Zwischen

der Senatsverwaltung für Inneres und Sport

und

dem Hauptpersonalrat für die Behörden, Gerichte und
nichtrechtsfähigen Anstalten des Landes Berlin

wird

auf Grundlage von

§ 74 Abs. 1 und Abs. 2 Satz 4, § 85 Abs. 1 Nr. 12, Abs. 2 Nr. 9, 10 des Personalvertretungsgesetzes (PersVG) in der Fassung vom 14. Juli 1994 (GVBl. S. 337, 1995 S. 24), zuletzt geändert durch Artikel I des Gesetzes vom 17. Juli 2008 (GVBl. S. 206) sowie § 13 Abs. 2 des Tarifvertrages über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen mit Geräten der Informationstechnik vom 23. März 1989 (TV Infotech) in der Fassung des ÄTV vom 18. Oktober 1996

folgende

Rahmendienstvereinbarung zur landesweiten Einführung und zum Betrieb des MS Exchange-Verbundes

geschlossen:

Diese Rahmendienstvereinbarung gilt für alle Dienststellen des Landes Berlin, bei denen Beschäftigte, die zum Hauptpersonalrat wählen, tätig sind.

1. Grundsätze

Die Vereinbarung regelt Einsatz und Betrieb des Microsoft Exchange-Verbundes für verwaltungsübergreifende Zusammenarbeit mit folgenden Funktionen:

- Nachrichtentransportverfahren,
- Speicherort für Nachrichten bis zum Abruf durch den Client,
- Bereitstellung mobiler Kommunikation,
- Bereitstellung Outlook Web Access (OWA), Wireless Mobile Service Application (WAP) und ActiveSync mit DirectPush,

- Bereitstellung Unified Message Service (UMS-Dienste),
- Bereitstellung Virenschutz und Spam-Filtermechanismen,
- Bereitstellung öffentlicher Ordnerstrukturen,
- Bereitstellung Terminkalender und Aufgaben-Listen,
- Bereitstellung des globalen Adressbuches.

Einführung und Betrieb erfolgen gemäß den Beschreibungen und Erklärungen der Beteiligungsvorlage des Informationstechnik-Dienstleitungszentrums Berlin (ITDZ) vom 28. März 2007 mit Ergänzung vom 10.10.2007, die dem Hauptpersonalrat im Auftrag der Senatsverwaltung für Inneres und Sport zur Beteiligung vorgelegt wurde (Beteiligungsvorlage, Anlage)*.

2. Öffentliche Ordner, Kalender, Aufgaben-Listen, Outlook Web Access, Besondere Interessengruppen, Personaldaten

Einrichtung, Verwendung und Verarbeitung der Daten öffentlicher Ordner, wie zum Beispiel Kalender und Aufgaben-Listen, werden in den Dienststellen mit den jeweils zuständigen (örtlichen) Personalräten in Form ergänzender Dienstvereinbarungen geregelt.
Besonderen (Interessen-)Gruppen - wie zum Beispiel Personalvertretungen – ist zu ermöglichen, eigenständige, nicht übergreifend zu nutzende, organisatorische Einheiten in der MS-Exchange-Struktur zu bilden.

Materiell den Personalakten zuzurechnende Personaldaten dürfen nicht in öffentlichen Ordnern gespeichert werden.

Nutzung und Betrieb des Zugriffs-Dienstes aus dem Internet – Outlook Web Access (OWA) – werden mit den jeweils zuständigen (örtlichen) Personalräten geregelt.

3. Adresslisten, Globale Adressliste

Globale und andere Adresslisten sind durch Dienst-/Arbeitsanweisungen, organisatorische Regelungen und technische Maßnahmen gegen Missbrauch zu schützen. Dabei ist zu beachten:

- Die in der globalen Adressliste verwendeten Datenfelder und ihre Verwendung sind in der Anlage B2.1 der Beteiligungsvorlage beschrieben.
  Die Anlage ist Teil der Rahmendienstvereinbarung.

- Die Globale Adressliste darf ausschließlich zur dienstlichen Aufgabenerfüllung verwendet werden.

Die jeweils zuständigen Personalvertretungen werden über festgestellte Missbräuche und datenschutzrechtliche Verstöße informiert.

* Betrieb und Einsatz mobiler Geräte sind in einer besonderen Rahmendienstvereinbarung geregelt.

4. Inkrafttreten, Kündigung

Die Rahmendienstvereinbarung tritt mit Unterzeichnung in Kraft.

Die Rahmendienstvereinbarung kann mit einer Frist von 3 Monaten gekündigt werden, gilt in diesem Fall jedoch fort, bis eine neue Rahmendienstvereinbarung zur landesweiten Einführung und zum Betrieb des Microsoft Exchange-Verbundes im Land Berlin mit dem HPR rechtsgültig geschlossen worden ist.

Soweit die unterzeichnenden Beteiligten sich nach wirksam gewordener Kündigung nicht auf eine neue Rahmendienstvereinbarung einigen können, kann jeder der beiden Beteiligten das Einigungsverfahren gemäß §§ 80, 81 PersVG betreiben. §§ 83, 81 Abs. 2 PersVG bleiben unberührt.

Berlin, den 06. Mai 2009

Im Auftrag

_____	_____
Senatsverwaltung für Inneres und Sport	Hauptpersonalrat

IT-Dienstleistungszentrum Berlin
Anstalt des öffentlichen Rechts

IT-Dienstleistungszentrum Berlin
Berliner Straße 112–115, 10713 Berlin

An den
Hauptpersonalrat für die Behörden,
Gerichte und nichtrechtsfähigen Anstalten
des Landes Berlin

Über

SenInnSport – ZS C 1 -

Bearbeiter: Frau Gieseler
Gesch. Z.: PF 1 Gi
(bei Antwort bitte angeben)

Zimmer: 610
Telefon: 90 12- 4338
intern (912)
FAX: 90 12- 3112
FAX (persönlich): 3599
Datum: 28.März 2007

Beteiligungsvorlage beim Hauptpersonalrat gem. § 59 PersVG Berlin und § 85 PersVG Berlin

hier: Microsoft Exchange-Organisation als Nachrichtenverarbeitungssystem und definierte Umgebung für verwaltungsübergreifende Zusammenarbeit

Sehr geehrte Damen und Herren,

als Verfahrensverantwortlicher im Sinne IT-Organisationsgrundsätze und der VV IT-Steuerung in der jeweils gültigen Fassung beabsichtige ich

☒ im Rahmen des Verfahrens : **Microsoft Active Directory Verzeichnisdienst**

☒ folgende Software : ..... **Microsoft Exchange 2000 Server**

☐ folgendes Fachkonzept : ..... _____

in der Version : ..... _____

☒ folgende Hardware und Dienstleistungen: _____

in der Version : ..... **Microsoft Exchange 2000 Server, Microsoft Exchange Server 2003 sowie Folgeversionen, sofern dort keine beteiligungsrelevanten Tatbestände im Sinne der Regelungen des PersVG Berlin vorliegen.**

☐ Software wie in Anlage 1 aufgeführt,

einzusetzen bzw. umzusetzen. [1]

[1] Mehrfachankreuzungen innerhalb dieser Frage sind möglich. Sollte der Beteiligungsgegenstand die Umsetzung eines Fachkonzeptes oder eines Gerätes sein, ist die Beachtung der Fragen, die sich ausschließlich auf Software beziehen, unerheblich.

A) Allgemeine Beschreibung

1. Einsatzzweck

☒ folgender Einsatz ist vorgesehen:

Standard Nachrichtenverarbeitungssystem und Plattform für verwaltungsübergreifende Zusammenarbeit im Active Directory Verbund der Berliner Verwaltung, sowie Nachrichtenverarbeitungssystem im Intranet der Berliner Verwaltung und mit Einschränkungen auch im Internet

☒ Detaillierte Darstellung des Einsatzzwecks in Anlage A1.

2. Einsatzbreite

Der Einsatz der Software bzw. die Umsetzung Fachkonzepts ist geplant

☐ für folgende Einrichtungen:

_____

☒ landesweit

☐ Auflistung der Einrichtungen in Anlage A2.

3. Nutzerkreis/Anwender

Die Software bzw. das Fachkonzept wird auf Arbeitsplätzen der folgenden Gruppen eingesetzt bzw. umgesetzt:[1]

☒ Infrastrukturbetreuender (voraussichtliche Anzahl: Alle)

☐ Anwendungssystembetreuender (voraussichtliche Anzahl:)

☐ Anwender (voraussichtliche Anzahl:)

☐ folgende Dienstkräfte:

_____

☐ alle Dienstkräfte der nutzenden Dienstelle (siehe Anlage A 2)

☐ Auflistung der Nutzer in Anlage A3.

[1] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.

4. Nutzungsumfang

Die Nutzung der Software bzw. des Fachkonzepts erfolgt durch die genannten Dienstkräfte[2]

- ☐ nach eigenem Ermessen des Nutzenden
- ☐ im Rahmen des auf Seite 1 genannten Verfahrens
- ☐ ist verfahrensunabhängig
- ☐ im Rahmen gesetzlicher Regelungen oder Arbeitsanweisungen
  - ☐ Auflistung :

    _____
  - ☐ Arbeitsanweisung in Anlage A4.1
- ☒ ist Bestandteil/Grundlage folgender Verfahren/Anwendungen
  - ☒ Auflistung :

    Active Directory Verzeichnisdienst der Berliner Verwaltung
  - ☐ Auflistung in Anlage A4.2

5. Art der Software

Die Software ist folgender Produktgruppe zuzuordnen:[3]

- ☐ Betriebssoftware
  - ☐ Betriebssysteme
  - ☐ Datenbanksysteme
  - ☐ Sicherheitssoftware
  - ☐ andere Kategorie (z.B.Middleware) :

    _____
- ☒ Anwendungssoftware
  - ☒ Standardprodukte
  - ☐ Querschnittsanwendungen (z. B. Dokumentenverwaltung)
  - ☐ spezielle Anwendungen (z.B. amts-/betriebsspezifische Fachanwendungen)

- ☒ Dienste

[2] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.
[3] Mehrfachankreuzungen innerhalb dieser Frage sind möglich. Sofern der Beteiligungsgegenstand die Umsetzung eines Fachkonzeptes oder der Einsatz eines Gerätes ist, ist die Beantwortung dieser Frage unerheblich.

☒ Elektronische Post (Mailing)
☐ Sicherheitsdienste
☐ Intranet-/Internet-Dienste
☐ Abrechnungsdienste (Billing)
☐ Datendienste, Sprachdienste
☐ andere Dienste _____

6. Hardware-Konfiguration

☒ folgende Hardware- / Softwarekonfiguration ist Voraussetzung für den Einsatz der Software :

Intel- und Intel-Processor kompatible Server-Hardwareplattform

☒ Auflistung der Hardware - Konfiguration in Anlage A6.

7. Beschreibung des Funktionsumfanges

☒ Der Einsatz der Software erstreckt sich auf folgenden Funktionsumfang:

Im Bereich Nachrichtenverarbeitung

- **Nachrichtentransportverfahren**
- **Speicherort für Nachrichten bis zum Abruf durch den Client**
- **Bereitstellung mobiler Kommunikation**
    - **Outlook Mobile Access (OMA),**
    - **Wireless Mobile Service Application (WAP),**
    - **ActiveSync mit DrecPush Technologie**
- **Bereitstellung Outlook Web Access (OWA) Kommunikation**
- **Bereitstellung Virenschutz und Spam-Filtermechanismen**
- **Bereitstellungvon Unified Message Service (UMS-Dienste)**

Im Bereich übergreifende Zusammenarbeit:

- **Bereitstellung von öffentlichen Ordnerstrukturen**
- **Bereitstellung von Terminkalender und To-Do-Listen**

Sowie bereichsübergreifend:

- **Bereitstellung des globalen Adressbuches**

☒ Beschreibung des Funktionsumfanges in Anlage A7.1
☒ Dokumentation des Herstellers in Anlage A7.2

8. Präsentation[4]

☒ CD in Anlage A8 (Produktbeschreibung)

☐ Lizenzbereitstellung per eMail :

_____

☐ Herunterladen (Download) aus dem Internet :

_____

☒ beim Verfahrensverantwortlichen des ITDZ

Name :.....**Peter Schwanke**

Anschrift : .....**ITDZ Berlin – PB 2 2 Sc**

Telefon-/Faxnr. : .....**9 (0) 222 - 6274**

☒ am : **12.03.2007** um :**10.00 Uhr** in :**DG Berliner Str 112-115, R. 904**

☐ nach Vereinbarung : ____

☐ beim Anwendenden

Name :..... _____

Anschrift : ..... _____

Telefon-/Faxnr. : ..... _____

☐ am : _____ um : _____ in : _____

☐ nach Vereinbarung : ____

☐ beim Lieferanten

Name :..... _____

Anschrift : ..... _____

Telefon-/Faxnr. : ..... _____

☐ am : _____ um : _____ in : _____

☐ nach Vereinbarung : ____

☐ beim Hauptpersonalrat

Name :..... _____

Anschrift : ..... _____

[4] Mehrfachankreuzungen innerhalb dieser Frage sind möglich. Es wird dringend empfohlen, mindestens einen Präsentationstermin anzubieten.

Telefon-/Faxnr. : ..... _____

☐ am : _____ um : _____ in : _____

☐ nach Vereinbarung : ____

☐ bei der Personalvertretung

Name :..... _____

Anschrift : ..... _____

Telefon-/Faxnr. : ..... _____

☐ am : _____ um : _____ in : _____

☐ nach Vereinbarung : ____

B) Beschreibung der Risikopotenziale und Mitbestimmungstatbestände

1. Leistungs- und Verhaltenskontrolle nach § 85 Abs. 1 Nr. 13 PersVG

Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Dienstkräfte zu überwachen :[5]

☐ Leistungs- und Verhaltenskontrollen sind ausgeschlossen.

☐ Folgende Regelungen zur Leistungs- und Verhaltenskontrolle werden in Ergänzung zu § 9 TV Infotechnik vereinbart :

_____

☒ Beschreibung in Anlage B1.

Darüber hinaus ist jegliche Speicherung und Auswertung von Daten zur Leistungs- und Verhaltenskontrolle unzulässig.

2. Verarbeitung personenbezogener Daten nach § 85 Abs. 2 Nr. 8 PersVG

Einführung, Anwendung, wesentliche Änderung oder wesentliche Erweiterung von automatisierter Verarbeitung personenbezogener Daten der Dienstkräfte außerhalb von Besoldungs-, Gehalts-, Lohn- und Versorgungsleistungen :[6]

☐ Es werden keine personenbezogenen Daten der Dienstkräfte verarbeitet.

[5] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.
[6] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.

☒ Die Speicherung personenbezogener Daten der Dienstkräfte ist erforderlich. Die Verarbeitung erfolgt in allen Phasen auf der Grundlage der Regelung der Rahmenvereinbarung zur Verarbeitung personenbezogener Daten vom 8. August 1991. Die Regelungen werden eingehalten.

☐ Folgende personenbezogenen Daten der Dienstkräfte werden verarbeitet (Dauer/ Zugriff / Übermittlungen) :

_____

☒ Beschreibung der personenbezogenen Daten in Anlage B2.1

☐ Zur Information ist die

- ☐ Stellungnahme des behördlichen Datenschutzbeauftragten zusätzlich in Anlage B2.2a
- ☐ Stellungnahme Berliner DSB zusätzlich in Anlage B2.2b

3. Software-Ergonomie

nach § 85 Abs. 1 Nr. 12 PersVG - Gestaltung der Arbeitsplätze;

☒ ist unbedeutend, weil (z.B. Spooler, Batchprogramme etc.):

Vom Nutzer unabhängig

☐ entspricht den Gestaltungsgrundsätzen der beteiligten Software:

_____

☐ nach Beschreibung / Gutachten / Zertifizierung gem. ISO EN 9241 Teile 10 bis 17 in Anlage B3

☐ Ein Gutachten ist in Auftrag gegeben.

4. Arbeitsablauforganisation

nach § 85 Abs. 2 Nr. 8 bis 10 in Verbindung mit Nr. 2 PersVG - Maßnahmen zur Hebung der Arbeitsleistung und zur Erleichterung des Arbeitsablaufs :[7]

☒ Auswirkungen sind geringfügig, weil (z.B. lediglich technische Unterstützung am individuellen Arbeitsplatz erfolgt wie bei Packprogrammen oder bei Tools zur Dokumentendarstellung):

_____

☐ Beschreibung der Arbeitsablauforganisation in Anlage B4.1

[7] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.

☒ Berechtigungskonzept in Anlage B4.2

☐ Betriebs- / Betreiberkonzept in Anlage B4.3

5. Schulung nach § 85 Abs. 2 Nr. 9 PersVG – neue Arbeitsmethoden[8]

☒ Schulungskonzept in Anlage B5

☐ ergibt sich aus der Dokumentation in Anlage A6

☐ durch den Hersteller :

_____

☐ über die integrierten Hilfefunktionen

☐ über Lernprogramm

☐ Einweisung / Beratung durch

_____

6. Rationalisierung gem. § 87 Nr. 2, 5, 6 und § 88 Nr. 7 PersVG

Bei der Übertragung der Aufgabenwahrnehmung bezüglich des vorliegenden Beteiligungstatbestandes handelt es sich nicht lediglich um eine vorübergehende Übertragung höher oder niedriger bewerteter Tätigkeiten. Nur bei Vorliegen dieser Voraussetzung sind die folgenden Fragen zu beantworten.[9]

☒ Der Einsatz der Software hat keine personalwirtschaftlichen Auswirkungen.

☐ Folgende Unterlagen befinden sich in der Anlage :[10]

- ☐ Beschreibung des Rationalisierungspotenzials (personalwirtschaftliche Auswirkungen) B6.1
- ☐ Wirtschaftlichkeitsbetrachtung B6.2
- ☐ Umsetzungskonzept B6.3
- ☐ Qualifizierungskonzept B6.4

[8] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.
[9] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.
[10] Mehrfachankreuzungen innerhalb dieser Frage sind möglich.

C) Erklärungen

Ich versichere, dass die der Einsatz der Software im beschriebenen Umfang erfolgt und sage zu, bei einer wesentlichen Änderung oder wesentlichen Ausweitung im Sinne des § 85 Abs. 2, Nr. 8 bis 10 PersVG eine weitere Beteiligungsvorlage einzureichen. Dies bedeutet: Wenn ein Versionswechsel der beteiligten Software entweder hinsichtlich des Nutzerkreises, des Nutzungsumfanges, des Einsatzzweckes und der Beschreibung der Risikopotenziale keine Veränderung mit sich bringt oder lediglich zur Verbesserung der Stabilität, der Beseitigung von Fehlern und Ergonomiemängeln führt, bedarf es keiner weiteren Beteiligungsvorlage. Die Informationspflicht nach § 73 PersVG bleibt unberührt.

☒ Ein Berechtigungskonzept muss in konkrete Zugriffsregelungen umgesetzt und nach § 85 Abs. 2 Nr. 10 PersVG bei den örtlichen Personalräten beteiligt werden. [11]

☒ Die weiteren Beteiligungsrechte der örtlichen Personalräte bleiben von diesen Maßnahmen unberührt. [12]

Ansprechpartner für das Beteiligungsverfahren ist

Name: ..... **Sonja Gieseler**

Dienststelle / Stellenzeichen : ..... **ITDZ Berlin, PF 1 Gi**

Telefon- / Faxnummer: ..... **9(0)222-4338, 9(0)222-3599**

Mailadresse: ..... **sonja.gieseler@itdz-berlin.de**

Fachlicher Ansprechpartner zur Software bzw. zum Fachkonzept ist

Name: ..... **Peter Schwanke**

Dienststelle / Stellenzeichen : ..... **ITDZ Berlin – PB 2 2 Sc**

Telefon- / Faxnummer: ..... **9(0) 222- 6274**

Mailadresse: ..... **peter.schwanke@itdz-berlin.de**

[11] Diese Frage ist nur zu beantworten, wenn sich die Beteiligungsvorlage an den Hauptpersonalrat richtet.
[12] Diese Frage ist nur zu beantworten, wenn sich die Beteiligungsvorlage an den Hauptpersonalrat richtet.

Ich bitte um Ihre kurzfristige Zustimmung zum Einsatz der genannten Software in dem beschriebenen Funktionsumfang nach den im Einzelnen beschriebenen Mitbestimmungstatbeständen.

Mit freundlichen Grüßen
Im Auftrag

Schade
Leiterin Personal

Folgende Anlagen sind dieser Beteiligungsvorlage beigefügt:

Bitte Zutreffendes ankreuzen	Nummer der Anlage	Bezeichnung der Anlage
☒	1	Name der Software
☒	A1	Detaillierte Darstellung des Einsatzzwecks
☐	A2	Auflistung der Einrichtungen
☐	A3	Auflistung der Nutzer
☐	A4.1	Arbeitsanweisung
☐	A4.2	Auflistung der Verfahren / Anwendungen
☒	A6	Auflistung der Hard-/ Software-Konfiguration
☒	A7.1	Beschreibung des Funktionsumfangs
☒	A7.1.1	Mobile Kommunikation und Exchange Server 2003
☒	A7.1.2	Outlook 2003 einschließlich Outlook Web Access (OWA)
☒	A7.1.3	Unified Messaging Service und Exchange Server 2003
☒	A7.1.4	Struktur der öffentlichen Ordner
☒	A7.1.5	Virenschutz- und Spamfiltermechanismen
☒	A7.1.6	Verwalten der globalen Adressliste
☒	A7.2	Dokumentation des Herstellers
☒	B1	Regelungen zur Leistungs- und Verhaltenskontrolle
☒	B2.1	Beschreibung der personenbezogenen Daten
☐	B2.2a	Stellungnahme des behördlichen DSB
☐	B2.2b	Stellungnahme des Berliner DSB
☐	B3	Zertifizierung nach ISO EN 9241, Teile 10 - 17
☐	B4.1	Beschreibung der Arbeitsablauforganisation
☒	B4.2	Berechtigungskonzept
☐	B4.3	Betriebs-/Betreiberkonzept
☒	B5	Schulungskonzept
☐	B6.1	Beschreibung des Rationalisierungspotenzials
☐	B6.2	Wirtschaftlichkeitsbetrachtung
☐	B6.3	Umsetzungskonzept

Bitte Zutreffendes ankreuzen	Nummer der Anlage	Bezeichnung der Anlage
☐	B6.4	Qualifizierungskonzept
☒	C 1	Antwort auf die Anfrage des Berliner Datenschutzbeauftragten
☒	C 2	Merkblatt für unerwünschte E-Mail
☒	E 1	Eingabehilfen für Personen mit Behinderungen

Anlage 1 : Microsoft Exchange Server Editionen

Exchange Server ist eine Server Applikation, die verschiedene zentralisierte oder verteilte Aufgaben und Funktionen in der Nachrichtenverarbeitung übernimmt. Im produktiven Einsatz befindliche Exchange Server Editionen, sind Ergebnis der konsequenten Weiterentwicklung der bewährten Exchange Server-Technologien, aus den Microsoft Produkten Exchange 5.5 unter Windows NT 4.0 und Windows 2000 Server.

Exchange Server umfasst mehrere Editionen, die Anforderungen unterschiedlichster Umgebungen erfüllen:

- Exchange Server 2000 Standard Edition,
- Exchange Server 2000 Enterprise Edition,

- Exchange 2003 Server Standard Edition,
- Exchange 2003 Server Enterprise Edition,

Exchange Server wird kontinuierlich vom Hersteller weiterentwickelt, neueste Version hierzu:

- Exchange Server 2007

Übersicht Microsoft Exchange Server Editionen

Exchange Server 2000 Standard Edition
Diese Edition erfüllt die Anforderungen, die kleine und mittlere Verwaltungseinheiten an die Nachrichtenverarbeitung und die Zusammenarbeit stellen, und dient bestimmten Nachrichtenverarbeitungsfunktionen.
Diese Edition basiert auf bewährten Technologien und gewährleistet ein sicheres, zuverlässiges, stabiles und ein jederzeit verfügbares Nachrichtenverarbeitungssystem.

Leistungsmerkmale:
● Outlook Web Access (OWA) inklusive
● Eine Speichergruppe mit bis zu zwei Postfachspeichern
● Postfachspeichergröße 16 GB

Exchange Server 2000 Enterprise Edition
Diese Edition ist für große Verwaltungen konzipiert und ermöglicht das Erstellen mehrerer Speichergruppen und Datenbanken. Die Enterprise Edition ist äußerst zuverlässig und leistungsfähig und bietet einen hohen wirtschaftlichen Nutzen. Die wesentlichen Unterschiede dieser Version zur Standard Edition bestehen in der Unterstützung von Hochleistungsservern und im Clustern. Das erlaubt das Verarbeiten großer Datenmengen und macht das System von Ausfällen unabhängig.

Leistungsmerkmale:
● Beinhaltet alle Funktionen der Standard Edition
● Vier Speichergruppen mit jeweils bis zu 5 Postfachspeicher
● Postfachspeichergröße 16GB
● x.400-Connector im Lieferumfang enthalten
● Clusterunterstützung
● Unterstützung für Front- /Backend-Architektur

Exchange 2003 Server Standard Edition
Diese Edition erfüllt die Anforderungen, die kleine und mittlere Verwaltungseinheiten an die Nachrichtenverarbeitung und die Zusammenarbeit stellen, und dient bestimmten Nachrichtenverarbeitungsfunktionen.

Diese Edition basiert auf bewährten Technologien und gewährleistet ein sicheres, zuverlässiges, stabiles und ein jederzeit verfügbares Nachrichtenverarbeitungssystem.

Leistungsmerkmale:
- Outlook Web Access (OWA) und Outlook Mobile Access (OMA) inklusive
- Eine Speichergruppe mit bis zu zwei Postfachspeichern
- Postfachspeichergröße 75 GB
- Speichergruppe für die Wiederherstellung

Exchange 2003 Server Enterprise Edition
Diese Edition ist für große Verwaltungen konzipiert und ermöglicht das Erstellen mehrerer Speichergruppen und Datenbanken. Mit der Enterprise Edition können Nachrichten in unbegrenztem Umfang gespeichert werden, und die Datenmenge ist nicht auf die Kapazität eines Servers beschränkt. Die Enterprise Edition ist äußerst zuverlässig und leistungsfähig und bietet einen hohen wirtschaftlichen Nutzen. Die wesentlichen Unterschiede dieser Version zur Standard Edition bestehen in der Unterstützung von Hochleistungsservern und im Clustern. Das erlaubt das Verarbeiten großer Datenmengen und macht das System von Ausfällen unabhängig.

Leistungsmerkmale:
- Beinhaltet alle Funktionen der Standard Edition
- Vier Speichergruppen mit jeweils bis zu 5 Postfachspeicher
- Postfachspeichergröße nur durch Hardware begrenzt
- x.400-Connector im Lieferumfang enthalten
- Clusterunterstützung
- Unterstützung für Front- /Backend-Architektur

Unterschiede der Exchange Server Editionen im Überblick

	Exchange 2000 Server		Exchange Server 2003	
Feature	**Standard Edition**	**Enterprise Edition**	**Standard Edition**	**Enterprise Edition**
Speichergruppen-unterstüzung	1	4	1	4
Datenbanken pro Speichergruppe	2	5	2	5
Wiederherstellungs-speichergruppe	Nicht unterstützt	Nicht unterstützt	Unterstützt	Unterstützt
Datenbankgröße	16 GB	16 GB	75 GB	unbegrenzt
Windows Clustering	Nicht unterstützt	Unterstützt	Nicht unterstützt	Unterstützt
Active Directory	Integriert	Integriert	Integriert	Integriert
X.400 Connector	Nicht unterstützt	Unterstützt	Nicht unterstützt	Unterstützt
Front- /Backend-architektur	Nicht unterstützt	Unterstützt	Unterstützt	Unterstützt
Outook Web Access	Integriert	Integriert	Integriert	Integriert
Outlook Mobile Acces	Nicht integriert	Nicht integriert	Integriert	Integriert

Anlage A1 : Detaillierte Darstellung des Einsatzzwecks

Der Betrieb der bestehenden Exchange-Organisation und die noch ausstehende Umstellung in den einheitlichen Modus (nur Exchange Installationen ab Version 2000 aufwärts) der Exchange-Organisation bewirken folgende maßgebliche Verbesserungen und Erweiterungen im bestehenden Nachrichtenverarbeitungssystem und in der Plattform für eine übergreifende Zusammenarbeit:

Generationswechsel

Neben den bereits nicht mehr vom Hersteller unterstützten Betriebssystemen Windows NT4.0 und Windows 2000 Server, endete zum 31.12.2005 der Mainstream-Support für Exchange 5.5 Installationen. Im Zuge des damit einhergehenden Fehlens von weiter führenden Supportleistungen durch den Softwarehersteller, hat das ITDZ zum 31.12.2006 ebenfalls bestehende Supportvereinbarungen für Exchange 5.5 Kunden aufgekündigt. Alternativ dazu sind in bestehenden Kunden- und Supportvereinbarungen, sowie im Neukundengeschäft Installation ab Exchange 2003 SP2 aufwärts als neuer Standard in der Exchange Organisation vereinbart worden.
Im Zuge der Abschaltung des letzten Exchange 5.5 Server in der bestehenden Organisation werden zukünftig neue und verbesserte Exchange Eigenschaften dem Nutzer, nach Umschaltung der gesamten Exchange Organisation in den einheitlichen Modus bereitgestellt.

Microsoft Active Directory Verzeichnisdienst

Mit dem Verzeichnisdienst von Microsoft, dem Active Directory wird die Möglichkeit, Benutzer, Computer, Drucker und weitere Netzwerkressourcen zentral zu konfigurieren und zu verwalten bereitgestellt. Die im Active Directory integrierte Exchange Organisation nutz Teile dieser Informationen zum Übertragen und Verarbeiten von Nachrichten zwischen Absender und Empfänger. Im Active Directory wird darüber hinaus der größte Teil der Konfigurationsinformationen über das integrierte Nachrichtenverarbeitungssystem gespeichert. Es enthält Informationen über die Konfiguration des Systems und über die Weiterleitung von Nachrichten von einem Nachrichtenverarbeitungssystem zu einem anderen Nachrichtenverarbeitungssystem.

Verwaltungsanforderungen

Die Administrierbarkeit von Softwareinstallationen ist ein zentrales Element der Funktionalität und Verfügbarkeit, sowie der Nutzerakzeptanz. Stark verbessert wurde das zentrale Verwaltungstool Exchange System Manager, insbesondere zum Anlegen, Verwalten und Konfigurieren von Objekten in der Exchange Organisation. Die zusätzlich vorhandenen Verwaltungstools des Active Directory ergänzen die Palette der verfügbaren Tools. Die zentrale Administrierbarkeit von Exchange durch neue, komfortable Funktionen und die Möglichkeit der Nutzung vorhandener Active Directory Verwaltungstools, stellen ein hohes Maß an Sicherheit und Systemverfügbarkeit sowie eine verbesserte Stabilität der Systeme dar. Die Verwaltung der gesamten Exchange Organisation wird durch eine begrenzte Gruppe von Administratoren sichergestellt.

Benutzeranforderungen

Gestiegene Anforderungen der Nutzer an die Funktionalität der Exchange Organisation können zukünftig neben der bestehenden Standard Nachrichtenverarbeitung wie folgt umgesetzt werden:

- **Remotezugriff-** Höhere Leistungsfähigkeit im Offline-Betrieb durch Einsatz und Nutzung des Exchange-Cachemodus in Outlook 2003.
- **Webzugriff-** Webzugriff auf Exchange-Informationen über das Intranet/Internet. Arbeiten mit Outlook Web Access 2003.
- **Mobilzugriff-** Anforderungen zur Einrichtung des Zugriffs auf Exchange-Informationen mit mobilen Geräten unter Windows Mobile 5.

Unterstützung für den Outlook 2003 Exchange-Cachemodus

Exchange 2003 unterstützt den Outlook 2003-Exchange-Cachemodus, bei dem Benutzer über einen lokalen Zwischenspeicher in Form einer OST-Datei auf Exchange-Informationen zugreifen können. Exchange stellt dabei sicher, dass das Postfach auf dem Server und die OST-Datei auf dem Clientcomputer synchronisiert bleiben, solange die Netzwerkverbindung verfügbar ist. Wenn die Netzwerkverbindung nur zeitweise besteht oder ganz unterbrochen wird, können Benutzer E-Mail-Daten aus den in der lokalen OST-Datei gespeicherten Informationen abrufen. Aktualisierungsanforderungen vom Clientcomputer an den Exchange-Server werden dadurch vermieden, so dass Benutzern von Outlook 2003 in Zeiträumen, in denen die Verbindung nur teilweise oder überhaupt nicht verfügbar ist, nicht die Meldung angezeigt wird, dass Daten vom Exchange-Server angefordert werden. Durch die Vermeidung von Aktualisierungsanforderungen vom Clientcomputer wird außerdem der Datenverkehr vom Clientcomputer zum Server reduziert.

Nutzung der Verbesserungen in Outlook Web Access 2003

Die neue Version von Outlook Web Access in Exchange Server 2003 enthält eine Reihe von Verbesserungen, z. B. formularbasierte Authentifizierung, Regeln, Rechtschreibprüfung und die Möglichkeit, digital signierte und verschlüsselte E-Mail-Nachrichten zu senden und zu empfangen. Die Benutzeroberfläche ist ebenfalls neu gestaltet und der Benutzerführung in Outlook 2003 angeglichen. So sind jetzt u. a. ein Vorschaufenster auf der rechten Seite und ein verbesserter Navigationsbereich verfügbar.

Die folgende Auflistung beschreibt die wichtigsten neuen Funktionen in Outlook Web Access für Exchange 2003:

- **Anzahl übertragener Bytes-** Durch Verringerung der Informationsmenge, die zwischen Server und Browser übertragen werden muss, kann die Geschwindigkeit von Outlook Web Access gesteigert werden.
- **Unterstützung von Komprimierung-** Für Outlook Web Access kann Komprimierungsunterstützung konfiguriert werden. Leistungssteigerung bei langsamen Netzwerkverbindungen von bis zu 50 %.
- **Formularbasierte Authentifizierung-** Aktivierung der neuen Anmeldeseite für Outlook Web Access, in der die Namen und Kennwörter der Benutzer nicht im Browser, sondern in einem Cookie gespeichert werden. Beim Schließen des Browsers wird das Cookie gelöscht. Zusätzlich wird das Cookie auch nach einem bestimmten Zeitraum der Inaktivität des Benutzers gelöscht. Zum Aktivieren der Anmeldeseite von Outlook Web Access muss auf dem jeweiligen Server die formularbasierte Authentifizierung aktiviert werden.

Nutzung der Unterstützung mobiler Geräte in Exchange 2003

In Exchange 2003 sind zwei Anwendungen integriert, die sowohl Geräte mit Microsoft Windows Mobile™ 5 als auch andere mobile Geräte unterstützen. Mit der Bereitstellung der Unterstützung für mobile Geräte in Exchange, können Benutzer über verschiedene mobile Geräte auf ihre Exchange-Informationen zugreifen. Exchange ActiveSync® und Outlook Mobile Access können Sie auf dieselbe Weise für den jeweiligen Exchange Server bereitgestellt werden, wie Outlook Web Access 2003.

- **Synchronisierung-** Durch Synchronisieren eines Geräts mit einem Exchange-Server können Benutzer auf ihre Exchange-Informationen zugreifen, ohne ständig mit einem Mobilnetzwerk verbunden sein zu müssen. Die Benutzer können die Verbindung ihres Mobilnetzbetreibers verwenden, um ihre Exchange-Informationen mit ihrem mobilen Gerät zu synchronisieren und offline auf diese Informationen zuzugreifen.
- **Mobiler Browserzugriff-** Exchange Server 2003 enthält die Anwendung Outlook Mobile Access, mit der Benutzer über mobile Geräte auf den Exchange-Server

zugreifen können, um E-Mail-Nachrichten, Kontakte, Kalenderdaten und Aufgaben anzuzeigen.

Aktivierung von RPC über HTTP

Mit RPC über HTTP unter Windows Server 2003 müssen Remotebenutzer die Verbindung zum Exchange-Server nicht mehr über ein virtuelles privates Netzwerk (VPN) herstellen. Benutzer, die Outlook 2003 ausführen, können über das Internet eine direkte Verbindung mit einem Exchange 2003-Server innerhalb einer Exchange-Organisation herstellen. Die Unterstützung von RPC über HTTP ist nur verfügbar, wenn auf allen Exchange-Servern, auf die Benutzer mit Outlook 2003 zugreifen, Exchange Server 2003 ausgeführt wird. RPC über HTTP wird zudem nur von Outlook 2003 unterstützt.

Integration und Nutzung von Internet Information Server 6

Innerhalb der Exchange-Organisation werden auf den beteiligten Exchange Servern virtuelle Protokollserver betrieben, diese ermöglichen unter anderem den Clientzugriff auf Exchange Informationen. Virtuelle Protokollserver sind bei ihren Operationen und Diensten von IIS (Internet Information Services) und dem Active Directory-Verzeichnisdienst abhängig. IIS und Exchange 2003 sind durch diese Protokollstapel und eine gemeinsam verwendete Speicherwarteschlange eng miteinander verbunden. Für die Bereitstellung, Verwaltung und Fehlerbehebung von Nachrichtenverarbeitungs-Diensten hat diese Integration Auswirkungen.

Kerberos-Authentifizierung

Exchange Installationen ab Version 2003 und Outlook 2003 verwenden Kerberos für die Authentifizierung von Benutzern auf Exchange Servern. Wenn im Netzwerk Windows Server 2003-Domänencontroller verwendet werden, können sich Benutzer über mehrere Gesamtstrukturen hinweg bei den Domänencontrollern in vertrauenswürdigen Gesamtstrukturen authentifizieren, so dass Benutzerkonten und Exchange Server in unterschiedlichen Gesamtstrukturen vorhanden sein können.
Exchange 2003 verwendet beim Senden von Anmeldeinformationen von Benutzern zwischen einem Exchange-Front-End-Server und dem Exchange-Back-End-Server Kerberos-Authentifizierung.

Public Key Infrastructure (PKI)

Viele der zuvor genannten Funktionalitäten in der Exchange Organisation setzen das Vorhandensein einer Public Key Infrastructure (PKI) im Active Directory Verzeichnis voraus.

Eine weiterführende Darstellung des Funktionsumfanges und der beteiligungsrelevanten Gesichtspunkte ist den nachfolgenden Anlagen zu entnehmen.

Anlage A6 : Soft- und Hardwareanforderungen

Softwarenaforderungen

Im Zusammenhang mit einer möglichen zukünftigen Skalierung der Exchange Installationen auf den jeweiligen Exchange Servern der Organisation wird der Einsatz von Windows Server 2003 Enterprise Edition als Basisbetriebssystem empfohlen. Diese Betriebssystemkomponente unterstützt zukunftsorientiert Arbeitsspeichererweiterung, Mehrprozessorarchitektur und Server-Clustering. Im Hinblick auf die Entwicklung und den weiteren Ausbau der IT-Umgebung einer Verwaltung / Behörde ist eine nicht zu vernachlässigende Infrastrukturentscheidung.
Im Hinblick auf die Version der zu installierenden Exchange Software, ist aufbauend auf das Basisbetriebsystem (wie oben benannt) zu beachten, dass bestimmte Exchange Feature an bestimmte Exchange Versionen gebunden sind (Siehe Anlage 1). Für eine zukunftsorientierte Exchange Installation wird daher vom ITDZ grundsätzlich die Exchange Server 2003 Enterprise Edition empfohlen. Diese Exchange Version bietet die meisten Feature zur Erweiterung der bestehenden Konfiguration.

Hardwareanforderungen

In Abhängigkeit von der Active Directory Integration der Verwaltung / Behörde bietet das ITDZ grundsätzlich zwei Alternativen zur Exchange Integration an.

1. zentrale Postfachressourcen (keine eigne Hardware für Exchange erforderlich)
2. dezentrale Postfachressourcen (eigene Serverhardware erforderlich)

Verwaltungen / Behörden die keine eigene Active Directory Domäne innerhalb der Gesamtstruktur der Berliner Verwaltung betreiben, erhalten ausschließlich zentrale Postfachressourcen. Dies bedeutet dass alle Active Directory und Exchange relevanten Konfigurationen ausschließlich durch administratives Personal des ITDZ durchgeführt werden. Verwaltungen / Behörden die über eine o.g. Domäne in der Gesamtstruktur verfügen, können zwischen beiden Alternativen, der kostengünstigeren bzw. der eigenverantwortlichen Integration wählen.
Zur Sicherstellung der Verfügbarkeit und Funktionalität des gesamten Exchange Verbundes ist eine Exchange Installation für dezentrale Postfachressourcen auf einer Hardware unter Beachtung folgender Aspekte jeweils skalierbar auszulegen:

- Anzahl der Postfächer pro Server,
- Größe der Postfächer pro Server,
- Größe der öffentlichen Ordner pro Server,
- Anzahl der Datenbanken pro Server,
- Netzverfügbarkeit und Geschwindigkeit,
- Anzahl der Clients die auf Exchange Server zugreifen.

Ausgangspunkt einer Skalierung hierbei ist eine Hardware mit:
Intel, oder Intel-Prozessor kompatibler Hardware wie z.B.

- 2 x Dual Core CPU Intel 5160
- 2 GB RAM
- 36 GB RAID 1 Betriebssystem + Exchange Transaktionsprotokolle
- 146 GB RAID 5 Exchangedatenbanken
- sowie Netzwerkkarten

Sowohl Arbeitsspeicher als auch Plattenkapazität sollten skalierbar ausgelegt sein. Plattensubsysteme wie SAN oder NAS gelten als skalierbar. In Abhängigkeit der Betriebssystem Version und der Exchange Version ist Server-Clustering und Exchange-Skalierung gegeben.

Anlage A7.1 : Beschreibung des Funktionsumfanges

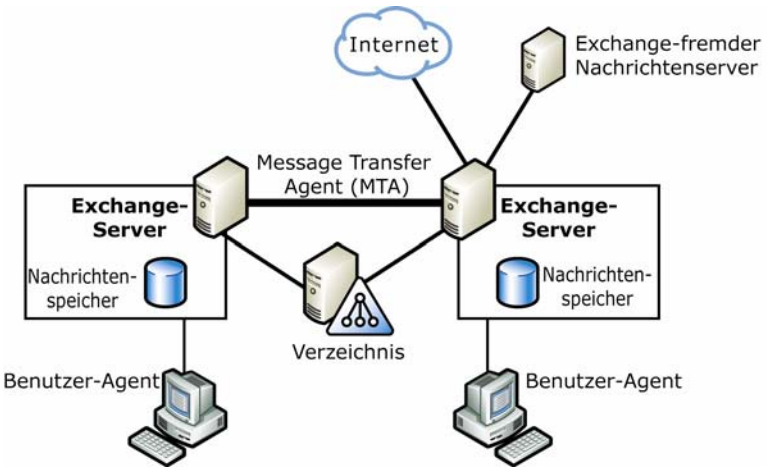
Die in dieser Vorlage zu beschreibende Microsoft Exchange-Organisation definiert ein Nachrichtenverarbeitungssystem innerhalb einer Active Directory Gesamtstruktur (Forrest). Der Betrieb einer Exchange-Organisation unter den Exchange Server Versionen ab 2000 aufwärts, setzt das Vorhandensein eines Microsoft Active Directory Verzeichnisdienstes voraus. Diese Exchange-Organisation wird im einheitlichen Modus vollständig die bisherige Exchange-Organisation im gemischten Modus (mit Exchange 5.5) ersetzen.

Microsoft Exchange Organisation

A Allgemeine Beschreibung	
Name und Version	Microsoft Exchange-Organisation ab Exchange Server 2000 aufwärts alle Editionen
Einsatzzweck	**Nachrichtenverarbeitungssystem und Plattform für übergreifende Zusammenarbeit**
Einsatzbreite	Landesweit
Nutzerkreis	Primär im vollen Funktionsumfang alle Dienstkräfte die an das Active Directory angeschlossen sind. Sekundär alle Nutzer im Intranet die über AD-Informationen verfügen und das Internet eingeschränkt, für dort veröffentlichte E-Mail Empfängeradressen
Nutzungsumfang	wie Nutzerkreis
Art der Software	Serverapplikation mit Clientschnittstelle (MS Outlook)
Hardwarevoraussetzungen	Mitgliedsserver im Active Directory Verzeichnisdienst
Softwarevoraussetzungen	Microsoft Exchange Server ab Version 2000

B Funktionsumfang

Die Exchange-Organisation enthält alle Exchange-Server, Domänencontroller, globalen Katalogserver, Benutzer und weitere Active Directory Verzeichnisobjekte, die zusammen als eine Einheit im System der Nachrichtenverarbeitung und als Plattform für die Zusammenarbeit fungieren.



Der Active Directory Verzeichnisdienst stellt das Sicherheitsteilsystem für die Exchange-Organisation bereit. Mit den Active Directory-Sicherheitsfunktionen wird gewährleistet, dass nur autorisierte Benutzer auf Postfächer zugreifen können und dass ausschließlich autorisierte Administratoren die Exchange-Konfiguration in der Organisation ändern können. Microsoft Exchange-Dienste greifen auf die in Active Directory gespeicherten Informationen zu und schreiben Informationen in das Active Directory Verzeichnis zurück.

Zum Funktionsumfang eines Nachrichtenverarbeitungssystems gehören:

Nachrichtentransportverfahren
Die Nachrichtenübertragung in der Microsoft Exchange-Organisation ist hauptsächlich Aufgabe des SMTP-Dienstes. Das SMTP- Transportmodul ist an der gesamten Nachrichtenverarbeitung beteiligt, unabhängig vom endgültigen Ziel der Nachricht. Eine Nachricht kann für einen Benutzer bestimmt sein, der sich auf demselben Server, einem anderen Server innerhalb der Exchange-Organisation oder einem Server in einem externen (Intranet oder Internet) Nachrichtenverarbeitungssystem befindet.

Liste aller Nutzer (hier globales Adressbuch)
Das globale Adressbuch ist die Zusammenstellung aller mailaktivierten Objekte in einer Active Directory Gesamtstruktur, diese Objekte befinden sich in unterschiedlichen Hostdomänen und werden erst durch den globalen Katalog domänenübergreifend erreichbar. Ein globaler Katalog ist ein Domänencontroller, der eine Kopie aller Active Directory Objekte in einer Gesamtstruktur speichert. Im globalen Katalog wird eine vollständige Kopie aller Objekte in dem Verzeichnis der Hostdomäne und eine Teilkopie aller Objekte für alle anderen Domänen in der Gesamtstruktur gespeichert Exchange-Server innerhalb Exchange-Organisation nutzen die Informationen des globalen Katalog zur Generierung und Abbildung des globalen Adressbuches.

Speicherort für Nachrichten bis zum Abruf durch den Client
Innerhalb einer Exchange Organisation speichert jeder einzelne Exchange-Server im Nachrichtenspeicher, d. h. im Exchange-Informationsspeicher, E-Mail-Nachrichten und andere Objekte in Postfächern und Öffentlichen Ordnern für die von diesem Server verwalteten Nutzer und Objekte. Darüber hinaus enthält der Informationsspeicher Nachrichtentabellen, die beim Weiterleiten von Nachrichten von Server zu Server vom Transportsubsystem zum temporären Speichern von Nachrichten verwendet werden. Der Exchange-Informationsspeicher ist zur Implementierung der Nachrichtendatenbanken von der ESE-Technologie (Extensible Storage Engine) abhängig.

Frontend Schnittstelle (Mail-Client) zur Kommunikation mit dem Mail-Server
Über die Frontend Schnittstelle kann auf das Nachrichtenverarbeitungssystem zugegriffen werden. Die Exchange-Organisation unterstützt eine Vielzahl unterschiedlicher Mail-Clients, einschließlich MAPI-Clients, HTTP-Clients sowie Clients, die POP3, IMAP4 und NNTP (Network News Transfer Protocol) verwenden. Die LDAP-Unterstützung (Lightweight Directory Access Protocol) für die Verzeichnissuche wird dagegen von Active Directory bereitgestellt. Das zum Einsatz kommende Frontend liegt daher in Verantwortung der Verwaltungseinheiten selbst. Microsoft Outlook z.B ist Bestandteil Microsoft Office Suite, dies ist die optimale Client Komponente, jedoch ist für die Funktionalität der Exchange Organisation Microsoft Outlook nicht zwingend erforderlich. ***Der Mail-Client ist eine vollständig separate Komponente, deren Funktionsumfang nicht Bestandteil dieser Beteiligungsvorlage ist.***

C Delta zur Vorgängerversion bis Exchange 5.5 unter Windows NT4.0

Element	Delta
Active Directory Verzeichnis	Bereitstellung des Verzeichnisdienstes zur Verwaltung aller relevanten Objekte in der Gesamtstruktur durch die Server der Exchange Organisation
Sicherheitsteilsystem	Die Server der Exchange Organisation verwenden ein Sicherheitsteilsystem von Windows Server 2003 zur Authentifizierung von Benutzern in der Exchange-Organisation. Mit dem Sicherheitsteilsystem wird sichergestellt, dass ausschließlich autorisierte Benutzer auf Postfächer zugreifen oder E-Mail-Nachrichten an angegebene Empfänger senden können.

Verwaltungsprogramme	Zentrale Elemente -> Exchange Systemmanager und SnapIn Active Directory Benutzer und Computer
Netzwerkprotokoll	TCP/IP-Standardprotokoll, andere Netzwerkprotokolle werden nicht unterstützt
Nachrichtenprotokoll	SMTP-Protokoll als Standard Nachrichtenprotokoll
Domain Name Service (DNS)	Die Server der Exchange Organisation lösen über DNS die IP-Adressen für andere Hosts, Domänencontroller und globale Katalogserver in einer Active Directory Gesamtstruktur, sowie für die E-Mail-Server in anderen Nachrichtenverarbeitungssystemen, in einem TCP/IP-Netzwerk auf.
Zertifikat basierte Authentifizierung	Der Active Directory Verzeichnisdienst steigert die Sicherheit im Netzwerk deutlich. Das Kerberos Protokoll ist ein Netzwerk- Authentifizierungsprotokoll, das die Identität von Benutzern authentifiziert, die versuchen, sich an einem Netzwerk anzumelden, und verschlüsselt deren Verbindungen durch Secret-Key Kryptografie. Exchange ActiveSync Zertifikat- basierte Authentifizierung nutzt die Kerberos-Transaktion im Exchange Frontend Server. Das heißt, das Client-Zertifikat wird auf einem Benutzerkonto abgebildet und der Exchange Frontend Server muss die Kerberos Constrained Delegation (KCD) freigegeben haben, um die Kerberos-Impersonation basierend auf dem Benutzer-Zertifikat durchzuführen. Damit müssen Zugangsdaten nicht mehr auf dem Gerät gespeichert werden, jedoch ist eine Public Key Infrastructure (PKI) erforderlich.
Unterstützung für Secure /Multipurpose Internet Mail Extentions (S/MIME)	Durch S/MIME wird die Sicherheit von Internet-E-Mail mithilfe digitaler Signaturen und Nachrichtenverschlüsselung ermöglicht. Durch digitale Signaturen werden Authentifizierung, Nichtabstreitbarkeit und Datenintegrität ermöglicht. Die Nachrichtenverschlüsselung gewährleistet Vertraulichkeit und Datenintegrität. Es handelt sich um eine Client zu Client Verschlüsselung, d.h. die Programme der Anwender verschlüsseln die Daten und senden diese über die Nachrichtenverarbeitungssysteme. Exchange sieht wie jedes andere Nachrichtenverarbeitungssystem nur die codierten Nachrichten, d.h. eine gültige Mail mit Absender und Empfänger, aber dann nur noch Sonderzeichen. S/MIME verwendet zur Bereitstellung von Signatur- und Verschlüsselungsfunktionen eine beliebige X.509v3-Infrastruktur öffentlicher Schlüssel (Public Key Infrastructure, PKI erforderlich). Der Vorteil der Verwendung des S/MIME-Standards für Sicherheitsfunktion ist, dass Verschlüsselung und Signatur einfach zu bedienen sind.
ActiveSync für die Synchronisierung tragbarer Geräte	Direkte Synchronisation von Pocket Outlook mit Microsoft Windows–powered mobilen Endgeräten, Wireless Synchronisation über GPRS oder UMTS, Internetzugriff über den Desktop-PC, wenn eine entsprechende Verbindung besteht, Authentifizierung und sichere Übertragung über die Domänen-Credentials, SSL und RPC over HTTPS, Mit Pocket Outlook (Windows Mobile 5 mit Security Feature Pack) können alle Postfachordner synchronisiert werden. Die Synchronisation ist optimiert auf Wireless Verbindungen.

Intelligenter Anti Spam-Filter SmartScreen-Filtertechnologie (IMF)	IMF (Intelligent Message Filter) schützt den einzelnen Exchange Server vor Überflutung durch Spam. IMF arbeitet mit Algorithmen nach dem Wahrscheinlichkeitsprinzip. E-Mail Nachrichten werden dabei nach einem Punktesystem auf Basis des Feedbacks bewertet. IMF ist in der Lage, 500.000 Spam-Eigenschaften auszuwerten. Nach einer IMF-Auswertung filtert SmartScreen die Spam-Mails. Regelmäßige Filter-Updates werden zur Verfügung gestellt.
Globale Annahme-/Verweigerungsliste (Blacklist/Whitelist)	Mithilfe der Verbindungsfilterung wird die globale Annahmeliste erstellt. Mit dieser Liste wird unabhängig von der Verwendung eines Sperrlistendienstanbieters festgelegt, ob von benannten IP-Adressen gesendete Nachrichten immer angenommen werden sollen. Alle in der globalen Annahmeliste aufgeführten IP-Adressen werden automatisch akzeptiert. Einträge in der globalen Annahmeliste haben Vorrang vor Einträgen in der globalen Verweigerungsliste. Durch Exchange Server wird die globale Annahmeliste vor der globalen Verweigerungsliste überprüft. Wenn über eine in der globalen Annahmeliste enthaltene IP-Adresse versucht wird, eine Verbindung zum Exchange-Server herzustellen, wird durch Exchange zunächst die globale Annahmeliste überprüft. Da Exchange eine Übereinstimmung für die IP-Adresse findet, wird die Verbindung angenommen, und es werden keine weiteren Verbindungsfilterungsprüfungen von Exchange durchgeführt.
Viren-API Drittanbieter Anti-Viren-Softwareanbindung (VSAPI 2.5)	Antivirus-Anbieter können infizierte E-Mail-Nachrichten markieren, so dass diese nicht mehr an den Empfänger übermittelt werden. Bisher konnte der böswilligen Inhalt zwar entfernt werden, eine Zustellung der E-Mail Nachricht jedoch konnte durch Dritt-Anbieter nicht verhindert werden. VSAPI kann durch ein OnSubmit Ereignis, in den Nachrichtentransport eingreifen. Diese Lösung scannt, Bridgeheadserver, Front-/Backend Server und Connector Server mit der gleichen Antivirus-API und Engine. Durch Auswertung der Nachrichten Headerinformationen können Absender-Information für die Übermittlung fakultativer Nachrichten über den böswilligen Inhalt an den Absender der Nachricht zurück gesendet werden.
Unterstützung des Sender-ID E-Mail-Authentifizierungsprotokoll	Zusätzliche Unterstützung bei der Abwehr von Mailbox-Phishing und anderen betrügerischen Mails (Spoofing), indem die IP-Adresse des E-Mail-Absenders gegen den vorgeblichen Besitzer der Domäne des Absenders abgeglichen wird. Bei Spoofing-Attacken täuscht eine Person oder ein Programm erfolgreich eine falsche Identität vor, um Zugang zu persönlichen Daten zu erlangen. Das Ergebnis der Sender ID-Überprüfung dient als Input für den Exchange Intelligent Message Filter (IMF). Der Absender muss dabei eine Liste gültiger IP-Adressen im DNS registriert haben, ansonsten wird durch Exchange der Nachrichtentransport an den Empfänger verweigert..

E-Mail Zugriff via Direct Push-Technologie	Es ist nicht mehr erforderlich sich mit dem mobilen Gerät bei Exchange zu melden (z.B. über Short Message Service (SMS)) um sicherstellen zu stellen, dass das mobile Gerät automatisch E-Mail Nachrichten vom Exchange Server abruft. Exchange Server nutzt eine vom Gerät aufrechterhaltene HTTP-Verbindung, um neue E-Mail-, Kalender-, Kontakt- oder Aufgaben-Benachrichtungen an das Gerät zu senden (Push).
Postfachzugriff über das Intranet/Internet (Outlook Web Access)	OWA baut eine Verbindung zu einem Exchange-Server auf, rein durch die Verwendung eines Browsers und dem bewährten HTTP-Protokoll. Diese Technik ermöglicht Fernzugriffe auf Postfachinformationen. Zur Steigerung der Sicherheit wird grundsätzlich die Verwendung des HTTPS-Protokolls erzwungen. Neben dem Postfach mit den Ordnern "Posteingang", "Postausgang", "Gesendete Objekte" und "Entwürfe" ist der Zugriff auf die von Outlook bekannten Funktionen wie den Kalender, die Aufgabenverwaltung oder die Notizen möglich. Mit OWA arbeitet man direkt auf dem Exchange Server. Alle Änderungen am Postfach sind verbindlich.
Postfachzugriff über mobile Geräte (Outlook Mobile Access)	Outlook Mobile Access (OMA) ist der Mobile Online Zugriff auf ein Postfach über einen entsprechenden PDA möglich. Die Menüführung ist dabei auf kleine Displays optimiert. Sofern die Unterstützung für nicht kompatible PDA-Geräte aktiviert ist, kann der Zugriff auch über einen Browser auf dem PC erfolgen. Folgende Funktionen unterstützt OMA: Mobiler Microbrowser Zugriff auf Server in der Exchange Organisation, Unterstützung für Browser welche HTML, XHTML, WAP 2.X und CHTML unterstützen, Zugriff auf Posteingang, Kalender, Kontakte und Aufgaben, Suchzugriff auf das globale Adressbuch
Frontend Komponente Microsoft Outlook	Durch Outlook 2003 kann eine sichere Internetverbindung über PRC over Http ohne VPN-Lösung hergestellt werden, Verbesserte Synchronisierung durch Datenkomprimierung zwischen Client und Server, Größere Speicherkapazität für persönliche Ordnerdateien (PST) durch neues Dateiformat, Kerberos-Authentifizierung des Client am Server, Exchange-Cachemodus wir vollständig unterstützt.
D Beteiligungsrelevante Merkmale	
Leistungs- und Verhaltenskontrolle	Leistungs- und Verhaltenskontrolle (nach §85 Abs. 1 Nr. 13 PersVG) ist ausgeschlossen. *Siehe auch Anlage B1*
Verarbeitung personenbezogener Daten	Die im Active Directory integrierte Nutzerverwaltung, die durch die Exchange-Organisation genutzt wird, stellt die Identität eines Nutzers im Gesamtsystem dar. *Umfang und Inhalt siehe Anlage B2.1*
Softwarergonomie	Es ergeben sich **keine** wesentlichen Veränderungen zu vorher betriebenen Exchange-Serverapplikationen.
Arbeitsablauforganisation	Benutzer verfügen über **keine**n Zugriff auf den Mitgliedsserver und die dort installierte Exchange Server Anwendung. Für Administratoren wird durch den Einsatz zahlreicher neuer Werkzeuge die Exchange Systemverwaltung erleichtert.

Schulung	Die Aneignung des notwendigen Wissens für die Administration der Exchange-Systemumgebung ist auf einen zahlenmäßig geringen Personalbestand beschränkt. Die Durchführung von Qualifizierungsmaßnahmen erfolgt durch InHouse-Schulungen bzw. Kursbelegung bei Drittanbietern
Rationalisierung	Der Einsatz dieser Applikationssoftware hat **keine** personalwirtschaftlichen Auswirkungen
E Entscheidung	
Stategisch / Technologisch	Ein Generationenwechsel in der Serverlandschaft der bestehenden Exchange-Organisation der Berliner Verwaltung hat bereits stattgefunden. Daher ist sowohl aus technologischen / wirtschaftlichen als auch aus Gründen der IT-Sicherheit sowie der Vereinheitlichung der Exchange-Systemumgebung die Einführung / Nutzung der Exchange Server Editionen ab Version 2000 als Standard Nachrichtenverarbeitungssystem und Plattform für übergreifende Zusammenarbeit auf der Basis des Microsoft Active Directory als implementierten Verzeichnisdienst in der Berliner Verwaltung gegeben. Die Abkündigung von Supportleistungen des Herstellers für Serversysteme unter Exchange 5.5 erfordert zusätzlich unmittelbar Handlungserfordernis.
Beteiligungsrelevant	Unter Berücksichtigung der in dieser Beteiligungsvorlage dokumentierten Verfahrensmerkmalen der Exchange Organisation und deren praktische Umsetzung für das produktiv System im Active Directory der Berliner Verwaltung, sowie der dabei herausgestellten beteiligungsrelevanten Aspekte, ist dem Aufbau und dem Betrieb der Exchange-Organisation als Nachrichtenverarbeitungssystem und Plattform für übergreifende Zusammenarbeit zuzustimmen.

_____ _____

Datum Unterschrift

Anlage A7.1.1: Mobile Kommunikation und Exchange Server 2003

Die Bereitstellung der mobilen Kommunikation mit Exchange Server vereint unterschiedliche Verfahren und Technologien unter Nutzung aktueller Sicherheitsstandards für den geschützten Zugriff auf Nachrichten und Daten innerhalb eines Nachrichtenverarbeitungssystems. Die mobile Kommunikation ermöglicht ausgewählten und / oder allen Nutzern im Bedarfsfalle, unter Einsatz von geeigneten Arbeitsmitteln sowohl den geschützten Zugriff von anderen Standorten innerhalb der Berliner Verwaltung (Intranet) aus als auch von Außerhalb (Internet) auf Informationen des Nachrichtenverarbeitungssystems. Nutzer der bereitgestellten mobilen Dienste unter Exchange Server 2003, können in Abhängigkeit von der Leistungsfähigkeit (Displaygröße, Speicherkapazität und weiterer Parameter) des jeweils eingesetzten mobilen Gerätes, einen uneingeschränkten oder nur einen teilweisen Zugriff auf die Gesamtheit der Daten und Nachrichten des ihnen zugeordneten Postfaches im Nachrichtenverarbeitungssystem erhalten. Die Gesamtheit der verfügbaren Möglichkeiten einer mobilen Kommunikation definiert sich über die Bereitstellung folgender Verfahren und Technologien:

- Outlook Mobile Access (OMA)
- ActiveSync mit DirectPush Technologie (MDA, PDA, Blackberry)
- Wireless Mobile Service Application (WAP)

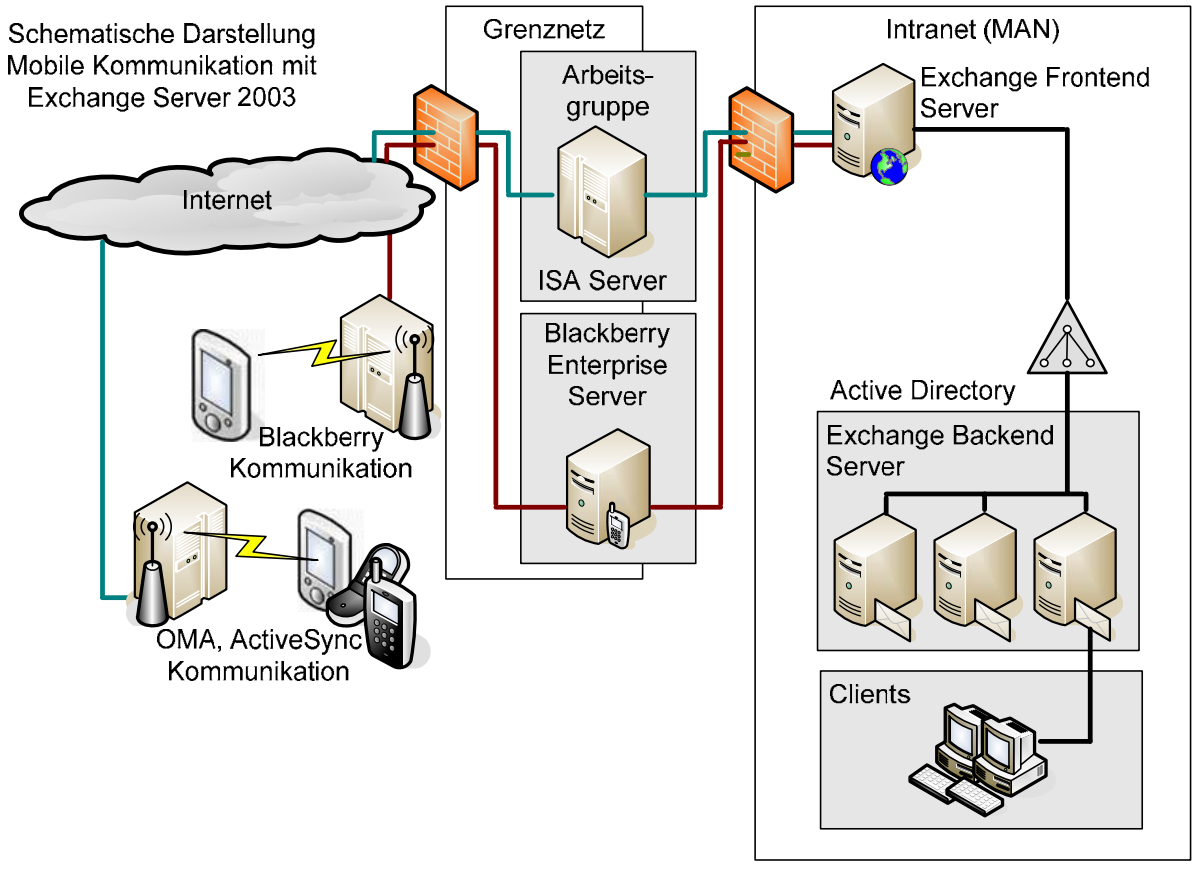


Abb. 1 Schematische Darstellung der mobilen Kommunikation mit Exchange Server 2003

Bereitstellung mobiler Dienste unter Exchange Server 2003

Während der Softwareinstallation eines Exchange Server 2003, werden alle erforderlichen Dienste und Technologien für den späteren Einsatz von mobilen Diensten unter Exchange Server 2003 installiert und konfiguriert. Die Bereitstellung der mobilen Dienste jedoch ist standardmäßig nach der Installation deaktiviert. Erst das Aktivieren der einzelnen Dienste ermöglicht die mobile Kommunikation.

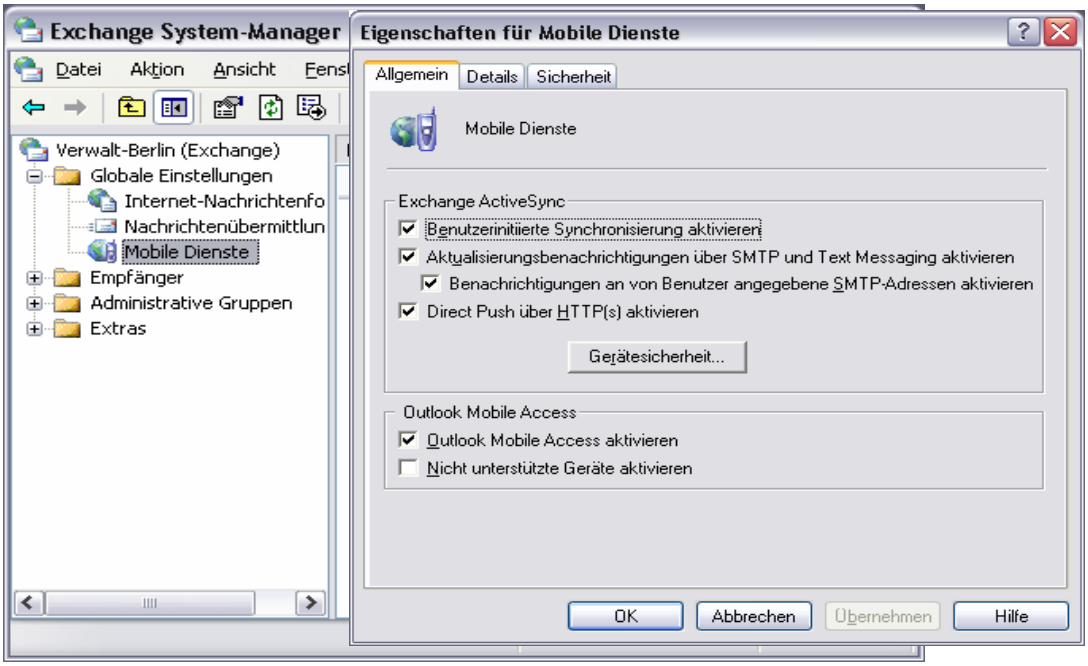


Abb.2 Aktivierung der Eigenschaften für mobile Dienste

Die Aktivierung der mobilen Dienste auf der Ebene der Exchange Organisation ermöglicht mobilen Clientgeräten den Zugriff auf die virtuellen Verzeichnisse „Microsoft-Server-ActiveSync“ und „OMA“.

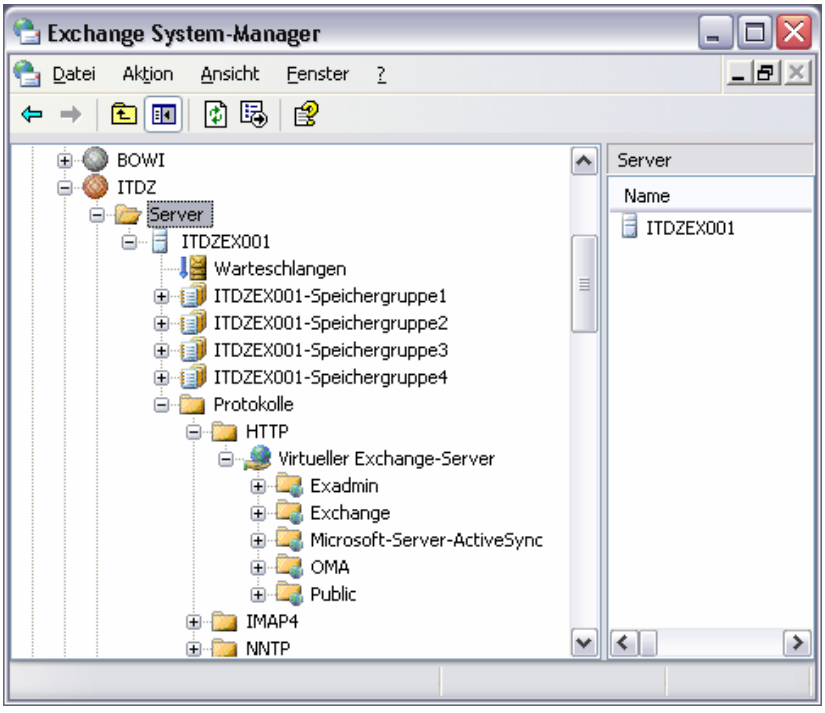


Abb.3 Konfiguration des virtuellen Exchange-Server für mobile Dienste

Diese virtuellen Verzeichnisse werden bereits bei der Installation von Exchange angelegt, jedoch erst mit Aktivierung der mobilen Dienste für einen Nutzerzugriff serverseitig freigegeben. Die Exchange Server Komponenten die durch Aktivierung der mobilen Dienste in das Nachrichtensystem eingreifen, nutzen die vorhandene Konfiguration des Active Directory und damit die Konfiguration des Nachrichtenverarbeitungssystems um Daten und Nachrichten einem oder mehreren Nutzern in einem Umfang bereit zustellen, der sich ausschließlich durch die Art des Zugriffs auf diese Informationen (mobile Geräte), von einem Zugriff mittels Standardmailclient (Outlook) unterscheidet.
Damit Anwender die auf dem Exchange Server aktivierten Dienste und virtuellen Verzeichnisse auch nutzen können, muss für den entsprechenden Nutzerkreis über das Verwaltungstool „Active Directory Benutzer und Computer“ ebenfalls, anlog zum jeweiligen Exchange Server, eine Aktivierung der entsprechenden Exchange Feature je Anwender zugelassen oder untersagt werden.

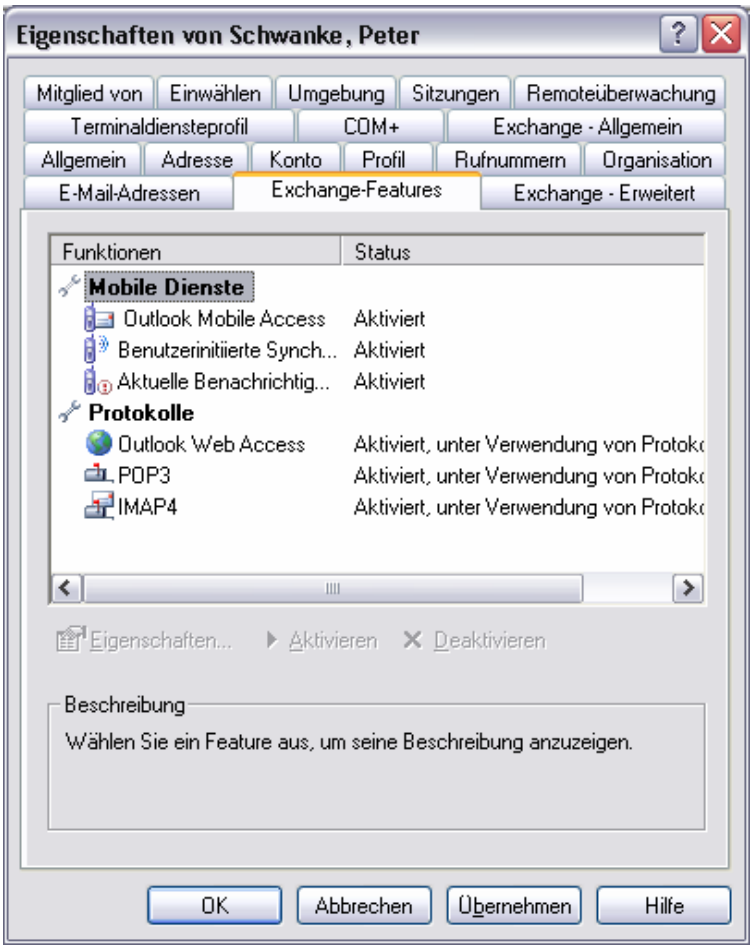


Abb. 4 Nutzerabhängige Aktivierung Mobiler Dienste in Active Directory

Outlook Mobile Access

Outlook Mobile Access stellt grundsätzlich durch den mobilen Zugriff auf Daten und Informationen ein komfortables Arbeiten unterwegs sicher. Der geschützte Datenaustausch erfolgt je nach Netzverfügbarkeit über GPRS, UMTS oder WLAN. Die Lösung basiert auf Exchange Server Standardkomponenten und benötigt keine zusätzliche Software. Outlook Mobile Access unterstützt beliebige Endgeräte und erlaubt den parallelen Zugriff auf Postfachinformationen eines Exchange Server über Handheld und Notebook.
Mobile Nutzer setzten hierfür sowohl Browseroberflächen als auch eine vertraute Windowsoberfläche auf mobilen Geräten für einen Zugriff auf E-Mails, Kalender und Kontakte ein.

Die Endgeräte verfügen somit entweder nur über einen integrierten Microbrowser oder aber über Pocket Office-Anwendungen, diese erlauben die Erstellung, Bearbeitung sowie den Empfang und Versand von Dokumenten und Anhängen von unterwegs, hingegen die Browseroberfläche Basisfunktionalitäten bereitstellt.

Abb. 5 OMA Zugriff: linke Seite über WAP und rechte Seite mit Pocket Office

Mit Einführung von Windows Mobile 5 Betriebssystemen für mobile Endgeräte verändert sich für den mobilen Nutzer vordergründig die Nutzeroberfläche des mobilen Gerätes, jedoch die wesentlichsten Änderungen von Windows Mobil 5 sind die Kommunikationsschnittstellen mit Exchange als Nachrichtenverarbeitungssystem. Die Integration des Messaging & Security Feature Pack als Zusatzkomponente von Windows Mobil 5 basierenden Endgeräten steigert hierzu vor allem die Nutzer- und Gerätesicherheit.

Exchange ActiveSync, Direct Push Technologie und Gerätesicherheit

Exchange ActiveSync ist ein Exchange-Synchronisierungsprotokoll, mit dem ein definiertes Postfach (Abb.4) mit einem Windows Mobile 5.0-basierten Gerät synchronisiert wird. Exchange ActiveSync ist optimiert für lange Wartezeiten, Netzwerke mit geringer Bandbreite und Clients mit geringen Kapazitäten, wenig Arbeitsspeicher, wenig Speicherplatz und einer schwachen CPU. Als Grundlage des Exchange ActiveSync-Protokolls dienen HTTP, SSL und XML.
Exchange Active-Sync bietet folgende Vorteile:

- Die Konsistenz der vertrauten Outlook-Benutzeroberfläche,
- Keine zusätzliche Software zur Installation / Konfiguration der mobilen Geräte erforderlich,
- Globale Funktionalität über einen Telefondienst mit Standardzugriff,

Windows Mobile 5-basierende Geräte mit Messaging & Security Feature Pack und die in Exchange Server 2003 SP 2 enthaltende Direct Push Technologie bietet einen neuen Ansatz für die Verteilung von Daten und Informationen vom Exchange-Postfach an das mobile Geräte eines Nutzers. Direct Push funktioniert mit Postfachdaten, einschließlich Posteingang, Kalender, Kontakte und Aufgaben. Direct Push Technologie verwendet eine bereits hergestellte HTTPS-Verbindung zwischen dem mobilen Gerät und dem Exchange-Server. Auf dem mobilen Gerät werden keine besonderen Konfigurationen mehr benötigt, in früheren Lösungen musste hier noch eine SMS vom mobilen Gerät zum Exchange Server gesandt werden um eine Kommunikationsstrecke aufbauen zu können.
Benutzer von mobile Geräten mit Messaging & Security Feature Pack sind in der Lage, Kontaktinformationen von Personen in der Globalen Address Liste (GAL) der Exchange Organisation zu empfangen. Die Nutzer erhalten alle Informationen, die zum erreichen der jeweiligen Kontakte im GAL erforderlich sind, ohne dass diese Daten auf den mobilen Geräten gespeichert sein müssen.

Exchange Server 2003 stellt die Möglichkeit der Konfiguration und Verwaltung einer zentralen Sicherheitsrichtlinie für mobile Geräte bereit.
Die zentrale Richtlinie erzwingt:

- den Passwortschutz, Kennwort für den Zugriff auf Exchange Server erforderlich,
- eine Kennwortrichtlinie, mind. 8 Zeichen sowie Großbuchstaben als auch Sonderzeichen müssen enthalten sein,
- Zeitdauer der Inaktivität des Gerätes bis zur neuerlichen Kennworteingabe, 30 Min
- Option „Gerät nach Fehlschlägen bereinigen“ ermöglicht das Löschen aller Daten auf dem mobilen Gerät nach einer festzulegenden Anzahl fehlgeschlagener Kennwort eingaben. Dieser Löschvorgang wird dem Nutzer unter Anzeige von Warnmeldungen und dem Herunterzählen von Zugriffsversuchen angekündigt.
- „Synchronisation nicht kompatibler Geräte erzwingen“, diese Richtlinieneinstellung ist deaktiviert, da hier Sicherheitsrisiken bestehen, die nicht von der Standardtechnologie (Messaging & Security Feature Pack) abgedeckt werden können.

Die zentrale Gerätesicherheitsrichtlinie wird auf der Eigenschaften Seite der mobilen Dienste im Exchange System Manager zentral verwaltet:

- In Form einer Liste aller mobilen Geräte, die von Nutzern verwendet werden (Siehe Abb. 2),

Verlorene, gestohlene oder auf andere Weise gefährdete mobile Geräte können durch greifen der Sicherheitsrichtlinie (fehlgeschlagene Kennworteingaben) oder direkt durch Geräteauswahl (Liste aller Geräte) innerhalb von Sekunden vollständig bereinigt, gelöscht werden (ausgenommen Daten auf einer Speicherkarte). Das mobile Gerät kann bei durchgesetzter Sicherheitsrichtlinie im o.g. Problemfall, ausschließlich des Empfangs zur Benachrichtigung über die Bereinigung und des Sendens eines Statusberichtes über den Stand der Bereinigung, keinen anderen Vorgang ausführen.

Zur weiteren Erhöhung der Gerätesicherheit und der Kommunikationssicherheit zwischen Exchange Server und den angeschlossenen mobilen Geräten kommt zusätzlich zur SSL-Standardauthentifizierung (HTTPS) die Integration der Infrastruktur für öffentliche Schlüssel (Public Key Infrastructure, PKI) unter Verwendung eines Microsoft-Zertifikatsserver zur Anwendung. Hierbei sind der private Schlüssel und das Zertifikat zur Clientauthentifizierung ausschließlich auf dem mobilen Gerät gespeichert. Wenn nicht autorisierte Nutzer versuchen durch falsche Kennworteingaben Gerätezugang zu erhalten wird automatisch die Bereinigung (wie oben beschrieben ausgeführt) und zusätzlich das Clientzertifikat gelöscht, somit kann dieses Gerät sich zusätzlich zur vollständigen Bereinigung des Gerätespeicherplatzes, nicht mehr am Exchange Server als gültiges mobiles Gerät anmelden.

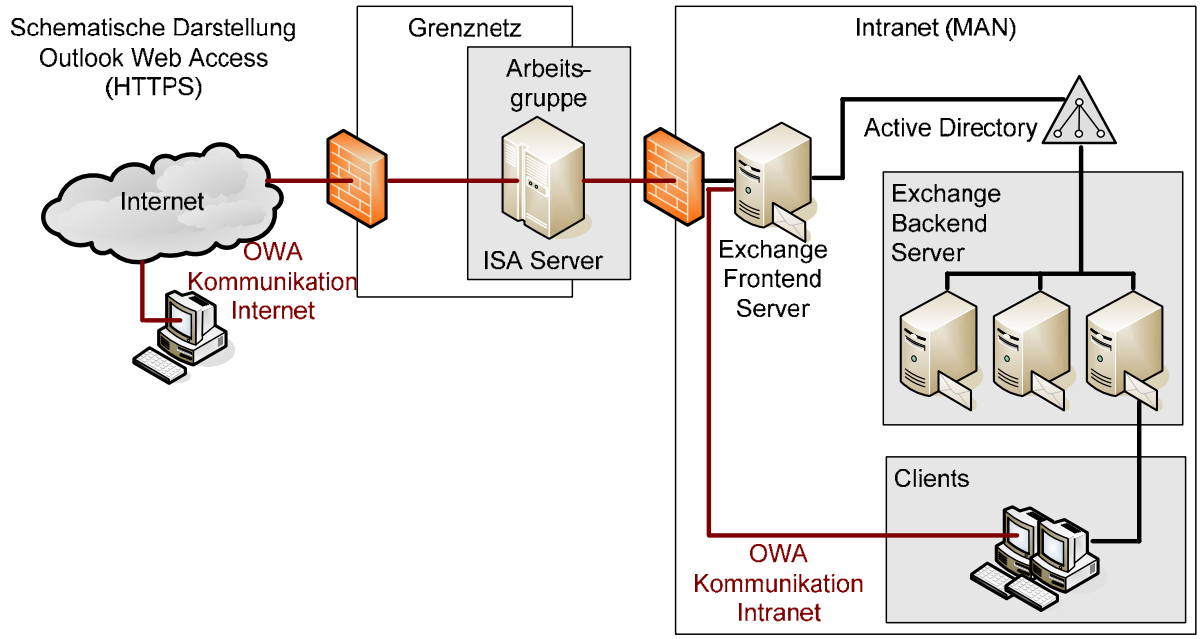
Mit der Bereitstellung einer PKI-Infrastruktur im Active Directory Verzeichnisdienst, wird nicht nur die Gerätesicherheit durch Clientzertifikat unterstützt, sondern parallel hierzu können auch Benutzer S/MIME- verschlüsselte Nachrichten auf ihren mobilen Geräten empfangen und versenden. Dies unterstützt die geschützte Kommunikation zwischen mobilen Endgeräten und dem Nachrichtenverarbeitungssystem sowohl auf der Nutzer- als auch auf der Geräteseite.

Anlage A7.1.2. : Outlook 2003 einschließlich Outlook Web Access (OWA)

Die grundsätzliche Bereitstellung von Diensten und Leistungsparametern eines Nachrichtenverarbeitungssystems unter Exchange Server ist unabhängig von der Clientkomponente mit der ein Nutzer auf Daten und Informationen seines Postfaches zugreifen möchte. Jedoch bietet ausschließlich Outlook 2003 die vollständige Unterstützung aller Feature eines Nachrichtenverarbeitungssystems unter Exchange Server.
Bestandteil dieser Anlage ist die ITDZ Workshop Schulungsunterlage (130 Seiten) zu Microsoft Outlook 2003 mit Stand vom 13. April 2007.

Outlook Web Access (OWA)

Outlook Web Access bietet jedem Nutzer unter Einsatz eines handelsüblichen aktuellen Webbrowser die Möglichkeit sowohl, aus dem Internet als auch aus dem Intranet, auf Nachrichten und Daten im eigenen Postfach zugreifen zu können. Outlook Web Access ist eine Exchange Server Komponente die keine Konfiguration auf Clientgeräten erfordert jedoch für den Nutzer den Funktionsumfang des Clientkomponente Outlook vollständig in einem Webbrowser abbildet.



Die Exchange Server Komponente OWA wird über den virtuellen HTTP-Server des jeweiligen Exchange Server bereitgestellt. Der Standardsicherheit wird über explizite SSL-Konfiguration (HTTPS) auf der Webseite der OWA-Komponente definiert.
Als Standard-URL für den Zugriff auf Postfachinformationen eines Nutzers wird für den Webbrowser die Adresse: https://<exchangeservername>/exchange benutzt.
Umfang und weitere Verfahrensweisen im Umgang mit Outlook Web Access sind der beigefügten Schulungsunterlage unter Pkt. 1.4 zu entnehmen.

Bereitstellung Terminkalender und To-Do-Listen

Basis für die Nutzung der Exchange Server Komponenten für eine verwaltungs-übergreifenden Zusammenarbeit ist die Bereitstellung von Ordnerstrukturen in den Informationsspeichern der einzelnen Exchange Servern der Exchange Organisation. Die Inhalte (Termine, Aufgaben) dieser Ordner werden durch regelmäßige automatische Replikation der einzelnen Exchange Informationsspeicher untereinander auf alle

Informationsspeicher der Exchange Server in der gesamten Exchange Organisation verteilt und stehen somit jedem Postfachnutzer im Active Directory zur Verfügung. Die Replikation der Ordnerinhalte ermöglicht somit ein Erstellen, Ändern und Aktualisieren der Informationen je nach Bearbeitungsstand.

Weiterführende Informationen und Erläuterungen zum Umfang und zur Nutzung dieser Komponenten sind in der beigefügten Schulungsunterlage unter Pkt. 5 Kalender/Termine und Pkt. 6 To-Do-Listen (Aufgaben) zu entnehmen.

Anlage A7.1.3. : Unified Messaging Service und Exchange Server 2003

Unified Messaging Service (UMS) ist ein optionaler Dienst, der über den normalen Funktionsumfang eines Nachrichtenverarbeitungssystem hinausgeht. Hierbei werden Dienstübergänge (Gataway's) definiert, die eine Kommunikation von normalerweise nicht kompatiblen Diensten untereinander ermöglichen. Hierzu gehört vorrangig das Versenden und Empfangen von FAX-, SMS-, VOICE- Nachrichten per E-Mail.
Die UMS- Kommunikationsplattform nutzt, wie das Nachrichtenverarbeitungssystem, das vorhandene Active Directory und stellt darüber hinaus definierte Gateway Funktionalitäten bereit, die eine Umwandlung eingehender FAX-Nachrichten in Bild- oder PDF-Dateien und eingehende Sprachnachrichten in Sounddateien sicherstellt. Die so konvertierten ursprünglich inkompatiblen Daten können nun als Anhang einer Nachricht an den Empfänger zugestellt werden.

