer wieder rückgängig zu machen.

- Das In-Place Update ist der einzige Weg, um das Betriebssystem auf Windows 2003 zu aktualisieren, da zuerst Exchange 2000 aktualisiert werden muss.

Diese Migration wird primär genutzt werden, um einen bestehenden Server auf Windows 2003 zu aktualisieren und Exchange 2003 die Voraussetzung dazu ist. Viele Exchange 2000-Server sind noch nicht sehr alt, so dass ein Tausch der Hardware nicht unbedingt ansteht.

12.1.3 Langsame Migration (Swing Server)

Migration über Monate hinweg

Größere Exchange-Installationen bestehen nicht nur aus einem oder zwei Servern an einem Standort, sondern bilden große Organisationen mit Tausenden von Benutzern ab. Mitte 2003 kursierten Annahmen von gerade mal 25 % aller bereits umgestellten Exchange 5.5-Systeme nach Exchange 2000 oder Exchange 2003. In größeren Installationen ist die Migration nicht durch eine Aktualisierung oder Neuinstallation eines Servers möglich, sondern das neue System muss einige Zeit parallel neben dem bisherigen Nachrichtensystem betrieben werden.

Während bei einer Verbindung von Exchange 5.5 und Exchange 2003 eher die Migration im Vordergrund steht, können Anbindungen an Notes oder GroupWise auch als Dauereinrichtung angelegt werden.

Das Prinzip dieser Migration beruht auf folgenden wesentlichen Faktoren:

- Abgleich der Verzeichnisinformationen

  Jedes E-Mail-System muss die Postfächer des anderen Systems als Empfänger auflösen können. Dieser Prozess muss während des gesamten Parallelbetriebs gewährleistet sein und gehört zu den aufwändigsten Aufgabenstellungen für einen Administrator.

- Austausch von Nachrichten

  Zwischen beiden Systemen müssen Nachrichten mit möglichst wenig Formatverlusten ausgetauscht werden können. Bei der Kopplung zwischen Exchange 5.5 und Exchange 2003 ist dies gegeben. Bei der Kopplung zu Fremdsystemen gelten aufgrund unterschiedlicher Designs Einschränkungen, z.B. für Einladungsnachrichten und Formulare.

- Austausch von Frei-/Belegt-Zeitplänen

  Sofern möglich, sollten auch die Frei-/Belegt-Zeiten der Terminpläne zwischen den Systemen abgeglichen werden, so dass eine Zeitplanung auch über die Grenzen des eigenen E-Mail-Systems möglich ist. Dies funktioniert nicht nur mit Exchange 5.5 und Exchange 2000, sondern auch mit Lotus Notes und GroupWise.

- Abgleich der Öffentlichen Ordner

  Die Öffentlichen Ordner von Exchange müssen ebenfalls zwischen beiden Versionen abgeglichen werden. Ein Abgleich mit gemeinsamen Ablagen fremder E-Mail-Systeme ist hingegen selten möglich und auch nicht immer erwünscht. Oft ist das Protokoll NNTP der kleinste gemeinsame Nenner, der überhaupt eine Kopplung ermöglicht.

Auf dieser Grundlage funktionieren alle Migrationen von Exchange 5.5 nach Exchange 2003 innerhalb der gleichen Organisation sowie die Migration von unterstützten Fremdsystemen wie Lotus Notes und Novell GroupWise.

Schritt 1: Kopplung der Adressbuchdienste

Der erste Schritt dieser Migration ist der Benutzer-Abgleich beider Welten. Bei der Verbindung mit einem Fremdsystem werden die Postfächer der einen Seite als externe Empfänger oder Kontakt auf der Gegenseite eingetragen.

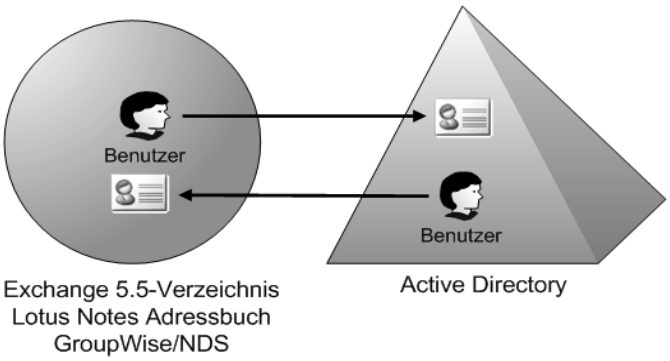


Abbildung 12.3 Verzeichnisabgleich zweier E-Mail-Systeme

Dies ist ein Unterschied im Vergleich zum Abgleich zwischen Exchange 5.5 und Exchange 2003. Der Active Directory Connector legt auf der Gegenseite keine Kontakte an, sondern vollwertige Postfach-Benutzer im Exchange 5.5-Verzeichnis sowie im Active Directory.

„Move Mailbox" kopiert Daten

Verschieben Sie nun die Postfächer von einem Exchange 5.5-Server oder fremden E-Mail-Server nach Exchange 2003, werden zuerst die Inhalte aus dem Quellpostfach in ein neues Zielpostfach kopiert. Nach diesem Schritt wird der Postfacheintrag im alten und neuen E-Mail-System angepasst, sodass die Einträge auf das neue Postfach verweisen.

Bei der Migration aus dem Fremdsystem wird der Kontakt im Active Directory gelöscht und ein Postfach angelegt. Dieses erhält die migrierten Nachrichten und die zuvor vorhandenen E-Mail-Adressen. Das Postfach im alten E-Mail-System wird gelöscht. Durch die Synchronisation der Verzeichnisse wird der Exchange 2003-Benutzer wieder als externer Empfänger im alten E-Mail-System angelegt.

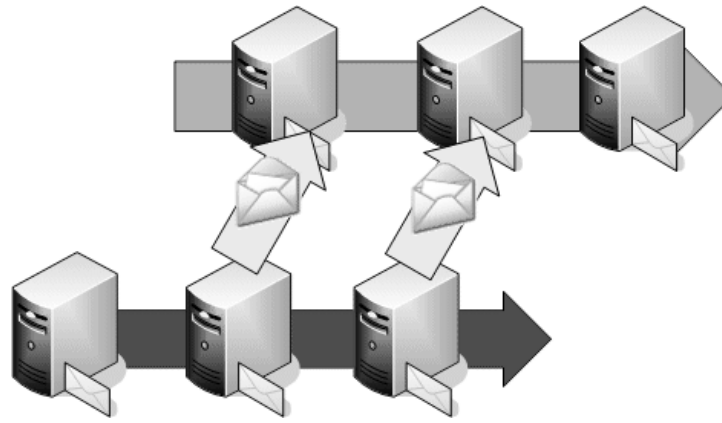


Abbildung 12.4 Migration durch Verschieben auf andere Server

Mit dieser Methode können über mehrere Wochen oder sogar Jahre hinweg die Postfächer langsam von einem Server auf neue Server verschoben werden. Die Öffentlichen Ordner in Exchange werden über die Replikation verlagert. Die Connectoren müssen manuell auf den neuen Servern eingerichtet werden.

Die relevanten Aspekte dieser Migration sind:

- Sie benötigen zusätzliche Hardware und Lizenzen, da Exchange 2003 nicht auf den bestehenden E-Mail-Servern installiert werden kann.
- Sie müssen beide Systeme miteinander verbinden können, damit während der Migration die Benutzer auf dem alten System mit den Anwendern auf Exchange 2003 möglichst reibungslos kommunizieren können.

Meilensteine setzen

- Die Migration zieht sich in der Regel über mehrere Wochen hin, in der beide Systeme administriert und unterstützt werden müssen. Einige Firmen migrieren schon mehrere Jahre von Exchange 5.5 auf Exchange 2000. Setzen Sie sich Ziele und Meilensteine. Besonders zum Ende zu sollten Sie aktiv die Migration beschleunigen. Viele Probleme sind in der Komplexität des Parallelbetriebs begründet.
- Sie können bei ernsten Problemen die Migration pausieren oder sogar wieder rückgängig machen und bis zur Lösung der Probleme warten.
- Bei der Migration von Exchange 5.5 nach Exchange 2003 innerhalb der gleichen AG sind bei Outlook keine Änderungen notwendig. Outlook erkennt beim Start, dass sich der Home-Server geändert hat, und passt das MAPI-Profil selbstständig an. Allerdings sollte der alte Server noch einige Zeit laufen, bis alle Clients die Profile geändert haben. Prüfen Sie die Notwendigkeit von Updates und Patches bei der Nutzung von Outlook 2003 mit Exchange 5.5, da der Client von einem anderen System, und zwar Exchange 2003 ausgeht.

- Bei der Migration von anderen E-Mail-Systemen können Sie Arbeitsplatz für Arbeitsplatz schrittweise umstellen, die Mitarbeiter schulen, wie sie die Postfächer migrieren, und Daten übernehmen. Allenfalls Anwender an wechselnden Arbeitsplätzen sowie Arbeitsgruppen mit einer engen Zusammenarbeit (Stellvertreter) sind als Block umzustellen.
- Connectoren können für das neue System eingerichtet, getestet und nach und nach aktiviert werden. Die alten Connectoren können als Sicherheit einige Zeit beibehalten und bei einem Fehler reaktiviert werden.

Die langsame Migration ist vielfach die bevorzugte Migration für größere Umgebungen oder wenn die neue Installation auf einer neuen Hardware stattfinden soll. Allerdings stellen der Parallelbetrieb zweier E-Mail-Systeme und besonders der Verzeichnisabgleich hohe Anforderungen an die Betreiber und die Administratoren.

12.1.4 Auswahl der optimalen Migration

Welcher der vorgestellten Migrationswege ist nun für Ihre Umgebung die optimale, und welche Wege sind überhaupt gangbar?

Setzen Sie bisher ebenfalls Microsoft Exchange ein, dann ist der Weg zu Exchange 2003 abhängig von der Exchange-Version. Folgende Grafik zeigt Ihnen die verschiedenen Wege von einer Exchange-Version auf die nächste Version, ungeachtet der eingesetzten Edition und Windows-Version.

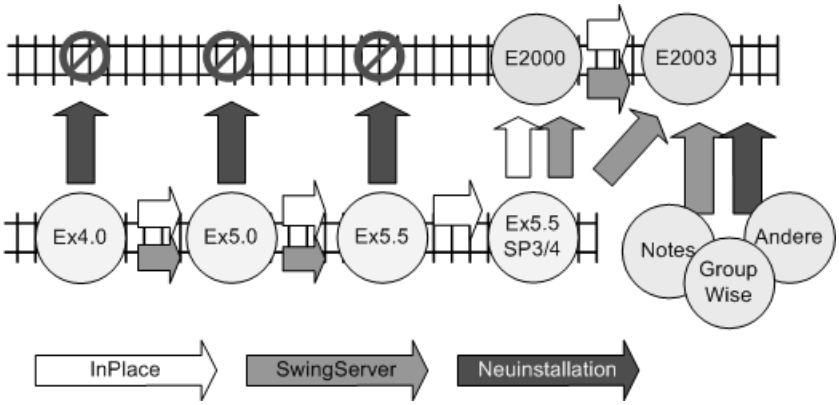


Abbildung 12.5 Mögliche Migrationswege

Alle Versionen vor Exchange 5.5 Service Pack 3 können nicht auf Exchange 2003 migriert werden. Exchange 2003 kann nur mit Exchange 5.5 SP 3 oder SP 4 sowie Exchange 2000 in einer Organisation zusammenarbeiten. Ältere Exchange 5.5-Server in der Organisation müssen daher zuerst auf den Mindeststand angehoben werden. Ein In-Place-Update auf Exchange 2003 geht nur von Exchange 2000 SP 3. Fremdsysteme können entweder im Rahmen einer Neuinstallation oder über die enge Kopplung der

Systeme mit einem Connector und entsprechendem Verzeichnisabgleich migriert werden.

Folgende Matrix verdeutlicht die möglichen und sinnvollen Migrationswege nach Exchange 2003 über die drei Varianten und eine vorläufige Gewichtung und die Häufigkeit der Anwendung.

Tabelle 12.1 Migrations-optionen

Bisheriges System	Neuaufbau	In-Place	Swing Server
Ohne E-Mail-System	👍 Einziger Weg	👎 nicht möglich	👎 nicht möglich
Exchange 4.0/5.x	👉 Möglich	nur über Ex5.5 SP3	nur über EX5.5 SP3
Exchange 5.5 SP 3/SP 4	👉 Selten	👍 in kleinen Umgebungen	👍👍 in größeren Umgebungen
Exchange 2000	👉 Selten	👍 oft	👍 o.k.
Notes	👍 Migrations-Wizard über Notes Client-Export	👎 nicht möglich	👍 Lotus Notes Connector mit Migrations-Wizard
GroupWise	👍 Migrations-Wizard über GroupWise Client-Export	👎 nicht möglich	👍 GroupWise Connector mit Migrations-Wizard
POP3/IMAP4	👍 Migrations-Wizard über POP3, IMAP4 und LDAP SMTP-Adressraum gemeinsam nutzen	👎 nicht möglich	👎 nicht möglich

12.2 Know-how zur Migration

Egal, für welchen Weg Sie sich entscheiden, viele Dinge sind für alle Migrationen allgemein gültig.

12.2.1 Frühjahrsputz

Es ist eine Illusion zu sagen, dass nach der Migration alles besser wird, wenn Sie vor der Migration das Ausgangssystem nicht aufräumen. Daher ist vor dem Start der Migration zuerst eine längst überfällige Analyse der bisherigen Systemlandschaft notwendig, bei der alte Postfächer, Verteiler und andere Reste entfernt werden. Es ist durchaus verständlich, bei einer Migration möglichst alles mit zu übernehmen, damit die Anwender später nicht den

Verlust beklagen. Jedoch erschweren und verzögern einige Dinge die Migration oder sind später selbst Ursache für Störungen in der Migration. Dies gilt besonders bei der Umstellung mit der Swing Server-Methode von Exchange 5.5 oder dem Update mit Connectoren von Notes und GroupWise. Folgende Dinge sollten Sie deshalb vorab korrigieren.

Altlasten entfernen

- Alte Connectoren entfernen

  Sehr viele Exchange 5.5-Server werden mit dem MS-Mail-Connector und cc:Mail-Connector installiert. Die meisten Firmen nutzen diese Connectoren überhaupt nicht, trotzdem sind diese mitsamt den Adresserweiterungen in der Organisation vorhanden. Damit diese Altlast nicht noch in die Exchange 2003-Organisation übernommen wird, sollten Sie schon vorab diese Connectoren deinstallieren. Sie können die Connectoren nicht im Exchange 5.5-Administrator löschen, sondern müssen diese über das Exchange 5.5-Setup deinstallieren. Das gleiche Vorgehen gilt für Fax-Connectoren und andere Fremdprodukte, die Sie nicht mehr benötigen oder nicht mit Exchange 2003 kompatibel sind. Dies ist insbesondere für Exchange 2003 wichtig, da die Empfängeraktualisierungsdienste die entsprechenden DLLs dieser Produkte zur Generierung der E-Mail-Adressen benötigen. Fehlen diese Module, kann der RUS keine E-Mail-Adressen erstellen.

- Alte Standorte und Server entfernen

  Prüfen Sie, ob in Ihrer Exchange-Organisation noch Server aufgelistet sind, die es schon lange nicht mehr gibt. Ebenso sollten alle Standorte, die nicht mehr existieren und zu denen Sie den Connector zur Verzeichnisreplikation entfernt haben, aus Ihrer Organisation verschwunden sein.

- Exchange 5.5 Service Pack und Windows Service Pack

  Deployment-Tools ausführen

  Der Installationsassistent von Exchange 2003 überprüft ebenfalls, ob alle Server in der Organisation die notwendigen Voraussetzungen für die Installation erfüllen. Allerdings kann es Ihren Zeitplan durcheinander werfen, wenn Sie erst bei der Installation von Exchange 2003 feststellen, welche Vorbedingungen noch zu erfüllen sind. Anhand der *Exchange Deployment Tools* (Exchange-CD) können Sie sehr viele Tests auch vorab ausführen, ohne das eigentlich Exchange-Setup zu starten.

- Verteiler aufräumen

  Übereinstimmung Verteiler — Sicherheitsgruppe prüfen

  Bislang sind die Verteiler im E-Mail-System unabhängig von den Sicherheitsgruppen des Active Directory gewesen. Durch die Einführung von Exchange 2003 werden aus allen Verteilern E-Mail-aktivierte Sicherheitsgruppen. Diese können Sie später auch für die Vergabe von Rechten auf Dateien und Freigaben nutzen. Daher ist eine Kontrolle wichtig, welche Mitglieder in einem Verteiler und welche Mitglieder in

einer bestehenden ähnlichen Sicherheitsgruppe vorhanden sind. Unstimmigkeiten bedürfen der Klärung.

Verteiler, für die es keine Verwendung mehr gibt, sollten entfernt werden. Dies reduziert später den Aufwand für den Abgleich zum Active Directory. Allein die Installation und Konfiguration des *Active Directory Connectors* legt die Exchange 5.5-Verteiler im Active Directory als Sicherheitsgruppen an.

- Inaktive Konten finden und entfernen

1:1-Beziehung, NTDSnoMatch sowie DS/IS-Consistency-Check

Das Gleiche gilt für Postfächer, deren Windows-Konten in der Domäne nicht mehr aktiv sind. In Exchange 5.x war es zudem möglich, einen Benutzer bei mehreren Postfächern als primäres Konto einzutragen. Sogar Gruppen konnten als Besitzer eines Postfachs fungieren. Solche Konstellationen müssen vor der Migration unbedingt aufgelöst werden. Wurden die Anmeldekonten der Benutzer bereits mit ADMT in das Active Directory migriert, dann sollten sich die Anwender auch mit diesem Konto am Active Directory anmelden, damit Sie das neue AD-Konto als primäres Benutzerkonto in Exchange 5.5 hinterlegen können.

Kontrollieren Sie ebenfalls, ob in Ihrer globalen Adressliste unbekannte oder alte Benutzer auftauchen. Ebenso ist es gute Praxis, die Anzahl der Empfänger der globalen Adressliste auf den verschiedenen Exchange 5.5-Servern zu vergleichen. Sofern Ihre Replikation korrekt funktioniert und einige Zeit keine Änderungen erfolgt sind, sollten diese Listen identisch sein. Kontrollieren Sie in diesem Schritt auch eventuell verborgene Konten!

- Rechte bereinigen

Eine wesentliche Arbeit vor der Migration ist die Beseitigung von alten Berechtigungen. Wird in Exchange 5.5 ein Anwender gelöscht, der direkt auf einem Öffentlichen Ordner berechtigt war, so bleibt das Recht im Öffentlichen Ordner als DN-Eintrag erhalten. Bei der späteren Migration findet Exchange 2003 diesen Benutzer jedoch nicht und verweigert die Konvertierung der Rechte. Sie sollten daher die DS/IS-Konsistenzanpassung von Exchange 5.5 durchführen, um die Berechtigungen von alten, nicht mehr existenten Benutzern in bestehenden Postfächern und Ordnern zu entfernen. In verteilten Umgebungen sind die Abhängigkeiten zu beachten, damit alle Änderungen auch repliziert wurden, ehe in einem anderen Standort ebenfalls diese Aktion gestartet wird.

- Fremdprodukte auf Kompatibilität prüfen

Kompatible 3rd-Party-Produkte?

Nicht alle Produkte sind auch für Exchange 2003 geeignet. Besonders Connectoren sind potenzielle Kandidaten, die Sie nach der Migration der Postfächer auf Exchange 2003 eventuell nicht mehr nutzen können. Programme, die bisher den Exchange 5.5-Administrator um eigene Felder

und Karteikarten erweitert haben, können in Exchange 2003 diese Informationen nicht mehr in das Active Directory schreiben. Fragen Sie den Hersteller, wie die Konfiguration dieser Connectoren erfolgen kann.

- Bisherige Datensicherung und Archivierung überdenken

  Backup und Datenschutz

  Ihre bisherige Virenschutz-Software und Datensicherung sind vermutlich nicht mit Exchange 2003 kompatibel. Entsprechende Aktualisierungen oder Produktauswahlverfahren müssen rechtzeitig gestartet werden. Die Bereitstellung entsprechender Mittel ist ebenfalls einzuplanen. Auch während und nach der Migration sollten Sie bereits die Server sichern. Eine besondere Frage stellt sich, wenn Sie auf Daten vor der Migration zugreifen müssen. Eventuell müssen Sie einen entsprechenden Server einige Zeit für diese Fälle bereithalten.

- Dokumentation und Abnahme

  Die während Ihrer Erfassung dokumentierten Ist-Zustände sollten Sie den Verantwortlichen präsentieren und die Abhängigkeiten bei der Migration erläutern. Bei jeder Migration ist der Aufwand im Verhältnis zu den Verlusten abzuwägen. Es wird immer Umstände geben, bei denen eine Änderung nur sehr zeitaufwändig auf das neue System umgesetzt werden kann. Informieren Sie aktiv die beteiligten Projektpartner, und holen Sie deren Einverständnis ein.

Dies sind die wichtigsten Prüfungen und Vorbereitungen vor der Migration. Leider läuft jede Migration etwas anders ab, so dass Sie auch immer etwas Reserve für unvorhergesehene Probleme einplanen sollten.

12.2.2 Active Directory-Migration

Für den Betrieb von Exchange 2003 ist immer ein Active Directory notwendig. Für jedes Postfach muss es ein entsprechendes Benutzer-Objekt in diesem Active Directory geben. Aus diesem Grund ist eine Exchange 2003-Einführung auch immer mit einer Active Directory-Einführung oder -Migration verbunden. Im Idealfall sollte der AD-Benutzer das globale Anmeldekonto für alle Aktionen im Netzwerk sein, da Sie sonst mit zusätzlichen deaktivierten Konten arbeiten müssen.

Dies bedeutet, dass Sie eventuell erst die aktuellen Benutzer aus einer NT 4-Domäne in das Active Directory überführen müssen. Damit stellen sich für die Migration zwei wichtige Fragen:

Wie werden die Benutzer migriert?

Für die Migration bestehender Windows NT 4.0-Benutzer in das Active Directory gibt es drei Alternativen, die für Exchange von Bedeutung sind:

- Update der Windows NT 4-Domäne

SID-bleibt bestehen

Durch ein In-Place-Update des Windows NT 4-PDC der bestehenden Domäne auf Windows 2003 bleiben alle Benutzer mit der SID erhalten. Dies bedeutet, dass die Exchange 5.5-Postfachkonten unverändert weiter genutzt werden können.