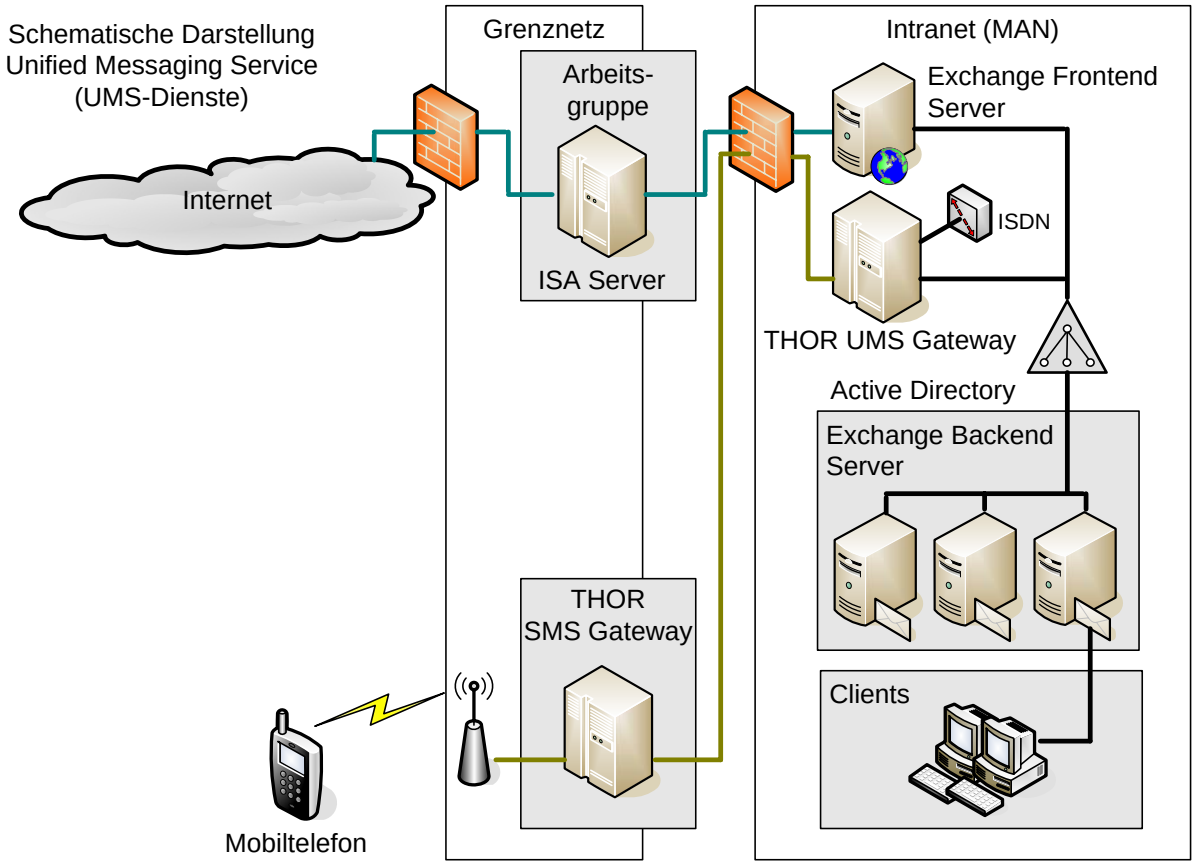


Abb. 1 Nachrichtenverarbeitungssystem und UMS-Integration

Vorteil für Nutzer dieser Lösung ist, dass kein Pflege- oder Administrationsaufwand an lokal vorgehaltenen Faxgeräten oder Sprachboxen anfällt, sowie eine Neubeschaffung lokaler Faxgeräte bzw. Telefonanschlüsse grundsätzlich entfällt. Der Nutzer ist unter anderem auch für derartige Nachrichten ständig, auch mobil, erreichbar. Selbst Wege von und zum Faxgerät entfallen.
Die Administration der UMS-Kommunikationsplattform erfolgt zentral durch administratives Personal des ITDZ.

Weiterführende Informationen zum Umgang mit der UMS-Lösung sind der beigefügten Schulungsunterlage „Microsoft Outlook 2003“ unter Pkt. 4 UMS-Funktionen zu entnehmen.

Anlage A7.1.4. : Struktur der öffentlichen Ordner

Öffentliche Ordner unter Exchange sind eine einfache und wirkungsvolle Weise, Informationen zu sammeln, zu organisieren und zu teilen. Die öffentliche Ordnerstruktur umfasst einen definierten Speicherbereich auf einem Exchange Server, auf den mehrere Nutzer parallel zugreifen können. Nutzer mit expliziten Zugriffsberechtigungen können Ordner und deren Inhalte verwalten, erstellen, ansehen und auch ändern. Zudem können öffentliche Ordner und deren Inhalte, über weitere Exchange Server innerhalb der Exchange Organisation repliziert und so an den jeweiligen anderen Exchange Server Standorten bereit gestellt werden, ohne die Netzwerkverbindungen durch permanenten Datenverkehr (z.B. durch Datei öffnen über Netzlaufwerkfreigaben) unnötig zu belasten.

Die Bereitstellung einer Struktur von öffentlichen Ordnern in der Exchange Organisation macht erst Sinn, wenn die damit verbundenen Möglichkeiten innerhalb von Exchange genutzt werden und damit wesentliche Vorteile gegenüber dem normalen NTFS-Dateisystem freigegeben werden können.

Die Struktur der öffentlichen Ordner gliedert sich in öffentliche und systemeigene Ordner.

1. Öffentliche Ordner
Öffentliche Ordner sind für Benutzer sichtbar und können als Kalender, Kontakt, Aufgabenblatt und Dokumentenablage dargestellt werden. Die Struktur der Öffentlichen Ordner wird über MAPI-Zugriffsrechte (Messaging Application Program Interface) und nicht über NTFS-Rechtevergabe (Dateisystem) verwaltet und dargestellt.

2. Systemordner
Systemordner sind versteckte Ordner für die interne Systemmanagementkommunikation. Die Exchange Server verwenden beispielsweise Teile dieser Ordner zu Bereitstellung der Öfflineadressbücher und Frei- & Gebucht Information.

Die gesamte Struktur der öffentlichen Ordner in der bestehenden Exchange Organisation ist genau einer administrativen Gruppe (LIT-Zentrale) zugeordnet. Innerhalb dieser administrativen Gruppe, kann die Ordner Struktur angezeigt und auf der obersten Ebene der Struktur zentral administriert werden. Eine delegierte Objektverwaltung nach Erstellung von Top-Level Foldern (Ordner der obersten Hierachie) ist hierbei durchgesetzt. Somit können die tatsächlichen Besitzer der jeweiligen Ordner administrativ, ab dieser Ebene tätig werden und weitere Unterordner angelegen und die ihnen zugewiesene Teilstruktur vollständig verwalten. Die bestehende Zentralisierung der Ordnerstruktur auf eine administrative Gruppe hat ursächliche Begründung in der Tatsache, dass die gesamte Ordnerstruktur ausschließlich für den Zugriff durch einen Client konfiguriert ist, der das MAPI-Zugriffsprotokoll unterstützt. Der typische MAPI-Client hierfür ist Microsoft Outlook. Outlook kann jedoch nur für den Zugriff auf eine MAPI-Ordnerstruktur konfiguriert werden. Wenn es auch möglich ist, in der Exchange Organisation mehrere Ordnerstrukturen in unterschiedlichen administrativen Gruppen anzulegen, so kann der MAPI-Client (Outlook) ausschließlich nur auf eine dieser Ordnerstrukturen zugreifen. Insofern ist eine verwaltungsübergreifende Arbeit innerhalb der öffentlichen Ordnerstrukturen nicht mehr sichergestellt, dieses Verfahren wird daher grundsätzlich zum heutigen Zeitpunkt ausgeschlossen.

Zugriff auf einzelne Ordner innerhalb der Hierachie wird durch Replikation von Ordnern und deren Inhalten sichergestellt. Ausgangspunkt der Bereitstellung von öffentlichen Ordnern ist hierbei grundsätzlich immer das Vorhandensein eines Informationsspeichers für öffentliche Ordner auf dem jeweiligen Exchange Server. Bei der Erstinstallation eines Exchange Server wird dieser Informationsspeicher für öffentliche Ordner automatisch mit der Installationsroutine angelegt. Ein neuer Exchange Server innerhalb der Exchange Organisation erhält durch die Verzeichnisdienstreplikation die Basis Informationen über die administrative Gruppe in welcher sich die zentrale Ordnerstruktur befindet und auf

welchen weiteren Exchange Servern ebenfalls ein Informationsspeicher für öffentliche Ordner vorhanden ist. Sämtliche Informationen die öffentliche Ordnerstruktur betreffend, werden nach erfolgreicher Verzeichnisdienstreplikation zwischen den Exchange Servern zukünftig ausschließlich per Mail ausgetauscht. Hierbei ist es erst einmal unerheblich, ob Postfachbesitzer eines bestimmten Exchange Server unmittelbaren Zugriff auf Teilstrukturen in der Hierachie haben oder nicht. Grundsätzlich sind zu diesem Zeitpunkt der Bereitstellung einer öffentlichen Ordnerstruktur alle Elemente dieser Struktur mailaktiviert, dies bedeutet sowohl die Serversysteme selbst, als auch jeder mailaktivierte Nutzer können Mail-Nachrichten an Elemente dieser Ordnerstruktur erfolgreich senden.

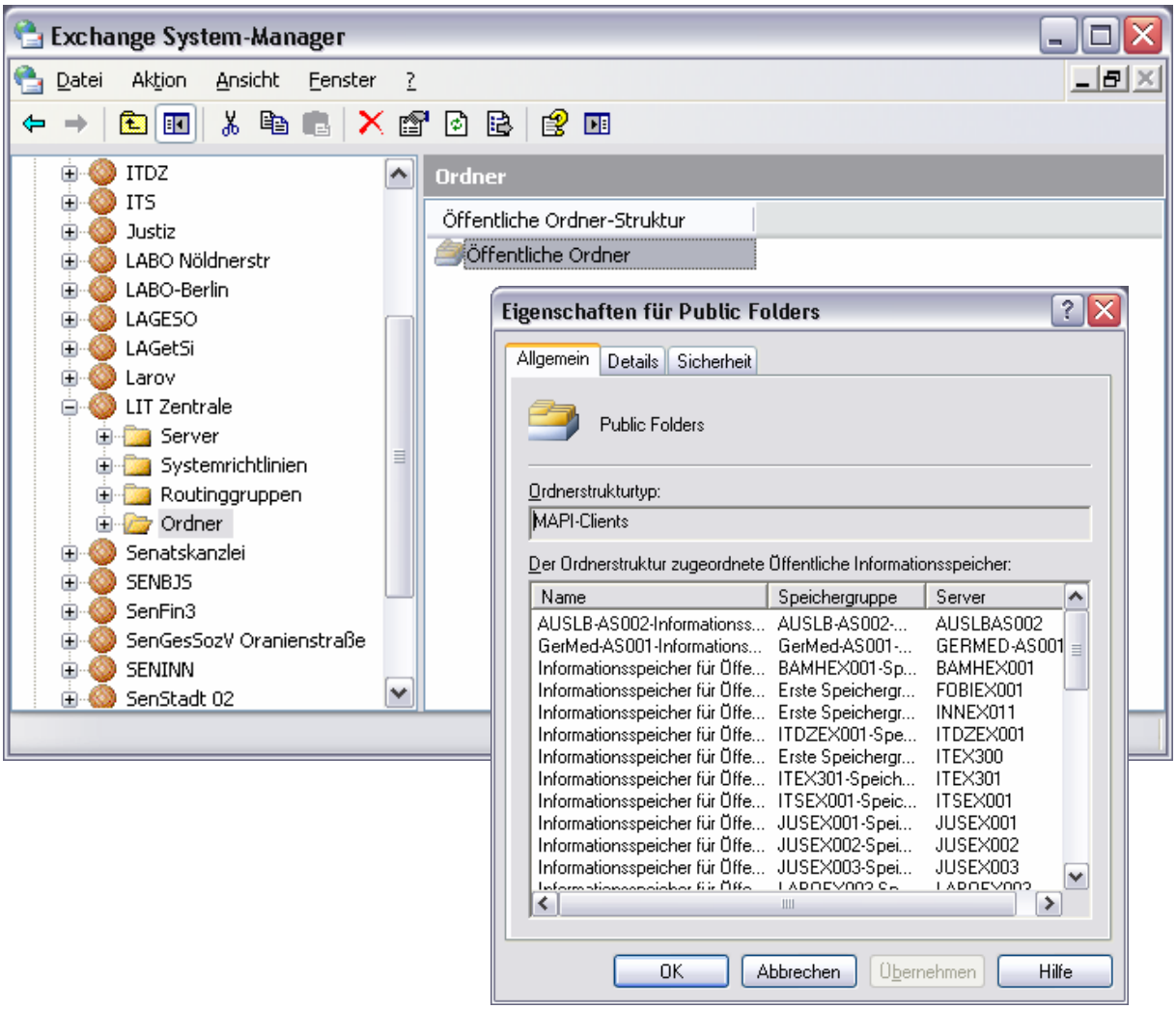


Abb. 1 Ordnerstruktur, Strukturtyp und zugeordnete Öffentliche Informationsspeicher

Die Exchange Server untereinander nutzen den Nachrichtenaustausch ausschließlich zur Aktualisierung der gesamten Ordnerstruktur (hinzugefügte, veränderte oder gelöschte Elemente), dies ist erforderlich damit mailaktivierte Nutzer immer eine aktuelle Struktur beim Outlook-Start vorfinden.

Verwaltungsübergreifende Zusammenarbeit

Auf der Ebene der Top-Level Folder Struktur kann ein einzelner neuer öffentlicher Ordner oder eine neue Ordnerteilstruktur nur durch Administratoren der administrativen Gruppe angelegt werden, in der die gesamte Ordnerstruktur angesiedelt ist. Für alle anderen mailaktivierten Nutzer ist der Zugriff auf die Top Level Folder Struktur verweigert. Die Sicherstellung einer derartigen Rechteverweigerung erfolgt durch Gruppenmitgliedschaft

der jeweiligen mailaktivierten Nutzer. Hierbei wird der Gruppe und damit jedem Mitglied innerhalb dieser Gruppe, das Recht zum Erstellen von Top-Level Foldern verweigert. Erst die MAPI-Rechtevergabe auf die bereits erstellten Ordner einer Teistruktur, ermöglichen eine Delegierung der administrativen Zuständigkeit.

Verfahrensschritte

- Das Anlegen einer neuen Teilstruktur innerhalb der bestehenden Ordnerstruktur erfolgt durch Beauftragung des jeweiligen Kunden gegenüber dem ITDZ
- Einrichten der Teilstruktur auf der Ebene Top-Level Folder,
- Delegierung der administrativen Verwaltung für diesen Top-Level Folder an den Auftraggeber durch MAPI-Rechtevergabe,
- Top-Level Folder unterliegen einer einheitlichen Namenskonvention innerhalb der Exchange-Organisation um die Eindeutigkeit der Teilstruktur sicherzustellen.
- Einrichten der Replikation der Inhalte der neuen Teilstruktur an den Exchange-Server des jeweiligen Auftraggeber,

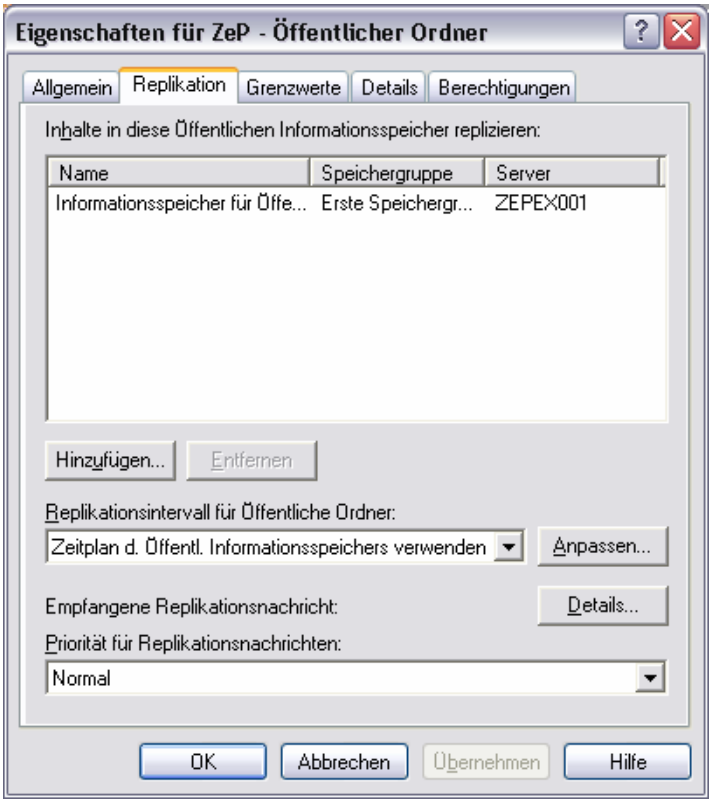


Abb. 2 Beispielhaft Inhaltliche Replikation von Ordnerstrukturen (Top-Level)

- Mit der inhaltlichen Replikation wird sichergestellt, dass alle Elemente dieser Teilstruktur auf dem jeweiligen Exchange-Server des Auftraggebers verfügbar und administrierbar sind.
- Mit dem Einrichten und Replizieren der neuen administrativen MAPI-Zugriffsrechte auf die jeweilige Teilstruktur, kann der Administrator einer Teilstruktur über den Outlook-Client auf die Teilstruktur zugreifen und weitere Konfigurationen für mailaktivierte Nutzer vornehmen.
- Nach Abschluss der Konfiguration der Teilstruktur können alle mailaktivierten Nutzer der Exchange Organisation über das globale Adressbuch an die einzelnen Elemente der Teilstruktur eine Mail-Nachricht senden.
- Einsehen und Ändern der Inhalte der einzelnen Elemente der jeweiligen Teilstruktur obliegt ausschließlich den mailaktivierten Nutzern die entsprechende MAPI-Zugriffsrechte erhalten haben.

Bereitstellen einer Teilstruktur in mehreren administrativen Gruppen

- Besteht die Notwendigkeit eine Teilstruktur der öffentlichen Ordner auf Exchange-Server unterschiedlicher administrativer Gruppen bereitzustellen, so muss dafür folgende Voraussetzung gegeben sein:
  - In der jeweiligen administrativen Gruppe existiert mindestens 1 Exchange-Server mit einem Informationsspeicher für öffentliche Ordner,
  - Einrichtung der Teilstruktur ist auf Ebene Top-Level Folder abgeschlossen,
  - Replikationsziele der Teilstruktur auf unterschiedlichen Exchange-Servern eingerichtet,

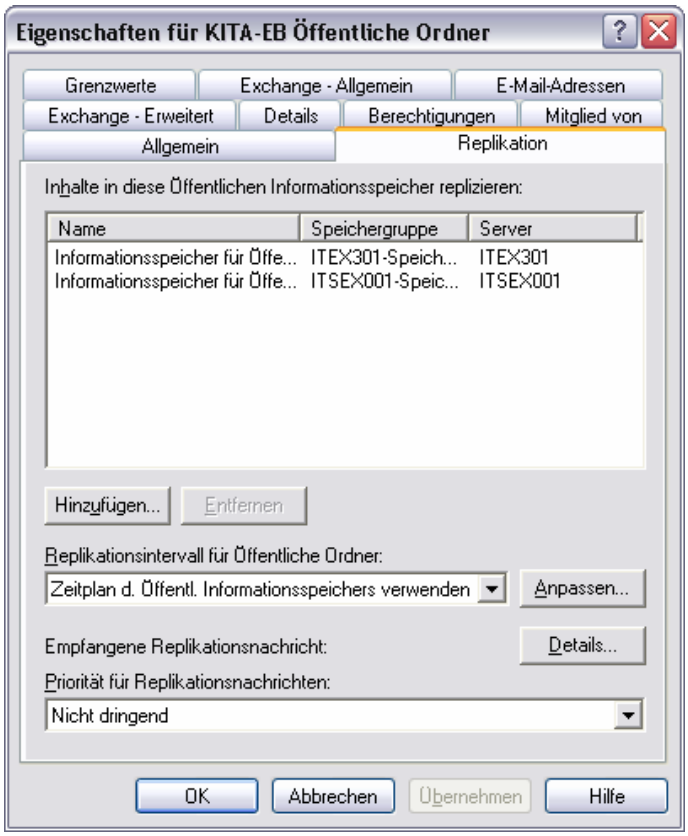


Abb. 4. Beispielhafte Darstellung der übergreifenden Zusammenarbeit

  - Die Notwendigkeit der Bereitstellung von Teilstrukturen ergibt sich aus den Erfordernissen der Zusammenarbeit von Bereichen unterschiedlicher Verwaltungsstrukturen und ist nicht durch das ITDZ beeinflussbar,
- Mit dieser Verfahrensweise ist es möglich Teile der Ordnerstruktur mailaktivierten Nutzern anderer administrativer Gruppen über den Outlook–Client bereitzustellen,
- Dies ist nicht die Bereitstellung von verwaltungsübergreifender Terminplanung und der Darstellung von Frei- / Gebucht Informationen,

Bereitstellen von Systemordnern für die übergreifende Zusammenarbeit

- Systemordner sind Bestandteil der Struktur der Öffentlichen Ordner, deren Verfügbarkeit ist ebenso abhängig von der Bereitstellung (Replikation) auf Exchange-Servern wie die der Öffentlichen Ordner Teilstrukturen,
- Im Gegensatz zur Struktur der Öffentlichen Ordner jedoch, wirkt die Bereitstellung der Systemordner vorrangig auf die Postfächer der Nutzer und nur mittelbar auf die über das Postfach verfügbare Öffentliche Ordner Struktur,
- Für die Bereitstellung der Frei- / Gebucht Information im Outlook-Kalender der jeweiligen Nutzer ist die Bereitstellung von Teilstrukturen des Systemordner SCHEDULE+FREE BUSY erforderlich,

- Für die Bereitstellung von Offline Adressbuch Informationen ist es erforderlich Teilstrukturen des Systemordner OFFLINE ADRESSBOOK zu replizieren,
- Auf Exchange-Servern auf denen Replikate dieser beiden Systemordner bereitgestellt wurden sind folgende zusätzliche Feature nutzbar:
    - OFFLINE ADDRESS BOOK:
        - Nutzer auf den jeweiligen Exchange-Servern können ein Offline Adressbuch herunterladen deren Umfang immer die Nutzer der eigenen administrativen Gruppe als auch die Nutzer derjenigen administrativen Gruppe beinhaltet deren Systemordner Teilstruktur als Replikat auf dem Exchange Server vorhanden ist.
    - SCHEDULE+FREE BUSY:
        - Nutzer auf den jeweiligen Exchange-Servern können die Terminplanung (Kalender) Funktionalität, sowie Frei-/Gebucht Information für alle Nutzer in ihrer administrativen Gruppe standardmäßig, sowie für Nutzer derjenigen administrativen Gruppe einsehen, deren Systemordner Teilstruktur als Replikat auf dem Exchange Server vorhanden ist.

Die Anlage von Replikaten auf Exchange-Servern in unterschiedlichen administrativen Gruppen ist für eine verwaltungsübergreifende Zusammenarbeit aufgrund der dezentralen Administration der gesamten Exchange-Organisation zwingend erforderlich. Die Replikation von Teilstrukturen (Öffentliche Ordner und Systemordner) wird zukünftig auch im Zuge von Verwaltungsumstrukturierungen nicht ausbleiben und unterliegt keinesfalls dem Entscheidungswillen des ITDZ, sondern ist vorrangig Kundenbezogen.

Anlage A7.1.5. : Virenschutz- und Spamfiltermechanismen

Das Nachrichtenverarbeitungssystem entwickelt sich immer weiter zu einem wichtigen und kritischen Dienst sowohl innerhalb des Active Directory Verbundes, als auch für die Kommunikation mit dem Internet. Es ist daher von entscheidender Bedeutung, dass sowohl Verfügbarkeit als auch Funktionalität des Nachrichtenverarbeitungssystems stabil und zuverlässig gegeben sind.
Unberechtigte Zugriffe durch Viren, Würmer oder eines Denial-of-Service-Angriffs (Anlage B1.1) stellen einen Bereich der Risiken dar, die beim alltäglichen Betrieb des Nachrichtenverarbeitungssystem auftreten können. Auch unerwünschte kommerzielle E-Mail-Nachrichten (SPAM) stellen aufgrund ihrer Menge und Komplexität eine Bedrohung für das Nachrichtenverarbeitungssystem dar.

Absichern der Clientumgebung
Das zum Einsatz kommende Nachrichtenverarbeitungssystem ist eine verteilte Client-/Serveranwendung, insofern muss bei der Umsetzung der geplanten Sicherheitsmechanismen für das gesamte Nachrichtenverarbeitungssystem auch die Clientumgebung berücksichtigt werden.
Folgende Aspekte sind hier zu betrachten:

- Nachrichtenverarbeitungsprotokolle die von Clients benutzt werden, wie z.B. POP3 oder IMAP4 sind aufgrund ihrer Sicherheitsrisiken per Default in der Exchange Organisation nicht aktiviert,
- Der Einsatz aktueller und gepatchter Clientkomponenten, sowie die regelmäßige Durchführung von Sicherheitsupdates für die Clientkomponenten obliegt dem Kunden,
- Benutzerinformation über Verfahrenswege und Nutzeraktionen beim Auftreten von E-Mail-Viren, Virenfalschmeldungen, Kettenbriefen und SPAM.

Maßnahmen gegen Viren
Viren die über E-Mail-Nachrichten übertragen werden, stellen eine der größten Bedrohungen für das Nachrichtenübermittlungssystem dar. Die wirksamste Methode im Kampf gegen Viren besteht in der Installation von Antivirensoftware. Wobei das jeweilige Signaturenupdate permanent auf einem aktuellen Stand zu halten ist.
Durch die Installation und Aktivierung von Antivirensoftwarekomponenten auf jeder Zwischenstation in der Nachrichtübertragungskette wird somit optimaler Schutz für jede Nachricht gewährleistet. Die beteiligten Komponenten der Übertragungskette erfüllen unterschiedliche Aufgaben, insofern verwendet das Antivirenmodul auf dem zentralen SMTP-Gateway-Server einen anderen MIME-Parser (Multipurpose Internet Mail Extensions) als, das auf einem Exchange Server installierte Modul. Der Exchange Server Parser unterscheidet sich wiederum von dem Parser den Outlook 2003 oder Outlook Web Access verwendet. Die Wahrscheinlichkeit des Erkennens und des Abfangens von E-Mail-Viren, wird neben dem Einsatz unterschiedlicher Parser in Nachrichtenübertragungskette noch dadurch erhöht, dass Antivirensoftwarekomponenten unterschiedlicher Hersteller zum Einsatz kommen.

Features zum Blockieren von Anlagen in Outlook und Outlook Web Access
Viren werden häufig in Form eines Dateianhanges weitergeleitet. Dies erfolgt auf offensichtliche Weise durch das Anhängen einer ausführbaren Datei (.EXE,.COM,.BAT,.VBS) an eine E-Mail-Nachricht, bzw. durch Einbettung von Viren in Makros. Um sich gegen derartige Viren zu schützen, stellt sowohl Outlook ab Version 2002 als auch Outlook Web Access ein Feature zum Blockieren von Anlagen zur Verfügung.
Bei beiden Clientkomponenten ist das Feature zum Blockieren von Anhängen nach Dateityp und MIME-Typ standardmäßig aktiviert. Mit dieser Konfiguration können Nutzer jeden Anhangtyp versenden, jedoch keine gefährlichen Anhänge der oben genannten Typen empfangen. Outlook Web Access ermöglicht es jedoch, im Gegensatz zu Outlook derartige Anhänge auf Datenträger zu speichern und dann separat zu öffnen.

Schutz gegen unerwünschte kommerzielle E-Mail-Nachrichten (SPAM)
SPAM verursacht auf verschiedene Arten Kosten, z.B. Zeitaufwand für den Nutzer zum Sortieren und Löschen, bis hin zur Reduzierung verfügbarer Bandbreiten und unnötig belegtem Speicherplatz auf Mailsystemen.
Folgende Aspekte sind hier zu betrachten:

- Unterweisung der Nutzer im Umgang mit SPAM,
- Einführung der in Outlook und Outlook Web Access vorhandenen Feature gegen SPAM,
- Erklärung der SCL-Infrastruktur (Spam Confidence Level),
- Einsatz von Filtertypen im Nachrichtenverarbeitungssystem

Unterweisung der Nutzer im Umgang mit SPAM
Tatsächlich stellen die Nutzer den wichtigsten Baustein beim Schutz vor SPAM dar. Das Verhalten der Nutzer beim Auftreten von SPAM ist maßgeblich ausschlaggebend für eine Weiterverbreitung oder Eindämmung der SPAM-Flut.

Feature in Outlook und Outlook Web Access gegen SPAM
Beide Clientkomponenten verfügen über Feature zum Schutz der Nutzer vor SPAM. Da die Aktivierung der Feature und deren Einstellungen im Postfach des jeweiligen Nutzer abgespeichert werden, gelten die aktivierten Einstellungen für beide Clientkomponenten, egal über welche der beiden Komponenten sich ein Nutzer an seinem Postfach anmeldet.

- Benutzerverwaltete Listen für gesperrte und sichere Absender,
- Blockierungsregeln für externe Inhalte,
- Regelbasierte Verwaltung von Junk-Mails,
- Definieren eines Junk-Mail Filter,

SCL-Infrastruktur (SPAM Confidence Level)
Exchange Server 2003 und die Clientkomponente Outlook 2003 stellen gemeinsam eine Infrastruktur bereit, die eine umfassende Lösung für die Bekämpfung von SPAM unterstützt. Systemeigene Funktionalitäten, sowohl auf der Server- als auch auf der Clientseite, ermöglichen Softwareherstellern mittels PlugIn's, SPAM-Erkennungsfilter in die Nachrichtenübertragungskette zu integrieren. SPAM-Filter werten Nachrichten aus, und legen fest mit welcher Wahrscheinlichkeit es sich bei einer bestimmten Nachricht um SPAM handelt. Hierzu wird der entsprechenden Nachricht eine Zahl zwischen 0 und 9, bei der es sich um die SCL handelt, zugewiesen. Der zugewiesene SCL-Wert zu einer Nachricht, gibt auf Grundlage der Merkmale einer Nachricht (wie z.B. Kopfzeile, Inhalt usw.) die Wahrscheinlichkeit an, mit der es sich bei dieser Nachricht um SPAM handelt. Eine Nachrichteneinstufung mit dem SCL-Wert 0 gibt an, dass es sich mit höchster Wahrscheinlichkeit nicht um SPAM handelt, während eine SCL-Wertung von 9 darauf hin weist, dass mit sehr hoher Wahrscheinlichkeit eine SPAM-Nachricht vorliegt.
In der Exchange Organisation wird die Nutzung der SCL-Wertung konfiguriert (Siehe Intelligenter Nachrichtenfilter (IMF) Anlage B1.1). Diese Konfiguration legt fest welche Nachrichten an die einzelnen Exchange Postfachserver in der Organisation weitergeleitet werden. Administratoren einzelner Exchange Postfachserver können dann entscheiden, ob eingehende Nachrichten mit einer entsprechend hohen SCL-Bewertung entweder direkt in den Ordner Junk-Mail des Postfachbesitzer übertragen werden, oder wie alle anderen Nachrichten mit geringerer SCL-Wertung in den Posteingang des jeweiligen Nutzers übertragen werden. Über eine zu definierende Richtlinie ist es dem Postfachadministrator auch möglich den Aufbewahrungszeitraum von Nachrichten im Junk-Mail-Ordner des Nutzers systemseitig zu definieren.
Die SCL-Infrastruktur berücksichtigt auch Sicherheits-, Blockier- und Empfangslisten des Benutzers sowie die Exchange Server Filterlisten.

Anlage A7.1.6. : Verwalten der globalen Adressliste (GAL)

Informationen zu Adresslisten

Eine *Adressliste* ist eine Sammlung von Empfänger- und anderen mailaktivierten Active Directory-Verzeichnisdienstobjekten. Jede Adressliste kann einen oder mehrere Objekttypen beinhalten (z. B. Benutzer, Kontakte, Gruppen, Öffentliche Ordner, Konferenz- und andere Ressourcen). Adresslisten können zum Organisieren von Empfängern und Ressourcen verwendet und auf diese Weise das Auffinden gewünschter Empfänger und Ressourcen vereinfachen. Adresslisten werden dynamisch aktualisiert. Beim Hinzufügen neuer Benutzer zur Exchange Organisation werden diese daher automatisch allen entsprechenden Adresslisten hinzugefügt.

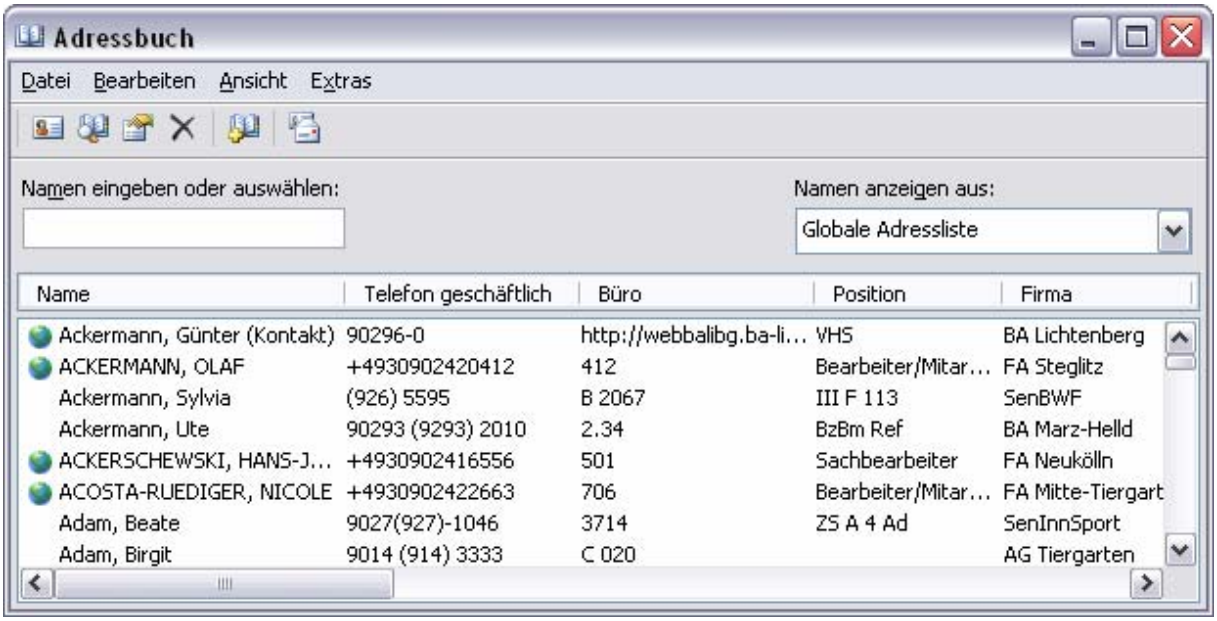


Abb. 1 Ansicht der GAL vom Outlook-Client

Adresslisten werden in Active Directory gespeichert. Daher wird für Benutzer mobiler Geräte, die die Verbindung mit dem Netzwerk beenden, auch die Verbindung mit diesen Adresslisten beendet. Sie können jedoch Offlineadressbücher für Benutzer erstellen, die vom Netzwerk getrennt sind. Diese OABs können auf die Festplatte des Benutzers herunter geladen werden. Um Ressourcen zu sparen, handelt es sich bei den OABs häufig um eine Teilmenge der Informationen in den tatsächlichen Adresslisten, die auf den Servern gespeichert sind.

Informationen zur globalen Adressliste (GAL)

Eine globale Adressliste (GAL) ist daher ein Verzeichnis, das Einträge für alle Gruppen, Benutzer und Kontakte der Exchange-Organisation enthält. Die GAL wird im Adressbuch der Clientkomponente auf dem Clientcomputer angezeigt. Als Untermenge zur GAL können wie oben beschrieben weitere Adresslisten definiert und im Adressbuch strukturiert angezeigt werden. Die globale Adressliste wird automatisch durch den Exchange Dienst „Microsoft Systemaufsicht“ gebildet. Hierfür ist es erforderlich das der Empfängeraktualisierungsdienst der Exchange Organisation Mail-Adressen nach LDAP-Abfragekriterien generiert, in deren Ergebnis die Systemaufsicht mailaktivierte Objekte automatisch in die globale bzw. in die jeweils zutreffende Adressliste einfügt. Das Ergebnis dieser Aktualisierung, kann nur über das Adressbuch der Clientkomponente geprüft werden.
Standardmäßig wird in der Exchange Organisation jedes mailaktivierte Objekt mindestens der GAL hinzugefügt. Administratoren ist es möglich über das SnapIn „Active

Directory Benutzer und Computer“ einzelne mailaktivierte Objekte von der Ansicht in den Adresslisten auszublenden.

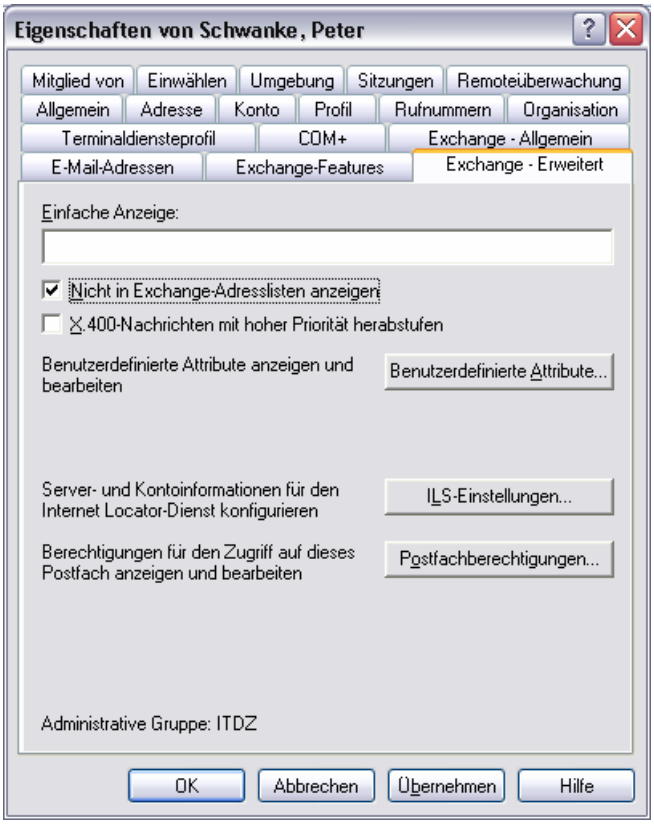


Abb. 2 Option zum Verhindern der Anzeige in den Adresslisten

Das Ausblenden von mailaktivierten Objekten aus den Exchange-Adresslisten allein, verhindert nicht das Zustellen bzw. Versenden von Mailnachrichten. Ausschließlich das Auffinden des jeweiligen mailaktivierten Objektes wird erschwert. Das Zustellen von Nachrichten kann nach wie vor über die Adresseingabe von Hand im Mail-Client sichergestellt werden, eine Auswahl aus den jeweiligen Adresslisten jedoch ist nicht mehr möglich. Das Vorhandensein einer vollständigen GAL ist Basisfunktionalität des Nachrichtenverarbeitungssystems.

Ändern und Aktualisieren der GAL

Die GAL ist eine dynamische Liste, die einer ständigen und permanenten Änderung unterliegt. Die Dynamik ist designbedingt systemgesteuert und daher unabhängig vom administrativen Eingriff. Änderungen und Aktualisierungen können auch von Hand angestoßen werden (z.B. durch Empfängeraktualisierungsdienst jetzt ausführen) haben aber nur temporär eine Bedeutung, da in regelmäßigen Zeitabständen (alle 2h) der jeweilige Empfängeraktualisierungsdienst den Automatismus startet.

Anlage A7.2
Herstellerdokumentation

Microsoft Windows Server System

Planen eines Exchange Server 2003-Messagingsystems

Gültig bis:	1. September 2004
Produktversion:	Exchange Server 2003 Service Pack 1
Überprüft von:	Exchange-Produktentwicklung
Neueste Informationen:	www.microsoft.com/exchange/library
Autor:	Michele Martin

Planen eines Exchange Server 2003-Messagingsystems

Michele Martin

Veröffentlicht: August 2003
Aktualisiert: Mai 2004
Für folgendes Produkt: Exchange Server 2003 Service Pack 1

Copyright

Danksagung

Projektredakteur: Brendon Bennett

Mitwirkende Verfasser: Jon Hoerlein, Joey Masterson, Teresa Appelgate, Patricia Anderson, Christopher Budd, Bill Ashcraft

Mitwirkende Redakteure: Janet Lowen (Linda Werner & Assoc), Alison Hirsch.

Technische Bearbeitung: Nino Bilic, Ladislau Conceicao, Aidan Delaney, Evan Dodds, Per Farny, Brad Owen, Scott Roberts, Exchange Product Team

Grafisches Design: Kristie Smith

Produktion: Sean Pohtilla, Joe Orzech

Inhaltsverzeichnis

Einführung

Messagingsysteme gehören heutzutage in immer mehr Unternehmen zu den betriebswichtigen Systemen. Daher werden strenge Anforderungen an die Zuverlässigkeit und Verfügbarkeit von E-Mail-Systemen gestellt. Ebenso wichtig ist der erhöhte Bedarf an neuen Funktionen in Messagingsystemen. Die Anforderungen der Benutzer entwickeln sich angesichts weltweit verteilter Unternehmen und mobil tätiger Mitarbeiter ständig weiter. All diese Faktoren stellen eine hohe Herausforderung für IT-Manager und Systemarchitekten dar, die absolut zuverlässige und ständig verfügbare Messagingsysteme entwickeln müssen, die den Ansprüchen der Benutzer genügen.

Für das Entwickeln eines erfolgreichen Microsoft® Exchange Server 2003-Messagingsystems müssen Sie die Möglichkeiten und Grenzen der Hard- und Software kennen, mit der Sie das Messagingsystem entwerfen. Unabhängig davon, ob Sie ein neues Exchange Server 2003-Messagingsystem entwickeln oder eine Aktualisierung einer früheren Exchange-Implementierung durchführen möchten, müssen Sie die Beschränkungen der Netzwerkinfrastruktur mit den Möglichkeiten des Messagingsystems, des Betriebssystems und der Benutzersoftware abstimmen.

Dieses Buch hilft Ihnen dabei, die bestehende Systemumgebung zu bewerten und die technischen Überlegungen zu verstehen, die Einfluss auf die Entwurfsentscheidungen haben. Dabei werden Empfehlungen für den Entwurf eines Exchange 2003-Messagingsystems gegeben. Außerdem werden Verbesserungen in Exchange 2003, Microsoft Windows Server™ 2003 und Microsoft Office Outlook® 2003 beschrieben und Fragen im Zusammenhang mit der Netzwerkinfrastruktur, der Hardware, dem Microsoft Active Directory®-Verzeichnisdienst und der Systemverwaltung erläutert. Darüber hinaus werden in diesem Buch Fragen besprochen, die für die Entwicklung eines absolut zuverlässigen und ständig verfügbaren Messagingsystems relevant sind, beispielsweise im Zusammenhang mit Speichertechnologien, Clustering, Serverabstimmung und Konfiguration von Clientcomputern.

Was wurde in diesem Dokument aktualisiert?

Seit Veröffentlichung der vorherigen Version dieses Dokuments wurden in den folgenden Abschnitten Inhalte hinzugefügt oder geändert:

- **Kapitel 1, „Aspekte beim Entwurf von Exchange 2003-Messagingsystemen“**
  Es wurde ein Hinweis über den vollständigen Download des Offlineadressbuchs hinzugefügt, der durchgeführt wird, wenn Sie den Exchange-Cachemodus verwenden und eine bedeutsame Verzeichnisänderung auftritt.
- **Kapitel 3, „Planen des Bereitstellungspfads“**
  Es wurde eine Referenz auf das Exchange-Profilaktualisierungstool (**Exprofre.exe**) hinzugefügt, mit dem Sie Outlook-Profile nach dem Verschieben von Postfächern zwischen Gesamtstrukturen aktualisieren können.
- **Kapitel 4, „Planen einer Standortkonsolidierung“**
  Ein neues Kapitel, in dem beschrieben wird, wie Sie Exchange von mehreren Remotestandorten zu einem zentralen Standort im gemischten Modus zusammenlegen.
- **Kapitel 6, „Einplanen hoher Verfügbarkeit“**
  Der Abschnitt „Änderungen des Berechtigungsmodells für Clustering“ wurde vertieft und der Abschnitt „IP-Adressen und Netzwerknamen“ wurde aktualisiert.

Welche Informationen bietet dieses Buch?

Dieses Buch enthält detaillierte Antworten auf die folgenden Fragen:

- Welche Faktoren müssen beim Entwerfen oder Aktualisieren eines Exchange 2003-Messagingsystems berücksichtigt werden? (Kapitel 1)
- Wie beeinflussen die neuen Funktionen in Exchange 2003, Windows Server 2003 und Outlook 2003 den Entwurfsprozess? (Kapitel 1)
- Wie kann Exchange in die Active Directory-Infrastruktur integriert werden? (Kapitel 2)
- Welche Empfehlungen werden in Bezug auf die Platzierung von Öffentlichen Ordnern und Frei-/Gebucht-Ordnern gegeben? (Kapitel 2)
- Wie können Exchange-Daten mit Standortkonsolidierungstools von Servern an Remotestandorten auf einen Server an einem zentralen Standort verschoben werden? (Kapitel 4)
- Welche Empfehlungen werden für das Routing und die Serverplatzierung gegeben? Wie kann die Speicherauslastung der Server optimiert werden? (Kapitel 5)
- In welchem Umfang können auf Grundlage der Netzwerkinfrastruktur und der ermittelten Anforderungen die Server zentralisiert werden? Welche Skalierungsmöglichkeiten und Beschränkungen weist Exchange 2003 auf? (Kapitel 5)
- Wie kann die Zuverlässigkeit und Verfügbarkeit des Messagingsystems maximiert werden? (Kapitel 6)

Für wen ist dieses Buch gedacht?

Dieses Buch richtet sich an IT-Experten, die für die Planung und den Entwurf von Exchange-Messagingsystemen in ihrem Unternehmen zuständig sind. Zum Beispiel:

- Systemarchitekten: Mitarbeiter, die für den Entwurf der Serverinfrastruktur sowie die Entwicklung von Strategien und Richtlinien für die Serverbereitstellung zuständig und an der Planung der Netzwerkverbindungen beteiligt sind.
- IT-Manager: Mitarbeiter, die technische Entscheidungen treffen und die darüber hinaus die IT-Mitarbeiter führen, die für die Infrastruktur, die Desktop- und Server-Bereitstellung sowie die standortübergreifende Verwaltung und den Betrieb der Server verantwortlich sind.
- Systemadministratoren: Mitarbeiter, die für das Planen und Bereitstellen von Technologien für Microsoft Windows®-Server und für das Bewerten und Empfehlen neuer IT-Lösungen verantwortlich sind.
- Messagingadministratoren: Mitarbeiter, die für das Implementieren und Verwalten des unternehmensweiten Messagings verantwortlich sind.

Welche Technologien werden in diesem Buch behandelt?

In diesem Buch wird ein allgemeiner Überblick über Technologien für Messagingsysteme und verwandte Gebiete gegeben und dabei auch auf Funktionen und Beschränkungen eingegangen. Weitere Informationen über bestimmte Technologien finden Sie in der Produktdokumentation von Windows, Outlook und Exchange. Dieses Buch enthält u. a. Informationen über folgende Technologien:

- Drahtlose Synchronisierung und Browserzugriff mit mobilen Geräten auf Microsoft Exchange
- Microsoft Office Outlook Web Access 2003
- Microsoft Outlook 2003-Exchange-Cachemodus
- Aufteilung von Active Directory-Gesamtstrukturen und -domänen für Microsoft Windows Server
- Microsoft Windows-Clustering
- Redundant Array of Independent Disks (RAID)
- Remote Procedure Call (RPC) über HTTP (Remoteprozeduraufruf über HTTP)
- Storage Area Networks (SANs)
- Volumeschattenkopie-Dienst

Wie ist dieses Buch aufgebaut?

Dieses Buch ist entsprechend den Schritten aufgebaut, die Sie normalerweise beim Planen eines Messagingsystems befolgen. Zu Beginn werden Richtlinien für das Bewerten der Anforderungen und das Überprüfen der bestehenden Netzwerkinfrastruktur vorgestellt. Anschließend erhalten Sie Informationen, die Sie beim Planen und Entwerfen des Systems unterstützen. Es werden Empfehlungen für die Integration von Exchange mit Active Directory, für das Platzieren der Hardware und für das Integrieren von Technologien gegeben, mit denen die Zuverlässigkeit und Verfügbarkeit maximiert werden können.

Kapitel 1, „Aspekte beim Entwurf von Exchange 2003-Messagingsystemen“
Dieses Kapitel hilft Ihnen dabei, die Unternehmens-, Verwaltungs- und Benutzeranforderungen zu überprüfen und eine technische Beurteilung der Umgebung vorzunehmen, in der Sie Exchange 2003 bereitstellen. Darüber hinaus erhalten Sie einen Überblick über bestimmte Funktionen in Windows Server, Exchange und Outlook, die Einfluss auf Planungs- und Entwurfsentscheidungen haben.

Kapitel 2, „Planen des Active Directory- und Verwaltungsmodells“
Dieses Kapitel hilft Ihnen dabei, Exchange in die Active Directory-Struktur zu integrieren. Außerdem erhalten Sie Informationen dazu, wie Sie das Verwaltungsmodell durch Überprüfen der Rollen in Ihrem Unternehmen entwerfen können.

Kapitel 3, „Planen des Bereitstellungspfads“
In diesem Kapitel werden die verschiedenen Pfade für das Bereitstellen von Exchange 2003 vorgestellt, abhängig davon, ob Sie bereits eine frühere Version von Exchange verwenden. Außerdem werden Bereitstellungspfade empfohlen, die der Situation in Ihrem Unternehmen am besten entsprechen.

Kapitel 4, „Planen einer Standortkonsolidierung“
In diesem Kapitel wird beschrieben, wie Sie Exchange von mehreren Remotestandorten an einem zentralen Standort im gemischten Modus zusammenlegen.

Kapitel 5, „Planen der Exchange-Infrastruktur“
In diesem Kapitel werden die technischen Anforderungen für Ihr Exchange-Messagingsystem bestimmt und die Konzepte erläutert, die beim Planen der Exchange-Infrastruktur von Bedeutung sind, beispielsweise Routing-Entwurf, Serverplatzierung, Servergröße und Serverabstimmung.

Kapitel 6, „Einplanen hoher Verfügbarkeit“
In diesem Kapitel werden Fragen besprochen, die für die Entwicklung eines absolut zuverlässigen und ständig verfügbaren Messagingsystems relevant

sind, beispielsweise im Zusammenhang mit Speichertechnologien, Clustering, Serverabstimmung und Konfiguration von Clientcomputern.

Anhang A, „Prüfliste für das Bewerten der bestehenden Umgebung“
Anhang A enthält eine Prüfliste mit physischen und logischen Faktoren, die Sie bei der Beurteilung der bestehenden Systemumgebung berücksichtigen sollten.

Anhang B, „Optimieren der Speicherauslastung“
Anhang B enthält Informationen über das Überwachen und Optimieren der Speicherauslastung auf den Servern.

Anhang C, „Ressourcen“
Anhang C enthält Verknüpfungen zu Quellen, mit denen Sie Ihr Verständnis des Planungs- und Bereitstellungsvorgangs von Exchange 2003 vertiefen können.

Anhang D „Eingabehilfen für Personen mit Behinderungen“
Anhang D enthält Informationen über Funktionen, Produkten und Diensten, mit denen Windows 2000, Windows Server 2003 und Exchange Server 2003 für Personen mit Behinderungen einfacher einzusetzen sind.

Aspekte beim Entwurf von Exchange 2003-Messagingsystemen

Bevor Sie mit dem Planen eines Microsoft® Exchange Server 2003-Messagingsystems beginnen können, müssen Sie eine Vielzahl von geschäftlichen und technischen Informationen sammeln. Viele Unternehmen haben eigene Methoden für die Systementwicklung etabliert, die Richtlinien für das Entwerfen und Aktualisieren von Systemen enthalten. Bei solchen Methoden werden zu Beginn in der Regel Anforderungen ermittelt und die bestehende Systemumgebung beurteilt. Dieser Ansatz für die Planungsphase ist auch dann empfehlenswert, wenn in Ihrem Unternehmen keine formelle Methode für die Systementwicklung verwendet wird.

Beim Planen eines Exchange Server 2003-Messagingsystems empfiehlt es sich, folgende Schritte einzuhalten:

- Ermitteln Sie zuerst die Geschäfts-, Verwaltungs-, Benutzer- und Sicherheitsanforderungen, und führen Sie eine technische Beurteilung der Umgebung durch, in der das Messagingsystem bereitgestellt werden soll.
- Beurteilen Sie dann die verfügbaren technischen Lösungen, und ermitteln Sie die erforderliche Struktur des neuen Exchange-Messagingsystems.
- Ermitteln Sie abschließend, welche weiteren Schritte erforderlich sind, um auf Grundlage der bestehenden Umgebung das gewünschte System bereitzustellen.

In diesem Kapitel wird vorausgesetzt, dass Sie alle Geschäfts-, Verwaltungs-, Benutzer- und Sicherheitsanforderungen für Ihr Messagingsystem ermittelt haben. Mithilfe der in diesem Kapitel enthaltenen Informationen können Sie die ermittelten Anforderungen bewerten. Zu diesem Zweck wird auf einige Aspekte in diesen Kategorien besonders eingegangen und erläutert, was diese Anforderungen für den Entwurf des Messagingsystems bedeuten. Dieses Kapitel enthält außerdem Empfehlungen für eine technische Beurteilung der bestehenden Umgebung. Abschließend wird ein Überblick über bestimmte Funktionen in Microsoft Windows Server™ 2003, Exchange 2003 und Microsoft Office Outlook® 2003 gegeben, die Einfluss auf Planungs- und Entwurfsentscheidungen haben.

Beurteilen der Anforderungen

Der Entwurf eines Exchange-Messagingsystems wird durch Geschäfts-, Verwaltungs-, Benutzer- und Sicherheitsanforderungen bestimmt. Da in einzelnen Unternehmen verschiedene Methoden zum Erfassen und Dokumentieren der jeweiligen Anforderungen verwendet werden, enthält dieser Abschnitt keine umfassende Liste aller möglichen Anforderungen. Stattdessen werden einige allgemeine Arten von Anforderungen und die damit verbundenen Fragestellungen erläutert, die Einfluss auf Ihre Planung haben können.

Geschäftsanforderungen

Sie müssen vor dem Planen eines Exchange-Messagingsystems u. a. folgende Geschäftsanforderungen ermitteln:

- Verträge über den Umfang von Serviceleistungen (Service Level Agreements, SLAs)
- Kostenbeschränkungen für Netzwerke und Hardware

- Kostenbeschränkungen für Software

Geschäftsanforderungen, insbesondere Kostenbeschränkungen, haben entscheidenden Einfluss darauf, ob es erforderlich ist, weitgehend innerhalb der vorhandenen Infrastruktur zu arbeiten, oder ob es möglich ist, die Netzwerkinfrastruktur, Hardware und Software zu aktualisieren.

Verträge über den Umfang von Serviceleistungen

Anforderungen in Bezug auf Verträge über den Umfang von Serviceleistungen (Service Level Agreements, SLAs) bestimmen, wie Faktoren wie Speicherung, Clustering sowie Sicherung und Wiederherstellung Ihr System beeinflussen. Beim Beurteilen von SLAs müssen Sie die Erwartungen Ihrer Firma bezüglich der Verfügbarkeit und Wiederherstellbarkeit des Systems ermitteln und dabei Faktoren wie die Nachrichtenübermittlungzeit, den Prozentsatz der Serververfügbarkeit, den Speicherbedarf pro Benutzer und die Wiederherstellungsdauer einer Exchange-Datenbank berücksichtigen. Ermitteln Sie die regulären Geschäftszeiten und die Erwartungen in Bezug auf geplante Ausfallzeiten für Systemwartungen. Ermitteln Sie außerdem eine Kostenabschätzung für nicht geplante Systemausfälle, um die erforderliche Fehlertoleranz für das Messagingsystem zu bestimmen.

Exchange 2003 und Windows Server 2003 enthalten neue Funktionen, die Einfluss auf die Systementwicklung im Hinblick auf die Erfüllung von SLAs haben können. Insbesondere der neue Volumeschattenkopie-Dienst kann positive Auswirkungen auf bestehende Beschränkungen von SLAs haben. Da Sicherungsvorgänge lange dauern können, mussten Sie in der Vergangenheit möglicherweise die Anzahl der Benutzer pro Postfachspeicher begrenzen, um SLA-Anforderungen in Bezug auf die Betriebszeit zu erfüllen. Beim Volumeschattenkopie-Dienst erfolgt die Sicherung jedoch über die Schattenkopie, so dass die von den Anwendungen verwendete Datenbank vom Sicherungsvorgang nicht beeinflusst wird. Mit dem Volumeschattenkopie-Dienst können Sie Exchange-Daten (oder beliebige Anwendungsdaten) schnell und mit minimalen Auswirkungen auf die E-Mail-Clients sichern. Auf diese Weise können Sie größere Datenbanken und mehr Benutzer pro Server unterstützen. In Verbindung mit Software und Hardware, die den Volumeschattenkopie-Dienst von Windows Server 2003 unterstützen, können Sie Exchange-Datenbanken beliebiger Größe (von 100 GB bis zu mehreren Terabyte) schnell sichern und wiederherstellen. Außerdem können Sie Cluster einrichten, die an mehreren physischen Standorten vorhanden sind. Durch diese Funktionen wird eine höhere Verfügbarkeit als bisher ermöglicht.

Kostenbeschränkungen für Netzwerke und Hardware

Finanzielle Beschränkungen in Bezug auf Aktualisierungen der bestehenden Netzwerkinfrastruktur und Hardware haben direkten Einfluss auf den Entwurf Ihres Exchange-Messagingsystems. Unter Umständen muss die bestehende Netzwerkinfrastruktur aktualisiert werden, um die Geschäfts- und Benutzeranforderungen zu erfüllen. Wenn hierbei Beschränkungen bestehen, kann es vorteilhaft sein, bestimmte Messagingfunktionen in Exchange 2003 zu verwenden, z. B. RPC über HTTP. Diese Funktion kann dazu beitragen, ie Messagingqualität bei langsamen und unzuverlässigen Netzwerkverbindungen zu verbessern.

Einige Funktionen in Exchange 2003, Windows Server 2003 und Outlook 2003 können dazu beitragen, die Gesamtbetriebskosten durch Konsolidierung oder Zentralisierung der Serverhardware deutlich zu reduzieren. So tritt beispielsweise bei Exchange 2003 eine geringere Speicherfragmentierung auf, so dass bei Exchange 2003-Servern mit schnellen Prozessoren mehr Benutzer pro Server verwaltet werden können. Dies gilt ebenfalls für Windows Server 2003, das über eine verbesserte Speicherverwaltung verfügt, so dass mehr Benutzer pro Server verwaltet werden können, bevor Beschränkungen durch eine zu hohe Speicherfragmentierung auftreten. Obwohl bei einer besseren Speicherverwaltung nicht unbedingt auch die

Prozessorleistung oder Skalierbarkeit deutlich steigt, können in der Regel mehr Benutzer pro Server verwaltet werden.

Weitere Informationen über neue Funktionen finden Sie unter „Informationen über die Versionen von Exchange, Windows und Outlook“ weiter unten in diesem Kapitel.

Kostenbeschränkungen für Software

Ebenso wie bei Aktualisierungen der Netzwerkinfrastruktur und Hardware können finanzielle Beschränkungen in Bezug auf Aktualisierungen von Betriebssystemen, Serveranwendungen und Anwendungen für Clientcomputer direkt den Entwurf Ihres Exchange-Messagingsystems beeinflussen. Wenn Sie beispielsweise Clientcomputer auf Outlook 2003 aktualisieren, kann der Exchange-Cachemodus dazu beitragen, langsame Netzwerkverbindungen oder Verbindungen mit geringer Bandbreite besser auszunutzen.

Verwaltungsanforderungen

Die Verwaltungsanforderungen Ihres Unternehmens haben beträchtliche Auswirkungen auf den Systementwurf, insbesondere wenn Sie die Verwaltungskosten durch einen Wechsel zu einer zentralisierteren Struktur reduzieren möchten.

Unternehmen implementieren in der Regel Verwaltungsmodelle, die sich einer der beiden folgenden Kategorien zuordnen lassen:

- **Zentralisierte Verwaltung** Eine einzelne Gruppe verwaltet das gesamte Exchange-System. Bei diesem Modell wird eine kleine Anzahl von administrativen Gruppen eingerichtet, unabhängig davon, ob ein einzelnes Datenzentrum oder mehrere Zweigstellen vorhanden sind. Alle Verwaltungsaufgaben werden von einer einzelnen IT-Gruppe ausgeführt. Dieses Modell ist typisch für kleine bis mittlere Unternehmen, kann aber auch in größeren Unternehmen zum Einsatz kommen, bei denen die einzelnen Zweigstellen über Netzwerkverbindungen mit hoher Bandbreite verbunden sind.
- **Verteilte Verwaltung** Die Verwaltung des Exchange-Systems ist auf die einzelnen Unternehmensbereiche oder Niederlassungen verteilt. Das betreffende Unternehmen richtet in der Regel mindestens eine administrative Gruppe für jeden Bereich oder jede Niederlassung ein, wobei jede administrative Gruppe wiederum Routinggruppen, Richtlinien, Server, Verzeichnishierarchien mit Öffentlichen Ordnern und andere Objekte umfasst, die zu den einzelnen Niederlassungen gehören. Eine zentrale IT-Gruppe kann für die Verwaltung von Standards und Richtlinien verantwortlich sein, führt jedoch nicht die alltäglichen Aufgaben der Systemadministration durch. Normalerweise kontrolliert jeder Bereich bzw. jede Niederlassung die eigenen Ressourcen und führt die Systemadministration eigenverantwortlich durch.

  Hinweis In Exchange 5.5 werden durch einen Standort sowohl administrative als auch Routinggrenzen definiert. In Exchange 2000 sind Standorte in administrative Gruppen und Routinggruppen unterteilt, um eine höhere Flexibilität zu ermöglichen. In Exchange 2000 und Exchange 2003 bezieht sich eine Routinggruppe auf eine Sammlung von ständig verfügbaren, zuverlässigen Servern, in der Nachrichten direkt von Server zu Server weitergeleitet werden. Eine administrative Gruppe ist eine Sammlung von Benutzern mit Administratorprivilegien, die nicht durch die Grenzen der Routinggruppe beschränkt ist.

Nach dem Ermitteln der Verwaltungsanforderungen in Ihrem Unternehmen können Sie besser beurteilen, ob eine zentralisierte oder verteilte Struktur oder eine Kombination aus beiden die optimale Lösung für Ihr Unternehmen darstellt. Weitere Informationen über die Abhängigkeiten zwischen der Verwaltung von Exchange und dem Active Directory®-Verzeichnisdienst finden Sie im Abschnitt „Informationen zur Bewertung der aktuellen Umgebung“ weiter unten in diesem Kapitel. Weitere

Informationen über das Planen
des Verwaltungsmodells finden Sie in Kapitel 2, „Planen des Active Directory- und Verwaltungsmodells“.

Benutzeranforderungen

Einige Benutzeranforderungen haben Einfluss auf die Planung Ihres Exchange-Messagingsystems, darunter die folgenden:

- **Remotezugriff** In Unternehmen, deren regionale Büros geografisch weit voneinander entfernt und untereinander mit langsamen Netzwerkverbindungen verbunden sind, wird von den Benutzern u. U. eine höhere Leistungsfähigkeit im Offlinebetrieb gewünscht. Wenn Sie diese Anforderung im Zusammenhang mit
  den bestehenden Geschäftsanforderungen und -beschränkungen beurteilen,
  können Sie ermitteln, ob in Ihrer Situation mithilfe von Funktionen wie dem Exchange-Cachemodus in Outlook 2003 eine höhere Leistungsfähigkeit im Offlinebetrieb erreicht werden kann.
- **Webzugriff** Die Benutzer wünschen möglicherweise einen Zugriff auf ihre Exchange-Informationen über das Internet. Das Arbeiten mit Microsoft Office Outlook Web Access 2003 für Remotebenutzer wurde durch eine verbesserte Leistung und verschiedene Änderungen in der Benutzeroberfläche vereinfacht. Möglicherweise müssen jedoch Investitionen für Betriebssystemaktualisierungen eingeplant werden. So können beispielsweise die Leistungssteigerungen durch
  neue Komprimierungsmethoden nur bei Verwendung des Betriebssystems Windows
  Server 2003 vollständig genutzt werden.
- **Mobilzugriff** Die Benutzer möchten möglicherweise über mobile Geräte auf ihre Exchange-Informationen zugreifen, beispielsweise über ein Gerät, das mit Microsoft Pocket PC 2002 Phone Edition betrieben wird.

Weitere Informationen über Verbesserungen in Bezug auf die Leistung und Benutzerfreundlichkeit in Microsoft Windows® und Exchange finden Sie weiter
unten in diesem Kapitel im Abschnitt „Informationen über die Versionen von
Exchange, Windows und Outlook“.

Sicherheit

Sicherheitsanforderungen können beträchtlichen Einfluss auf die zu entwerfende Active Directory-Struktur haben. So kann beispielsweise in Ihrem Unternehmen
die Anforderung bestehen, strenge Sicherheitsgrenzen zwischen den Verzeichnissen
der einzelnen Unternehmensbereiche einzuhalten. In diesem Fall müssen mehrere Gesamtstrukturen eingerichtet werden. Weitere Informationen über die Einrichtung
von mehreren Gesamtstrukturen finden Sie weiter unten in diesem Kapitel im Abschnitt „Active Directory“.

Informationen zur Bewertung der aktuellen Umgebung

Vor dem Entwurf des Exchange-Messagingsystems müssen Sie die physischen und logischen Faktoren der vorhandenen Systemumgebung verstehen. In Bezug auf
die physischen Faktoren hängt der Entwurf vor allem vom Typ und der Integrität der Netzwerkinfrastruktur ab. Diese Faktoren beeinflussen die Bereitstellung von Exchange,
die Platzierung der Server und die zu erwartende Leistung und Benutzerfreundlichkeit.
In Bezug auf die logischen Faktoren ist für den reibungslosen Betrieb von Exchange 2003 vor allem der Active Directory-Verzeichnisdienst von Bedeutung. Die Active Directory-Umgebung sollte also sehr zuverlässig

sein. Daher wird ausdrücklich empfohlen, beim Entwurf der Active Directory-Struktur die speziellen Anforderungen in Bezug auf Exchange zu berücksichtigen.

> **Wichtig** Vor dem Bereitstellen von Exchange 2003 muss bereits eine Active Directory-Infrastruktur vorhanden sein. Berücksichtigen Sie beim
> Planen der Active Directory-Umgebung die Anforderungen bezüglich Exchange.
> Mithilfe der Informationen in der Dokumentation zur Bereitstellung von Windows Active Directory und den Informationen in Kapitel 2 dieses Buches
> können Sie die optimale Active Directory-Umgebung für Ihr Unternehmen ermitteln.

In diesem Abschnitt werden verschiedene Aspekte der Netzwerkinfrastruktur und der Active Directory-Umgebung erläutert, die Sie beim Planen eines Exchange-Messagingsystems beachten sollten. In Anhang A, „Prüfliste für das Bewerten der bestehenden Umgebung“, finden Sie eine Prüfliste für die physischen und logischen Faktoren, die Sie beim Beurteilen der bestehenden Umgebung berücksichtigen sollten.

Netzwerkinfrastruktur

Als einen der ersten Schritte sollten Sie ein vollständiges Bild des vorhandenen physischen Netzwerks erstellen, mit dem Sie auswerten können, ob Ihre vorhandene Infrastruktur für die Unterstützung von Exchange geeignet ist. Durch diesen Vorgang können Sie einfacher erkennen, ob Sie das vorhandene LAN bzw. WAN aktualisieren müssen. Beginnen Sie mit einer einfachen Darstellung des gesamten Netzwerks, der die Standorte von Büros und die Verbindungen untereinander entnommen werden können, und fügen Sie dann weitere Details hinzu (Abbildung 1.1).

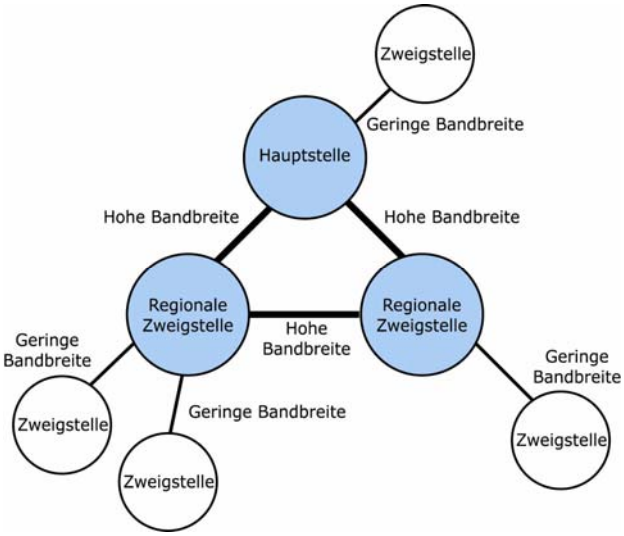


Abbildung 1.1 Anfängliche einfache Darstellung der Netzwerkinfrastruktur

Um ein genaues Bild der LAN- und WAN-Konfiguration zu erhalten, fertigen Sie ein Diagramm aller Standorte, Verbindungstypen und Netzwerktopologien (z. B. Bus, Token Ring oder Stern) an. Fügen Sie die Standorte von Firewalls und Perimeternetzwerken ein. Die Beurteilung sollte auch eine ausführliche Aufstellung der Hardware umfassen, die in der aktuellen Netzwerkinfrastruktur enthalten ist. Dies schließt Einzel- und Clusterserver, Router und Switches ein. Halten Sie auch die Logistik des Datenzentrums fest,

einschließlich Gestellplatz und Informationen über Kabel und die Stromversorgung. Die Prüfliste in Anhang A enthält die genauen Elemente, die Sie im Rahmen dieser Beurteilung untersuchen.

Grundsätzlich sollten Sie Ihre Netzwerkinfrastruktur nach den folgenden Gesichtspunkten beurteilen:

- Geografische Gegebenheiten
- Bandbreite und Wartezeiten
- Aktuelle Nutzung
- Aktuelles Messagingsystem

Diese Aspekte werden in den folgenden Abschnitten behandelt.

Geografische Gegebenheiten

Nachdem Sie die Standorte von Gebäuden, Geländen und Zweigstellen festgehalten haben, bestimmen Sie die Arten von Netzwerkverbindungen zu jedem Standort und die Platzierung von Routern und Switches. Ein umfassendes Wissen über diese Infrastruktur ist für die Festlegung der Anzahl der erforderlichen Exchange-Routinggruppen und der Server in jeder Routinggruppe hilfreich. Ihnen müssen auch die Punkte für die Übermittlung eingehender und ausgehender Nachrichten bekannt sein. Dies umfasst Nachrichten an Server in einer Exchange-Organisation und an Server außerhalb des Exchange-Messagingsystems.

Bandbreite und Wartezeiten

Bei der Planung des Messagingsystems ist es wichtig, die Gesamtmenge von Daten zu berücksichtigen, die in einem bestimmten Zeitraum über das Netzwerk übertragen werden können. Dieser Wert wird durch die Kombination von Bandbreite und Wartezeit bestimmt. Bei der Bandbreite handelt es sich um die Übertragungsgeschwindigkeit in Kilobit pro Sekunde. Die Wartezeit bezieht sich auf die Zeit in Millisekunden, die für die Übertragung von Daten von einem Punkt zu einem anderen benötigt wird. Diese beiden Faktoren haben entscheidenden Einfluss auf die Datenmenge, die einem bestimmten Zeitraum über das Netzwerk übertragen werden kann. Diese Faktoren haben außerdem eine direkte Auswirkung darauf, ob sich eine Transaktion für Benutzer schnell oder langsam gestaltet.

Bei der Bewertung der Netzwerkverbindungen müssen Sie die Bandbreite und die Wartezeit berücksichtigen, da durch bestimmte Netzwerkverbindungen zwar die Bandbreite maximiert, die Wartezeit jedoch möglicherweise verlängert wird. Beispielsweise ist mit einer Satellitenverbindung eine hohe Bandbreite möglich, die Wartezeit ist im Vergleich mit Leitungsverbindungen wie Frame Relay oder ISDN-DFÜ jedoch länger.

Bestimmen Sie bei der Zuordnung von Standorten und Verbindungen den Typ und die Geschwindigkeit der Netzwerkverbindung, und achten Sie dabei auf die Wartezeiten, die durch die Entfernungen der Standorte zueinander entstehen. Möglicherweise werden im Rahmen des Projekts auch Netzwerkaktualisierungen notwendig.

Aktuelle Nutzung

Ein weiterer wichtiger Gesichtspunkt ist die aktuelle Nutzung des Netzwerks. Untersuchen Sie sämtliche Aspekte der Netzwerknutzung, einschließlich der Verwendung durch Anwendungen und Benutzer. Werten Sie die Anwendungen aus, die momentan das Netzwerk verwenden, und beachten Sie dabei die Auswirkungen zukünftiger Projekte und Initiativen. Die zusätzlichen Auswirkungen von zukünftigen Anwendungen auf das Netzwerk müssen dabei mit eingeplant werden.

Bei der Beurteilung der aktuellen Nutzung ist es besonders wichtig, die Netzwerklast zu Spitzenzeiten zu berücksichtigen. Zum Bestimmen der Netzwerklast durch die Benutzer sollten Sie die Anzahl der Benutzer an verschiedenen Standorten und ihre typischen Anforderungen in Betracht ziehen.

Wenn ein Standort mehr als zehn Benutzer aufweist und mit geringer Bandbreite und hohen Wartezeiten verbunden ist, sollte dieser Standort im Offlinemodus betrieben werden. Für Standorte, die über Verbindungen mit geringer Bandbreite und hohen Wartezeiten verfügen, empfiehlt sich die Aktualisierung auf Windows Server 2003, Exchange 2003 und Outlook 2003, da Standorte mit dieser Ausstattung möglicherweise sämtliche Vorteile aus dem Exchange-Cachemodus von Outlook 2003 nutzen können.

Aktuelles Messagingsystem

Bei der Planung sollten Sie sich die folgenden Fragen über Ihr aktuelles Messagingsystem stellen:

- Welche Auswirkungen hat das aktuelle Messagingsystem auf das Netzwerk?
- Führen Sie zurzeit eine frühere Version von Exchange aus? Falls ja, verwenden Sie Exchange 5.5, Exchange 2000 oder beide Versionen im gemischten Modus?

Bei der Planung sollten Sie die Auswirkungen Ihres aktuellen Messagingsystems auf das Netzwerk bestimmen. Mit Lastsimulationstools wie dem Microsoft Exchange Server Load Simulation-Tool (**LoadSim.exe**) oder dem Exchange Stress and Performance (ESP)-Tool können Sie die Nutzung durch das aktuelle Messagingsystem simulieren.
Mit LoadSim wird die Auswirkung von hoher Nutzung durch Outlook-MAPI-Clients simuliert. Dadurch können Sie die beim Testen verwendeten Outlook-Profile anpassen. ESP simuliert die Auswirkung von hoher Last durch Nicht-MAPI-Clients wie Post Office Protocol (POP), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP) oder Outlook Web Access 2003. Sie können mit ESP auch die Last in einer Architektur simulieren, in der Front-End-Server enthalten sind.

Die zum Aktualisieren eines vorhandenen Exchange-Messagingsystems auf Exchange 2003 verwendete Methode hängt davon ab, ob Sie Exchange 5.5 oder Exchange 2000 ausführen. Wenn Sie zurzeit Exchange 5.5 unter Windows NT® Server, Version 4.0, betreiben, müssen Sie das Verschieben von Benutzerkonten nach Active Directory und die Synchronisierung der Verzeichnisinformationen einplanen. Während Exchange 5.5 über einen eigenen Verzeichnisdienst verfügt, ist bei Exchange 2003 Active Directory für die Verzeichnisdienste zuständig. Ihr Projektplan muss eine Methode für die Synchronisierung der beiden Verzeichnisse enthalten. Möglicherweise müssen Sie auch einplanen, dass die beiden Dienste über einen bestimmten Zeitraum nebeneinander betrieben werden, bis Sie Ihre Struktur vollständig auf Exchange 2003 und Active Directory übertragen können. Wenn Sie Exchange 2000 oder eine gemischte Umgebung mit Exchange 5.5 und Exchange 2000 ausführen, ist die Aktualisierung auf Exchange 2003 problemlos, vorausgesetzt, dass Active Directory bereits auf die momentanen Verzeichnisinformationen aktualisiert wurde. Aus diesem Grund müssen Sie den Zustand Ihrer Verzeichnisinformationen sorgfältig prüfen. Weitere Informationen zum Planen des Bereitstellungspfads von Exchange 5.5 auf Exchange 2003 finden Sie in Kapitel 3, „Planen des Bereitstellungspfads“.

Wenn Sie zurzeit Exchange 5.5 betreiben, sollten Sie auch in Erwägung ziehen, Exchange 2003 mit dem Exchange-Cachemodusfeature von Outlook 2003 zu verwenden. Auf diese Weise kann jeder Server mehr Benutzer verwalten, so dass die Anzahl der erforderlichen Exchange-Server verringert wird. Weitere Informationen über den Exchange-Cachemodus finden Sie unter „Informationen über die Versionen von Exchange, Windows und Outlook“ weiter unten in diesem Kapitel.

Active Directory

Neben der Beurteilung der aktuellen physischen Umgebung sollten Sie auch erkennen, wie Windows Server und Active Directory in Ihrer Organisation bereitgestellt werden. Exchange 2003 setzt Active Directory zum

Speichern und zur gemeinsamen Nutzung
von Verzeichnisinformationen unter Windows Server ein. Da diese beiden Komponenten nahtlos integriert sind, muss Ihre Planung eine gründliche Untersuchung der Auswirkungen von Exchange auf Active Directory und umgekehrt enthalten.

Wenn Active Directory bereits bereitgestellt ist, müssen Sie die aktuelle Active Directory-Struktur analysieren und ausarbeiten, wie Exchange in diese Struktur integriert werden kann. In diesem Abschnitt werden die hierfür wichtigsten Überlegungen beschrieben.

Wenn Sie Active Directory noch nicht bereitgestellt haben, ist der Entwurf einer Active Directory-Infrastruktur mit Exchange-Integration einfacher. Es wird empfohlen, dieses Buch vollständig durchzugehen, um die Abhängigkeiten zwischen Exchange und Active Directory zu verstehen. Umfassende Informationen über die Active Directory-Bereitstellung finden Sie auch in den folgenden Ressourcen:

- *Windows Server 2003 Deployment Kit*
  (http://go.microsoft.com/fwlink/?linkid=25197)
- *Best Practice Active Directory Design for Exchange 2000*
  (http://go.microsoft.com/fwlink/?LinkId=17837) (Dieses Whitepaper bezieht sich auf Exchange 2000, die Informationen gelten jedoch auch für Exchange 2003.)

Weitere Informationen über empfohlene Methoden für die Integration von Exchange 2003 mit
Active Directory finden Sie in Kapitel 2, „Planen des Active Directory- und Verwaltungsmodells“.

Im restlichen Teil dieses Abschnitts wird die Beurteilung Ihrer vorhandenen Active Directory-Struktur im Zusammenhang mit Exchange in den folgenden
Bereichen erläutert:

- Physische Struktur des Standortes
- Aufteilung nach Domänen und Gesamtstrukturen
- Verwaltung
- Platzierung des Domänencontrollers und des globalen Katalogservers

Physische Struktur des Standortes

Beginnen Sie mit einer Beurteilung der Windows Server-Standorte und der Verbindungen untereinander, wie weiter oben in diesem Kapitel unter „Netzwerkinfrastruktur“ erläutert. Exchange nutzt die Netzwerkinfrastruktur von Windows, so dass Sie keine gesonderte Infrastruktur für Exchange erstellen und verwalten müssen. Die Struktur des Point-to-Point-Routings ist ein Faktor, der besonders beachtet werden sollte. Beispielsweise sollten Sie bestimmen, ob Standort A über Standort B mit Standort C kommunizieren kann, oder ob Routingbeschränkungen vorliegen.

Aufteilung nach Domänen und Gesamtstrukturen

Aufgrund der engen Integration von Exchange mit Active Directory hat die Active Directory-Gesamtstruktur direkte Auswirkungen auf Ihre Exchange-Planung. Zwischen einer Active Directory-Gesamtstruktur und einer Exchange-Organisation besteht eine 1:1-Beziehung. Eine Exchange-Organisation kann nur eine einzige Active Directory-Gesamtstruktur umfassen. Ebenso kann in einer Active Directory-Gesamtstruktur nur eine Exchange-Organisation verwaltet werden. Das Verständnis
der aktuellen Gesamtstruktur und der Überlegungen hinter diesem Entwurf trägt zu der Entscheidung bei, ob als Host für Exchange eine vorhandene Gesamtstruktur verwendet oder eine neue Gesamtstruktur erstellt werden soll.

Der empfohlene Entwurf für Active Directory umfasst jedoch nur eine einzige Active Directory-Gesamtstruktur für die gesamte Organisation. Ihre Organisation

enthält möglicherweise mehrere Gesamtstrukturen, die für verschiedene Geschäftseinheiten stehen. Ein Grund für diesen Entwurf kann darin bestehen,
dass zwischen den Verzeichnissen für jede Geschäftseinheit strenge Sicherheitsgrenzen bestehen müssen.

In einem Szenario mit mehreren Gesamtstrukturen müssen Sie festlegen, welche Gesamtstruktur den Host für Exchange darstellen soll. Um den Verwaltungsaufwand möglichst gering zu halten, müssen Sie auch eine Übermittlungsmethode implementieren, so dass Änderungen in einer Gesamtstruktur an andere Gesamtstrukturen weitergegeben werden, beispielsweise mithilfe von Microsoft Identity Integration Manager (MIIS). Eine andere Möglichkeit besteht im Erstellen einer getrennten Gesamtstruktur, die nur für
die Verwaltung von Exchange bestimmt ist. Weitere Informationen über das Verringern
der Verwaltungsbelastung finden Sie in Kapitel 2, „Planen des Active Directory- und Verwaltungsmodells“.

> **Wichtig** Es wird empfohlen, für die gesamte Organisation nur eine einzige Active Directory-Gesamtstruktur einzurichten. Wenn in Ihrem Unternehmen
> jedoch strenge Sicherheitsgrenzen zwischen den Geschäftseinheiten erforderlich sind, müssen Sie möglicherweise mehrere Gesamtstrukturen einrichten. In Active Directory stellt eine Gesamtstruktur eine strikte Sicherheitsgrenze dar.
> Dies bedeutet, dass Administratoren in der Gesamtstruktur von anderen Gesamtstrukturen isoliert sind. Bei den Domänen handelt es sich jedoch in erster Linie um Verwaltungsgrenzen. Weitere Informationen über den Entwurf und die Verwaltung von Active Directory finden Sie in den technischen Artikeln *Best Practice Active Directory Design for Managing Windows Networks* (http://go.microsoft.com/fwlink/?LinkId=18348) und *Design Considerations for Delegation of Administration in Active Directory* (http://go.microsoft.com/fwlink/?LinkId=18349).

Beginnen Sie mit der Dokumentation der Gesamtstrukturen, Domänen und Windows-Standorte, aus denen Ihre Organisation besteht. Halten Sie fest, welche Server sich in den Domänen befinden und welches Betriebssystem auf jedem Server ausgeführt wird. Notieren Sie außerdem die Gruppen oder Personen, die für die Gesamtstrukturen, Domänen und Windows-Standorte verantwortlich sind.

Verwaltung

Das in der Organisation angewendete Verwaltungsmodell ist ein weiterer wesentlicher Punkt, der in Erwägung gezogen werden muss. Da in Exchange 2003 Active Directory verwendet wird, verwalten Sie Exchange gemeinsam mit dem Betriebssystem.
Mit Active Directory haben Sie die Möglichkeit, die Verwaltungsautorität über Organisationseinheiten in Active Directory-Benutzer und -Computer an Verzeichnisobjekte zu delegieren. Sie können die Windows-Verwaltungsberechtigungen in Active Directory auf der Ebene von Organisationseinheiten delegieren. Bei der Verwaltung von Exchange-Servern gruppieren Sie Server in eine administrative Gruppe und delegieren die Berechtigungen an diese Gruppe.

Bei der Dokumentation der Server in jeder Domäne der Gesamtstruktur sollten
Sie auch die Gruppen oder Personen festhalten, denen die Active Directory-Verwaltungsberechtigungen übertragen wurden. Anschließend können Sie mit
diesen Informationen auf der Grundlage Ihrer Geschäftsanforderungen bestimmen,
wie die Exchange-Server verwaltet werden sollen. Weitere Informationen über das Planen des Verwaltungsmodells finden Sie in Kapitel 2, „Planen des Active Directory- und Verwaltungsmodells“.

Platzierung des Domänencontrollers und des globalen Katalogservers

Bei der Dokumentation der Server in jeder Domäne geben Sie die Domänencontroller und die globalen Katalogserver an. Diese Informationen sind für die Planung einer Exchange-Organisation von großer Bedeutung, da Sie wissen müssen, wie sich die Benutzer an den einzelnen Standorten anmelden und wie Informationen zu globalen Adresslisten und Exchange-Objekte über die Gesamtstruktur repliziert werden. Ein

Domänencontroller ist auf die Domäne beschränkt, in der er installiert ist. Die Funktion eines globalen Katalogservers in Active Directory besteht darin, für Benutzerobjekte über alle Domänen in der Gesamtstruktur einen Teilattributsatz zu verwalten. Möglicherweise müssen Sie an der Platzierung dieser Server für Exchange Änderungen vornehmen. Weitere Informationen über die Platzierung von Servern in Active Directory finden Sie in Kapitel 2, „Planen des Active Directory- und Verwaltungsmodells“.

Informationen über die Versionen von Exchange, Windows und Outlook

Nachdem Sie Ihre Geschäftsanforderungen beurteilt und die vorhandene Umgebung dokumentiert haben, können Sie sich auf Grundlage der Informationen über die Messagingsoftware und das Betriebssystem für einen Entwurf entscheiden, der
die Ansprüche Ihres Unternehmens erfüllt.

Beim Entwerfen eines Exchange-Messagingsystems besteht ein schwieriger Schritt
im Abwägen der Geschäfts- und Benutzeranforderungen gegen die Möglichkeiten
des vorhandenen Systems. Für bestimmte Benutzeranforderungen ist es u. U. notwendig, Aktualisierungen des Netzwerkbackbones, der Serverhardware oder
der Betriebssystemsoftware zu empfehlen. In den folgenden Abschnitten werden die Features der aktuellen Versionen von Exchange, Windows Server und Outlook erläutert, die Auswirkungen auf Ihre Entwurfsentscheidungen haben. Mit diesen Features können Sie bestimmen, ob technische Aktualisierungen erforderlich sind.

Vergleichen der Windows Server-Versionen

In vielen Fällen trägt die Kombination von Exchange Server 2003, Windows Server 2003 und Outlook 2003 dazu bei, die Standorte von Firmen zu vereinheitlichen und die Anzahl von Servern an Remotestandorten zu verringern.

Windows Server 2003

Die folgenden Features und Änderungen in Windows Server 2003 wirken sich möglicherweise auf den Entwurf von Active Directory und Exchange aus:

- **Erhöhte Anzahl von Standorten pro Gesamtstruktur** Aufgrund der in Windows Server 2003 verbesserten Konsistenzprüfung (Knowledge Consistency Checker; KCC) und der verbesserten Erstellung der standortübergreifenden Topologie (Intersite Topology Generator; ISTG) können Gesamtstrukturen eine größere Anzahl von Standorten enthalten als unter Microsoft Windows 2000 Server. Bei Windows 2000 Server betrug die Grenze 300 Standorte pro Domäne. Eine Windows Server 2003-Domäne kann mehr als 3.000 Standorte enthalten. Diese Verbesserungen der Skalierbarkeit wirken sich möglicherweise auf Ihre Gesamtstruktur aus.
- **Volumeschattenkopie-Dienst** Windows Server 2003 enthält Volumeschattenkopie-Dienstfunktionen, mit denen Sie schnell und ohne großen Einfluss auf die E-Mail-Clients Onlinesicherungen von Anwendungsdatenvolumes durchführen können. Der Volumeschattenkopie-Dienst funktioniert mit Anwendungen, Betriebssystemen, Sicherungsprogrammen und Speicherhardware, so dass konsistente Schattenkopien
der Daten erstellt werden. Mit diesem Feature können Sie dynamische Wiederherstellungen durchführen und Daten durchsuchen, ohne dass dies Auswirkungen auf die Leistung hat.
- **SAN-Unterstützung (Storage Area Network)** SANs wurden in Windows Server 2003 in vieler Hinsicht verbessert. Dies schließt Verbesserungen beim Verbinden mit Volumes, die Handhabung von Fiber-Channel-SANs und Möglichkeiten zum Starten über ein SAN ein.

- **Anmeldung ohne lokalen globalen Katalogserver** Bei Windows Server 2003 können sich Benutzer ohne lokalen globalen Katalogserver anmelden. Bei diesem Feature werden die Anmeldeinformationen der Benutzer zwischengespeichert,
  so dass Anfragen an den globalen Katalogserver erheblich verringert werden.
  Die Möglichkeit der Anmeldung ohne lokalen globalen Katalogserver ist jedoch
  nur für Windows-Standorte ohne Exchange-Benutzer gedacht.

  Wichtig An Windows-Standorten mit Exchange-Benutzern wird es immer empfohlen, einen lokalen globalen Katalogserver zu installieren.

Windows 2000 Server

Wenn Sie Windows 2000 Server weiterhin als Betriebssystem verwenden oder einige Server auf Windows Server 2003 aktualisieren, stehen einige Features von Windows Server 2003 nicht zur Verfügung, bis Sie die Gesamtstruktur auf eine reine Windows Server 2003-Gesamtstruktur aktualisieren.

Insbesondere ist es für das RPC über HTTP-Feature von Outlook erforderlich, dass
auf dem Exchange-Server und einem globalen Katalogserver Windows Server 2003 ausgeführt wird und dass das Active Directory-Schema auf Windows Server 2003 aktualisiert wird.

Andere Features von Exchange 2003, z. B. der Volumeschattenkopie-Dienst, sind verfügbar, wenn Sie Exchange 2003 unter Windows Server 2003 betreiben, das Active Directory-Schema muss jedoch nicht auf Windows Server 2003 aktualisiert werden.

Verbesserungen in Exchange 2003

Exchange 2003 bietet in folgenden Bereichen eine verbesserte Funktionalität:

- Routing
- Unterstützung für den Volumeschattenkopie-Dienst
- Unterstützung für den Outlook 2003-Exchange-Cachemodus
- Outlook Web Access für Exchange 2003
- Unterstützung mobiler Geräte für Exchange 2003
- Outlook 2003

Einige dieser Verbesserungen hängen davon ab, ob Sie Windows Server 2003 oder Outlook 2003 verwenden. Diese Verbesserungen und ihre Abhängigkeiten werden
in den folgenden Abschnitten erläutert.

Verbesserungen beim Routing

In Exchange 2000 konnten durch Verbesserungen des Routings gegenüber Exchange 5.5 die früheren Hub-and-Spoke-Routingarchitekturen vermieden werden. Beispielsweise mussten Sie in Exchange 5.5 möglicherweise eine Hub-and-Spoke-Routingarchitektur einrichten, um feste Routingpfade zu unterstützen. Dazu mussten Sie wahrscheinlich mehrere Server bereitstellen, die am Hub-Standort nur für das Nachrichtenrouting zuständig waren.

Mit dem in Exchange 2000 eingeführten Verbindungsstatusrouting konnten die sendenden Server die beste Route über den Verbindungsstatus bestimmen. Durch
diese Änderung war ein Wechsel zu Peer-to-Peer-Netzwerken zwischen Routinggruppen möglich, da Nachrichten von jeder Routinggruppe über den Netzwerkbackbone eine direkte Route zur empfangenden Gruppe suchen konnten.

In Exchange 2003 werden die Verbindungsstatusrouting-Features von Exchange 2000 weiter verbessert, indem die Menge des Verbindungsstatus-Datenverkehrs auf zwei Arten verringert wird.

- Die Leistung wird über so genannte oszillierende Verbindungen verbessert. Dabei handelt es sich um Verbindungen, die nur zeitweise verfügbar bzw. nicht verfügbar sind. In Exchange 2003 werden die übertragenen Verbindungsstatusinformationen verringert, indem bestimmt wird, ob die Verbindung oszilliert. Wenn für eine Verbindung in einem bestimmten Intervall mehrere einander ausschließende Statusänderungen in der Verbindungsstatus-Warteschlange vorliegen, wird die Verbindung als oszillierend angesehen, und der Verbindungsstatus gilt als aktiv (in diesem Zeitraum nutzbar bzw. verfügbar). Durch die dauerhafte Aktivierung einer oszillierenden Verbindung anstelle einer ständigen Änderung des Verbindungsstatus wird der zwischen den Servern replizierte Datenverkehr für Verbindungsstatusinformationen verringert.
- Die Leistung wird für Standorte verbessert, zu denen lediglich eine Route vorliegt. In diesem Fall wird mit Exchange 2003 der Verbindungsstatus-Datenverkehr verringert, indem festgehalten wird, dass kein alternativer Pfad existiert und die Verbindungsstatusinformationen unterdrückt werden. Wenn kein anderer Pfad für eine Verbindung verfügbar ist, wird der Verbindungsstatus immer als aktiv gekennzeichnet. Zu versendende Nachrichten werden von Exchange in einer Warteschlange angeordnet und übertragen, wenn die Route zur Verfügung steht.

Durch diese beiden Änderungen wird die Leistung verbessert, da weniger Verbindungsstatusinformationen weitergegeben werden.

Volumeschattenkopie-Dienst

Die Anzahl der Benutzer, die theoretisch auf einem einzelnen Server unterstützt werden können, wird in der Praxis durch den Zeitaufwand eingeschränkt, der für eine Sicherung des Nachrichtenspeichers benötigt wird. Wenn Sie diese Einschränkung umgehen möchten, muss die Möglichkeit bestehen, Postfachspeicher und Informationsspeicher für Öffentliche Ordner schnell zu sichern und wiederherzustellen. Exchange 2003 verwendet den Volumeschattenkopie-Dienst von Windows Server 2003, um zu bestimmten Zeitpunkten schnell Sicherungen der Exchange-Daten zu erstellen.

Durch den Volumeschattenkopie-Dienst werden verschiedene Probleme mit zuvor verwendeten Sicherungsmethoden behoben. Wenn eine Exchange-Datenbank verbunden ist, können weiterhin zu jedem Zeitpunkt E-Mail-Transaktionen durchgeführt werden.
Wenn Sie zu einem bestimmten Zeitpunkt eine Schnellsicherung der Daten (eine Schattenkopie) anfertigen, können während des Sicherungsvorgangs weiterhinE-Mail-Transaktionen durchgeführt werden. Daher kann es nach Abschluss der Sicherung vorkommen, dass eine inkonsistente Kopie der Daten vorliegt. Da außerdem empfohlen wird, die Exchange-Datenbankdateien (EDB-Dateien), Transaktionsprotokolldateien und MIME-Inhalte (Multipurpose Internet Mail Extensions, STM-Dateien) auf getrennten Datenträgern zu speichern, können die Daten inkonsistent sein. Wenn Sie beispielsweise eine Schattenkopie der Daten anfertigen, während Änderungen auftreten, die noch nicht in das Protokoll geschrieben wurden, stimmen die Dateien nicht überein.

Ohne den Volumeschattenkopie-Dienst kann dieses Problem umgangen werden, indem Sicherungen im Offlinemodus durchgeführt werden. Dies bedeutet, dass Sicherungsvorgänge stattfinden müssen, während der Server nicht in Betrieb ist. Sie müssen Exchange in diesem Fall stets beenden, damit eine konsistente Sicherungskopie angefertigt werden kann. Bei dieser Herangehensweise treten jedoch Planungsprobleme auf, und die Vorteile von Sicherungen mittels Schattenkopien können nicht genutzt werden. Außerdem wird das Abschließen von Sicherungen erschwert, da Systeme in immer größerem Maße rund um die Uhr und ohne Betriebsunterbrechungen verfügbar sein müssen.

Durch den Volumeschattenkopie-Dienst wird eine konsistente Kopie der Daten zu einem bestimmten Zeitpunkt erstellt, während das System online ist. Nach dem Empfang einer Sicherungsanfrage sendet der

Volumeschattenkopie-Dienst eine Benachrichtigung an die Exchange-Dienste über den anstehenden Beginn einer Sicherung. Exchange kann dann durch Bereinigen von Festplattenstrukturen und Löschen von Caches und Protokolldateien die Sicherung vorbereiten.

Wichtig Exchange unterstützt den Volumeschattenkopie-Dienst für normale Sicherungen und Kopiesicherungen, jedoch nicht für inkrementelle und differenzielle Sicherungen.

Unterstützung für den Outlook 2003-Exchange-Cachemodus

Exchange 2003 unterstützt den Outlook 2003-Exchange-Cachemodus, bei dem Benutzer über einen lokalen Zwischenspeicher in Form einer OST-Datei auf Exchange-Informationen zugreifen können. Exchange stellt dabei sicher, dass das Postfach auf dem Server und die OST-Datei auf dem Clientcomputer synchronisiert bleiben, solange die Netzwerkverbindung verfügbar ist. Wenn die Netzwerkverbindung nur zeitweise besteht oder ganz unterbrochen wird, können Benutzer E-Mail-Daten aus den in der lokalen OST-Datei gespeicherten Informationen abrufen. Aktualisierungsanforderungen vom Clientcomputer an den Exchange-Server werden dadurch vermieden, so dass Benutzern von Outlook 2003 in Zeiträumen, in denen die Verbindung nur teilweise oder überhaupt nicht verfügbar ist, nicht die Meldung angezeigt wird, dass Daten vom Exchange-Server angefordert werden. Durch die Vermeidung von Aktualisierungsanforderungen vom Clientcomputer wird außerdem der Datenverkehr vom Clientcomputer zum Server reduziert.

Weitere Informationen über den Exchange-Cachemodus finden Sie unter „Verbesserungen in Outlook 2003“ weiter unten in diesem Kapitel.

Verbesserungen in Outlook Web Access 2003

Die neue Version von Outlook Web Access in Exchange Server 2003 enthält eine Reihe von Verbesserungen, z. B. formularbasierte Authentifizierung, Regeln, Rechtschreibprüfung und die Möglichkeit, digital signierte und verschlüsselte E-Mail-Nachrichten zu senden und zu empfangen. Die Benutzeroberfläche wurde ebenfalls neu gestaltet und der Benutzerführung in Outlook 2003 angeglichen. So sind jetzt u. a. ein Vorschaufenster auf der rechten Seite und ein verbesserter Navigationsbereich verfügbar.

Outlook Web Access für Exchange 2003 ist insbesondere bei langsamen Verbindungen leistungsfähiger als zuvor und reagiert daher wesentlich schneller auf Benutzereingaben.

In der folgenden Liste werden die wichtigsten neuen Funktionen in Outlook Web Access für Exchange 2003 kurz beschrieben:

- **Anzahl übertragener Bytes** Durch Verringern der Menge an Informationen, die zwischen Server und Browser übertragen werden müssen, wurde die Geschwindigkeit von Outlook Web Access gesteigert. Es werden weniger Bytes vom Server zum Browser übertragen. Beachten Sie jedoch, dass beim Anmeldevorgang mehr Bytes als beim Anmeldevorgang für Outlook 2003 übertragen werden.
- **Unterstützung von Komprimierung** Administratoren können für Outlook Web Access Komprimierungsunterstützung konfigurieren und so bei langsamen Netzwerkverbindungen eine Leistungssteigerung von bis zu 50 % erzielen. Outlook Web Access wurde für die Arbeit über langsame Netzwerkverbindungen optimiert, denen Datenkomprimierung unterstützt wird. Bei der Komprimierung werden in Outlook Web Access abhängig von den verwendeten Komprimierungseinstellungen entweder statische oder dynamische Webseiten oder beide Arten von Webseiten komprimiert. Datenkomprimierung macht sich für Benutzer in Leistungssteigerungen von bis zu 50 % über langsamere Netzwerkverbindungen bemerkbar, z. B. bei

herkömmlichen DFÜ-Verbindungen. Die Komprimierung können Sie im Exchange System-Manager aktivieren.

- **Formularbasierte Authentifizierung** Sie können eine neue Anmeldeseite für Outlook Web Access aktivieren, in der die Namen und Kennwörter der Benutzer nicht im Browser, sondern in einem Cookie gespeichert werden. Beim Schließen des Browsers wird das Cookie gelöscht. Zusätzlich wird das Cookie auch nach einem bestimmten Zeitraum der Inaktivität des Benutzers gelöscht. Auf der Anmeldeseite müssen Benutzer entweder ihren Domänen- und Benutzernamen sowie das Kennwort oder die E-Mail-Adresse und das Kennwort ihres vollständigen Benutzerprinzipalnamens (UPN) eingeben. Zum Aktivieren der Anmeldeseite von Outlook Web Access müssen Sie auf dem Server die formularbasierte Authentifizierung aktivieren.

Die Verbesserungen in Bezug auf Features, Funktionalität und Leistung können Entscheidungen darüber beeinflussen, wie Benutzer hauptsächlich auf ihre Exchange-Informationen zugreifen. Für Remotestandorte kann die Verwendung von Outlook Web Access besonders empfehlenswert sein. Dies muss beim Planen von WAN-Verbindungen und der Serverplatzierung berücksichtigt werden.

Unterstützung mobiler Geräte in Exchange Server 2003

In Exchange 2003 sind zwei Anwendungen integriert, die sowohl Geräte mit Microsoft Windows Mobile™ 2003 als auch andere mobile Geräte unterstützen. Wenn Sie die Unterstützung für mobile Geräte in Exchange bereitstellen, können Benutzer über verschiedene mobile Geräte auf ihre Exchange-Informationen zugreifen. Exchange ActiveSync® und Outlook Mobile Access können Sie auf dieselbe Weise für den Exchange-Server bereitstellen wie Outlook Web Access 2003. In der Standardeinstellung wird beim Installieren von Exchange die Synchronisierung und der Browserzugriff mit Outlook Mobile Access für alle Benutzer aktiviert.

- **Synchronisierung** Durch Synchronisieren eines Geräts mit einem Exchange-Server können Benutzer auf ihre Exchange-Informationen zugreifen, ohne ständig mit einem Mobilnetzwerk verbunden sein zu müssen. Die Benutzer können die Verbindung ihres Mobilnetzbetreibers verwenden, um ihre Exchange-Informationen mit ihrem Gerät mit Pocket PC 2002 Phone Edition oder ihrem Smartphone zu synchronisieren und offline auf diese Informationen zuzugreifen.
- **Aktuelle Benachrichtigungen** Aktuelle Benachrichtigungen sind automatisch erzeugte SMS-Nachrichten, die an das Windows Mobile-Gerät eines Benutzers gesendet werden, wenn eine neue E-Mail-Nachricht, ein neuer Kalendertermin oder ein neuer Kontakt im Postfach des Benutzers eingeht. Benutzer müssen ihre Geräte für den Empfang von aktuellen Benachrichtigungen konfigurieren.
- **Mobiler Browserzugriff** Exchange Server 2003 enthält die Anwendung Outlook Mobile Access, mit der Benutzer über mobile Geräte auf den Exchange-Server zugreifen können, um E-Mail-Nachrichten, Kontakte, Kalenderdaten und Aufgaben anzuzeigen.

Verbesserungen in Outlook 2003

Outlook 2003 bietet in folgenden Bereichen eine verbesserte Funktionalität:

- Exchange-Cachemodus
- RPC über HTTP
- Kerberos-Authentifizierung

Für einige dieser Verbesserungen müssen Sie Windows Server 2003 oder Outlook 2003 verwenden. Die Verbesserungen und ihre gegenseitigen Abhängigkeiten werden im Folgenden erläutert.

Exchange-Cachemodus

Mit dem Exchange-Cachemodus in Outlook 2003 wird vor allem die Benutzerfreundlichkeit für Benutzer erhöht, die in Büros mit langsamen Netzwerkverbindungen mit geringer Bandbreite arbeiten, da Benutzer E-Mail-Nachrichten entweder über einen lokalen Zwischenspeicher (eine OST-Datei) oder vom Exchange 2003-Server abrufen können. Exchange 2003 bietet eine bessere Unterstützung für den Exchange-Cachemodus als frühere Versionen von Exchange, da das Postfach auf dem Server und die OST-Datei
auf dem Clientcomputer effizient synchronisiert werden. Dadurch sind keine Aktualisierungsanforderungen vom Clientcomputer an den Exchange-Server mehr nötig.

Der Exchange-Cachemodus ist besonders bei Unternehmen mit mehreren Zweigstellen vorteilhaft, bei denen die Remotebenutzer über langsame und unzuverlässige Verbindungen arbeiten. Unabhängig davon, ob gerade eine Netzwerkverbindung verfügbar ist, können Benutzer über den lokalen Zwischenspeicher arbeiten. Exchange synchronisiert den lokalen Zwischenspeicher und das Serverpostfach, wenn eine Verbindung verfügbar ist. Darüber hinaus sind beim Exchange-Cachemodus weniger Anforderungen an den Server erforderlich. Dadurch wird die Serverauslastung pro Benutzer verringert, und es können pro Server mehr Benutzer unterstützt werden.

> **Hinweis** Wenn Outlook-Benutzer den Exchange-Cachemodus verwenden und eine bedeutsame Verzeichnisänderung auftritt, empfängt jeder Outlook-Clientcomputer einen vollständigen Download des Offlineadressbuchs. Dieser vollständige Download findet auf den Clientcomputern aller Remotestandorte statt, nicht nur auf denen
> am konsolidierten Standort. Der Download wird beispielsweise bei der Standortkonsolidierung durchgeführt. Weitere Informationen zu diesem Vorgang finden Sie in Kapitel 4, „Planen einer Standortkonsolidierung“.

Aspekte beim Bereitstellen des Exchange-Cachemodus

Beim Bereitstellen von Outlook 2003 in Ihrer Messagingumgebung können Sie Benutzern die Verwendung des Exchange-Cache-Modus für Outlook erlauben. Dabei empfiehlt es sich, die Bereitstellung schrittweise auszuführen. Wenn ein Benutzer eine Synchronisierung mit einem Exchange-Server startet, wird die OST-Datei auf dem Computer des Benutzers angelegt. Dabei werden alle Informationen im Postfach des Benutzers vom Server auf den Computer des Benutzers übertragen. Daher sollte die Bereitstellung schrittweise erfolgen, um die Anzahl der Benutzer zu verringern, die gleichzeitig die erste Synchronisierung zwischen dem Exchange-Server und ihrem Computer mit Outlook 2003 ausführen. Die Aufteilung der Bereitstellung des Exchange-Cachemodus in einzelne Phasen ist erforderlich, da Benutzer bei der ersten Synchronisierung eine vollständige Kopie ihres Postfaches vom Exchange-Server auf den lokalen Computer downloaden. Dieser erste Download kann sich negativ auf die Leistung des Exchange-Servers auswirken, wenn viele Benutzer gleichzeitig versuchen, ihr Postfach auf den lokalen Computer zu übertragen.

Die Datenmenge ist insbesondere dann von Bedeutung, wenn die Verbindung langsam ist und mehrere Benutzer gleichzeitig eine Verbindung herstellen. Wenn die Postfächer der Benutzer sehr groß sind (z. B. jeweils größer als 2 GB) kann die Synchronisierung mit der OST-Datei beträchtliche Auswirkungen auf die Netzwerkverbindung haben. Diese Situation kann vor allem in Unternehmen auftreten, in denen die Postfachgröße nicht beschränkt ist.

Beachten Sie außerdem, dass die OST-Datei in der Standardeinstellung im Verzeichnis für das jeweilige Profil angelegt wird. Wenn Benutzer servergespeicherte Profile verwenden (z. B. für verschiedene Zweigstellen), steht der Cache nur in einem der Profile zur Verfügung.

RPC über HTTP

Mit RPC über HTTP unter Windows Server 2003 müssen Remotebenutzer die Verbindung zum Exchange-Server nicht mehr über ein virtuelles privates Netzwerk (VPN) herstellen. Benutzer, die Outlook 2003 ausführen, können über das Internet eine direkte Verbindung mit einem Exchange 2003-Server innerhalb einer Unternehmensumgebung herstellen. Die Unterstützung von RPC über HTTP ist nur verfügbar, wenn auf allen

Exchange-Servern, auf die Benutzer mit Outlook 2003 zugreifen, Exchange Server 2003 ausgeführt wird. RPC über HTTP wird zudem nur von Outlook 2003 unterstützt. Außerdem muss auf allen Computern, die im Zusammenhang mit RPC über HTTP verwendet werden, Windows Server 2003 ausgeführt werden. Dies betrifft folgende Computer:

- Alle globalen Katalogserver
- Alle Exchange-Server, auf die Outlook 2003-Benutzer zugreifen

Nach dem Konfigurieren der empfohlenen Front-End- und Back-End-Serverarchitektur für Exchange mit ISA Server (Internet Security and Acceleration) können Benutzer für die Verbindung zu Exchange 2003-Servern RPC über HTTP verwenden.

> **Wichtig** Wenn Sie RPC über HTTP verwenden möchten, muss das bestehende Active Directory-Schema auf Windows Server 2003 aktualisiert werden.

Für das Bereitstellen von RPC über HTTP empfiehlt es sich, ISA Server mit Feature Pack 1 im Perimeternetzwerk zu installieren und den RPC-Proxyserver im Unternehmensnetzwerk einzubinden. Als RPC-Proxyserver kann der Exchange-Front-End-Server oder ein anderer Webserver verwendet werden, zu dem Benutzer eine Verbindung über das Internet herstellen können. Weitere Informationen über Bereitstellungsoptionen finden Sie unter „Verwenden von RPC über HTTP“ in Kapitel 5.

Zum Aktivieren von RPC über HTTP sind folgende Schritte erforderlich:

- **Konfigurieren eines Servers als RPC-Proxyserver** Wenn ein Server vorhanden ist, auf den Benutzer über das Internet zugreifen können, beispielsweise ein Exchange-Front-End-Server, können Sie diesen Server als RPC-Proxyserver konfigurieren. Dieser RPC-Proxyserver ist für die Festlegung der Anschlüsse verantwortlich, über die die Kommunikation mit den globalen Katalogservern und allen Exchange 2003-Servern erfolgt, mit denen die Outlook 2003-Clientcomputer kommunizieren müssen.
- **Konfigurieren des internen Netzwerks für die Verwendung von RPC über HTTP** Alle Computer, auf die Benutzer von Outlook 2003 zugreifen, z. B. alle Exchange Server 2003-Computer und die globalen Katalogserver, müssen für die Verwendung von RPC über HTTP konfiguriert werden. Darüber hinaus muss das Perimeternetzwerk so konfiguriert sein, dass Netzwerkverkehr mit RPC über HTTP aktiviert ist.

Kerberos-Authentifizierung

Bei Exchange 2003 und Outlook 2003 kann jetzt auch Kerberos für die Authentifizierung von Benutzern auf Exchange 2003-Servern verwendet werden. Wenn in Ihrem Netzwerk Windows Server 2003-Domänencontroller verwendet werden, können sich die Benutzer über mehrere Gesamtstrukturen hinweg bei den Domänencontrollern in vertrauenswürdigen Gesamtstrukturen authentifizieren, so dass Benutzerkonten und Exchange-Server in unterschiedlichen Gesamtstrukturen vorhanden sein können.

Exchange 2003 verwendet beim Senden von Anmeldeinformationen von Benutzern zwischen einem Exchange-Front-End-Server und dem Exchange-Back-End-Server Kerberos-Authentifizierung. Bei früheren Versionen von Exchange wurde für das Austauschen von Anmeldeinformationen zwischen einem Exchange-Front-End-Server und einem Exchange-Back-End-Server für Anwendungen wie Outlook Web Access die Standardauthentifizierung verwendet. Daher mussten zum Verschlüsseln des Datenverkehrs zwischen Exchange-Front-End-Servern und Exchange-Back-End-Servern Sicherheitsmechanismen wie IPSec (Internet Protocol Security, IP-Sicherheit) eingesetzt werden.

Zusammenfassung

Beim Planen der Platzierung von Exchange-Servern und der Verwaltung von Verzeichnissen und Servern empfiehlt es sich meist, mit einem zentralisierten Modell zu beginnen und anschließend bei Bedarf Server, Routinggruppen und administrative Gruppen hinzuzufügen. Mit den in Exchange 2003, Windows Server 2003 und Outlook 2003 verfügbaren Features haben Unternehmen die Möglichkeit, zentralisiertere Messagingsysteme als bisher einzurichten.

Mit der zunehmenden Verbreitung von schnellen Netzwerkverbindungen
hoher Bandbreite können Unternehmen mit geografisch weit verteilten Zweigstellen zudem ihre Hardware und Verwaltung zentralisieren, um die Anzahl der an Remotestandorten erforderlichen Server zu reduzieren. Die Faktoren, die Einfluss auf die Zentralisierung haben, lassen sich in folgende drei Kategorien einteilen:

- **Zentralisieren der Serverhardware für Remotestandorte** Die Kommunikation zwischen Clientcomputer und Server wird komprimiert. Der Datenverkehr wird durch Verbesserungen in der Outlook-RPC-Kommunikation und in der Outlook Web Access 2003-Komprimierung erheblich verringert. Exchange 2003 verfügt über eine Reihe von Features, mit denen Sie Standorte und administrative Gruppen besser konsolidieren können. Darüber hinaus kann mithilfe des Exchange-Cachemodus
  in Outlook 2003 die Anzahl der Server an Remotestandorten reduziert werden,
  die über Verbindungen mit hohen Wartezeiten an das Unternehmensnetzwerk angebunden sind.
- **Reduzieren der Anzahl von Servern** Unternehmen sind oft daran interessiert, die Anzahl der für Messagingsysteme nötigen Server zu verringern, um die Gesamtbetriebskosten zu senken. Ihr Unternehmen trifft möglicherweise die Entscheidung, die Anzahl der Server durch Investitionen in Hochleistungsserver
  zu reduzieren, beispielsweise Server mit hoher Prozessorgeschwindigkeit oder mehreren Prozessoren. Windows Server 2003 und Exchange 2003 unterstützen auch Hyperthreading. Dabei kann ein einzelner Prozessor mehrere Threads gleichzeitig ausführen, so dass es den Anschein hat, als wären mehrere Prozessoren vorhanden. Der betreffende Prozessor muss Hyperthreading unterstützen, und
  Sie müssen Windows Server 2003 und Exchange 2003 verwenden.
- **Zentralisieren der Server- und Verzeichnisverwaltung** Unternehmen können administrative Aufgaben bei Bedarf zentralisieren, um Verwaltungskosten zu sparen. Eines der Features, mit denen die Verwaltung vereinfacht werden kann, ist die verbesserte Methode zum Verschieben von Postfächern in Exchange System-Manager. Administratoren können Postfächer effizienter verschieben und Daten schneller wiederherstellen, wenn fehlerhafte Elemente gefunden werden. Außerdem können Start- und Endzeiten für das Verschieben von Postfächern festgelegt werden.

Planen des Active Directory- und Verwaltungsmodells

In Kapitel 1 wurde das vorhandene Modell für den Microsoft® Active Directory®-Verzeichnisdienst beurteilt (wenn Active Directory bereits implementiert war),
und es wurden die Verwaltungsanforderungen ermittelt. Nun können Sie mit dem Planungsvorgang für das Integrieren von Microsoft Exchange Server 2003 in das Active Directory-Modell beginnen. Außerdem können Sie die Exchange-Verwaltung planen, indem Sie prüfen, wie die Funktionen in Ihrem Unternehmen mit dem Verwaltungsmodell in Zusammenhang stehen, das Sie für Ihre Exchange-Organisation wählen.

In diesem Kapitel werden zu Beginn die verschiedenen Möglichkeiten für die Einbindung von Exchange in Active Directory erläutert. Anschließend wird untersucht, welche Optionen beim Entwerfen des Verwaltungsmodells zur Auswahl stehen.

Optionen für die Integration von Exchange in Active Directory

Da sowohl für Microsoft Windows Server™ 2003 als auch für Exchange 2003 der Active Directory-Verzeichnisdienst benötigt wird, müssen Sie festlegen, wie Exchange
in die Active Directory-Struktur integriert werden soll.

Beim Bereitstellen von Exchange muss eine stabile, funktionsfähige Active Directory-Infrastruktur vorhanden sein. Wenn Sie eine bestehende Microsoft Windows NT®-Umgebung aktualisieren, empfiehlt es sich, vor dem Bereitstellen von Exchange alle Windows NT-Konten und -Ressourcen zu Active Directory zu migrieren. Sie können jedoch Exchange auch dann bereitstellen, wenn der Migrationsvorgang von Windows NT-Objekten zu Active Directory noch nicht abgeschlossen ist, oder wenn Sie weiterhin für bestimmte Ressourcenobjekte eine Windows NT-Gesamtstruktur benötigen. In den
in diesem Abschnitt enthaltenen Beispielen werden diese verschiedenen Szenarien berücksichtigt.

Innerhalb jeder Gesamtstruktur können Sie Ressourcen zum Verwalten von Windows 2003 Server und Exchange 2000 Server kombinieren oder diese
Ressourcen getrennt verwalten. Das Kombinieren von Ressourcen wird durch
die Integration von Exchange in Windows Server 2003 ermöglicht.

Beim Integrieren von Exchange in Active Directory bestehen vier Möglichkeiten:

- **Einzelne Gesamtstruktur** Benutzer und deren Postfächer sind in derselben Gesamtstruktur enthalten.
- **Dedizierte Exchange-Gesamtstruktur (Ressourcengesamtstruktur)**
  Eine Gesamtstruktur ist ausschließlich für das Ausführen von Exchange und
  das Bereitstellen von Exchange-Postfächern reserviert. Die zu den Postfächern gehörenden Benutzerkonten sind in einer oder mehreren anderen Gesamtstrukturen enthalten.
- **Mehrere Gesamtstrukturen, in denen Exchange ausgeführt wird (klassische Variante mit mehreren Gesamtstrukturen)** Exchange wird in getrennten Gesamtstrukturen ausgeführt, E-Mail-Funktionen sind jedoch gesamtstrukturübergreifend verfügbar.
- **Fusionen und Übernahmen** Bei Fusionen und Übernahmen ist bis zur endgültigen Zusammenführung häufig die Koexistenz von Exchange-Organisationen erforderlich. Die Überlegungen bei der Planung entsprechen denen des Szenarios mit mehreren Gesamtstrukturen, erweitert um zusätzliche Punkte bezüglich Migrationen.

Dieser Abschnitt enthält ausführliche Informationen zu diesen Optionen und dient der Unterstützung bei der Entscheidung für die optimale Konfiguration Ihrer Organisation. Zusätzlich bieten die folgenden Quellen Informationen, die bei Ihren Entwurfsentscheidungen hilfreich sein können:

Hinweis Obwohl in einigen dieser Quellen Exchange 2000 behandelt wird, treffen die Informationen auch auf Exchange 2003 zu.

- *Multiple Forest Considerations*
  (http://go.microsoft.com/fwlink/?LinkId=21177)
- *Best Practice Active Directory Design for Exchange 2000*
  (http://go.microsoft.com/fwlink/?LinkId=17837)
- *Design Considerations for Delegation of Administration in Active Directory*
  (http://go.microsoft.com/fwlink/?linkid=18349)
- *Best Practice Active Directory Design for Managing Windows Networks*
  (http://go.microsoft.com/fwlink/?linkid=18348)

Einzelne Gesamtstruktur

Wenn in Ihrem Unternehmen eine einzelne Active Directory-Gesamtstruktur verwendet wird, können Sie Exchange in dieser Gesamtstruktur implementieren. Die Variante mit einer einzelnen Gesamtstruktur für Exchange wird empfohlen, da bei dieser Variante
die größte Anzahl von Features für das Mailsystem verfügbar ist und sich gleichzeitig ein optimales Verwaltungsmodell ergibt. Da alle Ressourcen in einer einzelnen Gesamtstruktur enthalten sind, enthält eine einzelne Globale Adressliste (GAL)
alle Benutzer für die ganze Gesamtstruktur. In Abbildung 2.1 wird dieses Szenario dargestellt.

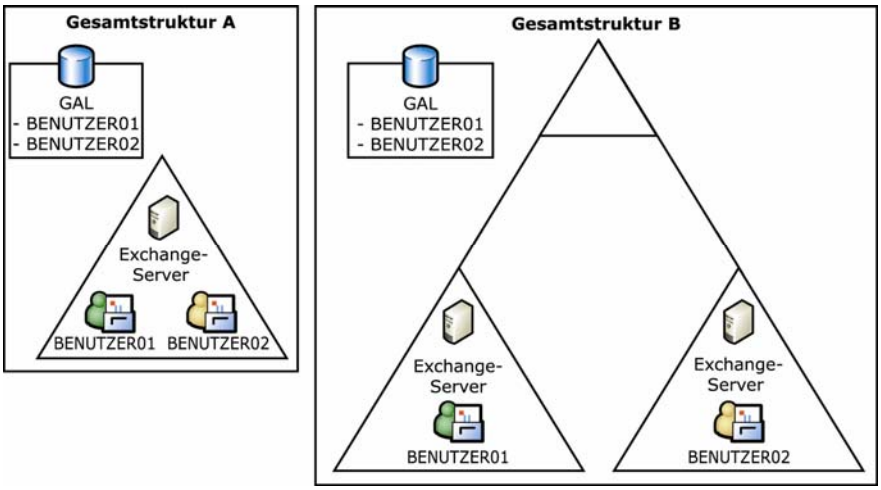


Abbildung 2.1 Zwei Beispiele für die Implementierung von Exchange in einer einzelnen Active Directory-Gesamtstruktur

Die Variante mit einer einzelnen Gesamtstruktur bietet folgende Vorteile:

- Größte Anzahl von Features für das Mailsystem
- Optimales Verwaltungsmodell

- Bestehende Active Directory-Struktur wird genutzt
- Vorhandene Domänencontroller und globale Katalogserver können verwendet werden
- Keine Übermittlung oder Synchronisierung erforderlich

Der Hauptnachteil bei dieser Option besteht darin, dass die Administratoren festlegen müssen, wie die Verantwortlichkeiten für das Verwalten von Active Directory- und Exchange-Objekten aufgeteilt werden.

Dedizierte Exchange-Gesamtstruktur (Ressourcengesamtstruktur)

In einigen Fällen kann es erforderlich sein, eine getrennte Active Directory-Gesamtstruktur einzurichten, die ausschließlich für Exchange reserviert ist. So kann es z. B. vorkommen, dass eine vorhandene Windows NT-Gesamtstruktur beibehalten werden soll. Möglicherweise möchten Sie auch die Verwaltung von Active Directory- und Exchange-Objekten trennen
und möchten daher eine getrennte Active Directory-Gesamtstruktur einrichten, die nur für Exchange vorgesehen ist. Diese Variante empfiehlt sich z. B. bei Unternehmen, in denen Sicherheitsgrenzen zwischen der Active Directory- und Exchange-Verwaltung erforderlich sind.

Die Exchange-Gesamtstruktur (auch als *Ressourcengesamtstruktur* bezeichnet) ist ausschließlich dafür reserviert, Exchange auszuführen und Postfächer zu verwalten.
Die Benutzerkonten sind in einer oder mehreren Gesamtstrukturen enthalten, die als *Kontengesamtstrukturen* bezeichnet werden und von der Ressourcengesamtstruktur getrennt sind.

Der aktivierte Benutzer der Kontengesamtstruktur ist mit einem Postfach verbunden, das einem deaktivierten Benutzer der Ressourcengesamtstruktur zugeordnet ist. Durch diese Konfiguration wird Benutzern der Zugriff auf Postfächer ermöglicht, die sich in anderen Gesamtstrukturen befinden. In diesem Szenario können Sie eine Vertrauensstellung zwischen der Ressourcengesamtstruktur und der Kontengesamtstruktur einrichten. Unter Umständen müssen Sie außerdem einen Übermittlungsprozess einrichten, damit beim Erstellen eines Benutzers in Active Directory durch einen Administrator gleichzeitig ein deaktivierter Benutzer mit einer Mailbox in Exchange erstellt wird.

> **Hinweis** Wenn die Benutzerkonten einen SID-Verlauf (Security Identifier, Sicherheitserkennung) besitzen, müssen Sie die SID-Filterung zwischen der Kontengesamtstruktur und der Ressourcengesamtstruktur deaktivieren (andernfalls sind die Benutzer nicht in der Lage, auf ihre Postfächer zuzugreifen). In den beiden folgenden Fällen werden für Konten SID-Verläufe gespeichert:
>
> - Wenn Sie zum Migrieren von Exchange 5.5 auf Exchange 2003 dem externen Migrationspfad folgen, wird für jedes neue Konto die alte SID im Attribut **SIDHistory** gespeichert.
> - Wenn Sie mit dem Active Directory-Migrationstool (ADMT) Konten von einer Gesamtstruktur in eine andere verschieben, wird für jedes neue Konto die alte SID im Attribut **SIDHistory** gespeichert.

Da alle Exchange-Ressourcen in einer einzelnen Gesamtstruktur vorhanden sind, enthält eine einzelne GAL alle Benutzer der kompletten Gesamtstruktur. In Abbildung 2.2 wird eine dedizierte Exchange-Gesamtstruktur dargestellt.

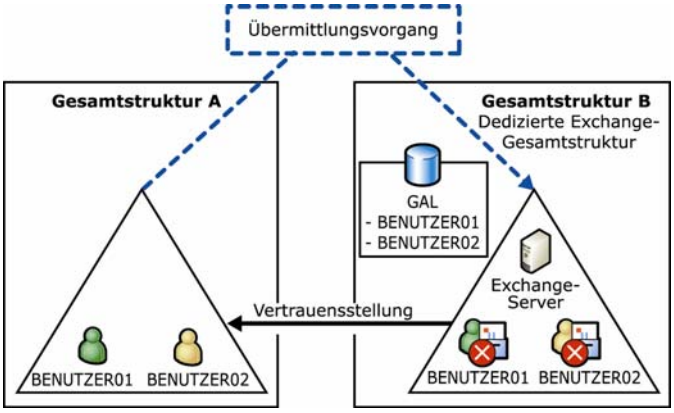


Abbildung 2.2 Getrennte, dedizierte Exchange-Gesamtstruktur

Der Hauptvorteil bei der Variante mit einer dedizierten Exchange-Gesamtstruktur liegt darin, dass eine Sicherheitsgrenze zwischen der Active Directory- und der Exchange-Verwaltung besteht.

Bei dieser Option ergeben sich jedoch beispielsweise folgende Nachteile:

- Die Vorteile einer Integration der Exchange- und Active Directory-Verwaltung werden nicht ausgenutzt, so dass sich ein Verwaltungsmehraufwand ergibt.
- An Microsoft Windows®-Standorten, an denen Exchange ausgeführt werden soll, müssen alle Domänencontroller und globalen Katalogserver jeweils doppelt vorhanden sein, wodurch erhöhte Kosten entstehen.
- Es muss ein Übermittlungsprozess vorhanden sein, damit Active Directory-Aktualisierungen in Exchange übernommen werden. (So muss z. B. beim Erstellen eines neuen Active Directory-Benutzers in Gesamtstruktur A ein postfachaktiviertes Platzhalterobjekt mit entsprechenden Berechtigungen erzeugt werden.) Wenn Sie in einer Gesamtstruktur ein Objekt erstellen, müssen Sie darauf achten, in der anderen Gesamtstruktur ebenfalls entsprechende Objekte zu erstellen. Wenn Sie beispielsweise in einer Gesamtstruktur einen Benutzer erstellen, stellen Sie sicher, dass in der anderen Gesamtstruktur ein Platzhalter für diesen Benutzer erstellt wird. Sie können die entsprechenden Objekte manuell erstellen, diesen Vorgang durch Skripts automatisieren oder dafür Software von Drittanbietern einsetzen.

  Wichtig Die GAL-Synchronisierungsfunktion von Microsoft Identity Integration Server 2003 (MIIS 2003) wurde nicht für das Modell mit einer Ressourcengesamtstruktur entwickelt. (Bei diesem befindet sich das Benutzerkonto in einer anderen Gesamtstruktur als das dazugehörige Postfach.) Obwohl Sie die GAL-Synchronisierung von MIIS 2003 nicht verwenden können, können Sie MIIS 2003 so konfigurieren, dass Objekte zwischen einer Ressourcengesamtstruktur und einer Kontengesamtstruktur übermittelt werden. Darüber hinaus können Sie mit der GAL-Synchronisierung die Ressourcengesamtstruktur mit anderen Exchange-Gesamtstrukturen synchronisieren (mit Ausnahme der Kontengesamtstruktur).

Eine andere Variante der Ressourcengesamtstruktur sind mehrere Gesamtstrukturen, bei denen in einer Gesamtstruktur Exchange ausgeführt wird. Wenn mehrere Active Directory-Gesamtstrukturen vorhanden sind, hängt die optimale Bereitstellungsmethode für Exchange vom Grad der Autonomie ab, der zwischen den einzelnen Gesamtstrukturen erforderlich ist. In Unternehmen, in denen Sicherheitsgrenzen (getrennte Gesamtstrukturen) für Verzeichnisobjekte erforderlich sind, Exchange-Objekte jedoch freigegeben werden dürfen, kann es empfehlenswert sein, Exchange in einer der Gesamtstrukturen bereitzustellen und dort auch die Postfächer für die anderen Gesamtstrukturen im Unternehmen einzurichten. Da alle Exchange-Ressourcen in

einer einzelnen Gesamtstruktur enthalten sind, enthält eine einzelne GAL alle Benutzer in allen Gesamtstrukturen. In Abbildung 2.3 wird dieses Szenario dargestellt.

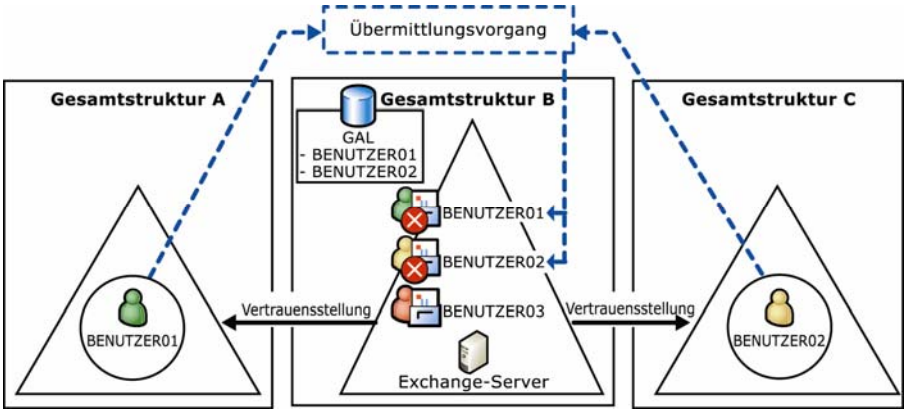


Abbildung 2.3 Mehrere Active Directory-Gesamtstrukturen, wobei in einer Gesamtstruktur Exchange ausgeführt wird

Bei dieser Option ergeben sich folgende Vorteile:

- Bestehende Active Directory-Struktur wird genutzt
- Vorhandene Domänencontroller und globale Katalogserver können verwendet werden
- Einhaltung strenger Sicherheitsgrenzen zwischen Gesamtstrukturen

Bei dieser Option ergeben sich jedoch beispielsweise folgende Nachteile:

- Es muss ein Übermittlungsprozess vorhanden sein, damit Active Directory-Aktualisierungen in Exchange übernommen werden. (So muss z. B. beim Erstellen eines neuen Active Directory-Benutzers in Gesamtstruktur A ein postfachaktiviertes, deaktiviertes Objekt mit entsprechenden Berechtigungen in Gesamtstruktur B erzeugt werden.)
- Gesamtstrukturadministratoren müssen festlegen, wie die Verantwortlichkeiten für die Verwaltung der Active Directory- und Exchange-Objekte aufgeteilt werden sollen.

Mehrere Gesamtstrukturen, in denen Exchange ausgeführt wird

Obwohl eine Topologie mit einer einzelnen Gesamtstruktur empfohlen wird, da sie die größte Anzahl von Messagingfunktionen bietet, sprechen verschiedene Gründe für eine Topologie mit mehreren Gesamtstrukturen. Dazu gehören folgende Szenarien:

- In Ihrer Organisation sind mehrere Unternehmensbereiche vorhanden, bei denen eine Trennung der Daten und Dienste erforderlich ist.
- In Ihrer Organisation sind mehrere Unternehmensbereiche mit unterschiedlichen Schemaanforderungen vorhanden.
- Sie haben eine Fusion, Übernahme oder Veräußerung zu bewältigen.

In jedem Fall besteht die einzige Möglichkeit, strenge Grenzen zwischen Unternehmensbereichen einzurichten, im Erstellen einer getrennten Active

Directory-Gesamtstruktur für jede Unternehmenseinheit. Wenn in Ihrer Organisation diese Active Directory-Konfiguration verwendet wird, besteht das bevorzugte Verfahren für die Implementierung von Exchange im Erstellen einer Exchange-Ressourcengesamtstruktur (Abbildung 2.3).

Wenn die Variante mit der Ressourcengesamtstruktur nicht durchführbar ist (z. B. bei Fusionen und Übernahmen oder wenn bereits in mehreren Gesamtstrukturen eigene Instanzen von Exchange ausgeführt werden), können Sie Exchange jedoch über mehrere Gesamtstrukturen implementieren (Abbildung 2.4). Diese Implementierung entspricht der klassischen Konfiguration mit mehreren Gesamtstrukturen. Ein Unternehmen verfügt in diesem Szenario über mehrere Active Directory-Gesamtstrukturen, von denen jede eine Exchange-Organisation enthält. Im Gegensatz zum Szenario mit einer Ressourcengesamtstruktur werden hierbei Benutzerkonten nicht von den zugehörigen Postfächern getrennt. Stattdessen befinden sich ein Benutzerkonto und das zugehörige Postfach in derselben Gesamtstruktur.

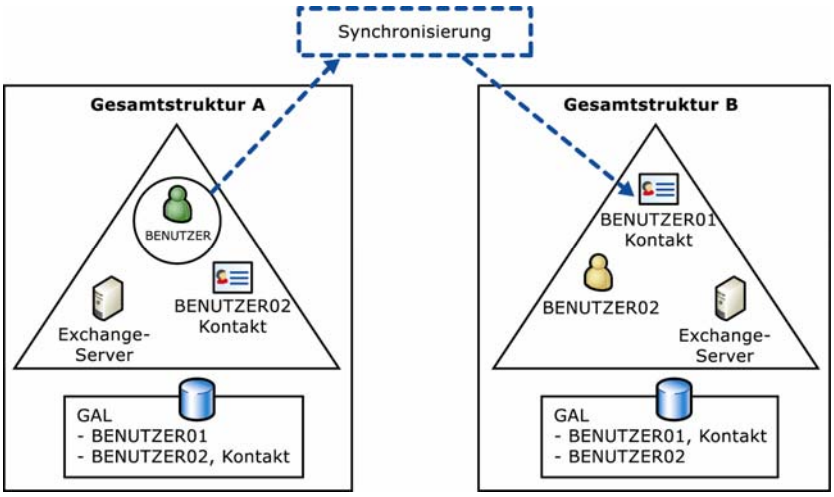


Abbildung 2.4 Bereitstellung von Exchange in mehreren Gesamtstrukturen mit Synchronisierung zwischen den Gesamtstrukturen (klassische Konfiguration mit mehreren Gesamtstrukturen)

Der Hauptvorteil dieses klassischen Szenarios mit mehreren Gesamtstrukturen besteht darin, dass Sie Datentrennung und Sicherheitsgrenzen zwischen den Exchange-Organisationen beibehalten können.

Bei dieser Option ergeben sich jedoch beispielsweise folgende Nachteile:

- Das Szenario mit mehreren Gesamtstrukturen bietet nicht die größte Anzahl an Messagingfunktionen.
- Regeln bleiben bei einer gesamtstrukturübergreifenden Verschiebung nicht erhalten.
- Da ein Benutzer oder eine Gruppe einer anderen Gesamtstruktur als Kontakt dargestellt wird, können Sie den Zugriff auf ein Postfach nicht an eine Person in einer anderen Gesamtstruktur vergeben. In den Zugriffsrechten eines Postfachs können keine Kontakte eingetragen werden.
- Stellvertreterberechtigungen von Postfächern bleiben beim Verschieben eines Postfachs von einer Gesamtstruktur in eine andere nicht erhalten.
- Obwohl Sie Frei/Gebucht-Informationen gesamtstrukturübergreifend synchronisieren und diese dann zur Planung von Besprechungen verwenden können, besteht nicht die Möglichkeit, Kalenderinformationen

eines Benutzers einer anderen Gesamtstruktur in Microsoft Office Outlook® mit der Funktion **Ordner eines anderen Benutzers öffnen** anzuzeigen.

- Da eine Gruppe einer anderen Gesamtstruktur als Kontakt dargestellt wird, können Sie die Gruppenmitglieder nicht anzeigen. Die Gruppenmitgliedschaft wird erst erweitert, wenn eine E-Mail-Nachricht an die Quellgesamtstruktur gesendet wurde.
- Ein Front-End-Server kann für einen Back-End-Server einer anderen Gesamtstruktur nicht als Proxyserver dienen. Diese Einschränkung gilt auch, wenn Sie einen Front-End-Server für Outlook Web Access oder Outlook Mobile Access verwenden.
- Beim Aktualisieren einer Organisation mit mehreren Gesamtstrukturen von Exchange 5.5 auf Exchange 2003 findet ab dem Moment keine Replikation an andere Gesamtstrukturen mehr statt, in dem Sie unter Exchange 5.5 die Connectors für die Verzeichnisreplikation (DRC, Directory Replication Connector) trennen. Dies ist erst wieder möglich, wenn das neue Synchronisierungstool (wie z. B. MIIS 2003) wirksam ist. Dadurch gehen einige Informationen (z. B. die Mitgliedschaft in Verteilerlisten) verloren, und Sie müssen diese erneut manuell eingeben.

Beachten Sie diese Punkte, wenn Sie sich zwischen der Bereitstellung einer einzelnen oder mehrerer Gesamtstrukturen entscheiden. Wenn Sie momentan mit getrennten Exchange 5.5-Standorten arbeiten und die Grenzen beibehalten möchten, sollten Sie die Vor- und Nachteile bei der Bereitstellung von mehreren Active Directory-Gesamtstrukturen und Exchange 2003-Organisationen auswerten.

Weitere Informationen zur Konfiguration von Exchange in einer Umgebung mit mehreren Gesamtstrukturen finden Sie in Kapitel 3 unter „Bereitstellen von Exchange in einer Umgebung mit mehreren Gesamtstrukturen“.

Fusionen und Übernahmen

Bei Fusionen, Übernahmen und Veräußerungen von Unternehmensbereichen kann es notwendig werden, zwei oder mehrere getrennte Exchange-Organisationen zusammenzuführen. Im Verlauf dieses Vorgangs müssen Sie wahrscheinlich für einen gewissen Zeitraum die Koexistenz der Exchange-Organisationen aufrechterhalten, bevor Sie diese zusammenführen können. Die Berücksichtigungen für dieses Szenario ähneln denen eines klassischen Szenarios mit mehreren Gesamtstrukturen. Insbesondere müssen Sie für die Dauer der Koexistenz die Verfügbarkeit von grundlegenden Messagingfunktionen, freigegebene GALs und freigegebene Frei/Gebucht-Informationen sicherstellen.

Das Vorgehen bei der Zusammenführung der Organisationen hängt von den eingesetzten Exchange-Versionen ab:

- Migrieren Sie bei der Zusammenführung von zwei Gesamtstrukturen, in denen Exchange 2000 oder Exchange 2003 ausgeführt wird, Konten mit dem Active Directory-Migrationstool (ADMT) und Postfächer mit dem Assistenten für die Migration (Abbildung 2.5).
- Halten Sie sich bei der Zusammenführung einer Gesamtstruktur, in der Exchange 5.5 ausgeführt wird, mit einer Gesamtstruktur, in der Exchange 2003 ausgeführt wird, an die Richtlinien für eine externe Migration von Exchange 5.5 auf Exchange 2003 (Abbildung 2.6).

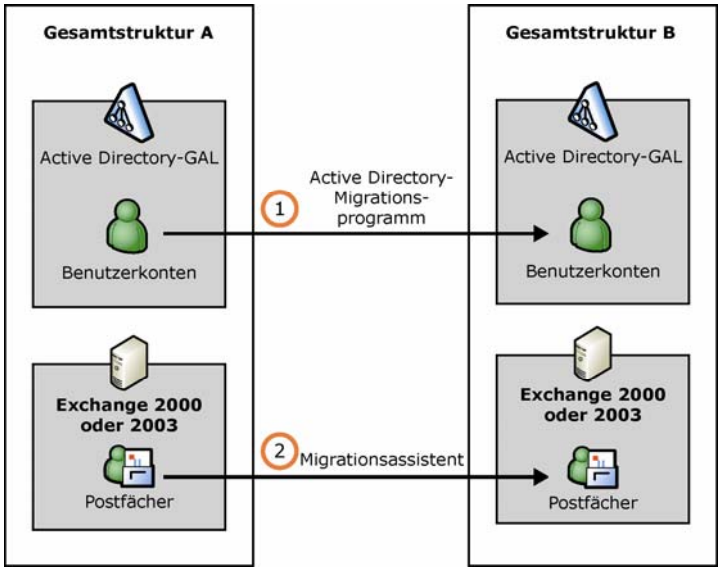


Abbildung 2.5 Zusammenführen von zwei Gesamtstrukturen, in denen Exchange 2000 oder Exchange 2003 ausgeführt wird

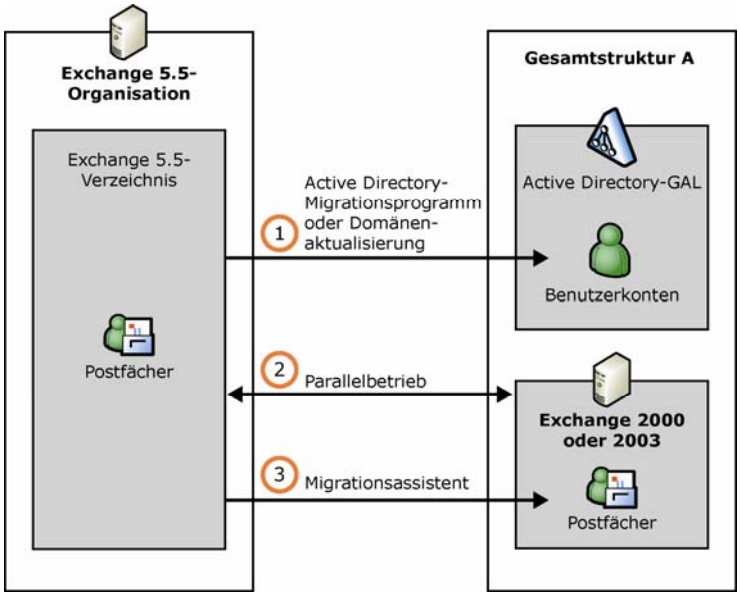


Abbildung 2.6 Zusammenführen einer Exchange 5.5-Gesamtstruktur mit einer Exchange 2003-Gesamtstruktur

Weitere Informationen zum Zusammenführen von Gesamtstrukturen finden Sie in Kapitel 3 unter „Wechsel von Exchange 5.5 zu Exchange 2003“ und „Bereitstellen von Exchange in einer Umgebung mit mehreren Gesamtstrukturen“.

Entscheidung für ein zentralisiertes oder verteiltes Verwaltungsmodell

Abhängig von den bestehenden Verwaltungs- und Sicherheitsanforderungen sowie den vorhandenen technischen Möglichkeiten können Sie ein zentralisiertes oder ein verteiltes Verwaltungsmodell oder eine Kombination aus beiden entwerfen. Diese Entscheidung hat insbesondere Einfluss darauf, ob eine oder mehrere administrative Gruppen eingerichtet werden müssen.

Administrative Gruppen bieten eine Möglichkeit zum Zusammenfassen von Objekten in Gruppen (z. B. Server, Richtlinien, Routinggruppen und Öffentliche Ordner-Hierarchien) und zum Definieren des Umfangs der Berechtigungen für die jeweilige Gruppe. Wenn es in Ihrer Organisation beispielsweise zwei Gruppen von Administratoren gibt, die zwei Exchange-Servermengen verwalten, können Sie zwei administrative Gruppen erstellen, die diese beiden Servermengen enthalten. Wenn Sie Berechtigungen einrichten möchten, können Sie den Sicherheitseinstellungen für die beiden administrativen Gruppen die entsprechenden Windows-Benutzer und -Gruppen hinzufügen. Active Directory übermittelt diese Einstellungen dann an alle Konfigurationsobjekte in der administrativen Gruppe. Zum Festlegen von Exchange-Berechtigungen für die administrativen Gruppen können Sie den Assistenten für die Zuweisung von Verwaltungsberechtigungen auf Exchange-Objekte verwenden. Mit diesem Assistenten wird das Zuweisen von Berechtigungen sowie das Erstellen und Verwalten von Zugriffssteuerungslisten (ACLs) vereinfacht.

Ein zentralisiertes Exchange-Verwaltungsmodell ist durch das Vorhandensein einer einzelnen administrativen Exchange-Gruppe (die Standardgruppe) sowie eine zentralisierte Serververwaltung und Richtlinienverwaltung gekennzeichnet. Beachten Sie, dass in Exchange 2003 das Verwaltungsmodell vollständig unabhängig von der physischen Infrastruktur ist, so dass das Verwaltungsmodell für Exchange auch dann zentralisiert sein kann, wenn in Ihrem Unternehmen mehrere Zweigstellen vorhanden sind. Es kann nur eine administrative Gruppe eingerichtet werden, es dürfen jedoch mehrere Routinggruppen vorhanden sein. Wie unter „Optionen für die Integration von Exchange in Active Directory“ weiter oben in diesem Kapitel beschrieben, können Sie die Variante mit einer einzelnen Gesamtstruktur implementieren, wenn das Verwaltungsmodell stark zentralisiert ist und keine strengen Sicherheitsgrenzen zwischen den einzelnen Unternehmensbereichen erforderlich sind.

Wenn die Exchange-Serververwaltung für einzelne logische Unternehmenseinheiten unabhängig voneinander erfolgen muss, ist u. U. ein verteiltes Modell erforderlich. Bei diesem Modell haben die einzelnen Unternehmensbereiche oder Niederlassungen volle Kontrolle über die Verwaltung der Exchange-Organisation, obwohl Standards und Richtlinien von einer zentralen Gruppe verwaltet werden können. Bei einem dezentralen Modell wird mindestens eine administrative Gruppe für jeden Bereich oder jede Niederlassung eingerichtet. Dieses Modell entspricht dem Standortmodell in früheren Versionen von Exchange und wird oft in Unternehmen mit mehreren unabhängigen Zweigstellen eingesetzt. Sie müssen außerdem entscheiden, ob es ausreicht, Unternehmensbereiche durch Verwendung von administrativen Gruppen zu trennen, oder ob strenge Sicherheitsgrenzen zwischen diesen Bereichen erforderlich sind. Wenn Sicherheitsgrenzen eingerichtet werden sollen, müssen die einzelnen Unternehmensbereiche getrennten Gesamtstrukturen zugeordnet werden, wie im Abschnitt „Optionen für die Integration von Exchange in Active Directory“ weiter oben in diesem Kapitel erläutert.

> **Hinweis** Die Supportkosten für einzelne Zweigstellen können sehr hoch sein. Daher sollten Sie diese Supportkosten gegen die Kosten für Investitionen in bessere Netzwerkverbindungen und eine Zentralisierung von Servern abwägen.

Bei einem gemischten Modell ist es möglich, die Verantwortung für die Verwaltung verschiedener geografischer Standorte auf spezialisierte administrative Gruppen aufzuteilen und gleichzeitig eine

zentralisierte administrative Gruppe für unternehmensweite Verantwortlichkeiten zuzuweisen. In diesem Fall legen
die Administratoren einer zentralisierten Gruppe für Organisationsrichtlinien unternehmensweite System- und Empfängerrichtlinien fest. In den Gruppen für
die einzelnen Zweigstellen werden tägliche Verwaltungsaufgaben definiert, die Administratoren an den verschiedenen geografischen Standorten ausführen. Jede
dieser Gruppen enthält weitere Objekte, wie Öffentliche Ordner und Server, die
von den lokalen Gruppen verwaltet werden.

> **Wichtig** Wenn Sie mit einer gemischten Exchange-Organisation arbeiten, d. h. mit Exchange 2000- oder Exchange 2003- und Exchange 5.5-Servern, wird in Exchange in der Standardeinstellung für jeden Exchange 5.5-Standort eine administrative Gruppe und eine Routinggruppe angezeigt.

Funktionen und Berechtigungen

Das flexible Zuweisen von Funktionen und Berechtigungen zu Administratoren unter Windows Server 2003 und Exchange eröffnet eine Vielzahl von Möglichkeiten zum Verwalten von Empfängern, Servern und Richtlinien. Zusätzlich zu den in Kapitel 1 behandelten Anforderungen müssen Sie berücksichtigen, wie die nachstehenden Funktionen von Active Directory und Exchange 2003 Ihre Strukturierung der administrativen Funktionen beeinflusst:

- Ein einzelner Administrator kann Aufgaben sowohl für Windows 2003 Server
  als auch für Exchange ausführen.
- Sie können Benutzer nach Sicherheitsaspekten, Berechtigungen, dem Standort, Domänen, Strukturen oder anderen Anforderungen organisieren und verwalten.
- Sie können Benutzer- und Gruppenzugriff nach Objektklasse zuweisen. Beispielsweise können Sie Administratoren die Berechtigung zum Anzeigen
  des Status des Postfachspeichers gewähren, nicht jedoch der Größe des Postfachs eines Benutzers.

Empfängerverwaltung und Serververwaltung

Mit der Einführung von Active Directory können Sie die Verwaltung von Servern und die Verwaltung von Empfängern trennen. Empfänger sind als Active Directory-Objekte wie beispielsweise Benutzer, Gruppen und Kontakte definiert. Sie erstellen in Active Directory-Benutzer und -Computer Postfächer, neue Benutzer und Verteilergruppen und führen zugehörige Aufgaben durch, da diese Objekte in Active Directory enthalten sind und von Active Directory verwaltet werden. Sie können jedoch Server, Connectors, Öffentliche Ordner, Adresslisten, Protokolle und Richtlinien im Exchange System-Manager konfigurieren.

Legen Sie fest, wer Verwaltungsaufgaben durchführt, beispielsweise die Verwaltung
der Benutzerkonten und den täglichen Betrieb von Exchange. Weil Active Directory von Exchange und Windows verwendet wird, sind einige dieser Aufgaben Erweiterungen der Verwaltung von Windows Server. Wenn eine Person alle Windows-Benutzer verwaltet, können Sie dieser Person auch die Verwaltung der Exchange-Empfänger übertragen, weil diese Aufgaben in einem engen Zusammenhang stehen. Wenn die administrativen Aufgaben für unterschiedliche Benutzer- und Servergruppen von verschiedenen Personen durchgeführt werden, können Sie mehrere administrative Gruppen einrichten, damit bei besonderen Umständen das Zuweisen von Berechtigungen zu einer Gruppe von Exchange-Objekten erleichtert wird.

Verwaltung und Routing

Legen Sie fest, wer in Ihrem Exchange-System für Verwaltung und Routing verantwortlich sein soll. Nach der Installation von Exchange wird anfangs der gemischte Modus verwendet, so dass Server, auf denen frühere Versionen von Exchange ausgeführt werden, in der Exchange-Organisation koexistieren können. Exchange-Organisationen, für

die keine weitere Koexistenz mit früheren Versionen von Exchange erforderlich ist, können im einheitlichen Modus betrieben werden. Beim Verwaltungsmodell für Organisationen im einheitlichen Modus werden Routing und Verwaltung getrennt: Sie können Server in administrativen Gruppen strukturieren, um Berechtigungen zu verwalten und Systemrichtlinien anzuwenden, und
Sie können Server zu Routinggruppen zuweisen, die sich über mehrere administrative Gruppen erstrecken, so dass der Nachrichtenverkehr so effizient wie möglich verwaltet
wird. Weitere Informationen zu administrativen Gruppen und Routinggruppen finden Sie unter „Routing-Entwurf“ in Kapitel 5.

Datenverwaltung

Legen Sie fest, wer Postfachspeicher und Informationsspeicher für Öffentliche Ordner verwalten soll. Je nachdem, wie Sie Ihr System strukturieren, ist die Öffentliche Ordner-Hierarchie innerhalb der Organisation möglicherweise nach Unternehmensbereichen oder Niederlassungen unterteilt. Sie können Berechtigungen verwenden, um festzulegen, wer die Öffentliche Ordner-Hierarchie in Ihrer Organisation verwaltet. Die Verantwortung für Sicherungs- und Wiederherstellungsaufgaben kann Exchange-Administratoren oder einer anderen Gruppe übertragen werden. Weitere Informationen zur Datenverwaltung und
zum Sichern von Ressourcen finden Sie in Kapitel 6, „Einplanen hoher Verfügbarkeit“.

Interoperabilität mit Exchange 5.5

Die Postfachverwaltung umfasst das Erstellen, Bearbeiten und Löschen von Postfächern, E-Mail-Adressen und zugehörigen Eigenschaften. In Exchange 2000 und Exchange 2003 ist die Postfachverwaltung in die Active Directory-Empfängerverwaltung integriert.

Verwaltung Öffentlicher Ordner

Ihre Entscheidungen hinsichtlich der Verwaltung Öffentlicher Ordner werden von der Netzwerkinfrastruktur, den Sicherheitsanforderungen und dem Verwaltungsmodell bestimmt. Von der Verwaltung Öffentlicher Ordner sind nicht nur Öffentliche Ordner, sondern auch Systemordner betroffen. Zu diesen Systemordnern gehört auch der Frei-/Gebucht-Ordner, über den gesteuert wird, ob Sie beim Einrichten einer Besprechung die Frei-/Gebucht-Informationen anderer Benutzer einsehen können. Wenn Sie die in Kapitel 1 vorgestellten Konzepte und die vorangegangenen Themen dieses Kapitels durchgearbeitet haben, verfügen Sie über ein gutes Verständnis Ihrer bestehenden Infrastruktur und der Punkte, die Auswirkungen auf das Verwaltungsmodell haben.

Mit den nachstehenden Funktionen Öffentlicher Ordner wird Ihnen die Verwaltung Öffentliche Ordner erleichtert:

- **Replikation** Ein Öffentlicher Ordner kann so konfiguriert werden, dass er Kopien (Replikate) auf mehreren Servern besitzt. Replikate eignen sich zum Verteilen
der Benutzerauslastung auf Servern, zum Verteilen Öffentlicher Ordner auf geografische Bereiche und zum Sichern der Daten Öffentlicher Ordner. Sie können einen Replikationsplan einrichten, der auf der Häufigkeit von Datenänderungen im Öffentlichen Ordner basiert. Sie können diesen Zeitplan für alle Öffentlichen Ordner oder für einen bestimmten Öffentlichen Ordner festlegen.
- **Öffentliche Ordner-Verweise** Wenn ein Clientcomputer einen anderen Server für den Zugriff auf die Inhalte des Öffentlichen Ordners einsetzen muss, wird von Exchange die Routinggruppenkonfiguration verwendet, um den Clientcomputer
an den anderen Server zu verweisen. Dieser alternative Server kann sich in einer anderen Routinggruppe befinden. Durch das Verwenden von Öffentliche Ordner-Verweisen können Benutzer auf Inhalte an beliebiger Stelle zugreifen, selbst wenn der angegebene, die Daten enthaltende Server unbekannt ist. Auf diese Weise

ist auch keine kostenbasierte Verweisliste mehr erforderlich, da die Kosten anhand der Connectorkosten für die Routinggruppe ermittelt werden.

Replikation Öffentlicher Ordner

Ein Öffentlicher Ordner kann so konfiguriert werden, dass er über Replikate auf mehreren Servern für Öffentliche Ordner verfügt. Replikate eignen sich zum Verteilen der Benutzerauslastung auf Servern, zum geografischen Verteilen Öffentlicher Ordner und für die Ausfallsicherheit der Daten Öffentlicher Ordner. Alle Replikate eines Öffentlichen Ordners sind gleich. Dies bedeutet, dass es kein Masterreplikat gibt.

Während der Replikation Öffentlicher Ordner wird die Öffentliche Ordner-Hierarchie auf jeden Server repliziert, für den in der Exchange-Organisation Öffentliche Ordner vorhanden sind. Die Inhalte werden jedoch nur auf Server repliziert, auf denen von einem Administrator Replikate eingerichtet wurden. Änderungen, die an Objekten in einem Replikat vorgenommen wurden, werden an alle anderen Replikate des Öffentlichen Ordners in der gesamten Organisation gesendet. Änderungen, die am Ordner, an den Eigenschaften des Ordners oder an der Öffentliche Ordner-Hierarchie vorgenommen wurden, werden auf alle Server repliziert.

Sind mehrere Replikate eines Öffentlichen Ordners vorhanden, werden von Benutzern hergestellte Verbindungen auf alle Replikate in einer Organisation verteilt. Wenn ein Replikat des Ordners auf dem Server für Öffentliche Ordner des Benutzers vorhanden ist, erfolgt der erste Verbindungsversuch mit diesem Replikat. Wenn die Verbindung mit dem Replikat nicht hergestellt werden kann, weil der Server nicht verfügbar ist oder eine Netzwerkverbindung nicht erfolgen kann, wird versucht, eine Verbindung zu einem anderen Server herzustellen. Wenn Routingconnectors Verweise auf Öffentliche Ordner aktivieren, werden Verbindungsversuche mit Servern in anderen Routinggruppen unternommen.

Planungsaspekte

In diesem Abschnitt werden spezifische Planungsaspekte und Empfehlungen für Öffentliche Ordner behandelt.

Dedizierte Server für Öffentliche Ordner

Zum Senden von Replikationsnachrichten für den Informationsspeicher für Öffentliche Ordner wird die E-Mail-Übertragung verwendet. Vom Informationsspeicher für Öffentliche Ordner werden Nachrichten nicht auf der Grundlage von Topologieinformationen repliziert. Wenn der Inhalt eines Öffentlichen Ordners geändert wird und über fünf Replikate verfügt, wird eine einzige Replikationsnachricht erzeugt und an alle fünf weiteren Informationsspeicher für Öffentliche Ordner adressiert. Aus diesem Grund hat die Routingtopologie großen Einfluss darauf, wie effizient Öffentliche Ordner repliziert werden.

Bei administrativen Gruppen mit mehr als drei Servern wird zum Trennen der Datenübertragungen für die Replikation Öffentlicher Ordner und dem E-Mail-Datenaufkommen in der Regel empfohlen, einen dedizierten Server für Öffentliche Ordner bereitzustellen. Durch das Bereitstellen eines dedizierten Servers für Öffentliche Ordner wird das Netzwerkaufkommen für Replikationen reduziert und die Verwaltung Öffentlicher Ordner vereinfacht. Löschen Sie nach dem Einrichten eines dedizierten Servers für Öffentliche Ordner die Informationsspeicher für Öffentliche Ordner auf den Postfachservern. Auf dem Server für Öffentliche Ordner hingegen müssen sich keine Postfächer befinden, doch für E-Mail-aktivierte Öffentliche Ordner ist ein Postfachspeicher erforderlich. Konfigurieren Sie anschließend die Postfachspeicher der Benutzer so, dass standardmäßig der dedizierte Server für Öffentliche Ordner verwendet wird.

Platzierung Öffentlicher Ordner

Wenn Ihre Exchange-Organisation aus mehreren voneinander entfernten Standorten besteht, stehen für Öffentliche Ordner zwei Optionen zur Auswahl. Sie können Replikate der Öffentlichen Ordner auf den lokalen Exchange-Servern platzieren, so dass jeder Standort über ein Replikat der Öffentlichen Ordner der anderen Standorte verfügt.
Sie können auch alle Informationen der Öffentlichen Ordner auf einem zentralen
Server im Datenzentrum oder Hub speichern, so dass nur eine einzelne, korrekte Datenquelle vorhanden ist.
Für die Auswahl der für Sie geeigneten Option müssen
Sie Datenzuverlässigkeit und Komfort gegeneinander abwägen. Außerdem ist die Entscheidung von den Benutzeranforderungen und dem Nutzungsverhalten abhängig.

Wenn Sie Ihre Exchange-Server zentralisieren möchten, werden Sie sich möglicherweise gegen die Installation eines Exchange-Servers für Öffentliche Ordner
in Remotestandorten entscheiden. Sie sollten jedoch beachten, dass der Zugriff auf Öffentliche Ordner nicht im gleichen Maße vom Exchange-Cachemodus profitiert
wie der Postfachzugriff, wenn die Standorte über Netzwerkverbindungen mit
niedriger Bandbreite und hohen Wartezeiten miteinander verbunden sind. Anders als Postfachdaten werden die Daten Öffentlicher Ordner nicht lokal auf dem Clientcomputer gespeichert (es sei denn, Sie fügen Ihren Offline-Favoriten einen Öffentlichen Ordner hinzu, da diese mit den Serverdaten synchronisiert werden). Anforderungen von Daten aus Öffentlichen Ordnern werden daher über die Remoteverbindung an einen Exchange-Server im Datenzentrum gerichtet. Dies bedeutet, dass der Zugriff auf Öffentliche Ordner von den Wartezeiten der Netzwerkverbindung abhängig ist.

Wenn keine lokalen Exchange-Server für Öffentliche Ordner vorhanden sind und der Serverzugriff über eine Verbindung mit niedriger Bandbreite und hohen Wartezeiten erfolgt, empfiehlt es sich, dass Benutzer auf Öffentliche Ordner mit Outlook Web Access 2003 zugreifen. Im Vergleich zu Outlook bietet Outlook Web Access in der
Regel schnelleren Zugriff auf Öffentliche Ordner, wenn kein lokaler Exchange-Server
für Öffentliche Ordner vorhanden ist.

> **Hinweis** Wenn Sie den Exchange-Cachemodus verwenden, werden für Benutzer
> von Outlook 2003 die Daten Öffentlicher Ordner nicht lokal zwischengespeichert. Anforderungen von Daten aus Öffentlichen Ordnern werden über die Remoteverbindung an einen Exchange-Server gerichtet. Das bedeutet, diese Anforderungen unterliegen ebenfalls den verbindungsspezifischen Wartezeiten. In den meisten Fällen ist ein Sofortzugriff auf Daten in Öffentlichen Ordnern nicht zwingend erforderlich. Sie
> sollten diese Anforderung jedoch beim Testen der Exchange-Infrastruktur in Ihre Betrachtungen einbeziehen und bei der Entscheidung berücksichtigen, ob diese Wartezeiten akzeptabel sind.

Platzierung von Systemordnern

Jeder Informationsspeicher für Öffentliche Ordner enthält Systemordner, die im Exchange System-Manager standardmäßig nicht sichtbar sind. (Klicken Sie zum Anzeigen der Systemordner unter **Ordner** mit der rechten Maustaste auf **Öffentliche Ordner**, und klicken Sie dann auf **Systemordner anzeigen**.) Zu den Systemordnern gehören u. a. die folgenden:

- Schedule+ Frei/Gebucht-Ordner
- Offlineadressbuch-Ordner

Schedule+ Frei/Gebucht-Ordner

Der Schedule+ Frei/Gebucht-Ordner enthält Informationen, die von Outlook-Benutzern verwendet werden können, um beim Planen von Besprechungen die Verfügbarkeit
der gewünschten Teilnehmer anzuzeigen. Für jede administrative Gruppe existiert

ein Frei/Gebucht-Ordner. Wenn für Ihr Verwaltungsmodell mehrere administrative Gruppen erforderlich sind, können Sie den Schedule+ Frei/Gebucht-Ordner so konfigurieren, dass darin Replikate der Frei/Gebucht-Ordner beliebiger oder aller anderen administrativen Gruppen geführt werden. Die Replikation erfolgt analog zu
der für Öffentliche Ordner. Da für jede administrative Gruppe ein Frei/Gebucht-Ordner zur Verfügung steht und eine administrative Gruppe sich über mehrere Routinggruppen erstrecken kann, ist es unter Umständen erforderlich, jeder Routinggruppe ein Ordnerreplikat hinzuzufügen. Auf diese Weise wird sichergestellt, dass Frei/Gebucht-Informationen immer lokal gespeichert sind. Überprüfen Sie unbedingt, ob für die Routinggruppenconnectors Öffentliche Ordner-Verweise zugelassen sind.

Der Zugriff auf die Frei/Gebucht-Informationen gehört zu den wichtigsten Vorüberlegungen. Beziehen Sie zuerst die Punkte Netzwerkverbindung und Bandbreite in Ihre Überlegungen ein. Wägen Sie diese anschließend gegen die Art und Weise ab, wie Benutzer Besprechungen planen, und bestimmen Sie dann den für Ihr Unternehmen vertretbaren Grad der Verzögerung. Für Frei/Gebucht-Informationen bedeutet dies, dass beim Planen von Besprechungen Verzögerungen beim Empfang der Frei/Gebucht-Informationen anderer Benutzer auftreten können, wenn Benutzer nicht über Zugriff auf eine lokale Kopie der Frei/Gebucht-Ordnerdaten verfügen. Wenn es von entscheidender Bedeutung ist, dass Benutzer an einem bestimmten Standort ständig Zugang zu aktuellen Planungsinformationen besitzen, müssen die Frei/Gebucht-Ordner zentral abgelegt werden, selbst wenn dies Verzögerungen für Benutzer mit sich bringt, die diese Informationen über Verbindungen mit geringer Bandbreite abrufen. Wenn schneller Zugriff auf Frei/Gebucht-Informationen wichtiger ist als das Bedürfnis
nach stets aktuellen Informationen, können Sie die Frei/Gebucht-Ordner auf lokalen Exchange-Servern einrichten.

Wenn Sie sich für diese Variante entscheiden, müssen Sie darüber hinaus festlegen, ob
auf dem lokalen Server Kopien der Frei/Gebucht-Ordner der jeweils anderen Standorte geführt werden sollen. Wenn Benutzer an verschiedenen Standorten nur selten gemeinsame Besprechungen planen, müssen nicht unbedingt lokale Replikate der Frei/Gebucht-Ordner anderer Standorte geführt werden.

> **Hinweis** Wie bei den Daten Öffentlicher Ordner werden Frei/Gebucht-Daten
> für Benutzer von Outlook 2003 nicht lokal zwischengespeichert, wenn Sie den Exchange-Cachemodus verwenden. Frei/Gebucht-Anforderungen unterliegen daher den Wartezeiten der Remoteverbindung.

Offlineadressbuch-Ordner

Der Offlineadressbuch-Ordner enthält Unterordner, in denen Offlineadresslisten gespeichert sind. Es empfiehlt sich, zum Erzeugen und Aktualisieren der Offlineadresslisten einen geeigneten Server auszuwählen. Wählen Sie zur Steigerung der Serverleistung einen Server aus, der nicht mit dem Ausführen anderer Aufgaben beschäftigt ist.

Bei Verwendung des Exchange-Cachemodus müssen Sie die Auswirkungen auf den Server berücksichtigen, die beim Download von Offlineadresslisten durch die Benutzer entstehen. Diese können erheblich sein, und zwar nicht nur beim jeweils ersten Download von Offlineadresslisten, sondern auch im täglichen Betrieb. Unter Umständen empfiehlt sich
das Einrichten von ein bis zwei Servern für die Verwaltung von Offlineadressbüchern.

Konfigurieren von Verweisen

Wie in Exchange 2000 sind Öffentliche Ordner-Verweise in Exchange 2003 transitiv.
Das bedeutet, wenn Öffentliche Ordner-Verweise zwischen den Routinggruppen A und B sowie den Routinggruppen B und C zulässig sind, gilt dies automatisch auch für Öffentliche Ordner-Verweise zwischen den Routinggruppen A und C. In Exchange 2000 mussten Sie zum Regulieren des Datenaufkommens zu Öffentlichen Ordnern separate Routinggruppen erstellen, die die Server für Öffentliche Ordner beinhalteten. Grund dafür war, dass Öffentliche Ordner-Verweise nur auf der Ebene der Routinggruppenconnectors aktiviert oder deaktiviert werden konnten. In Exchange 2003 können Verweise jedoch stattdessen auf Serverebene konfiguriert werden. Für jeden Exchange 2003-Server können Sie eine Liste der Server auswählen, zu denen Verweise zulässig sind. Sie

müssen daher nicht länger separate Routinggruppen erstellen, nur um Öffentliche Ordner-Verweise aktivieren oder deaktivieren zu können.

In einer durch schnelle Netzwerkverbindungen gekennzeichneten Topologie stellt das Datenaufkommen durch Verweise unter Umständen kein Problem dar. In der Standardeinstellung können Server Verweise zu allen anderen Servern durchführen. Solange schnelle und verlässliche Verbindungen bestehen, treten keine Probleme wegen zu hohem Datenaufkommen auf. Wenn jedoch Exchange-Server mit Replikaten Öffentlicher Ordner an Remotestandorten eingesetzt werden, deren Verbindungen hohe Wartezeiten aufweisen, empfiehlt es sich unter Umständen, das Öffentliche Ordner-Verweismodell anzupassen. Dazu werden bestimmte Server festgelegt, die Verweise entgegennehmen können.

Planen des Bereitstellungspfads

Die geeignetste Vorgehensweise zum Bereitstellen von Microsoft® Exchange Server 2003 ist abhängig davon, ob in der jeweiligen Organisation derzeit bereits eine ältere Version von Exchange im Einsatz ist. Das Aktualisieren von einer bestehenden Exchange 2000-Organisation ist relativ einfach. Die Migration von einer Exchange 5.5-Organisation auf Exchange 2003 erfordert jedoch zusätzliche Planung, da die Verzeichnisinformationen auf den Microsoft Active Directory®-Verzeichnisdienst und die Daten des Messagingsystems auf Exchange 2003 migriert werden müssen.
Im Allgemeinen stellt die zum Bereitstellen von Exchange 2003 und zum Migrieren der Daten des Verzeichnis- und Messagingsystems erforderliche Zeit für kleinere Unternehmen eine geringere Hemmschwelle dar. Für größere Unternehmen, bei denen die gleichzeitige Aktualisierung aller Standorte technisch unmöglich ist, kann die Bereitstellung jedoch Wochen und sogar Jahre in Anspruch nehmen. Sie müssen in jedem Fall die Exchange-Version des Active Directory Connectors (ADC) einsetzen, damit die Koexistenz zwischen den unterschiedlichen Organisationen gewahrt bleibt, bis alle Standorte von Exchange 5.5 aktualisiert sind.

Ermitteln Sie den für Sie am besten geeigneten Bereitstellungspfad, indem Sie die folgenden Fragen beantworten:

- Wird derzeit in Ihrer Organisation Exchange 5.5, Exchange 2000 oder eine Kombination der beiden Anwendungen eingesetzt?
- Empfiehlt es sich, Nachrichtendaten von einem anderen Messagingsystem als Exchange zu migrieren?
- Können Sie im Falle einer Migration von einer Exchange 5.5-Organisation kurz nach der Migration und vorübergehenden Koexistenz zu Exchange 2003 wechseln, oder müssen Sie einen längeren Zeitraum der Koexistenz einplanen?
- Wie lange würde es dauern, bis Sie zum einheitlichen Modus von Exchange 2003 wechseln können? Kann das Unternehmen bis zu diesem Zeitpunkt auf bestimmte Features verzichten?

In diesem Kapitel werden anhand dieser Schlüsselfragen die unterschiedlichen Bereitstellungspfade von Exchange 2003 vorgestellt. Außerdem werden die für die einzelnen Situationen empfohlenen Bereitstellungspfade behandelt.

Das Ziel: Ausführen von Exchange 2003 im einheitlichen Modus

Eine Exchange 2003-Organisation kann in zwei Modi betrieben werden: Einheitlicher und gemischter Modus. Im einheitlichen Modus steht der volle Funktionsumfang von Exchange 2003 zur Verfügung. Der gemischte Modus bietet dafür Interoperabilität mit Exchange 5.5. Bei der Installation von Exchange 2003 befindet sich Ihre Exchange-Organisation standardmäßig im gemischten Modus. Durch diese Standardeinstellung wird die weitere Interoperabilität mit Exchange 5.5 sichergestellt.

Der einheitliche Modus in Exchange 2003 entspricht im Wesentlichen dem einheitlichen Modus in Exchange 2000. (Die wenigen Ausnahmen sind in Tabelle 3.1 dargestellt.) Ausschlaggebend dafür, ob der einheitliche Modus verwendet werden kann, ist das Vorhandensein von Exchange 5.5-Servern. Wenn daher die von Ihnen verwendete Organisation eine Mischung aus Exchange 2000- und Exchange 2003-Servern, jedoch keine Exchange 5.5-Server enthält, können Sie die Exchange-Organisation im einheitlichen Modus betreiben.

Hinweis Es besteht keine direkte Beziehung zwischen dem Modus der Microsoft Windows®-Domäne und dem Modus einer Exchange-Organisation. Eine Ähnlichkeit besteht nur in Bezug auf die Benennung und auf Einschränkungen bei früheren Versionen.

Vorteile des einheitlichen Modus

Durch das Ausführen einer Exchange-Organisation im einheitlichen Modus steht Ihnen die vollständige Flexibilität von Exchange 2003 bei der Verwaltung Ihres Messagingsystems zur Verfügung.

Möglichkeiten beim Ausführen von Exchange 2003-Servern im einheitlichen Modus:

- Entfernen von ADC und SRS (Site Replication Service, Standortreplikationsdienst)
- Umbenennen der administrativen Gruppen
- Konsolidieren von administrativen Gruppen sowie Festlegen von Routinggruppen und administrativen Gruppen mit verbesserter Flexibilität
- Verschieben von Postfächern zwischen Servern in unterschiedlichen administrativen Gruppen

Einige für Exchange 2003 spezifische Features sind nur verfügbar, wenn die Exchange-Organisation im einheitlichen Modus ausgeführt wird:

- **Abfragebasierte Verteilergruppen** Eine abfragebasierte Verteilergruppe bietet dieselbe Funktionalität wie eine normale Verteilergruppe, doch statt der Festlegung einer statischen Mitgliedschaft von Benutzern können Sie in einer abfragebasierte Verteilergruppe eine LDAP-Abfrage (Lightweight Directory Access Protocol) für dynamische Mitgliedschaften verwenden. Abfragebasierte Verteilergruppen arbeiten zuverlässig in einer reinen Exchange 2003-Umgebung oder einer einheitlichen Exchange 2000- und Exchange 2003-Umgebung, in der alle Exchange 2000-Server mit Service Pack 3 (SP3) und globalen Katalogservern unter Microsoft Windows Server™ 2003 ausgeführt werden. Obwohl abfragebasierte Verteilergruppen auch unter Microsoft Windows 2000 Server eingesetzt werden können, ist die Leistungsfähigkeit unter Windows Server 2003 erheblich besser.
- **InetOrgPerson** Die InetOrgPerson-Objektklasse wird in einigen nicht von Microsoft stammenden LDAP- und X.500-Verzeichnisdiensten verwendet, um Personen innerhalb einer Organisation darzustellen. InetOrgPerson-Objekte werden in Exchange 2003 unterstützt, um die Migration von anderen LDAP-Verzeichnissen zu Active Directory effizienter durchführen zu können. Sie können ein InetOrgPerson-Objekt nur erstellen, wenn Sie einen Windows Server™ 2003-Domänencontroller einsetzen. InetOrgPerson-Objekte können nur in einer einheitlichen Exchange 2003-Organisation postfachaktiviert oder E-Mail-aktiviert sein.

In Tabelle 3.1 werden die im einheitlichen und gemischten Modus verfügbaren Features zusammengefasst.