Diese Methode wird oft bei einer einzigen, zu aktualisierenden Domäne eingesetzt. Sollen jedoch mehrere alte Domänen in eine Active Directory-Domäne zusammengefasst werden, können Sie dieses Verfahren nur für maximal eine der Domäne nutzen. Ausgeschlossen ist dieser Weg, wenn der Exchange 5.5-Server zugleich auch der PDC ist, da Exchange 5.5 nicht auf Windows 2003 funktioniert. Allenfalls ein Update über Windows 2000 als Zwischenschritt ist hier denkbar.

- Migration in neue Domäne mit SID-History

Alte SID hinzufügen

Mit dem Programm ADMT und anderen Tools kann der Anwender von einer bestehenden Domäne in eine neue native Active Directory-Domäne migriert werden. Dabei wird zwar ein neues Benutzerkonto mit neuer SID angelegt, aber die bisherige SID kann zusätzlich angefügt werden. Damit behält der Benutzer fast alle Berechtigungen, die er aufgrund seiner früheren SID hatte. Der Anwender kann sogar weiterhin auf sein Exchange 5.5-Postfach zugreifen. Migrieren Sie ebenfalls die Sicherheitsgruppen der früheren Domäne, so kann der Benutzer auch über die Rechte verfügen, die er bereits als Mitglieder dieser Gruppen hatte.

- Neuanlegen der Anwender

Neue SID

Bei der Umstellung von anderen Anmeldediensten (z.B. NetWare NDS) gibt es keine SID zu migrieren. Für Benutzer, die in solchen Umgebungen bereits mit Exchange gearbeitet haben, besteht bereits ein NT-Domänen-Konto (evtl. in der Exchange-Domäne), das Sie migrieren können.

Für die Migration von Exchange 5.5 sollten Sie immer sicherstellen, dass das primäre Benutzerkonto auf das Anmeldekonto verweist.

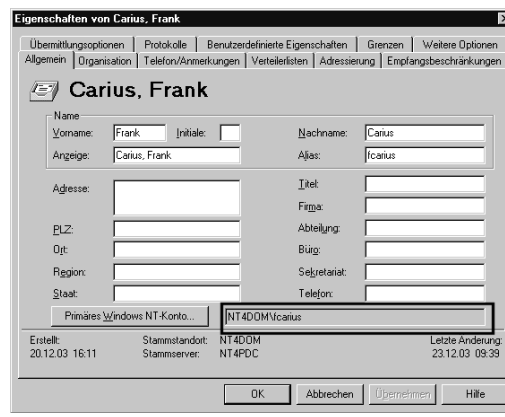


Abbildung 12.6 Exchange 5.5 „Primäres Windows NT-Konto“

Diese Zuordnung ist später für die Einrichtung des Active Directory Connectors wichtig, damit die Exchange-Informationen dem richtige AD-Konto zugeordnet werden.

Wenn Sie die alte NT 4-Domäne schon vor dem Abschluss der Migration aller Exchange 5.5-Server auflösen wollen, müssen Sie Exchange 5.5 ebenfalls in die neue Domäne migrieren. Dazu ist die Anpassung des Dienstkontos von Exchange notwendig, wie im TechNet-Artikel „152808 XADM: How to Change the Service Account“ beschrieben. Über diesen Weg sollten Sie am besten vor der Installation des ersten Exchange 2003-Servers die Exchange 5.5-Server umziehen.

Wann werden die Konten im Active Directory angelegt?

Meilensteine der Kontenmigration

Die zweite Frage betrifft den Zeitpunkt der Kontenmigration. Dies ist insbesondere wichtig für die Zusammenarbeit mit der im nächsten Abschnitt beschriebenen Funktion des *Active Directory Connectors* (ADC) sowie der Zusammenführung von Exchange-Einstellungen zu den Benutzerkonten.

- Vor der Exchange-Umstellung

  Benutzerkonten, die vor der Exchange-Migration schon in das Active Directory migriert wurden, erhalten durch den ADC anhand der SID die korrekten Exchange-Eigenschaften zugewiesen. Dies ist der einfachste und empfohlene Weg.

- Parallel zur Exchange-Umstellung

  Bei mehreren Standorten möchten Sie nicht unbedingt zweimal umher reisen, um zuerst das Active Directory und in einem zweiten Schritt Exchange 2003 einzuführen. In diesem Fall müssen Sie den Active Directory Connector früher einrichten. Der ADC legt ein Platzhalterkonto (deaktivierter Postfach-Benutzer) für alle noch nicht ins Active Directory migrierten Benutzer an. Wenn Sie später die Anwender Stück für Stück in das Active Directory migrieren, können Sie mit dem „*Assistent für die Active Directory-Kontenbereinigung*„ (ADCleanup) die Exchange-Einstellungen der deaktivierten Platzhalterkonten zu den neuen aktiven Benutzerkonten zusammenführen.

- Nach der Exchange-Migration

  Platzhalter für Multi-Forest-Benutzer

  Die Einführung eines Active Directory in einer größeren Firma zieht sich meist über eine längere Zeit hin. Oftmals ist noch gar nicht absehbar, wann die letzten NT 4-Domänen migriert werden. Ebenso betreiben einzelne Firmenteile sogar einen komplett eigenen Forest. In all diesen Fällen benötigen Sie die deaktivierten Platzhalterkonten in Ihrem Active Directory über einen längeren Zeitraum, bis unendlich. Diese Konstellation trifft auch zu, wenn Sie Exchange zentral betreiben, aber die einzelnen Abteilungen autark eigene Anmeldedomänen verwalten.

Alle drei Varianten der Benutzerumstellung sind möglich, so dass Sie bei der Einführung von Exchange 2003 keine Rücksicht auf die Active Directory-Migration der Anmeldedomänen nehmen müssen.

Best Practice: AD-Migration vor Exchange-Migration

Allerdings hat es sich bewährt, die Migration der Domänen in ein Active Directory vor der Exchange-Migration abzuschließen oder möglichst weit voranzutreiben. Zum einen ist damit das Active Directory längere Zeit verfügbar, hat seine Funktion bewiesen, und die Administratoren haben das entsprechende Know-how für den Betrieb aufgebaut. Zum anderen sind die Vorteile des Active Directory auch ohne Exchange ein hinreichender Grund für die Einführung.

Die Migration zu Exchange gestaltet sich einfacher, wenn die Komplexität während der Exchange-Migration nicht durch die Umstellung von Gruppen, Verteilern, Profilen und Arbeitsplätzen erhöht wird. Gerade im Hinblick auf die Active Directory Connector-Replikation sollten sich die AD-Strukturen im Zusammenhang mit Organisationseinheiten und Berechtigungen möglichst nicht ändern. Zu leicht wird vergessen, die entsprechende Anpassung in Exchange nachzupflegen.

12.2.3 Die Funktion des ADC

Für die Migration von Exchange 5.5 nach Exchange 2003 ist der *Active Directory Connector* (ADC) eine Schlüsselkomponente, ohne den Sie die Migration innerhalb der gleichen Organisation nicht durchführen können.

ADC synchronisiert Exchange-Informationen

Exchange 2003 benötigt die Adressinformation der Postfächer aus dem Active Directory, um Nachrichten zustellen und weiterleiten zu können. Exchange 5.5 hingegen speichert diese Informationen in der lokalen Verzeichnisdatenbank (DIR.EDB). Damit die Zusammenarbeit reibungslos funktioniert, müssen diese Informationen zwischen beiden Systemen synchronisiert werden. Diese Aufgabe übernimmt der Active Directory Connector mit den Verbindungsvereinbarungen (Connection Agreement, CA). Die Verbindungsvereinbarungen sind vom Administrator zu erstellen! Der ADC muss nicht zwingend auf einem Exchange-Server installiert werden. Sie können den ADC unabhängig von Exchange auch auf einem Domänencontroller oder einem anderen Server installieren. Auch ohne die Einführung von Exchange 2003 kann der ADC Ihnen die Verwaltung der Exchange 5.5-Benutzer vereinfachen, da Sie auch die Exchange 5.5-Eigenschaften in der Management-Konsole für Benutzer und Computer bearbeiten können. Aus diesem Grund war der ADC auch auf der Windows 2000 Server, als es Exchange 2000 noch nicht gab. In gemischten Umgebungen mit vielen Exchange 5.5-Servern und den entsprechenden Verbindungsvereinbarungen sollten Sie die Administration der Benutzer

trennen. Hier gilt die Devise: Exchange 5.5-Benutzer werden mit dem Exchange 5.5-Administratorprogramm bearbeitet, und die Exchange 2003-Benutzer mit der MMC für Benutzer und Computer.

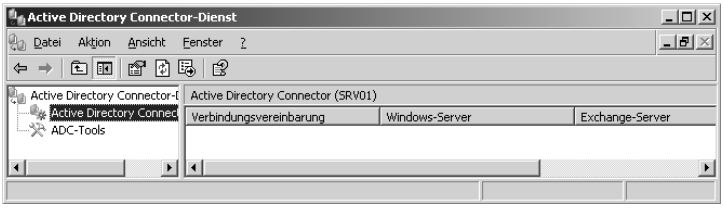


Abbildung 12.7 Management-Konsole des ADC

In der Management-Konsole des ADC müssen Sie manuell die entsprechenden Verbindungsvereinbarungen anlegen. Seit Exchange 2003 unterstützen die ADC-Tools diesen Schritt. Folgende Objekte werden durch den ADC repliziert:

- Benutzer

  Mailbox-enabled User

  Allen Exchange 5.5-Postfächern wird ein Benutzer im Active Directory zugeordnet, und die Exchange-Eigenschaften werden eingetragen. Damit kennen die Exchange 2003-Server auch alle Exchange 5.5-Postfächer. Weiter werden alle Exchange 2003-Benutzer vom ADC in Exchange 5.5 als Postfach eingetragen. Sie müssen sicherstellen, dass alle Postfächer repliziert werden, da ansonsten Nachrichten teilweise unzustellbar sind.

- Verteiler und Exchange-Gruppen

  USG/UDG

  Exchange 5.5-Verteiler werden im Active Directory als universelle Verteiler- oder Sicherheitsgruppen mit den entsprechenden Exchange-Attributen angelegt. Umgekehrt werden Exchange-aktivierte Gruppen aus dem Active Directory in Exchange 5.5 als Verteiler angelegt. Die Liste der Mitglieder wird ebenfalls synchronisiert.

- Öffentliche Ordner

  Public Folder-E-Mail-Adresse

  In Exchange 5.5 hatte jeder Öffentliche Ordner zwingend eine E-Mail-Adresse. Damit Exchange 2003-Server diese Adresse kennt, repliziert die entsprechende Verbindungsvereinbarung die Informationen in die spezielle Organisationseinheit „*Microsoft Exchange System Objects*“. Solange Sie noch Exchange 5.5-Server in Ihrer Organisation betreiben, ist jeder Ordner immer E-Mail-aktiviert. Auch diese Verbindungsvereinbarung ist durch den Administrator korrekt einzurichten.

- Konfiguration

  Diese besondere Verbindungsvereinbarung kann nicht manuell verändert werden, sondern wird von dem Standortreplikationsdienst (Site Replication Service, SRS) gepflegt. Sie dient dazu, die Konfiguration der Exchange 5.5-Organisation (Server, Connectoren etc.) mit den Konfigu-

rationseinstellungen von Exchange 2003 im Active Directory abzugleichen.

Als Faustregel benötigen Sie für jeden Exchange 5.5-Standort mindestens eine Verbindungsvereinbarung für die Synchronisation der Benutzer und Verteiler sowie eine zweite Verbindungsvereinbarung für die Öffentlichen Ordner. Wenn Sie mehrere Empfängercontainer in Exchange 5.5 und Organisationseinheiten im Active Directory unterscheiden, kann die Anzahl der Verbindungsvereinbarung sehr schnell in die Höhe schnellen. In größeren Firmen beansprucht allein die Planung und Installation aller Verbindungsvereinbarungen einige Zeit. Die Einrichtung aller Verbindungsvereinbarungen ist aber notwendig, ehe der erste Exchange 2003-Server installiert werden darf.

Object-CA's

Wir unterscheiden hier im Hinblick auf die Objekte drei verschiedene Typen von Verbindungsvereinbarungen des ADC:

- Empfängerverbindungsvereinbarungen für Benutzer, Verteiler und Kontakte (Recipient Connection Agreement). Sie müssen diese manuell erstellen.
- Öffentliche Ordner-Verbindungsvereinbarung für den Austausch der Ordner-E-Mail-Adressen (Public Folder Connection Agreement). Auch diese Verbindungsvereinbarungen müssen Sie erstellen.
- Konfigurations-Verbindungsvereinbarung für die Synchronisation der Konfiguration (Config-CA), die vom System erstellt wird.

Ziel und Quelle definieren

Jede Verbindungsvereinbarung enthält ein oder mehrere Quellen und ein Standardziel. Die Quellen weisen die Verbindungsvereinbarung an, die entsprechenden Empfängercontainer oder Organisationseinheiten auf Veränderungen zu überprüfen. Das Ziel ist das Standardziel für neue Objekte.

Replikationsrichtung

Ferner gibt es verschiedene Arten der Replikation. Hier stehen Ihnen drei unterschiedliche Richtungen zur Verfügung

- Von Exchange zu Windows (One-Way)

  Alle Objekte werden vom Exchange 5.5 in die Ziel-OU im Active Directory repliziert, und neue Exchange 5.5-Postfächer werden dort als Mailbox-Enabled-User angelegt.

- Von Windows zu Exchange (One-Way)

  Alle Exchange-aktivierten Objekte der Quell-OU werden in den Ziel-Empfängercontainer von Exchange 5.5 repliziert. Neue Objekte werden dort angelegt.

- In beide Richtungen (Two-Way)

  Der Ziel-Container in Exchange 5.5 stellt bei der Replikation den Quell-Container für Windows dar, sowie umgekehrt. Dieses CA garantiert eine

Synchronisation der Objekte in beide Richtungen und ist für das Verschieben von Postfächern erforderlich.

Best Practice

Achtung! Für jede Exchange Mixed Site müssen Sie unbedingt ein Two-Way-Connection Agreement erstellen. Es macht daher Sinn, diese sofort einzurichten und nicht erst später von einem One-Way-CA in ein Two-Way-CA zu ändern.

Bei der ersten Replikation versucht der ADC die entsprechenden Objekte richtig zuzuordnen. Hierbei bedient er sich bei der Replikation von Exchange 5.5 zum Active Directory der SID des Postfachbenutzers und versucht, diese im Active Directory zu finden. Kann der ADC dieses Objekt auflösen, dann fügt er die Exchange-Eigenschaften an diesen Benutzer an, selbst wenn dieses Objekt in einer anderen OU als der Ziel-OU liegt. Nur wenn der ADC keinen passenden Benutzer findet oder dem Konto bereits ein anderes Exchange-Postfach zugewiesen ist, legt der ADC einen neuen deaktivierten Benutzer im Standardziel an. Damit ist sichergestellt, dass auch die Exchange 2003-Server dieses Postfach kennen und Nachrichten dorthin weiterleiten können.

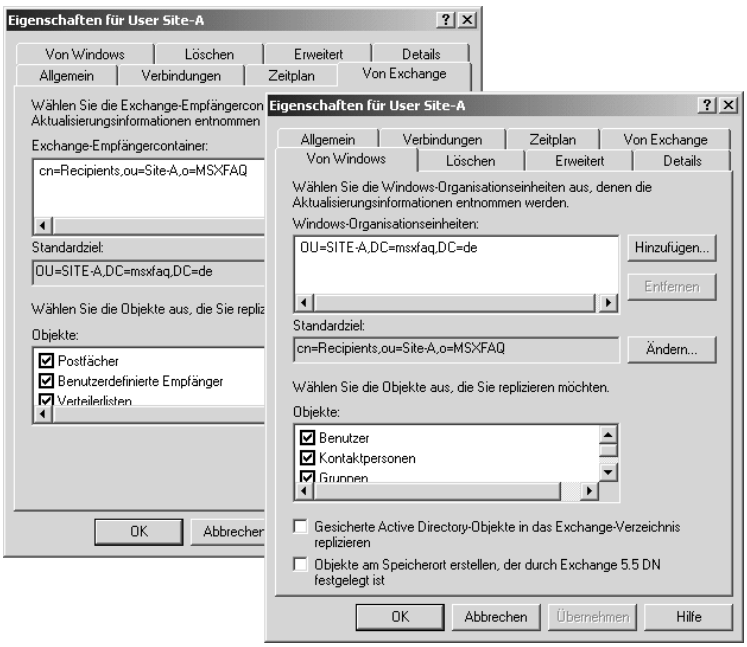


Abbildung 12.8 Einstellungen einer Recipient-CA

Benutzer, die nach der ersten Replikation verschoben wurden, kann der ADC durchaus auch an anderen Stellen verändern. Dazu pflegt der ADC eine eindeutige Kennzeichnung im Feld „ADC Global Names“ bei den einzelnen Objekten, so dass der ADC die einmal miteinander verbundenen Objekte immer wieder findet. Für die Korrektur einer falschen Verbindungsvereinbarung bedeutet dies, dass Sie dieses Feld bei den Objekten erst

löschen müssen. Ansonsten geht der ADC davon aus, dass diese Objekte schon von einem anderen Server repliziert werden. Doch ohne hinreichende Erfahrung damit sollten Sie besonders vorsichtig beim direkten Verändern der Attribute sein. Besonders Platzhalter-Objekte erfordern eine gesonderte Behandlung. Testen Sie diese Änderungen zuerst in einer Laborumgebung.

Zuordnung: OU - Empfängercontainer sicherstellen

Problematisch wird es, wenn bei der Replikation vom Active Directory zur Exchange 5.5-Organisation einige Benutzer in bestimmten Organisationseinheiten liegen, die von keiner Verbindungsvereinbarung überwacht werden. Wird solch ein Konto für die Benutzung von Exchange 2003 aktiviert, wird kein entsprechender Eintrag in Exchange 5.5 vorgenommen, und die Verzeichnisse sind nicht mehr synchron. Im einfachsten Fall erhält dieser Benutzer keine E-Mails aus der Exchange 5.5-Umgebung. Für einen längeren Parallelbetrieb sollten Sie eine regelmäßige Kontrolle der globalen Adressbücher in Exchange 5.5 und Exchange 2003 vorsehen. So erkennen Sie früh Inkonsistenzen in der Replikation.

ADC-Tools

Seit Exchange 2003 wird ein aktualisierter Active Directory Connector ausgeliefert, dessen Management-Konsole einen Assistenten (ADC-Tools) zur Einrichtung der entsprechenden Verbindungsvereinbarungen enthält. Hinzu kommt, dass Exchange 2003 bei der Installation abfragt, ob Sie Exchange 2003 in eine bestehende Organisation integrieren möchten. Ist dies der Fall, wird zusätzlich geprüft, ob diese ADC-Tools in Ihrer Organisation schon ausgeführt wurden.

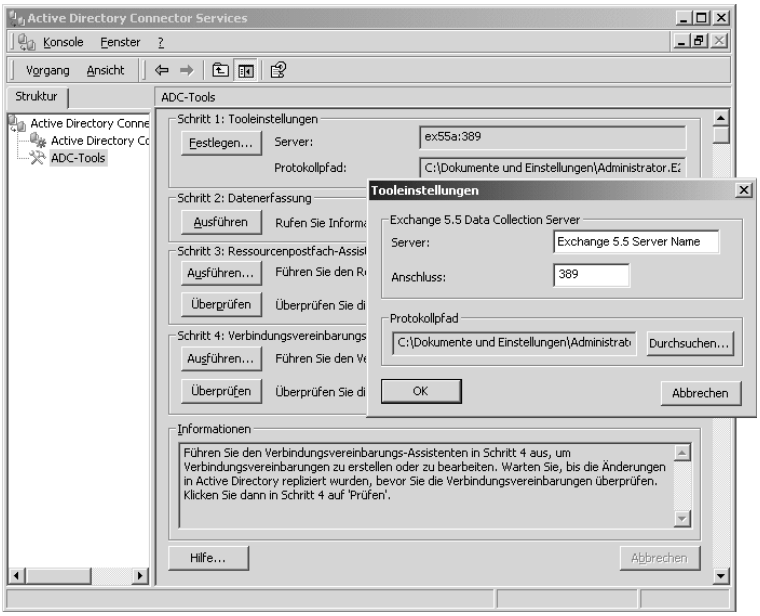


Abbildung 12.9
ADC-Tools

Diese Absicherung soll grobe Fehlkonfigurationen verhindern, aber kann natürlich nicht auf Dauer die korrekte Funktion sicherstellen.

- Im ersten Schritt müssen Sie einen Exchange 5.5-Server angeben, aus dem die ADC-Tools die bestehende Struktur der Exchange 5.5-Organisation auslesen. Dieser Server muss das Protokoll LDAP aktiviert haben und möglichst Ihre gesamte Exchange 5.5-Organisation kennen. Probleme mit dem Verzeichnisabgleich in Exchange 5.5 müssen Sie vorher beseitigen. Speziell wenn der Exchange 5.5-Server auf einem Windows 2000 Domänencontroller installiert ist, muss der LDAP-Port entsprechend korrigiert werden.
- Im zweiten Schritt wird die komplette Information über die Organisation ausgelesen und in einer XML-Datei abgelegt.
- Der dritte Schritt analysiert die gewonnenen Daten und versucht, alle Postfächer zu finden, für die das primäre Windows NT-Konto nicht eindeutig ist. Dies trifft oft für Ressourcenpostfächer zu, da ein Benutzer neben dem eigenen Postfach z.B. noch ein Support-Postfach besitzt. Solche Konstruktionen sind mit Exchange 2003 nicht möglich und sollten aufgelöst werden. Der Eintrag von „NTDSNoMatch“ in „Extention Attribute 10“ weist den ADC später an, diese Konten nicht einem bestehenden Benutzer zuzuweisen, sondern einen neuen AD-Benutzer für diese Ressource anzulegen. Der Assistent erlaubt die einfache Auswahl, welches Postfach das richtige Benutzerpostfach ist, und stellt sicher, dass die Rechte für den späteren Zugriff korrekt gesetzt werden.

NTDSNoMatch für Ressourcen-Postfächer

- Der vierte Schritt startet den Assistenten zum Einrichten der Verbindungsvereinbarungen. Die für den Betrieb notwendigen CAs werden bestimmt und können sofort angelegt werden. In den meisten Fällen ist diese bequeme Möglichkeit sogar die zuverlässigste Variante, nur in komplexeren Umgebungen sollten Sie selbst die Verbindungsvereinbarungen einrichten. Der Assistent kann dann in einem zweiten Durchlauf als Kontrolle gute Dienste leisten und Inkonsistenzen für Sie ausfindig machen.

Unterschätzen Sie nicht den ADC.