Tabelle 3.1 Im einheitlichen und gemischten Modus verfügbare Features

Feature	Verfügbar in gemischten Exchange 5.5-, Exchange 2000- und Exchange 2003-Organisationen?	Verfügbar im einheitlichen Exchange 2003- oder Exchange 2000-Modus?	Verfügbar in reinen Exchange 2003-Organisationen im einheitlichen Modus?
Verschieben von Postfächern zwischen Servern in derselben administrativen Gruppe	Ja	Ja	Ja

Feature	Verfügbar in gemischten Exchange 5.5-, Exchange 2000- und Exchange 2003-Organisationen?	Verfügbar im einheitlichen Exchange 2003- oder Exchange 2000-Modus?	Verfügbar in reinen Exchange 2003-Organisationen im einheitlichen Modus?
Verschieben von Postfächern zwischen Servern in unterschiedlichen administrativen Gruppen	Nein	Ja	Ja
Erstellen von administrativen Gruppen, die mehrere Routinggruppen umfassen	Nein	Ja	Ja
Verwenden von abfragebasierten Verteilungsgruppen	Nein	Ja	Ja
InetOrgPerson-Objekte können postfachaktiviert oder E-Mail-aktiviert sein	Nein	Nein	Ja

Ausführen im gemischten Modus

Damit eine Koexistenz zwischen Exchange 5.5, Exchange 2000 und Exchange 2003 möglich ist und Verzeichnisinformationen repliziert werden können, muss die Exchange 2000- und Exchange 2003-Konfiguration in einem Zustand verbleiben,
der von Exchange 5.5 erkannt werden kann. Wenn die Exchange-Organisation im gemischten Modus ausgeführt wird, ist die Interoperabilität der verschiedenen Exchange-Versionen gewährleistet. Für die sichere Koexistenz von Exchange 5.5-Verzeichnissen und Active Directory ist außerdem ADC von großer Bedeutung.

> **Hinweis** Aufgrund der Einschränkungen des Betriebs im gemischten Modus sollten Sie diesen nicht für den Betrieb Ihrer Organisation verwenden, wenn in dieser ausschließlich Exchange 2000- und Exchange 2003-Server eingesetzt werden, und wenn Sie sicher sind, dass Sie in der Organisation später keinen Exchange 5.5-Server installieren.

Der gemischte Modus ist nur für die Interoperabilität zwischen Exchange 2003- und Exchange 5.5-Servern bestimmt. Es wird empfohlen, zum einheitlichen Modus zu wechseln, sobald dies technisch möglich ist. Der Betrieb Ihrer Exchange-Organisation im gemischten Modus hat die nachstehenden Einschränkungen und Probleme zur Folge:

- Exchange 5.5-Standorte sind direkt administrativen Gruppen zugeordnet und umgekehrt.
- Sie können nur Postfächer zwischen Servern verschieben, die sich in derselben administrativen Gruppe befinden.
- Die Mitglieder der Routinggruppe dürfen nur aus Servern bestehen, die in der administrativen Gruppe installiert sind, die mit der Routinggruppe definiert wurde.

Hinweis Wenn sich jedoch eine Exchange 2003-Organisation im gemischten Modus befindet und Exchange 5.5-Standorte direkt administrativen Gruppen zugeordnet werden, können Sie die Routingstruktur für die Exchange 2003-Server in der Zusammenstellung weiter unterteilen, indem Sie Routinggruppen verwenden. Da im gemischten Modus eine bestimmte Routinggruppe nur einer einzigen administrativen Gruppe angehören kann, ist es nicht möglich, dass ein Server einer Routinggruppe angehört, die unter einer anderen administrativen Gruppe verwaltet wird. Bei Exchange 5.5-Servern werden diese Unterscheidungen nach Routinggruppe nicht vorgenommen. Stattdessen wird für Routingzwecke weiterhin die Standortgrenze verwendet.

Planen für den Wechsel zum einheitlichen Modus

Es sollte Ihr Ziel sein, den Zeitraum der Koexistenz von Exchange 5.5- und Exchange 2003-Servern so kurz wie möglich zu halten, damit Sie die Features von Exchange 2003 schnell vollständig nutzen können. Bedenken Sie, dass nach dem Wechsel einer Exchange 2003-Organisation vom gemischten Modus in den einheitlichen Modus keine Interoperabilität mehr mit Exchange 5.5-Systemen besteht. Exchange-Organisationen, die im einheitlichen Modus betrieben werden, können Exchange 2003- und Exchange 2000-Server enthalten. Sie können eine Exchange-Organisation nur in den einheitlichen Modus versetzen, wenn auf allen darin enthaltenen Exchange-Servern Exchange 2003 oder Exchange 2000 ausgeführt wird.

Ermitteln Sie, wann alle nachstehenden Bedingungen im Projektplan erfüllt sein werden, und planen Sie für diesen Zeitpunkt den Wechsel der Exchange-Organisation in den einheitlichen Modus:

- Es werden keine Exchange 5.5-Server mehr in Ihrer Organisation verwendet.
- Es ist nicht geplant, der Organisation später Exchange 5.5-Server hinzuzufügen, z. B. als Ergebnis einer Unternehmenszusammenführung oder durch den Erwerb eines Unternehmens mit Exchange 5.5-Servern.
- Für Ihr Unternehmen wird in Zukunft niemals Interoperabilität zwischen den Exchange 2003- oder Exchange 2000-Servern und Exchange 5.5 benötigt. (Für die Verbindung mit älteren Versionen von Exchange können Sie zwar Connectors einsetzen, doch diese Server befinden sich außerhalb der Exchange-Organisation.)
- Ihre Organisation verwendet keine Connectors oder Gatewayanwendungen, die nur mit Exchange 5.5 ausgeführt werden können.

Wichtig Nachdem der Wechsel vom gemischten Modus in den einheitlichen Modus durchgeführt wurde, kann diese Änderung nicht rückgängig gemacht werden, und zwischen der Organisation und Exchange 5.5-Systemen besteht keine Interoperabilität mehr. Ausführliche Informationen zur Vorgehensweise beim Wechsel in den einheitlichen Modus finden Sie im *Bereitstellungshandbuch für Exchange 2003* (http://go.microsoft.com/fwlink/?linkid=14576).

Installieren einer neuen Exchange 2003-Organisation

Das Bereitstellen von Exchange 2003 in einer Organisation, in der keine älteren Versionen von Exchange verwendet werden, ist recht einfach. Zu den wichtigsten Überlegungen gehört, ob die Organisation unter Windows 2000 Server oder Windows Server 2003 ausgeführt wird, und ob Active Directory auf eine für Exchange geeignete Weise implementiert ist. Des Weiteren müssen Sie unbedingt klären, ob Sie auch Verbindungen zu anderen Messagingsystemen als Exchange (z. B. Lotus Notes oder Novell

GroupWise) herstellen oder von diesen migrieren müssen. In diesem Fall benötigen Sie einen Plan zum Installieren und Ausführen von Connectors.

Weitere Informationen zur Vorgehensweise bei der Installation einer neuen Exchange 2003-Organisation finden Sie in den folgenden Ressourcen:

- *Bereitstellungshandbuch für Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=14576)
- Exchange 2003: Exchange-Bereitstellungstools (http://go.microsoft.com/fwlink/?LinkId=21231)

Aktualisieren von Exchange 2000

Wenn Ihre aktuelle Exchange-Umgebung aus einer reinen Exchange 2000-Organisation im einheitlichen Modus besteht, ist Active Directory bereits implementiert und unterstützt Exchange.

Beachten Sie unbedingt, dass Sie im Falle einer Aktualisierung eines Exchange 2000-Servers auf einen Exchange 2003-Server die folgenden Komponenten zuerst entfernen müssen, da diese in Exchange 2003 nicht unterstützt werden:

- Microsoft Mobile Information Server Exchange Event Source. Diese Komponente wird in Exchange 2003 durch die Exchange Mobile Browse-Komponente ersetzt.
- Instant Messaging Server, Microsoft Exchange 2000 Chat-Dienst, Microsoft Exchange 2000 Conferencing Server, Schlüsselverwaltungsdienst, Microsoft Exchange Connector für Lotus cc:Mail und Microsoft Exchange MS Mail Connector. Wenn Sie diese Dienste in Ihrer Organisation beibehalten möchten, sollten Sie Exchange 2003 nicht auf den Servern installieren, auf denen diese Dienste ausgeführt werden. Sie können weiterhin einen Exchange 2000-Server verwenden, um diese Komponenten auszuführen.

Sie sollten außerdem Drittanbieterdienste überprüfen, die von Exchange 2000 abhängig sind oder zusammen mit Exchange 2000 verwendet werden, um sicherzustellen, dass diese von Exchange 2003 unterstützt werden. Dies gilt beispielsweise für Sicherungssysteme, Antivirus-Anwendungen und andere Connectors (z. B. Fax-Connectors).

Weitere Informationen zum Aktualisieren von Exchange 2000 finden Sie in den folgenden Ressourcen:

- *Bereitstellungshandbuch für Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=14576)
- *Exchange 2003: Exchange-Bereitstellungstools* (http://go.microsoft.com/fwlink/?LinkId=21231)

Wechsel von Exchange 5.5 zu Exchange 2003

Wenn in Ihrer aktuellen Organisation Exchange 5.5, Exchange 2000 oder eine Kombination der beiden im gemischten Modus ausgeführt wird, stehen Ihnen mehrere Optionen für den Wechsel zu Exchange 2003 zur Verfügung. Wie bereits erwähnt, muss eine stabile Active Directory-Umgebung vorhanden sein, bevor Sie Exchange 2003 bereitstellen.

Sie müssen jedoch die Bereitstellung von Active Directory nicht notwendigerweise vollständig abgeschlossen haben, um Exchange 2003 bereitzustellen. Sie sind zum Beispiel unter Umständen noch nicht bereit, alle Microsoft Windows NT®-Konten zu Active Directory zu verschieben, möchten jedoch eine Active Directory-Domäne definieren, auf der

Exchange 2003-Postfächer gespeichert werden können. In diesem Fall können Sie ADC so einrichten, dass für die Windows NT-Konten Platzhalter in Active Directory erstellt werden können. Exchange 2003 verwendet diese Platzhalter, um die E-Mail-Funktionalität bei Exchange 5.5-Standorten zu gewährleisten, die nicht in einer Active Directory-Domäne bereitgestellt wurden. Sie können dann die Postfächer für diese Konten auf Exchange 2003-Server verschieben, die in einer Active Directory-Domäne bereitgestellt werden. Wenn Sie bereit sind, die Windows NT-Konten zu Active Directory hinzuzufügen (entweder durch Aktualisieren der Windows NT-Domäne oder mithilfe der Active Directory-Migrationstools), können Sie den Postfachplatzhalter mit dem Windows-Konto zusammenführen.

Abhängig von Ihren Anforderungen können Sie zwischen den beiden folgenden Pfaden wählen, um von Exchange 5.5 zu Exchange 2000 zu wechseln:

- **Standardpfad (empfohlen)** Exchange 2003 wird in der Exchange 5.5-Organisation bereitgestellt.
- **Externer Migrationspfad** Exchange 5.5-Daten werden in eine separate Exchange 2003-Organisation migriert.

Der empfohlene Bereitstellungspfad ist unabhängig von Ihrer aktuellen Umgebung immer der Standardpfad. Dies bedeutet die Installation von Exchange 2003 über eine bestehende Exchange 5.5-Organisation. Indem Sie diesen Installationspfad anwenden, können Sie die neuen Exchange Server-Bereitstellungstools in Exchange 2003 verwenden, die alle empfohlenen Schritte, Diagnosetools und Setupverknüpfungen enthalten, durch die die Installation von Exchange 2003 erleichtert wird.

Wenn es nicht möglich ist, Exchange 2003 in Ihrer vorhanden Exchange 5.5-Organisation zu installieren, können Sie Ihre Exchange 5.5-Daten auch in eine getrennte Exchange 2003-Organisation migrieren.

Im vorliegenden Abschnitt werden diese beiden Bereitstellungspfade vorgestellt.

Standardpfad: Bereitstellen von Exchange 2003 in der Exchange 5.5-Organisation (empfohlen)

Diese Methode wird empfohlen, da Sie auf diese Weise die Vorteile der Exchange Server-Bereitstellungstools nutzen können, die Sie durch den gesamten Prozess leiten. Die Exchange Server-Bereitstellungstools bieten empfohlene Schritte, Diagnosetools und Setupverknüpfungen, mit denen die Installation von Exchange 2003 erleichtert wird.

Bei dieser Methode installieren Sie ADC und verwenden die ADC-Tools, um Verbindungsvereinbarungen festzulegen, auf deren Grundlage Exchange 5.5-Verzeichnisinformationen mit Active Directory synchronisiert werden. Sie verbinden dann die Hardware des neuen Servers, auf dem Exchange 2003 ausgeführt wird, mit Ihrer bestehenden Exchange 5.5-Organisation. Abschließend verschieben Sie Postfächer und replizierte Öffentliche Ordner auf den neuen Server.

Diese Strategie ist optimal für Ihre Organisation geeignet, wenn Sie keine größeren Änderungen in der Architektur oder Topologie planen. Active Directory sollte stets innerhalb Ihrer Organisation bereitgestellt werden. Es ist jedoch nicht erforderlich, um all Ihre Microsoft Windows NT Server Version 4.0-Domänen oder -Benutzerkonten auf Windows 2000 Server oder Windows Server 2003 zu aktualisieren. Jeder Exchange 5.5-Standort muss mindestens einen Server enthalten, auf dem Exchange 5.5 mit SP3 ausgeführt wird. Es wird außerdem empfohlen, dass Ihre bestehende Organisation mindestens eine Active Directory-Domäne im einheitlichen Modus enthält.

Die folgenden Ressourcen enthalten vollständige Informationen zur Verwendung dieser Methode für die Bereitstellung von Exchange 2003:

- *Bereitstellungshandbuch für Exchange Server 2003*, verfügbar in der technischen Bibliothek für Exchange Server 2003 (http://go.microsoft.com/fwlink/?linkid=14576)

- *Exchange 2003: Exchange-Bereitstellungstools*, verfügbar auf der Exchange Server 2003-CD und zum Herunterladen auf der Exchange Server 2003-Website für Tools und Aktualisierungen (http://go.microsoft.com/fwlink/?LinkId=21316)

Externer Migrationspfad: Migration von Exchange 5.5-Daten zu einer separaten Exchange 2003-Organisation

Ein Alternative zum Hinzufügen eines neuen Exchange 2003-Servers zur Exchange 5.5-Organisation ist die Erstellung einer neuen Exchange 2003-Organisation und die Migration von Verzeichnisinformationen und Postfächern zur neuen Organisation. Mit diesem Verfahren installieren Sie eine neue Exchange 2003-Organisation und migrieren die zugehörigen Verzeichnis- und Messagingdaten in die neue Organisation. Bei dieser Methode ist es erforderlich, dass Ihre Zielorganisation über Active Directory verfügt.

Diese Option erfordert außerdem eine Kombination von Migrationstools, deren jeweilige Verwendung vom Umfang der Migration und Ihren Anforderungen an Systemkoexistenz abhängt. Es stehen Ihnen die folgenden beiden empfohlenen Arten für eine Bereitstellung von Exchange 2003 mithilfe dieser Methode zur Verfügung:

- Active Directory-Migrationstool → Assistent für die Migration
- Active Directory-Migrationstool (oder Aktualisierung der Kontendomäne) → ADC → Assistent für die Migration

Befinden sich die Konten in einer anderen Gesamtstruktur als die Postfächer, müssen Sie zwischen den beiden Gesamtstrukturen eine Vertrauensstellung einrichten, um den Benutzern den Zugriff auf ihre Postfächer zu ermöglichen.

Sie verwenden auch bei dieser Methode die Exchange Server-Bereitstellungstools, um die Standardbereitstellungsschritte zu durchlaufen, wählen jedoch während des Exchange-Setups die Option, sich nicht einer bestehenden Exchange 5.5-Organisation anzuschließen.

Weitere Informationen zur Verwendung dieser Methoden finden Sie im technischen Artikel *Migrating Mailboxes from Microsoft Exchange Server Version 5.5 to Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?LinkId=18351). Obwohl sich dieser Artikel auf Exchange 2000 bezieht, treffen die Beschreibungen auch auf Exchange 2003 zu.

Active Directory-Migrationstool → Assistent für die Migration

Die beste Vorgehensweise für kleine Unternehmen mit einer geringen Anzahl zu migrierender Postfächer besteht darin, erst das Active Directory-Migrationstools (ADMT) und anschließend den Assistenten für die Migration nach Exchange Server zu verwenden.

Erstellen Sie zuerst mit ADMT in Active Directory aktive Benutzerkonten. Wählen Sie die Option zur Migration der SIDs (Sicherheits-IDs) aus, damit ADMT die SID eines Quellkontos zum Verlaufsattribut (**SIDHistory)** des neuen Zielkontos hinzufügt. (Im nächsten Schritt verwendet der Assistent für die Migration diese SIDs für die Zuordnung von Postfächern zu Konten.) Zum Migrieren von SIDs muss die Exchange 2003-Zieldomäne jedoch im einheitlichen Modus ausgeführt werden.

> **Wichtig** Zum Migrieren von SIDs muss die Windows-Zieldomäne im einheitlichen Modus ausgeführt werden. Das Attribut **SIDHistory** ist im Domänenschema nur dann vorhanden, wenn die Windows-Domäne im einheitlichen Modus ausgeführt wird.

Migrieren Sie im Anschluss an die Konten die Postfächer mit dem Assistenten für die Migration. Wenn Sie beim Ausführen von ADMT die SIDs migriert haben, verwendet der Assistent für die Migration diese SIDs, um den neuen Konten die Postfächer zuzuordnen und anschließend die Konten in postfachaktivierte

Benutzerkonten umzuwandeln. Wenn Sie im ersten Schritt die SIDs nicht migriert haben, ist der Assistent für die Migration nicht in der Lage, ein Postfach einem Konto zuzuordnen, und erstellt stattdessen für die Zuordnung des Postfachs ein deaktiviertes Benutzerkonto.

Hinweis Als Alternative zum ADMT können Sie auch das Standardverfahren für die Aktualisierung von Windows NT Server Version 4.0 auf Windows Server 2003 durchführen. Dabei bleibt die SID ebenfalls erhalten.

Active Directory-Migrationstool (oder Aktualisierung der Windows-Domäne) → ADC → Assistent für die Migration

In großen Organisationen können Sie mit Active Directory Connector (ADC) den Benutzern ermöglichen, während des Migrationsvorgangs E-Mail-Nachrichten zu senden und zu empfangen. Beachten Sie vor dem Einrichten von ADC, dass es zwei Methoden zur Erstellung von Benutzerkonten im Zielverzeichnis gibt, bei denen die SIDs erhalten bleiben:

- Sie können die Windows NT-Domäne auf Windows Server 2003 aktualisieren. Dabei bleiben die SIDs der Konten erhalten.
- Sie können auch ADMT verwenden, sofern Sie die Option für die Migrieration der SID vom Quellkonto zum Attribut **SIDHistory** des Zielkontos aktivieren.

Wenn die SID für jedes Konto der neuen Gesamtstruktur erhalten bleibt (entweder durch eine Aktualisierung oder durch die Migration der SID in das Attribut **SIDHistory**), können Sie mit ADC E-Mail-aktivierte Konten erstellen. Führen Sie nach der Installation von ADC den Assistenten für die Migration aus, um die Postfächer zu verschieben.

Wichtig Zum Migrieren von SIDs muss die Windows-Zieldomäne im einheitlichen Modus ausgeführt werden. Das Attribut **SIDHistory** ist im Domänenschema nur dann vorhanden, wenn die Windows-Domäne im einheitlichen Modus ausgeführt wird.

Folgende Schritte müssen für dieses Migrationsszenario durchgeführt werden:

Erstellen Sie in der Zielgesamtstruktur nach einer der beiden folgenden Methoden neue Konten:

- Aktualisieren Sie die Domäne von Windows NT auf Windows 2000 oder Windows Server 2003. Dabei werden Konten mit erhaltenen SIDs erstellt.
- Migrieren Sie mit ADMT die Exchange 5.5-Postfächern zugeordneten Windows NT-Konten nach Active Directory, und erstellen Sie anschließend neue Active Directory-Benutzer. Dabei wird von ADMT für jeden neuen Benutzer das Attribut **SIDHistory** ausgefüllt.

ADC findet die neuen Active Directory-Benutzer und weist diesen E-Mail-Adressen zu. Dadurch werden sie zu E-Mail-aktivierten Benutzern.

Der Assistent für die Migration findet die Active Directory-Benutzer, indem er nach den entsprechenden SIDs sucht. Der Assistent für die Migration erstellt die entsprechenden Postfächer (hierbei werden die Benutzer postfachaktiviert) und migriert anschließend die Postfachdaten.

Wenn der Vorgang des Erstellens von Konten mithilfe des Active Directory-Migrationstools voraussichtlich längere Zeit in Anspruch nimmt, können Sie wahlweise zum Erstellen von Kontakten in Active Directory auch zuerst ADC einrichten. Wenn Sie ADC zuerst einrichten, können Active Directory-Benutzer während längerer Zeiträume der

Koexistenz E-Mail-Nachrichten mit Exchange 5.5-Benutzern austauschen. Wie bei der vorherigen Methode verwenden Sie dann das Active Directory-Migrationstool, um Kontenberechtigungen beizubehalten (z. B. Berechtigungen für Drucker, Dateifreigaben und andere Postfächer).

Wechsel von Exchange 2000 zu Exchange 5.5 im gemischten Modus

Wenn Exchange 5.5 und Exchange 2000 bereits koexistieren, ist Active Directory bereits implementiert und unterstützt Exchange. Active Directory Connector wird ausgeführt, um die Synchronisierung von Exchange 5.5 Directory und Active Directory aufrechtzuerhalten.

In diesem Fall stehen Ihnen die folgenden Optionen für die Bereitstellung von Exchange 2003 zur Verfügung:

- Aktualisieren einer der Exchange 2000-Server
- Bereitstellen eines neuen Exchange 2003-Servers

In beiden Fällen müssen Sie zuerst ADC auf allen Servern, auf denen ADC ausgeführt wird, auf die Version von ADC aktualisieren, die in Exchange Server 2003 enthalten ist. Außerdem sollten Sie sicherstellen, dass Ihre Verbindungsvereinbarungen ordnungsgemäß eingerichtet sind. Verwenden Sie dazu die in der Exchange 2003-Version von ADC bereitgestellten ADC-Tools.

> **Wichtig** Die ADC-Tools stellen anhand der Verzeichniskonfiguration Empfehlungen für Verbindungsvereinbarungen bereit. Um Probleme bei der Verzeichnisreplikation zu vermeiden, sollten Sie diese Empfehlungen unbedingt übernehmen.

Nachdem Sie alle Instanzen von ADC installiert haben und ADC-Tools ausführen, können Sie den ersten Exchange 2003-Server installieren oder einen Microsoft Exchange 2000-Server auf Exchange 2003 aktualisieren.

Beachten Sie unbedingt, dass Sie im Falle einer Aktualisierung eines Exchange 2000-Servers auf einen Exchange 2003-Server die folgenden Komponenten zuerst entfernen müssen, da diese in Exchange 2003 nicht unterstützt werden:

- Microsoft Mobile Information Server Exchange Event Sink. Diese Komponente wird in Exchange 2003 durch die Exchange Mobile Browse-Komponente ersetzt.
- Instant Messaging Server, Microsoft Exchange 2000 Chat-Dienst, Microsoft Exchange 2000 Conferencing Server, Schlüsselverwaltungsdienst, Microsoft Exchange Connector für Lotus cc:Mail und Microsoft Exchange MS Mail Connector. Wenn Sie diese Dienste in Ihrer Organisation beibehalten möchten, dürfen Sie Exchange 2003 nicht auf den Servern installieren, auf denen diese Komponenten ausgeführt werden.

Bereitstellen von Exchange in einer Umgebung mit mehreren Gesamtstrukturen

In Kapitel 2 werden die folgenden Szenarien zur Bereitstellung von Exchange in einer Umgebung mit mehreren Gesamtstrukturen behandelt:

- Dedizierte Exchange-Gesamtstruktur (Ressourcengesamtstruktur)

- Mehrere Gesamtstrukturen, in denen Exchange ausgeführt wird (klassische Variante mit mehreren Gesamtstrukturen)
- Fusionen und Übernahmen

In diesem Abschnitt werden hauptsächlich die Konfigurationsanforderungen für die Aktivierung der Messagingfunktionen in einem klassischen Szenario mit mehreren Gesamtstrukturen behandelt. Jedoch können Sie, abhängig von Ihren Anforderungen, einen Teil oder die gesamten Informationen auch für die Ressourcengesamtstruktur
und die Szenarien für Fusionen und Übernahmen verwenden.

Verfügbare Features in einer Umgebung mit mehreren Gesamtstrukturen

Die meisten E-Mail-Features wurden ursprünglich für die Verwendung in einer einzelnen Gesamtstruktur entworfen. Daher müssen Sie viele Entwurfsbeschränkungen hinnehmen, damit diese Features auch über mehrere Gesamtstrukturen hinweg verfügbar sind. Einige erweiterte Funktionen, z. B. Vergabe von Berechtigungen für den Postfachzugriff und Kalenderansicht, stehen für Benutzer in unterschiedlichen Gesamtstrukturen nicht zur Verfügung. In Tabelle 3.2 werden die E-Mail-Features für Umgebungen mit mehreren Gesamtstrukturen aufgeführt.

Tabelle 3.2 Features in Umgebungen mit mehreren Gesamtstrukturen

Feature	Über mehrere Gesamtstrukturen verfügbar?
Grundlegende E-Mail-Übertragung	Ja, Vertrauensstellungen zwischen den Gesamtstrukturen sind nicht erforderlich.
Gemeinsame globale Adressliste (GAL)	Ja, mit Microsoft Identity Integration Server 2003 (MIIS 2003).
Synchronisierung von Frei/Gebucht-Informationen	Ja, mit dem Tool für die Replikation zwischen Organisationen. In Microsoft Office Outlook® kann ein Besprechungsorganisator einer Besprechungsanfrage einen Teilnehmer aus einer anderen Gesamtstruktur hinzufügen und auf der Registerkarte **Terminplanung** die Verfügbarkeit des Teilnehmers überprüfen.
Synchronisierung von Öffentlichen Ordnern	Ja, mit dem Tool für die Replikation zwischen Organisationen.
Weiterleitung von Besprechungsanfragen	Ja, wenn Sie GAL-Synchronisierung konfiguriert und SMTP-Authentifizierung eingerichtet haben.
Verteilergruppen	Ja, eine Verteilergruppe einer anderen Gesamtstruktur wird als Kontakt dargestellt. Sie können E-Mail-Nachrichten an eine Verteilergruppe einer anderen Gesamtstruktur senden (jedoch nicht die Mitgliedschaft der Gruppe abfragen).
Secure Multipurpose Internet Mail Extensions (S/MIME)	Ja, mit manueller Konfiguration. Standardmäßig werden Benutzerzertifikate zwischen Gesamtstrukturen nicht synchronisiert. Konfigurieren Sie **userCertificate**, um S/MIME zu aktivieren. Die Schlüsselverwaltungsdienste von Exchange 2000 und Exchange 5.5 werden in einer Umgebung mit mehreren Gesamtstrukturen nicht unterstützt.
Übermittlungs-/Lesebestätigungen	Ja, wenn die globalen Einstellungen ordnungsgemäß konfiguriert wurden. (Hierzu können Sie verschiedene Optionen einstellen, wie

Feature	Über mehrere Gesamtstrukturen verfügbar?
	weiter unten in diesem Kapitel unter „Konfigurieren des Nachrichtenflusses zwischen Gesamtstrukturen“ erläutert wird.)
Über Gesamtstrukturen freigegebener SMTP-Namespace	Ja, wenn jede Organisation zusätzlich zum freigegebenen Namespace einen eindeutigen SMTP-Domänennamespace aufweist. Fügen Sie jeder Gesamtstruktur eine Empfängerrichtlinie hinzu, in der die eindeutige SMTP-Proxyadresse angegeben ist. (Wenn in der Gesamtstruktur Exchange 5.5 ausgeführt wird, repliziert ADC die zweite Proxyadresse in das Exchange 5.5-Verzeichnis, sofern Verbindungsvereinbarungen in beide Richtungen eingerichtet sind.)
Berechtigungen für Öffentliche Ordner	Nein, wenn Sie einen Öffentlichen Ordner mit dem Tool für die Replikation zwischen Organisationen replizierten, muss der Administrator jeder einzelnen Gesamtstruktur die Berechtigungen dieses Ordners einrichten.
Regeln	Nein, Regeln bleiben bei einer gesamtstrukturübergreifenden Verschiebung nicht erhalten.
Stellvertreter für Postfächer	Nein, da Benutzer oder Gruppen einer anderen Gesamtstruktur als Kontakte dargestellt werden, können Sie den Zugriff auf ein Postfach nicht an eine Person einer anderen Gesamtstruktur vergeben. In den Zugriffsrechten eines Postfachs können keine Kontakte eingetragen werden. Außerdem bleiben Stellvertreterberechtigungen von Postfächern beim Verschieben eines Postfachs von einer Gesamtstruktur in eine andere nicht erhalten.
Anzeigen des Kalenders	Nein, obwohl Sie Frei/Gebucht-Informationen gesamtstrukturübergreifend synchronisieren und diese dann zur Planung von Besprechungen verwenden können, können Sie Kalenderinformationen eines Benutzers einer anderen Gesamtstruktur nicht in Outlook mit der Funktion **Ordner eines anderen Benutzers öffnen** anzeigen.
Anzeigen von Gruppenmitgliedschaften	Nein, da eine Gruppe einer anderen Gesamtstruktur als Kontakt dargestellt wird, können Sie die Gruppenmitglieder nicht anzeigen. Die Gruppenmitgliedschaft wird erst erweitert, wenn eine E-Mail-Nachricht an die Quellengesamtstruktur gesendet wurde.
Connectors zu fremden Messagingsystemen	Ja, wenn eine Gesamtstruktur mit einem fremden Messagingsystem verbunden ist und Sie MIIS 2003 verwenden, können Sie die Kontakte des fremden Messagingsystems in andere Gesamtstrukturen replizieren.
Senden als	Nein, hierzu müssen sich die Benutzer in derselben Gesamtstruktur befinden.
Front-End-Server für mehrere Gesamtstrukturen	Nein, ein Front-End-Server kann für einen Back-End-Server einer anderen Gesamtstruktur nicht als Proxyserver dienen. Diese Einschränkung gilt auch, wenn Sie einen Front-End-Server für Outlook Web Access oder Outlook Mobile Access verwenden.
Exchange Instant Messaging-Dienst	Ja, jedoch können die Gesamtstrukturen nicht denselben Namespace gemeinsam verwenden.

Planen einer Bereitstellung mit mehreren Gesamtstrukturen

Wenn Sie Exchange in einer Umgebung mit mehreren Gesamtstrukturen installieren, müssen Sie zumindest die grundlegende E-Mail-Funktionalität bereitstellen, indem Sie den E-Mail-Nachrichtenfluss ermöglichen und eine allgemeine GAL erstellen. Abhängig von Ihren Anforderungen müssen Sie auch erweiterte E-Mail-Features einrichten, wie z. B. Synchronisierung von Frei/Gebucht-Informationen und Öffentlichen Ordnern.

Mit einigen zusätzlichen Entwicklungsschritten können Sie die Umgebung so konfigurieren, dass so viele Messagingfunktionen wie möglich über die Gesamtstrukturen bereitgestellt werden. Nachdem Sie Exchange in allen Gesamtstrukturen installiert oder aktualisiert haben, können Sie die Bereitstellung mit den folgenden Schritten abschließen:

1. Ermöglichen Sie den Benutzern zum Senden von E-Mails mit der GAL-Synchronisierung von MIIS 2003 das Durchsuchen einer allgemeinen GAL.

2. Eine funktionierende Netzwerkverbindung ist die einzige unbedingt zu erfüllende Anforderung für den Nachrichtenfluss zwischen Gesamtstrukturen.
   Es sind keine Vertrauensstellungen erforderlich, jedoch müssen Sie zwischen den Gesamtstrukturen SMTP-Connectors einrichten. Es wird außerdem dringend empfohlen, die Authentifizierung zwischen den Gesamtstrukturen zu aktivieren. Dadurch werden Funktionen wie die Auflösung der E-Mail-Adressen der Benutzer in die entsprechenden GAL-Anzeigenamen bereitgestellt.

3. Konfigurieren Sie erweiterte E-Mail-Features (z. B. die Freigabe von SMTP-Namespace und globalen Einstellungen).

4. Konfigurieren Sie das Tool für die Replikation zwischen Organisationen, um Frei/Gebucht-Informationen zu synchronisieren und Öffentliche Ordner zu replizieren. Damit Benutzer verschiedener Gesamtstrukturen gemeinsame Besprechungen planen können, müssen Sie die Frei/Gebucht-Informationen zwischen den Gesamtstrukturen replizieren. Weiterhin müssen Sie in allen Gesamtstrukturen Replikate einrichten, wenn Sie Öffentliche Ordner gemeinsam über die Gesamtstrukturen hinweg verwenden möchten.

5. Verschieben Sie nach Bedarf Postfächer und Konten zwischen den Gesamtstrukturen.

Die ersten beiden Schritte sind für grundlegendes Messaging erforderlich. Eine synchronisierte globale GAL muss für alle Gesamtstrukturen verfügbar sein, und eine Transportroute muss eingerichtet werden, damit zwischen ihnen Nachrichten übertragen werden können. In den weiteren Schritten werden erweiterte E-Mail-Features behandelt, die Sie abhängig von Ihren Anforderungen implementieren können.

Die folgenden Abschnitte bieten einen Überblick, wie Sie diese Features bereitstellen.

Verwenden der GAL-Synchronisierung von MIIS 2003

Standardmäßig beinhaltet eine globale Adressliste (GAL) die E-Mail-Empfänger einer einzelnen Gesamtstruktur. Wenn Sie in einer Umgebung mit mehreren Gesamtstrukturen arbeiten, können Sie mit der GAL-Synchronisierung von MIIS 2003 sicherstellen, dass die GAL jeder beliebigen Gesamtstruktur alle E-Mail-Empfänger der anderen Gesamtstrukturen enthält. Mit diesem Feature werden E-Mail-aktivierte Kontakte erstellt, die Empfängern aus anderen Gesamtstrukturen entsprechen. Dadurch können die Benutzer diese Kontakte in der GAL anzeigen und Nachrichten an diese senden. Beispielsweise werden Benutzer der Gesamtstruktur A in der Gesamtstruktur B als Kontakte angegeben und umgekehrt. Benutzer der

Zielgesamtstruktur können zum Senden einer Nachricht das Kontaktobjekt auswählen, das einen Empfänger einer anderen Gesamtstruktur darstellt.

Wenn in jeder Gesamtstruktur mindestens ein Exchange 2003-Server vorhanden ist, können Sie mit MIIS 2003 Gesamtstrukturen synchronisieren, in denen beliebige Kombinationen aus Exchange 5.5, Exchange 2000 und Exchange 2003 ausgeführt werden. (Die GAL-Synchronisierung funktioniert nicht in reinen Exchange 5.5-Gesamtstrukturen.) Mit MIIS 2003 werden die GALs synchronisiert, auch wenn sich die Quell- oder Zielgesamtstruktur im gemischten Modus befindet und ADC ausgeführt wird. In der Quellgesamtstruktur werden Exchange 5.5-Objekte von ADC mit Active Directory synchronisiert. MIIS 2003 verwendet anschließend die Objekte in Active Directory, um die Metaverzeichnisobjekte zu erstellen, die mit den anderen Gesamtstrukturen synchronisiert werden. In der Zielgesamtstruktur werden die Kontakte in das Exchange 5.5-Verzeichnis repliziert.

Wenn Sie ADC ausführen, sind einige zusätzliche Einstellungen erforderlich. In erster Linie müssen Sie zum Sicherstellen der Synchronisierung von Benutzern und Kontakten zwischen den Gesamtstrukturen ADC und die GAL-Synchronisierung von MIIS 2003 so konfigurieren, dass eine gemeinsame Organisationseinheit verwendet wird.

> **Hinweis** ADC ist nicht für die Synchronisierung zwischen Gesamtstrukturen geeignet. Mit ADC werden Exchange 5.5-Objekte und Active Directory synchronisiert, um eine Migration nach Active Directory zu ermöglichen. Synchronisieren Sie GALs zwischen Gesamtstrukturen mit MIIS 2003. Sie können MIIS 2003 selbst dann verwenden, wenn die Gesamtstrukturen im gemischten Modus betrieben werden und ADC ausgeführt wird.

Erstellen Sie zum Aktivieren der GAL-Synchronisierung Verwaltungsagenten, die E-Mail-aktivierte Benutzer, Kontakte und Gruppen aus den angegebenen Active Directory-Diensten in ein zentrales Metaverzeichnis importieren. Im Metaverzeichnis werden die E-Mail-aktivierten Objekte als Kontakte dargestellt. Gruppen werden als Kontakte ohne zugeordnete Mitgliedschaft dargestellt. Anschließend exportieren die Verwaltungsagenten die Kontakte in eine Organisationseinheit in der angegebenen Zielgesamtstruktur.

Die Quellgesamtstruktur ist für die an MIIS 2003 übermittelten E-Mail-aktivierten Objekte autorisierend. Wenn Sie in der Zielgesamtstruktur an den Attributen eines Objekts Änderungen vornehmen, werden diese Änderungen nicht an die Quellgesamtstruktur zurück übermittelt.

Beachten Sie beim Einrichten der GAL-Synchronisierung die folgenden Punkte:

- In jeder an der Synchronisierung teilnehmenden Gesamtstruktur ist ein getrennter Verwaltungsagent erforderlich.
- Um sicherzustellen, dass Verwaltungsagenten Kontakte in die Zielgesamtstrukturen exportieren können, muss der Server, auf dem MIIS 2003 ausgeführt wird, in der Lage sein, eine Verbindung zu einem Domänencontroller in jeder der teilnehmenden Gesamtstrukturen herzustellen. Verwaltungsagenten können mehrere Domänen verwalten, jedoch müssen sie anstelle von globalen Katalogservern auf Domänencontroller zugreifen, da auf globalen Katalogservern keine Kopien aller Namenskontexte mit Schreibzugriff vorhanden sind.
- Sie müssen beim Einrichten eines Verwaltungsagenten ein Konto mit den geeigneten Berechtigungen angeben.
- Wenn eine der Gesamtstrukturen einen Connector zu einem fremden Messagingsystem enthält, ist diese Gesamtstruktur standardmäßig autorisierend für die Kontakte. Diese Einstellung kann jedoch geändert werden. Weitere Informationen finden Sie weiter unten in diesem Kapitel unter „Konfigurieren des Nachrichtenflusses zwischen Gesamtstrukturen“.
- Benutzer können keine verschlüsselten E-Mail-Nachrichten aus einer Gesamtstruktur an eine Verteilergruppe einer anderen Gesamtstruktur senden. In Fällen, in denen Gesamtstrukturen über einen SMTP-Connector verbunden und mit der GAL-Synchronisierung synchronisiert werden, wird eine Verteilergruppe in der Zielgesamtstruktur als Kontakt dargestellt. Die Mitgliedschaft kann daher nicht erweitert werden.

Vollständige Informationen über die GAL-Synchronisierung von MIIS 2003 finden Sie in den folgenden Quellen:

- *Microsoft Identity Integration Server 2003 Global Address List Synchronization* (http://go.microsoft.com/fwlink/?LinkId=21270)
- Dokumentation zu Microsoft Identity Integration Server 2003 (MIIS 2003) (http://go.microsoft.com/fwlink/?LinkId=21271)

Unterstützte Topologien für GAL-Synchronisierung

Wie in der Dokumentation der GAL-Synchronisierung von MIIS 2003 beschrieben, müssen die Server, auf denen MIIS 2003 und die Exchange-Gesamtstrukturen ausgeführt werden, in einer vernetzten oder einer Hub-and-Spoke-Konfiguration angeordnet sein. Auch eine Kombination der beiden Konfigurationen wird unterstützt. Die Gesamtstrukturen können jedoch nicht in einer Kette verbunden werden. In den Abbildungen 3.1 und 3.2 werden die unterstützten Topologien veranschaulicht.

> **Wichtig** Die GAL-Synchronisierung von MIIS 2003 funktioniert nicht in einem Modell mit einer Ressourcengesamtstruktur (in dem Benutzerkonten und die dazugehörigen Postfächer in getrennten Gesamtstrukturen verwaltet werden). Obwohl MIIS 2003 so konfiguriert werden kann, dass Objekte zwischen einer Ressourcengesamtstruktur und einer Kontengesamtstruktur übermittelt werden, können Sie dazu nicht die GAL-Synchronisierung von MIIS 2003 verwenden. Sie können mit der GAL-Synchronisierung jedoch die Ressourcengesamtstruktur und andere Exchange-Gesamtstrukturen synchronisieren.

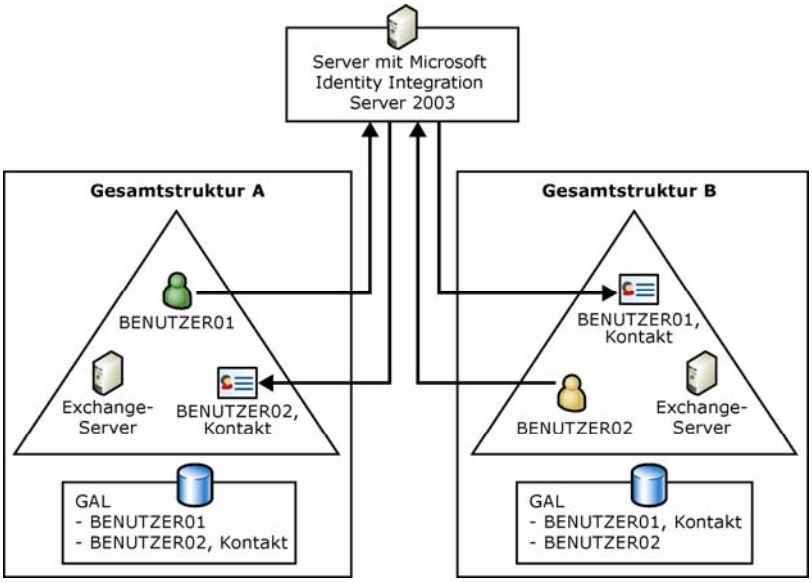


Abbildung 3.1 Hub-and-Spoke-Topologie

In einer Hub-and-Spoke-Topologie (Abbildung 3.1) wird auf einem einzelnen Server MIIS 2003 ausgeführt. Über diesen Server werden die gesamten Daten aller Gesamtstrukturen gelesen, Änderungen und Konflikte ausgewertet und die Änderungen an alle Gesamtstrukturen weitergegeben. Diese Topologie wird empfohlen, da sie zentral verwaltet und am einfachsten bereitgestellt werden kann.

> **Wichtig** Die für den MIIS 2003-Server konfigurierten Konten müssen über Schreibberechtigung für alle Gesamtstrukturen verfügen. In einigen Organisationen stellt dies eventuell ein Sicherheitsproblem dar.

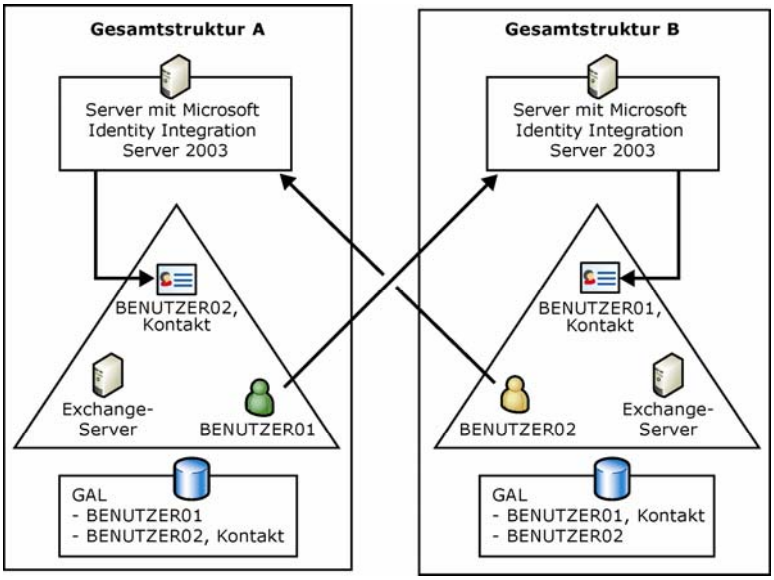


Abbildung 3.2 Unterstützte vernetzte Topologie

In einer vernetzten Topologie enthält jede Gesamtstruktur einen Server, auf dem MIIS 2003 ausgeführt wird. In jeder Gesamtstruktur müssen Verbindungen vom MIIS 2003-Server zu allen anderen Gesamtstrukturen eingerichtet werden. Diese Topologie ist komplex und wird ohne gründliche Pilottests nicht empfohlen. Der Hauptgrund für den Einsatz dieser Topologie besteht darin, dass in den Gesamtstrukturen kein Schreibzugriff auf deren Verzeichnisse gewährt werden muss. Lesezugriff ist jedoch erforderlich, denn die Verwaltungsagenten werden so konfiguriert, dass sie die Verzeichnisinformationen aller anderen Gesamtstrukturen lesen.

Konfigurieren des Nachrichtenflusses zwischen Gesamtstrukturen

Nach dem Einrichten der GAL-Synchronisierung müssen Sie sicherstellen, dass der E-Mail-Nachrichtenfluss zwischen den Organisationen und dem Internet ordnungsgemäß funktioniert. Für einen grundlegenden E-Mail-Nachrichtenfluss ist nur erforderlich, dass eine Route zu jeder benachbarten Gesamtstruktur aufgelöst werden kann. Vertrauensstellungen zwischen den Gesamtstrukturen sind nicht erforderlich.

Der E-Mail-Nachrichtenfluss wird durch die Netzwerkverbindung zwischen den Gesamtstrukturen sowie die Konfiguration der SMTP-Proxyadressen festgelegt.
Die ideale Konfiguration besteht aus direkten Netzwerkverbindungen zwischen den Gesamtstrukturen ohne Einsatz von Firewalls. (Wenn Sie zwischen den Gesamtstrukturen Firewalls einsetzen, müssen Sie die entsprechenden Anschlüsse freigeben.)

> **Hinweis** Zwischen den Gesamtstrukturen werden keine Informationen zu Verbindungsstatus oder Routingtopologie freigegeben.

Sie müssen zwischen den Gesamtstrukturen auch SMTP-Connectors einrichten. Ferner wird empfohlen, die Authentifizierung zwischen den Gesamtstrukturen zu aktivieren. Durch die Aktivierung der Authentifizierung erhalten Sie folgende Vorteile:

- Die Auflösung der Benutzernamen (Registrierungsschlüssel **ResolveP2**) erfolgt zwischen den Gesamtstrukturen automatisch, d. h. die E-Mail-Adresse eines Benutzers wird in den in Active Directory gespeicherten Benutzernamen aufgelöst.
- Es stehen zusätzliche Kalender- und E-Mail-Features zur Verfügung, z. B. Weiterleitung von E-Mail-Nachrichten.

Um gefälschte Identitäten (Spoofing) zu verhindern, ist in Exchange 2003 zum Auflösen des Absendernamens in den Anzeigenamen aus der GAL eine Authentifizierung erforderlich. Für eine Umgebung mit mehreren Gesamtstrukturen wird empfohlen, die Authentifizierung so zu konfigurieren, dass Benutzer, die E-Mail aus einer Gesamtstruktur in eine andere senden, in ihren Anzeigenamen aus der GAL aufgelöst werden, nicht in ihre SMTP-Adresse.

Um gesamtstrukturübergreifende SMTP-Authentifizierung zu aktivieren, müssen Sie in jeder Gesamtstruktur einen Connector erstellen, für den ein authentifiziertes Konto einer anderen Gesamtstruktur verwendet wird. Nachdem Sie die Authentifizierung aktiviert haben, wird jede zwischen den beiden Gesamtstrukturen über eine authentifizierte SMTP-Verbindung gesendete E-Mail-Nachricht zum entsprechenden Anzeigenamen aus der GAL aufgelöst. Weitere Informationen finden Sie im *Bereitstellungshandbuch für Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=14576).

Konfigurieren erweiterter E-Mail-Features

Die meisten Unternehmen besitzen eine Internetanbindung und mindestens einen veröffentlichten Domänennamen. Wenn jede Exchange-Organisation einen getrennten Namespace verwendet, ist für Kontakte, die zwischen den Organisationen synchronisiert werden, zum ordnungsgemäßen Weiterleiten lediglich eine SMTP-Adresse erforderlich. Möglicherweise arbeiten Sie jedoch mit mehreren Exchange-Organisationen und nur einem einzigen Namespace, der Ihr Unternehmen im Internet repräsentiert (z. B. „contoso.com“). In diesem Fall müssen Sie die Gesamtstrukturen voneinander unterscheiden, um die Namespaces der einzelnen Gesamtstrukturen beibehalten und E-Mail-Nachrichten trotzdem ordnungsgemäß in die einzelnen Gesamtstrukturen übertragen zu können.

Zusätzlich müssen Sie möglicherweise globale Einstellungen konfigurieren, um E-Mail-Features zu aktivieren oder zu deaktivieren, z. B. Abwesenheitsantworten, automatische Antworten und Übermittlungsberichte.

Konfigurieren eines freigegebenen SMTP-Namespaces

Wenn mit der GAL-Synchronisierung aus den E-Mail-Empfängern einer Quellgesamtstruktur Kontakte erstellt werden, wird für jeden Kontakt auf Grundlage der SMTP-Adressen die Eigenschaft **TargetAddress** erstellt. Wenn die Benutzer einer Gesamtstruktur eine E-Mail-Nachricht an einen Kontakt senden, wird die E-Mail daher an die Adresse in der Eigenschaft **TargetAddress** des Kontakts übermittelt, auch wenn der Benutzer manuell die primäre Antwortadresse eingegeben hat. Um festzulegen, welche **TargetAddress** dem Kontakt bei der GAL-Synchronisierung zugewiesen werden soll, wird die Eigenschaft **ProxyAddresses** des Empfängers mit der SMTP-Adresse verglichen, für die die Exchange-Organisation verantwortlich ist. Jede Organisation muss einen eindeutigen SMTP-Domänennamespace verwenden, so dass Kontakte eine eindeutige **TargetAddress** erhalten. Wenn Ihre Gesamtstrukturen keine eindeutigen Namespaces verwenden, können Sie der entsprechenden Empfängerrichtlinie für jede Exchange-Organisation, die gesamtstrukturübergreifend zu replizierende Benutzer enthält, eine eindeutige SMTP-Adresse hinzufügen. Anschließend werden Nachrichten, die an einen Kontakt gesendet werden, direkt zur Quellgesamtstruktur weitergeleitet, in der die Zieladresse in das tatsächliche Postfach aufgelöst und die Nachricht zugestellt wird.

Sie können Kontakte auch von einer Gesamtstruktur zu einer anderen Gesamtstruktur weiterleiten. Beim Einrichten der Verwaltungsagenten für die GAL-Synchronisierung können Sie auswählen, ob Nachrichten, die an in eine Gesamtstruktur importierte Kontakte gesendet werden, zurück durch diese Quellgesamtstruktur weitergeleitet werden. Wenn ein Connector zu einem fremden Messagingsystem vorhanden ist, wird eine E-Mail an einen Kontakt standardmäßig zu der Quellgesamtstruktur

(der Gesamtstruktur, die den Connector verwaltet) weitergeleitet. Diese Routingkonfiguration kann jedoch vom Administrator der Gesamtstruktur geändert werden.

> **Hinweis** Wenn in der Gesamtstruktur Exchange 5.5 ausgeführt wird, repliziert ADC die zweite Proxyadresse in das Exchange 5.5-Verzeichnis, sofern Verbindungsvereinbarungen in beide Richtungen eingerichtet sind.

Beispiel für SMTP-Routing in einer Umgebung mit mehreren Gesamtstrukturen: zwei Gesamtstrukturen, die beide eine Standardempfängerrichtlinie mit der SMTP-Proxyadresse „contoso.com“ verwenden. Um eindeutige Namespaces einzurichten, führen Sie in jeder Exchange-Organisation die folgenden Schritte durch:

- Fügen Sie in Organisation 1 der Standardempfängerrichtlinie die SMTP-Proxyadresse „Org1.contoso.com“ hinzu.
- Fügen Sie in Organisation 2 der Standardempfängerrichtlinie die SMTP-Proxyadresse „Org2.contoso.com“ hinzu.

Aktivieren Sie in beiden Fällen beim Hinzufügen der Proxyadresse das Kontrollkästchen **Diese Exchange-Organisation ist für die gesamte E-Mail-Übermittlung an diese Adresse verantwortlich**. Behalten Sie außerdem den Proxy von „contoso.com“ als primäre Adresse bei, so dass für Benutzer beim Senden von E-Mail-Nachrichten die Antwortadresse „user@contoso.com“ lautet (nicht „user@Org1.contoso.com“ oder „user@Org2.contoso.com“).

In einem weiteren Beispiel wird der Nachrichtenfluss in einer Hub-and-Spoke-Topologie veranschaulicht. In diesem Bespiel sind mehrere Exchange-Organisationen vorhanden, jedoch können alle Benutzer in einem einzigen Domänenraum adressiert werden (z. B. „@example.com“). In diesem Fall werden alle externen E-Mail-Nachrichten, die an „@example.com“ adressiert sind, an eine Organisation namens „OrgA“ mit einem zentralen Hub geleitet. Die Konfiguration von „OrgA“ enthält für jede Spoke-Organisation eine sekundäre SMTP-Proxyadresse. Eine dieser Adressen lautet „@OrgB.example.com“. Wenn in „OrgA“ eine an „BenutzerB@example.com“ gerichtete E-Mail eintrifft, wird die E-Mail in den Kontakt aufgelöst und an „OrgB“ umgeleitet. Wenn die Nachricht „OrgA“ verlässt, wird die Zeile **An** in die Eigenschaft **TargetAddress** geändert, um Routing zu ermöglichen, jedoch bleibt in der Zeile **Antwort an** die Adresse „BenutzerB@example.com“ erhalten.

Aus den folgenden Gründen wird beim Verschieben von Empfängern aus einer Organisation in eine andere nicht verhindert, dass Benutzer auf alte E-Mail-Nachrichten antworten:

- Die Nachricht enthält weiterhin die Eigenschaft **legacyExchangeDN**, so dass Empfänger auf die Nachricht antworten können.
- Bei der GAL-Synchronisierung wird eine sekundäre X.500-Proxyadresse für den verschobenen Benutzer erstellt, so dass alte Nachrichten auf Grundlage der Eigenschaft **legacyExchangeDN** ordnungsgemäß an das neue Postfach des Benutzers weitergeleitet werden können.

Beispielsweise sendet BenutzerA eine Nachricht an BenutzerB, der derselben Organisation angehört. Später wird BenutzerA in eine andere Organisation verschoben. In der ursprünglich von BenutzerA gesendeten E-Mail ist noch immer seine Eigenschaft **legacyExchangeDN** enthalten. Bei der GAL-Synchronisierung wird in der alten Organisation ein Kontakt für BenutzerA erstellt und diesem eine X.500-Adresse mit der alten Eigenschaft **legacyExchangeDN** zugewiesen. Dadurch kann BenutzerB auf die alte E-Mail-Nachricht antworten. Diese Antwort wird ihrerseits ordnungsgemäß an die Eigenschaft **TargetAddress** von BenutzerA weitergeleitet. Wenn ein Postfach sehr häufig verschoben wird, kann die Liste der sekundären Proxyadressen sehr groß werden.

SMTP-Relayserver

Wenn Sie die gesamten E-Mails mit einem SMTP-Relayserver aus dem Internet in die richtige Gesamtstruktur weiterleiten möchten, wird empfohlen, dass Sie selbst einen SMTP-Relayserver einrichten. Erstellen Sie auf dem SMTP-Relayserver SMTP-Connectors zu allen anderen Gesamtstrukturen, so dass E-Mail-Nachrichten direkt an die entsprechende Gesamtstruktur weitergeleitet werden. Diese Konfiguration bietet Ihnen die Möglichkeit, zum Lastenausgleich nach Anforderung weitere SMTP-Server hinzuzufügen. Sie können auch SMTP-Connectors hinzufügen, um die gesamte ausgehende Internetmail durch die neue Gesamtstruktur weiterzuleiten.

Konfigurieren von globalen Einstellungen

Um E-Mail-Features, wie z. B. Abwesenheitsantworten, automatische Antworten und Übermittlungsberichte, zu aktivieren oder zu deaktivieren, konfigurieren Sie für die entsprechenden Domänen Internet-Nachrichtenformate. Zum Konfigurieren von Internet-Nachrichtenformaten stehen die folgenden drei Methoden zur Verfügung:

- Konfigurieren Sie die Standarddomäne (*****) so, dass für alle Domänen dieselben Einstellungen gelten.
- Fügen Sie für jeden SMTP-Namespace eine getrennte Domäne für das Internet-Nachrichtenformat hinzu (z. B. „@OrgA.contoso.com“), und konfigurieren Sie anschließend die einzelnen Domänen unterschiedlich.
- Fügen Sie eine Domäne für das Internet-Nachrichtenformat hinzu, die Domänen mit einem allgemeinen Suffix repräsentiert (z. B. „@*.contoso.com“), und konfigurieren Sie dann die einzelnen Einträge unterschiedlich.

Die Internet-Nachrichtenformate befinden sich im Exchange-System-Manager unter **Globale Einstellungen**.

Freigeben von Frei/Gebucht-Informationen

In Unternehmen mit mehreren Exchange-Organisationen besteht eine häufige Anforderung in der Möglichkeit, Besprechungen, Termine und Kontaktinformationen mit Benutzern anderer Exchange-Organisationen zu koordinieren. Replizieren Sie diese Frei/Gebucht-Systemordner zwischen den Gesamtstrukturen daher mit dem Tool für die Replikation zwischen Organisationen. Wenn Ihr Unternehmen mit Öffentlichen Ordnern arbeitet, können Sie die Daten Öffentlicher Ordner mit dem Tool für die Replikation zwischen Organisationen auch in den Exchange-Organisationen gemeinsam verwenden.

> **Hinweis** Sie können das Tool für die Replikation zwischen Organisationen von der Exchange Server 2003-Website für Tools und Aktualisierungen downloaden (http://go.microsoft.com/fwlink/?LinkId=21316).

Das Tool für die Replikation zwischen Organisationen besteht aus zwei Programmen: dem Exchange Server-Replikations-Konfigurationdienstprogramm (**Exscfg.exe**) und dem Exchange Server-Replikationsdienst (**Exssrv.exe**). Mit Exscfg.exe erstellen Sie eine Konfigurationsdatei, mit der Exssrv.exe fortlaufend Informationen von einem Server auf einen anderen aktualisiert. Der Aktualisierungen sendende Server wird als Verleger bezeichnet, der die Aktualisierungen empfangende Server als Abonnent. Alle Replikationen erfolgen im Rahmen von MAPI-Sitzungen, die zwischen den Servern der Organisationen eingerichtet werden.

Mit dem Tool für die Replikation zwischen Organisationen werden Frei/Gebucht-Informationen für postfachaktivierte Benutzerobjekte und Kontaktobjekte für andere Organisationen veröffentlicht, vorausgesetzt, in der Zielorganisation sind entsprechende Kontaktobjekte (die bei der GAL-Synchronisierung erstellt wurden) vorhanden.
Die Kontakte werden anhand ihrer SMTP-Adressen zugeordnet. (Verwenden Sie beim Einrichten des Tools für die Replikation zwischen Organisation die Option **Frei/Gebucht-Daten des benutzerdefinierten Empfängers veröffentlichen**.) Dadurch können Sie die gesamten oder auch nur einen

Teil der Frei/Gebucht-Informationen von einer Organisation in eine andere replizieren. Jedoch werden Frei/Gebucht-Informationen nur in eine Richtung repliziert. Daher müssen Sie zwei Sitzungen einrichten, um Frei/Gebucht-Informationen in beide Richtungen zu aktualisieren.

Sie können mit dem Tool für die Replikation zwischen Organisationen keine Adressbücher oder Verzeichnisse ändern. Änderungen an Adressbüchern werden nicht an andere Organisationen weitergegeben. Diese Änderungen müssen Sie getrennt verarbeiten.

Ähnlich wie bei Frei/Gebucht-Informationen können Sie die gesamten oder nur einen Teil der Daten Öffentlicher Ordner von einer Organisation in andere replizieren. Im Gegensatz zu Frei/Gebucht-Informationen können Sie Öffentliche Ordner vom Verleger zum Abonnenten oder auch bidirektional replizieren. Dadurch sind weniger Sitzungen erforderlich. Außerdem unterstützt eine einzige Instanz des Tools für die Replikation zwischen Organisationen bis zu fünfzehn Sitzungen. Dies ermöglich es einem Server für Öffentliche Ordner, Daten von mehreren Verlegerservern zu abonnieren. Sie können einzelne Ordner angeben oder auch Ordner und Unterordner. Außerdem können Sie die Replikationshäufigkeit, die Protokolle der Replikation von Nachrichten und Ordnern sowie die dem Replikationsvorgang zur Verfügung gestellte Verarbeitungsleistung konfigurieren.

> **Wichtig** Mit dem Tool für die Replikation zwischen Organisationen werden keine Berechtigungen für Öffentliche Ordner repliziert. Wenn ein Öffentlicher Ordner in eine andere Gesamtstruktur repliziert wird, muss der Administrator dieser Gesamtstruktur die Berechtigungen für den Öffentlichen Ordner anpassen.

Ob Sie das Tool für die Replikation zwischen Organisationen als vernetzte oder als Hub-and-Spoke-Konfiguration einrichten, ist in erster Linie von der Anzahl der Organisationen in Ihrer Umgebung abhängig. Die vernetzte Konfiguration bietet sich für bis zu vier Organisationen an. Wenn Sie jedoch über mehr als vier Organisationen verfügen, lässt sich mit dem Tool für die Replikation zwischen Organisationen eine Hub-and-Spoke-Konfiguration möglicherweise leichter verwalten.

> **Hinweis** Es ist nicht empfehlenswert, für die Replikation zwischen Organisationen eine Ringtopologie zu verwenden. Da entlang des Ringes hohe Replikationswartezeiten sehr wahrscheinlich ist, kann ein Benutzer Informationen in einer Gesamtstruktur aktualisieren, die noch nicht durch Replikation aktualisiert wurden. Hierbei kann die letzte Aktualisierung durch die replizierte Aktualisierung überschrieben werden. Außerdem hängt in einer Ringtopologie die Kommunikation innerhalb des Ringes von jeder einzelnen Verbindung ab.

Ausführliche Konfigurationsinformationen über das Tool für die Replikation zwischen Organisationen erhalten Sie beim Download des Tools. Weitere Informationen zum Tool für die Replikation zwischen Organisationen finden Sie in den folgenden Microsoft Knowledge Base-Artikeln:

- 238573, „XADM: Installing, Configuring, and Using the InterOrg Replication Utility“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=238573)
- 238642, „XADM: Troubleshooting the InterOrg Replication Utility“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=238642)

Verschieben von Postfächern und Konten zwischen Gesamtstrukturen

Zum Migrieren von Konten und Postfächern von einer Exchange 2000 oder Exchange 2003-Organisation in eine getrennte Exchange 2000 oder Exchange 2003-Organization sollten Sie zuerst das Active Directory-Migrationstool (ADMT) und anschließend den Assistenten für die Migration nach Exchange verwenden.

Erstellen Sie zuerst mit ADMT in Active Directory aktive Benutzerkonten. Es wird empfohlen, dass Sie die Option zur Migration der SIDs auswählen, damit ADMT die SID eines Quellkontos dem Verlaufsattribut des neuen Zielkontos hinzufügt. (Der Assistent für die Migration verwendet diese SIDs im nächsten Schritt für die Zuordnung von Postfächern zu Konten.)

> **Hinweis** Zum Migrieren von SIDs muss die Windows-Zieldomäne im einheitlichen Modus ausgeführt werden.

Migrieren Sie im Anschluss an die Konten die Postfächer mit dem Assistenten für die Migration. Wenn Sie mit ADMT die SIDs migriert haben, verwendet der Assistent für die Migration diese SIDs, um den neuen Konten die Postfächer zuzuordnen und anschließend die Konten in postfachaktivierte Benutzerkonten zu konvertieren. Wenn Sie im ersten Schritt die SIDs nicht migriert haben, ist der Assistent für die Migration nicht in der Lage, ein Postfach einem Konto zuzuordnen. und erstellt stattdessen für die Zuordnung des Postfachs ein deaktiviertes Benutzerkonto.

In einigen Fällen müssen Sie möglicherweise zuerst die Postfächer und anschließend die Konten migrieren. In diesen Fällen erstellt der Assistent für die Migration deaktivierte Benutzerkonten, um die Postfächer zu speichern, und ordnet anschließend externen Windows NT-Konten neue Postfächer zu. Wenn Sie später mit ADMT Konten migrieren, werden in Active Directory neue Konten erstellt. Daher enthält Active Directory zwei Objekte, die sich auf denselben Benutzer beziehen. Führen Sie diese doppelten Objekte mit dem Assistenten für die Active Directory-Kontenbereinigung (**Adclean.exe**) zusammen. **Adclean.exe** wurde zusammen mit Exchange installiert, und Sie können den Assistenten über den Exchange-System-Manager starten (klicken Sie auf **Start**, zeigen Sie auf **Programme**, zeigen Sie auf **Microsoft Exchange**, zeigen Sie auf **Bereitstellung**, und klicken Sie dann auf **Assistent für die Active Directory-Kontenbereinigung**).

Im Zusammenhang mit dem Verschieben von Postfächern zwischen Gesamtstrukturen sind folgende Einschränkungen zu beachten. Planen Sie diese Situationen ein, und weisen Sie die Benutzer auf die vor und nach dem Verschieben durchzuführenden Schritte hin:

- Mit Outlook-Profilen können zwischen Gesamtstrukturen verschobene Benutzer nicht aufgelöst werden. Nachdem ein Benutzer verschoben wurde, muss das Profil mit dem Namen des neuen Servers aktualisiert werden, auf den der Benutzer verschoben wurde. Das Exchange-Profilaktualisierungstool (**Exprofre.exe**) ist ein Befehlszeilentool, das Sie auf Clientcomputern ausführen, um Outlook-Profile von Benutzern automatisch zu aktualisieren. Durch Exprofre.exe wird das Outlook-Standardprofil so geändert, dass Benutzer sich nach dem Verschieben bei ihren Postfächern anmelden können. Dieses Tool steht auf der Exchange Server 2003-Website für Tools und Aktualisierungen (http://go.microsoft.com/fwlink/?linkid=21316) zur Verfügung.
- Wenn Sie das Exchange-Cachemodus-Feature von Outlook verwenden, stellen Sie sicher, dass nach der Migration der Konten die neuen Profile auf dem Computer des Benutzers mit den richtigen OST-Dateien verbunden werden. Dadurch entfällt die Notwendigkeit, die OST-Dateien neu zu synchronisieren. Stellen Sie vor dem Verschieben der Benutzer außerdem sicher, dass diese ihre gesamten Offlinedateien mit dem Exchange-Server synchronisiert haben.
- Die Postfach-ACLs (Access Control Lists, Zugriffssteuerungslisten) und Stellvertreterberechtigungen bleiben beim Verschieben in eine andere Gesamtstruktur nicht erhalten.
- Veröffentlichte Zertifikate werden beim Verschieben nicht migriert. Außerdem können Sie nach dem Verschieben die Schlüsselverwaltungsdienst-Zertifikate nicht wiederherstellen. Zur Wiederherstellung dieser Zertifikate ist ein Domänenname erforderlich.
- Regeln bleiben bei einer gesamtstrukturübergreifenden Verschiebung nicht erhalten.

Weitere Informationen zur Verwendung des Assistenten für die Migration nach Exchange finden Sie im *Bereitstellungshandbuch für Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=14576).

Planen einer Standortkonsolidierung

Die Standortkonsolidierung umfasst das Verlagern von Microsoft® Exchange-Servern von Remotestandorten an einen größeren zentralen Standort, wobei Remotebenutzer über das Netzwerk auf ihre Postfächer und Öffentliche Ordner zugreifen können.

Die Standortkonsolidierung bietet die folgenden Vorteile:

- Die Exchange-Topologie wird vereinfacht.
- Sie können Exchange zentral verwalten und Verwaltungskosten verringern.
- Sie können die Hardware besser verwenden, da es weniger Postfach- und Hilfsserver (wie Server für Öffentliche Ordner, Frei/Gebucht-Server, Connectors, Bridgeheadserver usw.) gibt. Mit einem zentralisierten Rechenzentrum kann auch Skalierbarkeit und Verfügbarkeit gesteigert werden.
- Die Konsolidierung von Standorten kann Sie dabei unterstützen, Exchange in Ihrer Organisation im einheitlichen Modus auszuführen, indem die Anzahl der Exchange 5.5-Server vermindert wird.
- Mit weniger Postfachservern gibt es bei Sicherheitsproblemen weniger Angriffsziele.

  Hinweis Bezüglich der Standortkonsolidierung gibt es Einschränkungen. In diesem Kapitel werden diese Einschränkungen und weitere Überlegungen erläutert, mit denen Sie sich vertraut machen sollten, bevor Sie mit der Standortkonsolidierung beginnen.

Vor Exchange 2003 SP1 war es für die Konsolidierung von Standorten durch Verschieben von Exchange-Daten zwischen administrativen Gruppen erforderlich, dass die Exchange-Organisation im einheitlichen Modus betrieben wurde. Mit Exchange 2003 SP1 kann die Organisation jedoch auch den gemischten Modus verwenden. Wenn Sie aktuell Exchange 5.5 ausführen, müssen Sie nicht die Exchange 5.5-Server aller Standorte auf Exchange 2000 oder Exchange 2003 aktualisieren. Stattdessen können Sie sich von den Standortkonsolidierungstools, die in den Exchange Server-Bereitstellungstools des SP1 enthalten sind, durch den Vorgang führen lassen, in dem Postfächer, Verteilerlisten, benutzerdefinierte Empfänger und Öffentliche Ordner an den zentralen Standort verschoben und die Exchange 5.5-Server in den Ruhestand geschickt werden.

> **Hinweis** Wenn in Ihrer Organisation auf keinem Server Exchange 5.5 ausgeführt wird, die Organisation jedoch im gemischten Modus betrieben wird, oder wenn es relativ einfach ist, die Exchange 5.5-Server aus den Remotestandorten zu entfernen, wird empfohlen, dass Sie in den einheitlichen Modus umschalten, bevor Sie mit der Standortkonsolidierung beginnen. Durch dieses Vorgehen wird der Aufwand minimiert und die Probleme im Zusammenhang mit dem Verschieben von Exchange-Daten zwischen Standorten und administrativen Gruppen werden vermieden.

In diesem Kapitel werden die Probleme und das empfohlene Vorgehen bei der Standortkonsolidierung erläutert, wenn die Exchange-Organisation im gemischten Modus betrieben wird.

Wichtige Überlegungen für die Standortkonsolidierung im gemischten Modus

Bevor Sie die Konsolidierung von Exchange-Remotestandorten in Betracht ziehen, sollten Sie sowohl mit den folgenden Empfehlungen und Vorbedingungen in diesem Zusammenhang vertraut sein, als auch mit den Problemen, die während und nach
der Standortkonsolidierung auftreten können:

- **Aktualisieren von Clientcomputern auf Microsoft Office Outlook® 2003.** Bevor Sie Standorte konsolidieren, aktualisieren Sie die Clientcomputer am Remotestandort auf Outlook 2003 und aktivieren Sie den Exchange-Cachemodus. Der Exchange-Cachemodus ist eine wichtige Komponente der Standortkonsolidierung, da Remotebenutzer unabhängig davon, ob gerade eine Netzwerkverbindung besteht, auf dem lokalen Cache arbeiten können. Durch die Aktualisierung von Outlook auf den Clientcomputern und die Aktivierung des Exchange-Cachemodus wird eine lokale Kopie des Postfachs eines Benutzers erstellt. Wenn Sie vor dem Verschieben von Postfächern eine lokale Kopie erstellen, vermeiden Sie den hohen Download-Datenverkehr nach dem Verschieben der Postfächer vom lokalen Standort. Dieses Vorgehen ist besonders nützlich, wenn die Netzwerkbandbreite zwischen dem Remote- und dem zentralen Standort begrenzt ist. Obwohl Clientcomputer mit früheren Versionen von Outlook
und andere E-Mail-Anwendungen unterstützt werden, können diese Clientcomputer
aus dem Exchange-Cachemodus keinen Vorteil ziehen. Um Supportprobleme zu minimieren, sollten Sie außerdem Outlook 2003-Schulungen und -vorbereitungen
für Endbenutzer in den Aktualisierungsvorgang einplanen.
- **Aktualisieren von ADC auf Exchange 2003 SP1.** Verwenden Sie die Exchange 2003 SP1-Version von ADC (Active Directory Connector), in der
neue Funktionen enthalten sind, mit denen Objekte und Verteilerlisten nach
der Standortkonsolidierung bereinigt werden. Wenn Sie Postfächer zwischen
Standorten verschieben, aktualisiert ADC die Benutzerobjekte und Verteilergruppen, denen der Benutzer zugeordnet ist. Dadurch werden Änderungen zwischen Verzeichnissen repliziert und die Benutzer können weiterhin E-Mail-Nachrichten empfangen.
- **Konsolidieren von Microsoft Windows®-Domänen, sofern möglich.** Um Probleme beim Einstellen von Stellvertretern, Veröffentlichen von Zertifikaten
der Schlüsselverwaltungsdienste und Aktualisieren von Gruppen durch Outlook zu verhindern, wird empfohlen, dass Sie die Windows-Domänen der Remotestandorte und die Exchange-Postfächer gleichzeitig konsolidieren. Für den Microsoft Active Directory®-Verzeichnisdienst ist erforderlich, dass Outlook einen globalen Katalogserver verwendet, der sich in derselben Domäne wie das Objekt befindet, das Outlook aktualisieren möchte. Beispielsweise kann ein Benutzer, dessen Benutzerobjekt sich in der Remotedomäne befindet und der sich in der zentralen Domäne bei Outlook anmeldet, keine Stellvertreter einstellen. Der Grund hierfür ist, dass sich Outlook an die zentrale Domäne richtet, die Benutzerobjekte sich jedoch
in der Remotedomäne befinden. Der globale Katalogserver der zentralen Domäne enthält eine schreibgeschützte Kopie der Verzeichnisobjekte anderen Domänen. Wenn nicht die Möglichkeit besteht die Exchange- und die Windows-Domänen gleichzeitig zu konsolidieren, können Sie auf dem Outlook-Client den folgenden Registrierungsschlüssel konfigurieren, damit dieser einen globalen Katalogserver in der zentralen Domäne verwendet, in der sich die Verzeichnisobjekte befinden:

  Ort: HKEY_CURRENT_USER\Software\Microsoft\Exchange \Exchange Provider

  Name: DS Server

  Datentyp: REG_SZ (Zeichenfolge)

Wert: <vollqualifizierter Domänenname des globalen Katalogservers>

- **Anwenden des Hotfix für die DS/IS-Konsistenzanpassung (Directory Service/Information Store) und Verwenden der Anpassung zum Aufrechterhalten des Zugriffs auf Öffentliche Ordner in Exchange 5.5.** Wenn Sie Benutzer und Gruppen an den zentralen Standort verschieben, bevor Sie Öffentliche Ordner in Exchange 5.5 verschieben, sind die ACLs (Access Control Lists, Zugriffssteuerungslisten) der Öffentlichen Ordner falsch und die Benutzer können nicht auf die Öffenlichen Ordner zugreifen. Dieses Problem können Sie mit den beiden folgenden Optionen umgehen:
  - **Option 1**: Nach dem Verschieben der Benutzer und Gruppen können Sie die DS/IS-Anpassung ausführen und dadurch die ACLs der öffentlichen Ordner mit den neuen Informationen der Benutzer und Gruppen aktualisieren.
  - **Option 2**: Sie können zuerst die Öffentlichen Ordner an den zentralen Standort replizieren und dann die Benutzer und Gruppen verschieben. Stellen Sie außerdem sicher, dass Bezüge auf Öffentliche Ordner über die Connectors aktiviert sind.

    Hinweis Wenden Sie auf alle Exchange 5.5-Server mit Öffentlichen Ordnern den Hotfix für die Exchange 5.5-DS/IS-Konsistenzanpassung (verfügbar unter http://go.microsoft.com/fwlink/?linkid=3052&kbid=836489) an, bevor Sie mit der Konsolidierung von Exchange 5.5-Standorten beginnen. Nach einer Verschiebung von einem Standort zum anderen garantiert dieser Hotfix die korrekte Aktualisierung der ACLs von Öffentlichen Ordnern, so dass Benutzer und Gruppen weiterhin auf diese zugreifen können.

Kommentar [bb1]: Localization: This article will be public by the SP1 release date (5/12). It is crucial that this doc not be posted until that time.

- **Planen der vollständigen Downloads des Offlineadressbuchs.** Bevor Sie mehrere Postfächer zwischen Standorten verschieben, sollten Sie feststellen, ob Sie über ausreichend Bandbreite verfügen, um den vollständigen Download des Offlineadressbuchs für die Outlook-Clientcomputer aller Remotestandorte zu unterstützen. Weitere Informationen über die Gründe für einen vollständigen Download des Offlineadressbuchs finden Sie weiter unten in diesem Kapitel unter „Download des Offlineadressbuchs“.
- **Aktualisieren von Outlook-Profilen nach dem Verschieben von Postfächern.** Nachdem Sie Postfächer zwischen administrativen Gruppen verschoben haben, müssen Sie die Outlook-Profile aktualisieren, so dass die Benutzer sich bei den verschobenen Postfächern anmelden können. Das Exchange-Profilaktualisierungstool (**Exprofre.exe**) ist ein Befehlszeilentool, das Sie auf Clientcomputern ausführen, um Outlook-Profile von Benutzern automatisch zu aktualisieren. Durch **Exprofre.exe** wird das Outlook-Standardprofil so geändert, dass Benutzer sich nach dem Verschieben bei ihren Postfächern anmelden können. Dieses Tool steht auf der Exchange Server 2003-Website für Tools und Aktualisierungen (http://go.microsoft.com/fwlink/?linkid=21316) zur Verfügung.

Download des Offlineadressbuchs

Auf Outlook-Clientcomputern, die den Exchange-Cachemodus verwenden, ist zum Auflösen von E-Mail-Adressen ein Offlineadressbuch erforderlich. Das Offlineadressbuch ist auf einem Server für öffentliche Ordner gespeichert. In den folgenden Situationen findet ein vollständiger Download des Offlineadressbuchs statt:

- Wenn Sie einen Standort konsolidieren, wird für die Benutzer dieses Standorts, die den Exchange-Cachemodus verwenden und deren Postfächer verschoben wurden, ein vollständiger Download des Offlineadressbuchs durchgeführt. Dieser Download findet statt, wenn die entsprechenden Benutzer Outlook nach dem Verschieben des Postfachs zum ersten Mal starten.
- Wenn eine bedeutsame Anzahl an Verzeichnisänderungen stattfindet (z. B., wenn Sie viele Postfächer zwischen Standorten verschieben oder wenn Sie Änderungen an der Exchange-Topologie vornehmen), wird für die Benutzer aller Standorte, die den Exchange-Cachemodus verwenden, ein vollständiger Download des Offlineadressbuchs durchgeführt.

Weitere Informationen über die Auswirkung der vollständigen Downloads des Offlineadressbuchs und die Situationen, in denen diese stattfinden, finden Sie im Microsoft Knowledge Base-Artikel 839826 (http://go.microsoft.com/fwlink/?linkid=3052&kbid=839826).

Kommentar [bb2]: Localization : This article will be public by the SP1 release date (5/12). It is crucial that this doc not be posted until that time.

Hinweis Je nach Größe des Adressbuchs sowie der verfügbaren Bandbreite und den Wartezeiten der Verbindungen zu Remotestandorten, können die vollständigen Downloads des Offlineadressbuchs in Ihrer Organistion zu Einschränkungen führen.

Dieser umfangreiche Download kann im Netzwerk und in Outlook zu Leistungsproblemen führen. Beachten Sie beim Bestimmen der Dauer des Offlineadressbuchdownloads die Bandbreite der Netzwerkverbindungen mit den Remotestandorten, die zu übertragende Datenmenge und die Wartezeit der Netzwerkverbindung. Sie können die zu übertragende Datenmenge schätzen, indem Sie die Größe des Offlineadressbuchs mit der Anzahl der Benutzer am Remotestandort muliplizieren.

Beispiel Wenn das Offlineadressbuch 20 MB groß ist und 25 Outlook-Benutzer den Exchange-Cachemodus verwenden, beträgt die geschätzte zu replizierende Datenmenge 500 MB:

20 MB Offlineadressbuch × 25 Benutzer = 500 MB

Die Netzwerkwartezeit bezieht sich auf die Zeit, die im Netzwerk für die Übertragung von Daten von einem Punkt zu einem anderen benötigt wird. Anhand der Wartezeit können Sie bestimmen, wann eine Netzwerkverbindung überlastet ist. Mit einer langen Wartezeit ist die Datenübertragungsrate kleiner, d. h., dass eine Überlastung der Netzwerkverbindung erst später auftritt. Umgekehrt bedeutet eine kürzere Wartezeit, dass die Daten schneller übertragen werden und dadurch die Wahrscheinlichkeit steigt, dass die Verbindung überlastet wird, wenn viele Clients den Download des Offlineadressbuchs gleichzeitig durchführen.

Bevor Sie mehrere Postfächer zwischen Standorten verschieben, sollten Sie feststellen, ob Sie über ausreichend Bandbreite verfügen, um den vollständigen Download des Offlineadressbuchs für die Outlook-Benutzer am Remotestandort zu unterstützen. Außerdem sollten Sie die Auswirkung des Downloads auf das Netzwerk einschätzen, indem Sie die über das Netzwerk zu übertagende Datenmenge und die Netzwerkwartezeit berücksichtigen.

Frei/Gebucht-Funktionalität

Wenn Ihre Organisation im gemischten Modus betrieben wird und Sie Postfächer zwischen Standorten mit dem Assistenten zum Verschieben von Postfächern verschieben, aktualisiert dieser die entsprechenden Benutzobjekte mit dem neuen Attribut **legacyExchangeDN**.
Da der Assistent das Attribut **legacyExchangeDN** aktualisiert, müssen Sie keine Frei/Gebucht-Systemordner verschieben. Die Frei/Gebucht-Daten der Benutzer werden anhand des neuen Attributs **legacyExchangeDN** erneut veröffentlicht, wenn sich der Benuzter beim neuen Postfach anmeldet.

Hinweis Die Frei/Gebucht-Daten werden nicht sofort beim Verschieben von Postfächern zwischen Standorten auf den neuen Server übertragen. Stattdessen werden die Daten auf dem neuen Server 15 Minuten, nachdem der Benutzer sich beim Postfach angemeldet oder eine Kalenderaktion (wie Erstellen oder Annehmen einer Besprechungsanfrage) durchgeführt hat, veröffentlicht.

Bekannte Einschränkungen beim Standortkonsolidierungsvorgang

In diesem Abschnitt werden bekannte Einschränkungen bei der Standortkonsolidierung beschrieben. Der Standortkonsolidierungsvorgang wird von vielen Faktoren beeinflusst, beispielsweise von der Reihenfolge, in der Sie die einzelnen Schritte durchführen, dem Zeitraum, den die Replizierung der Verzeichnisinformationen in Anspruch nimmt, und dem Zeitraum, den die Replizierung der Exchange-Daten zwischen den Standorten dauert. Außerdem können weitere E-Mail-Features durch das Verschieben von Postfächern und Benutzern

zwischen Standorten beeinflusst werden. Sie sollten sich
vor der Planung der Standortkonsolidierung mit allen hier aufgeführten bekannten Problemen vertraut machen.

- **Beim Verschieben von Postfächern entsteht erhöhter Netzwerkverkehr.**
  Wenn Sie Postfächer zwischen Standorten verschieben, sollten Sie den zusätzlichen Netzwerkverkehr zwischen den Standorten einplanen. Der zusätzliche Datenverkehr entspricht der Summe der Größen der zu verschiebenden Postfächer.

- **Erhöhter Verzeichnisreplikationsverkehr.** Wenn Sie Postfächer von Exchange 5.5-Standorten an einen zentralen Exchange-Standort verschieben,
  gehen Sie von steigendem Verzeichnisreplikationsverkehr aus, während ADC
  am Remotestandort Benutzer und Verteilergruppen aktualisiert und alte Objekte entfernt. Die Dauer dieses Vorgangs variiert je nach Größe der Umgebung, der Replikationsgeschwindigkeit zwischen den Exchange 5.5-Standorten und der Replikationsgeschwindigkeit zwischen Exchange 5.5 und Active Directory. In der Standardeinstellung wird die Verzeichnisbereinigung alle 12 Stunden durchgeführt. In kleinen Umgebungen wird die Verzeichnisbereinigung möglicherweise in der nächsten automatischen Replikationssitzung abgeschlossen, in großen Umgebungen können hierfür mehrere Sitzungen erforderlich sein.

  Wichtig Sie können die Verzeichnisbereinigung beschleunigen, indem Sie
  die Replikation im Active Directory Connector-Manager und dem Administrationsprogramm von Exchange 5.5 initiieren.

- **Erhöhter Datenverkehr bei der Replikation Öffentlicher Ordner.** Wenn
  Sie Öffentliche Ordner mit dem Exchange-Migrationstool für Öffentliche Ordner (pfMigrate) an einen zentralen Standort verschieben, gehen Sie während der Aktualisierung der Öffentliche Ordner-Hierarchie und der Replikation der Öffentliche Ordner-Inhalte zwischen den Standorten von erhöhtem Datenverkehr aus. Das pfMigrate-Tool und die DS/IS-Konsistenzanpassung verursachen zusätzlichen Replikationsverkehr.

- **Möglicherweise kein Zugriff für Stellvertreter.** Um in Outlook den Zugriff für Personen mit Stellvertreterberechtigungen aufrecht zu erhalten, verschieben Sie
  die Manager und ihre Stellvertreter vom Exchange 5.5-Remotestandort an den zentralen Standort. Wenn es nicht möglich ist, sie zusammen zu verschieben, verschieben Sie zuerst den Manager und anschließend den Stellvertreter oder weisen Sie dem Stellvertreter die Zugriffsrechte nach dem Verschieben erneut zu.

- **Journalempfänger müssen erneut zugewiesen werden.** Ein Journalempfänger ist ein Benutzer, dessen Konto für den Empfang aller archivierten Nachrichten eines Postfachspeichers konfiguriert ist. Ordnen Sie die Zuweisung für den Journalempfängers einem anderen Benutzer zu, bevor Sie den aktuellen Journalempfänger zwischen den Standorten verschieben. Nach dem Verschieben können Sie den Benutzer wieder als Journalempfänger festlegen.

- **Posteingangsregeln funktionieren möglicherweise nicht.** Wenn sich das Postfach eines Benutzers nicht auf einem Server mit Exchange 2003 SP1 befindet, werden die Posteingangsregeln nicht funktionieren, die auf anderen zwischen Standorten verschobenen Benutzern aufbauen, da sich für diese das Attribut **legacyExchangeDN** geändert hat. Der Benutzer kann die Regeln jedoch wieder erstellen. Wenn sich das Postfach des Benutzers auf einem Exchange 2003 SP1-Server befindet, funktionieren die Regeln weiterhin. Dieses Problem hat keine Auswirkung auf Benutzer, deren Postfächer verschoben wurden, nur auf Benutzer mit Regeln, die auf verschobenen Benutzern aufbauen. Wenn sich die Postfächer aller Benutzer auf Exchange 2003 SP1-Servern befinden, funktionieren die Regeln wieder.

- **Benutzernamen werden in der globalen Adressliste von Exchange 5.5 möglicherweise kurzzeitig nicht angezeigt.** Möglicherweise werden in Exchange 5.5 Benutzernamen, die zwischen Standorten verschoben wurden, in der globalen Adressliste für eine kurze Zeit bis zum Abschluss der Verzeichnisreplikation nicht angezeigt. Während dieser Zeit ist das ursprüngliche Exchange 5.5-Objekt am Remotestandort ausgeblendet, und das neue Exchange 5.5-Objekt wird zum neuen Standort kopiert. Das globale Adressbuch von Exchange 2003 ist nicht betroffen.