Die Einrichtung und der Betrieb der Verbindungsvereinbarungen ist ein wichtiger Bestandteil der Migration, und diese Funktion muss während der gesamten Migration bis zur Abschaltung des letzten Exchange 5.5-Servers funktionsfähig bleiben. Denken Sie bei jeder Veränderung von Organisationseinheiten oder Empfängercontainern daran, auch die Verbindungsvereinbarungen gegebenenfalls anzupassen. Bei der Deinstallation von Exchange 5.5-Servern oder Windows Domänencontrollern müssen Sie prüfen, ob eine bestehende Verbindungsvereinbarung dadurch unwirksam wird und diese anpassen. Besondere Beachtung gelten den bisherigen Standorten mit Exchange 5.5, die nach Exchange 2003 migriert und deren letzter Exchange 5.5-Server entfernt wurde. Der SRS übernimmt dann in diesem Standort auf dem Port 379 die Aufgabe des vorherigen Exchange 5.5-Servers und dient als Replikationspartner für die Exchange 5.5-Welt.

Inter-Org-CA und Fremdsysteme

Der ADC kann auch dazu genutzt werden, Adressen aus anderen Verzeichnisdiensten per LDAP abzufragen und entsprechende Kontakte im Active Directory anzulegen. Diese Funktion ist nicht für die Migration erforderlich, sondern erlaubt den Austausch von Empfängerinformationen zwischen unterschiedlichen Exchange 2003-Organisationen oder anderen Verzeichnisdiensten.

Bei der Integration einer anderen Exchange-Organisation in Ihre Exchange 2003-Organisation können Sie organisationsübergreifende Verbindungsvereinbarungen (Inter-Org-CA) einrichten, mit deren Hilfe Sie die Adressinformationen der Benutzer übernehmen können und somit einen Parallelbetrieb für den Migrationszeitraum ermöglichen. Mittels Inter-Org-CA können Sie auch aktive Benutzer im Active Directory anlegen lassen.

Für die Migration von Lotus Notes oder Novell GroupWise ist der ADC nicht notwendig. Der Abgleich der Verzeichnisse zwischen dem fremden E-Mail-System und Exchange 2003 übernimmt die Verzeichnisreplikation des entsprechenden Connectors. Diese Komponente legt im Active Directory die entsprechenden Kontakte mit den externen E-Mail-Adressen an, die später bei der Migration schrittweise durch Postfächer ersetzt werden.

12.2.4 Standortreplikationsdienst

Der Standortreplikationsdienst (SRS) ist eine weitere wichtige Komponente für die Migration von Exchange 5.5 nach Exchange 2003. Da Exchange 2003 wesentliche Teile der Konfiguration im Active Directory ablegt, die Gegenseite Exchange 5.5 jedoch die eigene Verzeichnisdatenbank DIR.EDB nutzt, muss es einen Weg geben, auch diese beiden Informationen abzugleichen.

SRS synchronisiert Exchange-Infrastruktur

Diese Funktion erfüllt der Standortreplikationsdienst in Verbindung mit dem Active Directory Connector-Dienst. Der SRS ist allerdings nur notwendig, wenn Sie innerhalb einer Organisation sowohl Exchange 5.5 als auch Exchange 2000/2003-Server installieren.

Bei der Installation des ersten Exchange 2003-Servers in einen bestehenden Exchange 5.5-Standort wird der SRS automatisch mit installiert, die Config-CA eingerichtet und gestartet. Bei allen anderen Exchange 2003-Servern wird der Dienst zwar installiert, aber nicht gestartet und keine entsprechende Verbindungsvereinbarung eingetragen. Damit gibt es diesen Dienst in jeder gemischten Administrativen Gruppe genau einmal. Sie können zur Redundanz den SRS manuell bei weiteren Exchange 2003-Servern konfigurieren und starten. In Exchange 5.5-Standorten, die keinen Exchange 2003-Server enthalten, gibt es genauso wenig einen SRS-Dienst wie in den neu eingerichteten Exchange 2003 Administrativen Gruppen.

SRS simuliert Exchange 5.5-Server

Der SRS stellt sich für die Exchange 5.5-Server wie ein weiterer Exchange 5.5-Server dar, der auch in die Replikation des Verzeichnisdienstes (DIR.EDB) innerhalb des Standorts mit einbezogen wird, als würde auf dem Exchange 2003-Server zusätzlich noch ein rudimentärer Verzeichnisdienst von Exchange 5.5 laufen. Der SRS ist jedoch unabhängig vom eigentlichen Exchange 2003-Server.

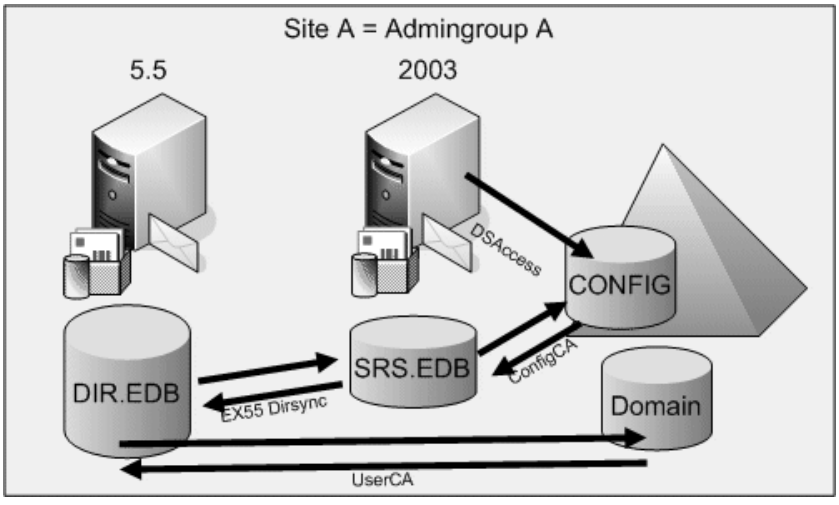


Abbildung 12.10 SRS-Funktion in einer gemischten Umgebung

Alle Informationen über Connectoren und Standorte in der Exchange 5.5-Umgebung werden über den normalen Exchange 5.5-Verzeichnisabgleich (Dirsync) auch in die SRS-Datenbank repliziert. Der Active Directory Connector liest mit der besonderen Verbindungsvereinbarung (ConfigCA) diese Informationen aus und repliziert diese mit dem Active Directory. Von dort erhalten die Exchange 2003-Server alle Exchange 5.5-Informationen.

Configuration-CA

Installieren Sie in Exchange 2003 neue Connectoren oder Server, dann werden diese Informationen vom ConfigCA gelesen und in die SRS-Datenbank geschrieben. So erhält auch die Exchange 5.5-Umgebung davon Kenntnis.

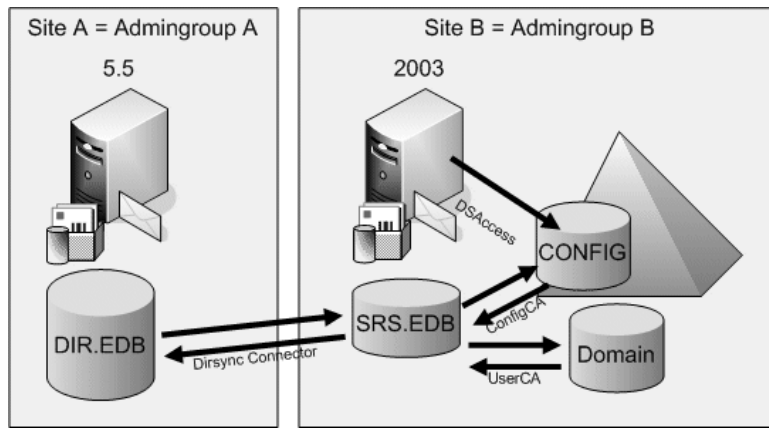
Der Abgleich der Benutzerinformationen erfolgt unabhängig hiervon über die Verbindungsvereinbarungen für Benutzer und Verteiler.

SRS und Administrative Gruppen ohne Exchange 5.5-Server

ADC-CA auf SRS verweisen

Findet die Migration eines Exchange 5.5-Standortes auf Exchange 2003 statt, dann sollte der SRS-Dienst bestehen bleiben, bis der letzte Exchange 5.5-Server in der *gesamten Organisation*, und nicht nur in diesem Standort entfernt worden ist. Zur Deinstallation des letzten Exchange 5.5-Server in diesem Standort müssen Sie alle betroffenen Verbindungsvereinbarungen umstellen. Der SRS übernimmt die Aufgabe, als Gegenstelle für den ADC zu fungieren, damit weiterhin alle Benutzer und Gruppen dieser reinen Exchange 2003-Administrativen Gruppe in der Exchange 5.5-Umgebung sichtbar werden.

Abbildung 12.11 SRS in einer nativen AG



DirSync auf SRS verweisen

Damit die Synchronisation der Infrastruktur weiterhin zwischen allen Standorten bzw. Administrativen Gruppen funktioniert, müssen Sie die Exchange 5.5-Verzeichnisreplikation anpassen oder ggf. einrichten. Auch die Exchange 5.5-Connectoren zur Verzeichnisreplikation (DirSync) müssen im Laufe der Migration auf den SRS umgestellt werden. Dazu müssen Sie sich

mit dem Exchange 5.5-Administrator auf den SRS-Server verbinden und die Änderungen durchführen.

SRS und native Administrative Gruppe

Eine weitere Besonderheit kommt der SRS-Datenbank zu, wenn Sie im Laufe der Migration eine neue Administrative Gruppe hinzufügen, in der nur Exchange 2003-Server installiert sind. Da diesem Standort niemals ein Exchange 5.5-Server installiert wurde, kann folglich auch kein ADC-Connection Agreement für Benutzer und Gruppen zu diesem Server eingerichtet werden. Die Einrichtung eines SRS für diese Funktion in einer nativen AG wird von der Management-Konsole aber auch nicht erlaubt. Der Abgleich der Benutzer und Verteiler ist indessen notwendig, da sonst die Empfänger dieses Standortes nicht in der Exchange 5.5-Umgebung sichtbar werden.

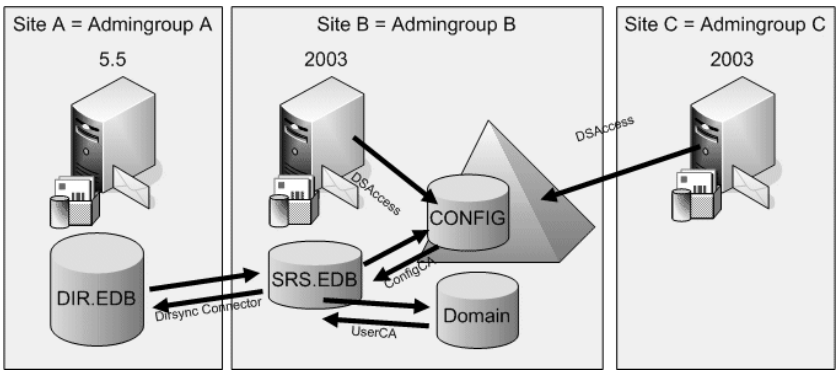


Abbildung 12.12 CAs mit einer Administrativen Gruppe ohne SRS

Hier kommt eine Besonderheit des SRS zum Tragen, die ein Exchange 5.5-Verzeichnisdienst nie leisten kann. Ein Exchange 5.5-Verzeichnisdienst kann nur die Daten im eigenen Standort ändern, alle replizierten Informationen aus entfernten Standorten sind für Exchange 5.5 generell „Read only“. Der SRS hingegen erlaubt auch die Modifikation der Objekte von anderen Standorten in seiner Datenbank.

CAs nutzen SRS einer Mixed AG

In Verbindung mit einer Recipients-CA für „C“ übernimmt der SRS einer anderen Administrativen Gruppe („B“) die Aufgabe, die Benutzer von „C“ in das Exchange 5.5-Verzeichnis einzutragen. Dazu müssen Sie jedoch eine Verbindungsvereinbarung für die Benutzer und Gruppen vom Active Directory zu diesem SRS einrichten. Ferner fügt der SRS auch die Connectoren (z.B. einen SMTP-Connector) der AG „C“ in die Exchange 5.5-Infrastruktur ein, ohne dass Sie dafür ein eigenes ConfigCA einrichten müssten.

SRS und Exchange 5.5-Administrator

Da die SRS-Datenbank eine ähnliche Funktion übernimmt wie der Verzeichnisdienst eines Exchange 5.5-Servers, können Sie sich mit dem Exchange 5.5-Administrator an die SRS-Datenbank verbinden. Der SRS-Dienst pflegt jedoch keine Benutzer in der Datenbank, sondern holt die Informationen direkt aus dem Active Directory. Dies ist auch der Grund, warum Sie im Exchange 5.5-Administrator zwar die Standorte anzeigen können, aber die Ansicht der Benutzer in den einzelnen Empfängercontainern fehlschlägt.

Anzeige der SRS-GAL über Exchange 5.5-Administrator

Sie können mit dem Exchange 5.5-Administrator aber jederzeit die *Globale Adressliste* (GAL) über den SRS kontrollieren. Die Anzahl der Objekte sollte nicht von der Globalen Adressliste Ihres Exchange 5.5-Servers abweichen. Ansonsten müssen Sie den Grund suchen, warum einige Empfänger nicht repliziert werden. Meist ist eine Fehlkonfiguration bei den Verbindungsvereinbarungen des Active Directory Connectors die Ursache.

12.2.5 Migration der Inhalte

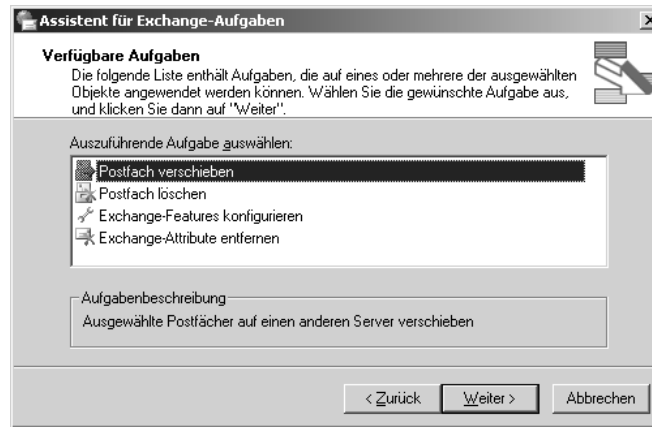
Die wichtigsten Informationen eines Nachrichtensystems sind die Inhalte, die Sie von dem bisherigen System auf das neue migrieren. Im Wesentlichen handelt es sich hierbei um die Informationen in den Postfächern und gemeinsamen Bereichen.

Migration Postfächer

Move Mailbox

Bei der Migration innerhalb der gleichen Exchange-Organisation können die Benutzer sehr problemlos von einem Server auf den neuen Server verschoben werden, solange sich beide Server in der gleichen Administrativen Gruppe befinden. Über das Kontextmenü der Management-Konsole für Benutzer und Computer (Abbildung 12.13) kann die Aktion gestartet werden.

Abbildung 12.13 Postfach mit der MMC verschieben



Innerhalb der AG

Dabei verbindet sich die Management-Konsole mit beiden Servern und überträgt die Nachrichten auf den neuen Server. Nach der erfolgreichen Übertragung werden Attribute, wie der Home-Server, im Active Directory und Exchange 5.5-Verzeichnis entsprechend angepasst. Der Anwender sollte während der Migration nicht mit dem Postfach verbunden sein und kann nach Abschluss der (ADC-)Replikation wie gewohnt weiter arbeiten. Die Berechtigungen, Ansichten, Regeln etc. bleiben erhalten. Das MAPI-Profil wird automatisch aktualisiert. Nur Benutzer, die mit POP3/IMAP4 auf den Server zugreifen, müssen den neuen Namen in Ihrer Anwendung eintragen.

In andere AG

Die Migration der Anwender in eine andere Administrative Gruppe bedeutet aus Sicht von Exchange 5.5 einen Umzug in einen anderen Standort. Dies ist weiterhin nur über einen Export der Informationen in eine PST-Datei und die Neuanlage des Anwenders zu realisieren und entsprechend aufwändig. EXMERGE ist das passende Werkzeug, um die Postfachinhalte mehrerer Anwender zu exportieren und nach der Neuanlage im neuen Standort wieder zu importieren. Allerdings sollten Sie diese Umstellung verzögern, bis die Exchange-Organisation in den Native Mode geschaltet wurde. Erst dann können Sie Postfächer zwischen Administrativen Gruppen verschieben.

Von „extern“

Bei der Migration der Inhalte von Drittsystemen erfolgt die Übernahme der Daten häufig über den Exchange-Migrations-Assistenten, der mittels des entsprechenden Clients (Notes, GroupWise oder IMAP4) die Informationen aus dem bisherigen E-Mail-System exportiert und in Exchange importiert. Zu beachten sind hierbei Sonderfälle, wenn die Anwender im Postfach nicht unterstützte Daten oder auch GroupWise-Archive oder lokale Notes-Datenbanken unterhalten. Damit im gleichen Schritt diese Inhalte migriert werden, müssen die Daten durch den Anwender vorab in das Postfach importiert werden.

Festplattenplatz laufend überprüfen

Sowohl dieser Import als auch die Migration der Benutzer auf Exchange-Server bedeutet temporär einen zusätzlichen Bedarf an sehr viel Festplattenplatz. Ebenso wachsen die Transaktionsprotokolle der Exchange-Datenbank bei der Migration der Postfächer sehr schnell an, dem Sie entgegenwirken sollten. Entweder führen Sie in der Zwischenzeit ein Backup aus, oder Sie aktivieren für den Zeitraum der Migration die Umlaufprotokollierung. Achten Sie auch darauf, dass keine Postfachbeschränkungen auf dem Exchange 2003-Server den Import stören.

Migration Öffentliche Ordner

Public Folder Replication

Die Öffentlichen Ordner von Exchange 5.5 werden über die Replikation der Inhalte nach Exchange 2003 migriert. Die Public Folder-Hierarchy wurde bereits bei der Installation des ersten Exchange 2003-Servers in der neuen Umgebung bekannt gemacht. Das Hinzufügen des neuen Servers in die Liste der Replikationspartner ist seit Exchange 2003 mit dem Skript

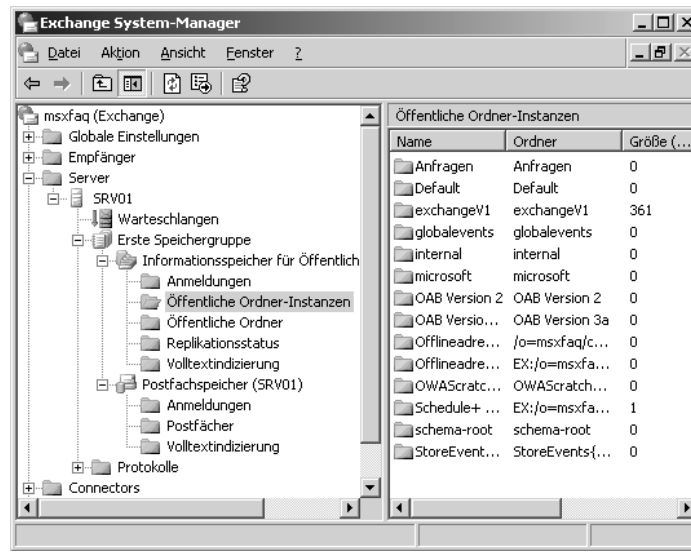
„pfmigrate.wsh“ einfacher möglich. Zuvor musste jeder Ordner einzeln oder komplette Strukturen auf einen Schlag im Exchange 5.5-Administrator angepasst werden. Nach der Replikation der Ordner müssen Sie im zweiten Schritt die Replikate von den bisherigen Exchange-Servern entfernen, ehe Sie diese deinstallieren können.

Auch hier gilt es, einige Besonderheiten zu beachten:

- Replikationszeitplan

  Prüfen Sie, ob die Ordner auch wirklich repliziert werden. Sowohl beim Ordner selbst als auch dem Informationsspeicher können Sie diese Werte anpassen. Da die Replikation durch einfache E-Mails erfolgt, kann dies einige Zeit dauern. Vor der Entfernung des alten Servers sollten Sie über die „Öffentlichen Ordner-Instanzen“ prüfen, ob alle Einträge repliziert sind (Abbildung 12.14).

Abbildung 12.14 Anzeige der Öffentlichen Ordner-Instanzen



  Allerdings wird die Replikation in Exchange so umgesetzt, dass ein Server zuerst alle lokalen Änderungen versendet, ehe der Ordner vom Server entfernt wird.

- Öffentliche Ordner-Rechte

  Exchange 2003 „rechnet“ die bisherigen MAPI-Berechtigungen von Exchange 5.5 in ACLs um. Prüfen Sie, ob dies erfolgreich war (Fehler-ID 9551 im Eventlog). Eventuell müssen Sie die Berechtigungen längst gelöschter Benutzer entfernen. Häufig ist das auch ein Hinweis darauf, dass noch nicht alle Benutzer aus Exchange 5.5 über eine Verbindungsvereinbarung in das Active Directory repliziert wurden. Ursache kann auch ein fehlender Trust zu einer NT 4-Domäne sein. Kontrollieren Sie

zudem, ob die E-Mail-Adressen der Öffentlichen Ordner in das Active Directory repliziert wurden (Public Folder-CA).

- Öffentliche Ordner-Verweise

  Der Anwender bekommt Abhängig von der Datenbank mit seinem Postfach einen Informationsspeicher für Öffentliche Ordner zugewiesen und erreicht somit alle Ordner in dieser Datenbank. Beim Zugriff auf Ordner, die nicht auf dem Server liegen, wird der Client an einen anderen Server in der gleichen Routinggruppe verwiesen, der ein Replikat des gewünschten Ordners hat. Exchange bietet auch die Möglichkeit, auf Öffentliche Ordner zuzugreifen, die sich nicht im gleichen Standort befinden. Der Zugriff auf Öffentliche Ordner in anderen Standorten erfolgte in Exchange 5.5 über eine explizite Konfiguration (Affinität). Dieser Weg wurde häufig genutzt, um Replikationskonflikte zu vermeiden, oder bei einem gelegentlichen Zugriff auf Replikate zu verzichten. Auch Exchange 2003-Benutzer können den Zugriff auf Ordner einer anderen Routinggruppe weiterhin nutzen. In den Eigenschaften des Routinggruppenconnectors können Sie die Verweise auf Öffentliche Ordner (Referral) allerdings explizit unterbinden (Abbildung 12.15). Damit unterscheiden sich die Voreinstellungen von Exchange 5.5 zu Exchange 2003.