- **Nach der Migration empfangen einige Benutzer möglicherweise Unzustellbarkeitsberichte.** Wenn nicht verschobene Exchange 5.5-Benutzer
  auf E-Mail-Nachrichten von verschobenen Exchange 5.5-Benutzern antworten, nachdem Sie Postfächer von Exchange 5.5 an den zentralen Standort verschoben haben, empfangen diese einen Unzustellbarkeitsbericht. Diese Situation bleibt bestehen, bis die Verzeichnisreplikation von Exchange 5.5 abgeschlossen ist. Diese Situation können Sie vermeiden, indem Sie die Replikation im ADC-Manager durch Auswählen von **Jetzt replizieren** erzwingen. Eine andere Möglichkeit ist, Exchange 5.5-Mail durch einen Exchange 2000- oder Exchange 2003-Bridgeheadserver umzuleiten, da diese Server in der Lage sind, E-Mail-Nachrichten an das neue Postfach weiterzuleiten.

  Hinweis Sie können Unzustellbarkeitsberichte vermeiden, indem Sie die Standortconnectors zwischen den Exchange 5.5-Standorten entfernen und Connectors zum zentralen Standort erstellen, so dass der gesamte E-Mail-Verkehr durch den zentralen Standort oder über einen Exchange 2003-Server weitergeleitet wird.

- **Ein autorisierter Benutzer muss eine Kalenderaktion durchführen, um Frei/Gebucht-Daten für Ressourcenpostfächer erneut zu veröffentlichen.** Wenn Sie Postfächer zwischen Standorten verschieben, werden die Frei/Gebucht-Daten nicht auf den neuen Server übertragen. Für Benutzer werden die Frei/Gebucht-Daten
  auf den neuen Servern 15 Minuten nachdem der Benutzer sich beim Postfach angemeldet oder eine Kalenderaktion (wie Erstellen oder Annehmen einer Besprechungsanfrage) durchgeführt hat veröffentlicht. Für Ressourcenpostfächer (wie Besprechungsräume) muss jedoch jemand mit dem entsprechenden Zugriff das Postfach öffnen und eine Kalenderaktion durchführen, damit die Frei/Gebucht-Daten erneut veröffentlicht werden.

- **Für den Schlüsselverwaltungsdienst ist der Export der Zertifikate erforderlich.** Der Schlüsselverwaltungsdienst funktioniert auch nach der Verschiebung von einem Standort zum anderen, wenn Sie X.509-Zertifikate der Version 3 verwenden, nicht jedoch bei Zertifikaten der Version 1. Bei Zertifikaten der Version 1 können zwischen Standorten verschobene Benutzer alte E-Mail-Nachrichten entschlüsseln, neue Nachrichten können jedoch nicht signiert oder verschlüsselt werden. Wenn Sie den Schlüsselverwaltungsdienst verwenden, exportieren Sie Ihre Zertifikate auch dann vor dem Verschieben von Benutzern zwischen Standorten, wenn der Dienst für den zentralen Standort von demselben Schlüsselverwaltungsdienst-Server bereitgestellt wird. Importieren Sie nach dem Verschieben die Zertifikate in den Schlüsselverwaltungsdienst-Server des zentralen Standorts. Führen Sie nach dem Verschieben das Exchange-Profilaktualisierungstool (**Exprofre.exe**) aus.

- **Für Exchange Conferencing Server muss in den einheitlichen Modus umgeschaltet werden.** Wenn Sie Exchange Conferencing Server ausführen, sollten Sie zuerst in den einheitlichen Exchange-Modus umschalten und dann die Standorte konsolidieren. Durch dieses Vorgehen können Sie Probleme mit den **legacyExchangeDN**-Attributen verhindern und eine durchgehende Funktionalität von Exchange Conferencing Server sicherstellen.

Standortkonsolidierung im gemischten Modus

Wenn an den zu konsolidierenden Standorten Exchange 5.5 ausgeführt wird, müssen Sie die Exchange 2003 SP1-Standortkonsolidierungstools verwenden, um sicherzustellen, dass Postfächer, Verteilerlisten, Empfänger und Öffentliche Ordner ordnungsgemäß und mit der geringsten Dienstunterbrechung verschoben werden. Dadurch soll nach dem Verschieben der Benutzer und Exchange-Daten an den zentralen Standort die ordnungsgemäße Übertragung von E-Mail-Nachrichten sichergestellt werden.

Führen Sie vor dem Konsolidieren der Inhalte von den Remotestandorten die folgenden Aktionen durch:

- Überprüfen Sie, ob Sie am zentralen Standort über ausreichend Serverressourcen verfügen, um die Exchange-Dienste zu bewältigen.

- Aktualisieren Sie am zentralen Standort alle Postfachserver und Server für Öffentliche Ordner auf Exchange 2003 SP1.
- Wenden Sie auf alle Exchange 5.5-Server für Öffentliche Ordner den Hotfix für die Exchange 5.5-DS/IS-Konsistenzanpassung an (verfügbar unter http://go.microsoft.com/fwlink/?linkid=3052&kbid=836489). Nach einer Verschiebung von einem Standort zum anderen garantiert dieser Hotfix die korrekte Aktualisierung der ACLs von Öffentlichen Ordnern, so dass Benutzer und Gruppen weiterhin auf diese zugreifen können.

  Wichtig Wenden Sie den Hotfix für die Exchange 5.5-DS/IS-Konsistenzanpassung an, bevor Sie mit der Standortkonsolidierung beginnen. Für die Standortkonsolidierungstools ist dieser Hotfix erforderlich.
- Aktualisieren Sie alle ADC-Server (Active Directory Connector) auf Exchange 2003 SP1. Stellen Sie sicher, dass die Verbindungsvereinbarungen mit allen Standorten in beide Richtungen gelten und dass an den Quell- und Zielstandorten Verbindungsvereinbarungen für Öffentliche Ordner vorhanden sind.

  Hinweis Es wird dringend empfohlen, dass Sie die Verbindungsvereinbarungen mit den ADC-Tools konfigurieren, um sicherzustellen, dass die Verzeichnisse ordnungsgemäß aktualisiert und die Mitgliedschaften in Verteilerlisten ordnungsgemäß bereinigt werden.

Gehen Sie bei der Konsolidierung von Standorten im gemischten Modus von Exchange folgendermaßen vor:

1. Erstellen Sie einen Standortkonsolidierungsplan. Erstellen Sie für jeden Standort einen dreistufigen Standortkonsolidierungszeitplan. Planen Sie die Replikation für Zeiten geringer Auslastung ein, z. B. für ein Wochenende. Stellen Sie sicher, dass am zentralen Standort Exchange 2003 bereitgestellt ist und dass Sie eine Koexistenz mit Exchange 5.5 eingerichtet haben. Aktualisieren Sie alle Exchange 2003-Zielserver auf Exchange 2003 SP1. Wenn Sie Outlook im Exchange-Cachemodus verwenden möchten, installieren Sie an allen Standorten Outlook 2003 und aktivieren Sie den Exchange-Cachemodus.

2. Die neueste Version der Exchange Server-Bereitstellungstools (verfügbar unter http://go.microsoft.com/fwlink/?LinkId=21231) enthält die Standortkonsolidierungstools, die Sie durch den Prozess des Verschiebens von Postfächern, Verteilerlisten, benutzerdefinierten Empfängern und Öffentlichen Ordnern an den zentralen Standort und der Abschaltung von Exchange 5.5-Servern führt. Verwenden Sie die Tools zur Vorbereitung der Standortkonsolidierung wie folgt:

   - Aktualisieren Sie alle ADC-Server auf Exchange 2003 SP1.
   - Wenden Sie auf allen Servern für Öffentliche Ordner den Hotfix für die DS/IS-Konsistenzanpassung an.
   - Fügen Sie dem zentralen Standort Replikate Öffentlicher Ordner hinzu, und planen Sie Zeit für die Replikation der Öffentlichen Ordner ein.

3. Verschieben Sie Exchange-Daten mit den Exchange Server-Bereitstellungstools an den zentralen Standort:

   - **Postfächer** Konsolidieren Sie die Inhalte vom Remotestandort an den zentralen Standort, indem Sie die Postfächer verschieben und die Benutzerprofile mit **Exprofre.exe** aktualisieren.
   - **Benutzerdefinierte Empfänger und Verteilerlisten** Aktualisieren Sie benutzerdefinierte Empfänger und Verteilerlisten, so dass sie den zentralen Standort wiederspiegeln, mit dem Tool zur Veränderung des Stammservers für das Objekt, das sie tatsächlich an den zentralen Standort verschiebt. Stellen Sie sicher, dass die richtigen Verbindungsvereinbarungen eingerichtet sind.

4. Folgen Sie den in den Exchange Server-Bereitstellungstools beschriebenen Schritten, um den Remotestandort zu entfernen:

   - Entfernen Sie die Replikate Öffentlicher Ordner mit PFMigrate, und folgen Sie anschließend dem Vorgehen zur Abschaltung von Exchange 5.5-Servern.
   - Stellen Sie mit dem Tool zur Veränderung des Stammservers für das Objekt sicher, dass die Verteilerlisten und benutzerdefinierten Empfänger erfolgreich vom Remotestandort entfernt wurden.

   Wiederholen Sie diese Schritte für jeden Standort, den Sie konsolidieren möchten.

5. Vollständige Anweisungen finden Sie in den folgenden Ressourcen:

- *Exchange 2003: Exchange-Bereitstellungstools* (http://go.microsoft.com/fwlink/?LinkId=21231)
- *Bereitstellungshandbuch für Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=21768)

Standortkonsolidierungstools

Beim Konsolidieren von Standorten gibt es möglicherweise viele Postfächer, Verteilerlisten, Kontakte und Öffentliche Ordner, die zwischen administrativen Gruppen verschoben werden müssen. Außerdem ändert sich nach dem Verschieben zwischen administrativen Gruppen der vorherige Exchange-DN (Distinguished Name) eines Objekts, und dies hat Auswirkungen auf die von diesem Attribut (**legacyExchangeDN**) abhängigen Dienste. Die folgenden Features und Tools von Exchange 2003 SP1 betreffen diese Punkte:

- **Exchange Server-Bereitstellungstools** Die neueste Version der Exchange Server-Bereitstellungstools führt Sie durch den Prozess des Verschiebens von Postfächern, Verteilerlisten, benutzerdefinierten Empfängern und Öffentlichen Ordnern an den zentralen Standort sowie der Abschaltung von Exchange 5.5-Servern. Die neuesten Exchange Server-Bereitstellungstools sind erhältlich unter http://go.microsoft.com/fwlink/?LinkId=21231.
- **Assistent zum Verschieben von Postfächern in Exchange 2003 SP1** Die Version des Assistenten zum Verschieben von Postfächern in Exchange 2003 SP1 bietet die Möglichkeit, Postfächer zwischen administrativen Gruppen zu verschieben.

  Wenn sich Ihre Exchange-Organisation im gemischten Modus befindet, zeigt Exchange 2003 in der Standardeinstellung für jeden Exchange 5.5-Standort eine administrative Gruppe und eine Routinggruppe an. Wenn in Ihrer Organisation vor Exchange 2003 SP1 Exchange 5.5-Server verwendet wurden, konnten Postfächer nur innerhalb derselben administrativen Gruppe verschoben werden. Dies bedeutete, dass Exchange 5.5-Remotestandorte nicht einfach an einen zentralen Exchange-Standort konsolidiert werden konnten.

  In Exchange 2003 SP1 können Postfächer im Exchange-System-Manager mit dem Assistenten zum Verschieben von Postfächern oder mit Active Directory-Benutzer und -Computer zwischen administrativen Gruppen verschoben werden.
- **Exchange-Profilaktualisierungstool** Das Exchange-Profilaktualisierungstool (**Exprofre.exe**) ist eine eigenständige ausführbare Datei zur automatischen Aktualisierung von Outlook-Benutzerprofilen. Die Benutzer können sich dadurch
  auch nach dem Verschieben zwischen administrativen Gruppen an ihren Postfächern anmelden. Um das Standardprofil zur Wiedergabe der neuen Informationen in Outlook zu aktualisieren, muss auf jedem Clientcomputer **Exprofre.exe** ausgeführt werden.
  Es wird empfohlen, dieses Tool über ein Anmeldeskript auszuführen.
- **Migrationstool für Öffentliche Ordner** Es wird empfohlen, Replikate von Öffentlichen Ordnern in Exchange 5.5 auf Exchange 2003-Servern zu erstellen. Durch die Erstellung von Replikaten haben die

Benutzer weiterhin Zugriff auf die Öffentlichen Ordner, nachdem sie vom Remotestandort an den zentralen Standort verschoben wurden.

Mit dem Migrationstool für Öffentliche Ordner (PFMigrate) können Öffentliche Ordner von Exchange 5.5-Remoteservern zum zentralen Exchange 2003-Server verschoben werden. Die neueste Version von PFMigrate enthält eine Befehlsoption zur Standortkonsolidierung (**/sc**), um Öffentliche Ordner zwischen administrativen Gruppen zu verschieben. PFMigrate ist als Teil der Exchange Server-Bereitstellungstools erhältlich (http://go.microsoft.com/fwlink/?LinkId=21231).

- **Tool zur Veränderung des Stammservers für das Objekt** Mit dem Tool zur Veränderung des Stammservers für das Objekt werden Verteilerlisten und Kontakte von Exchange 5.5-Remoteservern zum zentralen Exchange 2003-Server verschoben. Aktualisieren Sie bei der Standortkonsolidierung den vorherigen Distinguished Name für benutzerdefinierte Empfänger und Verteilerlisten mithilfe des Tools zur Veränderung des Stammservers für das Objekt mit dem zentralen Standort. Die Aktualisierung dieser Objekte stellt sicher, dass sie nach dem Entfernen des Remotestandorts nicht verloren gehen.

  Das Tool aktualisiert gleichzeitig den Server für die Aufgliederung der Verteilergruppen auf den von Ihnen angegebenen Server. Wenn Sie den Server für die Aufgliederung der Verteilergruppen von allen Verteilerlisten entfernen möchten, können Sie die Option **Server** leer lassen, damit die Verteilerlisten alle Server für die Aufgliederung der Verteilergruppen verwenden. Das Tool zur Veränderung des Stammservers für das Objekt ist erhältlich als Teil der Exchange Server-Bereitstellungstools (http://go.microsoft.com/fwlink/?LinkId=21231).

Szenario einer Standortkonsolidierung: Proseware, Inc.

Proseware, Inc. beschäftigt landesweit in fünf Filialen über 500 Menschen. Die Firmenzentrale in Seattle ist mit über 200 Mitarbeitern die größte Filiale. Die Firma verfügt über vier regionale Filialen mit Verbindungen mit hoher Bandbreite in Denver, Phoenix, Los Angeles und Miami.

Die Exchange-Dienste werden folgendermaßen verteilt:

- Die Firmenzentrale in Seattle verfügt über einen Exchange 5.5-Server, auf dem sich Öffentliche Ordner und Postfächer für 200 Benutzer befinden.
- Jede regionale Filiale verfügt über einen Exchange 5.5-Server, auf dem sich Öffentliche Ordner und Postfächer für 50 bis 100 Benutzer befinden.

Jede regionale Filiale verfügt über einen eigenen IT-Administrator, der für die Verwaltung der lokalen Server zuständig ist. Der Großteil der Server befindet sich jedoch in der IT-Organsiation in Seattle und wird dort verwaltet. Proseware, Inc. plant eine Aktualisierung auf Exchange 2003 und möchte gleichzeitig seine Exchange-Standorte konsolidieren. Support und Überwachungsvorgänge wurden kürzlich zentralisiert. Dies soll nun auch mit der Exchange-Verwaltung geschehen. Außerdem wächst die Benutzerbasis, die Postfachdaten und die Verwendung Öffentlicher Ordner nehmen zu und die Exchange-Server erreichen das Ende ihrer Lebensdauer.

Zur Anpassung an diese Umstände plant Proseware, Inc. die Einrichtung eines Rechenzentrums in Seattle, das Exchange-Dienste für die Standorte bereitstellen soll. Proseware, Inc. aktualisiert auf Outlook 2003 und verwendet den Exchange-Cachemodus. Um die Erreichbarkeit und Skalierbarkeit zu maximieren, soll das Rechenzentrum auf die Vorteile von Clustering und Sicherungen mithilfe des Volumeschattenkopie-Dienstes in Microsoft Windows Server™ 2003 zurückgreifen.

Obwohl allgemein empfohlen wird, vor einer Standortkonsolidierung in den einheitlichen Modus von Exchange zu schalten, wählt Proseware, Inc. aufgrund der Kosten, die beim Aktualisieren aller Exchange 5.5-Server auf Exchange 2003 entstehen würden nicht diesen Weg. Stattdessen sollen die Tools zur Standortkonsolidierung von

Exchange 2003 SP1 verwendet werden, um die Exchange-Daten zum zentralen Standort zu verschieben und die Exchange 5.5-Server aufzugeben.

Im letzten Teil dieses Abschnitts wird der Vorgang der Standortkonsolidierung von Proseware, Inc beschrieben.

Erstellen eines Standortkonsolidierungsplans

Zuerst setzt sich Proseware, Inc. mit den Tools zur Standortkonsolidierung, den Fragestellungen und den Anforderungen auseinander. Es wird ermittelt, ob genügend Serverressourcen im Rechenzentrum in Seattle vorhanden sind, um die Exchange-Dienste für alle regionalen Filialen unterstützen zu können.

Bei der Untersuchung der E-Mail-Anforderungen der Benutzer zeigt sich, dass die Ingenieure in der Filiale in Denver regelmäßig sehr große Dateien per E-Mail austauschen. Da für diesen Standort erforderlich ist, dass große Dateien über WAN-Verbindungen verschickt werden können, ist die Verlegung des Exchange-Servers vom Standort Denver zum zentralen Standort nicht praktikabel. Deshalb entscheidet Proseware, Inc. einen Exchange-Server in der Filiale Denver zu belassen. Der Server wird von Exchange 5.5 auf Exchange 2003 aktualisiert.

Nachdem festgelegt wurde, welche Standorte zu konsolidieren sind, wird ein Plan zur Standortkonsolidierung erstellt. Der Zeitplan für den Übergang wird für alle Filialen festgelegt. Aufgrund der durch die Replikation verursachten Netzwerkwartezeit wird entschieden, die Verschiebung der Öffentlichen Ordner und Postfächer am Wochenende vorzunehmen, wenn die geringste Netzwerkauslastung zu erwarten ist.

Bevor mit der Standortkonsolidierung begonnen wird, wird Exchange 2003 im Rechenzentrum in Seattle bereitgestellt, um sicherzustellen, dass Exchange im gemischten Modus ausgeführt wird. Insbesondere werden die Schritte und Tools der Exchange Server-Bereitstellungstools verwendet, um den ersten Exchange 2003-Server einzurichten und zu ermöglichen, dass Exchange 5.5 und Exchange 2003 nebeneinander bestehen können.

Da der Exchange-Cachemodus verwendet werden soll, werden auch die Clientcomputer in allen vier regionalen Filialen auf Outlook 2003 aktualisiert. Der Exchange-Cachemodus wird aktiviert, um eine lokale Kopie aller Postfächer der Benutzer zu erstellen. Durch die Erstellung einer lokalen Kopie vor dem Verschieben der Postfächer, wird der hohe Download-Datenverkehr nach dem Verschieben der Postfächer vom lokalen Standort vermieden.

Schließlich wird ein Probelauf mit Testpostfächern durchgeführt, bevor die tatsächliche Standortkonsolidierung beginnt. Der Test ermöglicht die Überprüfung des Vorgangs und das Sammeln von Daten bezüglich der Netzwerkbeeinträchtigungen und der Replikationsdauer.

Phase 1: Vorbereitungen für die Standortkonsolidierung

Proseware, Inc. beginnt mit der Standortkonsolidierung. Zuerst wird die Filiale in Phoenix konsolidiert. Folgende Schritte werden durchgeführt, wie in den Exchange Server-Bereitstellungstools beschrieben:

1. Proseware, Inc. vergewissert sich, dass alle ADC-Server auf die ADC-Version in Exchange 2003 SP1 aktualisiert wurden. Mit ADC-Tools wird überprüft, ob alle ADC-Verbindungsvereinbarungen ordnungsgemäß konfiguriert sind.

2. Proseware, Inc. aktualisiert alle Exchange 5.5-Server mit Öffentlichen Ordnern in allen vier regionalen Filialen mit dem Hotfix für die DS/IS-Konsistenzanpassung.

3. Am Freitagabend werden dem Exchange 2003-Server in Seattle mithilfe von PFMigrate Replikate der Öffentlichen Ordner hinzugefügt. Der Replikationsvorgang wird über das Wochenende fortgesetzt.

Phase 2: Konsolidieren von Standorten im gemischten Modus

Nachdem die Replikation der Öffentlichen Ordner erfolgreich abgeschlossen ist, wird der Standort Phoenix konsolidiert. Da die Verschiebung von Postfächern und die Verwendung des Tools zur Veränderung des Stammservers für das Objekt unter Umständen lange Wartezeiten mit sich bringen, wird diese Phase am Wochenende ausgeführt. Mit den Exchange Server-Bereitstellungstools werden die folgenden Schritte durchgeführt:

1. Proseware, Inc. verschiebt die Postfächer von Phoenix mit dem Assistenten zum Verschieben von Postfächern an den zentralen Standort.
2. Proseware, Inc. erstellt ein Anmeldeskript, das **Exprofre.exe** ausführt, wenn Benutzer sich am Montagmorgen anmelden. Dieses Skript aktualisiert die Outlook-Profile der Benutzer, so dass sie den neuen Standort widerspiegeln.
3. ADC-Tools wird erneut ausgeführt, um zu überprüfen, ob die geeigneten Verbindungsvereinbarungen festgelegt wurden. Die Vollständigkeit der Verzeichnisreplikation wird überprüft.
4. Mit dem Tool zur Veränderung des Stammservers für das Objekt werden die benutzerdefinierten Empfänger und Verteilerlisten in Phoenix aktualisiert, um den Standort in Seattle widerzuspiegeln.
5. Anschließend wird ADC-Tools nochmals ausgeführt, um zu überprüfen, ob die geeigneten Verbindungsvereinbarungen festgelegt wurden. Die Vollständigkeit der Verzeichnisreplikation wird überprüft.
6. Auf dem Exchange 5.5-Server in Phoenix wird die DS/IS-Konsistenzanpassung ausgeführt, um die ACLs für Öffentliche Ordner zu bereinigen.

Phase 3: Entfernen des Remotestandorts

Nach dem Abschluss von Phase 2 vergewissert sich Proseware, Inc., dass sich alle Exchange-Daten auf dem Exchange 2003-Server in Seattle befinden. Der Exchange-Server in Phoenix wird abgeschaltet. Mit den Exchange Server-Bereitstellungstools werden die folgenden Schritte durchgeführt:

1. Mit PFMigrate werden die Replikate der Öffentlichen Ordner vom Standort in Phoenix entfernt.
2. ADC-Tools wird ausgeführt, um zu überprüfen, ob die geeigneten Verbindungsvereinbarungen festgelegt wurden. Die Vollständigkeit der Replikation der Öffentlichen Ordner wird überprüft.
3. Mit dem Tool zur Veränderung des Stammservers für das Objekt wird ein Bericht erstellt, um sicherzustellen, dass die Verteilerlisten und benutzerdefinierten Empfänger erfolgreich vom Server in Phoenix entfernt wurden.
4. Proseware, Inc. führt die Schritte zum Entfernen der Exchange 5.5-Server in der Filiale in Phoenix durch.

Für die Filialen in Los Angeles und Miami wird der gleiche Vorgang wiederholt. Nach dem Abschluss verfügt Proseware, Inc. über einen Exchange 2003-Server in Seattle für die Benutzer in Phoenix, Los Angeles und Miami und über einen lokalen Exchange 2003-Server in Denver für die Benutzer vor Ort. Da Exchange 5.5 nicht mehr ausgeführt wird, wechselt Proseware, Inc. abschließend in den einheitlichen Modus.

Planen der Exchange-Infrastruktur

In Kapitel 1 haben Sie Ihre Anforderungen und Bedürfnisse sowohl aus der Unternehmens- als auch aus der Benutzerperspektive beurteilt und den Status
Ihrer aktuellen Umgebung ermittelt. In diesem Kapitel finden Sie Informationen, die Ihnen das Identifizieren der technischen Anforderungen für das Microsoft® Exchange-Messagingsystem erleichtern. Wenn Sie Ihre technischen Anforderungen identifiziert haben, können Sie eine Bestandsaufnahme durchführen und so ermitteln, welche Änderungen an Ihrer bestehenden Umgebung, einschließlich der Netzwerkinfrastruktur, der Hardware und den Software-Aktualisierungen, vorgenommen werden müssen. In diesem Kapitel werden die Konzepte erläutert, die Sie bei der Planung Ihrer Exchange-Infrastruktur beachten müssen. Folgende Bereiche werden beschrieben:

- Topologische Grenzen und Beschränkungen
- Zentralisierte und verteilte Messagingsysteme
- Routing-Entwurf
- Serverplatzierung
- Serverdimensionierung und -abstimmung

Topologische Grenzen und Beschränkungen

Bevor Sie mit der Planung Ihrer Exchange-Organisation beginnen, sollten Sie sich unbedingt mit den topologischen Grenzen und Beschränkungen sowie mit den bekannten Begrenzungen einer einzelnen Exchange-Organisation vertraut machen. Je einfacher der Entwurf angelegt ist, desto leichter kann die Topologie verwaltet werden. Als allgemeine Richtlinie gilt zu beachten, dass so wenig administrative Gruppen, Routinggruppen und Domänen wie möglich erstellt werden sollten.

Einige Beschränkungen sind Bestandteil von Exchange. Eine einzelne Exchange-Organisation kann keine der folgenden Beschränkungen überschreiten:

- 1000 Exchange-Server
- 1000 administrative Gruppen
- 100 Domänen

Zusätzlich wird empfohlen, nicht mehr als 150 Routinggruppen zu erstellen.

Zentralisierte und verteilte Messagingsysteme

Wenn Ihr Unternehmen aus mehreren Zweigstellen besteht, die alle über zuverlässige Netzwerkverbindungen mit hoher Bandbreite miteinander verbunden sind, können Sie unabhängig von den jeweiligen Entfernungen zwischen den einzelnen Zweigstellen ein zentralisiertes Messagingsystem implementieren. Ein zentralisiertes Messagingsystem bedeutet, dass alle Exchange-Server in einem zentralen Datenzentrum verwaltet werden und nur eine einzige Routinggruppe vorliegt. Bei der Planung eines Messagingsystems ist es empfehlenswert, mit diesem Modell zu beginnen, da es das kosteneffektivste Modell ist und sehr einfach verwaltet werden kann.

Wenn Ihr Unternehmen über Remotezweigstellen mit unzuverlässigen Netzwerkverbindungen mit hohen Latenzzeiten und geringer Bandbreite verfügt, können Sie Routinggruppen einrichten, um das Routing des

Nachrichtenverkehrs zwischen den Standorten zu steuern. Wie bereits in den beiden vorherigen Kapiteln erläutert, bedeuten Remotestandorte und mehrere Routinggruppen jedoch nicht, dass Sie Ihr Verwaltungsmodell nicht zentralisieren können. Zusätzlich zu den Features in Microsoft Windows Server™ 2003, Exchange 2003 und Microsoft Office Outlook® 2003 steht Ihnen auch die Möglichkeit zur Verfügung, Ihre Serverhardware durch Entfernen von Exchange-Servern von Remotestandorten zu konsolidieren. Durch diese Änderungen können Benutzer sich von Remotestandorten aus bei Microsoft Windows®-Diensten und Exchange 2003 anmelden und müssen außerdem weniger Leistungsverringerungs- oder Verbindungsprobleme in Kauf nehmen.

In diesem Abschnitt werden die Eigenschaften von zentralisierten und verteilten Messagingsystemen erläutert sowie einige Richtlinien für die Planung der einzelnen Modelle beschrieben.

Eigenschaften eines zentralisierten Messagingsystems

Ein zentralisiertes Messagingsystem besteht aus einem großen Datenzentrum, auf dem sich alle Serverressourcen befinden, einschließlich der globalen Katalogserver des Microsoft Active Directory®-Verzeichnisdienstes, der Domänencontroller und der Exchange-Server. Das Datenzentrum unterstützt alle Benutzer des Messagingsystems, unabhängig davon, ob eine lokale oder eine Remoteverbindung besteht. Ein zentralisiertes Messagingsystem verfügt über die folgenden Eigenschaften:

- Daten befinden sich an einem zentralisierten Standort und werden dort verwaltet, unabhängig davon, ob die Benutzer über eine Remoteverbindung zugreifen. Im Gegensatz dazu haben die Benutzer beim verteilten Modell einen lokalen Zugriff auf Postfächer, allerdings ist hier die Serververwaltung komplexer.
- Software-Aktualisierungen können von einem zentralisierten Standort bereitgestellt werden.
- Das Datenzentrum verfügt über Vorrichtungen für eine unabhängige Stromversorgung wie zum Beispiel eine unterbrechungsfreie Stromversorgung (USV) und über Notfallpläne mithilfe von vollständig ausgestatteten („hot site“) oder nicht ausgestatteten („cold site“) Ersatzstandorten. Ein vollständig ausgestatteter Ersatzstandort ist ein zur umfassenden betrieblichen Nutzung überlassener Standort eines Dienstanbieters, der Unternehmen die Kommunikationsausrüstung zur Verfügung stellt, die im Falle eines Datenverlusts zur Weiterführung des Betriebs erforderlich ist. Ein nicht ausgestatteter Ersatzstandort ist eine Dienstleistung, bei der Räumlichkeiten zur Verfügung gestellt werden, die jedoch vom jeweiligen Unternehmen selbst ausgestattet und eingerichtet werden müssen. Ein vollständig ausgestatteter Ersatzstandort bietet dem Unternehmen die Möglichkeit, den Betrieb schneller fortzusetzen. Die preisgünstigere Lösung ist jedoch der nicht ausgestattete Ersatzstandort.

Die Zentralisierung eines Systems wird meistens dann vorgenommen, wenn Unternehmen eine Reduzierung der Kosten durchführen müssen oder auf neue Sicherheitsanforderungen reagieren möchten. Diese Anforderungen führen in der Regel zu einer Zentralisierung der Standorte (die Anzahl der Sites, die Serverressourcen bereitstellen, wird verringert), zu einer physischen Konsolidierung (kleinere Server werden durch High-End-Server ersetzt), zu einer administrativen Konsolidierung und zu Datenkonsolidierung (Speicherlösungen, die Sicherungsfunktionen und Funktionen zur Wiederherstellung von Daten nach Datenverlust enthalten, werden zentralisiert).

Wichtige Überlegungen

Ziehen Sie einen zentralisierten Entwurf nur dann in Betracht, wenn die Vorbedingungen in den folgenden Bereichen erfüllt sind oder deren Erfüllung im Projektplan vorgesehen ist:

- **Clientupdates** Wenn Sie die Bereitstellung von Exchange 2003 planen, jedoch nicht die von Outlook 2003, steht der Exchange-Cachemodus Offlinebenutzern nicht zur Verfügung, und es kommt zu keiner Leistungsverbesserung. Wenn die Netzwerkverbindungen zwischen Clientcomputern und dem vorgesehenen Datenzentrum langsam und unzuverlässig sind, sollten Sie daher eine verteilte Struktur in Erwägung ziehen.
- **Hardwarekosten des Datenzentrums** Führen Sie eine Berechnung der Kosten für die Installation von High-End-Servern und Clustern im Datenzentrum im Vergleich zu den Einsparungen an Verwaltungskosten bei einer Zentralisierung der Serverstruktur durch. Es wird empfohlen, dass Sie die Back-End-Server in einer Clusterstruktur organisieren, um das System mit einer hohen Verfügbarkeit und Redundanz auszustatten. Dies führt jedoch auch zu höheren Vorauskosten. Diese Kosten werden jedoch durch Einsparungen bei den Betriebskosten und den Kosten für die Infrastruktur sowie durch geringere Ausfallszeiten und eine größere Skalierbarkeit mehr als ausgeglichen.
- **Notfallplanung** Wenn Sie Ihren Server und Ihre Datenressourcen innerhalb der Organisation zentralisieren, erhöhen Sie die Ausfallwahrscheinlichkeit nur einmal vorhandener Systemhardware. Sie müssen daher Notfallpläne für den Fall eines schweren Datenverlustes in Ihrem Datenzentrum aufstellen.
- **Netzwerkausfälle** Bedenken Sie die Auswirkungen eines Netzwerkausfalls auf Benutzer in Remotestandorten. Wenn für diese Benutzer der Outlook Exchange-Cachemodus aktiviert ist, kann diesem Problem weniger Beachtung geschenkt werden.
- **Einsparungen bei den Betriebs- und Verwaltungskosten** Durch eine Zentralisierung der Serverressourcen werden die Betriebskosten gesenkt, da Dienstkapazitäten und Wachstum durch eine effektivere Verwendung der Ressourcen erreicht werden können. Außerdem werden die Infrastrukturkosten gesenkt, die für Speicher- und Sicherungsanforderungen anfallen.
- **Datenspeicherung** Bei größeren zentralisierten Datenmengen müssen Sie zuverlässigere Speichersysteme verwenden, um die Integrität Ihrer Daten zu verbessern. Durch eine Reduzierung der Komplexität Ihrer Serverinfrastruktur können Sie außerdem leichter Dienste und Daten wiederherstellen, wenn ein Fehler auftritt.
- **LAN- und WAN-Verbindungen** Wenn Ihr aktuelles Netzwerk nicht über die erforderliche Bandbreite und Geschwindigkeit für die Zentralisierung von Servern verfügt, müssen Sie in Ihrem Projektplan eine Netzwerkaufrüstung vorsehen.
- **Sicherheit** Ein zentralisiertes Modell bietet eine einfachere Verwaltung der Sicherheit, und daher ein größeres Maß an Kontrolle. Aufgrund dieser effektiveren Kontrolle können für die Sicherheit zuständige Mitarbeiter leichter die neuesten Viruserkennungsdateien verwalten und rechtzeitig entsprechende Maßnahmen bei Sicherheitsproblemen einleiten. Ein weiterer Vorteil einer zentralisierten Struktur besteht darin, dass sich Ihr Server in einem Datenzentrum befindet, das Sie physisch sichern können.

Eigenschaften eines verteilten Messagingsystems

Eine Zweigstelle oder eine verteilte Messagingbereitstellung bedeutet, dass zahlreiche Zweigstellen oder kleinere verteilte Standorte über langsame Verbindungen zum Hub eines Unternehmens oder eines Datenzentrums verfügen. Die Zweigstellen haben ihre eigenen Exchange-Server, Domänencontroller und globalen Katalogserver. Ein verteiltes Messagingsystem wird in der Regel verwendet, wenn das Netzwerk den Datenverkehr zu einem zentralen Hub für Dienste nicht verarbeiten kann. Daher werden das Betriebssystem und die Messagingserver lokal platziert. Ein weiterer Grund können Benutzeranforderungen sein. Wenn die Anforderungen an die Benutzerleistung und -verfügbarkeit nicht durch die Verbindung zu einem Datenzentrum erfüllt werden können, müssen Sie möglicherweise Server an den Remotestandorten einrichten.

Eine Exchange-Bereitstellung in einer Zweigstelle verfügt über folgende Eigenschaften:

- Das Messagingsystem besteht aus einer großen Anzahl von Standorten (Zweigstellen), von denen jede über einen Exchange-Server, über Domänencontroller und mindestens einen globalen Katalogserver verfügt.
- Die Zweigstellenstandorte enthalten in der Regel eine kleine oder wechselnde Anzahl von Benutzern.
- Das Netzwerk ist meistens in einer Hub-and-Spoke-Topologie strukturiert.
- Die Netzwerkverbindungen zwischen den Zweigstellenstandorten und dem zentralen Hub oder Datenzentrum weisen in der Regel eine geringe Bandbreite und hohe Latenzzeiten auf oder sind unzuverlässig.

Die Bereitstellung eines verteilten Messagingsystems geschieht unter anderem aus den folgenden Gründen:

- Die Benutzer des Unternehmens sind über zahlreiche Standorte verteilt.
- Die Netzwerkinfrastruktur des Unternehmens kann den Datenverkehr zu einem zentralen Hub für Dienste nicht verarbeiten.
- Die Benutzeranforderungen geben vor, dass ein Server lokal eingerichtet werden muss, um eine optimale Benutzerleistung und -verfügbarkeit zu gewährleisten.

Wichtige Überlegungen

Berücksichtigen Sie die folgenden Punkte bei der Entscheidung über eine verteilte Struktur:

- **Software-Aktualisierungen** Die Bereitstellung von wichtigen Updates und Patches ist in einem verteilten Messagingsystem wesentlich anspruchsvoller.
- Wenn Sie RPC über HTTP einsetzen möchten, muss auf allen Computern in Ihrer Messagingumgebung, die im Zusammenhang mit RPC über HTTP verwendet werden, Windows Server 2003 ausgeführt werden. Dies betrifft auch alle globalen Katalogserver und alle Exchange Server, auf die Outlook 2003-Benutzer zugreifen.
- **Betriebs- und Verwaltungskosten** Verteilte Messagingsysteme erfordern viele Server und führen zu höheren Betriebs- und Verwaltungskosten.
- **Datenspeicher** Bei verteilten Servern ist die Dienstinfrastruktur komplexer. Dadurch ist das Wiederherstellen von Diensten und Daten schwieriger, wenn ein Fehler auftritt.
- **Netzwerkverbindungen** Wenn Sie Remote-Büros betreiben, wird empfohlen, eine Netzwerkgeschwindigkeit von mindestens 56 Kbps zwischen den Servern zum Hub-Standort oder zum Datenzentrum bereitzustellen. Zwischen einem Hub und einem Büro wird jedoch eine höhere Verbindungsgeschwindigkeit empfohlen.
- **Sicherheit** Die physische Sicherheit von Servern in Zweigstellen ist ein wichtiger Aspekt. In einer Zweigstellenstruktur müssen Sie entsprechende Vorkehrungen treffen, damit die Server physisch gesichert und nicht an öffentlich zugänglichen Orten aufgestellt sind.

Routing-Entwurf

Die Routingtopologie ist die Basis des Messagingsystems. Bei der Planung Ihrer Routingtopologie sollten Sie Überlegungen zum Netzwerk, zur Bandbreite und zu geografischen Standorten berücksichtigen. In diesem Abschnitt wird erläutert, wie mit Routing in Exchange Server 2003 eine Routingtopologie erstellt wird, die mit

Ihrem vorhandenen System und Netzwerk funktioniert. Außerdem wird gezeigt,
wie Connectors für die Kommunikation mit Empfängern außerhalb der Organisation entwickelt werden.

Mit dem Begriff Routing wird bezeichnet, wie mit Exchange Nachrichten zwischen den Servern ausgetauscht werden. Bei der Planung Ihrer Routingtopologie sollten Sie die Funktionsweise der Nachrichtenübertragung in Exchange verstehen, um eine optimale Nachrichtenübertragung zu gewährleisten. Sie sollten außerdem die Standorte der Connectors für Messagingsysteme außerhalb Ihrer Exchange-Organisation vorausplanen. Durch eine sorgfältige Planung kann die Menge des Netzwerkverkehrs reduziert und die Ausführung der Exchange- und Windows-Dienste optimiert werden.

Einsatzgebiete für Routinggruppen

Wenn einer der folgenden Faktoren zutrifft, sind möglicherweise mehrere Routinggruppen erforderlich:

- Die Netzverbindungen bieten nicht die erforderliche Konnektivität.
- Das zu Grunde liegende Netzwerk ist fehleranfällig.
- Es gibt mehrere Exchange 5.5-Standorte.
- Die Nachrichtenübertragung zwischen verschiedenen Standorten muss geplant oder gesteuert werden.
- Sie müssen administrative Beschränkungen in Bezug auf den Nachrichtenverkehr festlegen.

In Kapitel 1 haben Sie eine gründliche Beurteilung Ihrer vorhandenen Netzwerkinfrastruktur vorgenommen.
Vor Planung Ihrer Routingarchitektur sollten
Sie die folgenden Fragen auf Grundlage dieser Informationen beantworten:

- Wie sieht die aktuelle Netztopologie aus?
- Welcher Art sind die Verbindungen zwischen den Standorten, einschließlich verfügbarer Bandbreite und Wartezeiten?
- Welche anderen Anwendungen verwenden die Bandbreite, und welche Anwendungen sind für die Zukunft geplant?
- Wie viele Benutzer befinden sich an jedem Standort?
- Wo befinden sich die Benutzer, und welche Verwendungsmuster liegen vor?
  Mit welchen Gruppen kommunizieren die Benutzer?
- Welche Art von Geschäft betreibt Ihr Unternehmen? Ziehen Sie Tools in Betracht, die bereits Bandbreite beanspruchen (z. B. Verkaufssysteme).
- Wo befinden sich die Datenzentren?
- Wo sind Ihre Internetzugriffspunkte?
- Benötigen Sie standortübergreifenden Zugriff auf Öffentliche Ordner? Haben Sie Anwendungen oder Öffentliche Ordner, die zwischen verschiedenen Standorten eingesetzt werden?
- Müssen Sie Frei/Gebucht-Informationen standortübergreifend freigeben? (Frei/Gebucht-Informationen werden wie Verweise auf Öffentliche Ordner verwaltet.)
- Wie ist die aktuelle Active Directory-Struktur gestaltet, und wo befinden sich die globalen Katalogserver und die Domänencontroller? Wie sind die Windows-Standorte aufgebaut (d. h., sind sie auf Routinggruppen abgestimmt?)?

Wichtige Überlegungen

Mithilfe von Connectors zwischen den Routinggruppen kann der Nachrichtenfluss gesteuert werden. Zu viele Connectors können sich dabei jedoch negativ auswirken. Das Erstellen zu vieler Routinggruppen sollte daher vermieden werden. Es wird empfohlen, maximal 150 Routinggruppen zu verwenden. Wenn jedoch mehrere Verbindungen zu einem Ziel bestehen, können Sie Connectors festlegen, die den Nachrichtenfluss zwischen Routinggruppen steuern. Innerhalb einer Routinggruppe besteht eine Punkt-zu-Punkt-Kommunikation. Sie haben daher keine Möglichkeit, Pfade Pfade und Kosten festzulegen, um die kostengünstigste Strecke zwischen zwei Servern zu wählen. Beim Erstellen von Routinggruppen können Sie jedoch verschiedenen Pfaden Kosten zuweisen, um die Verwendung der effizientesten Route zu gewährleisten.

Zusätzlich zur Planung von Routinggruppen innerhalb Ihrer Organisation sollten Sie auch die Standorte der Connectors für Messagingsysteme außerhalb Ihrer Exchange-Organisation vorausplanen.

Serverplatzierung

Da Exchange Active Directory verwendet, müssen Sie bei der Planung der Bereitstellung von Exchange unbedingt Ihre Windows Server-Netzwerktopologie berücksichtigen. Um
eine optimale Leistung zu erhalten, sollten Sie grundsätzlich sicherstellen, dass Sie an jedem Windows-Standort, an dem Exchange installiert ist, über mindestens einen globalen Katalogserver verfügen. Benutzer können sich bei Windows Server 2003 zwar auch ohne globalen Katalogserver anmelden, bei Exchange ist dies jedoch nicht möglich. Bei Verwendung mehrerer Domänencontroller werden außerdem die Suchvorgänge im Netzwerk innerhalb von Domänen verteilt, und es besteht Ausfallsicherheit, wenn ein Domänencontroller nicht funktioniert. Weitere Informationen zur Planung von Windows-Standorten, Domänen und Domänencontroller finden Sie in der Dokumentation zu Windows Server.

Active Directory-Serverplatzierung

In Kapitel 1 haben Sie die aktuelle Struktur von Active Directory überprüft. In der folgenden Auflistung werden die Empfehlungen für die Platzierung von Active Directory-Domänencontrollern und globalen Katalogservern zur Unterstützung Ihrer Exchange-Organisation zusammengefasst:

- Stellen Sie sicher, dass das DNS am Hub-Standort und an allen Zweigstellen ordnungsgemäß konfiguriert ist. Stellen Sie sicher, dass sowohl die Namensauflösung als auch das DNS korrekt funktionieren.
- Stellen Sie sicher, dass es sich bei dem Server, der in der Infrastruktur als Masterserver dient, nicht um einen globalen Katalogserver handelt.
- An Zweigstellen mit mehr als 10 Benutzern muss an jedem Standort mit Exchange-Servern ein globaler Katalogserver installiert sein. Um Ausfallsicherheit zu gewährleisten, sollten idealerweise zwei globale Katalogserver bereitgestellt werden. Wenn ein physischer Standort nicht zwei globale Katalogserver aufweist, können Sie bestehende Domänencontroller als globale Katalogserver konfigurieren.
- Für Exchange ist WINS erforderlich.

In den folgenden Abschnitten finden Sie weitere Informationen zur Platzierung von globalen Katalogservern und Domänencontrollern.

Domänencontroller

In den meisten Bereitstellungsszenarien empfiehlt es sich nicht, Exchange 2003
auf Computern auszuführen, die auch als Windows-Domänencontroller fungieren.
Wird Exchange auf einem Domänencontroller ausgeführt, wird ausschließlich dieser
von Exchange verwendet. Daher sollten Sie Exchange-Server und Windows-Domänencontroller als separate

Computer konfigurieren. Fällt der Domänencontroller aus, kann Exchange keinen Failover auf einen weiteren Domänencontroller ausführen. Wenn die Server, auf denen Exchange ausgeführt wird, neben dem Antworten auf Anforderungen von Exchange-Clients keine weiteren Aufgaben als Domänencontroller ausführen müssen, erhöht sich außerdem die Leistung dieser Server unter hoher Belastung durch viele Benutzer.

Speichern Sie die Active Directory-Informationen auf mehr als nur einem Domänencontroller, um die Sicherheit dieser Informationen zu gewährleisten. Für den Fall, dass auf einem der Server ein Problem auftritt, sollten Sie zumindest über zwei Domänencontroller verfügen,
um sicherzustellen, dass Ihre Active Directory-Informationen nicht verloren gehen.

Stellen Sie außerdem sicher, dass für Ihre Domänencontroller ein zuverlässiger Sicherungsplan besteht. Unter Exchange 5.5 wurden durch das Sichern der Datei **Dir.edb** die Verzeichnisdaten des Servers gesichert. Bei Verwendung von Exchange 2000 und Exchange 2003 befinden sich die Exchange-Informationen jedoch in Active Directory, und Sicherungen der Domänencontroller sind unbedingt erforderlich. Stellen Sie sicher, dass in Ihrer Windows-Infrastruktur diese Informationen gesichert werden und die Zuverlässigkeit der Informationen gewährleistet ist.

Globale Katalogserver

Globale Katalogserver werden für die Anmeldung benötigt, da sie Informationen
über die globale Gruppenmitgliedschaft enthalten. Durch diese Mitgliedschaft wird
der Benutzerzugriff auf Ressourcen gewährt oder verweigert. Wenn die Verbindung mit einem globalen Katalogserver nicht möglich ist, kann die globale Gruppenmitgliedschaft eines Benutzers nicht ermittelt werden, und der Anmeldezugriff wird abgelehnt.

> **Hinweis** Obwohl für manche Features von Windows Server 2003 kein lokaler globaler Katalogserver benötigt wird, ist für die Verwendung von Exchange und Outlook ein solcher erforderlich. Sie benötigen einen globalen Katalogserver, um Exchange-Dienste (einschließlich Anmeldung, Gruppenmitgliedschaft und Speicherdienste) verwenden
> zu können und Zugriff auf die globale Adressliste (GAL) zu erhalten. Durch die lokale Bereitstellung von globalen Katalogservern für Server und Benutzer können Adressen-Lookups effizienter ausgeführt werden. Wenn das Abrufen eines globalen Katalogservers über eine langsame Verbindung durchgeführt wird, erhöht sich der Netzwerkverkehr und die Gesamtleistung wird beeinträchtigt.

Berücksichtigen Sie folgende Punkte, wenn Sie globale Katalogserver installieren:

- Alle Exchange Server und Benutzer sollten einen schnellen Zugriff auf einen globalen Katalogserver haben.
- Mindestens ein globaler Katalogserver muss in jeder Exchange Server-Domäne installiert werden.
- Es sollte im Allgemeinen ein Verhältnis von 4:1 zwischen den Prozessoren für Exchange und den Prozessoren für globale Katalogserver bestehen, vorausgesetzt, die Prozessoren haben ähnliche Geschwindigkeiten. Abhängig von Ihren Anforderungen können jedoch weitere globale Katalogserver erforderlich werden, wenn diese stärker beansprucht werden, ein großes Active Directory besteht oder umfangreiche Verteilerlisten zu verwalten sind.

Exchange-Server

Der Installationsort der Exchange-Server ist maßgeblich davon abhängig, ob Ihr Messagingsystem zentral oder verteilt eingerichtet werden soll. Nutzen Sie für Ihre Entscheidung, ob Benutzer Zugriff auf einen lokalen Exchange-Server benötigen,
die Ihnen vorliegenden Informationen zu Wartungsverträgen, Benutzeranforderungen und den Softwareversionen, die Sie in der Organisation bereitstellen.

Postfachserver

Bei Remotestandorten mit langsamen oder unzuverlässigen Netzwerkverbindungen müssen Sie feststellen, auf welche Weise sich Serviceunterbrechungen auf das Geschäft auswirken und in welchem Umfang Unterbrechungen akzeptabel sind. Wenn der Zugriff auf aktualisierte Exchange-Daten jederzeit gewährleistet sein muss, ist es erforderlich,
an den Remotestandorten Exchange-Server einzurichten. Wenn Sie sich nach Abwägen der Bereitstellungskosten für zusätzliche Server gegen die Kostenersparnisse eines zentralisierteren Modells dafür entscheiden, dass Diensteunterbrechungen bis zu einem gewissen Grad akzeptabel sind, können Sie möglicherweise alle Exchange-Server
in einem Datenzentrum bereitstellen. Beachten Sie, dass es in diesem Fall jedoch erforderlich werden könnte, auf Windows Server 2003 und Outlook 2003 zu aktualisieren, wenn Sie Features wie den Exchange-Cachemodus und RPC über HTTP nutzen und Remotebenutzern diese verbesserten Leistungen zur Verfügung stellen möchten.

Server für Öffentliche Ordner

Wenn Ihre Organisation, wie zuvor erörtert, aus mehreren Remotestandorten besteht, können Sie auf den lokalen Exchange-Servern Replikate von Öffentlichen Ordnern bereitstellen, so dass jeder Standort über ein Replikat der Öffentlichen Ordner
der anderen Standorte verfügt. Es besteht jedoch auch die Möglichkeit, die in den Öffentlichen Ordnern enthaltenen Informationen auf einem zentralen Server im Datenzentrum oder Hub zu speichern, so dass nur eine einzelne, korrekte Datenquelle vorhanden ist. Für Ihre Entscheidung müssen Sie Datenzuverlässigkeit und Komfort gegeneinander abwägen und außerdem die Benutzeranforderungen und das Nutzungsverhalten in Betracht ziehen.

Frei/Gebucht-Server

Der Zugriff auf die Frei/Gebucht-Informationen gehört zu den wichtigsten Überlegungen. Wenn keine lokale Kopie der Daten des Frei/Gebucht-Ordners vorhanden ist, müssen Benutzer beim Abrufen der Frei/Gebucht-Informationen anderer Benutzer zum Planen
von Besprechungen mit Zeitverzögerungen rechnen. Beachten Sie, wie Besprechungen
von Benutzern in Ihrer Organisation geplant werden. Die Voraussetzungen für den Zugriff auf aktualisierte Planungsinformationen können in den verschiedenen Unternehmen variieren. Wenn der Benutzerzugriff auf aktuelle Planungsinformationen zu jeder Zeit erforderlich ist, müssen die Frei/Gebucht-Ordner zentral abgelegt werden. Wenn ein schneller Zugriff wichtiger ist, als über aktuelle Informationen zu verfügen, können Sie
die Frei/Gebucht-Ordner auf lokal bereitgestellten Exchange-Servern ablegen. In diesem Fall kann es beim Empfangen von aktualisierten Frei/Gebucht-Informationen über das Netzwerk zu Verzögerungen kommen. Sie sollten den für Ihr Unternehmen vertretbaren Grad der Verzögerung festlegen.

Wenn Sie sich dafür entscheiden, dass Frei/Gebucht-Informationen auf lokalen Exchange-Servern abgelegt werden, wäre die nächste Überlegung, Kopien der Frei/Gebucht-Informationen anderer Standorte auf dem lokalen Server einzurichten. Wenn unter den Benutzern verschiedener Standorte nur selten Besprechungen geplant werden, ist es nicht unbedingt erforderlich, Replikate der Frei/Gebucht-Informationen der anderen Standorte lokal verfügbar zu machen. Wenn Sie jedoch entscheiden, lokale Kopien der Öffentlichen Ordner anderer Standorte zu führen, sollten Sie beachten,
dass in dem für einen Öffentlichen Ordner festgelegten Replikationszeitplan der Zeitpunkt bestimmt wird, an dem vorgenommene Änderungen übermittelt werden. Wenn Replikate von Frei/Gebucht-Informationen an mehreren Standorten verwaltet werden, kann es eine gewisse Zeit dauern, bis die an einem Standort vorgenommenen Änderungen an die anderen Standorte übermittelt werden. Daher ist es möglich, dass ein Benutzer für die Planung einer Besprechung auf die lokalen Frei/Gebucht-Daten zugreifen möchte, diese jedoch veraltet sind, da die an einem anderen Standort vorgenommenen Änderungen am Zeitplan noch nicht repliziert wurden.

Server für Offlineadresslisten

Exchange 2003 stellt mithilfe von Active Directory Dienste für Offlineadresslisten bereit. Die von Exchange erstellten Adresslistendateien werden in einem Öffentlichen Ordner gespeichert. Außerhalb arbeitende Benutzer können, um Informationen über andere Benutzer in der Organisation abzurufen, eine Verbindung zu Exchange herstellen und die Offlineadresslisten remote downloaden.

Beim Erstellen einer Offlineadressliste werden die der Offlineadressliste zugeordneten Adresslisten in eine einzelne Datendatei konvertiert und in einem Öffentlichen Systemordner gespeichert. Wenn Benutzer die Offlineadressliste downloaden, wird diese Datendatei als Informationsquelle verwendet.

Sie müssen einen geeigneten Server zum Erstellen und Aktualisieren der Offlineadresslisten auswählen. Je mehr Adresslisten eine Offlineadressliste enthält, desto mehr wird der für die Offlineadressliste ausgewählte Server beansprucht.

Bei Verwendung des Exchange-Cachemodus müssen Sie die Auswirkungen auf den Server berücksichtigen, die beim Download von Offlineadresslisten durch die Benutzer entstehen. Diese können erheblich sein, und zwar nicht nur beim jeweils ersten Download von Offlineadresslisten, sondern auch im täglichen Betrieb. Unter Umständen empfiehlt sich
das Einrichten von ein bis zwei Servern für die Verwaltung von Offlineadressbüchern.

Serverdimensionierung und -abstimmung

Verwenden Sie folgende Kapazitätsplanungstools, um die Anzahl der für die Bewältigung der Benutzerbelastung erforderlichen Exchange-Server zu ermitteln:

- Kapazitätsplanung und Topologierechner
- Microsoft Exchange Server Load Simulation-Tool (LoadSim.exe)
- Exchange Stress and Performance (ESP)-Tool
- Jetstress

  Wichtig Da einige dieser Tools Konten mit unsicheren Kennwörtern erstellen, sollten die Tools nur in Testumgebungen, jedoch nicht in Produktionsumgebungen verwendet werden.

Kapazitätsplanung und Topologierechner

Mit der Kapazitätsplanung und dem Topologierechner können Sie die erforderlichen Servergrößen für Ihre Exchange 2000- oder Exchange 2003-Topologie bestimmen.
Die Kapazitätsplanung und den Topologierechner finden Sie unter
http://go.microsoft.com/fwlink/?LinkId=1716.

Microsoft Exchange Server Load Simulation-Tool

Mit Microsoft Exchange LoadSim kann die Belastung für Exchange durch MAPI-Clients simuliert werden. Sie simulieren die Auslastung, indem Sie LoadSim-Tests auf Clientcomputern ausführen. Mithilfe dieser Tests werden Messaginganforderungen
an den Exchange-Server gesendet, die eine Belastung auf dem Server verursachen.

Mit den Ergebnissen dieser Tests können Sie folgende Aktionen durchführen:

- Berechnen der Clientantwortzeit für die Serverkonfiguration unter Clientlast

- Abschätzen der Anzahl von Benutzern pro Server
- Erkennen von Engpässen auf dem Server

Weitere Informationen zu LoadSim sowie Downloadmöglichkeiten für LoadSim finden Sie im *Microsoft Exchange 2000 Server Resource Kit* (http://go.microsoft.com/fwlink/?LinkId=1710) unter „Load Simulator“.

Exchange Stress and Performance-Tool

Das Exchange Stress and Performance (ESP)-Tool ist ein hoch skalierbares Belastungs- und Leistungstool für Exchange. Es simuliert eine große Anzahl von Clientsitzungen durch gleichzeitiges Zugreifen auf einen oder mehrere Protokolldienste. Die Aktionen jedes simulierten Benutzers werden durch Skripts gesteuert. Die Skripts enthalten
die Algorithmen für die Kommunikation mit dem Server. Die Skripts werden von Testmodulen (DLLs) ausgeführt. Die Testmodule stellen Serververbindungen über Internetprotokolle, Aufrufe der API-Funktionen (Application Programming Interfaces) oder über Schnittstellen wie OLE DB her.

ESP ist modular und erweiterbar und bietet zurzeit Module für die meisten Internetprotokolle, einschließlich der folgenden:

- WebDAV (Web Distributed Authoring and Versioning)
- Internet Message Access Protocol Version 4rev1 (IMAP4)
- Lightweight Directory Access Protocol (LDAP)
- OLE DB
- Post Office Protocol Version 3 (POP3)
- Simple Mail Transport Protocol (SMTP)

Weitere Informationen zum ESP-Tool und dem Download von ESP finden
Sie auf der Microsoft Exchange 2003-Website für Tools und Aktualisierungen
(http://go.microsoft.com/fwlink/?LinkId=21316).

Jetstress

Exchange 2003 beansprucht viel Festplattenspeicher und erfordert für den ordnungsgemäßen Betrieb ein schnelles und zuverlässiges Datenträgersubsystem. Mithilfe des Jetstress-Tools (Jetstress.exe) können Administratoren vor dem Einsatz des Exchange-Servers in der Produktionsumgebung die Leistung und Stabilität des Datenträgersubsystems in Exchange überprüfen. Weitere Informationen zu Jetstress finden Sie in Kapitel 6 unter „Testen der Festplattenleistung mit Jetstress“.

Optimieren der Speicherauslastung

Durch die Auslastung des virtuellen Adressraums eines Servers wird die Leistung und Skalierbarkeit des Postfachservers festgelegt. Bei Abnahme des verfügbaren virtuellen Speichers verringert sich auch die Leistung erheblich. Obwohl Exchange 2003 die Auslastung kleinerer und mittlerer Server automatisch optimiert, ist eine zusätzliche Abstimmung für Server mit mehr als 1 GB physischem Speicher erforderlich.

Weitere Informationen zum Überwachen und Optimieren der Speicherauslastung
auf den Servern finden Sie in Anhang B.

Protokollunterstützung in Exchange 2003

Wenn MAPI-, HTTP-, POP- oder IMAP-Benutzer unterstützt werden sollen, benötigen Sie bestimmte Empfehlungen für das Entwerfen der Topologie und das Konfigurieren des Netzwerks. In diesem Abschnitt finden Sie Empfehlungen für die Verwendung von Front-End-Servern und das Konfigurieren von RPC über HTTP.

Verwendung von Front-End-Servern

Soweit einzelne Protokolle in Ihrer Messagingumgebung unterstützt werden sollen, beginnt die Bereitstellung von Exchange mit der Definition Ihrer Serverarchitektur. Wenn Ihre Organisation über mehr als einen Exchange-Server verfügt, wird für den Clientzugriff die Front-End- und Back-End-Serverarchitektur für Exchange empfohlen. In diesem Entwurf werden verschiedene Überlegungen zum Clientzugriff für die Bereitstellung von Exchange berücksichtigt. Wenn MAPI, HTTP, POP3 oder IMAP4 unterstützt werden sollen, können Sie die Front-End- und Back-End-Serverarchitektur für Exchange verwenden, um folgende Vorteile zu nutzen:

- **Einzelner Namespace** Als wichtigsten Vorteil bietet die Front-End- und Back-End-Serverarchitektur die Möglichkeit, einen einzelnen, konsistenten Namespace einzusetzen, mit dem die Benutzer auf ihre Postfächer zugreifen können. Ohne einen Front-End-Server muss jeder Benutzer den Namen des Servers kennen, auf dem sein Postfach gespeichert ist. Dadurch wird die Verwaltung erschwert und die Flexibilität beeinträchtigt, da bei jeder Änderung oder Vergrößerung Ihrer Organisation Postfächer auf einen anderen Server verschoben und Benutzer entsprechend informiert werden müssen. Bei einem einzelnen Namespace können Benutzer denselben URL oder dieselbe POP- und IMAP-Clientkonfiguration verwenden, selbst wenn Server hinzugefügt oder entfernt und Postfächer verschoben werden. Außerdem wird durch das Erstellen eines einzelnen Namespace sichergestellt, dass der Outlook Web Access-, POP- oder IMAP-Zugriff auch dann skalierbar bleibt, wenn Ihre Organisation wächst.
- **Front-End-Server verteilen die Aufgabenverarbeitung auf verschiedene Server** Sie können Exchange 2003-Server so konfigurieren, dass diese die SSL (Secure Sockets Layer)-Datenübertragung zwischen dem Clientcomputer und dem Server unterstützen und so die Datenübertragung vor einem unbefugten Abfangen von Daten schützen. Das Ver- und Entschlüsseln des Nachrichtenverkehrs erfordert jedoch Prozessorzeit. Wenn eine SSL-Verschlüsselung verwendet wird, bietet die Front-End- und Back-End-Serverarchitektur einen Vorteil, da die Front-End-Server die gesamte Ver- und Entschlüsselung abwickeln können. Zusätzlich kann ein SSL-Beschleuniger verwendet werden, um die Auswirkung der Ver- und Entschlüsselung auf den Server weiter zu verringern. Ein SSL-Beschleuniger verbessert die Leistung, indem Verarbeitungsaufgaben von den Back-End-Servern entfernt werden. Dabei ist die Verschlüsselung von Daten zwischen dem Clientcomputer und dem Exchange-Server weiter möglich.
- **Sicherheit** Der Front-End-Server kann als einziger Zugriffspunkt an oder hinter einem Firewall positioniert werden, der so konfiguriert ist, dass eine Datenübertragung aus dem Internet nur am Front-End möglich ist. Da auf dem Front-End-Server keine Benutzerinformationen gespeichert werden, bietet dieser Server der Organisation eine zusätzliche Sicherheitsstufe. Außerdem kann der Front-End-Server so konfiguriert werden, dass Anforderungen vor der Weiterleitung authentifiziert werden. Dadurch werden die Back-End-Server vor DOS-Angriffen (Denial Of Service) geschützt.
- **Verbesserter IMAP-Zugriff auf Öffentliche Ordner** Mithilfe des IMAP-Protokolls kann ein Server einen Client an einen anderen Server verweisen. Exchange 2000 unterstützt diese Verweisfunktion, wenn ein Informationsspeicher für Öffentliche Ordner auf einem bestimmten Server den angeforderten Inhalt nicht enthält und der Client an einen anderen Server verwiesen werden muss. Für diese Funktion müssen die Clients jedoch IMAP-Verweise unterstützen, was bei den meisten Clients nicht der Fall ist. (Der Pine-Client und das Pine-Toolkit der University of Washington unterstützen beispielsweise Verweise.)

Wenn ein IMAP-Client, bei dem die Verweise nicht aktiviert sind, eine Verbindung über einen Front-End-Server herstellt, hat der Client Zugriff auf die gesamte Öffentliche Ordner-Hierarchie. Wenn ein Front-End-Server einen Befehl
an einen Back-End-Server weiterleitet, werden sämtliche Verweisantworten, die beim Versuch, auf einen auf dem Back-End-Server nicht verfügbaren Ordner zuzugreifen, zurückgegeben wurden, vom Front-End-Server automatisch abgewickelt. Dadurch
wird der Verweis für den Client transparent. Weitere Informationen zu IMAP-Clients
mit deaktivierter Verweisfunktion finden Sie in den Request for Comments (RFC)
2221 und RFC 2193.

Weitere Informationen zur Verwendung von Front-End-Servern finden Sie
m technischen Artikel *Using Microsoft Exchange 2000 Front-End Servers*
(http://go.microsoft.com/fwlink/?LinkId=14575). Obwohl sich das Whitepaper
auf Exchange 2000 bezieht, gelten die Beschreibungen auch für Exchange 2003.

Front-End- und Back-End-Exchange-Server-Szenarien

Obwohl die Exchange Front-End- und Back-End-Serverarchitektur auf unterschiedliche
Weise bereitgestellt werden kann, wird für diese Serverarchitektur in der Regel stets
dasselbe Bereitstellungsverfahren verwendet. Zuerst wird einem der Exchange-Server
bei der Bereitstellung die Rolle als Front-End-Server zugewiesen. Dieser Server ist danach
für das Routing aller Clientanforderungen an den geeigneten Back-End-Exchange-Server verantwortlich. Anschließend müssen Sie den Standort des Exchange-Servers festlegen. In Abhängigkeit vom Standort des Exchange-Servers konfigurieren Sie das interne Netzwerk
so, dass die Datenübertragung zwischen dem Front-End-Exchange-Server und den anderen Computern abgewickelt werden kann, mit denen ein Datenaustausch erforderlich ist. Schließlich erhalten Sie durch das Kombinieren der Exchange Front-End- und Back-End-Serverarchitektur mit Microsoft ISA Server (Internet Security and Acceleration) ein Clientzugriffsmodell mit erhöhter Sicherheit und Zuverlässigkeit.

Front-End- und Back-End-Funktionalität

Ein Front-End-Servers leitet wie ein Proxyserver Clientanforderungen an den geeigneten Back-End-Server oder die entsprechende Ressource weiter. Je nach verwendetem Client und Protokoll erfüllt der Front-End-Exchange-Server jedoch auch zusätzliche Aufgaben. Im nachstehenden Abschnitt wird die Zusammenarbeit des Front-End-Servers mit den jeweiligen Clients und Protokollen beschrieben.

Outlook

In Microsoft Office Outlook® 2003 sowie in älteren Versionen von Outlook wird für den Datenaustausch mit Exchange MAPI (Messaging Application Programming Interface) verwendet. Da MAPI-Clients für den Datenaustausch mit Exchange RPC-Aufrufe (Remote Procedure Call) verwenden, ist es schwierig, Remotezugriff auf Exchange bereitzustellen. In Exchange Server 2003 und Outlook 2003 kommt jedoch für den Remotezugriff auf Exchange die RPC über HTTP-Netzwerkkomponente von Windows für IIS (Internet Information Services) zum Einsatz. Wenn Sie RPC über HTTP verwenden, senden Outlook 2003-Clients alle Datenübertragungen an den Exchange-Server über Anschluss 80 (HTTP) oder Anschluss 443 (HTTPS).

RPC über HTTP

Für den Remotezugriff auf Exchange konfigurieren Sie die Exchange-Bereitstellung so, dass RPC über HTTP aktiviert ist. Wenn Sie Exchange für die Verwendung von RPC über HTTP konfigurieren, wird der Exchange-Front-

End-Server als RPC-Proxyserver verwendet. Der RPC-Proxyserver bearbeitet dann für den Client alle RPC über HTTP-Anforderungen und leitet diese an die geeignete Back-End-Ressource weiter. Zusätzlich werden die Back-End-Ressourcen einschließlich des globalen Katalogservers und der Back-End-Exchange-Server speziell für den Datenaustausch mit dem Front-End-Exchange-Server konfiguriert. Wenn Sie ISA Server als erweiterten Firewall verwenden, wird ISA Server so konfiguriert, dass das virtuelle RPC-Verzeichnis auf dem RPC-Proxyserver veröffentlicht wird und Clients Verbindungen zu den jeweiligen Exchange-Servern herstellen können. ISA Server kann
so konfiguriert werden, dass der Datenverkehr über Anschluss 80 oder 443 überwacht
und geprüft wird. Auf diese Weise können Sie den Netzwerkverkehr zu Ihrem Exchange Front-End-Server besser kontrollieren.

Sichern von Exchange mit ISA Server 2000

Als empfohlene Alternative zum Platzieren des Exchange 2003-Front-End-Servers
im Perimeternetzwerk können Sie ISA Server bereitstellen. ISA Server wird dabei
als erweiterter Firewall eingesetzt, mit dem die Kontrolle des Datenverkehrs aus dem Internet in das Netzwerk erleichtert wird. Bei dieser Konfiguration platzieren Sie alle Exchange 2003-Server innerhalb des Unternehmensnetzwerks und verwenden ISA
Server als erweiterten Firewallserver, der im Perimeternetzwerk dem Datenverkehr
aus dem Internet ausgesetzt ist.

Der gesamte ankommende und an die Exchange-Server gerichtete Internet-Datenverkehr (z. B. Anforderungen aus Outlook Web Access, Outlook Mobile Access, mittels POP3, IMAP4 sowie Datenübertragungen von Outlook 2003-Clients mit RPC über HTTP usw.) werden von ISA Server verarbeitet. Wenn eine Anforderung an einen Exchange-Server bei ISA Server eingeht, wird diese an die geeigneten Exchange-Server im internen Netzwerk weitergeleitet. Die internen Exchange-Server geben die angeforderten Daten
an ISA Server zurück, und ISA Server sendet dann die Daten über das Internet an den Client. Abbildung 5.1 zeigt ein Beispiel für eine empfohlene ISA-Bereitstellung.

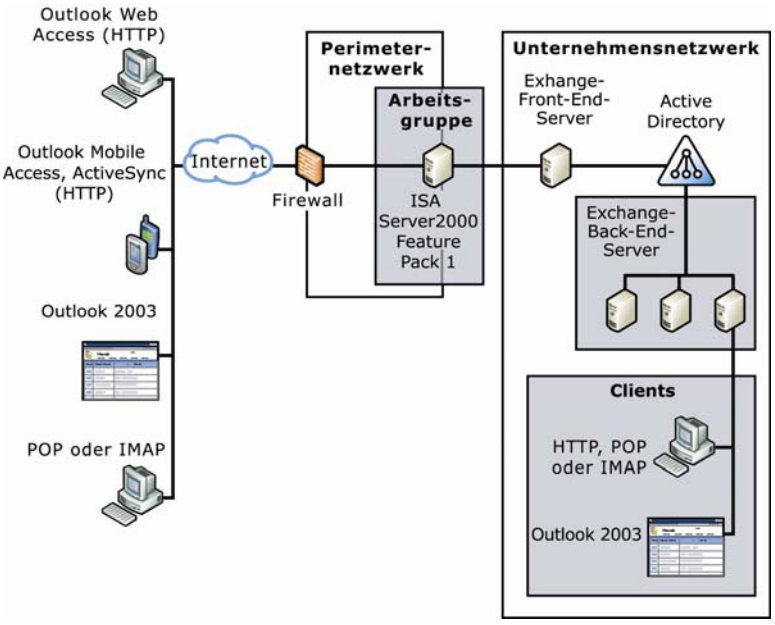


Abbildung 5.1 Durch ISA Server geschütztes Bereitstellen von Exchange 2003

Das Verwenden von ISA Server als erweiterten Firewallserver im Perimeternetzwerk zum Schutz des Messagingnetzwerks bietet folgende Vorteile:

- ISA Server ist kein Mitglied der Domäne. Eine Beschädigung von ISA Server bedeutet keine Verletzung der Sicherheit Ihrer Domäne.
- Da ISA Server kein Mitglied der Domäne darstellt, ist auch kein Datenverkehr mit einem Domänencontroller oder globalen Katalogserver erforderlich. Auf diese Weise wird die Anzahl der zwischen dem Perimeternetzwerk und dem internen Unternehmensnetzwerk geöffneten Anschlüsse verringert.
- ISA Server kann aus dem Internet stammenden und an die Exchange-Server gerichteten Datenverkehr vorauthentifizieren und so dazu beitragen, dass nur authentifizierter Datenverkehr in das Unternehmensnetzwerk weitergeleitet wird.
- ISA Server kann bestimmte Arten von unbefugtem Netzwerkverkehr wie beispielsweise DOS-Angriffe (Denial Of Service) und Anschlussscans erkennen und unterbinden.

Verwenden von RPC über HTTP

Mithilfe des Features RPC über HTTP in Windows Server 2003 können Benutzer von Outlook auch beim Einsatz von Firewalls Verbindungen über das Internet zu ihrem Exchange-Server herstellen. Als Bereitstellungsstrategie wird empfohlen, ISA Server 2000 mit Feature Pack 1 als Sicherheitsinfrastruktur zu verwenden, oder ISA Server innerhalb des Perimeternetzwerks und den Exchange Front-End-Server (als RPC-Proxyserver) innerhalb des Unternehmensnetzwerks zu platzieren. Sie können auch den als RPC-Proxyserver verwendeten Exchange 2003-Front-End-Server innerhalb des Perimeternetzwerks platzieren.

Wenn Sie ISA Server als Reverse-Proxyserver verwenden, stehen Ihnen mehrere Bereitstellungsoptionen zur Verfügung. Weitere Informationen zum Installieren von ISA Server als Reverse-Proxyserver für Exchange finden Sie im *Bereitstellungshandbuch für Exchange Server 2003* (http://go.microsoft.com/fwlink/?linkid=14576).

Wenn Sie RPC über HTTP in Ihrer Unternehmensumgebung bereitstellen, stehen Ihnen zwei grundlegende Bereitstellungsoptionen zur Verfügung, je nachdem, wo Sie Ihren RPC-Proxyserver platzieren:

- **Option 1 (empfohlen)** Stellen Sie ISA Server im Perimeternetzwerk bereit, und platzieren Sie den RPC-Proxyserver (den Exchange Front-End-Server) innerhalb des Unternehmensnetzwerks.

  Hinweis Wenn Sie ISA Server als erweiterten Firewallserver verwenden, stehen Ihnen mehrere Bereitstellungsoptionen zur Verfügung. Weitere Informationen zum Installieren von ISA Server als erweiterten Firewallserver finden Sie in der Dokumentation *Using Microsoft Exchange 2000 Front-End Servers* (http://go.microsoft.com/fwlink/?LinkId=14575).

- **Option 2** Platzieren Sie den Exchange 2003-Front-End-Server, der als RPC-Proxyserver verwendet wird, innerhalb des Perimeternetzwerks.

Die beiden Optionen werden in den folgenden Abschnitten genau beschrieben.

Option 1: ISA Server im Perimeternetzwerk

Die erste Option ist die Verwendung von ISA Server im Perimeternetzwerk und das Platzieren des RPC-Proxyservers (Front-End) innerhalb des Unternehmensnetzwerks. Dies ist die empfohlene Variante. Wenn Sie zum Routing von RPC über HTTP-Anforderungen ISA Server im Perimeternetzwerk verwenden und den Exchange-Front-End-Server im Unternehmensnetzwerk platzieren,

müssen Sie im internen Firewall nur Anschluss 80
oder Anschluss 443 öffnen, damit Outlook 2003-Clients mit Exchange kommunizieren können. Darüber hinaus können Sie den internen Firewall zwischen ISA Server und
dem Unternehmensnetzwerk vollständig entfernen, da in ISA Server mit Feature Pack 1 zusätzliche Sicherheitsfeatures zur Verfügung stehen, die herkömmliche Firewalls nicht bieten. Abbildung 5.2 zeigt dieses Bereitstellungsszenario.

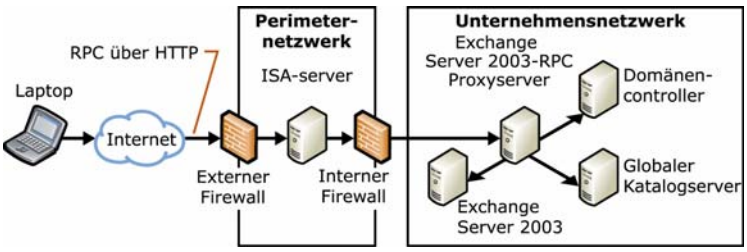


Abbildung 5.2 Bereitstellen von RPC über HTTP unter Verwendung von ISA-Server als Reverse-Proxyserver im Perimeternetzwerk

Wenn sich der Server mit ISA Server im Perimeternetzwerk befindet, ist er für das Routing von RPC über HTTP-Anforderungen an den Exchange-Front-End-Server verantwortlich, der als RPC-Proxyserver verwendet wird. In diesem Szenario verwendet der RPC-Proxyserver vorgegebene Anschlüsse für den Datenaustausch mit anderen Servern, die RPC über HTTP verwenden.

Option 2: RPC-Proxyserver im Perimeternetzwerk

Obwohl diese Konfiguration nicht empfohlen wird, können Sie den Exchange Server 2003-Front-End-Server, der als RPC-Proxyserver verwendet wird, innerhalb
des Perimeternetzwerks platzieren. In diesem Szenario legen Sie eine beschränkte Anzahl von Anschlüssen fest, die der RPC-Proxyserver benötigt. Abbildung 5.3 zeigt dieses Bereitstellungsszenario. Beachten Sie, dass der Exchange-Front-End-Server
im folgenden Beispiel zusätzlich zu den Anschlüssen für RPC über HTTP für den Datenaustausch mit dem internen Unternehmensnetzwerk weiterhin alle Standardanschlüsse benötigt.

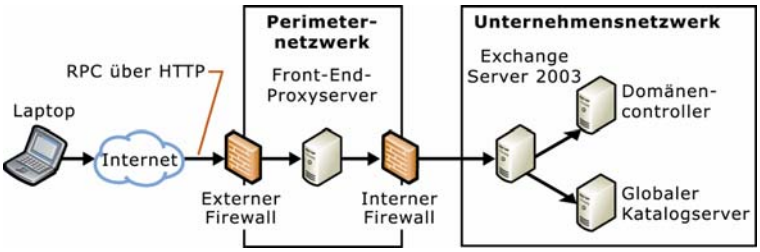


Abbildung 5.3 Bereitstellen von RPC über HTTP auf dem Exchange-Front-End-Server im Perimeternetzwerk

Weitere Informationen über die Konfiguration der RPC über HTTP-Bereitstellungsoptionen 1 und 2 finden Sie weiter unten in diesem Kapitel unter „Bereitstellen von RPC über HTTP“. Zur Wiederholung: In diesem Szenario verwendet der RPC-Proxyserver vorgegebene Anschlüsse, um mit anderen Servern zu kommunizieren, die RPC über HTTP verwenden.

Bereitstellen von RPC über HTTP

Gehen Sie zum Bereitstellen von RPC über HTTP folgendermaßen vor:

1. Konfigurieren Sie Ihren Exchange-Front-End-Server als einen RPC-Proxyserver.
2. Konfigurieren Sie das virtuelle RPC-Verzeichnis in Internet Information Services (IIS) auf dem Exchange-Front-End-Server.
3. Konfigurieren Sie die Registrierung auf dem Exchange 2003-Computer, der mit dem RPC-Proxyserver kommuniziert so, dass von Exchange 2003 angegebene Anschlüsse für die RPC über HTTP-Kommunikation verwendet werden.
4. Öffnen Sie die angegebenen Anschlüsse auf der internen Firewall für RPC über HTTP sowie die Standardanschlüsse für Exchange-Front-End-Kommunikation.
5. Erstellen Sie ein Profil für Ihre Benutzer für die Verwendung von RPC über HTTP.

Nachdem Sie diese Schritte durchgeführt haben, können die Benutzer mit RPC über HTTP auf den Exchange-Front-End-Server zugreifen.

Um RPC über HTTP verwenden zu können, müssen Sie Windows Server 2003 auf folgenden Computern ausführen:

- Allen Exchange 2003-Servern, auf die mit RPC über HTTP zugegriffen wird
- Dem Exchange 2003-Front-End-Server, der die Rolle als RPC-Proxyserver übernimmt
- Alle Domänencontroller, die mit den Outlook 2003-Clients kommunizieren, und die Exchange 2003-Server, die für die Verwendung von RPC über HTTP konfiguriert wurden
- Der globale Katalogserver, der von Outlook 2003-Clients verwendet wird, und die Exchange 2003-Server, die für die Verwendung von RPC über HTTP konfiguriert wurden

Exchange 2003 muss auf allen Exchange-Servern installiert sein, die der RPC-Proxyserver verwendet. Zusätzlich muss auf allen Clientcomputern, auf denen Outlook 2003 ausgeführt wird, Microsoft Windows XP Service Pack 1 (SP1) oder höher einschließlich der Aktualisierung „Windows XP Patch: RPC Updates Needed for Exchange Server 2003 Beta“ (http://go.microsoft.com/fwlink/?LinkId=16687) ausgeführt werden.

Einplanen hoher Verfügbarkeit

In diesem Kapitel werden Fragen besprochen, die für die Entwicklung eines absolut zuverlässigen und ständig verfügbaren Messagingsystems relevant sind, beispielsweise im Zusammenhang mit Speichertechnologien, Clustering, Serverabstimmung und Clientkonfiguration.

Um ein zuverlässiges und ständig verfügbares Messagingsystem zu entwerfen, müssen Sie die Fehlertoleranz des Systems maximieren. Fehlertoleranz bezieht sich auf die Fähigkeit eines Systems, trotz teilweisen Systemausfällen weiter zu funktionieren.
In einer fehlertoleranten Serverorganisation wird durch vorbeugende Maßnahmen
die Wahrscheinlichkeit des Auftretens eines schwerwiegenden Ausfalls gering gehalten, und im Falle eines solchen Ausfalls werden dessen Auswirkungen minimiert.

Um die Fehlertoleranz der Microsoft® Exchange Server 2003-Organisation sicherzustellen, müssen Sie auf verschiedenen Ebenen der Infrastruktur entsprechende Maßnahmen ergreifen. In Abbildung 6.1 werden die verschiedenen Ebenen dargestellt und die Maßnahmen zusammengefasst, die Sie auf der jeweiligen Ebene zum Maximieren
der Fehlertoleranz unternehmen können.

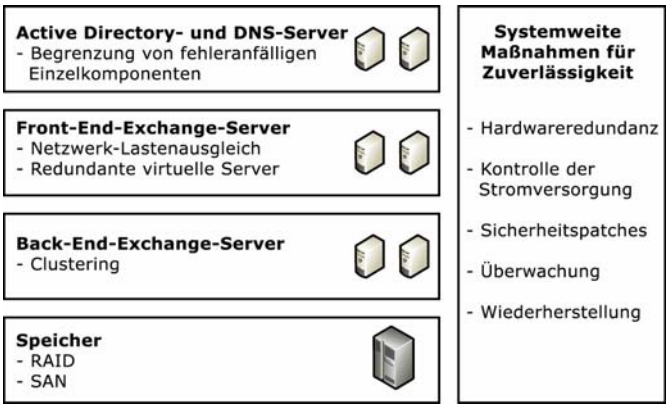


Abbildung 6.1 Maßnahmen für erhöhte Zuverlässigkeit des Messagingsystems

Im verbleibenden Teil dieses Kapitels werden die unterschiedlichen Möglichkeiten behandelt, wie Sie bereits beim Systementwurf auf jeder Stufe der Messagingsystem-Infrastruktur eine erhöhte Fehlertoleranz des Messagingsystems einplanen können:

- **Maßnahmen für systemweite Zuverlässigkeit** Berücksichtigen Sie im gesamten System solche Punkte wie Hardwareredundanz, Kontrolle der Stromversorgung und Systemüberwachung.
- **Microsoft Active Directory®-Verzeichnisdienst- und DNS-Verfügbarkeit** Stellen Sie sicher, dass die Domänencontroller, globalen Katalogserver und DNS-Server vor Ausfällen geschützt sind.
- **Front-End-Server-Verfügbarkeit** Setzen Sie zum Erhöhen der Verfügbarkeit Netzwerklastenausgleich und zusätzliche virtuelle Server ein.
- **Back-End-Server- und Exchange-Daten-Verfügbarkeit** Partitionieren
Sie die Exchange-Dateien, und verwenden Sie Serverclustering.

- **Speicherlösungen für Exchange-Daten** Verwenden Sie RAID- (Redundant Array of Independent Disks) und SAN-Technologien (Storage Area Network), um die Fehlertoleranz zu erhöhen.

Systemweite Maßnahmen für erhöhte Zuverlässigkeit

Sie können bereits beim Entwurf eine Reihe von Maßnahmen zur Erhöhung der Fehlertoleranz in das System einplanen, von denen nicht nur das Messagingsystem sondern auch das gesamte Netzwerk profitiert. In den folgenden Abschnitten werden die nachstehenden Möglichkeiten zum Maximieren der Fehlertoleranz behandelt:

- Hardwareredundanz
- Kontrolle der Stromversorgung
- Sicherheitspatches und Antivirusmaßnahmen
- Überwachung
- Planung für die Wiederherstellung nach Datenverlust

Hardwareredundanz

Es ist von entscheidender Bedeutung, dass Sie in Ihre Planung spezielle Server und Speicherhardwarekonfigurationen aufnehmen, durch die die Hardware der Exchange-Organisation mehrfach vorhanden ist, um auf diese Weise die Anzahl nur einmal vorhandener und damit ausfallanfälliger Systemhardware zu minimieren. Durch das Einplanen dieser mehrfachen Hardwarekonfigurationen kann einer der Pfade für Eingabe-/Ausgabedaten oder eine physische Hardwarekomponente eines Servers (z. B. Computer, Netzwerk oder SAN-Komponenten) ausfallen, ohne den Betrieb des Servers zu beeinträchtigen.

Welche Hardware zum Minimieren der Anzahl nur einmal vorhandener Systemkomponenten verwendet wird, ist davon abhängig, für welche Komponenten Sie Redundanz einplanen möchten. In einige der neuesten Produkte von Hardwareherstellern ist in die Hardware der Server- und Speicherlösungen bereits Redundanz eingebaut. Einige Hardwarehersteller bieten sogar Hardwareimplementierungen wie Sicherungs- und Wiederherstellungshardware für Exchange an.

Neben der Sicherstellung, dass Ihre Organisation angemessene Ersatzhardware oder Spezialhardware enthält, können Sie auch die Auswirkungen eines Hardwareausfalls oder anderen Problems (z. B. eines Softwareausfalls oder Sicherheitsproblems) minimieren, indem Sie die weiteren Punkte in diesem Abschnitt berücksichtigen.

> **Hinweis** Eine detaillierte Beschreibung zusätzlicher diese Art von Hardware betreffenden Technologien über die dargestellten Technologien hinaus würde den Rahmen dieser Dokumentation sprengen. Weitere Informationen über die Implementierung von Hardware zum Minimieren von einzelnen Fehlerquellen finden Sie auf der Microsoft Exchange-Website (http://go.microsoft.com/fwlink/?LinkId=21573).

Kontrolle der Stromversorgung

Für Server, auf denen unternehmenswichtige Daten gespeichert werden, ist besonders bei umfangreichen Serverbereitstellungen die Verwendung einer unterbrechungsfreien Stromversorgung (USV) und

einer Akkureserve zur Erhöhung der Ausfalltoleranz unerlässlich. Eine USV und eine Akkureserve bieten Schutz gegen Spannungsspitzen
und kurzzeitige Stromausfälle, durch die Ihre Server und die darauf gespeicherten Daten beschädigt werden können. Wenn der Serverstandort für den ordnungsgemäßen Betrieb der Hardware klimatisiert werden muss, ziehen Sie in Betracht, das entsprechende Steuerungssystem ausfalltolerant zu gestalten. (Halten Sie beispielsweise für jedes Kühlelement eine Akkureserve bereit.)

Sicherheitspatches und Antivirusmaßnahmen

Ergreifen Sie die nachstehenden Vorsichtsmaßnahmen, um die Server in Ihrer Exchange-Organisation vor zufälligen oder absichtlich herbeigeführten Beschädigungen zu bewahren, die zu Ausfallzeiten führen können:

- Wenden Sie auf die Server stets alle aktuellen Sicherheitspatches an. Durch das Abonnement des Microsoft Security Notification-Dienstes wird sichergestellt, dass Sie über alle veröffentlichten Security Bulletins für jedes Produkt von Microsoft umgehend informiert werden. Wenn Sie den Dienst abonnieren möchten, besuchen Sie die Website für Benachrichtigungen zur Produktsicherheit (http://go.microsoft.com/fwlink/?LinkId=12217).
- Stellen Sie sicher, dass die Zugriffsberechtigungen ordnungsgemäß eingerichtet sind.
- Betreiben Sie die Server in einer physischen Umgebung, in der nicht autorisierte Personen keinen Zugang haben.
- Stellen Sie sicher, dass auf allen Servern angemessene Antivirussoftware installiert ist. Achten Sie darauf, die Software stets mit den neuesten Virussignaturdateien zu aktualisieren. Verwenden Sie dazu u. U. auch das Feature zur automatischen Aktualisierung der verwendeten Antivirus-Software.

  Wichtig Scanprogramme auf Dateiebene führen bei Verwendung mit Exchange zu Problemen. Wenn Sie ein Virenscanprogramm auf Dateiebene einsetzen möchten, müssen Sie die Exchange-Verzeichnisse vom Scan ausschließen. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 328841, „XADM: Exchange and Antivirus Software“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=328841).

Überwachung

Zum Maximieren der Zuverlässigkeit des Systems müssen Sie in der Lage sein, Ihre
Server ständig zu verwalten und zu überwachen sowie Probleme unverzüglich zu beheben. Beim Auftreten eines Problems müssen Sie schnell reagieren können, damit Sie die
Daten wiederherstellen und so schnell wie möglich wieder verfügbar machen können. Microsoft Operations Manager Exchange Management Pack ist eine systemweite Überwachungslösung, die Sie mit Exchange 2000 verwenden können. Weitere Informationen über Microsoft Operations Manager finden Sie in der Onlinedokumentation *Monitoring Exchange 2000 with Microsoft Operations Manager 2000* (http://go.microsoft.com/fwlink/?LinkId=18177 Microsoft Operations Manager
Exchange Management Pack ist Bestandteil von Exchange 2003.

Planung für die Wiederherstellung nach Datenverlust

Zusätzlich zu den umfassenden Anstrengungen, die Sie zur Erhöhung der Fehlertoleranz der physischen Infrastruktur unternehmen, müssen Sie auch eine sorgfältig geplante Sicherungs- und Wiederherstellungsstrategie entwickeln. Weitere Informationen über die Entwicklung eines Plans für die Wiederherstellung bei Datenverlust finden Sie

in der Onlinedokumentation *Disaster Recovery for Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?linkid=18350). Obwohl sich diese Dokumentation auf Exchange 2000 bezieht, gelten die vorgestellten Konzepte im Wesentlichen auch für Exchange 2003.

Active Directory- und DNS-Server-Verfügbarkeit

Exchange ist in großem Maße von Active Directory und DNS (Domain Name System) abhängig. Stellen Sie aus diesem Grund sicher, dass Domänencontroller, globale Katalogserver und DNS-Server in Ihrer Organisation gut gegen mögliche Ausfälle geschützt sind.

In den meisten Bereitstellungsszenarien empfiehlt es sich nicht, Exchange auf Computern auszuführen, die auch als Microsoft Windows Server™ 2003-Domänencontroller fungieren. Stattdessen sollten Sie Server, auf denen Exchange und Microsoft Windows® ausgeführt werden, als separate Computer konfigurieren, da auf diese Weise bei Problemen auf einem Computer der andere nur mit geringer Wahrscheinlichkeit ebenfalls betroffen ist. Wenn die Server, auf denen Exchange ausgeführt wird, neben dem Antworten auf Anforderungen von Exchange-Clients keine weiteren Aufgaben als Domänencontroller ausführen müssen, erhöht sich außerdem die Leistung dieser Server unter hoher Belastung durch viele Benutzer.

Speichern Sie zusätzlich die Informationen auf mehr als einem Domänencontroller, um die Sicherheit der Active Directory-Informationen weiter zu erhöhen. Falls auf einem der Server ein Problem auftritt, muss zur Sicherheit mindestens ein weiterer Server verfügbar sein, damit die Active Directory-Informationen nicht verloren gehen.

Front-End-Server-Verfügbarkeit

Ergreifen Sie für Exchange-Front-End-Server zur Erhöhung der Fehlertoleranz des Messagingsystems die folgenden Maßnahmen:

- Verwenden des Netzwerklastenausgleichs
- Erstellen redundanter virtueller Server

Verwenden des Netzwerklastenausgleichs

In einer Unternehmens- oder Hostingumgebung empfiehlt sich unter Umständen der Lastenausgleich der Front-End-Server. Unter Windows steht diese Funktion über den Netzwerklastenausgleich zur Verfügung.

Beim Windows-Netzwerklastenausgleich werden mindestens zwei Server zum Netzwerklastenausgleich-Cluster mit einer eigenen IP-Adresse zusammengefasst. Jeder Computer empfängt den Datenverkehr an seine eigene eindeutige IP-Adresse und an die gemeinsame IP-Adresse. Jedes Mitglied des Netzwerklastenausgleich-Clusters führt einen Hash-Algorithmus durch, um eingehende Clientanforderungen anhand der IP-Adresse des Clients, der verwendeten Anschlussnummer und weiterer Informationen einem der Mitglieder des Netzwerklastenausgleich-Clusters zuzuordnen. Beim Eintreffen eines Datenpakets führen alle Server oder Hosts denselben Hash-Algorithmus durch. Als Ergebnis wird einer der Hosts ermittelt. Dieser Host antwortet dann auf das Datenpaket. Die Zuordnung ändert sich nicht, solange die Anzahl der Hosts im Netzwerklastenausgleich-Cluster gleich bleibt.

Erstellen redundanter virtueller Server

Beim Konfigurieren des Netzwerklastenausgleichs erstellen Sie auf allen Front-End-Servern im Netzwerklastenausgleich-Cluster identische virtuelle Server. Durch das Konfigurieren redundanter virtueller Server wird der Lastenausgleich erleichtert. Außerdem müssen die Konfigurationen aller Server im Netzwerklastenausgleich-Cluster identisch sein. Andernfalls kann das Verhalten der Clients in Abhängigkeit des Servers, über den sie geroutet sind, variieren.

Back-End-Server- und Exchange-Daten-Verfügbarkeit

Es gibt eine Reihe von Empfehlungen zum Maximieren der Verfügbarkeit der Exchange-Daten auf Back-End-Servern. Oberstes Ziel ist es, die Exchange-Anwendungsdaten
und -Messagingdaten so zu partitionieren, dass die Fehlertoleranz erhöht und die Problembehebung erleichtert wird. Partitionieren Sie die Exchange-Anwendungsdaten und -Messagingdaten wie folgt:

- **Verwenden der empfohlenen Vorgehensweise zur Serverpartitionierung** Trennen Sie die Exchange-Anwendungsdateien
  von den Exchange-Daten.
- **Speichern der Transaktionsprotokolldateien und Datenbankdateien** Speichern Sie diese Dateien getrennt, um die Fehlertoleranz zu erhöhen und die Wiederherstellung der Daten zu optimieren.
- **Verwenden von Serverclustering** Fassen Sie die Back-End-Server zu Clustern zusammen, um die Verfügbarkeit des Messagingsystems zu optimieren.

Empfohlene Vorgehensweise zur Serverpartitionierung

Zur Erhöhung der Fehlertoleranz und leichteren Fehlerbehebung sollten Sie die Festplatten so partitionieren, dass die Exchange-Anwendungsdateien, Exchange-Datenbankdateien und Exchange-Transaktionsprotokolldateien alle auf unterschiedlichen Datenträgern abgelegt sind, um die Leistung zu erhöhen und die Menge an wiederherzustellenden Daten zu verringern. (Weitere Informationen über das Speichern von Transaktionsprotokolldateien und Datenbankdateien finden Sie im Abschnitt „Speichern von Transaktionsprotokolldateien und Datenbankdateien“ weiter unten in diesem Kapitel.)

Wenn Sie die Festplatten diesen Empfehlungen entsprechend partitionieren, ist jeder Gruppe von Dateien ein eigener Laufwerkbuchstabe zugeordnet. Auf diese Weise
haben Sie eine bessere Übersicht, welche Partitionen entsprechend dem verwendeten Wiederherstellungsverfahren bei Datenverlust jeweils gesichert werden müssen.

In Tabelle 6.1 wird ein möglicher Partitionierungsplan für einen Exchange-Server dargestellt, der über sechs Festplatten und zwei Speichergruppen verfügt, die jeweils vier Datenbanken enthalten. Da die Anzahl der für Ihren Exchange-Server verwendeten Festplatten und Speichergruppen von der in diesem Beispiel verwendeten abweichen kann, übertragen Sie das im Beispiel veranschaulichte Prinzip auf Ihre eigene Serverkonfiguration. Beachten Sie in Tabelle 6.1, dass die Laufwerke E:, F:, G: und H: möglicherweise auf externe Speichergeräte verweisen.

Tabelle 6.1 Exchange-Festplattenpartitionierungsplan

Festplatte	Laufwerkskonfiguration
Festplatte 1	Laufwerk C: (NTFS) – Windows-Betriebssystemdateien und Auslagerungsdatei.
Festplatte 2	Laufwerk D: (NTFS) – Exchange-Dateien und zusätzliche Serveranwendungen (z. B. Antivirus-Software und Resource Kits).
Festplatte 3	Laufwerk E: (NTFS) – Transaktionsprotokolldateien für Speichergruppe 1.
Festplatte 4	Laufwerk F: (NTFS) – Datenbankdateien für Speichergruppe 1.
Festplatte 5	Laufwerk G: (NTFS) – Transaktionsprotokolldateien für Speichergruppe 2.
Festplatte 6	Laufwerk H: (NTFS) – Datenbankdateien für Speichergruppe 2.

Die in diesem Abschnitt dargestellten Partitionierungsempfehlungen können Sie unabhängig davon anwenden, ob Sie die Exchange-Datenbankdateien auf einem Server oder einer erweiterten Speicherlösung (z. B. ein SAN) speichern. Zusätzlich zur Partitionierung empfiehlt es sich, Technologien wie Festplattenspiegelung (RAID-1) und verteilte Speicherung auf mehreren Festplatten mit Paritätsprüfung (RAID-5 oder RAID-6) einzusetzen. Weitere Informationen zu diesen Technologien finden Sie im Abschnitt „Exchange-Datenspeicherlösungen“ weiter unten in diesem Kapitel.

Speichern von Transaktionsprotokolldateien und Datenbankdateien

Wie im vorhergehenden Abschnitt besprochen, müssen Sie zur Gewährleistung einer Fehlertoleranz für den Fall eines Festplattenausfalls Ihre Exchange-Transaktionsprotokolldateien und Datenbankdateien auf getrennten physischen Festplattenlaufwerken speichern. Außerdem können Sie durch Speichern dieser Protokolldateien und Datenbankdateien auf getrennten Laufwerken die Festplatten-E/A-Leistung deutlich verbessern.

> **Hinweis** Die Vorgänge, die auf den Datenbanken innerhalb einer Speichergruppe durchgeführt wurden, können nachverfolgt werden, da jede Speichergruppe über eigene Transaktionsprotokolldateien verfügt. Transaktionsprotokolldateien enthalten einen sequenziellen Datensatz von jedem auf einer Datenbank durchgeführten Vorgang. Transaktionsprotokolldateien werden erst gelöscht, nachdem eine normale oder inkrementelle Sicherung für alle Datenbanken einer Speichergruppe durchgeführt wurde.

Wenn ein Verlust der Festplatte mit den Exchange-Datenbanken vorliegt, können Sie die beschädigte Festplatte ersetzen und dann die aktuellsten Sicherungen wiederherstellen. Nachdem Sie die Datenbanken wiederhergestellt haben, werden durch automatische Wiedergabe der Protokolldateien aller nach der Sicherung aufgetretenen Transaktionen die aufgezeichneten Transaktionen aus den Protokolldateien auf die Datenbanken der Festplatte übertragen. Dieser Vorgang kann sowohl „Hard Recovery“-Vorgänge als auch „Soft Recovery“-Vorgänge enthalten. Hard Recovery bezieht sich auf den Vorgang der Wiedergabe von Transaktionsprotokolldateien von Band, nachdem eine Datenbank aus einer Onlinesicherung wiederhergestellt wurde. Wenn Exchange nach der Hard Recovery ermittelt, dass auf dem Server weitere Protokolldateien zur Wiedergabe zur Verfügung stehen, werden diese weiteren Protokolldateien durch einen Soft Recovery-Vorgang in der wiederhergestellten Datenbank wiederhergestellt.

Besteht ein Verlust der Festplatte mit den Transaktionsprotokolldateien, nicht jedoch der Festplatte mit Ihren Datenbanken, müssen die Exchange-Daten nicht aus der Sicherung wiederhergestellt werden. Der Verlust der Festplatte mit den Transaktionsprotokolldateien ist jedoch gefährlicher als der Verlust der Festplatte mit den Datenbanken. Der Grund hierfür ist, dass Transaktionen, die in Protokolldateien, nicht jedoch in physischen Datenbankendateien auf der Festplatte aufgezeichnet wurden, nicht wiedergegeben werden können. Dies erhöht die Wahrscheinlichkeit des Verlusts von Daten, die weder in den Protokolldateien noch in der aktuellsten Sicherung enthalten waren. Werden die

Datenbanken getrennt, werden die Transaktionen im Speicher in die Datenbanken der Festplatte geschrieben, um diese zu aktualisieren (auch als „dirty shutdown“ bzw. „fehlerhaftes Herunterfahren“ bezeichnet). Verwenden Sie zum Reparieren **ESEUTIL**, um diese Datenbanken konsistent ohne die fehlenden Protokolldateien wiederherzustellen. Wenn Sie verlorene Transaktionsprotokolldateien wiederherstellen möchten, kopieren Sie zuerst die inkonsistenten Datenbankdateien (*.EDB- und *.STM-Dateipaare) an einen sicheren Ort. Stellen Sie dann die
Datenbank aus der Sicherung wieder her, und geben alle zur Verfügung stehenden Transaktionsprotokollen wieder. Reparieren Sie dann die inkonsistente Datenbank, und stellen Sie sie anschließend entweder in einer Speichergruppe für die Wiederherstellung oder auf einem anderen Wiederherstellungsserver der Gesamtstruktur bereit. Verwenden Sie abschließend **ExMerge.exe**, um die Änderungen aus der inkonsistenten Datenbank wiederherzustellen und in die wiederhergestellte Datenbank zu verschieben.

> **Wichtig** Wenn Sie Ihre Exchange-Datenbanken und Transaktionsprotokolldateien auf derselben physischen Festplatte speichern und diese Festplatte ausfällt, können nur die Daten wiederhergestellt werden, die vor der letzten Sicherung vorhanden waren.

Sie können die zur Wiederherstellung nach einem Festplattenausfall benötigte Zeit minimieren, indem Sie jede Exchange-Speichergruppe auf einer separaten Festplatte speichern. Wenn nur eine Festplatte ausfällt und sich jede Speichergruppe auf einer separaten physischen Festplatte befindet, müssen Sie nur die Speichergruppe auf der ausgefallenen Festplatte wiederherstellen.

Festplattendefragmentierung

Während der Festplattendefragmentierung werden Daten auf den Festplatten eines Servers neu angeordnet, um die Dateien für effizienteres Lesen zusammenhängender zu gestalten. Durch Defragmentierung der Festplatte wird die Festplattenleistung verbessert und reibungsloses und effizientes Ausführen der Server in Ihrer Exchange-Organisation gewährleistet.

Da eine erhebliche Festplattenfragmentierung zu Leistungsproblemen führen kann, sollten Sie in regelmäßigen Abständen, oder wenn die Serverleistung unter das normale Niveau fällt, ein Festplattendefragmentierungsprogramm (z. B. **Defragmentierung**) ausführen. Stellen Sie sicher, dass Ihre Festplatten vor kurzem defragmentiert wurden, da zum Speichern eines erheblich fragmentierten Dateisystems mehr Lesevorgänge erforderlich sind.

Auch Exchange-Datenbanken müssen defragmentiert werden. Standardmäßig
erfolgt auf Exchange-Datenbanken täglich eine Onlinedefragementierung. Sie können Offlinedefragmentierungen mithilfe von **ESEUTIL** ausführen. Die Datenbanken müssen hierfür offline sein. Eine Offlinedefragmentierung für Exchange-Datenbanken wird normalerweise nur dann empfohlen, wenn eine große Anzahl Benutzer von dem
Server, auf dem Exchange 2003 ausgeführt wird, verschoben wird. Da durch Offlinedefragmentierung die Datenbankseiten vollständig geändert werden, sollten
Sie sofort nach der Offlinedefragmentierung neue Sicherungen der Exchange 2000-Datenbanken erstellen. Weitere Informationen zur Online- und Offlinedefragmentierung finden Sie unter „Online and Offline Defragmentation“ im technischen Artikel *Disaster Recovery for Microsoft Exchange 2000 Server* (http://go.microsoft.com/fwlink/?linkid=18350).

Aspekte zum Festplattenspeicher

Stellen Sie sicher, dass für die Server, auf denen Exchange ausgeführt wird, ausreichend Speicherplatz auf der Festplatte zur Verfügung steht. Sie benötigen ausreichend Speicherplatz, um sowohl die Datenbank als auch die Protokolldateien wiederherstellen zu können.

Es kann vorkommen, dass eine Sicherung zu groß ist, um am Originalspeicherort wiederhergestellt zu werden. Beispielsweise könnten eine normale Sicherung, die wöchentlich ausgeführt wird plus sechs Tage differenzielle Sicherungen bei der Wiederherstellung mehr Speicherplatz erfordern, als auf dem Server zur

Verfügung steht. Ob die Wiederherstellung mehr Speicherplatz erfordert, als zur Verfügung steht, ist von der Anzahl der während einer Woche erzeugten Protokolldateien abhängig.
Ein Server, auf dem 2.000 Protokolldateien pro Woche erzeugt werden, erfordert z. B. 10 GB Protokolldateispeicherplatz, zusätzlich zu dem für die Datenbank erforderlichen Speicherplatz.

Das tägliche Durchführen von normalen Sicherungen reduziert die Größe des erforderlichen Speicherplatzes für die Wiederherstellung von Exchange-Datenbanken. Der Grund hierfür ist, dass bei normalen Sicherungen die Transaktionsprotokolldateien bis zu dem Zeitpunkt der Sicherung gelöscht werden. Wenn Sie also Ihre Exchange-Datenbanken wiederherstellen müssen, sollten Sie täglich normale Sicherungen durchführen. Damit wird gewährleistet, dass nicht mehr Protokolldateien, als an einem Tag anfallen, wiederhergestellt werden müssen.

Außerdem darf das Datenbanklaufwerk (die Festplatte mit den .edb- und .stm-Dateien) nur bis maximal 50 % belegt sein. Dies führt zwar dazu, dass ein Teil des Festplattenspeichers ungenutzt bleibt. Aus folgenden Gründen können dadurch jedoch erweiterte Server-Ausfallzeiten reduziert werden:

- Datenbanken können schneller wiederhergestellt werden als mit einem vollen Laufwerk (vor allem, wenn das Dateisystem fragmentiert ist).
- Offlinedefragmentierungen können auf derselben physischen Festplatte durchgeführt werden; die Datenbanken müssen also nicht auf einen Wartungsserver kopiert werden. (Für diese Aufgabe wird wesentlich mehr Zeit benötigt als für das Kopieren von Datenbankdateien in ein temporäres Verzeichnis auf derselben physischen Festplatte.)
- Vor der Wiederherstellung kann eine Kopie der Datenbanken auf derselben physischen Festplatte gesichert werden. Sollte während des Wiederherstellungsvorgangs ein Problem auftreten, können Sie dann versuchen, die Datenbanken zu reparieren (wenn die vorhandene Sicherung beispielsweise fehlerhaft ist). Es wird daher empfohlen, dass
  Sie vor dem Wiederherstellen einer Datenbank die aktuelle Datenbank und die Protokolldateien verschieben oder kopieren.

  Hinweis Aufgrund der Größe einer durchschnittlichen Datenbank kann sich Ihre Ausfallzeit durch das Kopieren der aktuellen Datenbank auf ein anderes physisches Festplattenlaufwerk oder auf einen anderen Server um mehrere Stunden erhöhen. Wenn jedoch ausreichend lokaler Festplattenspeicherplatzauf demselben physischen Laufwerk zur Verfügung steht, können Sie die aktuellen Datenbankdateien vor der Wiederherstellung mithilfe einer Eingabeaufforderung oder mit Windows Explorer in einen anderen Ordner verschieben.

Verwenden des Serverclusterdienstes

Der Clusterdienst von Microsoft Cluster Server ist ein Windows Server-Feature, das Administratoren zur Verfügung gestellt wird, um permanente Verfügbarkeit von Serverressourcen zu gewährleisten.

Vor dem Planen und Bereitstellen von Exchange 2003-Clustern müssen Sie mit den Konzepten des Clusterdienstes vertraut sein. Viele Ressourcen, einschließlich Windows Server 2003-Hilfe, *Microsoft Windows Server 2003 Resource Kit* und Websites, wie z. B. Microsoft Developer Network (MSDN®), enthalten Informationen zu den Clustering-Konzepten von Windows Server 2003. Eine Auflistung weiterer Ressourcen finden
Sie am Ende dieses Dokuments.

Vorteile des Clustering

Durch das Erstellen von Exchange-Clustern wird eine hohe Verfügbarkeit sichergestellt, so dass unternehmenswichtige Anwendungen im Falle eines Ausfalls weiterhin ausgeführt werden können.

Ein gängiger IT-Ausdruck für maximale Zuverlässigkeit lautet „fünf Neunen“. Dies bedeutet, dass ein Server zu 99,999 % der Zeit ausgeführt wird und pro Jahr nur 5 Minuten Ausfallzeit anfallen. Für die meisten Unternehmen sind jedoch solche strengen Anforderungen an die Betriebszeit nicht erforderlich.

Für die häufigsten Verwendungsszenarien ist eine Betriebszeit von 99,99 % angemessen, da dieser Prozentwert weniger als einer Stunde Ausfallzeit pro Jahr entspricht. Aberdeen Group, Inc. fand heraus, dass mit Windows Server bereits 99,95 % Betriebszeit erreicht werden, bevor die Server für die Umgebung vollständig optimiert und die IT-Mitarbeiter mit der Verwendung des neuen Betriebssystems vertraut sind.

Durch das Erstellen von Exchange-Serverclustern wird die Zuverlässigkeit von Windows nutzbar gemacht, so dass Sie ständig verfügbare Exchange-Cluster erstellen können. Auf der Windows-Website http://go.microsoft.com/fwlink/?LinkId=9066 finden Sie den Bericht der Aberdeen Group, Inc. sowie weitere Informationen zur Zuverlässigkeit von Windows.

In den folgenden Abschnitten wird die Zuverlässigkeit in Exchange-Clustern behandelt.

Exchange 2003-Clusteringfeatures

Exchange 2003 bietet eine Reihe von Verbesserungen für das Clustering. Exchange 2003 unterstützt z. B. bis zu acht Knoten und enthält neue Features
für mehr Sicherheit. Für Exchange 2003 wurde auch die Leistung von Exchange-Clustering verbessert. Insbesondere wurde die Zeit reduziert, die ein Server für
den Failover zu einem neuen Knoten benötigt.

Es folgen einige der wichtigsten Updates in Bezug auf Exchange-Clustering für Exchange 2003:

- **Unterstützung für Cluster mit bis zu acht Knoten** Exchange bietet bei der Verwendung mit Windows Server 2003 Enterprise Edition oder Windows Server 2003 Datacenter Edition erweiterte Unterstützung für Aktiv/Passiv-Clusterkonfigurationen mit bis zu acht Knoten.
- **Unterstützung für Datenträger-Bereitstellungspunkte** Exchange bietet bei der Verwendung mit Windows Server 2003 Enterprise Edition oder Windows Server 2003 Datacenter Edition zusätzliche Unterstützung für Datenträger-Bereitstellungspunkte.
- **Verbesserte Failoverleistung** Exchange verfügt über eine verbesserte Clusterleistung, die dadurch erreicht wird, dass ein Server für den Failover zu einem neuen Knoten weniger Zeit benötigt.
- **Erhöhte Sicherheit** Exchange-Clusterserver sind jetzt noch sicherer. Beispielsweise wurde das Exchange 2003-Berechtigungsmodell geändert, und das Kerberos-Authentifizierungsprotokoll ist standardmäßig aktiviert.
- **Verbesserte Überprüfung der Vorbedingungen** Exchange führt jetzt weitere Vorbedingungsprüfungen durch, so dass sichergestellt werden kann, dass Ihre Clusterserver ordnungsgemäß bereitgestellt und konfiguriert werden.

In den folgenden Abschnitten werden einige dieser Features genauer erläutert.
Weitere Informationen über die Exchange-Clusterbildung finden Sie in den folgenden Ressourcen, die in der technischen Bibliothek für Exchange Server 2003 (http://go.microsoft.com/fwlink/?LinkId=21277) zur Verfügung stehen:

- Informationen zur Bereitstellung finden Sie unter „Bereitstellen von Exchange 2003 in einem Cluster“ im *Bereitstellungshandbuch für Exchange Server 2003* (http://go.microsoft.com/fwlink/?LinkId=21768).
- Informationen zur Verwaltung finden Sie unter „Verwalten von Exchange-Clustern“ im *Exchange Server 2003-Administratorhandbuch* (http://go.microsoft.com/fwlink/?LinkId=21769).

  Hinweis Einige der in diesem Abschnitt erläuterten Verbesserungen des Clustering werden verfügbar, wenn das Betriebssystem Windows Server 2003 zusammen mit Exchange 2003 verwendet wird. Weitere Vorteile von Windows Server 2003 für

die Server Ihrer Exchange 2003-Cluster werden im technischen Artikel *Technical Overview of Windows Server 2003 Clustering Services* (http://go.microsoft.com/fwlink/?LinkId=16303) beschrieben.

Unterstützung für Cluster mit bis zu acht Knoten

Exchange 2003 bietet durch die Unterstützung von Exchange-Clustern mit bis zu acht Knoten erweiterte Clustering-Funktionen. Cluster mit acht Knoten werden nur bei der Verwendung mit Windows Server 2003 Enterprise Edition oder Windows Server 2003 Datacenter Edition unterstützt. Als weitere Bedingung für die Einrichtung von Clustern mit drei oder mehr Knoten muss mindestens ein Knoten passiv sein.

Hinweis Alle Empfehlungen für Exchange 2003-Clustering beziehen sich auf Aktiv/Passiv-Clusterkonfigurationen. Aktiv/Aktiv-Clustering wird für zwei Knoten unterstützt.

Unterstützung für Datenträger-Bereitstellungspunkte

Datenträger-Bereitstellungspunkte werden jetzt für freigegebene Festplatten unterstützt, wenn auf den Knoten Ihres Clusters Windows Server 2003 Enterprise Edition oder Datacenter Edition mit vier oder mehr Knoten ausgeführt wird. Datenträger-Bereitstellungspunkte sind Verzeichnisse, die dauerhaft auf bestimmte Festplattenlaufwerke verweisen. (Beispielsweise können Sie **C:\Data** so konfigurieren, dass dieses Verzeichnis auf ein Festplattenlaufwerk verweist.) Durch Bereitstellungspunkte müssen Sie nicht jedem Festplattenlaufwerk einen Laufwerkbuchstaben zuweisen, wodurch die Beschränkung auf 26 Laufwerkbuchstaben umgangen werden kann.

Weitere Informationen über bereitgestellte Laufwerke und deren Erstellung finden Sie in der Windows Server 2003-Dokumentation.

Verbesserte Failoverleistung

Die beim Exchange 2003-Clustering benötigte Zeit eines Knotens für den Failover zu einem anderen Knoten wurde reduziert. Dies führt zu einer Verbesserung der Gesamtleistung. Die folgenden Abschnitte enthalten Informationen über die Verbesserungen bei den Failoverzeiten.

Verbesserte Abhängigkeitshierarchie für Exchange-Dienste

Exchange 2003 bietet eine verbesserte Abhängigkeitshierarchie für Exchange-Dienste, wodurch die für einen Serverfailover benötigte Zeit verringert werden kann. Insbesondere die Exchange-Protokolldienste, die in voherigen Versionen vom Informationsspeicher
von Microsoft Exchange abhängig waren, sind jetzt vom Dienst „Microsoft Exchange-Systemaufsicht“ abhängig (Abbildungen 6.2 und 6.3).

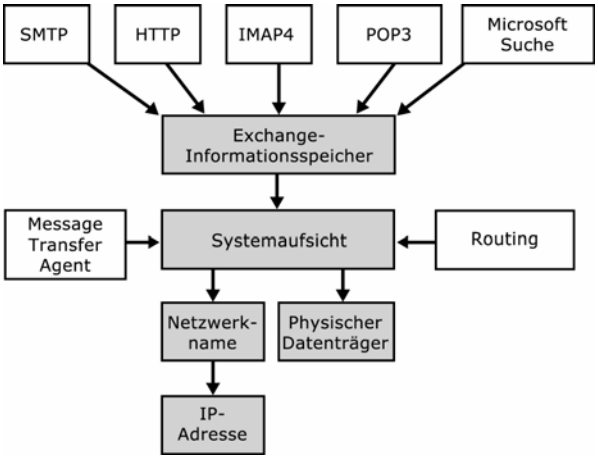


Abbildung 6.2 Hierarchie der Abhängigkeiten bei Exchange 2000

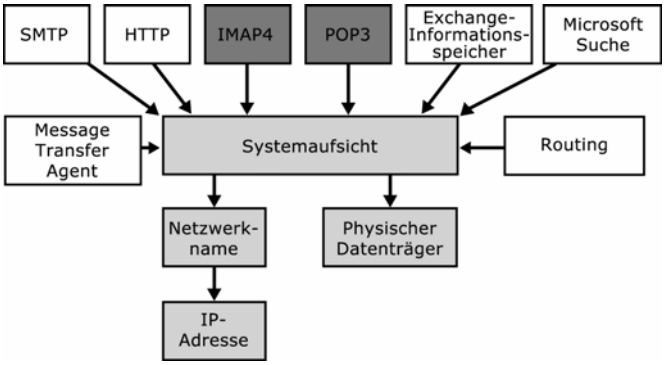


Abbildung 6.3 Hierarchie der Abhängigkeiten bei Exchange 2003

> **Hinweis** In Exchange 2003 werden beim Erstellen eines neuen virtuellen Exchange-Servers die IMAP4- und POP3-Protokollressourcen (Internet Message Access Protocol Version 4rev1 und Post Office Protocol Version 3) nicht mehr automatisch erstellt.

Wenn ein Failover auftritt, können die Exchange-Postfachspeicher, die Informationsspeicher für öffentliche Ordner und die Exchange-Protokolldienste durch diese verbesserte Hierarchie gleichzeitig gestartet werden. Daraus ergibt sich, dass alle Exchange-Ressourcen (außer der Systemaufsichtsdienst) gleichzeitig gestartet und angehalten werden können, wodurch die Failoverzeiten verbessert werden. Außerdem müssen andere Dienste nicht erneut gestartet werden, wenn der Exchange-Informationsspeicher angehalten wird.

Ein weiterer Vorteil ist die Reduzierung von Ausfallzeiten, die durch Failover von virtuellen Exchange-Servern entstehen. Hierdurch können mehrere Minuten eingespart werden.

Verbesserte Erkennung der verfügbaren Knoten

Wenn Exchange 2003 unter Windows Server 2003 ausgeführt wird, wird der freie Knoten vom Clusterdienst automatisch erkannt. Die Gesamtzeit, die Exchange für

den Failover zu dem freien Knoten benötigt, ist reduziert. Dadurch wird die Ausfallzeit bei einem geplanten oder ungeplanten Failover geringer.

Erhöhte Sicherheit

Exchange 2003-Clustering enthält die folgenden Sicherheitsfeatures:

- Änderungen des Berechtigungsmodells für Clustering
- Kerberos ist auf virtuellen Exchange-Servern standardmäßig aktiviert
- IPSec-Unterstützung (Internet Protocol Security) von Front-End-Servern auf Back-End-Clusterserver
- IMAP4- und POP3-Ressourcen werden beim Erstellen eines virtuellen Exchange-Servers nicht standardmäßig hinzugefügt

Im folgenden Abschnitt werden die einzelnen Features genauer erläutert.

Änderungen des Berechtigungsmodells für Clustering

Die zum Erstellen, Löschen oder Ändern eines virtuellen Exchange-Servers erforderlichen Berechtigungen wurden in Exchange 2003 geändert. Diese Änderungen lassen sich am besten anhand eines Vergleichs mit dem Exchange 2000-Berechtigungsmodell verdeutlichen.

> **Hinweis** In den folgenden Abschnitten bezeichnet der Begriff „Cluster-Administrator“ die Person, die in Ihrer Organisation die Exchange-Cluster verwaltet.

Exchange 2000-Berechtigungsmodell

Ein Exchange 2000-Cluster-Administrator kann einen virtuellen Exchange-Server nur erstellen, löschen oder ändern, wenn das Konto des Cluster-Administrators und das Clusterdienstkonto über die folgenden Berechtigungen verfügen:

- Ist der virtuelle Exchange-Server der erste virtuelle Exchange-Server in der Organisation, wird die Berechtigung **Exchange-Administrator - Vollständig** auf Organisationsebene benötigt.
- Ist der virtuelle Exchange-Server nicht der erste virtuelle Exchange-Server in der Organisation, wird die Berechtigung **Exchange-Administrator - Vollständig** auf Verwaltungsgruppenebene benötigt.

Exchange 2003-Berechtigungsmodell

Das Berechtigungsmodell wurde in Exchange 2003 geändert. Für das Clusterdienstkonto von Windows sind keine Exchange-spezifischen Berechtigungen mehr erforderlich. Das bedeutet, dem Clusterdienstkonto von Windows muss nicht mehr die Funktion **Exchange-Administrator – Vollständig** zugewiesen sein, weder auf Ebene der Exchange-Organisation noch auf Ebene der administrativen Gruppe. Die Standardberechtigungen für das Clusterdienstkonto von Windows in der Gesamtstruktur sind für die Funktion in Exchange ausreichend.

Der Cluster-Administrator muss wie in Exchange 2000 über die folgenden Berechtigungen verfügen:

- Wenn es sich beim virtuellen Exchange-Server um den ersten virtuellen Exchange-Server in der Exchange-Organisation handelt, muss der Cluster-Administrator Mitglied einer Gruppe sein, die über die Funktion **Exchange-Administrator - Vollständig** auf Organisationsebene verfügt.

- Wenn es sich beim virtuellen Exchange-Server nicht um den ersten virtuellen Exchange-Server in der Organisation handelt, muss der Cluster-Administrator ein Konto verwenden, das Mitglied einer Gruppe ist, die über die Funktion **Exchange-Administrator - Vollständig** auf der Ebene der administrativen Gruppe verfügt.

Abhängig von dem Modus, in dem die Exchange-Organisation ausgeführt wird (einheitlicher oder gemischter Modus) und abhängig von der Topologiekonfiguration müssen die Cluster-Administratoren jedoch über die folgenden zusätzlichen Berechtigungen verfügen:

- Wenn die Exchange-Organisation im einheitlichen Modus betrieben wird und sich der virtuelle Exchange-Server in einer Routinggruppe befindet, die sich über mehrere administrative Gruppen erstreckt, muss der Cluster-Administrator Mitglied einer Gruppe sein, der die Funktion **Exchange-Administrator - Vollständig** auf administrativer Gruppenebene für alle administrative Gruppen zugewiesen ist, über die sich die Routinggruppe erstreckt. Wenn sich der virtuelle Exchange-Server beispielsweise in einer Routinggruppe befindet, die sich über die erste und zweite administrative Gruppe erstreckt, muss der Cluster-Administrator ein Konto verwenden, das Mitglied einer Gruppe ist, der die Funktion **Exchange-Administrator - Vollständig** für die erste administrative Gruppe zugewiesen ist, und das ebenfalls Mitglied einer Gruppe ist, der die Funktion **Exchange-Administrator - Vollständig** für die zweite administrative Gruppe zugewiesen ist.

  Hinweis Routinggruppen in Exchange-Organisationen, die im einheitlichen Modus ausgeführt werden, können sich über mehrere administrative Gruppen erstrecken. Routinggruppen in Exchange-Organisationen, die im gemischten Modus ausgeführt werden, können sich nicht über mehrere administrative Gruppen erstrecken.

- In Topologien, wie z. B. übergeordneten/untergeordneten Domänen, in denen der Clusterserver der erste Exchange-Server der untergeordneten Domäne ist, benötigen
  Sie die Berechtigung **Nur Exchange-Administrator** auf Organisationsebene, um den für den Empfängeraktualisierungsdienst in der untergeordneten Domäne zuständigen Server festzulegen.

Kerberos auf virtuellen Exchange-Servern standardmäßig aktiviert

Kerberos ist für Windows 2000 Server und höher das Authentifizierungsprotokoll und ermöglicht gegenseitige Authentifizierung. Der Windows-Clusterdienst unterstützt jedoch Kerberos-Clustergruppen erst seit Windows 2000 Server Service Pack 3 (SP3). Daher diente für Exchange-Clusterserver das ältere Authentifizierungsprotokoll, NTLM, als Standard-Authentifizierungsprotokoll.

Da Kerberos im Windows-Clusterdienst unter Windows 2000 SP3 oder höher oder Windows Server 2003 und Exchange 2003 unterstützt wird, wird Kerberos standardmäßig aktiviert, wenn Sie einen virtuellen Exchange-Server auf einem Server mit Windows Server 2003 oder Windows 2000 SP3 erstellen.

IPSec-Unterstützung von Front-End-Servern auf Back-End-Clusterserver

IPSec (Internet Protocol security) kann verwendet werden, wenn ein sicherer Kanal zwischen Front-End- und Back-End-Clusterservern erforderlich ist. Diese Konfiguration wird vollständig unterstützt, wenn sowohl auf dem Front-End- als auch auf dem Back-End-Server Exchange 2003 unter Windows Server 2003 ausgeführt wird.

IMAP4- und POP3-Ressourcen, die nicht standardmäßig hinzugefügt werden

Um erhöhte Sicherheit zu gewährleisten, werden beim Erstellen eines virtuellen Exchange-Servers die IMAP4- und POP3-Protokollressourcen nicht mehr erstellt.
Weitere Informationen zur Aktivierung von IMAP4 oder POP3 finden Sie im *Exchange Server 2003*-

Administratorhandbuch in Kapitel 8, „Verwalten von Exchange-Clustern“ (http://go.microsoft.com/fwlink/?linkid=14576).

Überprüfen der Clustering-Vorbedingungen

Um sicherzustellen, dass Ihre Cluster die aktuellen Exchange-Anforderungen erfüllen, führt Exchange 2003 mehr Vorbedingungsprüfungen für Cluster als vorherige Versionen von Exchange durch. Exchange 2003 führt beispielsweise mehr Vorinstallationsprüfungen auf den Knoten Ihres Clusters durch, um sicherzustellen, dass Exchange ordnungsgemäß auf Ihren Clusterknoten installiert ist. Parallel dazu führt Exchange 2003 beim Erstellen und Entfernen von virtuellen Exchange-Servern mehr Prüfungen auf Ihrem Cluster durch, um sicherzustellen, dass Ihre virtuellen Exchange-Server ordnungsgemäß konfiguriert sind.

Informationen zum Verständnis von Exchange 2003-Clustering

Mithilfe des Clusteringfeatures unter Windows können Sie für Serveranwendungen, wie z. B. Exchange, Skalierbarkeit und hohe Verfügbarkeit erreichen. Ein Cluster besteht aus einzelnen Computern (auch als Knoten bezeichnet), die in einem Clusterdienst zusammenhängend funktionieren. Diese Computer fungieren als Netzwerkdienstanbieter oder als Reservecomputer, die beim Auftreten von Problemen Serveroperationen für andere Knoten übernehmen. Clustering bietet Fehlertoleranz und Zuverlässlichkeit. Abhängig von der Konfiguration Ihres Clusters kann durch Clustering außerdem die Wiederherstellung verlorener Daten einzelner Server vereinfacht werden.

In einer Clusterumgebung wird Exchange als virtueller Server ausgeführt (nicht als eigenständiger Server), da jeder Knoten eines Clusters die Führung über einen virtuelle Server übernehmen kann. Wenn bei dem Knoten, auf dem der virtuelle Exchange-Server ausgeführt wird, Probleme auftreten, wird der virtuelle Exchange-Server für kurze Zeit offline geschaltet, bis ein anderer Knoten die Steuerung über den beschädigten Knoten übernommen hat.

Sie können für Ihre Exchange-Cluster entweder eine Aktiv-/Passiv- oder eine Aktiv-/Aktiv-Konfiguration verwenden, wobei die Aktiv/Passiv-Konfiguration empfohlen wird.

In diesem Abschnitt werden die folgenden Aspekte von Exchange 2003-Clustering besprochen:

- Windows-Clustering
- Virtuelle Exchange-Server
- Quorumdatenträger-Ressource
- Clusterkonfigurationen
- Erforderliche Versionen von Windows und Exchange
- Beispiel für eine Clustertopologie mit zwei Knoten
- Informationen zum Verständnis von Failovers
- IP-Adressen und Netzwerknamen

Windows-Clustering

Zum Erstellen von Exchange 2003-Clustern müssen Sie Windows-Clustering verwenden. Windows-Clustering ist ein Feature der Windows Server 2003 Enterprise Edition und der Windows Server 2003 Datacenter Edition. Der Windows-Clusterdienst ist die wesentliche Softwarekomponente, die alle Aspekte von Windows-Clustering steuert. Wird Exchange 2003 Setup auf einem

Knoten eines Windows Server 2003-Clusters ausgeführt, wird die Cluster-gestützte Version von Exchange automatisch installiert. Exchange 2003 verwendet folgende Windows-Clustering-Features:

- **Shared-Nothing-Architektur** Obwohl andere Windows-Anwendungen über die Option zur Verwendung einer Architektur mit freigegebenen Laufwerken oder einer Shared-Nothing-Architektur verfügen, erfordern Exchange 2003-Back-End-Cluster die Verwendung einer Shared-Nothing-Architektur. In einer Shared-Nothing-Architektur können zwar alle Knoten des Clusters auf freigegebene Daten zugreifen, dies kann jedoch nicht gleichzeitig geschehen. Wenn z. B. in einem Cluster mit zwei Knoten eine physische Datenträgerressource Knoten 1 zugewiesen ist, kann Knoten 2 erst auf die Datenträgerressource zugreifen, wenn Knoten 1 offline geschaltet wird, ausfällt, oder wenn die Datenträgerressource manuell nach Knoten 2 verschoben wird.
- **Ressourcen-DLL** Windows kommuniziert mit Ressourcen in einem Cluster mithilfe einer Ressourcen-DLL. Exchange 2003 bietet zum Kommunizieren mit dem Clusterdienst eine eigene benutzerdefinierte Ressourcen-DLL (genannt **Exres.dll**) an. Die Kommunikation zwischen dem Clusterdienst und Exchange 2003 ist so angepasst, dass alle Windows-Clusteringfunktionen zur Verfügung stehen.
- **Gruppen** Exchange 2003 verwendet Windows-Clustergruppen, um virtuelle Exchange-Server in einem Cluster zusammenzufassen. Ein virtueller Exchange-Server in einem Cluster ist eine Windows-Clustergruppe mit Clusterressourcen, wie z. B. einer IP-Adresse und der Exchange 2003-Systemaufsicht.
- **Ressourcen** Virtuelle Exchange-Server beinhalten Windows-Clusterdienstressourcen, wie z. B. IP-Adressressourcen, Netzwerknamenressourcen und physische Datenträgerressourcen. Virtuelle Exchange-Server beinhalten außerdem ihre eigenen Exchange-spezifischen Ressourcen. Nach dem Hinzufügen der Systemaufsichtsinstanz-Ressource (eine Exchange-spezifische Ressource) zu einer Windows-Clustergruppe werden in Exchange automatisch die anderen wesentlichen Exchange-bezogenen Ressourcen erstellt, z. B. die Instanz des virtuellen HTTP-Servers, die Instanz des Informationsspeichers und die MS Search-Instanz.

Virtuelle Exchange-Server

Wenn Sie einen Exchange 2003-Cluster erstellen möchten, müssen Sie eine Windows Server 2003-Clustergruppe anlegen und dieser Gruppe bestimmte Ressourcen hinzufügen. Beim Einrichten von Exchange 2003-Clustern werden logische Server erstellt, die als „virtuelle Exchange-Server“ bezeichnet werden. Im Gegensatz zu einem eigenständigen (nicht geclusterten) Computer, auf dem Exchange 2003 ausgeführt wird, besteht ein virtueller Exchange-Server aus einer Clustergruppe, in der ein Failover ausgeführt werden kann, wenn der Server ausfällt, auf dem der virtuelle Exchange-Server ausgeführt wird. Wenn einer der Computer im Cluster ausfällt, übernimmt einer der verbleibenden Knoten im Cluster die Aufgaben des ausgefallenen virtuellen Exchange-Servers. Clients können dann unter demselben Exchange-Servernamen auf den neuen Server zugreifen.

Ein virtueller Exchange-Server ist eine Clustergruppe, für die mindestens die folgenden Ressourcen verfügbar sein müssen:

- eine statische IP-Adresse
- ein Netzwerkname
- eine oder mehrere freigegebene physische Laufwerke
- eine Exchange 2003 Server-Systemaufsichtsressource (Die Systemaufsichtsressource installiert andere erforderliche Exchange-Ressourcen.)

In Abbildung 6.4 werden die Ressourcen eines Exchange 2003-Clusters und die Ressourcenabhängigkeiten dargestellt.

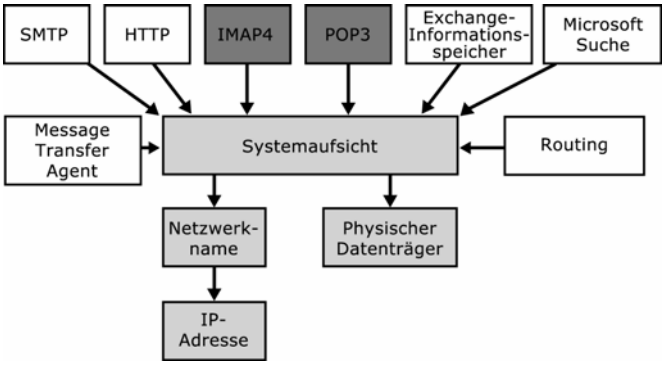


Abbildung 6.4 Exchange 2003-Ressourcen und Abhängigkeiten

Hinweis In Exchange 2003 werden die IMAP4- und POP3-Ressourcen beim Erstellen eines neuen virtuellen Exchange-Servers nicht automatisch erstellt. Weitere Informationen zu IMAP4- und POP3-Ressourcen finden Sie im *Exchange Server 2003-Administratorhandbuch* in Kapitel 8, „Verwalten von Exchange-Clustern“, (http://go.microsoft.com/fwlink/?linkid=14576).

Verbindungen von Clientcomputern zu einem virtuellen Exchange-Server werden auf dieselbe Weise hergestellt wie Verbindungen zu einem eigenständigen Computer, auf dem Exchange 2003 ausgeführt wird. Windows Server 2003 stellt die IP-Adressressource, die Netzwerknamenressource und die Datenträgerressourcen bereit, die dem virtuellen Exchange-Server zugeordnet sind. Exchange 2003 stellt die Systemaufsichtsressource und andere erforderliche Ressourcen zur Verfügung. Beim Erstellen der Systemaufsichtsressource werden alle anderen erforderlichen und abhängigen Ressourcen ebenfalls installiert.

In Tabelle 6.2 werden die Komponenten von Exchange 2003 und deren Abhängigkeiten beschrieben.

Tabelle 6.2 Beschreibung der Exchange Server 2003-Clusterressourcen und ihrer Abhängigkeiten

Komponente	Beschreibung	Abhängigkeit
Systemaufsicht	Die Systemaufsicht ist die grundlegende Ressource, über die das Erstellen und Löschen aller Ressourcen im virtuellen Exchange-Server gesteuert wird.	Netzwerknamenressource und freigegebene Datenträgerressourcen
Exchange-Informationsspeicher	Stellt Postfachspeicher und Informationsspeicher für Öffentliche Ordner für Exchange Server zur Verfügung.	Systemaufsicht
SMTP	Steuert Relay und Übertragung von E-Mails.	Systemaufsicht
IMAP4*	Optionale Komponente, die Zugriff auf E-Mail-Nachrichten für IMAP4-Clients ermöglicht.	Systemaufsicht
POP3*	Optionale Komponente, die Zugriff auf E-Mail-Nachrichten für POP3-Clients ermöglicht.	Systemaufsicht

HTTP	Ermöglicht den Zugriff auf Exchange-Postfächer und Öffentliche Ordner über HTTP (z. B. Microsoft Office Outlook® Web Access für Exchange 2003).	Systemaufsicht
Instanz von Exchange MS Search	Ermöglicht Inhaltsindizierung für den virtuellen Exchange-Server.	Systemaufsicht
Message Transfer Agent (MTA)	Pro Cluster kann nur ein MTA verwendet werden. Der MTA wird auf dem ersten virtuellen Exchange-Server erstellt. Alle weiteren virtuellen Exchange-Server hängen von diesem MTA ab. Der MTA ist für die Kommunikation mit X.400-Systemen und die Verbindung zu Exchange 5.5 verantwortlich.	Systemaufsicht
Routingdienst	Erstellt die Verbindungsstatustabellen.	Systemaufsicht

Hinweis Nur einer der virtuellen Exchange-Server in einem Cluster verfügt über eine MTA-Ressource. Alle anderen Exchange-Ressourcen sind in jedem der virtuellen Exchange-Server vorhanden.

* In Exchange 2003 werden die IMAP4- und POP3-Ressourcen beim Erstellen eines neuen virtuellen Exchange-Servers nicht automatisch erstellt. Weitere Informationen über die IMAP4- und POP3-Ressourcen finden Sie im *Exchange 2003-Administratorhandbuch* in Kapitel 8, „Verwalten von Exchange-Clustern“ (http://go.microsoft.com/fwlink/?linkid=14576).

In Exchange 2003-Clustern werden die folgenden Windows- und Exchange 2000-Komponenten nicht unterstützt:

- Active Directory Connector (ADC)
- Exchange 2003-Kalender-Connector
- Exchange Connector für Lotus Notes
- Exchange Connector für Novell GroupWise
- Microsoft Exchange-Ereignisdienst
- Standortreplikationsdienst (SRS)
- Network News Transport Protocol (NNTP)

Hinweis In Exchange 2003-Clustern wird NNTP nicht unterstützt. Der NNTP-Dienst ist eine Teilkomponente von Windows Server 2003-Internetinformationsdienste (IIS) und wird für die Installation von Exchange 2003 in einem Cluster weiterhin benötigt. Nach der Installation von Exchange 2003 in einem Cluster steht der NNTP-Dienst jedoch nicht weiter zur Verfügung.

Quorumdatenträger-Ressource

Der wichtigste Datenträger im Cluster wird als Quorumdatenträger-Ressource festgelegt. Die Quorumdatenträger-Ressource verwaltet Konfigurationsdaten in der Quorumprotokolldatei, im Clusterdatenbank-Prüfpunkt und den

Ressourcenprüfpunkten. Der Quorumdatenträger stellt außerdem permanenten physischen Speicherplatz für den Fall von Systemausfällen
zur Verfügung. Da die Clusterkonfiguration auf der Quorumdatenträger-Ressource verwaltet wird, müssen alle Knoten im Cluster in der Lage sein, mit dem Knoten zu kommunizieren, dem der Datenträger zugeordnet ist.

In Abbildung 6.5 wird eine Quorumdatenträger-Ressource in einem Cluster mit zwei Knoten dargestellt.

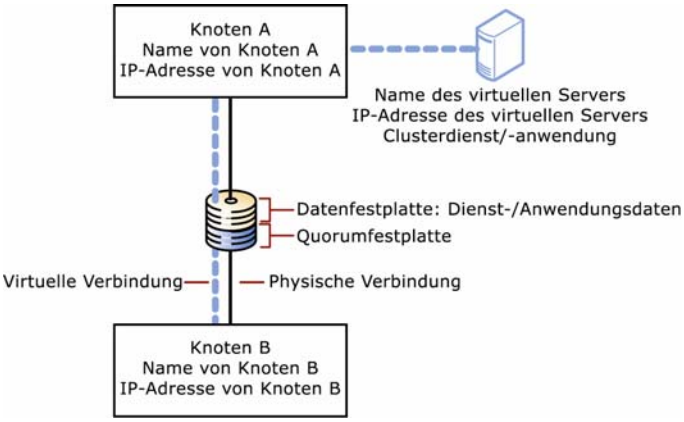


Abbildung 6.5 Quorumdatenträger-Ressource in einem Cluster mit zwei Knoten

Wenn ein Cluster erstellt wird oder die Netzwerkkommunikation zwischen den Knoten
in einem Cluster fehlschlägt, verhindert die Quorumdatenträger-Ressource, dass die Knoten mehrere Cluster bilden. Um einen Cluster zu bilden, muss ein Knoten die Besitzrechte an der Quorumdatenträger-Ressource übernehmen. Wenn ein Knoten beispielsweise während des Suchvorgangs keinen Cluster findet, versucht der Knoten, durch Übernahme der Besitzrechte an der Quorumdatenträger-Ressource einen eigenen Cluster zu bilden. Wenn die Übernahme der Besitzrechte an der Quorumdatenträger-Ressource jedoch fehlschlägt, kann der Knoten keinen Cluster bilden.

In der Quorumdatenträger-Ressource wird die aktuellste Version der Cluster-Konfigurationsdatenbank in Form von Wiederherstellungsprotokollen und Registrierungsprüfpunkt-Dateien gespeichert. Diese Dateien enthalten Clusterkonfigurations- und Statusdaten für jeden Knoten. Wenn ein Knoten
einem Cluster beitritt oder einen Cluster bildet, aktualisiert der Clusterdienst
die Kopie der Konfigurationsdatenbank für diesen Knoten. Wenn ein Knoten
einem bestehenden Cluster beitritt, ruft der Clusterdienst die Konfigurationsdaten
aus den anderen aktiven Knoten ab.

Der Clusterdienst verwendet die Wiederherstellungsprotokolle der Quorumdatenträger-Ressource, um folgende Anforderungen durchzusetzen:

- Nur eine einzelne Gruppe von aktiven, kommunizierenden Knoten kann als Cluster arbeiten.
- Ein Knoten darf nur dann einen Cluster bilden, wenn dieser Knoten die Besitzrechte an der Quorumdatenträger-Ressource erfolgreich übernimmt.
- Ein Knoten darf einem vorhandenen Cluster nur beitreten oder in diesem bleiben, wenn der betreffende Knoten mit dem Knoten kommunizieren kann, der über die Besitzrechte an der Quorumdatenträger-Ressource verfügt.

  Hinweis Legen Sie für virtuelle Exchange-Server neue Clustergruppen an. In der Clustergruppe mit der Quorumdatenträger-Ressource sollte kein virtueller Exchange-Server erstellt werden.

Clusterkonfigurationen

Beim Clustering können Sie eine Gruppe unabhängiger Server als einzelnes System verwalten. Jeder Server im Cluster verfügt über eigenen Arbeitspeicher, eigene
Prozessoren und eigene Netzwerkkarten, alle Server verwenden jedoch ein gemeinsames Speichermedium. Alle Server verfügen zudem über identische Prozessoren und über dieselbe Menge an Arbeitsspeicher. Diese Server können über ein getrenntes privates Netzwerk verbunden werden, das nur der Clusterkommunikation zwischen den Knoten dient.

> **Hinweis** Obwohl Exchange so konfiguriert werden kann, dass mehrere virtuelle Server auf einem einzelnen Knoten unterstützt werden, empfiehlt es sich, auf jedem Knoten im Cluster nur einen einzelnen virtuellen Server auszuführen.

In den folgenden Abschnitten werden verschiedene Exchange 2003-Clusterkonfigurationen erläutert. Ermitteln Sie vor dem Erstellen der Exchange
2003-Cluster, welche Verfügbarkeit für die Benutzer erforderlich ist. Anschließend können Sie die optimale Hardwarekonfiguration für den Exchange 2003-Cluster festlegen.

Sie können entweder Aktiv/Passiv- oder Aktiv/Aktiv-Exchange 2003-Cluster installieren, obwohl die Verwendung einer Aktiv/Passiv-Clusterkonfiguration empfohlen wird.

Aktiv/Passiv-Clustering

Beim Aktiv/Passiv-Clustering beinhaltet ein Cluster einen primären und einen oder mehrere sekundäre Knoten. Die sekundären Knoten befinden sich im Leerlauf, bis
ein Failover auf einem primären Knoten auftritt. Wenn der primäre Knoten in einem Aktiv/Passiv-Cluster ausfällt oder offline geschaltet wird, wird das Problem vom Clustering-Feature von Windows behoben. Der ausgefallene Knoten wird offline geschaltet, und dessen Aufgaben werden von einem sekundären Knoten übernommen. Dieser Vorgang dauert meist nur wenige Minuten. Daher stehen die Exchange-Ressourcen im Cluster nur kurze Zeit nicht für Benutzer zur Verfügung.

In Exchange wird die folgende Konfiguration als Aktiv/Passiv-Cluster definiert:

> Anzahl von virtuellen Exchange-Servern < Anzahl von Knoten im Cluster

Aktiv/Aktiv-Clustering

Beim Aktiv/Aktiv-Clustering sind beide Knoten in einer Clustergruppe aktiv. (Die Aufgaben im Cluster werden von beiden Knoten ausgeführt.) Wenn ein Knoten in einem Aktiv/Aktiv-Cluster ausfällt oder offline geschaltet wird, übernimmt der verbleibende Knoten im Cluster die Aufgaben des ausgefallenen Knotens.

> **Wichtig** Aus Gründen der Systemleistung und Skalierbarkeit wird Aktiv/Aktiv-Clustering nicht empfohlen.

In Exchange wird folgende Konfiguration als Aktiv/Aktiv-Cluster definiert:

> Anzahl von virtuellen Exchange-Servern = Anzahl von Knoten im Cluster

Clustergruppen

Beim Konfigurieren eines Exchange-Clusters müssen Sie Gruppen für die Verwaltung des Clusters und der virtuellen Exchange-Server im Cluster erstellen. Sie können jeden virtuellen Exchange-Server unabhängig konfigurieren. Beachten Sie beim Erstellen von Clustergruppen folgende Empfehlungen:

- Legen Sie beim Erstellen von Gruppen im Clusterdienst eine getrennte Gruppe für die Quorumdatenträger-Ressource an, um eine Fehlertoleranz für den Cluster zur Verfügung zu stellen.
- Weisen Sie den Clusterressourcen jeder Gruppe eigene physische Festplatten zu.
  So kann vermieden werden, dass beim Ausfall einzelner Festplatten Clusterressourcen in anderen Gruppen beeinträchtigt werden.

- Verwenden Sie getrennte physische Festplatten für die Speicherung der Transaktionsprotokolldateien und Datenbankdateien eines virtuellen Exchange-Servers. Die Verwendung getrennter Festplatten kann verhindern, dass bei
  einem Ausfall einer einzelnen Festplatte sowohl die Protokolldateien als auch
  die Datenbankdateien für den betreffenden virtuellen Exchange-Server verloren gehen. Diese Empfehlung gilt auch für eigenständige Exchange-Server.

Erforderliche Versionen von Windows und Exchange

Für das Erstellen von Exchange-Clustern sind bestimmte Versionen von Windows
und Exchange erforderlich. In Tabelle 6.3 sind die entsprechenden Anforderungen aufgeführt.

Tabelle 6.3 Erforderliche Versionen von Windows und Exchange

Windows-Version	Exchange-Version	Verfügbare Clusterknoten
Beliebiger Server der Windows 2000 Server- oder Windows Server 2003-Reihe	Exchange Server 2003 Standard Edition	Keiner
Windows 2000 Server oder Windows Server 2003 Standard Edition	Exchange Server 2003 oder Exchange Server 2003 Enterprise Edition	Keiner
Windows 2000 Advanced Server	Exchange Server 2003 Enterprise Edition	Bis zu zwei
Windows 2000 Datacenter Server	Exchange Server 2003 Enterprise Edition	Bis zu vier
Windows Server 2003 Enterprise Edition	Exchange Server 2003 Enterprise Edition	Bis zu acht
Windows Server 2003 Datacenter Edition	Exchange Server 2003 Enterprise Edition	Bis zu acht

Beispiel für eine Clustertopologie mit zwei Knoten

In Abbildung 6.6 wird ein Beispiel für eine Clustertopologie mit zwei Knoten dargestellt. Beide Clusterknoten gehören derselben Domäne an. Die Clusterknoten sind mit
dem öffentlichen Netzwerk und mit einem privaten Clusternetzwerk verbunden.
Als physische Datenträgerressource wird der freigegebene Datenträger im Cluster verwendet.

Wenn nur einer der Clusterknoten über die Besitzrechte an einem virtuellen Exchange-Server verfügt, liegt eine Aktiv/Passiv-Konfiguration vor. Wenn beide Knoten über
die Besitzrechte an einem oder mehreren virtuellen Exchange-Servern verfügen,
oder wenn einer der beiden Knoten über die Besitzrechte an zwei virtuellen Exchange-Servern verfügt, liegt eine Aktiv/Aktiv-Konfiguration vor (Abbildung 6.6).

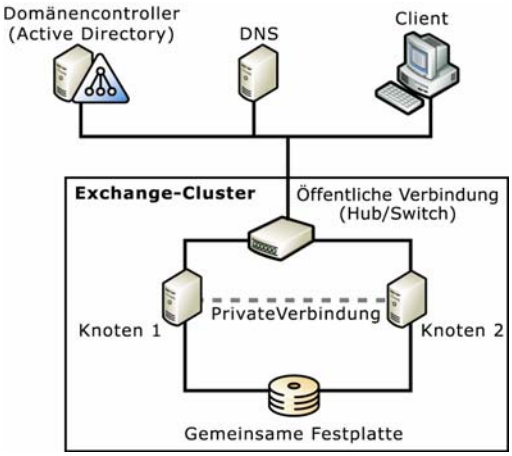


Abbildung 6.6 Beispiel für einen Exchange-Cluster mit zwei Knoten

Informationen zum Verständnis von Failovervorgängen

Die Failoverzeit ist bei virtuellen Exchange-Servern ein wichtiger Faktor. Um eine hohe Verfügbarkeit zu gewährleisten, muss die Failoverzeit kurz sein. Für Failover gibt es zwei Situationen: geplante und ungeplante Failover.

Bei einem geplanten Failover besteht folgendes Szenario:

1. Der Exchange-Administrator verschiebt mithilfe des Clusterdienstes den virtuellen Exchange-Server auf einen anderen Knoten.
2. Alle Ressourcen des virtuellen Exchange-Servers werden offline geschaltet.
3. Die Ressourcen werden auf den vom Exchange-Administrator angegebenen Knoten verschoben.
4. Alle Ressourcen des virtuellen Exchange-Servers werden online geschaltet.

Bei einem ungeplanten Failover besteht folgendes Szenario:

1. Eine oder mehrere Ressourcen des virtuellen Exchange-Servers fallen aus. Der Ausfall wird bei der nächsten Lebenszyklusprüfung (IsAlive) oder beim Ausfall einer der Ressourcen entdeckt.
2. Der Clusterdienst schaltet alle abhängigen Ressourcen automatisch offline.
3. Wenn die ausgefallene Ressource für den automatischen Neustart konfiguriert ist (Standardeinstellung), versucht der Clusterdienst, die ausgefallene Ressource und alle abhängigen Ressourcen neu zu starten.
4. Wenn die Ressource erneut ausfällt:
   - Der Clusterdienst versucht erneut, die Ressource neu zu starten.

   – oder –

   - Wenn die Ressource so konfiguriert ist, dass die Gruppe davon betroffen ist (Standardeinstellung), und innerhalb eines bestimmten Zeitraums (Standardeinstellung: 300 Sekunden) eine bestimmte Anzahl von Ausfällen

für die Ressource überschritten wurde (Standardeinstellung: 3), schaltet der Clusterdienst alle Ressourcen im virtuellen Exchange-Server offline.

5. Für alle Ressourcen wird ein Failover auf einen anderen Knoten im Cluster ausgeführt, d. h., die Ressourcen werden auf einen anderen Knoten verschoben. Wenn ein Eintrag in der Liste **Bevorzugte Besitzer** vorhanden ist, wird der betreffende Knoten für den Failovervorgang ausgewählt.
6. Der Clusterdienst versucht, alle Ressourcen des virtuellen Exchange-Servers auf dem neuen Knoten online zu schalten.
7. Wenn dieselbe oder eine andere Ressource auf dem neuen Knoten erneut ausfällt, wiederholt der Clusterdienst die vorherigen Schritte und führt bei Bedarf einen Failover auf einen weiteren Knoten aus (oder zurück auf den ursprünglichen Knoten).
8. Wenn der virtuelle Exchange-Server wiederholt ausfällt, führt der Clusterdienst innerhalb eines festgelegten Zeitraums (Standardeinstellung: 6 Stunden) nicht mehr als eine maximale Anzahl von Failovervorgängen für den virtuellen Exchange-Server durch (Standardeinstellung: 10). Danach bleibt der virtuelle Exchange-Server in einem ausgefallenen Zustand.
9. Wenn Failback konfiguriert wurde (in der Standardeinstellung deaktiviert), verschiebt der Clusterdienst den virtuellen Exchange-Server zurück auf den ursprünglichen Knoten, wenn dieser wieder verfügbar ist. Dies geschieht abhängig von der Gruppenkonfiguration entweder sofort oder zu einer bestimmten Tageszeit.

IP-Adressen und Netzwerknamen

Meist beinhaltet ein Cluster ein öffentliches Netzwerk, das Clientcomputer für die Verbindung zu virtuellen Exchange-Servern verwenden, und ein privates Netzwerk für die Kommunikation zwischen Clusterknoten. Beim Erstellen der virtuellen Exchange-Server müssen Sie über eine ausreichende Anzahl von statischen IP-Adressen verfügen. Wenn *n* die Anzahl von Clusterknoten und *e* die Anzahl virtueller Exchange-Server darstellt, verfügt ein Cluster mindestens über 2**n* + *e* + 1 IP-Adressen und *n* + *e* + 1 NetBIOS-Namen:

- Jeder Knoten des Clusters verfügt über zwei statische IP-Adressen (die öffentliche und die private Netzwerk-IP-Adresse jedes Knotens) und über einen NetBIOS-Namen.
- Der Cluster selbst verfügt über eine statische IP-Adresse und einen NetBIOS-Namen.
- Jeder virtuelle Exchange-Server verfügt über eine statische IP-Adresse und einen NetBIOS-Namen.

Es wird jedoch dringend empfohlen, dass von einem Cluster mit <*n*> Knoten und <*e*> virtuellen Exchange-Servern 2**n* + *e* + 2 IP-Adressen verwendet werden. Der Summand **+2** in dieser Gleichung repräsentiert die beiden zusätzlichen IP-Adressen, durch die die beiden Ressourcen Quorumdatenträger und Microsoft Distributed Transaction Coordinator (MSDTC) in ihren jeweiligen Gruppen gespeichert werden können. (Hierbei handelt es sich um eine Empfehlung für Windows Server 2003.) Daher ist die empfohlene Anzahl statischer IP-Adressen für einen Cluster mit zwei Knoten sechs, zuzüglich der Anzahl virtueller Exchange-Server. Bei einem Cluster mit vier Knoten sollten zehn statische Adressen zuzüglich der Anzahl der virtuellen Exchange-Server zur Verfügung stehen.

Wichtig Es wird ausdrücklich empfohlen, dass Sie beim Bereitstellen von Clustern statische IP-Adressen und ein privates Netzwerk für die Clusterkommunikation verwenden. Wenn Sie DHCP (Dynamic Host Configuration-Protokoll) verwenden, können Clientcomputer keine Verbindung zum Cluster herstellen, und der gesamte Cluster kann ausfallen, wenn der DHCP-Server die IP-Lease nicht erfolgreich erneuert. Es wird ausdrücklich empfohlen, ein privates Netzwerk für die Clusterkommunikation zu verwenden. Andernfalls wird bei einem Ausfall der öffentlichen Netzwerkverbindung auf einem Knoten die Kommunikation der Clusterknoten untereinander unterbrochen, so dass der Failover für die betroffenen Ressourcen verhindert wird. Dies kann zum Ausfall des gesamten Clusters führen.

Eine übliche und zuverlässige Konfiguration für einen Exchange Server-Cluster mit vier Knoten besteht in einer Struktur, in der drei aktive und ein passiver Knoten vorhanden sind. Bei dieser Struktur wird versucht,

die Prozessor-, Datenträger-, Speicher- und Netzwerkauslastung des Computers gleichmäßig zu verteilen, so dass bei keiner Komponente vorzeitig ein Engpass auftritt.

In Abbildung 6.7 wird der in diesem Abschnitt beschriebene Exchange-Cluster mit vier Knoten dargestellt.

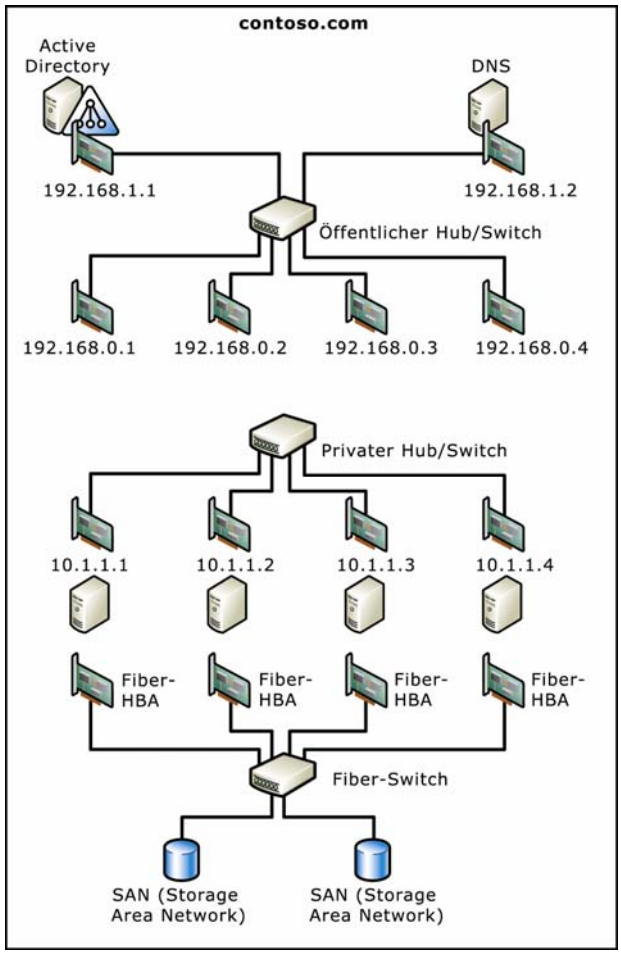


Abbildung 6.7 Beispiel für einen Exchange-Cluster mit vier Knoten

Aspekte beim Planen von Clustern

Folgende Aspekte sollten Sie beim Planen von Exchange 2003-Clustern beachten. Diese Informationen betreffen Exchange 2003-Cluster unter Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows Server 2003 Enterprise Edition und Windows Server 2003 Datacenter Edition.

Beachten Sie beim Planen von Exchange-Clustern folgende Aspekte:

- Einrichten dedizierter Computer für Exchange
- Getrennte Festplatten für Protokolldateien

- Speichergruppenbeschränkungen
- Laufwerkbuchstabenbeschränkungen

In den folgenden Abschnitten werden dieses Aspekte genauer erläutert.

Einrichten dedizierter Computer für Exchange

Neben Exchange 2003 können in einem Servercluster weitere Anwendungen ausgeführt werden. Die Leistung von virtuellen Exchange-Servern wird jedoch beim Ausführen mehrerer Anwendungen auf einem Knoten beeinträchtigt. Beachten Sie Folgendes
bei der Entscheidung, ob dedizierte Computer für Exchange eingerichtet werden sollen:

- Wenn Sie mehrere Anwendungen in einem Cluster ausführen, empfiehlt es sich, für jede Anwendung einen Knoten zu reservieren und sicherzustellen, dass genügend passive Knoten verfügbar sind.
- Wenn Sie mithilfe von Clustern Exchange-Dienste für Benutzer bereitstellen, empfiehlt es sich, nur Exchange 2003 in dem Cluster auszuführen und andere Anwendungen auf getrennter Hardware auszuführen.
- Optimale Ergebnisse werden erzielt, wenn Failovervorgänge für virtuelle Exchange-Server nicht auf Knoten erfolgen, auf denen andere Anwendungen ausgeführt werden.
- Die Clusterknoten eines Exchange 2003-Clusters müssen Mitgliedsserver einer Domäne sein. Bei Exchange 2003-Clustern wird die Verwendung von Clusterknoten als Domänencontroller oder globale Katalogserver nicht unterstützt.

Weitere Informationen über die Leistung von Exchange 2003-Clustern finden Sie im *Exchange Server 2003-Administratorhandbuch* in Kapitel 8, „Verwalten von Exchange-Clustern“ (http://go.microsoft.com/fwlink/?linkid=14576).

Getrennte Festplatten für Protokolldateien

Wenn die Speichergruppen für einen virtuellen Exchange-Server so konfiguriert sind, dass sich die Protokolldateien und die Datenbanken auf getrennten Gruppen von physischen Laufwerken befinden, müssen alle Laufwerke als Datenträgerressourcen in demselben virtuellen Exchange-Server konfiguriert werden. Dabei müssen sich alle Daten auf einem freigegebenen Datenträger befinden, und alle physischen Datenträgerressourcen müssen Teil der Exchange-Clustergruppe sein. In diesem Fall kann für die Protokolldateien und
die Datenbanken der Speichergruppe ein Failover auf einen anderen Knoten ausgeführt werden, wenn der virtuelle Exchange-Server offline geschaltet wird.

> **Hinweis** Die Systemaufsichtressource sollte als von allen Datenträgerressourcen, die Exchange-Daten enthalten, abhängig konfiguriert werden.

Speichergruppenbeschränkungen

Exchange 2003 ist auf vier Speichergruppen pro Server beschränkt. Dies ist eine physische Beschränkung, die ebenfalls für jeden Knoten eines Clusters gilt. Diese Beschränkung kann bei Aktiv/Aktiv-Konfigurationen problematisch sein. Aktiv/Passiv-Konfigurationen werden jedoch nicht beeinträchtigt. In Tabelle 6.4 wird diese Beschränkung dargestellt.

Tabelle 6.4 Eine Aktiv/Aktiv-Exchange 2003-Clusterkonfiguration mit zwei Knoten und zu vielen Speichergruppen

Virtueller Exchange-Server	Status	Speichergruppennamen
Knoten 1 EVS1	Aktiv	Speichergruppe 1, Speichergruppe 2, Speichergruppe 3
Knoten 2 VES2	Aktiv	Speichergruppe 1, Speichergruppe 2

In Tabelle 6.4 enthält der Exchange-Cluster fünf Speichergruppen. Wenn VES2 auf Knoten 2 einen Failover auf Knoten 1 ausführt, kann Knoten 1 keine Verbindung zu einer der Speichergruppen von Knoten 2 herstellen, da bei Knoten 1 die Grenze von vier Speichergruppen für einzelne Clusterknoten überschritten ist. Daher wird VES2
auf Knoten 1 nicht online geschaltet. Wenn Knoten 2 noch verfügbar ist, führt VES2 einen Failover zurück auf Knoten 2 aus.

> **Hinweis** In Exchange 2003 wird eine fünfte Speichergruppe für Sicherungen
> und Wiederherstellungen unterstützt. Sie können die fünfte Speichergruppe jedoch nicht zum Erstellen neuer Benutzerpostfächer verwenden.

Laufwerkbuchstabenbeschränkungen

Bei Exchange 2003-Clustern mit vier oder mehr Knoten besteht eine weitere Einschränkung, die Sie vor dem Einrichten des Clusters berücksichtigen müssen. Unter Windows können
pro Server nur 24 Laufwerkbuchstaben vergeben werden. Wenn Sie planen, den Hauptteil der Datenträger auf dem Server als freigegebene Clusterressourcen zu verwenden, gilt die Beschränkung auf 24 Laufwerkbuchstaben nicht nur für jeden einzelnen Knoten, sondern auch für den gesamten Cluster. Unabhängig von der Anzahl von Knoten im Cluster können nur 23 freigegebene Datenträger verwendet werden. (Der Grund dafür, dass die maximale Anzahl von freigegebenen Datenträgern 23 und nicht 24 ist, besteht darin, dass ein Datenträger pro Knoten für den Systemdatenträger reserviert werden muss.)

Es empfiehlt sich, einen Laufwerkbuchstaben für die Datenbanken und einen Laufwerkbuchstaben für die Protokolldateien jeder Speichergruppe zu verwenden.
In einem Cluster mit vier Knoten und drei virtuellen Exchange-Servern können
bis zu 12 Speichergruppen verwendet werden. Daher sind unter Umständen mehr
als 24 Laufwerkbuchstaben in einem Cluster mit vier Knoten erforderlich.

In den folgenden Abschnitten erhalten Sie weitere Informationen zum Planen einer Cluster-Speicherlösung, abhängig davon, ob Sie Windows 2000 oder Windows Server 2003 als Betriebssystem verwenden.

Laufwerksbeschränkungen unter Windows 2000

Bei bestimmten Clusterkonfigurationen mit vier Knoten, auf denen Windows 2000 Datacenter Server ausgeführt wird, müssen Sie unter Umständen
ein oder mehrere Laufwerke deaktivieren, um weitere freigegebene Datenträger im Cluster verwenden zu können. So kann es beispielsweise sinnvoll sein, die CD-ROM- oder DVD-ROM-Laufwerke auf den Servern zu deaktivieren. Beachten Sie, dass beim Maximieren der Anzahl von freigegebenen Datenträgern ggf. die Anzahl der möglichen Netzwerkfreigaben reduziert wird.

> **Hinweis** Da beim Windows-Clustering die Verwendung von Datenträger-Bereitstellungspunkten (eine Art logisches Laufwerk) nicht unterstützt wird, können Sie unter Windows 2000 keine Datenträger-Bereitstellungspunkte für freigegebene Exchange-Datenträger verwenden. Datenträger-Bereitstellungspunkte können jedoch für lokale Laufwerke, z. B. CD-ROM- oder DVD-Laufwerke verwendet werden.

Diese Beschränkung bei den Laufwerkbuchstaben muss beim Entwerfen der Speichergruppen- und Datenbankarchitektur für einen Exchange-Cluster unter Windows 2000 Datacenter Server beachtet werden.

Datenträgerkonfiguration mit drei Speichergruppen

In Tabelle 6.5 werden einige Beispielkonfigurationen und mögliche Laufwerksbeschränkungen aufgeführt.

Die in Tabelle 6.5 beschriebene Anordnung ist sehr zuverlässig. Jede Speichergruppe (Speichergruppe 1, Speichergruppe 2 und Speichergruppe 3) verfügt über ein dediziertes Laufwerk für die Datenbanken und ein dediziertes Laufwerk für die Protokolldateien. Für das SMTP-Warteschlangenverzeichnis des virtuellen Exchange-Servers wird ein weiterer Datenträger verwendet. Bei dieser Struktur können Sie jedoch nicht mehr als drei Speichergruppen pro virtuellem Exchange-Server verwenden.

Tabelle 6.5 Eine Architektur mit drei aktiven und einem passiven Knoten und drei virtuellen Exchange-Servern mit jeweils drei Speichergruppen

Knoten 1 (VES1, aktiv)	Knoten 2 (VES2, aktiv)	Knoten 3 (VES3, aktiv)	Knoten 4 (passiv)
Datenträger 1: SMTP/MTA	Datenträger 8: SMTP	Datenträger 15: SMTP	Datenträger 22: Quorum
Datenträger 2: Datenbanken von Speichergruppe 1	Datenträger 9: Datenbanken von Speichergruppe 1	Datenträger 16: Datenbanken von Speichergruppe 1	Datenträger 23: MSDTC
Datenträger 3: Protokolle von Speichergruppe 1	Datenträger 10: Protokolle von Speichergruppe 1	Datenträger 17: Protokolle von Speichergruppe 1	
Datenträger 4: Datenbanken von Speichergruppe 2	Datenträger 11: Datenbanken von Speichergruppe 2	Datenträger 18: Datenbanken von Speichergruppe 2	
Datenträger 5: Protokolle von Speichergruppe 2	Datenträger 12: Protokolle von Speichergruppe 2	Datenträger 19: Protokolle von Speichergruppe 2	
Datenträger 6: Datenbanken von Speichergruppe 3	Datenträger 13: Datenbanken von Speichergruppe 3	Datenträger 20: Datenbanken von Speichergruppe 3	
Datenträger 7: Protokolle von Speichergruppe 3	Datenträger 14: Protokolle von Speichergruppe 3	Datenträger 21: Protokolle von Speichergruppe 3	

Festplattenkonfiguration mit vier Speichergruppen

Mit dem in Tabelle 6.6 angegebenen Entwurf wird eine weitere Speichergruppe hinzugefügt. Damit die Beschränkung auf 23 Datenträger eingehalten wird, werden jedoch die Datenbanken jeder der vier Speichergruppen (Speichergruppe 1, Speichergruppe 2, Speichergruppe 3 und Speichergruppe 4) pro virtuellem Exchange-Server auf jeweils zwei Datenträgern kombiniert. Die Datenbankdateien (EDB und STM) von Speichergruppe 1 und Speichergruppe 2 werden auf einem gemeinsamen Volume gespeichert, und die Datenbankdateien von Speichergruppe 3 und Speichergruppe 4 werden ebenfalls auf einem gemeinsamen Volume gespeichert. Der Vorteil dieses Entwurfs besteht darin, dass alle vier Speichergruppen in einem Cluster mit vier Knoten verwendet werden können. Der Entwurf hat den Nachteil, dass die Volumes für die Speichergruppen-Datenbanken möglicherweise

sehr groß sein müssen. Wenn der Datenträger einer Datenbank einen Fehler aufweist, sind außerdem zwei Speichergruppen betroffen und nicht nur eine.

Tabelle 6.6 Eine Architektur mit drei aktiven und einem passiven Knoten und drei virtuellen Exchange-Servern (VES) mit jeweils vier Speichergruppen

Knoten 1 (VES1, aktiv)	Knoten 2 (VES2, aktiv)	Knoten 3 (VES3, aktiv)	Knoten 4 (passiv)
Datenträger 1: SMTP/MTA	Datenträger 8: SMTP	Datenträger 15: SMTP	Datenträger 22: Quorum
Datenträger 2: Datenbanken von Speichergruppe 1 und Speichergruppe 2	Datenträger 9: Datenbanken von Speichergruppe 1 und Speichergruppe 2	Datenträger 16: Datenbanken von Speichergruppe 1 und Speichergruppe 2	Datenträger 23: MSDTC
Datenträger 3: Protokolle von Speichergruppe 1	Datenträger 10: Protokolle von Speichergruppe 1	Datenträger 17: Protokolle von Speichergruppe 1	
Datenträger 4: Protokolle von Speichergruppe 1	Datenträger 11: Protokolle von Speichergruppe 2	Datenträger 18: Protokolle von Speichergruppe 2	
Datenträger 5: Datenbanken von Speichergruppe 3 und Speichergruppe 4	Datenträger 12: Datenbanken von Speichergruppe 3 und Speichergruppe 4	Datenträger 19: Datenbanken von Speichergruppe 3 und Speichergruppe 4	
Datenträger 6: Protokolle von Speichergruppe 3	Datenträger 13: Protokolle von Speichergruppe 3	Datenträger 20: Protokolle von Speichergruppe 3	
Datenträger 7: Protokolle von Speichergruppe 4	Datenträger 14: Protokolle von Speichergruppe 4	Datenträger 21: Protokolle von Speichergruppe 4	

Windows Server 2003-Datenträger-Bereitstellungspunkte

Datenträger-Bereitstellungspunkte werden jetzt für freigegebene Festplatten unterstützt, wenn auf den Knoten Ihres Clusters Windows Server 2003 Enterprise Edition oder Datacenter Edition mit mindestens vier Knoten ausgeführt
wird. Datenträger-Bereitstellungspunkte (auch als NTFS-Abzweigungspunkte oder bereitgestellte Laufwerke bezeichnet) sind Verzeichnisse, die permanent auf bestimmte Festplattenlaufwerke verweisen. (Beispielsweise können Sie **C:\Data** so konfigurieren, dass dieses Verzeichnis auf ein Festplattenlaufwerk verweist.) Durch Datenträger-Bereitstellungspunkte müssen Sie nicht jedem Festplattenlaufwerk einen Laufwerkbuchstaben zuweisen. Auf diese Weise kann die Beschränkung auf 26 Laufwerkbuchstaben umgangen werden.

Weitere Informationen zu Datenträger-Bereitstellungspunkten und deren Erstellung finden Sie in der Windows Server 2003-Dokumentation.

Beachten Sie beim Installieren von Datenträger-Bereitstellungspunkten in Clustern Folgendes:

- Achten Sie darauf, eindeutige Datenträger-Bereitstellungspunkte zu erstellen, so dass keine Konflikte mit vorhandenen lokalen Laufwerken an einem beliebigen Knoten im Cluster auftreten.

- Erstellen Sie keine Datenträger-Bereitstellungspunkte mit Verweisen zwischen Festplatten auf dem Clusterspeichergerät (Clusterfestplatten) und den lokalen Festplatten.
- Erstellen Sie keine Datenträger-Bereitstellungspunkte von der Clusterfestplatte, auf der die Quorumdatenträger-Ressource enthalten ist. Sie können jedoch einen Datenträger-Bereitstellungspunkt von der Quorumdatenträger-Ressource zu einer Clusterfestplatte erstellen.
- Datenträger-Bereitstellungspunkte von einer Clusterfestplatte zu einer anderen müssen sich in derselben Clusterressourcengruppe befinden und vom Stammdatenträger abhängig sein.

Es wird empfohlen, bei Exchange 2003-Clustern mit mindestens vier Knoten Datenträger-Bereitstellungspunkte zu verwenden. Pro Speichergruppe sollte ein Stammdatenträger verwendet werden. Die Protokolle können auf dem Stammdatenträger und die Datenbank auf dem bereitgestellten Laufwerk gespeichert werden. Wenn nicht mehr genügend Laufwerkbuchstaben zur Verfügung stehen (z. B. in einem Cluster mit 8 Knoten), können Sie einen einzelnen Stammdatenträger verwenden. Um das Risiko von Datenverlusten zu minimieren, sollten Sie in diesem Fall jedoch keine Daten auf dem Stammdatenträger speichern. Sie benötigen für jeden virtuellen Exchange-Server einen Stammdatenträger.

Weitere Informationen über das Hinzufügen eines Datenträger-Bereitstellungspunkts zu einem virtuellen Exchange-Server finden Sie im *Bereitstellungshandbuch für Exchange Server 2003* in Kapitel 6, „Bereitstellen von Exchange 2003 in einem Cluster“ (http://go.microsoft.com/fwlink/?linkid=14576).

Cluster-Hardwarekompatibilitätsliste

Unter Windows Server 2003 Enterprise Edition und Windows Server 2003 Datacenter Edition unterstützt Microsoft nur vollständige Serverclustersysteme, die im Windows Server-Katalog (http://go.microsoft.com/fwlink/?LinkId=17219) ausgewählt wurden. Wenn Sie herausfinden möchten, ob Ihr System oder Ihre Hardwarekomponenten einschließlich der Clusterfestplatten kompatibel sind, durchsuchen Sie die Hardware in diesem Katalog. Bei einem geografisch verteilten Cluster müssen sowohl die Hardware- als auch die Softwarekonfiguration zertifiziert und im Windows Server-Katalog aufgeführt sein.

Die in zertifizierten Clusterkonfigurationen verwendeten Netzwerkschnittstellenkarten (NICs) müssen ebenfalls im Windows-Katalog ausgewählt werden.