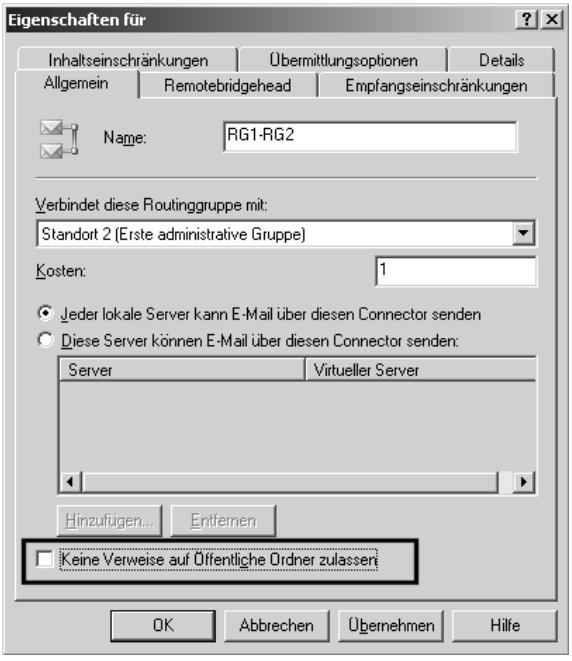


Abbildung 12.15 Öffentliche Ordner-Verweise bei Connectoren

Prüfen Sie, auf welche Ordner Ihre Benutzer zugreifen und überlegen Sie, ob Sie eine Replikation der Inhalte auf einen lokalen Server einrichten

oder sich für einen Verweis entscheiden. Beachten Sie dabei auch die Kosten der Connectoren.

- Transaktionsprotokolle

  Auch die Replikation der Ordnerinhalte als E-Mails bedeuten ein Anwachsen der Datenbank-Transaktionsprotokolle. Behalten Sie bei größeren Änderungen den freien Speicherplatz der Festplatten im Auge.

Bei der Migration von anderen Systemen gibt es keine allgemein gültigen Vorgehensweisen für die Übernahme der Daten in Exchange. Sofern die Informationen über News (NNTP) erreichbar sind, wäre hierüber eine Übernahme denkbar. Die Konzepte gemeinsamer Bereiche sind in anderen Systemen wie Lotus Notes und Novell GroupWise so unterschiedlich, dass hier individuelle Überlegungen angestellt und Migrationswege ermittelt werden müssen.

12.2.6 Migration der Connectoren

Parallel zur Migration der Inhalte können auch die Verbindungen der bisherigen Server zum Internet und zu anderen Diensten auf das neue System umgestellt werden. Bei der Migration von Exchange 5.5 nach 2003 müssen Sie auch die Verbindungen zwischen den Standorten entsprechend anpassen. Es ist problemlos möglich, parallel Connectoren im alten und neuem System zu betreiben und somit schrittweise die Umstellung ohne Unterbrechungen durchzuführen.

Besonders größere Firmen stellen sehr früh die Connector-Server auf Exchange 2003 um, weil sie von den verbesserten Routing-Fähigkeiten profitieren möchten.

Internet-Verbindung umstellen

Nur die eingehenden Verbindungen aus dem Internet müssen Sie dagegen direkt umstellen, anstatt parallel betreiben. Alle Nachrichten gehen dann nur noch auf dem neuen System ein. Die Umstellung ist problemlos, wenn die Adressbücher beider Systeme synchron sind. Nur dann kann das neue System auch die Benutzer auflösen, die noch nicht migriert sind und die Nachrichten zustellen.

12.2.7 Assistent für die Migration

Die Installation der Exchange-Verwaltungsprogramme installiert auch den "*Assistent für die Migration*" (Migration-Wizard) im Startmenü. Der Name könnte darauf hinweisen, dass dieser Assistent Sie durch alle Schritte einer Migration leitet. Dies ist jedoch nicht der Fall. Vielmehr handelt es sich hierbei um ein Hilfsprogramm, das einzig und allein die Inhalte eines fremden Systems bzw. fremder Organisation nach Exchange 2003 migriert.

Der „Assistent für die Migration“ ist nicht erforderlich, wenn Sie Anwender von einem Exchange-Server auf einen anderen Exchange-Server in der gleichen Administrativen Gruppe verschieben oder innerhalb einer Organisation von Exchange 5.5 nach Exchange 2003 migrieren.

Aber auch für die Migration von Fremdsystemen ist dieses Programm kein Assistent, der Ihnen die Einrichtung der Connectoren zu Lotus Notes und GroupWise abnimmt oder die Adressbücher zwischen verschiedenen E-Mail-Systemen abgleicht. Der Assistent für die Migration exportiert die Inhalte der ausgewählten Postfächer aus einem der unterstützten Quellsysteme nach Exchange 2003 (Abbildung 12.16).

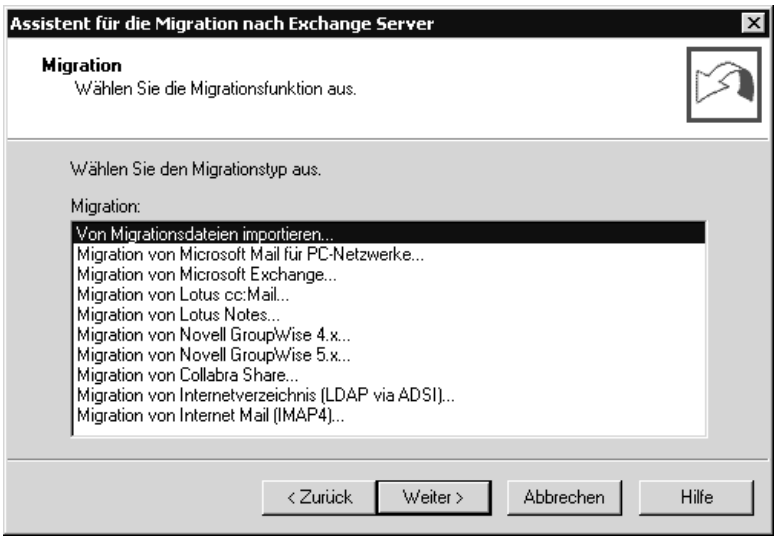


Abbildung 12.16 Exchange-Assistent für die Migration

Der Assistent kann aus den verschiedensten Quellen die Inhalte nach Exchange 2003 migrieren. Die Migration selbst kann dabei in einem Schritt oder in zwei Schritten erfolgen.

- Ein-Schritt-Migration

  Die Daten werden aus dem bestehenden System exportiert, in einem Verzeichnis zwischengespeichert und danach direkt in den Exchange 2003-Server importiert. Dies bedeutet, dass beide E-Mail-Server aktiv und erreichbar sein müssen.

- Zwei-Schritt-Migration

  Hierbei können die beiden Schritte Export und Import zeitlich getrennt ablaufen. Dies ist notwenig, wenn der aktuelle E-Mail-Server auch der neue Exchange 2003-Server wird und Sie die Daten einige Stunden zwischenlagern müssen. Diese Migration ist ebenfalls geeignet, die Daten über einen Standort hinweg zu übertragen, wenn die Verbindung

zwischen beiden Systemen die Übertragung der Datenmengen nicht zulässt.

Bei reinen Umzügen von Exchange-Postfächern bietet sich jedoch auch das Programm EXMERGE an, das die Inhalte mehrerer Postfächer in PST-Dateien exportieren und wieder importieren kann.

Bei der Migration von Benutzern aus einem fremden E-Mail-System übernimmt der Assistent jedoch nur die Aufgabe, die Inhalte zu übertragen. Die Einrichtung eines Lotus Notes- oder GroupWise-Connectors und der Abgleich der Adressen muss vom Administrator geleistet werden. Indessen übernimmt der Assistent auch Benutzer-Informationen wie Adress-Daten und E-Mail-Adressen von fremden Exchange 5.5-Organisationen.

Wann immer Sie den Assistent zur Migration einsetzen, sollten Sie folgende Schritte beachten und entsprechend die Migration planen:

Vor der Migration

- Auflösen von Archiven und lokalen Ablagen

  GroupWise, Notes, aber auch Exchange erlauben die Ablage und Archivierung von Nachrichten. Diese Daten sind in der Regel nur mit der Original-Anwendung lesbar. Damit Sie diese Daten migrieren können, müssen diese wieder in das Postfach zurück übertragen werden. Beachten Sie die temporär zusätzlich notwendigen Speicherplatzkapazitäten und eventuell gesetzte Postfachbeschränkungen.

  E-Mail-Systeme, die nur über POP3 erreichbar waren, kennen keine Ablage der Nachrichten auf dem Server. Hier muss die Migration der Daten direkt auf dem Client erfolgen. Manchmal ist es notwendig, die Daten erst mit Outlook Express aus der Fremdanwendung zu importieren und im zweiten Schritt diese Daten nach Outlook zu übernehmen.

- Notieren Sie Berechtigungen und Gruppenmitgliedschaften

Berechtigungen und Regeln gehen verloren

  Notieren Sie sich bisherige Gruppen, Verteiler und Berechtigungen. Die Migration der Daten erfolgt in ein neues Postfach, so dass diese Einstellungen eventuell von Hand nachgeführt werden müssen. Dies betrifft auch Regeln und Stellvertreterfunktionen.

- Verschlüsselte Dateien

  Immer mehr Anwender versenden und erhalten verschlüsselte Nachrichten (PGP, S/MMIME). Die verschlüsselten Nachrichten selbst können meist exportiert werden, aber Sie sollten vorab prüfen, ob die Nachrichten auch nach der Migration in Exchange 2003 entschlüsselt werden können. Eventuell müssen die Anwender Ihre Nachrichten vor der Migration erst unverschlüsselt abspeichern.

Während der Migration

Um eine korrekte Migration aller Daten zu gewährleisten, müssen Sie Vorkehrungen treffen, damit die Inhalte des Servers ab einem bestimmten Zeitpunkt nicht mehr verändert werden:

- Ausstehende Daten übertragen

  Vergewissern Sie sich, dass alle Benutzer bereits formulierte und zur Übertragung vorbereitete Nachrichten versenden bzw. mit dem Server synchronisieren. Dies ist besonders für die Anwendergruppe notwendig, die mit Ihrem Notebook unterwegs ohne eine Serververbindung arbeitet und nur ab und zu die Informationen repliziert. Neben Outlook unterstützen auch Notes, GroupWise und andere Clients diese Arbeitsweise.

- Zugriff der Anwender blockieren

  Nachdem alle Nachrichten der Anwender in das E-Mail-System übertragen wurden, müssen Sie verhindern, dass die Benutzer während der Migrationsphase auf die Daten zugreifen und diese verändern. Dies ist der schwierigste Punkt, da viele E-Mail-Systeme keine Funktion anbieten, um Anwender auszusperren. Die Deaktivierung des Anmeldekontos ist in Zeiten eines „Single Sign On“ nicht immer möglich, da damit jeder Zugriff auf andere Ressourcen ebenfalls blockiert wird. Ein Beenden der Dienste ist ebenfalls nicht möglich, da Sie selbst zur Migration darauf zugreifen müssen. Oftmals ist eine gezielte Änderung der IP-Leitwege ein gangbarer Weg, um kompletten Subnetzen den Weg zum Server zu verbauen. Exchange selbst kann dank eines speziellen Schlüssels in der Registrierung den Zugriff auf bestimmte Benutzer begrenzen. Der TechNet-Artikel „146764 XADM: Limiting Logons to the Information Store“ beschreibt das Vorgehen.

- Queues leeren und Empfang verhindern

  Daten-Versand und -Empfang blockieren

  Der letzte Schritt vor der Migration ist die Blockade neuer Nachrichten. Sorgen Sie dafür, dass alle Nachrichten in Warteschlangen noch übermittelt werden, aber eingehende Nachrichten den Server nicht mehr erreichen können. Beenden Sie dazu die entsprechenden Dienste und Connectoren. Sichern Sie diese Dienste gegen eine erneute irrtümliche Aktivierung durch Überwachungsprozesse oder andere Administratoren. Erst wenn alle Warteschlangen Ihres Servers leer sind, können Sie mit der Migration der Nachrichten beginnen.

- Server überwachen

  Bei der eigentlichen Migration sollten Sie sowohl den Quell- als auch den Zielserver überwachen. Die Übertragung von großen Datenmengen kann Datenbanken schnell wachsen lassen oder Server überfordern.

Nach der Migration

Nachdem das Postfach mit dem Migrations-Wizard auf den Exchange 2003-Server übertragen worden ist, sind weitere Nacharbeiten notwendig:

- Postfächer kontrollieren

  Testen Sie anhand der Größe und einer Anmeldung, ob die Migration die Inhalte korrekt und vollständig übernommen hat. Prüfen Sie als Administrator, ob die E-Mail-Adressen und sonstige Exchange-Eigenschaften des neuen Postfachs mit den alten Adressen übereinstimmen oder zumindest als zusätzliche Adressen hinzugefügt worden sind. Dies ist wichtig, damit Rückläufer und Antworten auf früher gesendete Nachrichten weiterhin ankommen.

- Verzeichnisreplikation sicherstellen

Verzeichnisse beider Seiten prüfen

  Sind beide Systeme über eine Verzeichnisreplikation verbunden, dann müssen Sie das Postfach nach der erfolgreichen Übernahme im alten System löschen, unsichtbar machen oder dessen E-Mail-Adresse entfernen, damit über einen Verzeichnisabgleich ein Kontakt bzw. externer Empfänger mit den alten Adressen angelegt werden kann. Existierte vorher ein AD-Kontakt für den Benutzer, dann müssen Sie diesen löschen, damit das neue Postfach diese E-Mail-Adresse erhält.

- Verteiler und Berechtigungen aktualisieren

  Das neue Postfach ist höchstwahrscheinlich noch nicht in den gleichen Verteilern aufgenommen, in denen es zuvor als Mitglied geführt war. Dies ist ebenso zu korrigieren wie die Zugriffsrechte dieses Benutzers auf andere Postfächer (Stellvertreterfunktion) und im Gegenzug auch die Berechtigungen anderer Benutzer auf dieses neue Postfach.

- Testnachrichten

  Senden Sie Testnachrichten in allen Variationen an das neue Postfach, von den Benutzern des gleichen Exchange 2003, sowie auch als Anwender des alten E-Mail-Systems und später auch aus dem Internet. Versenden Sie Nachrichten von diesem Postfach an andere Empfänger. Prüfen Sie auch die Antwortadresse und den angezeigten Namen auf ihre Richtigkeit. Den Test zum Empfang aus dem Internet sollten Sie erst durchführen, wenn alle Postfächer mit den richtigen E-E-Mail-Adressen ausgestattet sind.

- Archivierung und Sicherung

  Durch die Migration enthält das Postfach oft auch Nachrichten, die im bisherigen System bereits archiviert waren. Auch ein neuer Exchange-Server hat nur begrenzt Speicherplatz. Prüfen Sie, ob über die Archivfunktion von Outlook, Exmerge oder eine eigene Archivlösung diese Elemente aus dem produktiven Präsenzspeicher migriert werden

können. Danach sollten Sie auch die gewünschten Postfachrichtlinien bezüglich der Größe wieder aktivieren.

So kann Ihnen der Assistent für die Migration sehr gut dabei helfen, die Nachrichten aus den Postfächern Ihres alten E-Mail-Systems nach Exchange 2003 zu migrieren.

12.2.8 Stolperfallen bei der Migration

Wann immer eine Migration von einem System zu einem anderen System ansteht, müssen gewisse Einschränkungen in Kauf genommen werden. Die meisten Migrationen erlauben eine Übernahme der bestehenden Nachrichten und oft auch von Kontakten und Terminen. Aber da jeder Hersteller in gewisser Weise seine eigene Suppe kocht, wird es immer Informationen geben, die sich nicht reibungslos übernehmen lassen. Einige Beispiele sollen Sie für solche Probleme sensibilisieren. Einige Sonderfälle können durch eine geeignete Anpassung, Migration oder Skripte abgefangen werden.

- Globale Unterbrechung

  Lange Ausfälle vermeiden

  Aktualisieren Sie einen Server direkt, nimmt das System über einen Zeitraum von mehreren Stunden keine Nachrichten an. Zieht sich die Migration aufgrund von Problemen länger hin, ist es möglich, dass die Absender wartender Nachrichten eine Statusmeldung vom eigenen E-Mail-Server erhalten. Diese Meldungen weisen darauf hin, dass der Empfänger nicht erreichbar ist und das System weiterhin eine Zustellung versucht. Dies ist im Grund nicht kritisch, da die meisten Systeme im Internet die Zustellung bis zu drei Tage lang versuchen. Dennoch sollten Sie auf die entsprechenden Rückfragen der Mitarbeiter und Kunden gerüstet sein, die Sie über diesen „Missstand“ informieren möchten.

- Unterbrechungen pro Postfach

  Zeitplanung nutzen

  Wenn ein Postfach von einem Server zum anderen Server verschoben wird, dann ist für eine kurze Zeit dieses Postfach nicht erreichbar. Nachrichten in dieser kurzen Zeitspanne werden entweder unzustellbar oder landen in einem Postfach, das gerade gelöscht wird. Sie könnten einfach den kompletten Empfang für diese Zeit deaktivieren, aber damit stören Sie alle anderen Anwender ebenso, und eine Lösung für interne Nachrichten haben Sie damit noch nicht geschaffen. Seit Exchange 2003 können Sie die Verschiebung von Postfächern auch nach einem Zeitplan ausführen lassen.

- Quittungen

  Umgang mit Quittungen

  Stellen Sie sich vor, ein Anwender sendet eine Nachricht per Einschreiben. Ehe das Einschreiben kommt, wird der Anwender von dem System nach Exchange 2003 migriert. Diese Migration dauert einige Zeit,

und die Quittung des Empfängers erreicht Ihr System. Je nachdem, wie perfekt Ihre Migration erfolgt ist, wird die Quittung dem Benutzer auf dem Exchange 2003-Server zugestellt oder als unzustellbar verworfen. Aber selbst dann bleibt immer noch die Frage, ob Outlook eine Quittung der damals gesendeten Nachricht zuordnen kann.

- Antworten schlagen fehl

Rückmeldungen annehmen

Gerade leistungsfähige Nachrichtensysteme wie Notes, GroupWise und Exchange 5.5 nutzen intern nicht die SMTP-Adresse als Schlüssel für die Zustellung einer Nachricht, sondern eigene Adressen. Zwar sind nach der Migration alle Nachrichten vorhanden, aber die Rückmeldungen der Absender ist aufgrund der spezifischen alten Adresse eventuell nicht mehr zustellbar. Daher migriert Exchange in der Regel auch alle früheren E-Mail-Adressen des Benutzers mit. Dies funktioniert bei Notes und GroupWise recht gut. Bei anderen Systemen ist dieser Fall zu prüfen, und Sie müssen eventuell die Anwender informieren, dass bei einer Antwort die Empfängeradresse neu eingegeben oder aus dem aktuellen Adressbuch ausgewählt werden muss.

- Archive

Migration von Archiven

Diverse Programme beinhalten eigene Archivmöglichkeiten. Nicht nur Outlook erlaubt es, alte Nachrichten in ein Archiv abzulegen. In dem Fall ist es eine einfache PST-Datei. Auch GroupWise und Notes erlauben die Ablage in lokalen Dateien. Diese sind natürlich bei einer servergestützten Migration nicht erreichbar und mit der neuen Anwendung vermutlich nicht mehr zu öffnen. Prüfen Sie vorher, ob Ihr alter Server noch ausreichend Platz für die Rückübertragung dieser Daten hat, und denken Sie für Exchange 2003 über eine serverbasierte Archivierung nach. Lokale Archive sind nur für den privaten Einsatz zu gebrauchen.

- Änderungen im Produktverhalten

Veränderungen verschiedener Produkt-Versionen beachten

Eine Änderung im Verhalten von Exchange 2000 und 2003 hat einigen Administratoren bei der Migration von Exchange 5.5 vermehrt Probleme bereitet. Nachrichten an Öffentliche Ordner wurden nicht zugestellt, weil sich die Standardberechtigungen mit Exchange 2000 geändert haben. Nach der Korrektur dieser Einstellungen wurden die Nachrichten nicht mehr als „E-Mail“, sondern als „Notiz“ im Ordner abgelegt. Somit scheitern einige Programme zur automatisierten Weiterverarbeitung der Daten. Erst mit Exchange 2000 Service-Pack 3 und einem Hotfix können Sie diese Einstellung wieder zurückstellen. Auch Outlook 2003 bringt mit dem Cached Mode einen Festplattenkiller für die Arbeitsplätze mit sich. Bei mehreren Profilen mit einer eigenen großen OST-Datei kann speziell auf älteren Systemen der Platz auf der lokalen Festplatte knapp werden.

- Neue Standardwerte

  Grenzwerte und Default-Einstellungen

  Die Installation von Exchange 2003 setzt unter anderem neue Standardwerte im System. Wird eine bestehende Exchange-Organisation aktualisiert, werden die internen Nachrichten auf 10240 KB begrenzt. Ebenso entfällt seit Exchange 2000 per Default die Benachrichtigung an das Internet, die aufgrund von Regeln oder dem Abwesenheitsassistenten erzeugt wird. Öffentliche Ordner waren in Exchange 2000-Standardeinstellung für „anonyme" Absender nicht mehr erreichbar, in Exchange 2003 ist dies wieder möglich. Auch solche Aspekte sind bei einer Migration zu beachten.

- Nicht migrationsfähige Elemente

  Weiterleitung statt Migration?

  Speziell bei der Umstellung von Fremdsystemen werden Sie immer wieder auf besondere Elemente treffen, die nicht 1:1 nach Exchange 2003 zu konvertieren sind. So gibt es sowohl bei Lotus Notes als auch mit Novell GroupWise bestimmte Informationen, die nicht konvertiert werden können, da die zugrunde liegenden Prinzipien zu unterschiedlich sind. Andere Fremdsysteme bieten überhaupt keine Schnittstelle an, um die Informationen zu exportieren oder vom Client zu übernehmen. In solchen Fällen könnte die Weiterleitung aller Informationen an das neue Exchange-Postfach eine Lösung sein. Prüfen Sie auf jeden Fall vorab, welche Inhalte nicht oder nur teilweise migriert werden können.

Dieser kleine Abriss soll Ihnen aufzeigen, dass eine Migration mit zunehmender Firmengröße nicht mehr trivial ist und selbst die beste Dokumentation sowie die wirklich sehr guten Assistenten von Exchange 2003 nicht immer ausreichend sind. Selbst ein Update von Exchange 5.5 nach Exchange 2003 ist keineswegs ein einfacher Prozess. Zwar sind beide Produkte von Microsoft, aber die Unterschiede im Design sind sehr groß.