Es wird empfohlen, eine Clusterkonfiguration aufzustellen, die in allen Clusterknoten identische Speicherhardware enthält. Dadurch wird die Konfiguration vereinfacht, und mögliche Kompatibilitätsprobleme werden vermieden.

Aspekte der Skalierbarkeit

Die Festlegung der Größe und Skalierbarkeit Ihrer Cluster hängt davon ab, wie Sie die Servercluster implementieren möchten. In diesem Abschnitt werden die folgenden Aspekte der Clustergröße behandelt:

- Festlegen der Größe von Aktiv/Passiv-Clustern
- Festlegen der Größe von Aktiv/Aktiv-Clustern
- Zu testende Serverkomponenten
- Kapazitätsplanungstools

Festlegen der Größe von Aktiv/Passiv-Clustern

Aktiv/Passiv-Cluster sind die empfohlene Konfiguration für Exchange-Servercluster. Windows 2000 Advanced Server unterstützt Aktiv/Passiv-Cluster mit zwei Knoten,

und Windows 2000 Datacenter Server unterstützt Aktiv/Passiv-Cluster mit zwei, drei oder vier Knoten.

Exchange 2003 unterstützt Cluster mit bis zu acht Knoten. Exchange-Cluster mit acht Knoten werden nur bei der Verwendung mit Windows Server 2003 Enterprise Edition oder Windows Server 2003 Datacenter Edition unterstützt. Als weitere Bedingung für die Einrichtung eines Clusters mit acht Knoten muss mindestens ein passiver Knoten vorhanden sein.

Sie können die Größe für Aktiv/Passiv-Cluster mit der Kapazitätsplanung und dem Topologierechner ermitteln. Dies unterschiedet sich nicht von der Herangehensweise bei Einzelserver-Bereitstellungen.

> **Hinweis** Es wird dringend empfohlen, die ermittelten Größen vor der Bereitstellung unter Laborbedingungen mit dem Microsoft Exchange Server Load Simulation-Tool (**LoadSim.exe**) zu testen. Weitere Informationen über LoadSim finden Sie weiter unten in diesem Kapitel unter „Microsoft Exchange Server Load Simulation-Tool“.

Festlegen der Größe von Aktiv/Aktiv-Clustern

Aktiv/Aktiv-Cluster werden als Konfiguration für Exchange-Servercluster nicht empfohlen. Exchange unterstützt nur Aktiv/Aktiv-Cluster mit zwei Knoten.

Wenn Sie Ihre Aktiv/Aktiv-Cluster mit der Kapazitätsplanung und dem Topologierechner planen, gelten zwei wichtige Einschränkungen:

- Stellen Sie sicher, dass die Anzahl der gleichzeitig vorliegenden Benutzerverbindungen pro Knoten 1.900 nicht überschreitet. Wenn mehr als ein virtueller Exchange-Server pro Knoten vorhanden ist, stellen Sie sicher, dass die Summe aller gleichzeitig vorliegenden Benutzerverbindungen 1.900 nicht überschreitet.
- Stellen Sie sicher, dass die durchschnittliche Prozessorauslastung pro Server 40 % nicht überschreitet.

> **Hinweis** Vor der Bereitstellung müssen Sie die ermittelten Größen mit LoadSim unter Laborbedingungen testen. Weitere Informationen über LoadSim finden Sie weiter unten in diesem Kapitel unter „Microsoft Exchange Server Load Simulation-Tool“.

Nach der Bereitstellung des Clusters müssen Sie die folgenden Aufgaben durchführen:

- Überwachen Sie die Anzahl der gleichzeitigen Verbindungen (Benutzer) pro Knoten. Wenn die Anzahl der gleichzeitigen Benutzer pro Knoten für mehr als 10 Minuten den Wert 1.900 übersteigt, entfernen Sie Benutzer von diesem Knoten.
- Überwachen Sie die Prozessorauslastung jedes Servers im Cluster. Wenn die Prozessorauslastung (durch Benutzer entstandene Last) für mehr als 10 Minuten 40 % übersteigt, entfernen Sie Benutzer von diesem Knoten. In diesem Wert sind Auslastungserhöhungen durch Verwaltungsaufgaben, z. B. das Verschieben von Benutzern, nicht enthalten.

Zu testende Serverkomponenten

Bevor Sie Cluster in Ihrer Organisation verfügbar machen, müssen Sie unbedingt ihre Kapazität testen.

In der folgenden Liste werden einige Hardwarekomponenten aufgeführt, die getestet werden müssen:

- Einzelne Computerkomponenten wie Festplatten und Controller, Prozessoren und Arbeitsspeicher (RAM)
- Externe Komponenten wie Router, Bridges, Switches, Kabel und Anschlüsse

Im Folgenden sind einige der Belastungstests angegeben, die Sie einrichten müssen:

- Test der Clusterleistung unter starker Netzwerkauslastung
- Test der Clusterleistung bei häufigen Ein-/Ausgaben (E/A) auf derselben Festplatte
- Test der Clusterleistung bei hoher Auslastung der Exchange-Dienste
- Test der Clusterleistung bei einer großen Anzahl gleichzeitiger Anmeldeversuche
- Durchführung eines Failover aller virtuellen Exchange-Server auf alle Knoten (mindestens jeweils einmal)

Kapazitätsplanungstools

Ermitteln Sie mit den folgenden Tools die Größe und Skalierbarkeit der Server.

Kapazitätsplanung und Topologierechner

Mit der Kapazitätsplanung und dem Topologierechner können Sie die erforderliche Servergröße für Exchange 2000- oder Exchange 2003-Servercluster bestimmen. Die Kapazitätsplanung und der Topologierechner sind auf der Microsoft Exchange-Website unter http://go.microsoft.com/fwlink/?LinkId=1716 erhältlich.

Microsoft Exchange Server Load Simulation-Tool

Mit Microsoft Exchange-LoadSim können Sie die Auslastung von MAPI-Clients für Exchange ermitteln. Sie simulieren die Auslastung, indem Sie LoadSim-Tests auf Clientcomputern ausführen. In diesen Tests werden Messaginganforderungen an den Exchange-Server gesendet, und somit Last erzeugt.

Mit den Ergebnissen dieser Tests können Sie folgende Aktionen durchführen:

- Berechnen der Clientantwortzeit für die Serverkonfiguration unter Clientlast
- Abschätzen der Anzahl von Benutzern pro Server
- Erkennen von Engpässen auf dem Server

Weitere Informationen zu LoadSim sowie Downloadmöglichkeiten für LoadSim finden Sie im *Microsoft Exchange 2000 Server Resource Kit* (http://go.microsoft.com/fwlink/?LinkId=1710) unter „Load Simulator“.

Exchange Stress and Performance-Tool

Das Exchange Stress and Performance (ESP)-Tool ist ein hoch skalierbares Belastungs- und Leistungstool für Exchange. Es simuliert eine große Anzahl von Clientsitzungen durch gleichzeitiges Zugreifen auf einen oder mehrere Protokolldienste. Die Aktionen jedes simulierten Clients werden durch Skripts gesteuert. Die Skripts enthalten die Algorithmen für die Kommunikation mit dem Server. Die Skripts werden von Testmodulen (DLLs) ausgeführt. Die Testmodule stellen Serververbindungen über die jeweilige IP, Aufrufe der API-Funktionen (Application Programming Interfaces) oder über Schnittstellen wie OLE DB her.

ESP ist modular und erweiterbar und bietet derzeit Module für die meisten Internetprotokolle, einschließlich der folgenden:

- WebDAV (Web Distributed Authoring and Versioning)
- IMAP4
- LDAP
- OLE DB

- POP3
- SMTP

Weitere Informationen zum ESP-Tool sowie eine Downloadmöglichkeit für ESP finden Sie auf der Microsoft Exchange-Website unter http://go.microsoft.com/fwlink/?LinkId=1709.

Volumeschattenkopie-Dienst und Cluster

Das Bereitstellen einer Schattenkopie auf einem Einzelserver weist Unterschiede zum Bereitstellen einer Schattenkopie in einem Cluster auf. Auf einem Einzelserver können Sie eine Schattenkopie erstellen und diese auf demselben Computer importieren. In einem Cluster tritt jedoch beim Erstellen einer Schattenkopie und dem anschließenden Versuch, diese auf einem Computer im selben Cluster zu importieren, ein Konflikt der Datenträgersignatur auf.

Diese Situation wird im folgenden Beispiel veranschaulicht.

Ein Einzelcomputer weist die Datenträgersignatur 1234 auf. Sie erstellen eine Schattenkopie, durch die eine LUN (Logical Unit Number) 9 mit der Datenträgersignatur 1234 erstellt wird, die mit der ursprünglichen Signatur identisch ist. Sie können LUN 9 auf einem anderen Server importieren, da dort kein Konflikt mit der Datenträgersignatur vorliegt. Sie können LUN 9 auch auf demselben Server importieren, denn die Datenträgersignatur wird dabei automatisch in eine andere Zahl umgewandelt, z. B. 9999.

Angenommen, ein Server mit der Datenträgersignatur 1234 wird in einem Cluster bereitgestellt. Sie erstellen eine Schattenkopie, durch die LUN 9 mit der Datenträgersignatur 1234 erstellt wird. Sie können LUN 9 auf einem Server in einem anderen Cluster importieren, da dort kein Konflikt mit der Datenträgersignatur vorliegt. Sie können LUN 9 jedoch nicht auf einem anderen Server im selben Cluster importieren, da die Datenträgersignatur weiterhin den Wert 1234 aufweist und dadurch ein Konflikt innerhalb des Clusters ausgelöst wird. Sie können diesen Konflikt z. B. dadurch vermeiden, dass Sie die Schattenkopie in einem SAN (Storage Area Network) oder auf einem Server in einem getrennten Cluster aufbewahren und von dort auf sie zugreifen.

Exchange-Datenspeicherlösungen

Microsoft empfiehlt, zum Speichern der Exchange-Dateien ein SAN (Storage Area Network) zu verwenden. Durch diese Konfiguration werden Leistung und Zuverlässigkeit des Servers optimiert.

> **Wichtig** Microsoft empfiehlt grundsätzlich die Verwendung von DAS- (Direct Access Storage) oder SAN-Arraylösungen, da mit dieser Konfiguration die Leistung und Zuverlässigkeit von Exchange optimiert werden. Microsoft unterstützt keine Lösungen mit Speichergeräten, die mit dem Netzwerk verbunden werden.

Mit einem SAN (Storage Area Network) erhalten Sie Möglichkeiten der Speicherung und der Speicherverwaltung für Unternehmensdaten. In SANs wird mit Fibre Channel-Umschalttechnologie eine schnelle und zuverlässige Verbindung zwischen dem Speicher und den Anwendungen erreicht.

Ein SAN enthält drei Hauptkomponentenbereiche:

- Fibre Channel-Umschalttechnologie
- Speicherarrays zum Speichern und Schützen der Daten
- Speicher- und SAN-Verwaltungssoftware

Hardwarehersteller bieten komplette SAN-Pakete an, in denen die erforderliche Hardware, Software und Unterstützung enthalten ist. Mit SAN-Software werden Redundanzen im Netzwerk und im Datenfluss optimiert, indem mehrere Pfade zu den gespeicherten Daten zur Verfügung gestellt werden (siehe Abbildung 6.8). Da die SAN-Technologie relativ neu

ist und ständig weiterentwickelt wird, können Sie eine vollständige SAN-Lösung planen und bereitstellen, in der das zukünftige Wachstum und neue SAN-Technologien integriert werden können. Durch die SAN-Technologie werden Verbindungen von Systemen mehrerer Hersteller mit verschiedenen Betriebssystemen mit Speicherprodukten von unterschiedlichen Herstellern ermöglicht.

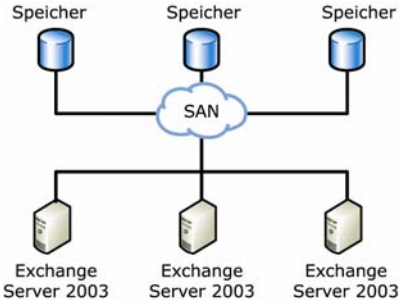


Abbildung 6.8 SAN-Speicherlösung

Derzeit sind SAN-Lösungen am besten für Unternehmen und IT-Abteilungen geeignet, die große Datenmengen speichern müssen.

Obwohl die anfänglich hohen Bereitstellungskosten ein Problem darstellen können, ist eine SAN-Lösung u. U. dennoch vorzuziehen, da die langfristigen Gesamtbetriebskosten niedriger ausfallen können als die Kosten für die Verwaltung vieler direkt angeschlossener Speicherarrays. Ziehen Sie insbesondere die folgenden Vorteile von SAN-Lösungen in Betracht:

- Wenn Sie momentan über viele Arrays verfügen, die von mehreren Administratoren verwaltet werden, können Administratoren durch die zentralisierte Verwaltung des gesamten Speichers für andere Aufgaben freigesetzt werden.
- Die Verfügbarkeit ist höher als bei allen anderen Einzellösungen, da die umfassende und flexible Zuverlässigkeit eines vom Hersteller unterstützten SAN nicht zu übertreffen ist. Einige Unternehmen müssen mit starken Umsatzverlusten rechnen, wenn die Dienste für Messaging und Zusammenarbeit ausfallen. Wenn in Ihrem Unternehmen möglicherweise als Ergebnis eines nicht verfügbaren Messagingdienstes große Umsatzverluste zu erwarten sind, kann die Bereitstellung einer SAN-Lösung eine kosteneffektive Maßnahme darstellen.

Bevor Sie in ein SAN investieren, sollten Sie die Kosten Ihrer aktuellen Speicherlösung in Bezug auf Hardware und administrativen Aufwand berechnen und die Notwendigkeit von zuverlässigem Speicher in Ihrem Unternehmen bewerten.

Vorteile von SANs (Storage Area Network) für Exchange

Im Folgenden werden einige Vorteile aufgeführt, die sich aus der Implementierung einer SAN-Lösung in Ihrer Exchange 2003-Organisation ergeben:

- Für Exchange 2003 ist eine hohe E/A-Bandbreite erforderlich, die nur von einem an ein SAN angeschlossenes Speicherarray geboten wird. Im Gegensatz dazu kann durch Netzwerkspeicherlösungen, die auf den Zugriff auf Exchange 2003-Datenbankdateien über den Netzwerkstack angewiesen sind, das Risiko von Datenfehlern und Leistungsverlusten erhöht werden.
- Bei Exchange 2003 müssen außerdem Postfächer und Öffentliche Ordner auf einem Laufwerk vorhanden sein, das sich lokal auf dem Exchange-Server befindet. Diese Anforderung wird von SAN-Lösungen

erfüllt, die über eine lokale Fibre Channel-Verbindung mit dem Exchange-Server verbunden sind. Andere Speicherlösungen, die zum Verwalten der Datenträgerressourcen auf eine Netzwerkumleitung zurückgreifen, erfüllen diese Anforderung nicht.

- SANs sind hochgradig skalierbar. Dies ist für Exchange eine wichtige Erwägung. Mit wachsenden Maildaten und dem beständigen Erweitern der Postfachgrenzen müssen Sie die Speicherkapazität und den E/A-Durchsatz erhöhen. Wenn Ihre Organisation erweitert wird, können einem SAN problemlos weitere Datenträger hinzugefügt werden. Wählen Sie ein SAN, das Speichervirtualisierung unterstützt. Auf diese Weise wird das Hinzufügen von Speicher sowie das schnelle Zuweisen zu Ihren Exchange-Servern vereinfacht. Mithilfe von Speichervirtualisierung können Sie Speicherdatenträger dann erwerben, wenn Ihr Budget dies zulässt.
- Durch die Skalierbarkeit von SANs ist es auch möglich, die Exchange-Organisation zu erweitern, indem Sie Server hinzufügen. In SANs können Sie mehrere Exchange-Server zu mehreren Speicherarrays hinzufügen und den Speicher dann zwischen ihnen aufteilen.
- Über die Verwendung von Spiegelung und Schattenkopien mit dem Volumeschattenkopie-Dienst werden die Sicherungen, Wiederherstellungen
und die allgemeine Verfügbarkeit in einem SAN verbessert.

Planen einer Speicherlösung

Bei der Planung einer Speicherstrategie für Exchange 2003 müssen drei Kriterien
in Einklang gebracht werden: Kapazität, Verfügbarkeit und Leistung. Die getroffene Wahl für die Implementierung der Speicherlösung wirkt sich auf die verbundenen Kosten für die Verwaltung der Exchange 2003-Umgebung aus.

- **Kapazität** In Exchange 2003 entspricht die Gesamtkapazität etwa der Anzahl von Postfächern multipliziert mit der Speichermenge, die jedem Postfach zugewiesen wurde. Wenn Ihre Organisation Öffentliche Ordner unterstützt, müssen Sie die entsprechende Menge von Festplattenspeicher hinzufügen, die für die Verwaltung des Informationsspeichers für Öffentliche Ordner erforderlich ist.
- **Verfügbarkeit** Der Grad der für Ihr Messagingsystem erforderlichen E-Mail-Verfügbarkeit hängt von den Anforderungen Ihres Unternehmens ab. Bei einigen Unternehmen wird E-Mail nur in geringem Ausmaß genutzt und wird daher nicht
als wichtig eingestuft, in anderen Unternehmen ist E-Mail jedoch ein erfolgsentscheidender Dienst. Je nach der Priorität, die E-Mail in Ihrem Unternehmen einnimmt, unterscheiden sich die Investitionen und die zugewiesenen Ressourcen für eine durchgängig verfügbare E-Mail-Lösung. Die allgemeine Verfügbarkeit wird durch Redundanz erhöht. Sie können Redundanz erreichen, indem Sie Anwendungen für Prozessorredundanz in Clustern anordnen oder eine redundante RAID-Lösung (Redundant Array of Independent Disks) für Datenredundanz implementieren.
- **Leistung** Die Leistungsanforderungen sind ebenfalls in jedem Unternehmen unterschiedlich. In diesem Kapitel wird die Leistung im Hinblick auf den Durchsatz betrachtet. Der Durchsatz wird in Bezug auf Speichertechnologie daran gemessen, wie viele Lese- und Schreibvorgänge pro Sekunde mit einem Speichergerät durchgeführt werden können.

Bevor Sie eine Speicherlösung für Exchange 2003 entwickeln, sollten Sie ermitteln, wie diese drei Kriterien in Ihrem Unternehmen bewertet werden. Dies betrifft insbesondere die Abwägung der Verfügbarkeit gegenüber der Leistung. In diesem Abschnitt wird hauptsächlich der Postfachspeicher behandelt, doch die Prinzipien und Konzepte können ebenso auf den Informationsspeicher für Öffentliche Ordner übertragen werden.

Bei der Installation von Exchange 2003 werden alle Daten lokal gespeichert, standardmäßig auf dem Laufwerk, auf dem Exchange installiert wird. Zum Ermitteln der mit dieser Standardkonfiguration verbundenen Kapazität, des Verfügbarkeitsgrades und der Leistung müssen Sie die folgenden Faktoren in Betracht ziehen:

- Anzahl und Geschwindigkeit der Prozessoren

- Menge des Arbeitsspeichers (RAM)
- Servertyp (Postfachserver, Server für Öffentliche Ordner, Connectorserver usw.)
- Anzahl der physischen Festplatten

Aufgrund der vielen Variablen beim Ermitteln der Größe und Kapazität sollten Sie hierzu die unter „Kapazitätsplanungstools“ weiter oben in diesem Kapitel beschriebenen Tools verwenden. Wenn die Standardkonfiguration Ihren Ansprüchen nicht genügt, sollten Sie grundsätzliche eine andere Speicherlösung einplanen, mit der die Kapazität, Leistung und Verfügbarkeit von Exchange maximiert wird. In den folgenden Abschnitten werden die Faktoren erläutert, die Sie bezüglich des Speichers beachten sollten.

Allgemeine Speicherprinzipien

Unabhängig von der ausgeführten Anwendung sollten Sie die folgenden Speicherprinzipien beachten, mit denen Sie die Kapazität, die Leistung und die Verfügbarkeit maximieren können:

- Sie können die jeweils erforderliche Prozessorauslastung verringern, indem Sie eine spezialisierte Hardwarelösung implementieren, z. B. RAID oder ein SAN mit RAID-Technologie. In diesem Szenario wird angenommen, dass Sie eine Hardwarelösung übernehmen und auf dem Hostcomputer keine Software-RAID-Lösung ausführen.
- Sie können auch die für Transaktionen durchschnittlich erforderliche Zeit reduzieren, indem Sie Dateien mit sequenziellem Zugriff von Dateien mit wahlfreiem Zugriff trennen. Durch das getrennte Speichern von Dateien mit sequenziellem Zugriff bleiben die Köpfe der Festplatte bei sequenziellen E/A-Vorgängen in der jeweils erforderlichen Position, so dass weniger Zeit zum Suchen der Daten erforderlich ist.
- Mit mehreren kleineren Festplatten wird eine bessere Leistung erzielt als mit einer großen Festplatte. Wenn Sie beispielsweise 72 GB Daten speichern müssen, sollten Sie vier Festplatten mit jeweils 18 GB verwenden und nicht eine Festplatte mit 72 GB. Grundsätzlich nimmt die Geschwindigkeit mit der Anzahl der Festplatten zu.

Mit den Informationen in den folgenden Abschnitten können Sie diese Speichertechnologien vergleichen und einander gegenüberstellen.

RAID-Lösungen

Durch den Einsatz einer RAID-Lösung können Sie die Fehlertoleranz in Ihrer Exchange-Organisation erhöhen. In einer RAID-Konfiguration wird ein Teil der physischen Speicherkapazität dafür verwendet, redundante Informationen zu den auf den Festplatten enthaltenen Daten zu speichern. Bei den redundanten Informationen handelt es sich entweder um Paritätsinformationen (bei RAID-5-Datenträgern) oder um eine vollständige, separate Kopie der Daten (bei gespiegelten Datenträgern). Mithilfe der redundanten Informationen können Daten bei Fehlern wiederhergestellt werden.

Wenn Sie sicherstellen möchten, dass die Server, auf denen Exchange ausgeführt wird, beim Ausfall eines einzelnen Datenträgers weiterhin funktionsfähig bleiben, können
Sie Datenträgerspiegelung oder Stripesets mit Parität auf den Festplatten in der Exchange-Organisation verwenden. Beim Verwenden der Datenträgerspiegelung und von Stripesets mit Parität werden zu den Daten auf den Festplatten redundante Daten erstellt.

Obwohl bei der Datenträgerspiegelung doppelte Datenträger erstellt werden, die auch beim Ausfall eines Datenträgers in einem der Spiegelsätze weiterhin funktionsfähig bleiben, wird durch die Datenträgerspiegelung nicht verhindert, dass unter Umständen beschädigte Dateien auf beide Spiegelsätze geschrieben werden oder andere Dateifehler auftreten. Verwenden Sie die Datenträgerspiegelung daher nicht als Ersatz für die regelmäßige Sicherung wichtiger Daten auf den Servern.

> **Hinweis** Beim Verwenden von Redundanzverfahren wie Parität wird die höhere Fehlertoleranz durch eine etwas geringere Festplatten-E/A-Leistung erkauft.

Da Transaktionsprotokolldateien und Datenbankdateien wichtig für den zuverlässigen Betrieb von Servern sind, auf denen Exchange ausgeführt wird, empfiehlt es sich, die Transaktionsprotokolldateien und Datenbankdateien der Exchange-Speichergruppe auf getrennten physischen Laufwerken zu speichern. Sie können auch die Datenträgerspiegelung oder Stripesets mit Parität verwenden, um zu verhindern, dass beim Ausfall einer einzelnen physischen Festplatte ein Teil des Messagingsystems ausfällt. Weitere Informationen über Datenträgerspiegelung und Stripesets mit Parität finden Sie in der Dokumentation zu Windows Server 2003.

Beim Implementieren einer RAID-Konfiguration empfiehlt es sich, ausschließlich ein Hardware-RAID-Produkt und keine Softwarefeatures für fehlertolerante Datenträger zu verwenden.

In den folgenden Abschnitten werden die vier wichtigsten Implementierungen von RAID erläutert: RAID-0, RAID-1, RAID-0+1 und RAID-5. Obwohl es viele andere RAID-Implementierungen gibt, sind diese vier Typen repräsentativ für den Einsatz von RAID-Lösungen.

RAID-0

RAID-0 ist ein Stripeset-Datenträgerarray. Jeder Datenträger wird logisch so partitioniert, dass ein „Stripe“ (Streifen) über alle Datenträger im Array verläuft und so eine einzelne logische Partition bildet. Wenn z. B. eine Datei in einem RAID-0-Array gespeichert wird und die betreffende Anwendung die Daten auf Laufwerk D speichert, verteilt das RAID-0-Array die Datei über das logische Laufwerk D (siehe Abbildung 6.9). In diesem Beispiel ist die Datei über alle sechs Datenträger verteilt.

Abbildung 6.9 RAID-0-Datenträgerarray

Unter dem Aspekt der Leistung stellt RAID-0 die effizienteste RAID-Technologie dar, da hierbei auf alle sechs Datenträger gleichzeitig geschrieben werden kann. Wenn Anwendungsdaten auf allen Datenträgern gespeichert sind, werden die Datenträger am effizientesten genutzt.

Der Nachteil von RAID-0 liegt in der geringen Fehlertoleranz. Wenn die Exchange-Postfachdatenbanken auf einem RAID-0-Array gespeichert sind und ein einzelner Datenträger ausfällt, müssen Sie die Postfachdatenbanken und Transaktionsprotokolldateien auf einem funktionsfähigen Datenträgerarray wiederherstellen. Wenn Sie die Transaktionsprotokolldateien auf diesem Array speichern und ein Datenträger ausfällt, können Sie zudem nur den Zustand der Postfachdatenbanken zum Zeitpunkt der letzten Sicherung wiederherstellen.

RAID-0 wird daher für die Verwendung mit Exchange nicht empfohlen.

RAID-1

Bei RAID-1 wird ein gespiegeltes Datenträgerarray verwendet, bei dem zwei Datenträger gespiegelt werden (Abbildung 6.10).

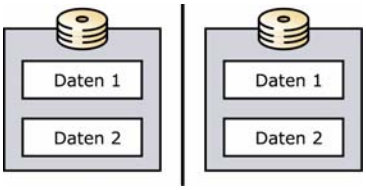


Abbildung 6.10 RAID-1-Datenträgerarray

RAID-1 stellt die zuverlässigste Variante der drei RAID-Array-Typen dar, da alle Daten beim Schreiben gespiegelt werden. Sie können jedoch nur die Hälfte der Speicherkapazität auf dem Datenträger verwenden. Obwohl dies ineffizient erscheinen mag, stellt RAID-1 die bevorzugte Option für Daten dar, bei denen es auf höchste Zuverlässigkeit ankommt.

RAID-0+1

Bei einem RAID-0+1-Datenträgerarray lässt sich eine optimale Leistung bei gleichzeitiger Redundanz erreichen, da hierbei Elemente von RAID-0 und RAID-1 kombiniert werden (Abbildung 6.11).

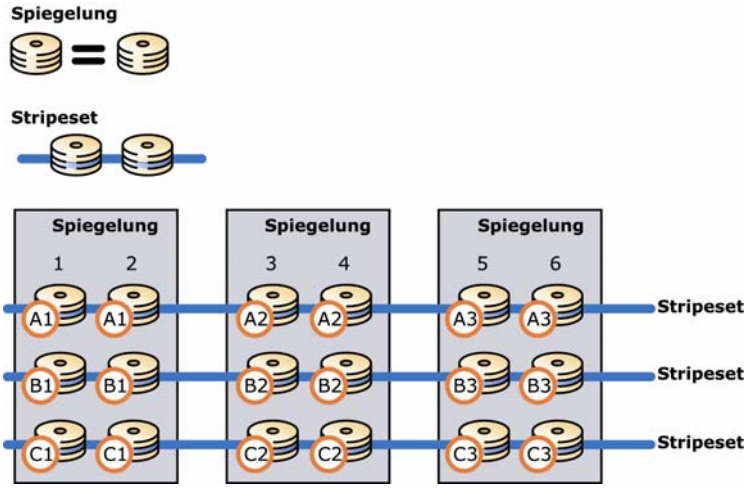


Abbildung 6.11 RAID-0+1-Datenträgerarray

In einem RAID-0+1-Datenträgerarray werden Daten auf beiden Datenträgergruppen gespiegelt (RAID-1) und dann als Stripesets auf den Laufwerken gespeichert (RAID-0). Jeder physische Datenträger ist im Array doppelt vorhanden. Bei einem RAID-0+1-Datenträgerarray mit sechs Datenträgern stehen drei Datenträger für die Datenspeicherung zur Verfügung.

RAID-5

Bei RAID-5 wird ähnlich wie bei RAID-0 ein Stripeset-Datenträgerarray verwendet, und die Daten werden über das Array verteilt. RAID-5 enthält jedoch darüber hinaus auch Paritätsinformationen. Das bedeutet, dass eine Methode vorhanden ist, mit der die Integrität der im Array gespeicherten Daten sichergestellt werden kann. Wenn ein Datenträger im Array ausfällt, können die Daten dadurch aus den verbleibenden Datenträgern wiederhergestellt werden (Abbildung 6.12). RAID 5 stellt daher eine zuverlässige Speicherlösung dar.

Abbildung 6.12 RAID-5-Datenträgerarray

Für die Verwaltung der Parität auf den Datenträgern wird jedoch ein Anteil von 1/n des verfügbaren Speicherplatzes benötigt (wobei *n* gleich der Anzahl von Laufwerken im Array ist). Wenn beispielsweise sechs 9-GB-Festplatten vorhanden sind, steht insgesamt ein Speicherplatz von 45 GB zur Verfügung. Um die Verwaltung von Paritätsinformationen zu gewährleisten, wird ein Schreibvorgang in zwei Schreibvorgänge und einen Lesevorgang im RAID-5-Array umgewandelt, was zu einer Verringerung der Gesamtleistung führt.

Der Vorteil einer RAID-5-Lösung liegt darin, dass RAID-5 sehr zuverlässig ist und der Speicherplatz auf den Datenträgern effizienter als bei RAID-1 und RAID-0+1 genutzt wird.

RAID-Lösungen im Vergleich

Da die Speicherkapazität ein relativ konstanter Faktor ist, können RAID-Lösungen gut durch einen Vergleich der Kosten, der Leistung und der Zuverlässigkeit bei gleicher Speicherkapazität beurteilt werden. In Tabelle 6.7 wird von den folgenden Voraussetzungen ausgegangen:

- Es werden 90 GB an Daten gespeichert.
- Sie verwenden 9-GB-Laufwerke.
- Die Arrays können Daten mit einer Rate von 100 E/A-Vorgängen pro Sekunde auf Datenträger schreiben.

Tabelle 6.7 Vergleich von RAID-Lösungen

RAID-Lösung	Anzahl von Laufwerken (Kosten)	Maximale Anzahl von Schreibvorgängen pro Sekunde	Maximale Anzahl von Lesevorgängen pro Sekunde	Zuverlässigkeit
RAID-0	10	1000	1000	Niedrig
RAID-0+1	20	1000	2000	Sehr hoch
RAID-5	11	275	1100	Hoch

> **Hinweis** RAID-1 wird in der Tabelle nicht berücksichtigt, da bei einer RAID-1-Lösung nur zwei Datenträger verwendet werden können. Für das Speichern von 90 GB Daten wären zwei 45-GB Laufwerke erforderlich, was zu einem wesentlich geringeren Durchsatz führen würde.

Die Zuverlässigkeit kann beurteilt werden, indem die Auswirkung betrachtet wird, die der Ausfall eines Datenträger auf die Integrität der Daten hätte. Bei RAID-0 wird keine Form von Redundanz implementiert, so dass beim Ausfall eines einzelnen Datenträgers in einem RAID-0-Array eine volle Wiederherstellung der Daten erforderlich ist. RAID-0+1 ist die zuverlässigste der drei Lösungen, da zwei oder mehr Datenträger ausfallen müssen, um einen potenziellen Datenverlust herbeizuführen. Mit anderen Worten müssen sehr spezielle Gruppen von Datenträgern ausfallen, damit Daten verloren gehen.

Die Kosten lassen sich durch Betrachtung der Anzahl von Datenträgern beurteilen, die für das Array erforderlich sind. Die RAID-0+1-Implementierung ist am kostenintensivsten, da doppelt so viel Speicherplatz vorhanden sein muss, wie eigentlich benötigt wird. Bei dieser Konfiguration ergibt sich jedoch in Bezug auf die maximalen Lese- und Schreibraten auch eine wesentlich höhere Leistung als bei einer RAID-5-Konfiguration mit derselben Kapazität.

Aspekte im Zusammenhang mit Exchange 2003

Berücksichtigen Sie beim Planen einer Speicherlösung die folgenden Features von Exchange 2003:

- Sie können den Volumeschattenkopie-Dienst verwenden, der im nächsten Abschnitt genauer beschrieben wird.
- Die in Exchange gespeicherten Daten werden nicht alle auf dieselbe Weise verwaltet. Daher ist es nicht optimal, eine einzelne Speicherlösung für alle Datentypen zu verwenden.
- Bei Servern, auf denen keine Postfächer oder Öffentlichen Ordner verwaltet werden, z. B. Connector-Server, können fortgeschrittene Speicherlösungen u. U. nicht optimal genutzt werden, da Daten auf diesen Servern meist nur kurz gespeichert und dann an einen anderen Server weitergeleitet werden. In einigen Fällen empfiehlt sich für solche Server eine RAID-0-Konfiguration.
- Je Exchange 2003-Server werden bis zu vier Speichergruppen unterstützt. In jeder Speichergruppe werden eigene Transaktionsprotokolldateien verwaltet, und es werden bis zu fünf Datenbanken unterstützt. Ihre Strategie für die Wiederherstellung nach Datenverlusten spielt eine wichtige Rolle bei der Entscheidung, wie viele Speichergruppen und Datenbanken bei der geplanten Speicherlösung unterstützt werden müssen. Im Plan zur Wiederherstellung sollten die Anforderungen Ihres Unternehmens bezüglich der Wiederherstellungsdauer enthalten sein. Von diesen Anforderungen hängt ab, welche Speicherkonfiguration in Ihrem Fall optimal ist.
- Bei Exchange erfolgt der Zugriff auf Transaktionsprotokolldateien sequenziell und der Zugriff auf Datenbanken wahlfrei. Daher empfiehlt es sich, die Transaktionsprotokolldateien (sequenzieller Zugriff) getrennt von den Datenbanken (wahlfreier Zugriff) zu speichern, um die E/A-Leistung und die Fehlertoleranz zu maximieren. Insbesondere sollten Sie jede Gruppe von Transaktionsprotokolldateien auf einem eigenen Array verwalten, getrennt von den Speichergruppen und Datenbanken.

SAN (Storage Area Networks) und Volumeschattenkopie-Dienst

Mithilfe der Onlinesicherung von Exchange 2003 werden automatisch die Datenbank- und Transaktionsprotokolldateien abgerufen und synchronisiert, die für eine erfolgreiche Wiederherstellung von Exchange 2003 erforderlich sind. Die Onlinesicherung von Exchange 2003-Datenbanken erfolgt auf demselben Weg wie der reguläre Datenbankzugriff. Wenn dieser Zugriff über das Netzwerk erfolgt, müssen durch die Sicherungs- und Wiederherstellungsvorgänge u. U. wesentlich höhere Bandbreitenanforderungen zu Spitzenzeiten eingeplant werden.

Um eine schnelle Sicherung und Wiederherstellung zu gewährleisten, wird bei mehreren SAN-Lösungen die Onlinesicherung von Exchange 2003 umgangen, und Sicherungen werden stattdessen mit dem neuen und schnelleren Volumeschattenkopie-Dienst ausgeführt. Um die Vorteile des Volumeschattenkopie-Dienstes voll auszunutzen, müssen Sie beim Sichern und Wiederherstellen von Daten eine geeignete, Exchange-kompatible Sicherungsanwendung verwenden. Außerdem müssen Sie Hardware verwenden (z. B. einen Speicherarray), die den Volumeschattenkopie-Dienst unterstützt. Erkundigen Sie sich bei Ihrem Händler, ob diese Features von den von Ihnen verwendeten Produkten unterstützt werden.

> **Wichtig** Wenn Sie eine Volumeschattenkopie-Sicherungslösung für Exchange 2003 implementieren, ist der Anbieter der Sicherungsanwendung Ihr Hauptansprechpartner für Supportfragen in Zusammenhang mit

Sicherung und Wiederherstellung, und der Anbieter des Speicherarrays ist für alle Fragen im Zusammenhang mit Speicherarrays zuständig.

Nähere Informationen zum Windows Server 2003 Volumeschattenkopie-Dienst finden Sie im technischen Artikel *Storage Management Using Windows Server 2003 and Windows Storage Server 2003 Virtual Disk Service and Volume Shadow Copy Service* (http://go.microsoft.com/fwlink/?LinkId=26119).

Weitere Informationen zur Verwendung des Volumeschattenkopie-Dienstes mit Exchange 2003 finden Sie im Microsoft Knowledge Base-Artikel 822896, „Exchange Server 2003-Dienste für Datensicherung und Volumeschattenkopie“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=822896).

Informationen zum Sichern von Exchange 2003-Daten mithilfe von Hotsplit-Sicherungen und Snapshot-Sicherungen, bei denen der Volumeschattenkopie-Dienst nicht verwendet wird, finden Sie im Microsoft Knowledge Base-Artikel 311898, „XADM: Hot Split Snapshot Backups of Exchange“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=311898).

Hinweis Ein SAN (Storage Area Network) stellt eine Lösung für die weiter oben in diesem Kapitel unter „Laufwerkbuchstabenbeschränkungen“ erläuterte Ausnahme dar. Wenn Sie den Volumeschattenkopie-Dienst zusammen mit Server-Clustering verwenden, können Datenträgern mit derselben Datenträgersignatur im Cluster nicht zwei verschiedene Laufwerkbuchstaben zugewiesen werden. Ein SAN löst dieses Problem, da Sie die Schattenkopie an einem anderen Speicherort im SAN verwalten können.

Platzieren von Exchange-Daten auf Speichergeräten

Exchange speichert Daten hauptsächlich an drei Speicherorten:

- SMTP-Warteschlangenverzeichnis
- Datenbankdateien (EDB- und STM-Dateien)
- Transaktionsprotokolldateien

SMTP-Warteschlangenverzeichnis

Im SMTP-Warteschlangenverzeichnis werden SMTP-Nachrichten zwischengespeichert, bis sie in einer Datenbank gespeichert (abhängig vom Nachrichtentyp in einer öffentlichen oder privaten Datenbank) oder an einen anderen Server oder Connector gesendet werden.

Normalerweise werden Nachrichten nur kurz in der SMTP-Warteschlange gespeichert. Daher sollte bei der Speicherlösung für die SMTP-Warteschlange vor allem die Leistung optimiert werden, und erst dann die Kapazität und Zuverlässigkeit. Beim Ausfall von Downstreamprozessen kann es jedoch erforderlich sein, große Datenmengen in der SMTP-Warteschlange zu speichern. Daher stellt ein RAID-0 Array nicht unbedingt die beste Speicherlösung für SMTP-Warteschlangen dar. Im Allgemeinen sollten Sie nur dann RAID-0 verwenden, wenn der Verlust von E-Mail-Nachrichten als akzeptabel angesehen wird. RAID-1 stellt eine gute Lösung dar, da hierbei eine gewisse Mindestzuverlässigkeit bei angemessenem Durchsatz erreicht werden kann.

In Exchange 2003 können Sie nun mithilfe des Exchange System-Managers den Speicherort des Warteschlangenverzeichnisses ändern. Sie finden diese Option im Exchange System-Manager auf der Registerkarte **Nachricht** für das virtuelle SMTP-Serverobjekt.

EDB- und STM-Dateien

Eine Exchange-Datenbank besteht aus einer EDB-Datei im Rich-Text-Format und einer STM-Datei mit MIME-Inhalten (Multipurpose Internet Mail Extensions).

In der EDB-Datei werden folgende Elemente gespeichert:

- Alle MAPI-Nachrichten
- Die Tabellen, die vom Prozess **Store.exe** zum Auffinden aller Nachrichten verwendet werden
- Prüfsummen für die EDB- und STM-Dateien
- Zeiger auf die Daten in der STM-Datei

Die STM-Datei enthält Nachrichten, die mit interneteigenen Inhalten übertragen werden. Da der Zugriff auf diese Dateien wahlfrei erfolgt, können beide Dateien
auf demselben Datenträger platziert werden.

Beim Planen der Speicherlösung für diese Dateien, sollten Sie auf eine zuverlässige Lösung setzen. RAID-0 ist somit keine empfehlenswerte Option. Nach der Zuverlässigkeit hängt die Entscheidung für eine Lösung vor allem davon ab, ob Sie die Leistung (RAID-1) oder die Kapazität (RAID-5) optimieren möchten. Wenn möglich, verwenden Sie für diese Dateien RAID-1 (oder RAID-0+1).

Sie können Öffentliche Ordner auf einem RAID-5-Array speichern, da Daten in Öffentlichen Ordnern meist einmal geschrieben und oft gelesen werden. RAID-5
bietet eine verbesserte Leistung bei Lesevorgängen.

Transaktionsprotokolldateien

Jede Speichergruppe erzeugt eine eigene Gruppe von Transaktionsprotokolldateien. Mithilfe von Transaktionsprotokolldateien kann der Zustand von EDB- und STM-Dateien verwaltet und deren Integrität sichergestellt werden. Neue Transaktionen werden gleichzeitig in der Protokolldatei und im Arbeitsspeicher gespeichert. Transaktionen
in Protokolldateien haben ein anderes Format als Exchange-Nachrichten. Sie enthalten Transaktionsdaten und geben an, an welcher Stelle die Daten in der EDB-Datei gespeichert werden sollen. Vor dem endgültigen Speichern der Transaktionen in der EDB-Datei erfolgt der Benutzerzugriff auf die Transaktionen über den Arbeitspeicher. Wenn die Serverlast sinkt, werden die Transaktionen anschließend in der EDB-Datei permanent gespeichert. Das Zwischenspeichern von Transaktionen im Arbeitsspeicher und die verzögerte Aktualisierung der Datenbankdateien auf dem physischen Datenträger wird als „Lazy Write“ (verzögertes Schreiben) bezeichnet.

Bei einem Systemausfall können die Datenbanken mithilfe der letzten Transaktionsprotokolldateien wiederhergestellt werden. Wenn Sie Zugriff auf die letzte Sicherung und die Transaktionsprotokolldateien seit dieser Sicherung haben, können Sie alle Daten wiederherstellen. Wenn jedoch Transaktionsprotokolldateien verloren gehen, sind die zugehörigen Daten verloren.

Sie können die Leistung und Fehlertoleranz von Exchange-Servern beträchtlich erhöhen, wenn Sie jede Gruppe von Transaktionsprotokolldateien auf einem getrennten Laufwerk verwalten. Da jede Speichergruppe über eine eigene Gruppe von Transaktionsprotokollen verfügt, sollte die Anzahl der dedizierten Transaktionsprotokolllaufwerke für den Server
der Anzahl der geplanten Speichergruppen entsprechen. Bei einer SAN-Lösung kann
der virtuelle Speicherplatz in getrennte virtuelle Laufwerke für Speichergruppen und Transaktionsprotokolldateien aufgeteilt werden. Da Transaktionsprotokolldateien darüber hinaus entscheidend für den zuverlässigen Betrieb der Server sind, sollten Sie die Laufwerke vor einem Ausfall schützen, idealerweise durch eine Hardwarespiegelung mithilfe von RAID. Es empfiehlt sich, eine RAID-0+1-Konfiguration zu verwenden, bei der Daten gespiegelt und dann als Stripeset gespeichert werden.

Hinweis Verteilen Sie die Datenbanklaufwerke über mehrere SCSI-Kanäle oder -Controller (Small Computer System Interface), konfigurieren Sie diese jedoch als ein einzelnes logisches Laufwerk, um die SCSI-Bus-Sättigung zu minimieren.

Eine Beispielkonfiguration sieht wie folgt aus:

- C:\ System- und Startdateien (Spiegelsatz)
- D:\ Auslagerungsdatei
- E:\ Transaktionsprotokolldateien für Speichergruppe 1 (Spiegelsatz)
- E:\ Transaktionsprotokolldateien für Speichergruppe 2 (Spiegelsatz)
- G:\ Datenbankdateien für beide Speichergruppen (mehrere Laufwerke, konfiguriert als Hardware-Stripesets mit Parität)

  Hinweis Folgende Laufwerke müssen NTFS-formatiert sein:

  - die Systempartition
  - Die Partition mit den Exchange-Binärdateien
  - Partitionen, die Transaktionsprotokolldateien enthalten
  - Partitionen, die Datenbankdateien enthalten
  - Partitionen, die andere Exchange-Dateien enthalten

Testen der Festplattenleistung mit Jetstress

Exchange 2003 beansprucht viel Festplattenspeicher und erfordert für den ordnungsgemäßen Betrieb ein schnelles und zuverlässiges Datenträgersubsystem. Mithilfe des Jetstress-Tools (Jetstress.exe) können Administratoren vor dem Einsatz
des Exchange-Servers in der Produktionsumgebung die Leistung und Stabilität des Datenträgersubsystems in Exchange überprüfen.

Das Jetstress-Tool überprüft die Datenträgerleistung durch Simulieren einer Exchange-Datenträger-E/A-Last. Sie können den Systemmonitor, die Ereignisanzeige und ESEUTIL (Extensible Storage Engine Utility) zusammen mit Jetstress verwenden, um zu überprüfen, ob das verwendete Datenträgersubsystem die von Ihnen definierten Leistungskriterien erfüllt oder übertrifft.

Sie können zwei Arten von Tests mit dem Jetstress-Tool ausführen: den Jetstress-Test für die Datenträgerleistung und den Jetstress-Belastungstest für das Datenträgersubsystem. Der Test für die Datenträgerleistung dauert zwei Stunden und ermöglicht Aussagen über die Leistung und die erforderliche Größe Ihrer Speicherlösung. Der Belastungstest für das Datenträgersubsystem dauert 24 Stunden und ermöglicht das ausführliche Testen der Speicherzuverlässigkeit innerhalb eines bestimmten Zeitraums. Es empfiehlt sich, beide Tests auszuführen, um die Integrität und Leistung des Datenträgersubsystems gründlich zu testen.

Nach dem erfolgreichen Abschluss des Jetstress-Tests für die Datenträgerleistung und des Jetstress-Belastungstests für das Datenträgersubsystem in einer Testumgebung können Sie mit dem nächsten Schritt im Exchange 2003-Bereitstellungsprozess beginnen. Sie haben sichergestellt, dass das Exchange 2003-Datenträgersubsystem in Bezug auf die geplante Benutzeranzahl und das geplante Benutzerprofil über eine angemessene Größe verfügt und die von Ihnen festgelegten Leistungskriterien erfüllt.

Hinweis Jetstress wird nur bei Verwendung von Exchange 2000 oder Exchange 2003 oder neueren Versionen von **ESE.DLL** unterstützt. Daher wird Jetstress auch nur unter Windows 2000 Server, Windows Server 2003, Windows 2000 Advanced Server und Windows Server 2003 Datacenter Edition unterstützt. Unter Microsoft Windows NT® Server bis Version 4.0 wird Jetstress nicht unterstützt.

Anhänge

Prüfliste für das Bewerten der bestehenden Umgebung

In der folgenden Prüflist werden die physischen und logischen Faktoren erläutert,
die wie in Kapitel 1 beschrieben bei der Bewertung Ihrer aktuellen Umgebung berücksichtigt werden müssen.

	Physische Ausrüstung
	Grundfläche des Datenzentrums
	Gestellplatz
	Netzwerkkapazität
	WAN (möglicherweise für die Bereitstellung von Verbindungen mit höherer Bandbreite erforderlich)
	Entfernungsgrad zwischen den einzelnen physischen Standorten (Wartezeiten beachten)
	LAN-Aufrüstung
	Backbone
	Modempools oder andere Datenfernübertragung
	Hardwareanforderungen
	Server
	Hauptspeicher
	Prozessor
	Speichergrenzwerte
	Netzwerkschnittstellenkarten (NICs) für Netzwerke mit hoher Bandbreite
	Router
	Hauptspeicher
	Prozessor
	Switches
	Firewalls
	Leistung
	Verträge über den Umfang von Serviceleistungen (SLA) für die Stromversorgung
	Geplante Leistungsaufnahme
	Unterbrechungsfreie Stromversorgung (UPS) oder andere Vorrichtungen für eine unabhängige Stromversorgung (Generatoren usw.)
	Ausgewiesener vollständig ausgestatteter „Ersatzstandort“

	Personal
	Schulungen für neu eingeführte Technologien und Verfahren
	Personalaufstockung
	Administratoren
	Support-Personal

	Geografie
	Zeitzonenprobleme
	Sprachen

	WAN
	Kapselungsaufrüstung (asynchroner Übertragungsmodus [ATM] usw.)
	Optimierung (Permanent Virtual Circuits [PVC] für Frame Relay)
	Qualität der Verbindungen insgesamt

	LAN
	Änderung in der Kapselung (Token Ring zu Ethernet)
	Entfernung oder Aufrüstung von Layer 2-Geräten

	Netzwerkadresse
	TCP/IP End-to-End
	Anzahl der IP-Hops zwischen Endpunkten
	Überlegungen in Bezug auf das Subnet (Überlegungen zum Standort des Microsoft® Active Directory®-Verzeichnisdienstes)
	Gerätekonfiguration
	Router und offene Anschlüsse
	Switches
	Firewalls und offene Anschlüsse
	Anschlüsse und Layer 4-Protokolle, die für das Filtern und Sperren von Geräten aktiviert sind
	Alle Verschlüsselungs- und Entschlüsselungsvorgänge
	Alle Formatänderungen (z. B. andere E-Mail-Gateways und X.400-Connectors)
	RPC-Verbindungen (Remoteprozeduraufruf)
	Network Basic Input/Output System (NetBIOS)
	Infrastruktur öffentlicher Schlüssel (PKI, Public Key Infrastructure)
	Virtuelles privates Netzwerk (VPN)
	Gemeinsam genutzte Abhängigkeiten zwischen Internet Information Services (IIS), Simple Mail Transfer Protocol (SMTP) und Network News Transfer Protocol (NNTP)

	DNS
	Windows® Internet Name Service (WINS)

	Netzwerkbetriebssystem
	Gemeinsam genutzte Abhängigkeiten zwischen DHCP, NTLM, NTLMv2 und LM
	Windows NT® Server Version 4.0-Domänenstruktur: Vertrauensstellungen, primäre Domänencontroller, Sicherungsdomänencontroller
	Windows 2000 Server oder Windows Server™ 2003 Active Directory
	Gesamtstruktur
	Domänenstruktur
	Migration
	Standortstruktur

	Sicherheit
	Kerberos
	Migration
	Sicherheitsprinzipien
	SID-Verlauf (Security Identifier)

	Verzeichnisse
	Migration
	Active Directory Connector
	Metaverzeichnisse

	Verwaltung
	Migration
	Zuweisung von Berechtigungen
	Verwaltung

Optimieren der Speicherauslastung

Dieser Anhang enthält Informationen zum Überwachen und Optimieren der Speicherauslastung auf den Servern.

Überwachen der Speicherauslastung

Sie können das Anwendungsprotokoll der Ereignisanzeige sowie **Leistungsprotokolle und Warnungen** (Option **Systemleistung** im Untermenü **Verwaltung**) auf Probleme mit dem virtuellen Speicher überprüfen. Im Anwendungsprotokoll wird die Warnung 9582 angezeigt, wenn der größte freie Block des virtuellen Speichers nur noch 32 MB groß ist. Wenn eine solche Warnung angezeigt wird, starten Sie den Speicherprozess von Exchange bei der nächsten Gelegenheit neu. Wenn der größte Speicherblock auf 16 MB abfällt, wird der Fehler 9582 nochmals angezeigt. Dies bedeutet, dass der Server ausfallen kann. Deshalb sollten Sie den Server bei der nächsten Gelegenheit neu starten. Wenn auf diese Ereignisse nicht reagiert wird, können gelegentliche Fehler bei der Übermittlung von E-Mail-Nachrichten und bei der IMAIL-Konvertierung auftreten (12800-Ereignisse).

Überwachen Sie in **Leistungsprotokolle und Warnungen** die folgenden Indikatoren:

- **Leistungsindikator „Max. Blockgröße des VS“ im MSExchangeIS-Objekt.** Auf einem ordnungsgemäß ausgeführten Server beträgt die Größe des größten freien Blocks mehr als 200.000.000 Byte (200 MB). Wenn der Wert darunter liegt, sollten Sie den Server aufmerksam überwachen.
- **Auslagerungsfähige Poolseiten im Speicherobjekt:** Werte über 200 MB weisen auf ein Problem hin, es sei denn, es werden gerade Datensicherungen ausgeführt. Bei Datensicherungen wird jede Seite im Cache-Manager durch eine Poolauslagerungsseite gesichert.
- **Nicht Auslagerungsfähige Poolseiten im Speicherobjekt:** Werte über 100 MB weisen auf ein Problem hin.
- **Freie Tabelleneinträge für Seitenauslagerungsdateien im Speicherobjekt:** Werte unter 3000 weisen auf ein Problem hin.
- **Arbeitsseiten im Prozessobjekt:** Ein Aufwärtstrend weist auf mögliche Speicherverluste hin.

Wenn ein Server Anzeichen eines geringen virtuellen Adressraums aufweist, sollten Sie die folgenden Einstellungen anpassen. Wenn diese Einstellungen nicht für Microsoft® Exchange optimiert werden, wird in der Ereignisanzeige das Ereignis 9665 angezeigt.

- Wenn auf dem Server Microsoft Windows® 2000 Advanced Server oder Windows Server™ 2003 ausgeführt wird und mindestens 1 GB physischer Speicher verfügbar ist, legen Sie in der Datei „Boot.ini“ den Parameter „/3GB“ wie folgt fest.
- Wenn auf dem Server Windows Server 2003 (jede Version) ausgeführt wird, konfigurieren Sie die Einstellung „/USERVA“ und den Registrierungsschlüssel „SystemPages“ wie nachstehend beschrieben. Wenn auf dem Server Windows 2000 ausgeführt wird, vergewissern Sie sich, dass Windows 2000 SP3 oder eine höhere Version installiert ist.
- Wenn auf dem Server physischer Speicher von mindestens 1 GB vorhanden ist, legen Sie den Registrierungsparameter „HeapDeCommitFreeBlockThreshold“ wie nachstehend beschrieben fest.
- Optimieren Sie ggf. die Cachegröße der Informationsspeicher-Datenbank wie nachstehend beschrieben.

Ereignis 9665

Exchange überprüft zu Beginn des Speicherprozesses, ob der Speicher optimal konfiguriert ist. Wenn die Speichereinstellungen nicht optimal sind, wird in der Ereignisanzeige das Ereignis 9665 angezeigt. Die Meldung wird in den folgenden Fällen ausgegeben:

- Auf dem Server wird Windows 2000 ausgeführt, und der Wert für „SystemPages“ in der Registrierung liegt außerhalb des Bereichs von 24000 bis 31000.
- Der Server verfügt über mindestens 1 GB Speicher. Der Parameter **/3GB** wurde jedoch nicht angegeben.
- Auf dem Server wird Windows Server 2003 ausgeführt, er verfügt über einen Speicher von mindestens 1 GB, der Parameter „/3GB“ ist festgelegt, doch die /USERVA-Einstellung ist nicht vorhanden oder liegt außerhalb des Bereichs von 3030 bis 2970.

Wenn dieses Ereignis ausgegeben wird, überprüfen Sie die Einstellungen für „SystemPages“ und „HeapDeCommitFreeBlockThreshold“ in der Registrierung sowie den Parameter „/3GB“ und die Einstellung „/USERVA“ in der Datei „boot.ini“. Die folgenden Abschnitte enthalten Empfehlungen für die einzelnen Einstellungen.

Hinweis Sie können die Überprüfung der Speicherkonfiguration durch Einfügen des in Tabelle B.1 dargestellten Registrierungsschlüssels deaktivieren.

Tabelle B.1 Registrierungsschlüssel für das Deaktivieren der Überprüfung der Speicherkonfiguration

Pfad	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ ParametersSystem\
Parameter	Suppress Memory Configuration Notification
Typ	REG_DWORD
Einstellung	1

Hinweis Die Überprüfung der Speicherkonfiguration wird nicht auf Servern ausgeführt, auf denen Microsoft® Small Business Server installiert ist.

Festlegen des Parameters „/3GB“

In der Standardeinstellung reservieren Windows 2000 Advanced Server und Windows Server 2003 für Prozesse im Benutzermodus (beispielsweise „Store.exe“) einen virtuellen Adressraum von 2 GB. Wenn ein Server über physischen Speicher von mindestens 1 GB verfügt, legen Sie den Parameter „/3GB“ in der Datei „Boot.ini“ fest, um den virtuellen Adressraum zu vergrößern.

Verwenden Sie den Parameter „/3GB“ nur auf Servern, auf die die folgenden Kriterien zutreffen:

- Der Server verwaltet Exchange 2003-Postfächer oder Öffentliche Ordner.
- Auf dem Server ist mindestens 1 GB an physischem Speicher verfügbar.

Es wird nicht empfohlen, diesen Parameter auf Servern zu verwenden, auf denen keine Informationsspeicher für Öffentliche Ordner oder Postfächer gespeichert sind.

Weitere Informationen zum Parameter „/3GB“ finden Sie im Microsoft Knowledge Base-Artikel 266096, „XGEN: Exchange 2000 Requires /3GB Switch with More Than 1 Gigabyte of Physical RAM“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=266096).

Wichtig Der Parameter „/3GB“ wurde für Windows 2000 Advanced Server und alle Versionen von Windows Server 2003 entwickelt. Legen Sie den Parameter „/3GB“ nicht unter Windows 2000 Standard fest.