12.2.9 Allgemeine Überwachung

Sie haben anhand der Beschreibungen zum Active Directory Connector, zur Übernahme der Daten und bei vielen anderen Hinweisen schon bemerkt, dass eine Migration nicht ohne die Kontrolle der Systemumgebung ablaufen sollte. Die Einrichtung entsprechender Überwachungshilfen ist nicht erst nach dem Ende der Migration zur Sicherstellung des Regelbetriebs sinnvoll, sondern gerade auch vor und bei der Migration ein wichtiges Hilfsmittel zur Sicherstellung der Funktion. Die wichtigsten Prüfungen sind:

- Kontrolle des Eventlog

  Monitoring vor, während und nach der Migration

  Im Eventlog schreiben Exchange und Windows Fehlermeldungen und Warnungen, die Ihnen meist frühzeitig schon Hinweise auf aufkommende

Probleme melden. So stehen hier Fehler der Active Directory-Replikation, ebenso wie auch Probleme bei der Umrechnung von ACLs auf Öffentliche Ordner. Über die Karteikarte DIAGNOSEPROTOKOLL in den Eigenschaften des Exchange-Servers können Sie Exchange anweisen, viel mehr Informationen zu berichten.

- Kontrolle der ADC-Fehlerdateien

  Der Active Directory Connector legt je Verbindungsvereinbarung ein eigenes Verzeichnis unter dem Programmverzeichnis an (C:\Programme\MSADC\MSADC\<Name des CA>). Dort finden Sie Textdateien mit den Fehlern bei der Replikation. Besonders in dem Fall, dass Löschaktionen von den CAs nicht repliziert werden, müssen Sie diese Dateien regelmäßig kontrollieren und die erforderlichen Löschoperationen nach einer Prüfung manuell durchführen.

- Speicherplatz

  Prüfen Sie den freien Speicherplatz auf Ihren Servern. Gerade bei der Migration werden temporäre Daten und Transaktionsprotokolle sehr groß.

- Netzwerkfunktion

  Hilfsprogramme wie REPLMON, DCDIAG und NETDIAG helfen Ihnen bei der Suche nach Problemen im Active Directory und der Einbindung der Server in das Netzwerk. Speziell REPLMON kann nicht nur die Active Directory-Replikation überwachen, sondern bei Fehlern entsprechend eine E-Mail senden oder eine Nachricht im ohnehin überwachten Eventlog ablegen.

- Globales Adressbuch vergleichen

  Ob Ihr ADC richtig arbeitet, prüfen Sie mittels ADC-Tools. Als Stichprobe sollten Sie die Anzahl der Empfänger der globalen Adressliste in Exchange 5.5 mit der Anzahl der Empfänger in Exchange 2003 vergleichen. Unterschiede sollten Sie analysieren und korrigieren. In größeren Umgebungen lohnt es sich, den Prozess zu automatisieren und mit einem Skript die Einträge zu lesen und miteinander zu vergleichen.

Dies sind nur einige der Prüfungen, die für die Migration besonders wichtig sind. Diese Maßnahmen sind zusätzlich zu der allgemein vorgesehenen Überwachung der Systeme zu sehen.

12.3 Beispiele

Die folgenden Beispiele beschreiben die einzelnen Schritte der Migration und was Sie dabei besonders beachten sollten. Diese Methoden haben sich im

Laufe der letzten drei Jahre bewährt, aber im Einzelfall sind andere Migrationswege und Varianten der beschriebenen Beispiele besser geeignet.

Prüfen Sie auf jeden Fall vorab, z.B. in einer Testumgebung, ob Sie die einzelnen Schritte verstanden haben und diese Methode in Ihrer Umgebung einsetzbar ist. Die folgenden Kurzbeschreibungen sind keine ausreichende Grundlage für eine Migration. Für die meisten Migrationswege gibt es entsprechend ausführliche White Papers von Microsoft.

Besonders wenn Sie bei der Migration auch das Active Directory von Windows 2000 auf Windows 2003 aktualisieren, sollten Sie den TechNet-Artikel „Q325379 How to Upgrade Windows 2000 Domänencontrollers to Windows Server 2003“ gelesen und die notwendigen Änderungen durchgeführt haben.

12.3.1 Exchange 2000 nach Exchange 2003

Die Aktualisierung von Exchange 2000 nach Exchange 2003 stellt die sicher einfachste Variante dar (Abbildung 12.17).

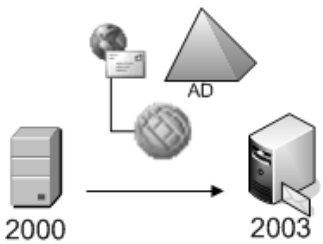


Abbildung 12.17 Exchange-In-Place-Update

Sofern alle anderen Programme mit Exchange 2003 kompatibel sind, können Sie dieses Update auf zwei Wege durchführen:

Update oder Move?

- In-Place-Update

  Soll die bestehende Hardware des Exchange 2000-Servers auch der neue Exchange 2003-Server sein soll, dann stellt ein In-Place-Update den schnellsten und einfachsten Weg dar. Sie müssen nur sicherstellen, dass alle bisher installierten Produkte (Virenscanner, Datensicherung, Fax-Connectoren etc.) auch mit Exchange 2003 arbeiten. Eine Unterbrechung von einigen Stunden sollten Sie jedoch einplanen.

  Das In-Place-Update des Servers auf Exchange 2003 ist auch der Weg, um das Betriebssystem auf Windows 2003 zu aktualisieren. Exchange muss hierbei zuerst aktualisiert werden, da Exchange 2000 nicht kompatibel mit Windows 2003 ist.

- Swing Server

  Ist der bestehende Server jedoch zu klein oder zu langsam, oder soll dieser abgelöst werden, stellt die Installation eines zweiten Servers in die

gleiche Administrative Gruppe und Routinggruppe den besten Weg dar. Zudem wird durch diese Migration vermieden, dass der komplette Server für einige Stunden nicht erreichbar ist.

Durch die Migration einzelner Postfächer und Öffentlicher Ordner sind nur diese für kurze Zeit nicht verfügbar. Zudem erlaubt diese Methode eine Veränderung der Hardware und die Neuinstallation auf einem frischen System. Das Restrisiko eines In-Place-Updates wird so umgangen. Nach der Verlagerung aller Inhalte und Connectoren kann der alte Server über das Exchange-Setup einfach deinstalliert werden.

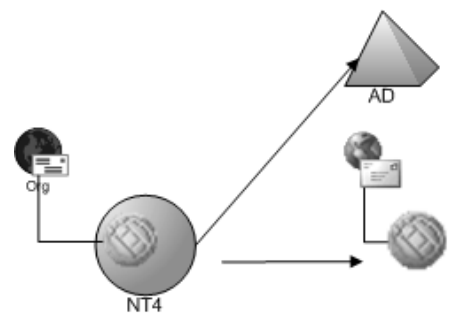
Diese Migration funktioniert auch problemlos, wenn noch andere Exchange 2000- oder Exchange 5.5-Server mit in der Umgebung sind. Wobei Sie darauf achten müssen, dass Sie die Funktion der SRS-Server und ADC ebenfalls umziehen müssen.

Bei der Installation wird das Schema des Active Directory für Exchange 2003 erweitert. Wenn Sie mehrere Domänen im Active Directory nutzen, dann sollten Sie vorab in allen Domänen ein „Setup /DomainPrep“ durchführen.

12.3.2 Exchange 5.5 nach Exchange 2003 (Single Site)

Viele Firmen nutzen nur einen einzigen Exchange 5.5-Server, der mitsamt der Windows NT 4-Domäne migriert werden soll. Dazu kommt, dass die Hardware meist schon sehr alt ist, so dass die langsame Migration von Exchange 5.5 nach Exchange 2000/2003 die am häufigsten durchgeführte Migration ist. Selbst wenn mehrere Exchange 5.5-Server vorhanden sind, ändert sich nichts am prinzipiellen Vorgehen.

Abbildung 12.18 Migration einer Site nach Exchange 2003



Move Mailbox innerhalb einer AG

Dabei wird nach der Active Directory-Migration und dem Einsatz des Active Directory Connectors ein Exchange 2003-Server in die Organisation installiert. Nach und nach werden die Inhalte verschoben, Connectoren umkonfiguriert und die Exchange 5.5-Server entfernt, bis am Ende alle Server mit Exchange 2000/2003 installiert sind. Die Migration zieht sich meist über mehrere Wochen hin, verursacht fast keine Unterbrechung für die

Anwender und kann schrittweise erfolgen. In diesem Beispiel wird davon ausgegangen, dass das Active Directory bereits installiert ist und die Benutzer im Active Directory arbeiten. Das primäre Windows NT-Konto in den Exchange 5.5-Postfacheigenschaften enthält bereits das AD-Konto.

Vor der Migration

Vor der Exchange-Migration wurde bereits ausgeführt:

- Neuaufbau oder Migration des Active Directory
- Migration der Benutzerkonten

  Übernahme der Benutzer und Exchange-Dienstkonten durch ein In-Place-Update des NT 4-PDC oder durch die Migration mit ADMT.
- Migration der Server

  Die Exchange 5.5-Server sind Mitgliedsserver oder Domänencontroller des aktuellen Active Directory.
- Exchange 5.5 Cleanup

  Die Exchange 5.5-Organisation wurde bereits bereinigt, d.h., nicht mehr benötigte Connectoren, alte Postfächer und überflüssige Ordner wurden entfernt. Über die DSI/IS-Konsistenzanpassung wurden die Rechte auf Öffentliche Ordner korrigiert. Die primären NT-Konten der Postfächer sind die Active Directory-Konten.

Die Migration selbst erfolgt nach folgendem Ablaufschema:

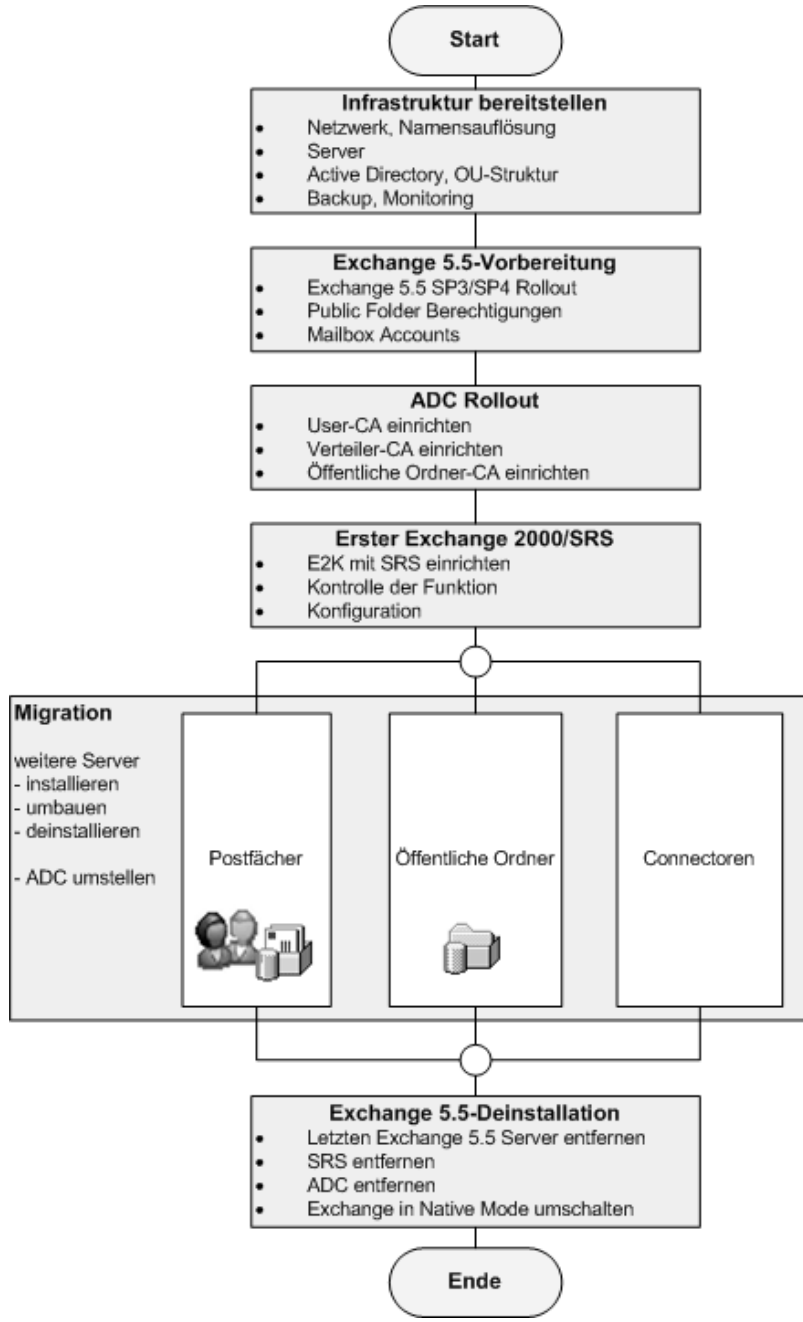


Abbildung 12.19 Ablaufdiagramm für die Migration eines Standorts

Migrationsphase

- Installation des Exchange 2003-ADC

  Durch die Installation des Active Directory Connectors wird das Schema für Exchange 2003 erweitert.

- Ausführen der ADC-Tools und Einrichtung der CAs

  Spätestens hier werden die ADC-Tools feststellen, wie korrekt Sie beim Aufräumen Ihrer Exchange 5.5-Umgebung gearbeitet haben. Nach der Einrichtung der Verbindungsvereinbarungen repliziert der ADC die Objekte.

- Vorbereiten des Active Directory

  Alle Domänen, in denen später Exchange-aktivierte Benutzer, Verteiler oder Öffentliche Ordner abgelegt werden, müssen mit dem Aufruf

  „Setup /DomainPrep“

  vorbereitet werden. Diese Änderungen benötigen einige Zeit, bis alle Replikate aktualisiert sind.

- Installation Exchange 2003 und Kontrolle der Replikation

  Nach der Installation des ersten Exchange 2003-Servers, müssen Sie sicherstellen, dass alle Exchange 5.5-Empfänger auch in das Active Directory repliziert sind. Der erste Exchange 2003-Server in einem Standort betreibt den Standortreplikationsdienst. Mit dem Exchange 5.5-Administrator können Sie sich mit dieser Datenbank verbinden und die Anzahl der Empfänger mit Exchange 5.5 vergleichen. Die Einträge hier müssen mit dem Globalen Adressbuch in Exchange 5.5 übereinstimmen.

  Synchronisation der Verzeichnisse sicherstellen

  Solange dies nicht gewährleistet ist, darf der Exchange 2003-Server keine aktive Rolle bei der Übermittlung von Nachrichten übernehmen, da es sonst zu nicht zustellbaren Nachrichten führen kann. Kontrollieren und korrigieren Sie die Konfiguration des Active Directory Connectors. Erst wenn beide Verzeichnisdienste synchron sind, können Sie die Migration fortsetzen.

- Migration der Inhalte und Connectoren

  Die Benutzer, Öffentlichen Ordner und Connectoren werden schrittweise auf die neuen Server verschoben.

- Entfernen des Exchange 5.5-Servers

  Nachdem der Server keine Funktion mehr innehat, kann er über das Exchange 5.5-Setup deinstalliert werden. Das Setup prüft dabei einige Abhängigkeiten und stellt sicher, dass alle Elemente verschoben wurden. Nur wenn Sie sicher sind, dass die vom Setup bemängelten Punkte nicht zutreffen oder eine Deinstallation an anderen Problemen scheitert, können Sie den Server von Hand deinstallieren. Dabei sind die Schritte im

TechNet-Artikel „284148 XADM: How to Remove the Last Exchange-Server 5.5 Computer from an Exchange 2000 Administrative Group“ zu beachten.

- Native Mode

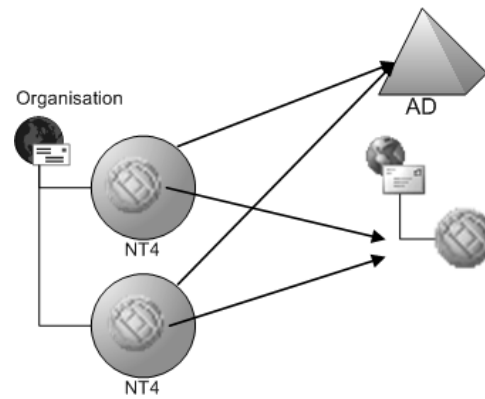
  Nachdem alle Exchange 5.5-Server und die Standortreplikationsdienste entfernt sind, steht der Umschaltung in den Exchange 2003 Native Mode nichts mehr im Wege.

Dies sind die wesentlichen Schritte, wenn Sie eine Exchange 5.5-Organisation mit nur einem Standort in eine Exchange 2003-Organisation überführen wollen.

12.3.3 Exchange 5.5-Multi Site nach Exchange 2003

Exchange 2003 bietet die Möglichkeit, in einer Administrativen Gruppe mehrere Routinggruppen zu betreiben. Dies ist die Ausgangssituation für diese Migrations-Methode. In der Exchange-Organisation sollen zwei Exchange 5.5-Standorte in zwei Windows NT 4-Domänen in eine Administrative Gruppe einer Active Directory-Domäne überführt werden.

Abbildung 12.20 Migration zweier Sites in eine Administrative Gruppe



Das besondere Problem bei dieser Migration ist, dass die Postfächer von einem der zwei Exchange 5.5-Standorte bislang nur über den Umweg einer PST-Datei zu einer Administrativen Gruppe migriert werden konnten. Ein Exchange 5.5-Standort wird bei der Migration innerhalb der gleichen Organisation als eine eigene Administrative Gruppe dargestellt. Erst später im Native Mode ist die Zusammenführung der Postfächer über einen Server möglich.

Besteht der Bedarf, aus mehreren Exchange 5.5-Standorten eine Administrative Gruppe zu formen, welche eventuell aus mehreren Routinggruppen besteht, dann gibt es bis zum SP1 drei Varianten der Migration. Mit Service Pack 1 ist es jetzt möglich, Postfächer auch im Mixed

Mode über Standorte hinweg zu verschieben. Diese Migrationsart wird unter Kapitel 12.4 „Konsolidierung von Standorten“ beschrieben.

Gleiche Organisation und Zusammenführung nach der Migration

Sie können die Exchange 5.5-Standorte klassisch nach Exchange 2003 migrieren, indem Sie die entsprechende Anzahl an Servern und Active Directory-Verbindungen einsetzen und nach der Migration aller Daten die Exchange 5.5-Server entfernen.

Erst Native Mode, dann AG-Konsolidierung

Erst dann kann die Exchange-Organisation in den Native Mode geschaltet werden. Im Native Mode können Sie die Anwender problemlos zwischen Servern in verschiedenen Administrativen Gruppen verschieben. Leider ist es nicht möglich, einen Server in eine andere Administrative Gruppe zu verschieben. Besteht Ihre Organisation aus räumlich verteilten Standorten und Sie möchten diese unter Exchange 2003 als eine Administrative Gruppe verwalten, dann können Sie folgende Migration durchführen:

1. Sie installieren einen neuen Server „SRV3“ in die Administrative Gruppe „AG1“ am Standort „Ort2“. Dieser Server gehört zur Routinggruppe des zweiten Standorts „RG2“.
2. Im zweiten Schritt verschieben Sie alle Anwender vom Server „SRV2“ in der AG2 auf den Server „SRV3“. Danach deinstallieren Sie Server „SRV2“. Die Administrative Gruppe AG2 können Sie nun ebenfalls löschen.
3. Wenn Sie den alten Server „SRV2“ wieder für die Daten verwenden wollen, können Sie diesen diesmal in die Administrative Gruppe „AG1“ neu installieren und alle Postfächer wieder zurückschieben.

Über diesen Weg können Sie im Native Mode mehrere Administrative Gruppen nach und nach auflösen. Während der gesamten Zeit können entsprechend eingerichtete Routinggruppen die Kommunikation optimieren.

Gleiche Organisation und Auflösen eines Standorts

Es kann aber sein, dass die Firma aus einem großen Hauptstandort und vielen kleinen Nebenstandorten besteht. Hier ist die zweimalige Migration auch aus Kostenaspekten ein Problem, da Sie erst die komplette Exchange 5.5-Migration abschließen müssen, um die Administrativen Gruppen zusammenzuführen.

Besser: Standort-konsolidierung

Während bisher nur die „manuelle“ Migration oder Drittprodukte mit entsprechenden Lizenzkosten in Frage kam, bietet Service Pack 1 die Konsolidierung von Standorten an. Können Sie aus bestimmten Gründen nicht das neue Tool einsetzen, ist bei der alternativen Migration der Niederlassungen wie folgt vorzugehen.

Move mittels Daten-Export und -Import

1. Die Benutzer und deren Daten des entfernten Standorts werden exportiert (z.B. mit EXMERGE) und die Einträge in Exchange gelöscht. Die Verbindungsvereinbarung des ADC sollte dabei so eingestellt sein, dass das Active Directory-Konto nicht gelöscht wird, sondern nur die Exchange-Eigenschaften entfernt werden. Damit bleiben die SIDs erhalten.
2. Die Connectoren zu den anderen Standorten werden gelöscht, und der Server wird deinstalliert. Damit werden auch die Postfächer aus der Exchange-Organisation entfernt.
3. Ein neuer Exchange 2003-Server wird vor Ort direkt in die richtige Administrative Gruppe installiert und in eine eigene Routinggruppe aufgenommen. Die Connectoren zur Verbindung mit der neuen Routinggruppe werden eingerichtet.
4. Die Anwender werden im Active Directory wieder für Exchange aktiviert. Kontrollieren Sie anhand der Empfängerrichtlinien die neu zugewiesenen E-Mail-Adressen.
5. Importieren Sie die Inhalte der Benutzer.

Dieser Vorgang ist relativ zügig durchführbar, bedeutet aber, dass die Benutzer aus der Organisation gelöscht und neu angelegt werden. Eine Folge davon ist, dass Nachrichten an diese Postfächer für den Zeitraum der Migration als unzustellbar gelten und Berechtigungen auf Öffentliche Ordner, Stellvertretereinstellungen, lokale MAPI-Profile und eventuell vorhandene Offline-Dateien ungültig werden. Auch standortübergreifende Verteiler müssen Sie eventuell erneut anpassen.

Diese Migration eignet sich daher nur für kleine Niederlassungen, bei der die Vorteile einer vom Native Mode unabhängigen Migration überwiegen. Sie sollten jedoch die neuen Möglichkeiten der Standortkonsolidierung seit SP1 prüfen, um die Nachteile dieser „manuellen“ Migration zu umgehen.

Neuaufbau

Vor- und Nachteile abwägen

Ähnlich der Auflösung eines Standortes über einen Export der Inhalte könnte auch die komplette Exchange-Organisation unabhängig von der bisherigen Exchange 5.5-Umgebung neu implementiert werden. Über entsprechende SMTP-Connectoren ist eine Verbindung zwischen beiden Organisationen möglich. Verbindungsvereinbarungen des Active Directory Connectors (Inter-Org) gleichen die Adressen der beiden Organisationen ab.

Auch hier müssen die Benutzer neu angelegt werden, so dass alle Nachteile der vorherigen Migration erhalten bleiben. Zudem können immer nur die Mitarbeiter eng miteinander arbeiten, die in der gleichen Organisation sind. Die Replikation von Öffentlichen Ordnern und Frei-/Belegt-Zeiten ist über das *Inter-Org Replikations-Tool* möglich. Trotzdem zählt diese Migration zu

den eher ambitionierten Ansätzen, aus einer Exchange 5.5-Organisation eine Exchange 2003-Umgebung zu formen, deren Einsatz wohl überlegt sein muss. Es ist allerdings einer der wenigen möglichen Wege, wenn der Name der Organisation geändert werden muss.

12.3.4 Erweiterung im Mixed Mode

Anhand der Erweiterung einer bestehenden Exchange 5.5/2003-Umgebung um eine weitere Administrative Gruppe lässt sich gut die Funktion des SRS und des ADC erläutern.

Sie sind mitten in der Migration Ihrer bestehenden Organisation von Exchange 5.5 nach Exchange 2003. Über den Active Directory Connector werden alle Empfänger synchronisiert, und der SRS in den bereits migrierten Administrativen Gruppen repliziert die Konfigurationsinformationen.

Nun kauft Ihr Geschäftsführer eine neue Firma hinzu, die Sie in die Exchange-Organisation als eigenständige Administrative Gruppe mit einem Exchange 2003-Server integrieren sollen. Die neue eigene Domäne für diese administrativ eigenständige Tochter können Sie noch sehr einfach in Ihren Active Directory-Forest integrieren. Die Domäne können Sie ebenfalls mit dem Exchange-Setup mittels Parameter „DomainPrep“ sehr schnell für den Einsatz von Exchange 2003 vorbereiten.

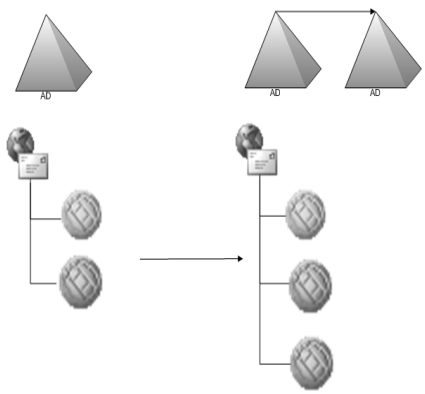


Abbildung 12.21 Erweiterung um eine Administrative Gruppe

Der Exchange 2003-Server wird wahrscheinlich vor Ort installiert, damit der schnelle Zugriff der Anwender gewährleistet ist. Damit stellt sich die Frage, ob der Server in die dortige Domäne installiert wird oder ob sich alle Exchange-Server in einer zentralen Domäne befinden. Im Beispiel gehen wir davon aus, dass die neue Tochter soweit eigenständig ist, dass sie auch ihren Exchange 2003-Server selbst verwaltet und dieser in der Domäne vor Ort installiert wird.

Durch die Installation des Exchange 2003-Servers vor Ort in einer eigenen Administrativen Gruppe wird auch eine eigene Routinggruppe angelegt. Dies ist notwendig, da der Native Mode von Exchange aufgrund der Existenz der Exchange 5.5-Server in anderen Standorten noch nicht genutzt werden kann. Zwischen der Routinggruppe der Tochter und der Routinggruppe der Zentrale muss ein Connector eingerichtet werden.

Interessant wird nun die Konfiguration im Hinblick auf die Benutzer. Da die Benutzer der Firmentochter in der Domäne vor Ort angelegt und für Exchange aktiviert werden, muss es eine geeignete Empfängerrichtlinie für diese Anwender geben. Zusätzlich müssen Sie auch prüfen, ob ein Empfängeraktualisierungsdienst existiert, der die Benutzer in der Tochter-Domäne mit E-Mail-Adressen versieht. Damit die Änderungen schnell aktiv werden, sollte der Empfängeraktualisierungsdienst auf dem Exchange-Server der Tochter laufen und auch einen Domänencontroller vor Ort ansprechen.

Bleibt noch die Frage, wie die bestehenden Exchange 5.5-Server Kenntnis von den Anwendern auf diesem Server bekommen. Die Information, dass es eine neue Administrative Gruppe und damit aus Sicht von Exchange 5.5 einen neuen Standort gibt, wird über das *ConfigCA* nach kurzer Zeit in die Exchange 5.5-Umgebung repliziert.

In allen bisherigen Migrations-Standorten wurde eine Verbindungsvereinbarung für Benutzer und Verteiler eingerichtet, die einen Abgleich zwischen der OU im Active Directory und einem Empfängercontainer auf Exchange 5.5-Seite hergestellt hat. In dieser neuen administrativen Gruppe gibt es weder einen Exchange 5.5-Server noch einen Standort-replikationsdienst (SRS).

Neue AG mit Exchange 5.5 verbinden

In diesem Fall übernimmt ein anderer SRS in der Organisation die Aufgabe, stellvertretend die Benutzer nach Exchange 5.5 zu replizieren. Sie müssen daher eine Verbindungsvereinbarung zwischen der Tochter-OU/Domäne mit einem SRS in Ihrer Exchange-Organisation (z.B. Zentrale) einrichten. Der ADC und der SRS erkennen diesen Sonderfall und tragen die Daten in die SRS-Datenbank (Zentrale) für die entfernte Site bzw. AG ein. Über diesen Umweg erhalten auch die Exchange 5.5-Server die Benutzerinformationen der neuen Administrativen Gruppe. Zur Erinnerung: Der SRS stellt seine Dienste auf dem Port 379/TCP bereit. Dies ist bei der Einrichtung der Verbindungsvereinbarungen einzutragen.

Prüfen Sie jedoch genau, ob Sie durch die Funktion des *Cached Mode* von Outlook 2003 in Verbindung mit Exchange 2003 auf einen eigenen Server in einer kleineren Niederlassung verzichten können, und einen Teil der gesparten Ausgaben in eine etwas leistungsstärkere WAN-Verbindung investieren..

12.3.5 Fremdsystem ohne Connector

Auch für die Migration von Fremdsystemen gibt es zwei mögliche Wege. In diesem Beispiel wird davon ausgegangen, dass es keinen Connector zur direkten Verbindung von Exchange 2003 mit dem bisherigen E-Mail-System gibt, der auch die Adressen abgleichen kann.

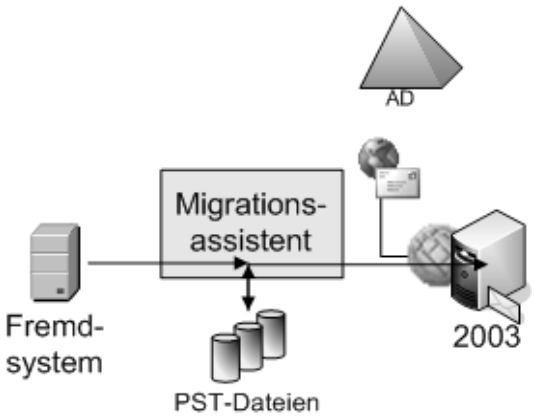


Abbildung 12.22 Migration von einem Fremdsystem ohne Connector

Sie können sich zwischen zwei Alternativen entscheiden:

Umstellen

„Quick & Dirty“

Sie installieren Exchange 2003, ohne das bisherige E-Mail-System zu berücksichtigen, und richten alle Benutzer mit den E-Mail-Adressen sein. Zu einem festgelegten Zeitpunkt stellen Sie Ihren Internet-Zugang um, damit eingehende Nachrichten nur noch nach Exchange 2003 zugestellt werden. Ab diesem Moment müssen Sie dafür sorgen, dass alle Anwender mit dem neuen System arbeiten können und niemand mehr das alte System verwendet.

Inwieweit die Daten aus dem alten System übernommen werden können, hängt von der Art und der Ablage der Informationen ab. Bei serverbasierten Lösungen wie Lotus Notes, Novell GroupWise oder IMAP4-Servern kann die Umstellung mit dem Exchange-Migrationsassistenten erfolgen. Andere Lösungen legen die Daten meist lokal ab. Hier könnten die leistungsfähigen Importfunktionen von Outlook oder der Umweg über Outlook Express einen Import auf dem Client erlauben.

Migrieren

Beschwerlicher Parallelbetrieb ohne Verzeichnisabgleich

Wenn eine „Ad-hoc“-Umstellung aufgrund der Größe des Unternehmens, der Datenmengen oder anderer Gründe nicht möglich ist, dann erfordert dies einen Parallelbetrieb der beiden Systeme für einen möglichst kurzen Zeitraum. Die Verbindung zwischen beiden Systemen wird mit dem Protokoll SMTP hergestellt. Sie installieren Exchange 2003 und richten die

Verbindung so ein, dass Exchange alle Nachrichten annimmt. Weiterhin konfigurieren Sie, dass Exchange alle Nachrichten an unbekannte Benutzer an das bisherige E-Mail-System weiterleitet und alle Nachrichten, auch für das Internet, von dem bisherigen E-Mail-System annimmt. Dann leiten Sie alle eingehenden Nachrichten an Exchange 2003 weiter und alle ausgehenden Nachrichten des alten Systems an Exchange um. Nun ist Exchange in den Nachrichtenfluss eingebunden.

Sie können nun schrittweise einen Benutzer in Exchange 2003 anlegen und seine Daten aus dem Postfach des alten Systems exportieren, dieses löschen und die Daten in Exchange importieren. Dank der Leitwege können die Anwender untereinander anhand der SMTP-Adresse weiterhin miteinander Nachrichten austauschen.

Damit die Anwender das System während der Migrationsphase einfacher nutzen können, sollten Sie diese Konstellation erweitern. Es ist sinnvoll, die die Anwender des Fremdsystems in Exchange 2003 (AD) als Kontakt oder externen Empfänger einzutragen, sowie umgekehrt. Solche Abgleiche können eventuell mit dem ADC oder mit eigenen Skripten erfolgen.

Der Wechsel von einem Fremdsystem ohne einen Connector ist eine anspruchsvolle Aufgabe, die umso komplizierter wird, je mehr Benutzer zu migrieren sind. Die erste Variante erfordert viele Änderungen in kurzer Zeit, eine Betriebsunterbrechung und viele Helfer, um alle Arbeitsplätze zeitnah umzustellen. Für eine längere Migration müssen Sie einen Abgleich der Adressen mit eigenen Mitteln entwickeln. Auch in diesem Fall sind Unstimmigkeiten nicht ganz zu verhindern. Daher sollte auch diese Phase möglichst kurz sein.

Das fremde E-Mail-System kann in diesem Beispiel natürlich auch eine andere Exchange-Organisation sein, bei der Sie den Namen der Organisation ändern müssen oder die Sie durch einen Zukauf in Ihre Organisation integrieren müssen.

12.3.6 Fremdsystem mit Connector

Für einige E-Mail-Systeme wie Lotus Notes oder Novell GroupWise liefert Microsoft mit Exchange 2003 Connectoren aus, die eine enge Anbindung der jeweiligen Systeme an Exchange 2003 erlauben. Der Connector ermöglicht eine direkte Übermittlung der Nachrichten zwischen den Systemen ohne Umweg über SMTP, den Abgleich der Adressbücher und den Abgleich von Frei-/Belegt-Zeiten. Durch diese drei wichtigen Funktionen kann eine fast reibungslose, aber langsame Migration des anderen E-Mail-Systems nach Exchange 2003 durchgeführt werden.

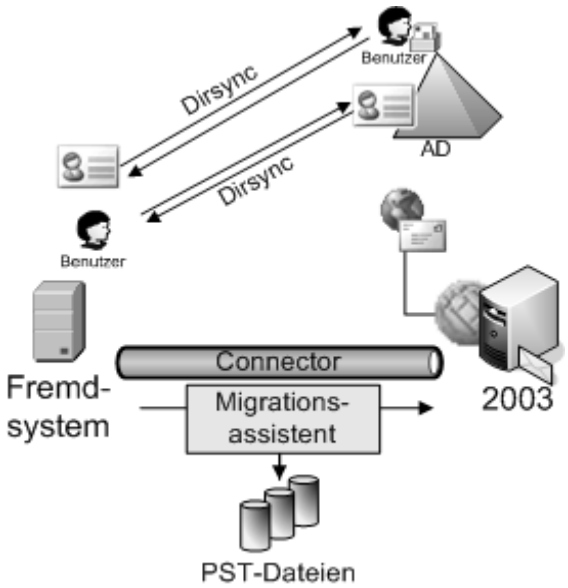


Abbildung 12.23 Migration mit Connector

Sie installieren eine neue Exchange 2003-Organisation entsprechend Ihrer Planung und binden an einer Stelle einen Exchange 2003-Server mit dem Connector zum Fremdsystem ein. Bei Migrationen sollten Sie prüfen, ob ein eigener Server für den Betrieb des Connectors sinnvoll ist, da sowohl der Connector zu Notes als auch zu GroupWise einen installierten Client des jeweiligen E-Mail-Systems für die Kommunikation benötigt. Dies Vorgehen erlaubt nach der Migration die restlose Entfernung des Servers ohne Überreste eines Notes- oder GroupWise-Clients auf Ihrem wichtigen Postfachserver.

Sowohl in GroupWise als auch in Notes sind umfangreiche Konfigurationen notwendig, damit der Exchange-Connector über den Client auf die verschiedenen Adressbücher, Ordner und Informationen zugreifen kann und dort als fremdes E-Mail-System sichtbar wird. Die Einrichtung bewirkt, dass jedes Exchange 2003-Postfach zusätzlich eine Notes- oder GroupWise-Adresse zugewiesen bekommt. In dem fremden E-Mail-System wird Ihre Exchange 2003-Organisation wie eine Foreign Domain (Notes) oder externes Postoffice (GroupWise) sichtbar. Der Verzeichnisabgleich des Connectors sorgt dafür, dass die Exchange 2003-Empfänger im jeweiligen System als E-Mail-Empfänger im Adressbuch hinzugefügt werden.

Die Empfänger des anderen E-Mail-Systems werden im Active Directory als Kontakte mit der jeweiligen Notes- oder GroupWise-E-Mail-Adresse eingetragen. So können auch alle Exchange 2003-Anwender problemlos diese Personen aus dem Adressbuch auswählen und über den Connector erreichen. Der Connector bedient den entsprechenden Adressraum, so dass Nachrichten an diese Empfänger nicht über das Internet gesendet werden.

Ebenso konvertiert der Connector die Formate der Nachrichten sehr viel besser, so dass sogar Termineinladungen und Formatierungen möglich sind.

Zusätzlich erlaubt der „Calendar Connector“ für Notes und GroupWise die Übertragung der Frei-/Belegt-Zeiten in das jeweils andere System. So installiert ist auch ein Parallelbetrieb beider Systeme über einen längeren Zeitraum möglich.

Für die Migration kommt wieder der Assistent für die Migration zum Einsatz, der z.B. auf einem Connector-Server gestartet wird, da hier sowohl der Client des fremden E-Mail-Systems als auch ein MAPI-Subsystem installiert ist. Sie können alternativ einen Arbeitsplatz mit dem fremden Client und den Exchange-Verwaltungswerkzeugen ausstatten.

Der Assistent zur Migration überträgt die Inhalte aus den Postfächern der ausgewählten Benutzer in ein neu angelegtes Exchange 2003-Postfach. Danach muss das Postfach im alten E-Mail-System entfernt werden, um über den Verzeichnisabgleich den dazugehörenden Kontakt im Active Directory zu löschen. Das neue Exchange 2003-Postfach wird zu einem externen Empfänger im fremden E-Mail-System, der auf das neue Exchange 2003-Postfach verweist. Allerdings müssen Sie das Postfach wieder in die entsprechenden Verteiler aufnehmen. Während der Migration ist es für Anwender im jeweils anderen System nicht möglich, Ihre Stellvertreter-funktionen auszuüben. Sie müssen daher prüfen, ob Abteilungen oder andere logische Gruppen als Block migriert werden sollten.

12.4 Konsolidierung von Standorten

Mit Exchange 5.5 bedeutete die Aufteilung in Standorten nicht nur eine Möglichkeit zur Verbindungssteuerung, sondern zugleich auch die Trennung der administrativen Zuständigkeit. Im Exchange 200x Native Mode hingegen können diese beiden Faktoren getrennt betrachtet werden. Innerhalb einer Administrativen Gruppe kann der Nachrichtenfluß mit mehreren Routinggruppen gesteuert werden. Mit dem Exchange SP1 wird die Konsolidierung mehrerer Standorte im Mixed Mode vereinfacht, da die Benutzer bei der Migration von einem Standort in eine andere Administrative Gruppe verschoben werden können. Bislang war dies nur über den Umweg mit EXMERGE möglich, wodurch unter anderem auch die Berechtigungen der Anwender und Mitgliedschaften in Verteilern verloren gingen. Die erforderliche Anpassung der Profile erfolgt durch das mit SP1 verfügbare Hilfsprogramm EXPROFRE. Öffentliche Ordner werden über den Replikationsweg zur anderen Administrativen Gruppe „verschoben“ und behalten dadurch die Berechtigungen.

Bevor Sie mit der Konsolidierung beginnen, sollten Sie eine zentrale Administrative Gruppe planen und ein Konzept zur Zusammenführung der Standorte festlegen. Lesen Sie dazu auch die Microsoft-Dokumente zur Planung und Bereitstellung von Exchange 2003.

Das Tool zur Standortkonsolidierung ist in den Bereitstellungstools „*ExDeploy SP1*“ enthalten. Nach dem Auspacken des Tools starten Sie dazu die Datei „Exdeploy.hta“. Die Konsolidierung besteht aus drei Phasen:

- Vorbereitung der Umgebung
- Durchführung der Konsolidierung
- Entfernen des Remotestandorts

Abbildung 12.24 Konsolidierung von Standorten im gemischten Modus

12.4.1 Vorbereitung der Umgebung

Exchange 2003 SP1 erforderlich

Voraussetzung für die Standortkonsolidierung ist das Service Pack 1 auf dem Exchange 2003-Zielserver. Zuvor müssen die ADC-Dienste sowie die Front-End-Server mit SP1 aktualisiert werden. Anschließend installieren Sie SP1 auf allen Postfachservern, zu denen die Postfächer verschoben werden, sowie auf dem Server für Öffentliche Ordner, sofern diese Dienste getrennt installiert sind. Diese Migration ist nur in einer gemischten Umgebung mit Exchange 5.5 und Exchange 200x in der gleichen Organisation erforderlich. In einer nativen Exchange-Organisation konnten Sie die Anwender schon immer zwischen Administrativen Gruppen verschieben.

Outlook 2003 im Cache Modus

Anwender, die Outlook 2003 mit dem Cachemodus einsetzen, behalten bei Einsatz von EXPROFRE ihre OST-Datei. Dadurch wird nach dem Verschieben auf den neuen Standort ein hoher Datentransfer vermieden, da nur noch die Änderungen seit der letzten Synchronisation benötigt werden. Beachten Sie, dass für den Einsatz von Outlook 2003 ein kritisches Update auf dem Exchange 5.5-Server erforderlich ist. Outlook 2003 bringt durch einige Aktionen den Exchange 5.5-Informationsspeicher zum Absturz

(Microsoft TechNet-Artikel 829418 „Information Store intermittently stops responding and an access violation occurs in EcDSDNFromSz“).

ADC prüfen

Prüfen Sie die ADC-Verbindungsvereinbarungen. Die Verbindungsvereinbarungen, die diese Benutzer verwalten, müssen bidirektional konfiguriert sein, damit die Änderungen auf beiden Seiten durchgeführt werden. Die Verbindungsvereinbarung für Öffentliche Ordner muss ebenfalls für beide Standorte (Ziel und Quelle) bestehen.

Hotfix 836489

Auf allen Exchange 5.5-Server der Organisation ist vorab Service Pack 4 sowie ein Hotfix für die DS/IS-Konsistenzanpassung zu installieren. Dieser Hotfix ist Voraussetzung für die Ausführung des Standortkonsolidierungstools. Sie können den Fix unter der Microsoft Knowledge-Base-Artikel-Nr. 836489 unter „www.microsoft.de/technet“ herunterladen.

Verschieben von Connectoren

Sofern sich auf dem Remotestandort noch weitere Connectoren oder andere Dienste befinden, sollten Sie diese ebenfalls auf andere Exchange-Server verschieben wie beispielsweise Internet Mail-Connectoren.

Replikation Public Folder

Die Öffentlichen Ordner des Remotestandorts müssen nun in den Zielstandort repliziert werden. Nutzen Sie dazu das Public-Folder Migration Tool *PFMigrate* und warten Sie die Replikation der Öffentlichen Ordner ab.

Einige Besonderheiten sollten Sie bei der Konsolidierung beachten:

Einschränkungen

- Verschieben Sie immer die Postfächer von Managern mit Stellvertretern zusammen, damit die Berechtigungen nicht verloren gehen.
- Bei Einsatz des Schlüsselverwaltungsdienstes müssen Sie die Zertifikate (X.509 v3) vorher exportieren und nach dem Verschieben auf den zentralen Servern wieder importieren.
- Während des Migrationszeitraums werden evtl. die Benutzer des Remotestandortes für kurze Zeit nicht in der Exchange 5.5-GAL (globalen Adressliste) angezeigt. Die Exchange 2003-GAL dagegen ist nicht betroffen.
- Einige Posteingangsregeln basierend auf die migrierten Postfächer funktionieren nicht mehr, können jedoch wiederhergestellt werden.
- Für das Verschieben zwischen Standorten im Mixed Mode müssen Sie einen Exchange 5.5-Server oder einen SRS-Server nutzen.

12.4.2 Durchführung der Konsolidierung

In der Phase 2 der Standortkonsolidierung werden alle Inhalte des Remotestandortes zum zentralen Standort verschoben. Vergewissern Sie sich vorab, dass die Öffentlichen Ordner bereits repliziert wurden.

Postfach über AG hinweg verschieben

Microsoft hat mit Service Pack 1 die Funktion „Verschieben der Postfächer“ erweitert. Unter den Exchange-Aufgaben in *Active Directory Benutzer und Computer* finden Sie die Option „Verschieben zwischen Administrativen Gruppen“. Im Zielstandort wird ein neues Postfach erstellt, und alle Inhalte werden vom Quellstandort dorthin kopiert. Im Quellstandort wird das Postfach versteckt. Gleichzeitig erhält das Postfach eine zweite X.500-Adresse sowie einen zusätzlichen Eintrag für ADC-Global-Names. Somit kann das System immer wieder den Ursprungsstandort herausfinden und E-Mails zustellen, die an die alte X.400-Adresse gesendet werden. Gruppenmitgliedschaften und Berechtigungen bleiben im Active Directory unverändert, da das Benutzerobjekt beibehalten wird. Prüfen Sie noch einmal Ihre ADC-Connectoren und warten Sie die Replikation zwischen Exchange 5.5 und Exchange 200x ab.

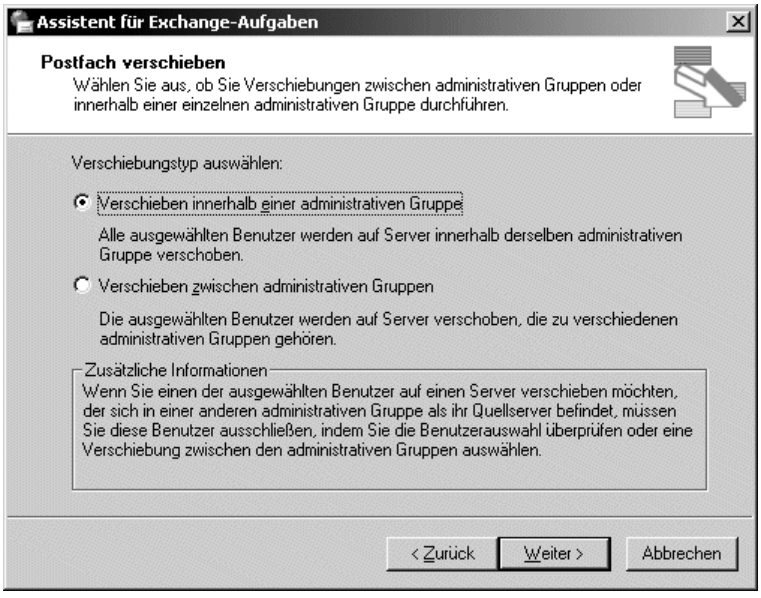


Abbildung 12.25 Postfächer zwischen Standorten verschieben

Verteiler und Kontakte „umziehen“

Zum Umziehen der Verteiler und Kontakte (Benutzerdefinierte Empfänger) muss der Stammserver der Objekte geändert werden. In der grafischen Oberfläche der Exchange-Bereitstellungstools können Sie die gewünschten Daten eingeben und das Tool ausführen.

Abbildung 12.26 „Object Rehome“

Im ersten Schritt werden die Objekte auf dem alten Standort gesucht und in eine Datei geschrieben (ToBeMoved.xml). Hier können Sie die Verteiler und Kontakte noch mal prüfen und gegebenenfalls bearbeiten. Anschließend starten Sie die Änderung des Stammservers über den Link in der grafischen Oberfläche. Exchange ändert dann den „Legacy Exchange DN“ und somit den Stammserver auf den neuen zentralen Server. Die Protokolldatei „ExDeploy.log“ des Bereitstellungstool zeigt Ihnen den Erfolg des Vorgangs an. Auch nach diesem Schritt sollten Sie die ADC-Verbindungsvereinbarungen prüfen und diese bei Bedarf anpassen.

Nachdem der Kopiervorgang der Postfächer sowie Verteiler und Kontakte abgeschlossen ist, aktualisieren Sie die Berechtigungsliste (ACLs) der Öffentlichen Ordner mit Hilfe der DS/IS-Konsistenzanpassung. Starten Sie die Konsistenzanpassung auf dem Quellserver direkt unter den Eigenschaften des Servers.

12.4.3 Entfernen des Remotestandorts

Public Folder-Replikate vom Quellserver löschen

Es befinden sich nun noch Öffentliche Ordner auf dem Quellserver. Prüfen Sie, ob alle Ordner korrekt zum zentralen Standort repliziert wurden. Die Systemordner wie Offline Adressbuch (OAB), Frei/Gebucht-Zeiten und EventConfig brauchen nicht repliziert werden, da sie in der zentralen Administrativen Gruppe neu erstellt werden. Sofern der Remoteserver das OAB generiert hat, sollten Sie für diese Aufgabe einen anderen Server definieren. Führen Sie das Skript PFMigrate aus, um die Replikate der Öffentlichen Ordner vom Remotestandort zu entfernen.

Entfernen von Connectoren

Nutzen Sie die bereitgestellten Tools, um den Erfolg der ganzen Aktion zu überprüfen. Sind keine Exchange-Objekte am Remotestandort zurückgeblieben, können Sie mit dem Abbau des Servers beginnen. Dazu entfernen Sie zuerst die ADC-Verbindungsvereinbarungen für Benutzer und Öffentlichen Ordnern. Löschen Sie die Replikationsconnectoren des Exchange 5.5-Verzeichnisses sowie die Standortconnectoren auf beiden Seiten jeder Verbindung. Damit diese Änderung im System richtig erkannt wird, sollten Sie das Routing innerhalb der Standorte neu berechnen, die mit dem Remoteserver verbunden waren. Zum Schluss können Sie den Exchange 5.5-Server deinstallieren.

12.5 Exchange-Profilaktualisierungstool

Exprofre.exe aktualisiert Outlook-Profile

Ein großer Nachteil jeder Migration zwischen Exchange-Organisationen oder Administrativen Gruppen im gemischten Modus war bislang immer die Umstellung der lokalen Outlook-Profile. Dies kostete nicht nur einen entsprechenden Zeitaufwand, sondern führte auch zu vielen Fehlern und Problemen während der Migrationsphase.

Das Exchange-Profilaktualisierungstool (Exprofre.exe) passt das Outlook-Standardprofil nun so an, dass sich die Benutzer nach dem Verschieben des Postfachs problemlos anmelden können. Dabei erstellt es keine neuen Profile, sondern ändert nur vorhandene Informationen. Das Tool kann z.B. über ein Anmeldeskripte oder eine Gruppenrichtlinie beim Anwender gestartet werden. Somit ist eine schnelle Umstellung der Outlook-Profile nach dem Verschieben gewährleistet.

Vor der Änderung des Standardprofils erstellt Exprofre eine Sicherungskopie, um bei erfolgloser Aktion die Umstellung wieder rückgängig zu machen. Das Tool erkennt ein verschobenes Postfach an der X.500-Adresse und aktualisiert das Standardprofil mit den neuen Benutzer- und Server-Eigenschaften. Das Offlineadressbuch wird gelöscht und muss vom Anwender neu herunter geladen werden. OST-Dateien von Outlook XP und älter können nicht weiter verwendet und müssen neu angelegt und die Inhalte repliziert werden. ExProfRE löscht die alte OST-Datei oder benennt sie um.

Kommandozeilenoptionen

Exprofre wird über Befehlszeilenoptionen gesteuert, die Sie mit dem Parameter „/?“ erhalten. Sie finden das *Exchange Profile Update* auf http://www.microsoft.com/exchange/downloads/2003/default.mspx.
Folgende Kommandozeilen können Sie für Exprofre anwenden:

- Verschieben zwischen Exchange-Organisationen

```
Exprofre.exe /targetgc=<Ziel-GC> /v /n /logfile=<Laufwerk:\Pfad>
```

  Beim Verschieben in eine neue Gesamtstruktur sind die meisten Outlook-Informationen veraltet und müssen an die neue Organisation angepasst werden. Alte Informationen werden dabei gelöscht. Sie benötigen dafür die Angaben eines Globalen Katalogserver der Zielorganisation, einer Protokolldatei, die Optionen „/v“ für Aktivierung der Ausgabe und „/n“ für das Löschen der Outlook-Nicknamendatei (.nk2 oder .nick).

- Verschieben zwischen Administrativen Gruppen

```
Exprofre.exe /targetgc=<Ziel-GC> /v /f /a
/logfile=<Laufwerk:\Pfad> /n
```

  In diesem Fall behalten ändern sich nur wenige Profildaten. Sie können das Offlineadressbuch „/a“, die Favoriten „/f“ sowie die Nicknamendateien behalten.

Teil V

Anhang und Index

13

Anhang

13 Anhang

13.1 Dokumentation

Bitte füllen Sie folgendes Formular vor oder während der Installation aus, damit Sie immer wieder schnell Zugriff auf die eingestellten Werte haben. Die hier gemachten Angaben beschreiben die Installation dieses Buches. Ihre Parameter für die produktive Installation werden hiervon abweichen.

Die dokumentierten Werte sollen Ihnen später im Falle einer Wiederherstellung, Erweiterung und Nachinstallation helfen und die Arbeit vereinfachen. Die Bedeutung der einzelnen Einstellungen finden Sie in den Kapiteln 7 bis 9.

Neben der Dokumentation ist auch eine Archivierung der Installationsmedien wünschenswert. Ideal ist die Anlage eines Archivordners pro Server, in dem neben den Handbüchern, Kopien von Rechnung und Lieferschein auch die Dokumentation und die Installationsmedien ihren Platz haben. So suchen Sie später nicht die passenden Datenträger bei einer Veränderung oder Wiederherstellung.

13.1.1 Netzwerkdaten

Für das Netzwerk sind folgende Parameter definiert.

Tabelle 13.1 Netzwerkparameter

	Parameter	Buch/Beispiel	Ihre Einstellungen
N1	Netzwerk IP-Adresse und Subnetzmaske	192.168.0.0/24	
N2	Standardgateway	192.168.0.1	
N3	IP-Bereich der Clients	192.168.0.100-254	
N4	DNS-Server für intern	192.168.0.10	
N5	DNS-Server für Internet-Auflösung	192.168.0.1	

Wenn Sie weitere Subnetze betreiben, sollten Sie die Dokumentation entsprechend erweitern.

13.1.2 Windows-Server-Daten

Folgende Daten beschreiben die Windows-Server-Installation:

Tabelle 13.2 Windows-Server-Einstellungen

	Parameter	Buch/Beispiel	Ihre Einstellungen
S1	Name des Servers	SRV01.msxfaq.local	
S2	Hardware-Beschreibung	Pentium 2 GHz LAN: Intel Pro100 DISK: Raid ServRaid 0:0 IBM 36 GB 0:1 IBM 36 GB	
S3	Festplatten-konfiguration	Pack A: 0:0+0:1 RAID1 C: 7,9 GB NTFS D: 28 GB NTFS Z: CD-Rom	
S4	IP-Adresse/Netzmaske Gateway DNS-Server	192.168.0.0/24 192.168.0.1 192.168.0.10	
S5	Windows-Installationsumfang	Windows 2003 Lizenznummer: + IIS6 + Net Framework + SNMP + NETMON + SMTP + NNTP	
S6	DHCP-Einstellungen: Bereichsname Bereich Ausschluss Default Gateway DNS-Server DNS-Name	 Client1 192.168.0.1- 255 192.168.0.1-099 192.168.0.1 192.168.0.10 msxfaq.local	
S7	DNS-Server Forwarder Zone 1 (Fwd Zone) Zone 2 (Rev Zone)	 192.168.0.1 msxfaq.local 0.168.192.in-addr.arpa	

13.1.3 Active Directory-Daten

Einstellungen des Active Directory:

	Parameter	Buch/Beispiel	Ihre Einstellungen
A1	Name des Forests	msxfaq.local	
A2	Name der Domäne NetBIOS-Name	msxfaq.local MSXFAQ	
A3	Name der Site	Bellheim	
A4	AD-Rollen und Funktionen: GC-Server Schema-Master Domainname-Master PDC-Emulator RID-Master Infrastrukturmaster	 Srv01.msxfaq.local Srv01.msxfaq.local Srv01.msxfaq.local Srv01.msxfaq.local Srv01.msxfaq.local Srv01.msxfaq.local	

Tabelle 13.3 Active Directory-Daten

13.1.4 Exchange 2003-Daten

Einstellungen für Exchange 2003:

	Parameter	Buch/Beispiel	Ihre Einstellungen
E1	Name der Exchange-Organisation	MSXFAQ	
E2	Name der ersten Administrativen Gruppe	Erste administrative Gruppe	
E3	Default SMTP-Domäne	msxfaq.de	
E4	Nachrichten-Tracking	7 Tage	
E5	Postfachrichtlinien/-limits (Warnung, Senden verbieten, Alles verbieten)	100000 KB 120000 KB 150000 KB	
E6	Öffentliche Ordner-Größe/-Verfallszeit	300000 KB keine	
E7	Pfade: Postfachspeicher Öffentliche Ordner Protokolldateien	 D:\EXCHSRVR\MDBDATA D:\EXCHSRVR\MDBDATA D:\EXCHSRVR\MDBDATA	

Tabelle 13.4 Netzwerk-parameter

13.1.5 Internet-Anbindung

Einstellungen der Internet-Anbindung:

Tabelle 13.5 Internet-Einstellungen

	Parameter	Beispiel	Ihre Einstellungen
I1	Name des Verbindungsproviders	T-Online DSL	
I2	Name des Zugangsproviders	GMX-DSL	
I3	MX-Record Username Kennwort	Dyndns.org fcarius **********	
I4	Firewall und Umsetzung	Router NAT	
I5	Smarthost Username Kennwort	Mail.1und1.de P123456 *********	
I6	POP3-Server Username Kennwort	Entfällt — —	

13.1.6 Exchange-Dienste

In der Systemsteuerung Ihres Computers finden Sie in Zusammenhang mit Exchange notwendige Dienste. Einige Dienste sind Bestandteil des Betriebssystems und werden von Exchange nur erweitert.

Tabelle 13.6 Exchange-Dienste

Abkürzung	Bedeutung Typ
MSADC	Microsoft Active Directory Connector Dieser Dienst sorgt für die Synchronisation der Verzeichnisse zwischen Exchange 5.5 und Exchange 2003. Er ist nur in gemischten Umgebungen erforderlich und entsprechende Verbindungsvereinbarungen müssen konfiguriert werden. Eine Inter-Org-Migration ist ebenfalls mit diesem Dienst möglich.
MSExchangeSA	Microsoft Exchange-Systemaufsicht Die Systemaufsicht ist der erste zu startende Dienst, von dem die meisten anderen Exchange-Dienste abhängig sind. Die Systemaufsicht überwacht die Funktion der einzelnen Dienste und meldet Ausfälle im Eventlog. Im Gegensatz zu Exchange 5.5 werden beim Beenden dieses Dienstes jedoch nicht alle anderen Exchange-Dienste beendet.

Abkürzung	Bedeutung Typ
IMAPSvc	Microsoft Exchange IMAP4 Dieser Dienst erlaubt den Anwendern den Zugriff über das Protokoll IMAP4. Wenn Sie diesen Zugriff nicht benötigen, sollten Sie diesen Dienst deaktivieren. Sie können die Funktion in der Management-Konsole jedoch auch pro Anwender deaktivieren.
MSExchangeMTA	Microsoft Exchange MTA-Stacks Dieser Dienst erlaubt den Versand und Empfang von Nachrichten über den X.400-Connector. Zusätzlich übernimmt der MTA die Verbindung zu Exchange 5.5-Servern und -Gateways, die mit dem Exchange 5.5-SDK entwickelt wurden.
MSExchangeES	Microsoft Exchange-Ereignis Dieser Dienst führt weiterhin Skripte aus, die seit Exchange 5.5 in einzelnen Ordnern hinterlegt werden können. Diese Skripte sind neben den Regeln eine weitere Möglichkeit, auf dem Server automatisch Nachrichten zu verarbeiten. Mit Exchange 2000/2003 sind zu diesen Skripten die leistungsfähigeren Event Sinks hinzugekommen. Der Dienst ist zur Kompatibilität weiter vorhanden, muss aber zur Funktion erst mit einem Benutzerkonto konfiguriert und gestartet werden.
MSExchangeIS	Microsoft Exchange-Informationsspeicher Dieser Dienst betreibt die Exchange-Datenbank und ist damit zentrale Komponente eines Exchange-Servers. Der Dienst kann in der Enterprise Edition bis zu vier Speichergruppen und 20 Datenbanken betreiben.
RESvc	Microsoft Exchange-Routingmodul Zusammen mit dem SMTP-Dienst übernimmt das Routingmodul die Verarbeitung und die Weiterleitung der Nachrichten in den entsprechenden Warteschlangen.
MSExchangeSRS	Microsoft Exchange-Standortreplikationsdienst Der SRS dient zur Replikation der Konfigurationsdaten in einer gemischten Umgebung. Zusammen mit dem ConfigCA des Active Directory Connectors werden die beiden Welten verbunden. In einer reinen Exchange 2000/2003-Umgebung ist der SRS nicht erforderlich und deaktiviert.
MSExchangeMGMT	Microsoft Exchange-Verwaltung Dieser Dienst wurde erstmalig mit Exchange 2000 SP2 installiert und verbindet Exchange mit WMI. Der Dienst ist z.B. erforderlich, um Nachrichten über den Nachrichtenstatus zu verfolgen. Durch diesen Dienst werden aufwändige Nachforschungen in den Protokolldateien gesteuert.

Abkürzung	Bedeutung Typ
SMTPSvc	Simple Mail Transfer Protocol (SMTP) Diese Windows-Komponente wird durch die Installation von Exchange erweitert und ist sowohl für den Versand von Nachrichten in das Internet, in der gleichen Routinggruppe und über Connectoren verantwortlich sowie auch für den Empfang von Nachrichten.
POP3Svc	Microsoft Exchange POP3 Dieser Dienst erlaubt den Anwendern einen Zugriff über POP3 auf das Postfach. Um den Zugriff global zu sperren, können Sie den Dienst deaktivieren. Alternativ können Sie auch bei jedem Anwender POP3 sperren oder in den Eigenschaften des Diensts den Zugriff auf bestimmte IP-Bereiche begrenzen. Dieser Dienst ist nicht dazu geeignet, Sammelpostfächer über POP3 abzuholen.
NNTPSvc	Network News Transfer Protocol (NNTP) Um über das Protokoll NNTP auf Öffentliche Ordner zuzugreifen, muss dieser Dienst gestartet sein.
W3SVC	WWW-Publishingdienst Dieser Dienst betreibt die verschiedenen Webseiten, die Sie für die Nutzung von Exchange als Anwender oder Administrator benötigen. Selbst wenn Sie den Zugriff mittels Outlook Web Access nicht benötigen, sollten Sie den Dienst nicht beenden, da sonst auch die Verwaltung der Öffentlichen Ordner nicht mehr möglich ist.
IISADMIN	IIS-Verwaltungsdienst Der Verwaltungsdienst ist die zentrale Instanz zur Überwachung und zum Betrieb der Internet-Dienste und muss gestartet sein.

Nicht aufgeführt sind hier die optionalen Dienste wie für eine GroupWise- oder Note-Anbindung sowie für Fax, SMS oder andere Services.

Den Namen der Abkürzung können Sie auf der Kommandozeile (cmd) oder in Skripten zum Stoppen und Starten der Dienste nutzen. Beachten Sie hierbei aber die Abhängigkeiten der Dienste. Neben den in der Systemsteuerung eingetragenen Abhängigkeiten gibt es auch logische Abhängigkeiten.

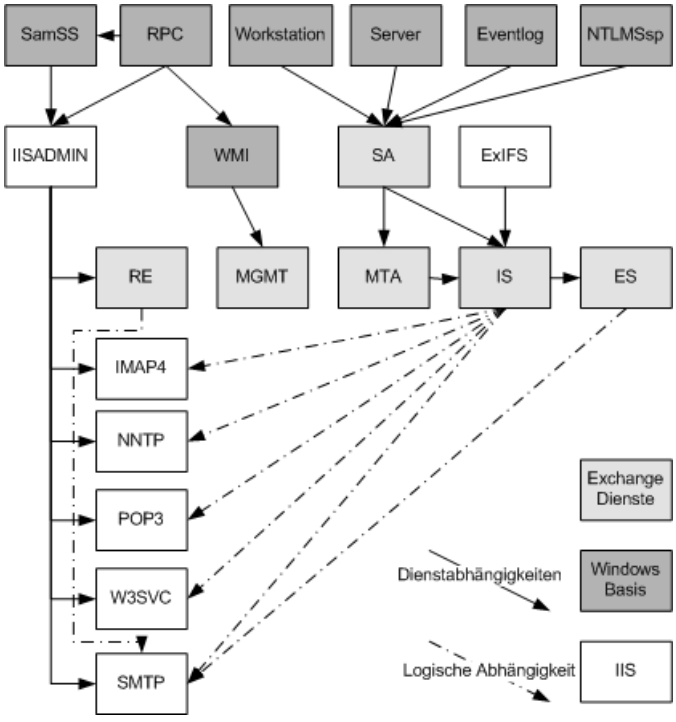


Abbildung 13.1 Abhängigkeiten der Dienste

Sie können z.B. den Informationsspeicher herunterfahren, ohne dass sich der POP3-Dienst beendet. Der POP3-Dienst wird die Verbindungsversuche der Anwender noch annehmen, aber keine Daten aus Exchange liefern.

13.1.7 Virtuelle Verzeichnisse im IIS

Im IIS werden durch Exchange folgende virtuelle Verzeichnisse angelegt:

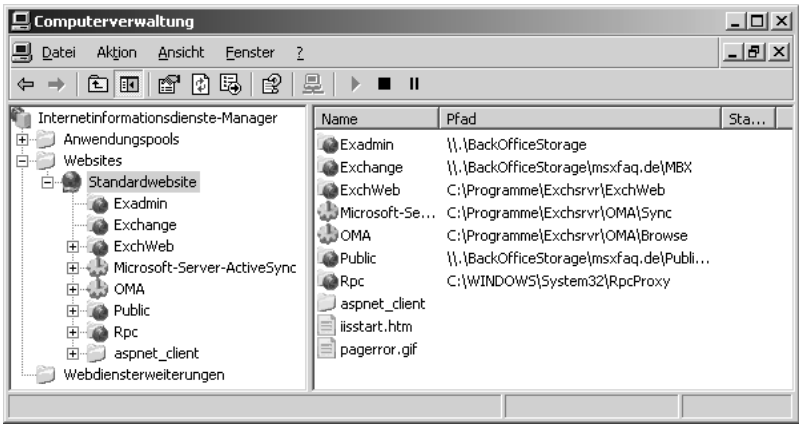


Abbildung 13.2 Virtuelle Verzeichnisse

Die Bedeutung der einzelnen Verzeichnisse:

Tabelle 13.7 IIS-Verzeichnisse

Abkürzung	Bedeutung
Exchange	Über dieses virtuelle Verzeichnis greifen die Benutzer über OWA auf ihr Postfach zu.
Public	Dieses Verzeichnis dient für den Zugriff auf Öffentliche Ordner.
ExchWeb	In diesem Verzeichnis liegen alle Hilfsmodule, ActiveX-Controls, Skripte und Bilder, die von den Clients benötigt werden. Durch die Trennung der Webinhalte ist auf diesem Verzeichnis nur ein lesender Zugriff notwendig.
Exadmin	Über dieses virtuelle Verzeichnis greift der Exchange System-Manager auf die Konfiguration der Öffentlichen Ordner zu. Wenn dieses Verzeichnis nicht erreichbar ist, weil Sie z.B. im IIS Beschränkungen auf IP-Adressen eingetragen haben oder SSL erzwingen, können Sie keine Öffentlichen Ordner mehr verwalten.
Microsoft-Server-ActiveSync	Dieses besondere Verzeichnis wird von Pocket Outlook nutzt, um die Postfachdaten eines Anwenders zu synchronisieren.
OMA	Der Zugriff über das Verzeichnis OMA erlaubt WAP-Devices einen Zugriff auf die Inhalte des Postfachs.
RPC	Um mit Outlook 2003 über HTTP eine Synchronisation zu ermöglichen, muss der Windows 2003-Dienst „RPC-über-HTTP-Proxy“ installiert sein. Das virtuelle Verzeichnis RPC im IIS wird hierfür eingerichtet.

Alle Verzeichnisse werden durch die Installation von Exchange automatisch korrekt angelegt. Über den Exchange System-Manager können Sie weitere virtuelle Server und virtuelle Verzeichnisse konfigurieren. Sie sollten nur die Einstellung direkt im IIS-Manager anpassen, die Sie nicht über den Exchange System-Manager einstellen können, z.B. die Einrichtung von Zertifikaten.

13.2 Kurzreferenz

13.2.1 Wichtige TCP/IP-Ports

Exchange 2003 und Windows 2003 nutzen folgende TCP/IP-Ports zur Kommunikation:

Port	Bezeichnung	Funktion
53/TCP 53/UDP	DNS	Um Nachrichten per SMTP zu versenden und die Domänencontroller zu finden, muss Exchange über DNS die Namen zu IP-Adressen auflösen können. Dieser Port wird aber auch vom Betriebssystem selbst genutzt.
123/UDP	NTP	Eine korrekte Uhrzeit ist auf allen Servern für die Funktion erforderlich. Dies ist nicht nur wichtig, damit alle E-Mails einen korrekten Zeitstempel tragen, sondern auch die Anmeldungen über das Protokoll Kerberos sind für die Funktion notwendig.
25/TCP 465/TCP	SMTP SMTP/SSL	Die Übertragung von Nachrichten mittels SMTP erfolgt über diesen Port. Dies betrifft sowohl den Versand in und den Empfang aus dem Internet als auch die Kommunikation der Server untereinander in der gleichen Routinggruppe oder über Connectoren. Auch Anwender, die ihr Postfach mittels POP3 oder IMAP4 lesen, liefern ihre Nachrichten per SMTP am Server ein.
110/TCP 995/TCP	POP3 POP3/SSL	Anwender, die mit dem Protokoll POP3 ihre E-Mails vom Exchange-Server abholen, müssen den Server über diesen Port erreichen können. Wenn Sie mit einem POP3-Sammelkonto arbeiten, muss das entsprechende Hilfsprogramm den E-Mail-Server des Providers über den Port 110 erreichen können.
143/TCP 993/TCP	IMAP4 IMAP4/SSL	Analog zu POP3 müssen Anwender über diesen Port den Server erreichen können, um Nachrichten zu lesen.
119/TCP 563/TCP	NNTP NNTP/SSL	Der Zugriff auf Öffentliche Ordner kann auch per NNTP erfolgen. Dazu muss der Anwender den Exchange-Server auf diesen Ports erreichen.

Port	Bezeichnung	Funktion
80/TCP 443/TCP	HTTP HTTPS	Diese beiden Ports haben bei Exchange 2003 eine zentrale Rolle. Über den IIS wird nicht nur Outlook Web Access erreicht, sondern auch die Zugriffe für ActiveSync, OMA sowie die Administration der Öffentlichen Ordner erfolgen über HTTP. Bei Exchange 2000 wird dieser Port auch noch für Instant Messaging und den Conference Server genutzt.
135	MS-RPC Portmapper	Über diesen Port verbinden sich alle Dienste über RPC, um den Port für den angeforderten Dienst zu erhalten. Dazu gehört Outlook ebenso wie das Nachrichten-Tracking, die Management-Konsole und andere Programme.
Dynamisch	ExchangeDS	Der Exchange-Verzeichnisdienst ist einer der Ports Beim Einsatz einer Firewall können Sie den Port in der Registrierung vorgeben.
Dynamisch	ExchangeIS	Auch der Informationsspeicher nutzt bei jedem Neustart immer wieder einen anderen Port, den die Clients zuerst über den RPC-Dienst in Erfahrung bringen müssen. Beim Einsatz mit einer Firewall können Sie den Port in der Registrierung vorgeben.
389/TCP 636/TCP 3268/TCP 3269/TCP	LDAP LDAP/SSL LDAP-GC LDAP-GC/SSL	Exchange liest seine Konfiguration und die Liste der Empfänger aus dem Active Directory. Dazu erfolgt der Zugriff auf die Domänencontroller über diese Ports. Exchange 5.5 nutzt den Port 389 ebenfalls. Wird Exchange 5.5 jedoch auf einem Windows 2000/2003-Domänencontroller betrieben, müssen Sie Exchange 5.5 auf einen alternativen Port (z.B. 390) umkonfigurierten.
379/TCP	SRS	Der Standortreplikationsdienst in einer gemischten Exchange-Umgebung ist über den Port 379 erreichbar. Dies ist für die Einrichtung von Verbindungsvereinbarungen über Firewalls hinweg besonders wichtig.
691/TCP	SMTP/LSA	Über diesen Port kommuniziert die Exchange Routing Engine innerhalb der Routinggruppe mit den anderen Servern.
102/TCP	X.400	Der Einsatz des X.400-Connectors nutzt diesen Port zum Verbindungsaufbau über TCP/IP.

Port	Bezeichnung	Funktion
1720 522 1503 1731	H.323 Video ULS T.120 Audio	Diese Ports werden von Clients und Diensten genutzt, die mit NetMeeting und Exchange 2000 arbeiten. Mit Exchange 2003 werden diese Dienste nicht mehr benötigt, da die Funktionen entfallen.

Zum Einsatz der einzelnen Ports gibt es auch in der TechNet und Exchange-Produktdokumentationen weiterführende Informationen:

- 148732 XADM: Setting TCP/IP Port Numbers for Internet Firewalls
- 278339 XGEN: TCP/UDP Ports used by Exchange 2000 Server
- XCON: Configuring MTA TCP/IP Port # for X.400 and RPC Listens

13.2.2 Abkürzungen

Tabelle 13.8 Abkürzungen

Abkürzung	Bedeutung
AD	Active Directory Microsoft-Verzeichnisdienst zur Speicherung von Benutzern, Gruppen, Computern und anderen Informationen.
ADC	Active Directory Connector Hilfsprogramm zur Kopplung des Exchange 5.5-Verzeichnisses mit dem Active Directory. Die erste Version wurde mit Windows 2000 ausgeliefert. Die Installation und Konfiguration des ADC ist in einer gemischten Umgebung von Exchange 5.5 und Exchange 2000/2003 zwingend erforderlich.
ADMT	Active Directory Migration Tool Dieses Programm erlaubt die Migration von Benutzern, Computern, Servern und Diensten aus einer Windows NT 4-Domäne in das Active Directory unter Beibehaltung der Kennwörter und der meisten Berechtigungen. Es ist damit unverzichtbar bei einer Konsolidierung mehrerer Domänen in eine Active Directory-Domäne.
ADS	Active Directory Service Alternativer Begriff für das Active Directory
ADSI	Active Directory Service Interface Von Microsoft definierte Programmierschnittstelle, um Informationen im Active Directory zu lesen und zu schreiben.

Abkürzung	Bedeutung
ADUC	Active Directory Users and Computers Kurzfassung für die Management-Konsole zur Verwaltung von Benutzern, Gruppen, Computern und anderen Objekten in der Active Directory Domäne.
AG	Administrative Gruppe Logische Zusammenfassung mehrerer Exchange-Server zu einer administrativen Einheit. Bei der Migration von Exchange 5.5 wird jeder Exchange Standort 1:1 zu einer Administrativen Gruppe.
API	Application Programming Interface Beschreibung und Schnittstelle zu einem System. Auf Grundlage einer API können Sie selbst Programme schreiben. Beispiele für APIs bei Exchange sind CDO, CDOEXM, MAPI, AVAPI
ASP	Active Server Pages Eine Funktion des IIS, um ausführbaren Code in Webseiten dynamisch auszuführen und die Ausgaben an den Client zu senden.
ASR	Automatic System Recovery Neue Funktion von Windows 2003, um mittels einer Diskette und einem Bandlaufwerk einen Server sehr schnell wieder herstellen zu können.
AVAPI	Antivirus API Von Microsoft für Exchange definierte Schnittstelle, um Virenscanner in der Exchange-Datenbank einzubinden.
BCC	Blind Carbon Copy, Blindkopien Beim Versenden einer E-Mail können Sie nicht nur Empfänger und Kopieempfänger angeben. BCC-Empfänger erhalten ebenfalls eine Kopie der Nachricht.
BE	Back-End-Server Bezeichnung für Postfachserver, die im internen Netzwerk stehen. Der Zugriff auf diese Server erfolgt über Front-End-Server.
CA	Certificate Authority Bezeichnung für ein System, welches Zertifikate ausstellt.
CA	Connection Agreement (Verbindungsvereinbarung)
CDO	Collaboration Data Objects Schnittstelle für den Zugriff auf Nachrichten.
CDOEXM	CDO for Exchange Management Schnittstelle, um Exchange-Server zu administrieren, z.B. um über Skripte einzelne Datenbanken bereitzustellen oder herunterzufahren.
DC	Domain Controller
DDNS	Dynamic DNS

Abkürzung	Bedeutung
DHCP	Dynamic Host Configuration Protocol Protokoll zur dynamischen Vergabe von IP-Adressen und anderen Parametern in einem TCP/IP-Netzwerk.
DirSync	Directory Synchronisation Connector Verzeichnisreplikationsdienst in Exchange 5.5
DN	Distinguished Name
DNS	Domain Name Service
DSG	Distribution Security Group Active Directory Gruppe zur Bildung von Verteilern ohne SID
E2K3	Kurzform für Exchange Server 2003
EDB	Exchange Database Bezeichnung für die Dateien, die Exchange für die Ablage von Nachrichten und anderen Informationen nutzt.
ESE	Extensible Storage Engine Bezeichnung für die Datenbank von Exchange
ESM	Kurz für Exchange System-Manager
ESMTP	Extended SMTP Erweiterung des SMTP-Standards um zusätzliche Befehle.
FE	Front-End-Server Bezeichnung für Exchange-Server ohne lokale Postfächer, die den Zugriff der Anwender auf die Back-End-Server (BE) weiterleitet.
Firewall	System zur Kontrolle und Steuerung von Verbindungen zwischen Systemen und Netzwerken. Häufig eingesetzt, um Verbindungen zum Internet gegen Eindringlinge abzusichern und Missbrauch zu vermeiden.
FQDN	Full Qualify Domain Name Bezeichnung für den kompletten Namen eines Objektes. Zum Beispiel ist der FQDN in der Musterinstallation Srv01.msxfaq.local
FSMO	Flexible Single Master of Operations Roles Bezeichnung für Funktionen, die nur ein Domänencontroller im Forest oder in der Domäne halten kann. Diese Funktionen sind wichtig, um Konflikte durch eine Replikation zu vermeiden.
GAL	Global Address List Verzeichnis, in dem sich alle Exchange-Objekte wie Postfächer, Verteiler, Kontakte und Öffentliche Ordner-Adressen befinden. Sie wird über den Globalen Katalog aufgebaut.

Abkürzung	Bedeutung
GC	Global Catalog (Globaler Katalog) Besonders konfigurierte Domänencontroller, die eine Teilmenge aller Informationen des gesamten Forest vorhalten.
GPO	Group Policy (Gruppenrichtlinie)
HTTP	Hypertext Transfer Protocol
IIS	Internet Information Server
IMAP4	Internet Message Access Protocol Ähnlich zu POP3 ein Protokoll zum Lesen von Nachrichten auf einem Mailserver.
Inter-Org	Inter-Organizational Organisationsübergreifende Aktion in Exchange
IPsec	IP Security Standard zur Verschlüsselung von Netzwerkpaketen in einem LAN oder zur Verbindung von Netzwerken über das Internet (VPN)
IS	Kurzform für Information Store
ISA	Internet Security and Acceleration Server Microsoft-Server zur Absicherung von Systemen und Netzwerken gegen das Internet oder andere Netze. Siehe Firewall.
ISP	Internet Service Provider
LDAP	Lightweight Directory Access Protocol
MAPI	Messaging Application Programming Interface
MB	Kurzform für Mailbox
MIME	Multipurpose Internet Mail Extensions Codierungsstandard zur Umwandlung von Sonderzeichen in einen Zeichensatz, der von allen Mailsystemen problemlos übertragen werden kann. Siehe auch UUENCODE.
MMC	Microsoft Management Console
MOM	Microsoft Operation Manager Microsoft-Produkt zur Überwachung von Systemen
MS	Kurzform von Microsoft
MTA	Mail Transfer Agent
MTBF	Mean Time Before Failure Angabe zur Ausfallwahrscheinlichkeit eines Geräts
MVP	Most Valuable Professional Jährlich neu vergebene Auszeichnung für besonderes Engagement für ein Produkt in Newsgroups oder Webseiten.

Abkürzung	Bedeutung
MX	MaileXchange Besonderer Eintrag im DNS-Server, damit andere Systeme den für diese Domäne zuständigen Mailserver auflösen können.
NAT	Network Address Translation Methode zur Übersetzung von IP-Adressen. Sehr häufig in Gebrauch, wenn viele Systeme in einem privaten Netzwerk über eine gemeinsame offizielle IP-Adresse auf das Internet zugreifen.
NDR	Non-delivery Report Statusmeldungen von Mailservern über die Unzustellbarkeit einer Nachricht.
NLBS	Network Loadbalancing Services Funktion von Windows, um mehrere Server mit der gleichen IP-Adresse zu betreiben und damit eine höhere Verfügbarkeit bestimmter Dienste zu erreichen
NNTP	Network News Transport Protocol Protokoll zur Übertragung von News
NSPI	Name Service Provider Interface Schnittstelle des GC für den Zugriff von Clients auf den Globalen Katalog. (ähnlich dem Exchange 5.5-Verzeichnisdienst).
NTP	Network Time Protocol Standard zur Abfrage und dem Abgleich von Uhrzeiten im Netzwerk. Windows 2000 nutzt ebenfalls NTP, um alle Systeme synchron zu halten.
OAB	Offline Address Book Lokale Kopie des Serveradressbuchs für die Arbeit unterwegs.
ORG	Organization
OST	Offline Folder Store Lokale Datei, in der Outlook eine synchronisierte Kopie eines Exchange-Postfachs vorhält. Diese erlaubt den Zugriff auf Informationen, wenn der Exchange-Server nicht erreichbar oder nicht verfügbar ist.
OU	Organizational Unit Organisationseinheit im Active Directory
PAB	Personal Address Book Erlaubt die lokale Speicherung von Adressdaten in einer Datei. Durch die Nutzung von Outlook-Kontakten sind PAB-Dateien kaum noch erforderlich.
PDC	Primary Domain Controller
PF	Kurz für Public Folder

Abkürzung	Bedeutung
PGP	Pretty Good Privacy Programm zur Verschlüsselung von Nachrichten. Siehe auch S/Mime.
POP3	Post Office Protocol Internet-Standard zum Abrufen von Nachrichten von einem Mailserver.
PST	Personal Folder File Erlaubt die lokale Ablage von Nachrichten außerhalb des Exchange-Servers.
QoS	Quality of Service Standard, um Übertragungsbandbreite in Netzwerken zu steuern und zu privilegieren.
QS	Qualitätssicherung
RAID	Redundant Array of Independent Disks Verbund mehrerer Festplatten, um den Ausfall von einzelnen Festplatten abzusichern.
REPLMON	Programm zu Kontrolle der Active Directory-Replikation
RID	Relative Identifier Jeder Benutzer erhält eine SID, die aus einem statischen Teil der Domäne und einem relativen Teil (RID) besteht.
RID-Master	FSMO-Rolle zur zentralen Vergabe der RID in einer Domäne, damit keine RID doppelt verwendet werden.
RIS	Remote Installation Service Windows 2000/2003-Dienst zur schnellen Installation von Computern über das Netzwerk.
RPC	Remote Procedure Call
RTF	Rich Text Format
RUS	Recipient Update Service Prozess zur Aktualisierung von Empfängern anhand der Empfängerrichtlinien.
S/Mime	Erweiterung des MIME-Standards um die Möglichkeit der Verschlüsselung und Signierung von Nachrichten.
SA	Exchange-Systemaufsicht (msExchangeSA)
SAM	Datenbank für lokale Benutzer
SAN	Storage Area Network Bezeichnung für die Trennung der Massenspeicher von den Servern in eigene Speichernetzwerke. Dies erlaubt in der Regel schnellere Sicherungen, eine höhere Verfügbarkeit und größere Flexibilität.

Abkürzung	Bedeutung
SDK	Software Development Kit Programme, Dokumentationen und Anleitungen zur Entwicklung von Software für ein System.
SG	Storage Group
SID	Security Identifier Eindeutige Kennung für jedes Sicherheitsobjekt. Jeder Benutzer und jede Sicherheitsgruppe besitzen eine SID, welche an verschiedenen Stellen zur Vergabe von Berechtigungen genutzt wird.
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol (Internet Mail)
SNMP	Simple Network Management Protocol Standard zum Management von Netzwerkkomponenten und Servern.
SRS	Site Replication Service Bildet auf einem Exchange 2003-Server eine Teilfunktion eines Exchange 5.5-Verzeichnisdienst zur Replikation nach.
SSL	Secure Socket Layer
STM	Streaming Media Ein Teil der Exchange-Datenbank zur Ablage von Nachrichten. Die STM-Dateien können immer nur zusammen mit den EDB-Dateien genutzt werden.
SUS	Software Update Service Software zum automatischen Download und zur Verteilung von kritischen Aktualisierungen von Microsoft im eigenen Netzwerk.
TLF	Top Level Folder Ordner der ersten Ebene im öffentlichen Informationsspeicher. Sehr häufig werden diese Ordner von Administratoren angelegt und Berechtigungen hierauf vergeben, damit Unterordner von den Anwendern selbst verwaltet werden können
TLH	Top Level Hierarchy
TLS	Transport Layer Security Bezeichnung für die Verschlüsselung von Nachrichten auf dem Transportprotokoll. So kann z.B. SMTP und POP3 auch den Datenverkehr mittels SSL verschlüsseln. Andere Verschlüsselungen sind z.B. VPN auf dem IP-Protokoll oder die Verschlüsselung der E-Mail mittels S/MIME.
UCE	Unsolicited Commercial E-Mail Anderer Begriff für SPAM oder unerwünschte oder unaufgefordert zugesandte Werbenachrichten.

Abkürzung	Bedeutung
UDG	Universal Distribution Group Verteiler im Active Directory, welcher auf alle globalen Katalogen repliziert wird, aber keine SID enthält. Diese Gruppe kann nicht zur Vergabe von Berechtigungen genutzt werden.
USG	Universal Security Group Besondere Gruppe im Active Directory, welche nur im Native Mode existiert und im gesamten Forest im globalen Katalog repliziert ist.
USN	Update Sequence Numbers Laufende Nummer, um Änderungen im Active Directory zu erkennen und zu replizieren.
USV	Unterbrechungsfreie Stromversorgung
UUCP	Unix to Unix Copy Früher häufig genutztes Verfahren, um Nachrichten zwischen zwei Mailsystemen auszutauschen, und mittlerweile fast vollständig durch SMTP verdrängt.
UUDECODE UUENCODE	Unix to Unix Encode Verfahren zur Umcodierung von Nachrichten von 8 Bit nach 7 Bit. Viele Mailsysteme können nur 7-Bit-ASCII-Zeichensätze verarbeiten. Siehe auch MIME.
VPN	Virtual Private Network Gesicherte verschlüsselte Verbindung zwischen zwei Netzwerken oder Computern über ein öffentliches Netzwerk.
VSAPI	VirusScan API Exchange-Schnittstelle für Virenscanner
W2K3	Kurz für Windows Server 2003
WAP	Wireless Application Protocol Standard für den Zugriff von Mobiltelefonen und anderen Geräten auf besonders für geringe Bandbreiten aufbereitete Daten.
WebDAV	Web-based Distributed Authoring and Versioning Definition für das Bearbeiten von Dokumenten auf Servern über http. Wird zum Beispiel. von Exchange, FrontPage und SharePoint genutzt..
WINS	Windows Internet naming service Wandelt Computernamen in IP-Adressen um.
WMI	Windows Management Instrumentation Allgemein zugängliche Schnittstelle von Windows zum Auslesen und Konfigurieren von Parametern eines Windows-Systems.
WSS	Web Storage System

13.2.3 Begrifflichkeiten Deutsch – Englisch

In der folgenden Übersicht finden Sie die häufig benutzten Begriffe für Microsoft Exchange und Active Directory. Die Liste soll Ihnen helfen, die Begriffe auch im Englischen zuzuordnen, um im Internet und in der TechNet immer die aktuellsten Informationen und Hilfestellungen bei Problemen zu erhalten. Die Übersetzung ins Deutsche erfolgt meist wesentlich später, und einige Publikationen und TechNet-Artikel erhalten Sie nur in englischer Sprache.

Tabelle 13.9 Begriffe Deutsch-Englisch

Deutsch	Englisch
Windows-Verzeichnisdienst	Active Directory
Empfängerrichtlinie	Recipient Policy
Empfängeraktualisierungsdienst	Recipient Update Service
Informationsspeicher	Information Store
Speichergruppe	Storage Group
Postfachspeicher	Mailbox Store
Informationsspeicher für Öffentliche Ordner	Public Folder Store
Speichergruppe für die Wiederherstellung	Recovery Storage Group
Standortreplikationsdienst	Site Replication Service
Verbindungsvereinbarung	Connection Agreement
Nachrichtenverfolgung	Message Tracking
Standort	Site
Verweis auf Öffentlicher Ordner	Public Folder Referral
Globale Adressliste	Global Address List
Gemischter Exchange-Standort/ Administrative Gruppe	Mixed (Vintage) Site
Organisationsübergreifend	Inter-Organizational
Verteiler	Distribution Group

Index

C

D

E

F

M

N

O

P

Q

R

S

T

U

V

W

X

Z