Konfigurieren von „/USERVA“ und „SystemPages“

Wenn auf dem Server Windows 2000 ausgeführt wird, müssen Sie den Registrierungsschlüssel „SystemPages“ auf einen Wert zwischen 24000 und 31000 festlegen. Der Registrierungsschlüssel „SystemPages“ befindet sich im folgendem Pfad:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\SystemPages
```

Wenn auf dem Server Windows Server 2003 ausgeführt wird, legen Sie den Wert von „SystemPages“ auf Null fest, und geben Sie in der Datei „Boot.ini“ den Parameter „/USERVA=3030“ an. Mit diesen Einstellungen können auf dem Server mehr Tabelleneinträge für Seitenauslagerungsdateien angelegt werden. Dies ist insbesondere für große Systeme von hoher Bedeutung.

Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel 810371, „XADM: Using the /Userva Switch on Windows 2003 Server-Based Exchange Servers“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=810371).

Festlegen des Registrierungsschlüssels „HeapDeCommitFreeBlockThreshold“

Der Registrierungsschlüssel „HeapDeCommitFreeBlockThreshold“ steuert die Menge des freien Speichers, die erforderlich ist, bevor der Heap-Manager Speicher freigibt. Der Standardwert ist Null. Das bedeutet, dass der Heap-Manager jede Auslagerungsseite von 4 KB freigibt, die verfügbar wird. Mit der Zeit kann der virtuelle Adressraum fragmentiert werden. Bei Servern mit einem physischen Speicher von mindestens 1 GB können Sie den Registrierungsschlüssel auf einen höheren Wert festlegen, um die Fragmentierung zu verringern oder zu verhindern. Legen Sie den Registrierungsschlüssel entsprechend Tabelle B.2 fest, und starten Sie den Server neu. Weitere Informationen zum Registrierungsschlüssel **HeapDeCommitFreeBlockThreshold** finden Sie im Microsoft Knowledge Base-Artikel 315407, „XADM: The 'HeapDeCommitFreeBlockThreshold' Registry Key“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=315407).

Tabelle B.2 Einstellungen für den Registrierungsschlüssel „HeapDeCommitFreeBlockThreshold“

Pfad	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
Parameter	HeapDeCommitFreeBlockThreshold
Typ	REG_DWORD
Standard	Null
Empfohlene Einstellung*	262144

* Dieser Wert ist die Anzahl von Blöcken in Dezimalsschreibweise. Der empfohlene Wert ist 262144. Dies entspricht einem hexadezimalen Wert von 0x00040000.

Anpassen der Cachegröße der Informationsspeicher-Datenbank

Im Cache der Informationsspeicher-Datenbank (auch als Extensible Storage Engine-Puffer bezeichnet) werden Datenbanktransaktionen zwischengespeichert, bevor sie in die Datenbank übernommen werden. In der Standardeinstellung sind in Exchange 2003 dafür 896 MB reserviert, wenn auf dem Server der Parameter „/3GB“ festgelegt ist. Wenn der Parameter „/3GB“ nicht angegeben ist, werden 576 MB reserviert. In den folgenden Fällen kann durch das Anpassen der maximalen Puffergröße die Leistung gesteigert werden:

- Wenn auf dem Server Exchange 2003 und andere serverseitige Anwendungen ausgeführt werden, verkleinern Sie den Puffer, um die Speicherbelegung durch Exchange zu begrenzen.
- Erhöhen Sie auf Servern mit einer Speichergröße von mehr als 2 GB die Größe des Puffers (bis maximal 1200 MB).

Verwenden Sie vor dem Erhöhen der maximalen Puffergröße **Leistungsprotokolle und Warnungen** zum Überwachen der Informationsspeicherinstanz des Leistungsindikators „Virtuelle Bytes“ (im Prozess-Objekt) unter normaler Belastung. Dieser Leistungsindikator gibt die aktuelle Größe des vom Prozess „Store.exe“ verwendeten virtuellen Adressraums an (in Byte). Der Wert muss unter 2,8 GB liegen, wenn der Parameter „/3GB“ festgelegt ist. Er muss unter 1,8 GB liegen, wenn der Parameter „/3GB“ nicht festgelegt ist. Setzen Sie bei höheren Werten die maximale Puffergröße nicht herauf. Wenn die Werte darunter liegen, können Sie die maximale Puffergröße bis auf 1.200 MB erhöhen. Wenn beispielsweise der Parameter „/3GB“ festgelegt ist und die Anzahl virtueller Bytes bei hoher Auslastung 2,5 GB beträgt, können Sie die maximale Puffergröße um ca. 300 MB erhöhen.

Beachten Sie, dass bei Servern mit Adressraumfragmentierungsproblemen das Erhöhen der Puffergröße die Serverleistung beeinträchtigen kann. Bei einem größeren Puffer wird ein größerer Teil des virtuellen Adressraums belegt. Das Vergrößern des Puffers kann zur Instabilität des Systems führen.

Verwenden Sie zum Anpassen der maximalen Puffergröße Active Directory Service Interface (ADSI) Edit, um den Wert von „msExchESEParamCacheSizeMax“ zu ändern. Weitere Informationen zum Ändern des Wertes **msExchESEParamCacheSizeMax** finden Sie im Microsoft Knowledge Base-Artikel 266768, „XSTR: How to Modify the Store Database Maximum Cache Size“ (http://go.microsoft.com/fwlink/?linkid=3052&kbid=266768). Warten Sie nach dem Festlegen des Wertes, bis der Microsoft Active Directory®-Verzeichnisdienst den Wert in der kompletten Gesamtstruktur repliziert hat. Starten Sie anschließend den Microsoft Exchange-Informationsspeicherdienst neu.

> **Wichtig** Achten Sie darauf, nicht den Wert „msExchESEParamCacheSizeMin“ auszuwählen.

In Tabelle B.3 sind die Standardwerte für die maximale Puffergröße und entsprechende Empfehlungen aufgeführt. Der Wert wird als Anzahl von Seiten ausgedrückt und muss zur Gewährleistung der Effizienz auf ein genaues Vielfaches von 8192 festgelegt werden.

Tabelle B.3 Standardwerte für die maximale Puffergröße und entsprechende Empfehlungen

Standardgröße für /3GB-Server	229376 (896 MB)
Standardgröße für Nicht-/3GB-Server	147456 (576 MB)
Empfohlener Höchstwert	307200 (1,2 GB)
Sehr große Server mit eingeschränktem Adressraum	196608 (768 MB)

Ressourcen

Weitere Information über Microsoft® Exchange Server finden Sie auf der Microsoft Exchange Server-Website (http://go.microsoft.com/fwlink/?linkid=21573). Zusätzlich finden Sie in den folgenden technischen Artikeln, Resource Kits und Microsoft Knowledge Base-Artikeln wertvolle Informationen zu Begriffen und Verfahren für
die Wiederherstellung von Daten nach einem Datenverlust.

> **Hinweis** Eine selbstextrahierende ausführbare Datei mit allen technischen Artikeln und Onlinedokumentationen des Exchange-Produktteams finden Sie als Download unter http://go.microsoft.com/fwlink/?LinkId=10687.

Websites

Technische Bibliothek für Microsoft Exchange Server 2003
(http://go.microsoft.com/fwlink/?linkid=14576)

Tools und Aktualisierungen für Exchange Server 2003
(http://go.microsoft.com/fwlink/?LinkId=21316)

MSDN®-Website
(http://go.microsoft.com/fwlink/?LinkId=21574)

Microsoft Identity Integration Server 2003 (MIIS 2003)-Dokumentation
(http://go.microsoft.com/fwlink/?LinkId=21271)

Exchange Server 2003-Dokumentationen

Exchange Server 2003-Administratorhandbuch
()

Bereitstellungshandbuch für Exchange Server 2003
()

Technische Artikel

Deploying Microsoft Exchange 2000 Server Clusters
(http://go.microsoft.com/fwlink/?LinkId=6271)

Storage Solutions for Microsoft Exchange 2000 Server
(http://go.microsoft.com/fwlink/?LinkId=1715)

Best Practice Active Directory Design for Exchange 2000
(http://go.microsoft.com/fwlink/?LinkId=17837)

Best Practice Active Directory Design for Managing Windows Networks
(http://go.microsoft.com/fwlink/?LinkId=18348)

Design Considerations for Delegation of Administration in Active Directory
(http://go.microsoft.com/fwlink/?LinkId=18349)

Deploying Microsoft Exchange 2000 Server Clusters

(http://go.microsoft.com/fwlink/?LinkId=14578)

Disaster Recovery for Microsoft Exchange 2000 Server
(http://go.microsoft.com/fwlink/?LinkId=18350)

Migrating Mailboxes from Microsoft Exchange Server Version 5.5 to Exchange 2000 Server
(http://go.microsoft.com/fwlink/?linkid=18351)

Monitoring Exchange 2000 with Microsoft Operations Manager 2000
(http://go.microsoft.com/fwlink/?linkid=18177)

Multiple Forest Considerations
(http://go.microsoft.com/fwlink/?LinkId=21177)

Microsoft Identity Integration Server 2003 Global Address List Synchronization
(http://go.microsoft.com/fwlink/?LinkId=21270)

Tools

Tools und Aktualisierungen für Exchange Server 2003
(http://go.microsoft.com/fwlink/?LinkId=21316)

Exchange Stress and Performance-Tool (ESP) – Build 5531.0
(http://go.microsoft.com/fwlink/?LinkId=1709)

Kapazitätsplanung und Topologierechner für Exchange 2000
(http://go.microsoft.com/fwlink/?LinkId=1716)

Load Simulator im *Exchange 2000 Server Resource Kit*
(http://go.microsoft.com/fwlink/?LinkId=1710)

Resource Kits

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

Sie können eine Kopie des *Microsoft Exchange 2000 Server Resource Kits* bei Microsoft Press® unter http://go.microsoft.com/fwlink/?LinkId=6544 bestellen.

Windows Server 2003 Deployment Kit
(http://go.microsoft.com/fwlink/?LinkId=25197)

Sie können eine Kopie des Microsoft Windows *2003 Server Deployment Kits* bei Microsoft Press unter http://go.microsoft.com/fwlink/?LinkId=27096 bestellen.

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

Sie können eine Kopie des Microsoft Windows *2000 Server Resource Kits* bei Microsoft Press unter http://go.microsoft.com/fwlink/?LinkId=6546 bestellen.

Microsoft Knowledge Base-Artikel

Die folgenden Microsoft Knowledge Base-Artikel stehen im Internet zur Verfügung unter http://support.microsoft.com/.

266096, „XGEN: Exchange 2000 erfordert Parameter /3GB bei mehr als 1 Gigabyte physischem RAM“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=266096)

266768, „XSTR: How to Modify the Store Database Maximum Cache Size“

(http://go.microsoft.com/fwlink/?linkid=3052&kbid=266768)

272314, „XADM: Preparing a Mixed Mode Organization for Conversion to Native Mode“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=272314)

305145, „How to: Remove the IFS Mapping for Drive M in Exchange 2000 Server“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=305145)

311898, „XADM: Hot Split Snapshot Backups of Exchange“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=311898)

315407, „XADM The 'HeapDeCommitFreeBlockThreshold' Registry Key“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=315407)

810371, „XADM: Using the /Userva Switch on Windows 2003 Server-Based Exchange Servers“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=810371)

238573, „XADM: Installing, Configuring, and Using the InterOrg Replication Utility“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=238573)

238642, „XADM: Troubleshooting the InterOrg Replication Utility“
(http://go.microsoft.com/fwlink/?linkid=3052&kbid=238642)

Anlage B1 : Verhaltens- und Leistungskontrolle (§85 I Nr. 13 PersVG)

Jeder Infrastrukturbetreiber ist verpflichtet, die zur Aufrechterhaltung des Dienstbetriebes und zur Absicherung der gesamten Netzwerkumgebung generierten Ereignisse zu protokollieren.

Hierzu zählen insbesondere:

- unberechtigte Anmeldeversuche,
- unberechtigte Zugriffe auf Domänenressourcen,
- unberechtigte Zugriffe auf andere Sicherheitsprincipals.

Die Erforderlichkeit einer Ereignisprotokollierung zu den o.g. Kriterien erfolgt ausschließlich zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung und Aufrechterhaltung des Dienstbetriebes für die Exchange Organisation auf den beteiligten Mitgliedsservern. Es ist hierbei sichergestellt, dass Protokolleinträge vorübergehend und ausschließlich aus verarbeitungstechnischen Gründen erstellt und nach ihrer ordnungsgemäßen Nutzung automatisch mit dem ältesten Ereignis beginnend überschrieben werden. Die Infrastrukturbetreiber stellen durch Protokollkonfigurationen sicher, dass nicht wahllos eine Registrierung aller Aktivitäten zu den o.g. Kriterien erfolgt. Als eine angemessene Konfiguration der Registrierung von Aktivitäten in Protokolldateien, gilt die Begrenzung der Protokollierung auf sensible Aktivitäten innerhalb der o.g. Kriterien. Es werden daher alle systemseitig vorhandenen Möglichkeiten genutzt, damit wirklich nur Aktivitäten mit einem erhöhten Schutzbedarf registriert werden. Keinesfalls werden derartig erzeugte Protokolldateien für eine Leistungs- und Verhaltenskontrolle genutzt,

Mitgliedsserver in der Exchange-Organisation

Sicherheitsverwaltungseinstellungen (Überwachung)

Die hier beschriebenen Sicherheitsverwaltungseinstellungen betreffen ausschließlich Objekte (Benutzer- und Computerobjekte sowie andere Netzwerkressourcen) auf Servern der Exchange-Organisation. Die Einheitlichkeit in Bezug auf die Sicherheitsverwaltungseinstellungen ist per Definition dieser Einstellungen auf jedem dieser Server aufrechtzuerhalten. Sicherheitsverwaltungseinstellungen sollten sowohl erfolgreiche als auch erfolglose Zugriffe erkennen, die eine Gefahr für das Netzwerk oder deren Ressourcen darstellen und deren Wertigkeit als Sicherheitsrelevant eingestuft wurde.

Definieren von Ereignisprotokolleinstellungen

Jedes durch eine Sicherheitsverwaltungseinstellung generierte Ereignis wird in der Ereignisanzeige des jeweiligen Exchange Server angezeigt. Für die Mitgliedsserver der Exchange-Organisation, werden die Einstellungen für die Ereignisanzeige über Gruppenrichtlinien definiert, so wird sichergestellt dass auf jedem Mitgliedsserver einheitliche Einstellungen wirken.

Zu überwachende Ereignisse

Das Serverbetriebssystem bietet folgende Kategorien für Sicherheitsereignisse an.

- Anmeldeereignisse,
- Kontoanmeldeereignisse,
- Objektzugriff,
- Verzeichnisdienstzugriff
- Rechteverwendung,
- Prozessnachverfolgung,
- Systemereignisse und
- Richtlinienänderungen

Gruppenrichtlinien allgemein

Für die Server der Exchange-Organisation innerhalb der Active Directory Gesamtstruktur, werden die Einstellungen für die Sicherheitsverwaltung über Gruppenrichtlinien definiert, so wird sichergestellt dass auf jedem dieser Server einheitliche Einstellungen wirken.

Richtlinienname:

GPO-Exchange-Server-Sicherheit

Umfang der Standard Richtliniendefinition für Exchange Server:

- Definition der Sicherheitseinstellungen für die Überwachungsrichtlinie
- Definition der Sicherheitseinstellungen für das Ereignisprotokoll

Weitere Definitionen von Gruppenrichtlinienobjekten oder deren Eigenschaften sind für die Funktionalität und die Bereitstellung der Mitgliedsserver in der Exchange-Organisation nicht erforderlich jedoch für den Betrieb des Active Directory per Vorgabestandard des ITDZ definiert, zugewiesen und wirksam:

Richtlinienname:

Default Domain Policy

Umfang der Richtliniendefinition:

- Definition der Sicherheitseinstellungen für Kontorichtlinien/Kennwortrichtlinien
- Definition der Umbenennung des Administrator- und Gastkonto

Sicherheitsrelevante Richtlinieneinstellungen

Die ***GPO-Exchange-Server-Sicherheit*** ist die Richtlinie, die verantwortlich ist für die Sammlung und Protokollierung von Ereignissen die als Sicherheitsrelevant eingestuft wurden. Die Protokollierung findet in Ereignisprotokollen statt. Eine Protokollierung erfolgt ausschließlich im Sicherheitsprotokoll des jeweiligen Domänencontrollers. Hierbei wird per Richtlinie bei Bedarf automatisch mit dem ältesten Ereignis beginnend das Protokoll überschrieben. Die zu protokollierenden Ereignisse sind auf das minimal erforderliche Maß (*siehe Richtlinieneinstellungen*) reduziert. Eine Leistungs- und Verhaltenskontrolle erfolgt hierbei nicht. Der generelle Zugriff auf die Ereignisprotokollierung ist durch Zugriffs Control List (ACL) Berechtigungen nur für Administratoren möglich. Weitere Sicherheitsverwaltungsrichtlinien in deren Ergebnis benutzerabhängige Protokolleinträge generiert werden sind nicht definiert.
Detailliert wird in der folgenden Abbildung dargestellt welche Ereignisse hierzu gesammelt und protokolliert werden.

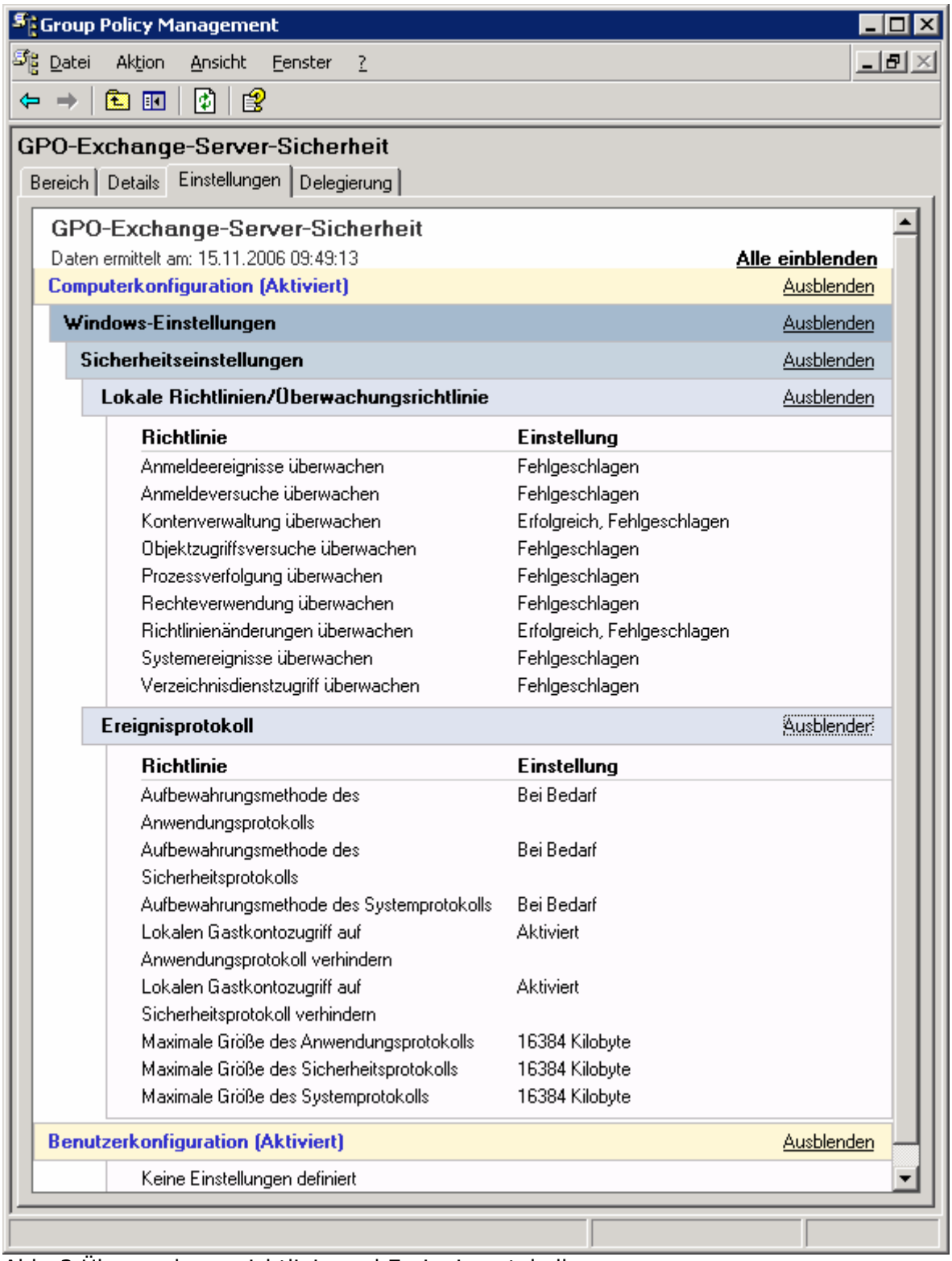


Abb. 2 Überwachungsrichtlinie und Ereignisprotokoll

Verfolgung des Nachrichtenflusses einzelner Mails (Protokollierung)

Mitgliedsserver der Exchange-Organisation besitzen die Möglichkeit, den Nachrichtenfluss des gesamten Nachrichtenverkehrs zu protokollieren. Pro Tag wird eine Protokolldatei für den jeweiligen Exchange Server angelegt. Das Durchsuchen und analysieren der Protokolldateien gibt den notwendigen Aufschluss über den Weg einer Nachricht durch das System. Die Nachrichtenverfolgung muss explizit aktiviert werden.

Die Mitgliedsserver legen Übermittlungsinformationen zu allen übertragenen Nachrichten in Textdateien ab, die auch über Netzwerkfreigaben zu erreichen sind. Über die Netzwerkfreigabe greifen Exchange interne Tools zu, um den Laufweg einer Nachricht durch das System nach zu verfolgen. Freigabe und NTFS-Zugriffsrechte auf diese Netzwerkfreigabe sind eingeschränkt *(siehe Anlage B1.1)*.
Weiterhin kann und sollte je Mitgliedsserver eingestellt werden, wie lange diese Protokolldateien vorgehalten werden. ITDZ Vorgabe und Systemstandard sind 7 Tage, d.h. nach einer Woche löscht der Exchange Server die älteren Protokolldateien selbstständig *(siehe Anlage B1.1)*. Die Einstellungen erfolgt durch den Exchange System-Manager über die Eigenschaften der Mitgliedsserver in jeder administrativen Gruppe *(siehe Anlage B1.1)*. Die tatsächliche Dauer der Aufbewahrungsfrist dieser Protokolldateien obliegt dem Exchange Administrator der jeweiligen Verwaltung / Behörde in der Exchange Organisation, dieser kann den Vorgabestandard individuell ändern.

Datensatzaufbau des Nachrichtenprotokolls:

- Protokoll enthält Datensätze jedoch keine Überschriften bzw. Feldbezeichnungen,
- Protokolldatensätze sind durch eine Leerzeile (CL RF) voneinander getrennt,
- Einzelne Datenfelder sind durch Tabulator voneinander getrennt.

Protokolldateien sind Textdateien und können problemlos mit einem Editor geöffnet und bearbeitet werde. In den Protokolldateien sind keine Information über den Inhalt der Mail oder den Namen von Anlagen oder deren Inhalte verfügbar. Maximal der Betreff kann bei Exchange 2000/2003 mit protokolliert werden. Eine einfache schnelle Auswertung ist mit dem Exchange System-Manager möglich. Über den Menüpunkt "Extras - Nachrichtenstatus" können diese Protokolldateien dazu genutzt werden, den Verlauf einer Mail zu kontrollieren. Der Exchange Systemmanager liest die Protokolldatei ein und wenn die Nachricht an einen anderen Server übergeben wurde, liest er auf diesem Server weiter. (Dies ist der Grund für die o.g. Netzwerkfreigabe). So kann im Fehlerfall sehr genau nachvollzogen werden, wann eine Nachricht durch welches Nachrichtenverarbeitungssystem gelaufen ist. Die Funktionalität ist auf die Mitgliedsserver der Exchange-Organisation begrenzt, verlässt eine Nachricht die Exchange-Organisation, kann nur die letzte bzw. wird eine Nachricht an einen Empfänger in der Exchange-Organisation übermittelt, kann nur der erste, Übergabepunkt protokolliert werden *(siehe Anlage B1.1)*.

Zur Vereinheitlichung der Nachrichtenprotokollierung auf Exchange Servern werden Systemrichtlinien definiert und zugewiesen diese wirken auf alle Exchange Server einer administrativen Gruppe *(siehe Anlage B1.1)*.

Übermittlungs- und Empfangseinschränkungen (Beschränkungen)

Verbindungsbeschränkungen

Die Parameter für die Nachrichtenbeschränkung, auf dem jeweiligen virtuellen SMTP-Server sind konfiguriert, dazu zählen:

- die maximale Anzahl von Empfängern pro Nachricht,
- die maximale Nachrichtengröße,
- die maximale Anzahl von gleichzeitigen Verbindungen mit dem SMTP-Server,

Die Konfiguration der Parameter beruht erstrangig in der Übernahme der Richtlinien in der Exchange-Organisation. Diese Beschränkungen werden nicht nur übernommen, sondern können auch auf jedem virtuellen SMTP-Server selbst neu definiert werden. Die Beschränkungsvorgaben der Exchange-Organisation jedoch können nicht überschritten werden. Die Vorgaben unterstützen grundsätzlich einen Schutz vor, auf Mailübertragung basierende Denial-of-Service Angriffe gegen Exchange Server der Organisation.

Speicherbeschränkungen

Zum Schutz vor einer unverhältnismäßig hohen Anzahl von E-Mail-Nachrichten an einen bestimmten Exchange Server (Denial-of-Service Angriff) mit dem Ziel, den verfügbaren Festplattenspeicherplatz drastisch zu minimieren, sowie grundsätzlich in Anbetracht der endlichen Kapazität des verfügbaren Festplattenspeicherplatzes sind Parameter für die Speicherbeschränkung von:

- Postfächern und Öffentlichen Ordnern definiert.

Die Beschränkungsparameter werden per Richtlinie für die o.g. Speicherbereiche je Exchange Server separat definiert (entsprechend verfügbarer Festplattenkapazität abzüglich des Speicherplatzes für die Gesamtheit aller Postfächer bzw. der Anzahl der Replikate von Öffentlichen Ordnern auf diesem Server und einer Kapazitätsreserve). Die Parameter der Speicherbeschränkungen können einzeln für Postfachbesitzer und oder Öffentliche Ordner überschrieben werden. Hier gelten dann die Werte die vom Standard abweichen. Exchange Administratoren der jeweiligen Exchange Server, sind verantwortlich für die Verwendung der verfügbaren Festplattenkapazität.
(Für die Definition von Beschränkungen siehe auch Anlage B1.1)

Umgang mit vorhandenen und gelöschten Objekten (Aufbewahrung)

Die Aufbewahrungsfristen entsprechend den Grundsätzen des Steuer- und Handelsrechts, für steuerrelevante Unterlagen der Buchhaltung, Rechnungen, Buchungen, Bilanzen und Organisationsunterlagen sowie versandte und empfangene Handelsbriefe einschließlich der geschäftsrelevanten E-Mails, gelten grundsätzlich nicht für die Exchange-Organisation. Exchange ist kein Archivierungssystem im Sinne der o.g. Rechtsvorschriften, sondern nur ein Nachrichtenverarbeitungssystem mit endlicher Möglichkeit zur Aufbewahrung.
Im Rahmen definierter Postfachgrenzen (Richtlinien) können Nutzer E-Mailnachrichten speichern. Automatische Sicherungsszenarien realisieren, dass die entsprechenden Postfachinhalte auf entfernte Medien gesichert werden. Sowohl die Postfachgröße, als auch die Anzahl verfügbarer Datensicherungen ist begrenzt. Zyklisch muss der Postfachbesitzer Speicherplatz durch Löschen bzw. Auslagern von Postfachinformationen freigeben, um den normalen Geschäftbetrieb mit seinem Postfach fortführen zu können. Bei der Freigabe von Speicherplatz, beabsichtigt und unbeabsichtigt gelöschte E-Mail Nachrichten bleiben vom Nutzer unabhängig, noch einen per Richtlinie definierten Zeitraum (*Standard 7 Tage*), auf dem Exchange Server zum Zwecke einer eventuellen zeitnahen Wiederherstellung erhalten. Eine Wiederherstellung von Postfachinhalten nach Ablauf dieser Aufbewahrungszeit, ist nur aus verfügbaren Datensicherungen möglich. Die Definition und Festlegung einer Anzahl verfügbarer Datensicherungen, obliegt jeder Verwaltung / Behörde selbst.
(Für die Definition von Aufbewahrungsfristen siehe auch Anlage B1.1)

Anlage B1.1 :

Ereignisprotokollierung, Grenzen und Beschränkungen

Lokale Richtlinie/Überwachungsrichtlinie

Anlage B1 benennt Kategorien und stellt grafisch die für Mitgliedsserver der Exchange-Organisation definierte Richtlinie zur Überwachung sicherheitsrelevanter Ereignisse auf Exchange Servern dar.
Unter Bezugnahme auf diese Angaben wird auf Mitgliedsserver der Exchange-Organisation wie folgt protokolliert:

Richtlinie:	**Einstellung**
Anmeldereignisse überwachen	**Fehlgeschlagen**
Anmeldeversuche überwachen	**Fehlgeschlagen**

Protokollierung:

- Jedes Mal wenn ein Benutzer an einem Exchange Server durch Eingabe einer falschen Anmeldekennung oder aber durch Eingabe eines unzulässigen Kennwortes versucht eine Anmeldung herbeizuführen, wird dies auf dem jeweiligen Server protokolliert.
- fehlgeschlagene Anmeldeereignisse werden generiert, wenn die Anmeldsitzung und das entsprechende Token erstellt bzw. gelöscht werden.
- Zu den Anmeldeereignissen zählen hierbei sowohl Computer- als auch Benutzeranmeldeereignisse,

Folgende Ereigniskennungen werden Protokolliert:

Ereigniskennung	Beschreibung
529	Der Anmeldeversuch ist mit einem unbekannten Benutzernamen oder einem bekannten Benutzernamen mit einem falschen Kennwort erfolgt.
531	Ein Anmeldeversuch ist mit einem deaktivierten Konto erfolgt.
532	Ein Anmeldeversuch ist mit einem abgelaufenen Konto erfolgt.
533	Der Benutzer darf sich an diesem Computer nicht anmelden.
534	Der Benutzer hat versucht, sich mit einem unzulässigen Anmeldetyp anzumelden (z. B. Netzwerkanmeldung, interaktive Anmeldung, Batchanmeldung, Dienstanmeldung oder interaktive Anmeldung).
535	Das Kennwort für das angegebene Konto ist abgelaufen.
537	Der Anmeldeversuch ist aus anderen Gründen fehlgeschlagen.
539	Das Konto wurde zu dem Zeitpunkt gesperrt, als der Anmelde-versuch erfolgte.

Die folgenden Sicherheitsereignisse können mithilfe von Einträgen für Anmeldeereignisse bzw. -versuche diagnostiziert werden:

Lokaler Anmeldeversuch ist fehlgeschlagen.

Folgende Ereigniskennungen zeigen fehlgeschlagene Anmeldeversuche an: 529, 531, 532, 533, 534 und 537. Die Ereigniskennungen 529 und 534 werden angezeigt, wenn eine falsche Kombination aus Benutzername und Kennwort für ein lokales Konto eingegeben wurde. Diese Ereignisse können auch auftreten, wenn ein Benutzer sein Kennwort vergessen hat oder das Netzwerk über die Netzwerkumgebung durchsucht.

Kontomissbrauch.

Die Ereigniskennungen 531, 532 und 533 können den Missbrauch eines Benutzerkontos anzeigen. Die Ereigniskennungen weisen darauf hin, dass die Kombination Konto/Kennwort zwar richtig eingegeben wurde, andere Beschränkungen aber die erfolgreiche Anmeldung verhindern.

Kontosperrungen.

Die Ereigniskennung 539 zeigt an, dass das Konto gesperrt wurde.

Richtlinie:	**Einstellung**
Kontenverwaltung überwachen	**Erfolgreich,Fehlgeschlagen**

Protokollierung:

- Bei Erstellung, Löschung oder Änderung von Benutzer oder Gruppenkonten,
- Ermittlung wann ein Sicherheitsprincipal erstellt wurde und wer diese Aufgabe ausgeführt hat,

Folgende Ereigniskennungen werden Protokolliert:

Ereigniskennung	Beschreibung
624	Benutzerkonto wurde erstellt.
625	Benutzerkontotyp wurde geändert.
626	Benutzerkonto wurde aktiviert.
627	Versuch einer Kennwortänderung wurde unternommen.
628	Benutzerkontokennwort wurde festgelegt.
629	Benutzerkonto wurde deaktiviert.
630	Benutzerkonto wurde gelöscht.
631	Globale Gruppe mit aktivierter Sicherheit wurde erstellt.
632	Globales Gruppenmitglied mit aktivierter Sicherheit wurde hinzugefügt.
633	Globales Gruppenmitglied mit aktivierter Sicherheit wurde entfernt.
634	Globale Gruppe mit aktivierter Sicherheit wurde gelöscht.
635	Lokale Gruppe mit aktivierter Sicherheit wurde erstellt.
636	Lokales Gruppenmitglied mit aktivierter Sicherheit wurde hinzugefügt.
637	Lokales Gruppenmitglied mit aktivierter Sicherheit wurde entfernt.
638	Lokale Gruppe mit aktivierter Sicherheit wurde gelöscht.
639	Lokale Gruppe mit aktivierter Sicherheit wurde geändert.
641	Globale Gruppe mit aktivierter Sicherheit wurde geändert.
642	Benutzerkonto wurde geändert.
643	Domänenrichtlinien wurden geändert.
644	Benutzerkonto wurde gesperrt.

Die folgenden Kontenverwaltungsereignisse können mithilfe von Sicherheitsprotokoll-einträgen diagnostiziert werden:

Erstellung eines Benutzerkontos.

Die Ereigniskennungen 624 und 626 zeigen das Erstellen und Aktivieren von Benutzerkonten an.

Benutzerkontokennwort wurde geändert.

Die Änderung eines Kennwortes durch eine andere Person als den Benutzer kann darauf hindeuten, dass ein Konto von einem anderen Benutzer übernommen wurde. Die Ereigniskennungen 627 und 628. zeigen an, dass eine Kennwortänderung erfolgreich durchgeführt wurde.

Benutzerkontostatus wurde geändert.

Alle Vorkommnen der Ereigniskennungen 629 und 630 sollten untersucht werden, um sicherzustellen, dass sie autorisierte Transaktionen darstellen.

Änderung von Sicherheitsgruppen.

Änderungen globaler Gruppenmitgliedschaften werden in Ereignissen mit den Kennungen 632 und 633 aufgezeichnet. Änderungen lokaler Domänengruppen-mitgliedschaften werden in Ereignissen mit den Kennungen 636 und 637 aufgezeichnet.

Kontosperrung.

Bei der Sperrung eines Kontos werden zwei Ereignisse auf dem PDC-Emulator protokolliert. Ein Ereignis der Kennung 644 zeigt an, dass der Kontoname gesperrt wurde. Zur Angabe des gesperrten Kontos wird daraufhin ein Ereignis der Kennung 642 aufgezeichnet. Dieses Ereignis wird nur am PDC-Emulator protokolliert.

Richtlinie:	**Einstellung**
Objektzugriffsversuche überwachen	**Fehlgeschlagen**

Protokollierung:

- Einträge werden generiert, sobald ein Handle zu einem Objektzugriff fehlschlägt,

Durch die Überwachung des Objektzugriffs werden die folgenden Ereignisse im Sicherheitsprotokoll angezeigt:

Ereigniskennung	Beschreibung
560	Für ein bereits bestehendes Objekt wurde Zugriff gewährt.
562	Ein Handle zu einem Objekt wurde geschlossen.
563	Ein Objekt wurde in der Absicht geöffnet, es zu löschen.
564	Ein geschütztes Objekt wurde gelöscht.
565	Für einen bereits bestehenden Objekttyp wurde Zugriff gewährt.

Richtlinie:	**Einstellung**
Prozessverfolgung überwachen	**Fehlgeschlagen**

Protokollierung:

- Fehlgeschlagene Versuche der Erstellung und Beendigung von Prozessen werden im Ereignisprotokoll angezeigt,
- Auch der Versuch eines Prozesses, ein Handle zu einem Objekt zu generieren oder indirekten Zugriff auf ein Objekt zu erhalten, wird aufgezeichnet.

Folgende Ereignisse werden bei einer fehlgeschlagenen Prozessverfolgung angezeigt:

Ereigniskennung	Beschreibung
592	Erstellen eines neuen Prozess fehlgeschlagen.
593	Prozess beenden fehlgeschlagen.
594	Ein Handle zu einem Objekt wurde dupliziert.
595	Ein indirekter Zugriff auf ein Objekt wurde erhalten.

Richtlinie:	**Einstellung**
Rechteverwendung überwachen	**Fehlgeschlagen**

Standardmäßig sind die folgenden Benutzerrechte von der Überwachung ausgeschlossen:

- Umgehen der durchsuchenden Überprüfung,
- Debuggen von Programmen,
- Erstellen eines Tokenobjekts,
- Ersetzen eines Tokens auf Prozessebene
- Generieren von Sicherheitsüberwachungen
- Sichern von Dateien und Verzeichnissen
- Wiederherstellen von Dateien und Verzeichnissen

Die folgenden Ereignisse werden bei aktivierter Überwachung der Rechteverwendung generiert:

Ereigniskennung	Beschreibung
576	Bestimmte Rechte wurden zum Zugriffstoken eines Benutzers hinzugefügt.
577	Ein Benutzer hat versucht, einen privilegierten Systemdienstevorgang auszuführen.
578	Rechte wurden in Bezug auf ein bereits geöffnetes Handle für ein geschütztes Objekt verwendet.

Die folgenden Rechteverwendungsereignisse können mithilfe von Sicherheitsprotokoll-einträgen diagnostiziert werden:

Als Teil des Betriebssystems handeln

Die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht SeTcbPrivilege. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dies gilt beispielsweise für den **GetAdmin**-Angriff, bei dem ein Benutzer versucht hat, sein Konto zur Administratorengruppe hinzuzufügen, die dieses Recht verwendet.

Die einzigen Einträge für dieses Ereignis sollten die für das Systemkonto und weitere dem Benutzerrecht zugewiesene Dienstkonten sein.

Systemzeit ändern.

Die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht SeSystemtimePrivilege.

Erzwingen des Herunterfahrens von einem Remotesystem aus

Die Ereigniskennungen 577 und 578 mit dem angezeigten Benutzerrecht SeRemoteShutdownPrivilege. Die Sicherheits-ID (SID), der das Benutzerrecht zugeordnet ist, und der Benutzername des Sicherheitsprincipals, der das Recht zugeordnet hat, sind in den Ereignisdetails enthalten.

Verwalten von Überwachungs- und Sicherheitsprotokollen

Die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht SeSecurityPrivilege. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis tritt auf, wenn das Ereignisprotokoll gelöscht wird und wenn Ereignisse zur Rechteverwendung in das Sicherheitsprotokoll geschrieben werden.

Herunterfahren des Systems

Die Ereigniskennungen 577 mit dem angezeigten Recht SeShutdownPrivilege. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis tritt auf, wenn ein Versuch unternommen wurde, den Computer herunterzufahren.

Übernehmen des Besitzes von Dateien und anderen Objekten

Die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht SeTakeOwnershipPrivilege. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt.

Richtlinie:	**Einstellung**
Richtlinienänderungen überwachen	**Erfolgreich,Fehlgeschlagen**

Protokollierung:

- Änderungsversuche an der Überwachungsrichtlinie, anderen Richtlinien und an Benutzerrechten,

Folgende Ereigniskennungen werden Protokolliert:

Ereigniskennung	Beschreibung
608	Ein Benutzerrecht wurde zugewiesen.
609	Ein Benutzerrecht wurde entfernt.
610	Eine Vertrauensstellung mit einer anderen Domäne wurde erstellt.
611	Eine Vertrauensstellung mit einer anderen Domäne wurde entfernt.
612	Überwachungsrichtlinie wurde geändert.

Die zwei wichtigsten Ereignisse, sind die Ereignisse mit den Kennungen 608 und 609. In den Ereignisdetails dieser Ereignisse ist die Sicherheits-ID (SID) aufgeführt, der das Benutzerrecht zugeordnet ist, sowie der Benutzername des Sicherheitsprincipals, der das Recht zugeordnet hat.

Als Teil des Betriebssystems handeln.
Ereigniskennungen 608 und 609 mit dem Benutzerrecht *seTcbPrivilege* in den Ereignisdetails.

Hinzufügen von Arbeitsstationen zur Domäne.
Ereignisse mit dem Benutzerrecht *SeMachineAccountPrivilege* in den Ereignisdetails.

Sichern von Dateien und Verzeichnissen.
Ereignisse mit dem Benutzerrecht *SeBackupPrivilege* in den Ereignisdetails.

Umgehen der durchsuchenden Überprüfung.
Ereignisse mit dem Benutzerrecht *SeChangeNotifyPrivilege* in den Ereignisdetails. Dieses Benutzerrecht ermöglicht das Durchsuchen einer Verzeichnisstruktur auch dann, wenn sie keine anderen Zugriffsrechte für das Verzeichnis besitzen.

Systemzeit ändern.
Ereignisse mit dem Benutzerrecht *SeSystemtimePrivilege* in den Ereignisdetails. Dieses Benutzerrecht ermöglicht einem Sicherheitsprincipal das Ändern der Systemzeit.

Erstellen von dauerhaft freigegebenen Objekten.
Ereignisse mit dem Benutzerrecht *SeCreatePermanentPrivilege* in den Ereignisdetails. Der Inhaber dieses Rechtes kann Datei- und Druckfreigaben erstellen.

Debuggen von Programmen.
Ereignisse mit dem Benutzerrecht *SeDebugPrivilege* in den Ereignisdetails. Der Inhaber dieses Rechtes kann mit jedem beliebigen Prozess eine Verbindung herstellen. Dieses Recht ist standardmäßig nur Administratoren zugewiesen.

Erzwingen des Herunterfahrens von einem Remotesystem aus.
Ereignisse mit dem Benutzerrecht *SeRemoteShutdownPrivilege* in den Ereignisdetails.

Erhöhen der Zeitplanungspriorität.
Ereignisse mit dem Benutzerrecht *SeIncreaseBasePriorityPrivilege* in den Ereignisdetails. Ein Benutzer mit diesem Recht kann Prozessprioritäten ändern.

Wiederherstellen von Dateien und Verzeichnissen.
Ereignisse mit dem Benutzerrecht *SeRestorePrivilege* in den Ereignisdetails.

Herunterfahren des Systems.

Ereignisse mit dem Benutzerrecht *SeShutdownPrivilege* in den Ereignisdetails. Ein Benutzer mit diesem Benutzerrecht kann das System herunterfahren, um die Installation eines neuen Gerätetreibers zu initialisieren.

Übernehmen des Besitzes von Dateien und anderen Objekten.

Ereignisse mit dem Benutzerrecht *SeTakeOwnershipPrivilege* in den Ereignisdetails. Ein Benutzer mit diesem Benutzerrecht kann auf beliebige Objekte oder Dateien auf dem NTFS-Datenträger zugreifen, indem er deren Besitz übernimmt.

Richtlinie:	**Einstellung**
Systemereignisse überwachen	**Fehlgeschlagen**

Protokollierung:

Systemereignisse werden generiert, wenn ein Benutzer oder ein Prozess Aspekte der Computerumgebung ändert,

Dies führt zu folgenden Ereigniskennungen im Ereignisprotokoll:

Ereigniskennung	Beschreibung
512	Windows wird gestartet.
513	Windows wird heruntergefahren.
514	Ein Authentifizierungspaket wurde von der lokalen Sicherheitsautorität (LSA oder Local Security Authority) geladen.
515	Ein vertrauenswürdiger Anmeldevorgang wurde bei der lokalen Sicherheitsautorität registriert.
516	Die für das Einreihen von Sicherheitsereignismeldungen in Warteschlangen zugewiesenen internen Ressourcen sind ausgelastet. Dies führt zu einem Verlust von Sicherheitsereignismeldungen.
517	Das Sicherheitsprotokoll wurde gelöscht.
518	Die Sicherheitskontenverwaltung hat ein Benachrichtigungspaket geladen.

Die Ereigniskennungen können zur Erfassung einiger Sicherheitsprobleme verwendet werden:

Herunterfahren / Neustarten des Computers

Die Ereigniskennung 513 kennzeichnet das Herunterfahren von Windows. Es ist wichtig, den Zeitpunkt zu kennen, zu dem Server heruntergefahren oder neu gestartet wurden.

Ändern oder Löschen des Sicherheitsprotokolls

Ereigniskennungen 612 und 517 ermitteln, welcher Benutzer die Überwachungsrichtlinie geändert hat.

Richtlinie:	**Einstellung**
Verzeichnisdienstzugriff	**Fehlgeschlagen**

Protokollierung:

Ein versuchter Verzeichniszugriff wird im Sicherheitsprotokoll als Verzeichnisdienstereignis mit der Kennung 565 angezeigt. Nur durch Untersuchung der Details des Sicherheitsereignisses kann ermittelt werden, welchem Objekt das Ereignis zugeordnet werden kann.

Beschränkungen auf Ebene der Exchange Organisation

Die Exchange-Organisation definiert zentral Vorgaben und Beschränkungen die einerseits für alle Exchange Server der Organisation bindend sind und andererseits von den einzelnen Exchange Servern übernommen werden müssen, damit diese zentralen Konfigurationen auf den einzelnen Exchange Servern wirksam werden können. Konfigurationen dieser Art können nur über das Exchange Verwaltungstool Exchange Systemmanager ausgeführt werden.

Übermittlungs- und Empfängereinschränkungen

Die standardmäßigen Übermittlungs- und Empfängereinschränkungen werden in der gesamten Exchange-Organisation nur einmal definiert und sind dann ohne weitere Einzelkonfiguration für alle Exchange Server der Organisation grundsätzlich verbindlich.

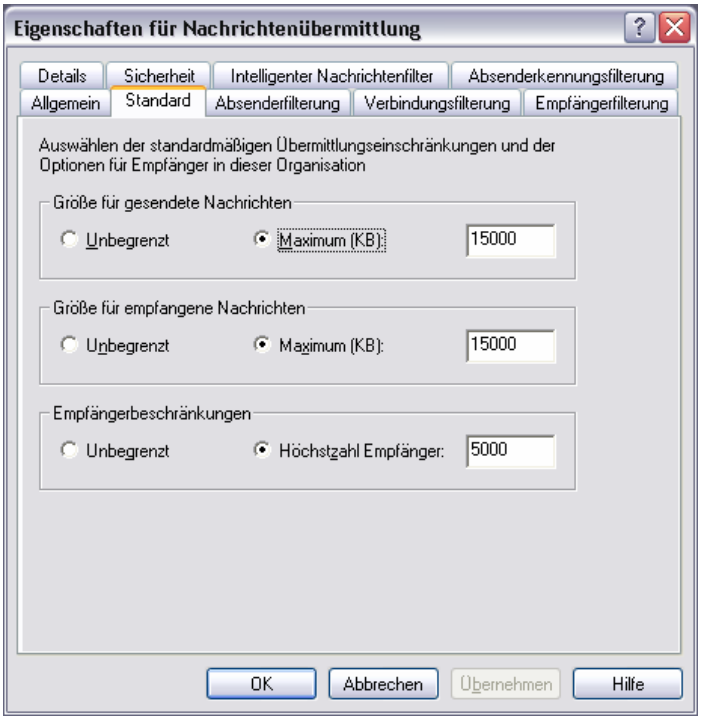


Abb. Übermittlungs- und Empfängereinschränkungen

Mit Definition der Größen für gesendete und empfangene Nachrichten wird für jedes mailaktivierte Konto in der Exchange Organisation festgelegt, dass die maximale Größe einer Nachricht 15 MB nicht überschreiten darf. Nachrichten die größer als das hier definierte Maximum sind, werden von Exchange Servern der Organisation abgewiesen und nicht übermittelt. Die Größendefinition ist eine zentrale Vorgabe, sowie Resultat analytischer Erhebungen über verfügbare Postfachressourcen, sowohl innerhalb als auch außerhalb der Exchange Organisation. Die Größenbeschränkung schützt und vereinheitlicht die Nachrichtenübermittlung für die gesamte Exchange-Organisation.
Eine Änderung dieser zentralen Vorgaben, kann auf jedem Exchange Server der Organisation, durch explizite Definition auf der Registerseite „Nachrichten“ der Eigenschaften des jeweiligen virtueller Server für SMTP durchgeführt werden. Hierbei kann die neue Größendefinition ausschließlich kleiner als die Vorgabe sein. Eine Größenangabe über dem Vorgabewert der Exchange-Organisation wird ignoriert.

Absenderfilterung

Die Absenderfilterung stellt ein Schutzmechanismus der Exchange-Organisation, vor einer Nachrichtenübermittlung von nicht überprüfbaren Nachrichtenquellen dar. Es wird sichergestellt das eingehende Nachrichten die der Absenderliste entsprechen blockiert werden und Nachrichten ohne Absenderinformationen werden generell abgewiesen.

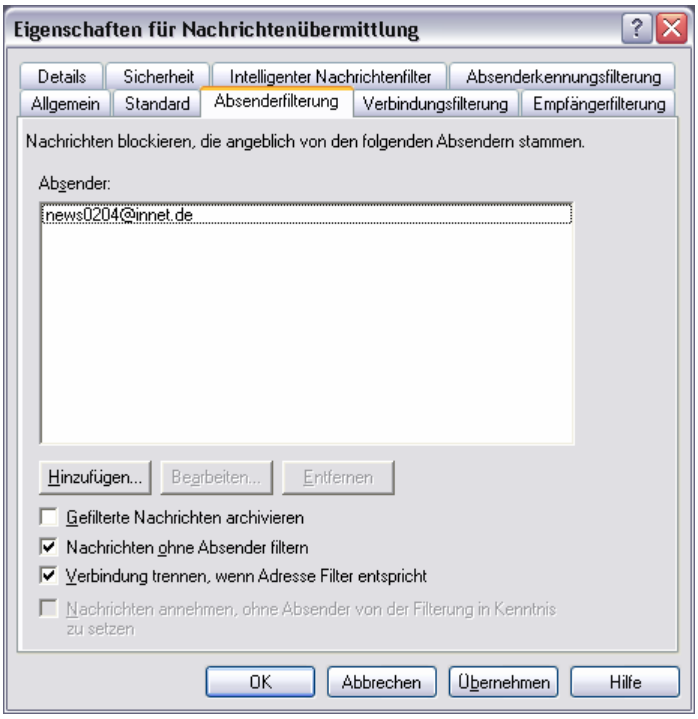


Abb. Absenderfilterung

Empfängerfilterung

Die Empfängerfilterung schützt die Exchange Organisation vor Nachrichtenfluten an kompromittierte Empfänger (z.B. SPAM Flut an im Internet veröffentlichte Mailadressen) sowie an Empfängeradressen von Anwendern die diese (entspr. Liste) Empfängeradressen nicht mehr nutzen, als optionale Komponente auch vor Nachrichten an Empfänger die gar nicht in der Exchange Organisation existent (Verzeichnisabgleich) sind.

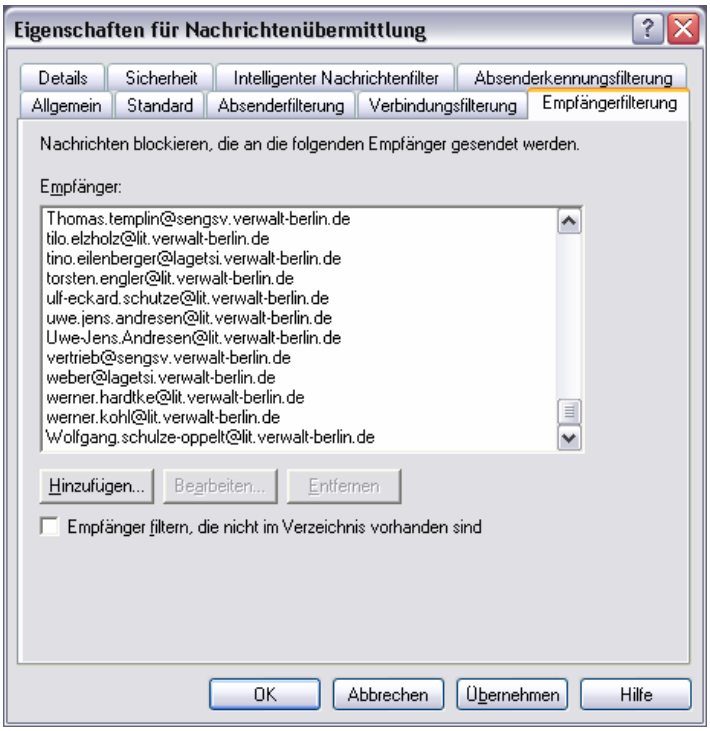


Abb. Empfängerfilterung

Sowohl Absender- als auch Empfängerfilterung muss auf jedem virtuellem SMTP Server in der Exchange Organisation explizit aktiviert werden.

Intelligenter Nachrichtenfilter (IMF)

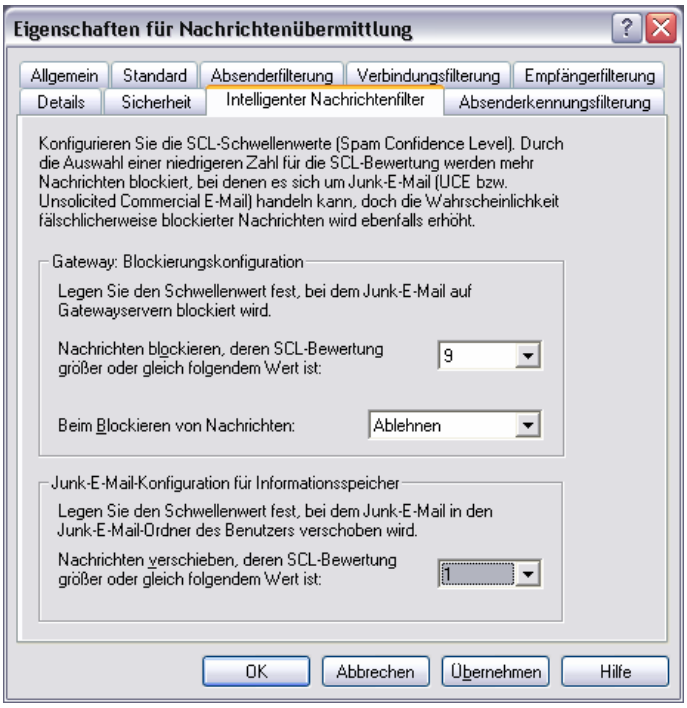


Abb. Intelligenter Nachrichtenfilter (IMF)

Der IMF wird auf oberster Ebene der Exchange-Organisation definiert, dieser muss auf jedem virtuellem SMTP-Server in den administrativen Gruppen explizit übernommen werden. (*Siehe auch Anlage C2 Merkblatt unerwünschte E-Mail*)

Aktivieren der Nachrichtenprotokollierung pro Exchange Server

Das Einschalten der Protokollierung auf Mitgliedsservern der Exchange Organisation ist Standardvorgabe.

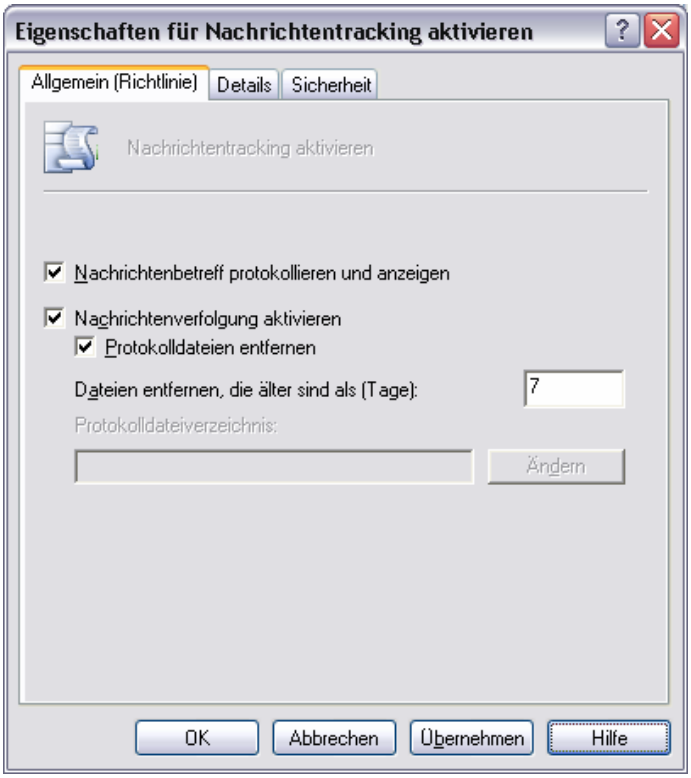


Abb. Nachrichtenprotokollierung

Postfachgrenzen pro Exchange Server und pro Postfachspeicher

Die Definition von Postfachgrenzen ist wesentlicher Bestandteil des Gesamtkonzeptes der Nachrichtenverarbeitung innerhalb der Exchange-Organisation. Nur durch Definition und Zuweisung von Postfachgrenzen kann sichergestellt werden, dass vorhandene und zugewiesene Ressourcen verwaltet und administriert werden können. Grenzwerte müssen definiert werden, jedoch ist der jeweilige Grenzwert abhängig von den verfügbaren Ressourcen und der Anzahl der Nutzer, die auf dieses Ressourcen zugreifen. Eine Systemrichtlinie für Postfachgrenzen wird daher als Standard vordefiniert und dem entsprechenden Postfachspeicher zugewiesen,

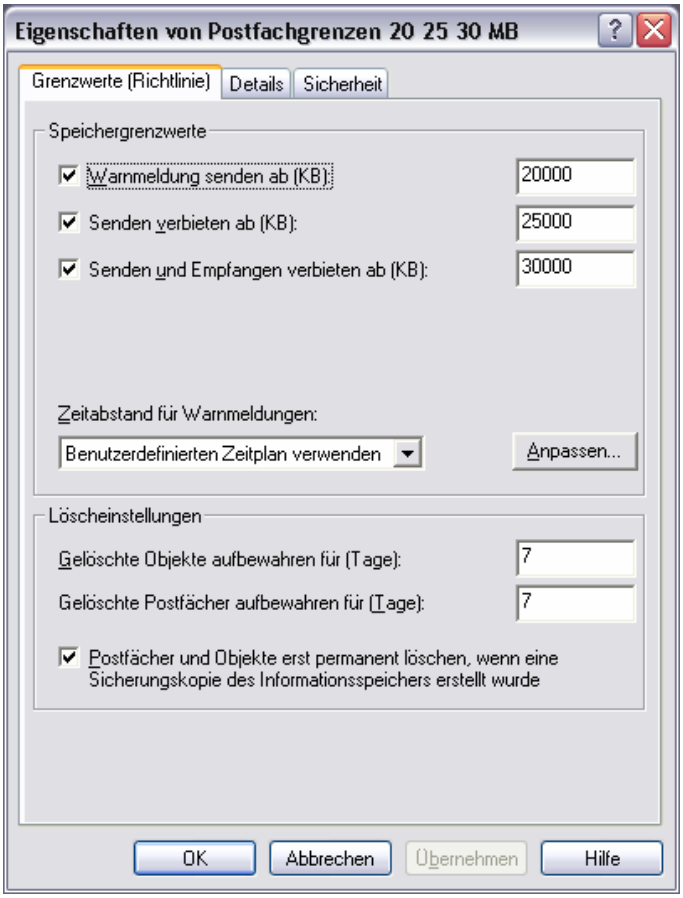


Abb. Postfachgrenzen

Wichtiger Bestandteil dieser Systemrichtlinie ist die Definition der Löscheinstellungen. Die Aufbewahrungsdauer gelöschter Objekte, bestimmt die Zeitdauer in der gelöschte Objekte aus dem Postfach der Nutzer weiterhin auf dem jeweiligen Exchange Server im Postfachspeicher aufbewahrt werden, bevor eine vollständige Löschung der Objekte durch den Exchange Server selbst ausgeführt wird. Nutzer die über Client Komponenten auf ihr Postfach auf dem Exchange Server zugreifen und Objekte aus ihrem Postfach löschen, bekommen diese Objekte über ihre Client Komponente auch nicht mehr angezeigt, jedoch werden diese gelöschten Objekte noch mind. 7 Tage (*Exchange Standard*) im Postfachspeicher aufbewahrt, somit ist eine Wiederherstellung versehentlich gelöschter Objekte relativ einfach möglich. Darüber hinaus ist es möglich, bereits im Active Directory gelöschte vollständige Postfächer ebenfalls innerhalb einer zu definierenden Zeitspanne *(hier ebenfalls 7 Tage Exchange Standard*) ohne administrativen Aufwand wiederherzustellen. Die Dauer der jeweiligen Aufbewahrungsfrist ist abhängig von den verfügbaren Ressourcen. Die Notwendigkeit der Definition dieser Aufbewahrungsfrist begründet sich vor allem in den abgeschlossenen Servicevereinbarungen mit dem Endanwender hinsichtlich Wiederherstellungs- und Verfügbarkeitszeiten von Postfachinformationen.

Nahtlos daran anschließend ist die Option, Postfächer und einzelne Objekte erst permanent zu löschen, wenn hiervon mindestens jeweils eine Sicherungskopie erstellt wurde. Ohne diese Sicherung wäre eine Wiederherstellung überhaupt nicht möglich.

Grenzen für Öffentliche Ordner pro Exchange Server und pro Informationsspeicher für Öffentliche Ordner

Adäquat zu den definierten Grenzen für einzelne Postfachspeicher verhält sich die Definition für den Informationsspeicher für Öffentliche Ordner. Dieser Informationsspeicher existiert im Unterschied zum Postfachspeicher, jeweils nur einmal pro Exchange Server. In diesem Informationsspeicher werden die Struktur der Öffentlichen Ordner der aktuellen administrativen Gruppe und replizierte Ordnerstrukturen anderer administrativer Gruppen für eine übergreifende Zusammenarbeit verwaltet.

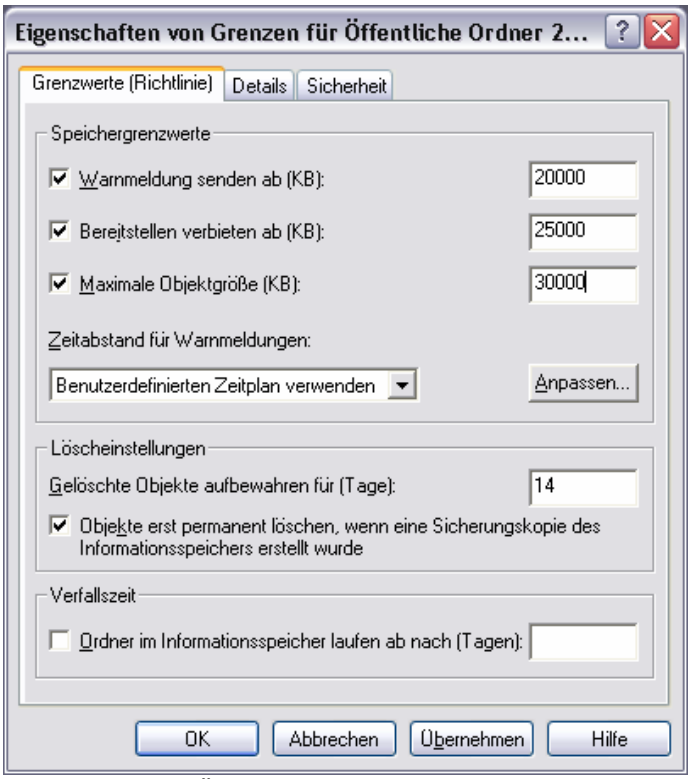


Abb. Grenzen Öffentlicher Ordner

Virtueller Standardserver für SMTP pro Administrative Gruppe

Beschränkungen die über die Eigenschaften eines virtuellen SMTP-Servers definiert werden, überschreiben nicht die Beschränkungsvorgaben der Exchange Organisation. Änderungen werden nur wirksam, wenn die Größenangaben unterhalb der Organisationsvorgaben liegen.

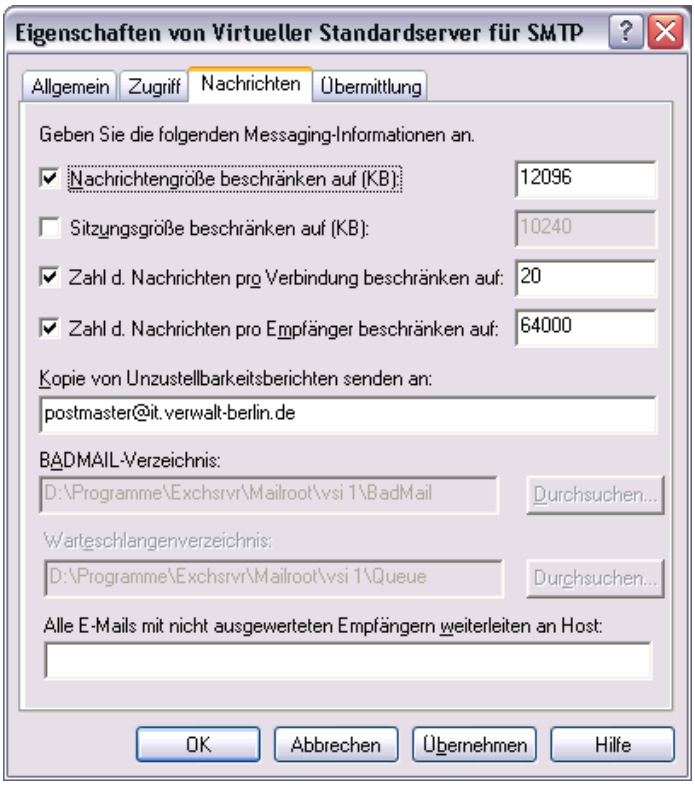


Abb. Virtueller SMTP-Server

Ebenfalls muss auf den Eigenschaftsseiten des virtuellen SMTP-Server die Übernahme der auf der Ebene der Exchange Organisation definierten Filterregeln explizit ausgewählt werden, damit diese vordefinierten Regeln auch greifen können.

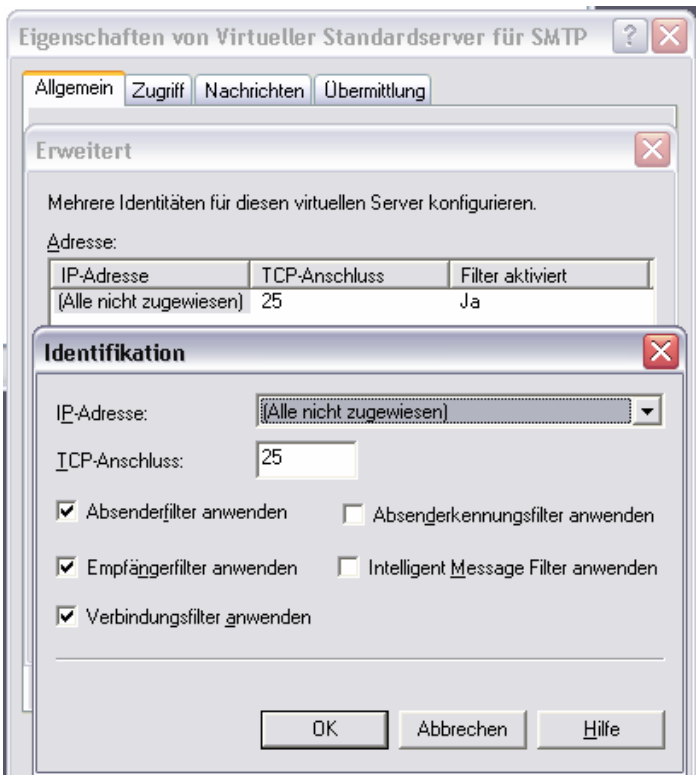


Abb. Filteraktivierung

Beschränkungen für mailaktivierte Active Directory Objekte

Änderungen an Active Directory Objekten (Nutzer, Gruppen, Ordner) werden nicht über das Verwaltungstool Exchange System-Manager sondern über das Verwaltungstool Active Directory Benutzer und Computer realisiert. Vor allem Grenzwerte und Aufbewahrungsfristen für Nachrichten können über dieses Tool zusätzlich geändert werden. Dies jedoch erhöht den administrativen Verwaltungsaufwand und erschwert eine einheitliche Verwaltung der Objektkonten.

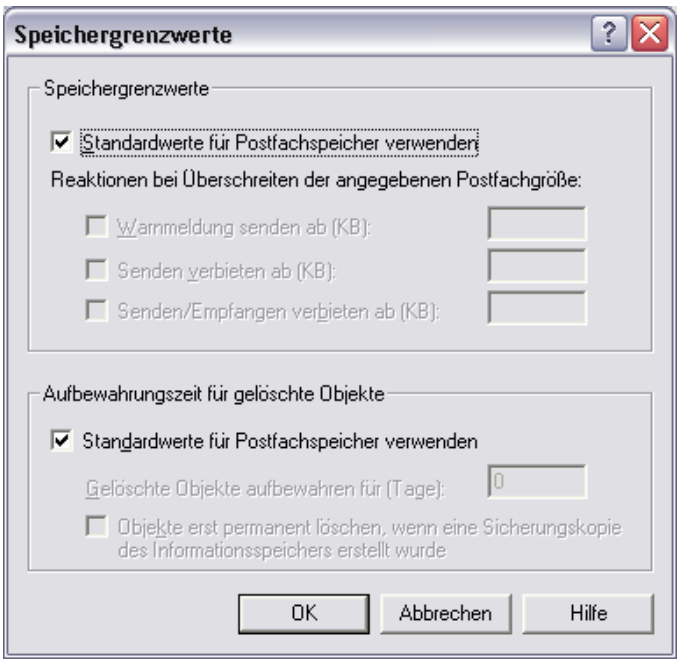


Abb. Benutzer Speichergrenzwerte

In der Abbildung Benutzer Speichergrenzwerte kann der Standardwert für die Postfachgröße, sowie die Dauer der Aufbewahrungsfrist überschrieben werden.

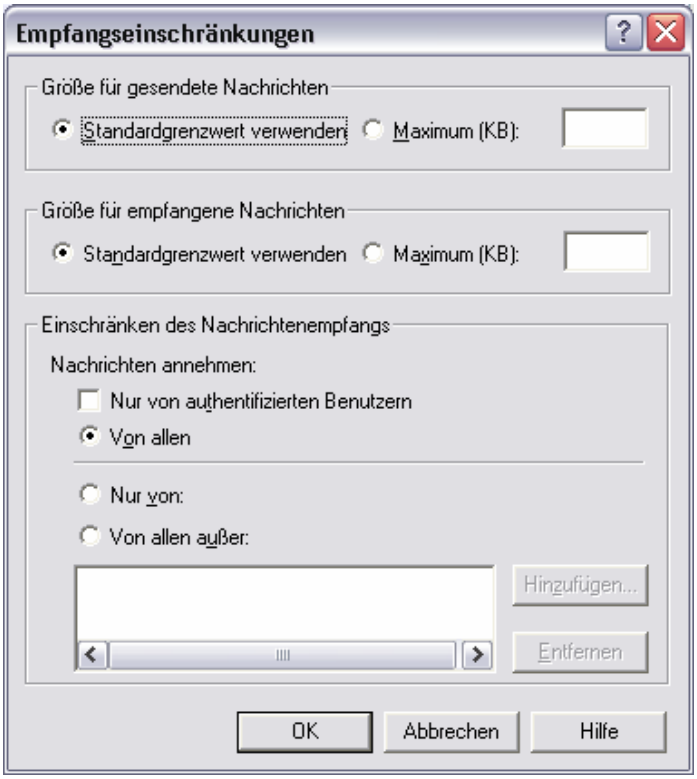


Abb. Benutzer Empfangseinschränkungen

Im Dialog Empfangseinschränkungen können die Werte für gesendete und empfangene Nachrichten von Hand angepasst werden, überschreiten diese angepassten Werte jedoch die Größenbeschränkungen der Exchange-Organisation (*hier Standardgrenzwert genant*) werden diese neue Werte nicht akzeptiert, d.h. hier von Hand eingetragene Größen können nur unterhalb der Standardgrenzen liegen.

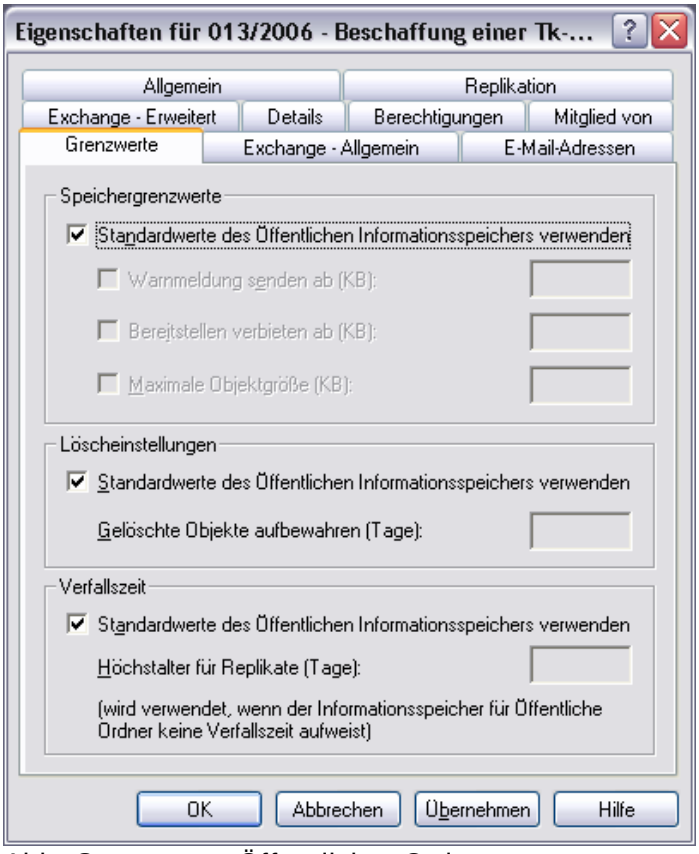


Abb. Grenzwerte Öffentlicher Ordner

Analog zu den Grenzwerten eines Benutzers können die Standardgrenzwerte für andere mailaktivierte Objekte wie z.B. Öffentliche Ordner ebenfalls per Hand angepasst werden. Ein Überschreiben der Standardwerte ist möglich, jedoch wird dies nicht unterstützt.
Für die Löscheinstellungen und Verfallszeiten können entsprechende Beschränkungen über die konfigurierten Standardwerte hinaus definiert werden.

Anlage B2.1 : Beschreibung der personenbezogenen Daten

Benutzerobjekte im Active Directory sind einer physisch vorhandenen Person zugeordnet. Diese Objekte werden als Sicherheitsprincipals bezeichnet, denen eine Sicherheitskennung zugewiesen ist. Objekte mit Sicherheitskennung können sich am Netzwerk anmelden und auf Domänenressourcen zugreifen.
Das Benutzerobjekt im Active Directory ist eines der zentralen Objekte die maßgeblich durch Umfang und Qualität der Datenerfassung für dieses Objekt, den Inhalt und den Funktionsumfang des gesamten Active Directory beeinflussen. Als zentrales Element der Datenhaltung ist das Active Directory für die Bereitstellung der Benutzerobjekt-Informationen im gesamten Netzwerk verantwortlich.

Personenbezogene Daten im Überblick

Im Active Directory besteht das Benutzerobjekt aus zahlreichen Attributen. Von dieser Vielzahl an Attributen wird im Active Directory der Berliner Verwaltung nur ein Bruchteil mit Informationen gefüllt.
Folgenden Attributen eines Benutzerobjektes werden zur eindeutigen Zuordnung zu einer physischen Person ein oder mehrere Datenwerte zugewiesen. Die Attribute eines Benutzerobjektes lassen sich in folgende Kategorien einteilen:

- Attribute zur Identifizierung eines Benutzerobjektes und
- Anwendungsorientierte Attribute eines Benutzerobjektes (**Fett**)

Attribut	Eintrag	Bemerkung
Vorname	Vorname des Benutzers	mit Bindestrich zwischen mehreren Vornamen
Nachname	Nachname des Benutzers	mit Bindestrich zwischen mehreren Nachnamen
Anzeigename	Globale Adressbuchansicht	Der Anzeigename wird generell in der Form Nachname Titel von, Vorname eingetragen.
Büro	Raumnummer des Benutzers am Arbeitsort.	
Rufnummer	Telefonnummer des Benutzers am Arbeitsort	z.B. 9012(912) – 6666
E-MailAdresse	Vorname.Nachname@Verwaltung	mehrere Einträge möglich
Strasse; PLZ; Stadt; Land	Adresse des Arbeitsortes des Benutzers.	
Anrede	Stellen-/Bearbeiterzeichen des Benutzers	
Abteilung	Abteilungsbezeichnung, in der der Benutzer tätig ist.	Kein Pflichtfeld
Firma	Behördenabkürzung, in der der Benutzer tätig ist.	z. B. LEA
Benutzeranmeldename	Windows Anmeldename	Authentifizierung an der Domäne
Postfachspeicher	Ablageort des Postfaches	Physikalischer Ablageort der Postfachinformationen
Alias	Verknüpfungsattribut zwischen Active Directory und Exchange	Verbindung zwischen Abnmeldename und Postfach
Benutzerdefinierte Attribute 9,10	Unified Messaging (UMS) Attribute	Fax, Voice und SMS Erweiterungen

Abbildung 1 Tabellarische Übersicht der Benutzerattribute

Zusätzlich zum Benutzerobjekt werden im Active Directory für Personen die sich nicht im Active Directory authentifizieren (*Kunden, Lieferanten etc*.) Kontaktobjekte angelegt. Inhalt und Umfang der zu erfassenden Daten unterscheidet sich vom Benutzerobjekt nur dadurch, dass eine Authentifizierung im Active Directory mit einem Kontaktobjekt nicht möglich ist, der Umfang der erfassten Informationen ist jedoch gleich zusetzen..

Verarbeitung der Attribute zur Identifizierung eines Benutzerobjektes

Vorname, Nachname, Namenszusätze
Diese Attribute dienen der Identifizierung einer Person beim Eintragen in das Active Directory, sowie bei der Generierung von Basisdaten wie E-Mail-Adresse und Benutzeranmeldename.

Strasse, PLZ, Stadt, Land
Die Adresse besteht aus den Attributen Straße, Postleitzahl, Stadt und Land. Sie dient der Abspeicherung der dienstlich gemeldeten Postadresse eines Benutzerobjektes auch zur Identifizierung im globalen Adressbuch.

Büro
Das Attribut identifiziert einen Raum der Verwaltung / Behörde der dem Beschäftigten als Arbeitsplatz zugeordnet ist. Das Attribut unterstützt die Koordinierung der Verwaltung von Benutzern und technischen Ressourcen, inklusive dem Netzwerkmanagement.

Rufnummer
Das Attribut enthält die dienstliche Telefonnummer, unter der ein Beschäftigter zu erreichen ist. Die Verwendung dieses Attributes reicht vom Eintrag in das globale Adressbuch bis hin zum Facility Management im Zusammenhang mit der Bereitstellung von Telekommunikationsressourcen.

Anrede
Das Attribut Anrede enthält Stellen- und oder Bearbeiterkennzeichen für die jeweilige Person in ihrer entsprechenden Organisationseinheit. Aus diesen Werten sind vor allem Rechte und notwendige Ressourcen in den jeweiligen Organisationseinheiten ableitbar.

Firma, Abteilung
Die Attribute enthalten Werte für die Funktionen bzw. Positionen einer Person innerhalb des Kontexts der jeweiligen Verwaltung / Behörde. Aus diesen Werten lassen sich Rollen, Rechte und benötigte Ressourcen ableiten. So wird unter anderem die Möglichkeit, in Abhängigkeit von der Zugehörigkeit zu einem bestimmten Wert im Attribut Firma die Hauptmailadresse der Person generiert.

Verarbeitung der anwendungsorientierten Attribute eines Benutzerobjektes

Authentifizierung eines Benutzers (Benutzeranmeldename)
Jeder physisch vorhandenen Person ist im Active Directory ein Benutzerobjekt zugeordnet. Über dieses Objekt authentifiziert sich die physische Person gegenüber dem zugeordneten Domänencontroller im Netzwerk mit Eingabe eines Benutzeranmeldenamens und eines Passwortes. Benutzeranmeldenamen sind eindeutig.

E-Mail Adresse
Im Active Directory gilt ein Objekt (Benutzer, Kontakt, Verteilerliste, Öffentlicher Ordner) als mailaktiviert wenn für dieses Objekt mindestens eine E-Mail Adresse definiert ist. Postfachaktivierten Objekten hingegen muss tatsächlich im Active Directory ein Postfach zugeordnet sein. Nur einem Benutzerobjekt kann im Active Directory ein Postfach zugewiesen werden. Einem Benutzerobjekt können jedoch auch mehrere E-Mail Adressen zugewiesen werden, jedoch ist immer nur einer dieser E-Mail Adressen seine SMTP-Hauptadresse (Absenderadresse).

Globales Adressbuch (Anzeigename)
Das globale Adressbuch gewährleistet im Active Directory die Auswahl / Suche von Benutzerobjekten zum Zwecke der weiterführenden Kommunikation (*Mailverkehr, Telefonie*) zwischen einzelnen Benutzern und Benutzergruppen. Ausschließlich mailaktivierte Objekte können in diesem globalen Adressbuch angezeigt werden.

Postfachzugriff
Jedem Benutzerobjekt im Active Directory kann nur genau ein Exchange Postfach zugewiesen werden. Über diese bereitgestellte Postfachressource, kann ein Benutzerobjekt aktiv am System der Nachrichtenverarbeitung und der Plattform für übergreifende Zusammenarbeit teilhaben. Sicherheitsprincipals gewährleisten hierbei die Identität des jeweiligen Benutzerobjektes anderen Benutzerobjekten gegenüber. Im Active Directory wird ein Alias Attribut verwendet um das entsprechende Postfach dem jeweiligen Benutzer zu zuordnen.

Postfachressource
In einer Active Directory Gesamtstruktur mit integrierter Exchange-Organisation kann der physikalische Ablageort der Postfachinformationen auf einem beliebigen Exchange Server der Organisation erfolgen. Nur das Benutzerobjekt selbst, besitzt ein Attribut Postfachspeicher, im dem dieser Ablageort näher beschrieben ist.

Benutzerdefinierte Attribute
Benutzerdefinierte Attribute im Active Directory haben die Aufgabe zusätzlich, über das bereits vorhandene Maß an definierten Objektattributen für den einzelnen Benutzer hinaus, weitere Informationen über Benutzer zu speichern. Diese Attribute sind wahlfrei und erlauben somit eine zusätzliche Definition von erforderlichen Merkmalen. Im Active Directory der Berliner Verwaltung werden diese Attribute (9,10) für die integrierte Unified Messaging Lösung (UMS) benutzt. Diese Lösung stellt SMS, FAX und Voice-Mail über

Zugriffskontrolle auf Domänenressourcen
Dem Benutzerobjekt ist die korrespondierende Zugriff Control List (ACL) zugeordnet. Über diese eindeutige Zuordnung gewährleistet Active Directory den Zugriff oder das Verwehren von oder auf Ressourcen (*Filesystem, Peripherie und andere Netzwerkressourcen*).

Verwaltung anderer Sicherheitsprincipals
Benutzerobjekte im Active Directory werden zur Verwaltung / Administration der gesamten Netzwerkumgebung genutzt. Dementsprechend können Benutzerobjekte (*administrative Benutzerobjekte*) andere Benutzerobjekte (*Sicherheitsprincipals*) zum Zugriff auf bestimmte Ressourcen im gesamten Netzwerk direkt administrieren, d.h. Benutzerattribute hinzufügen, ändern oder löschen, den Zugriff auf das Filesystem einschränken oder erweitern, Ressourcen (*Software, Drucker, Scanner u.ä.*) verfügbar machen oder entziehen.

Überwachungsaufgaben
Die vollständige Steuerung der Netzwerkumgebung über Sicherheitsprincipals und korrespondierende Zugriffs Control Listen auf Netzwerkressourcen stellt auch die Möglichkeit der Überwachung nicht autorisierter Zugriffe auf Netzwerkressourcen in Form von Protokolleinträgen im Ergebnis definierter und aktiver Überwachungsrichtlinien im Netzwerk dar.

Anlage B4.2 : Berechtigungskonzept

Berechtigungsdefinitionen in der Exchange Organisation

Die Exchange-Organisation unterstützt den Betrieb mehrerer Exchange Server in großen Umgebungen. Innerhalb der Exchange-Organisationen besteht die Anforderung, die administrativen Berechtigungen zu delegieren und zu trennen. Die Exchange Organisation trägt diesen Anforderungen Rechnung, indem die Organisation durch die Bildung von administrativen Gruppen eine Delegierung von Berechtigungen erlaubt. (*Siehe auch Anlage C1 Antwort auf Anfrage des Berliner DSB*).

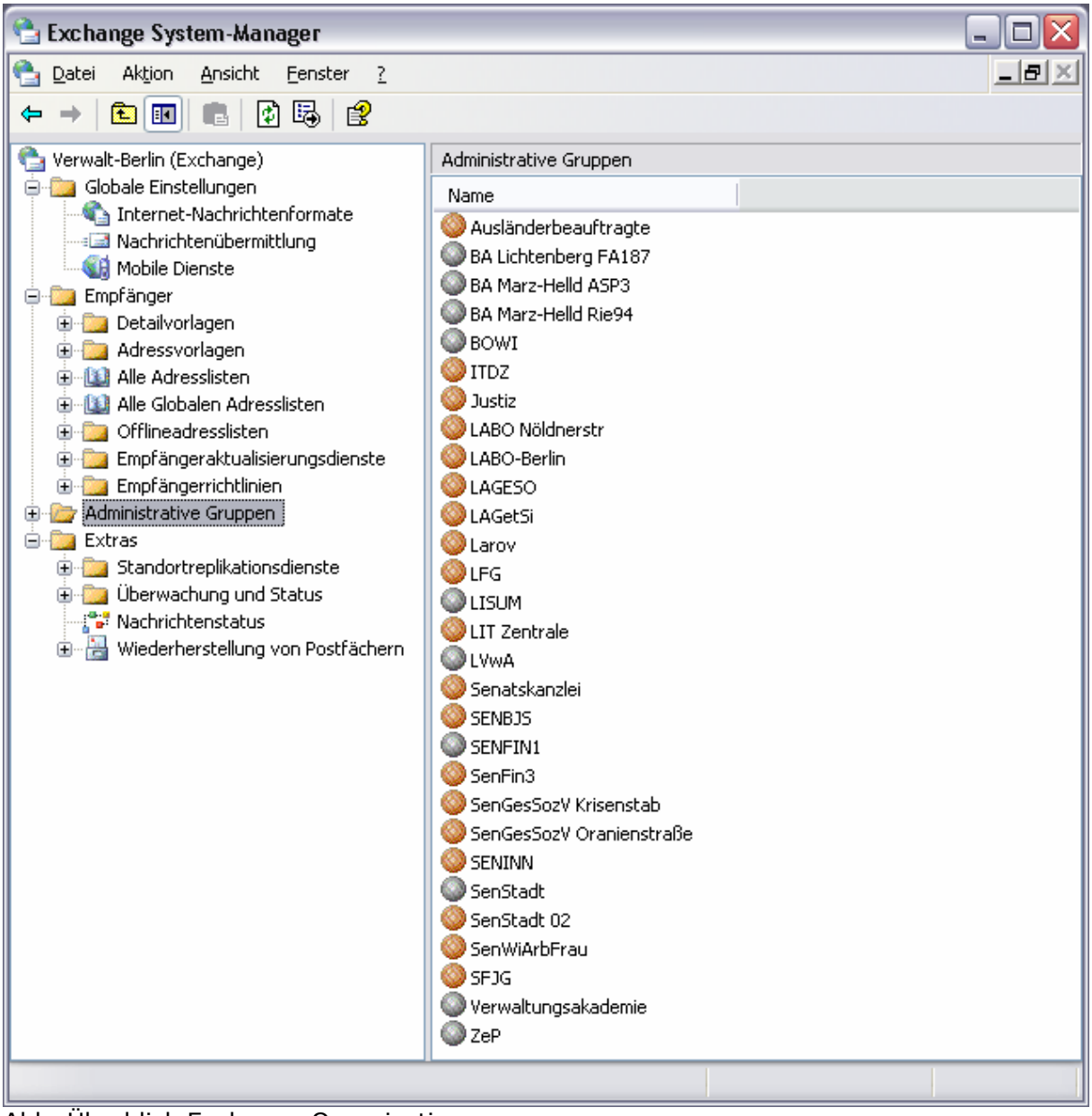


Abb. Überblick Exchange Organisation

Exchange Daten und Active Directory

Zwischen Exchange-bezogenen Berechtigungen und dem Active Directory-Verzeichnisdienstes bestehen unmittelbare Zusammenhänge. In Active Directory ist die Datenspeicherung in drei logische Segmente unterteilt, die als Namenskontexte bezeichnet werden. Die Änderungen in jedem Namenskontext werden getrennt zwischen

denjenigen Domänencontrollern repliziert, die innerhalb der Gesamtstruktur Kopien (Replikate) desselben Namenskontextes speichern:

- Schemanamenskontext
- Konfigurationsnamenskontext
- Domänennamenskontext

Die Namenskontexte und ihre Inhalte können mit dem Verwaltungstool „ADSI-Bearbeitung" angezeigt werden.

Schemanamenskontext

In jeder Gesamtstruktur ist nur ein Schemanamenskontext vorhanden. Der Schemanamenskontext enthält die Definitionen aller Objekte, die in Active Directory instanziiert werden können. Zusätzlich werden in diesem Kontext die Definitionen aller Attribute gespeichert, die in Active Directory Teil von Objekten sein können. Jeder Domänencontroller verfügt über eine Kopie der Schemaverzeichnispartition mit uneingeschränktem Schreibzugriff. Schemaaktualisierungen sind jedoch nur auf dem Domänencontroller zulässig, der als Betriebsmaster für das Schema agiert.
Das Stammobjekt des Schemanamenskontextes enthält ein untergeordnetes Objekt für jede Klasse von Objekten, die in der Active Directory-Gesamtstruktur instanziiert werden können, sowie ein Objekt für jedes Attribut, das Teil eines Objekts in der Active Directory-Gesamtstruktur sein kann.
Exchange Server ab der Version 2000 aufwärts erweitern das Schema, so dass Exchange-Objekte (z. B. E-Mail-aktivierte Empfänger und Exchange-Datenbanken) in der Organisation instanziiert werden können. Es sind keine Exchange-bezogenen Berechtigungen erforderlich, um das Schema zu erweitern. Diese Funktion steht ausschließlich den Schemaadministratoren in der Gesamtstruktur zur Verfügung.

Konfigurationsnamenkonzept

In jeder Gesamtstruktur ist nur ein Konfigurationsnamenskontext vorhanden, in dem Konfigurationsdaten für die Gesamtstruktur gespeichert werden, die für die einwandfreie Funktion von Active Directory als Verzeichnisdienst erforderlich sind. So werden beispielsweise alle für Replikationsvorgänge erforderlichen Informationen in der Konfigurationspartition gespeichert, die außerdem zur Standorttopologie gehörige Informationen enthält. Informationen, die Active Directory zum Erstellen der Verzeichnisstrukturhierarchie verwendet, werden in der Konfigurationspartition gespeichert, ebenso wie netzwerkweite, dienstspezifische Informationen, die Anwendungen zum Herstellen von Verbindungen zu Dienstinstanzen in der Gesamtstruktur benötigen. Jeder Domänencontroller verfügt über eine Kopie der Konfigurationspartition mit uneingeschränktem Schreibzugriff.
Von Exchange innerhalb des Konfigurationsnamenskontextes gespeicherte Daten werden vor nicht autorisierten Zugriffen durch die Sicherheitsberechtigungen geschützt, die mit dem Assistenten für die Zuweisung von Verwaltungsberechtigungen auf Exchange-Objekte innerhalb des Exchange-System-Managers konfiguriert wurden.
Enterprise-Administratoren und Domänenadministratoren der Stammdomäne können Exchange-bezogene Funktionen begrenzt durchführen, ohne dass mit dem Assistenten für die Zuweisung von Verwaltungsberechtigungen auf Exchange-Objekte Rechte gewährt werden müssen. Folgende Berechtigungen sind diesen Sicherheitskontexten nicht zugewiesen: „Vollzugriff", „Untergeordnete Objekte löschen", „Struktur löschen" und „Keine speziellen Berechtigungen". Domänenadministratoren der Stammdomäne und Enterprise-Administratoren können z. B. Exchange-Informationsspeicher bereitstellen oder deren Bereitstellung aufheben.

Domänennamenskontext

Jede Domäne wird im Active Directory durch einen Domänennamenskontext dargestellt. Im Domänennamenskontext werden Benutzer, Computer, Gruppen und andere Objekte für die jeweilige Domäne gespeichert. Alle Domänencontroller, die Mitglied der Domäne sind, verfügen über eine Kopie der Domänenverzeichnispartition mit uneingeschränktem

Schreibzugriff. Zusätzlich befindet sich auf allen Domänencontrollern in der Gesamtstruktur, die den globalen Katalog verwalten, auch eine schreibgeschützte partielle Kopie aller anderen Domänennamenskontexte in der Gesamtstruktur. Die Hauptaufgabe des Domänennamenskontextes besteht darin, Domäneninhalte zu speichern, d. h. Informationen zu Benutzern, Gruppen und Computern. Ebenso werden einige domänenspezifische Konfigurationsdaten im Systemcontainer der Domänenpartition gespeichert.
E-Mail-aktivierte Empfänger aus Exchange Server ab Version 2000 aufwärts werden im Domänennamenskontext gespeichert. Daher sind zum Bearbeiten E-Mail-aktivierter Empfänger ggf. Berechtigungen für das Objekt und innerhalb der Exchange-Organisation erforderlich.

Exchange Funktionen und Berechtigungen

Exchange differenziert bei der Vergabe von Berechtigungen zwischen, den Rechten auf die Exchange-Organisation, auf die Administrativen Gruppen (*Exchange Server*) und auf die Exchange aktivierten Objekte (*Benutzer, Kontakte, Verteiler etc*).
Hierzu wird ein dreistufiges Berechtigungsmodel mittels des Verwaltungstool „Exchange-System-Manager" durchgesetzt, in deren Ergebnis die Berechtigungen durch Vererbung auf darunter befindliche Objekte weitegereicht werden.

- **Exchange-Administrator – Nur Ansicht**

  Der Benutzer bzw. die Gruppe kann sämtliche Exchange Server-Computerinformationen einsehen. Ein als „Exchange-Administrator – Nur Ansicht" eingerichteter Sicherheitskontext verfügt über die folgenden Rechte:

  Rechte innerhalb der Organisation:
  - Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Container MsExchConfiguration (dieses Objekt und untergeordnete Container).
  - Berechtigung „Status des Informationsspeichers anzeigen" für Organisationscontainer (dieses Objekt und untergeordnete Container).

  Rechte der administrativen Gruppe:
  - Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Container MsExchConfiguration (nur dieses Objekt).
  - Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Organisationscontainer (nur dieses Objekt).
  - Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Container Administratorgruppen (nur dieses Objekt).
  - Berechtigungen „Lesen", „Objekt auflisten", „Inhalt auflisten" und „Status des Informationsspeichers anzeigen" für den Container Administratorgruppen (dieses Objekt und untergeordnete Container).
  - Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für die Container MsExchRecipientsPolicy, Adresslisten, Adressierung, „Globale Einstellungen" und Systemrichtlinien (dieses Objekt und untergeordnete Container).

- **Exchange-Administrator – Administrator**

  Der Benutzer bzw. die Gruppe kann sämtliche Exchange Server-Computerinformationen verwalten. Ein als Exchange-Administrator eingerichteter Benutzer verfügt über die folgenden Rechte:

  Rechte innerhalb der Organisation:
  - Alle Berechtigungen (außer „Ändern") für den Container MsExchConfiguration (dieses Objekt und untergeordnete Container).
  - Verweigern der Berechtigungen „Empfangen als" und „Senden als" für den Organisationscontainer (dieses Objekt und untergeordnete Container).

Rechte der administrativen Gruppe:

- Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Container MsExchConfiguration (nur dieses Objekt).
- Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Organisationscontainer (dieses Objekt und untergeordnete Container).
- Alle Berechtigungen (außer „Ändern", Verweigern der Berechtigungen „Senden als" und „Empfangen als") für den Container Administratorgruppe (dieses Objekt und untergeordnete Container).
- Alle Berechtigungen (außer „Ändern") für den Verbindungscontainer (dieses Objekt und untergeordnete Container).
- Berechtigungen „Lesen", „Objekt auflisten", „Inhalt auflisten" und „Schreiben" für den Container Offlineadresslisten (dieses Objekt und untergeordnete Container).

- **Exchange-Administrator – Vollständig**

  Der Benutzer bzw. die Gruppe kann sämtliche Exchange Server-Computerinformationen verwalten und Berechtigungen bearbeiten. Ein als Exchange-Administrator mit vollständigen Berechtigungen eingerichteter Sicherheitskontext verfügt über die folgenden Rechte:

  Rechte innerhalb der Organisation:

  - Berechtigungen für einen Vollzugriff auf den Container MsExchConfiguration (*dieses Objekt und untergeordnete Container*).
  - Verweigern der Berechtigungen „Empfangen als" und „Senden als" für den Organisationscontainer (dieses Objekt und untergeordnete Container).
  - Berechtigungen zum Lesen und Ändern des Containers für gelöschte Objekte im Konfigurationsnamenskontext (dieses Objekt und untergeordnete Container).

  Rechte der administrativen Gruppe:

  - Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Container MsExchConfiguration (*nur dieses Objekt*).
  - Berechtigungen „Lesen", „Objekt auflisten" und „Inhalt auflisten" für den Organisationscontainer (dieses Objekt und untergeordnete Container).
  - Vollzugriff und Verweigern der Berechtigungen „Senden als" und „Empfangen als" für den Container Administratorgruppen (dieses Objekt und untergeordnete Container).
  - Vollzugriff (außer Ändern) auf den Verbindungscontainer (dieses Objekt und untergeordnete Container).
  - Berechtigungen „Lesen", „Objekt auflisten", „Inhalt auflisten" und „Schreiben" für den Container Offlineadresslisten (*dieses Objekt und untergeordnete Container*).

Berechtigungen auf der Ebene Exchange Organisation

Auf der Ebene der Exchange-Organisation und auf der Ebene der Administrativen Gruppen wird die Objektverwaltung dazu verwendet, Delegierungen von Berechtigungen einzurichten. Objektverwaltung auf der Ebene der Exchange-Organisation erfolgt ausschließlich durch administratives Personal des ITDZ. Das ITDZ ist mit dem Aufbau und dem Betrieb der Exchange-Organisation für das Land Berlin beauftragt, eine Delegierung von Zugriffsrechten an administratives Personal aus anderen Verwaltungen / Behörden erfolgt hierbei grundsätzlich nicht. Der Exchange Sicherheitskontext (*Exchange-Administrator - Vollständig*) wird ausschließlich von dem Objekt (*Nutzer oder Gruppe*) verwaltet, in dessen Kontext der erste Exchange Server in der Exchange-Organisation installiert wurde.

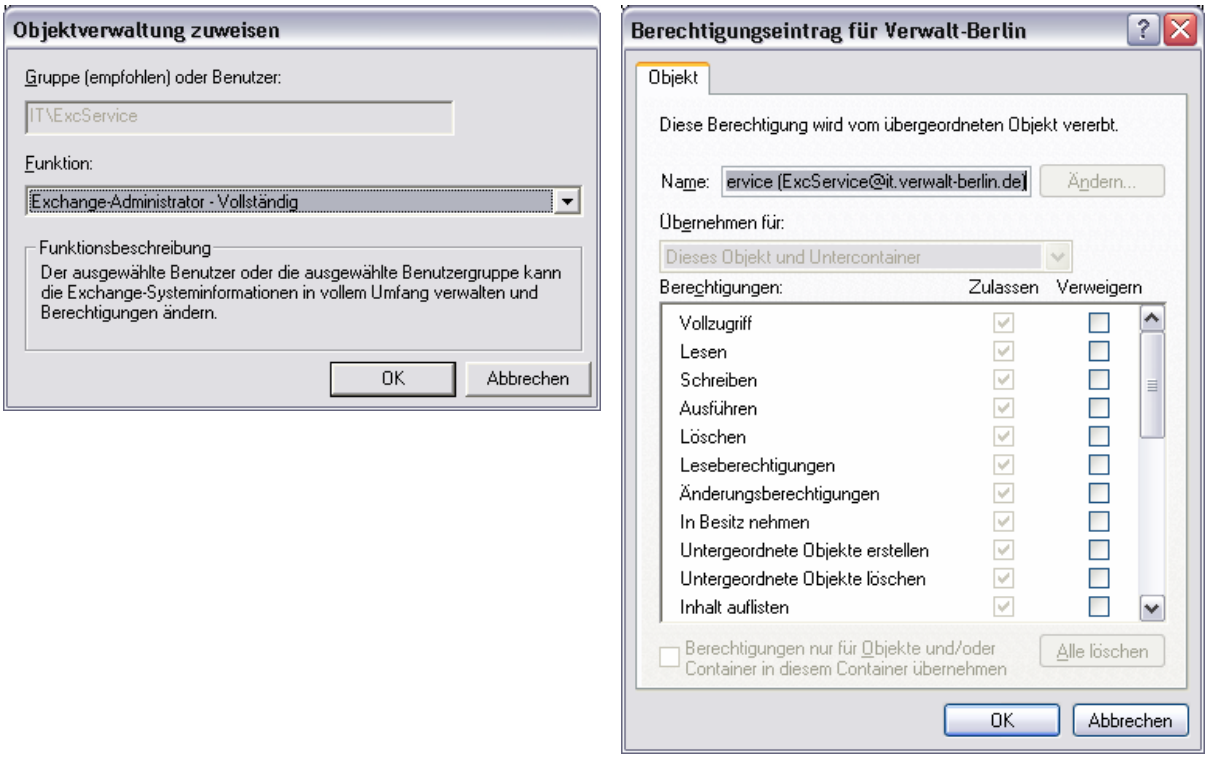


Abb. Exchange-Administrator - Vollständig

Der Berechtigungsfokus für diesen Sicherheitskontext steht auf Vollzugriff (*siehe Abbildung*) für dieses Objekt (Verwalt-Berlin) und Untercontainer (*z.B. Administrative Gruppen*), d.h. dieser Kontext kann Objekte und Container in der Exchange-Organisation administrieren und Berechtigungen vergeben.
Wie bereits weiter oben in dieser Anlage benannt werden, sämtliche Exchange Informationen werden in unterschiedlichen Active Directory Partitionen gespeichert. Der hier beschriebene Sicherheitskontext (*Exchange-Administrator – Vollständig*) auf der Ebene der Exchange-Organisation, hat schreibenden Zugriff (*Vollzugriff*) auf die Exchange Informationen in der Konfigurationspartition (*administrative Gruppen, die Routinggruppen, Exchange Server, Connectoren*) des Active Directory. Die Informationen dieser Partition werden im gesamten Forrest repliziert. Losgelöst von der Konfigurationspartition des Active Directory, speichert Exchange auch Informationen in der jeweiligen Domänenpartition der Hostdomänen im gesamten Forrest. Diese Partition enthält die Informationen der Benutzer, d.h. welcher Benutzer ist mailaktiviert und hat auf welchem Server sein Postfach. Grundsätzlich liest Exchange die Information, welcher Benutzer eine Mailadresse hat und wo dessen Postfach liegt, aus den Domänenpartitionen des Active Directory. Da das Active Directory aus mehreren Domänen besteht, wird der Zugriff auf Informationen über einen vorhandenen / erreichbaren Globalen Katalog Server gelesen, welcher die Konfigurationspartition und eine Teilmenge aller Domänenobjekte (*Domänenpartition*) des gesamten Forrest enthält. Dieser Globale Katalog ist nur "Readonly" verfügbar. Daher werden für Änderungen immer die Schreibrechte auf dem Objekt in der Quelldomäne benötigt. Über derartige Berechtigungen verfügt der Sicherheitskontext (*Exchange-Administrator – Vollständig*) auf der Ebene der Exchange-Organisation grundsätzlich nicht (*Siehe auch Abschnitt Berechtigungen auf E-Mail-aktivierte Objekte und deren Postfachressourcen*).

Berechtigungen auf Administrativen Gruppen

Für die Zuweisung von Berechtigungen auf administrative Gruppen wird grundsätzlich die Objektverwaltung im Exchange-System-Manager verwendet. Unterhalb des Containers „Administrative Gruppen" wird hierbei durch Hinzufügen neuer administrativer Gruppen (*neue Exchange Server*) und einer gleichzeitigen Delegierung (*Objektverwaltung*) von Zugriffsberechtigungen auf diese neuen Gruppen, die dezentrale Administration der Exchange-Organisation durchgeführt.

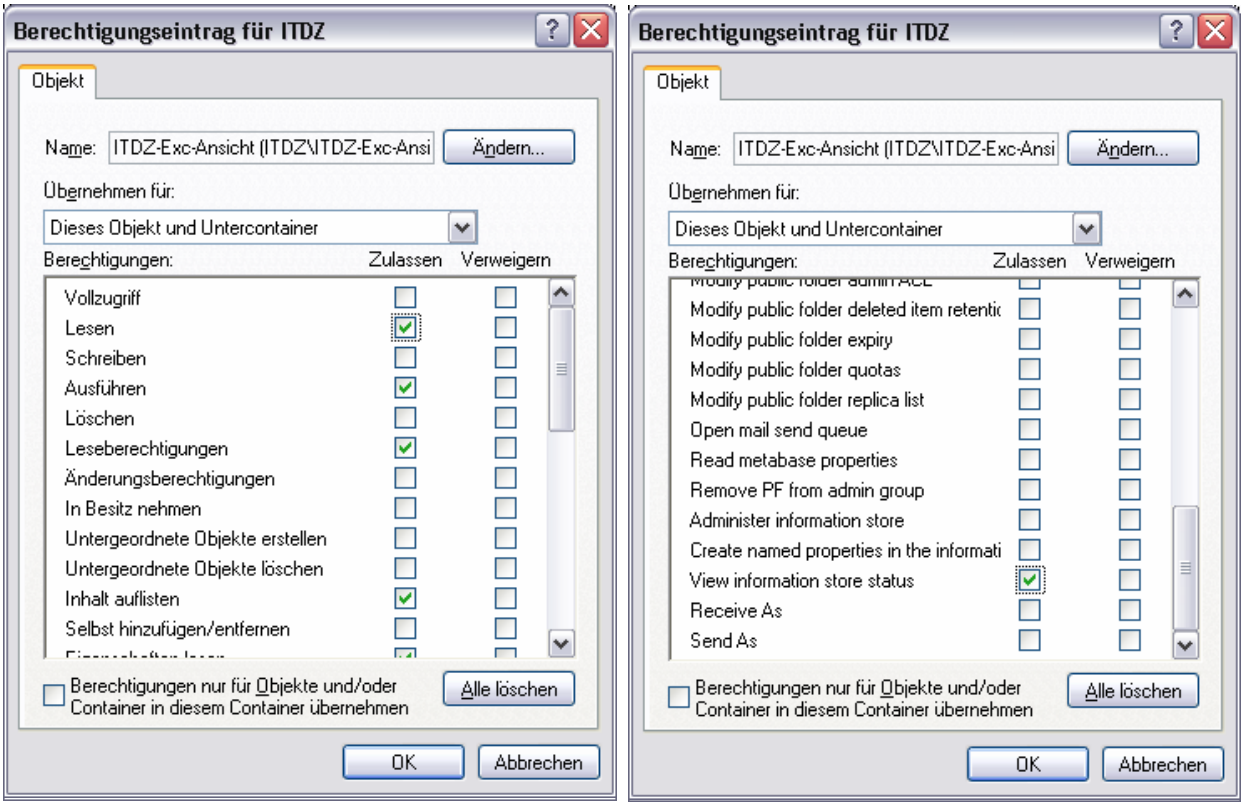


Abb. Exchange Berechtigungsgruppen auf der administrativen Gruppe ITDZ

Die Zuweisung von Berechtigungen über die Objektverwaltung ab der Ebene Administrative Gruppe, beinhaltet für die Berechtigungsgruppe Exchange-Administrator – Vollständig, das Leserecht auf die Konfiguration der Exchange-Organisation einschließlich aller vorhandenen administrativen Gruppen, zuzüglich das Vollzugriffsrecht und das Recht Berechtigungen ab dieser Ebene zu vergeben (*eigene Administrative Gruppe*). Die erforderlichen Berechtigungen zur vollständigen dezentralen Verwaltung ab der Administrativen Gruppe (*hier z.B. ITDZ*) sind damit in der Exchange Organisation gegeben. Dieser neue Sicherheitskontext kann weitere Exchange Berechtigungsgruppen (*Exchange-Administrator und Exchange-Administrator – Nur Ansicht*) über die Objektverwaltung auf dieser Administrativen Gruppe berechtigen.

Zur Komplettierung der Vollzugriffs- und Änderungsrechte für Exchange Berechtigungsgruppen (*Exchange-Administrator – Vollständig und Exchange-Administrator*) müssen für die jeweiligen Sicherheitskontexte die diesen Exchange Berechtigungsgruppen angehören, zusätzlich zwingender weise lokale Administratorberechtigungen auf den jeweiligen Exchange Server Computern eingerichtet werden. Erst die Kombination aus Exchange Berechtigungen und Administratorrechten auf den jeweiligen Servern ermöglichen die Exchangeadministration im geforderten Umfang. Sicherheitskontexte im Rahmen der Exchange Berechtigungsgruppe Exchange-Administrator – Nur Ansicht, verfügen grundsätzlich nur über Leserechte und benötigen hierzu keine lokalen administrativen Rechte auf Server Computer.

Die Zuweisung von Exchange Berechtigungen über die im Exchange System Manager integrierte Objektverwaltung, stellt sicher dass die notwendigen Zugriffsrechte für die

Administration der Exchange Konfiguration den Sicherheitskontexten auf den jeweiligen Ebenen der Exchange-Organisation zugeordnet und weiter vererbt werden. Ebenfalls stellt die Objektverwaltung sicher, das den Sicherheitskontexten der Exchange Berechtigungsgruppen (*Exchange-Administrator – Vollständig und Exchange-Administrator*) der Zugriff auf das Recht „Senden als" und das Recht „Empfangen als" explizit verweigert wird. Mit dieser Zugriffsverweigerung wird per Standard sichergestellt, dass kein Exchange Administrator gleichzeitig zu seinen Exchange Berechtigungen auch Zugriffsrechte auf Nutzerpostfächer und Postfachinhalte erhält.

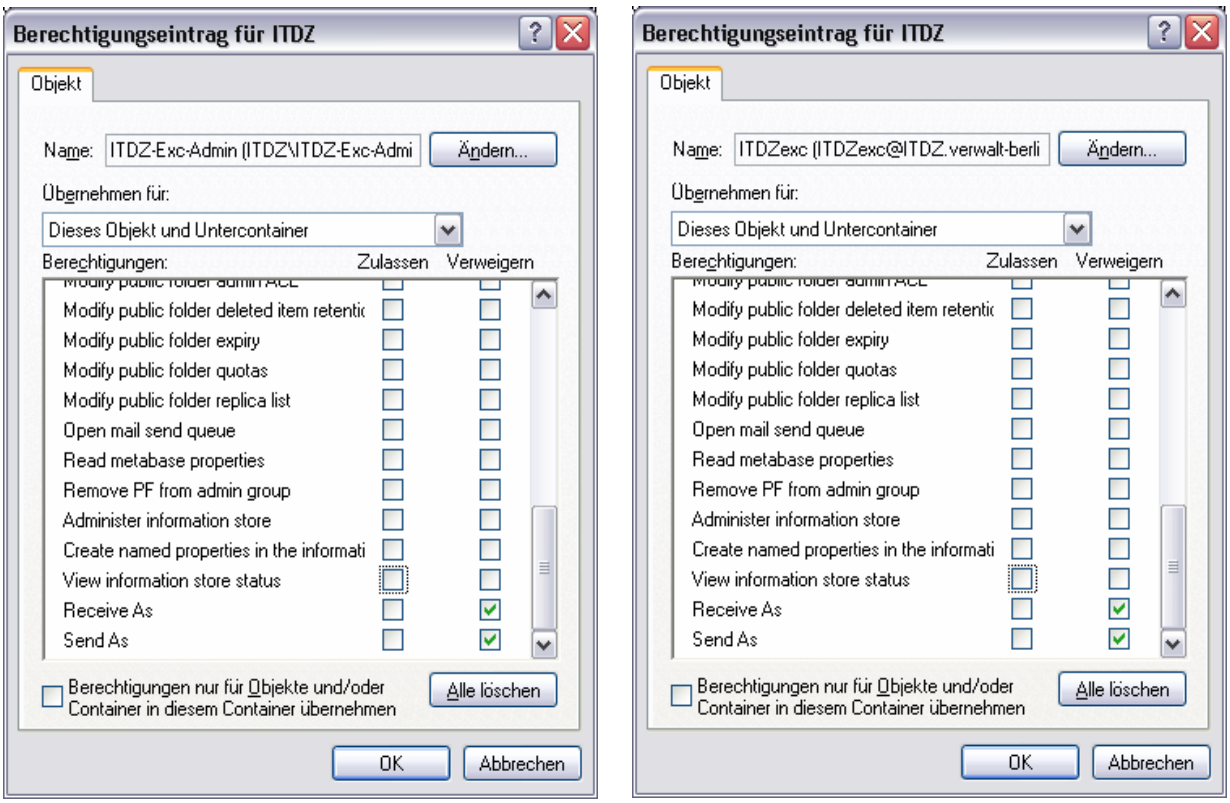


Abb. Standard Verweigerungsrechte

Berechtigungen auf Exchange Servern

Grundlage für eine Exchange Installation auf einer Serverhardware ist ein Windows Server Betriebssystem ab der Version 2000 aufwärts. Es ist zwingend erforderlich, dass die Serverhardware Mitglied einer Active Directory Domäne ist. Exchange Installationen werden durch das ITDZ standardmäßig auf Mitgliedsserver einer entsprechenden Domäne ausgeführt. Die Exchange Installation auf einem Domänencontroller ist hierbei grundsätzlich eine Ausnahme, die nur auf Kundenwunsch hin in kleineren Umgebungen ausgeführt wird. Gegen eine Installation auf einem Domänencontroller, spricht vor allem ein dabei entstehendes Sicherheitsrisiko (*Domänen-Administratoren sind lokale Administratoren auf einem Domänencontroller*). Die Trennung von Domänenverwaltung und Exchange-Verwaltung ist nicht mehr möglich. Exchange ist eine Anwendung, hier finden zahlreiche Updates und Änderungen während des Betriebes statt, die Anzahl der erforderlichen Neustarts eines Exchange-Servers sind wesentlich höher, als die eines Domänencontrollers. Ein Neustart bedeutet auch immer Einschränkung der Redundanz der jeweiligen Domäne.

Auf Mitgliedsservern ist jeder lokale Administrator berechtigt Dienste zu starten und Dienste zu stoppen, Registrierungswerte zu verändern, Dateien auszutauschen usw. Ein lokaler Administrator selbst ist jedoch kein Administrator über die Exchange-Dienste und deren Konfiguration, dies sind Eigenschaften und Berechtigungen die im Active Directory verankert sind. Exchange Installationen auf Mitgliedsservern sind besonders gut geschützt, auf diesen Mitgliedsservern können z.B. Domänenadministratoren ausgesperrt werden und umgekehrt ein lokaler Administrator ist nicht automatisch

Domänenadministrator. Eine Trennung der administrativen Verantwortlichkeit zwischen Domäne und Exchange kann hier sauber vollzogen werden.

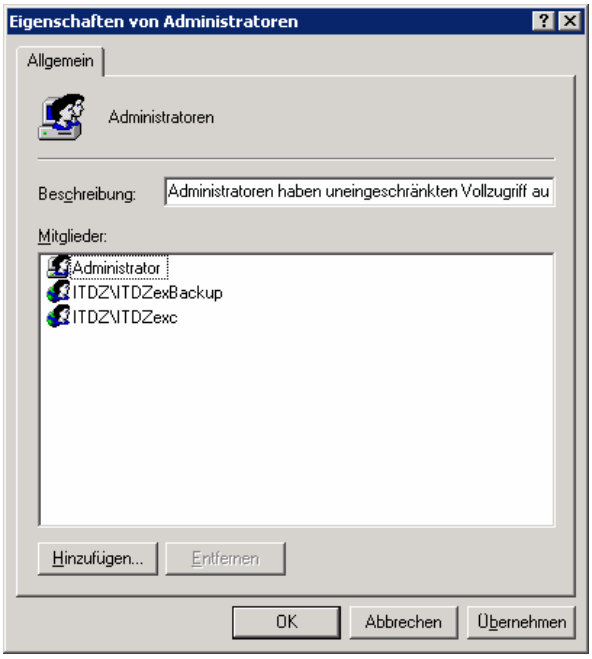


Abb. Lokale Administratoren auf Exchange-Server Computer (hier Server ITDZEX001)

Berechtigungen auf E-Mail-aktivierte Objekte und deren Postfachressourcen

Eine der wesentlichen Neuerungen bei der Einführung von Exchange Server ab Version 2000 aufwärts, gegenüber Exchange 5.5, ist das Vorhandensein restriktiver Standardberechtigungen auf mailaktivierte Objekte und deren Postfachressourcen. Unter Exchange 5.5 konnte z.B. ein Anwender im Sicherheitskontext des Exchange Administrator auch auf alle Postfächer des jeweiligen Standortes per Default zugreifen. Dies ist mit Einführung von Exchange Server ab Version 2000 aufwärts nicht mehr möglich. Zuständig hierfür ist per Standard die Vererbung einer Verweigerung auf das Recht „Senden als" und „Empfangen als" für Exchange Administratoren.
Um explizite Berechtigungen auf mailaktivierte Objekte vergeben zu können, wird das Active Directory Benutzer und Computer Verwaltungstool oder aber Microsoft Outlook als Exchange Client Komponente verwendet. Anwender haben die Möglichkeit über die Client Komponente, ohne Einsatz von Exchange Administratoren, im Rahmen der Selbstverwaltung, anderen Anwendern den Zugriff auf ihr persönliches Postfach durch Definition und Einrichtung von Stellvertreterberechtigungen Zugriff zu ermöglichen. Stellvertreter können je nach Berechtigung auf alle Ordner des Postfaches zugreifen.

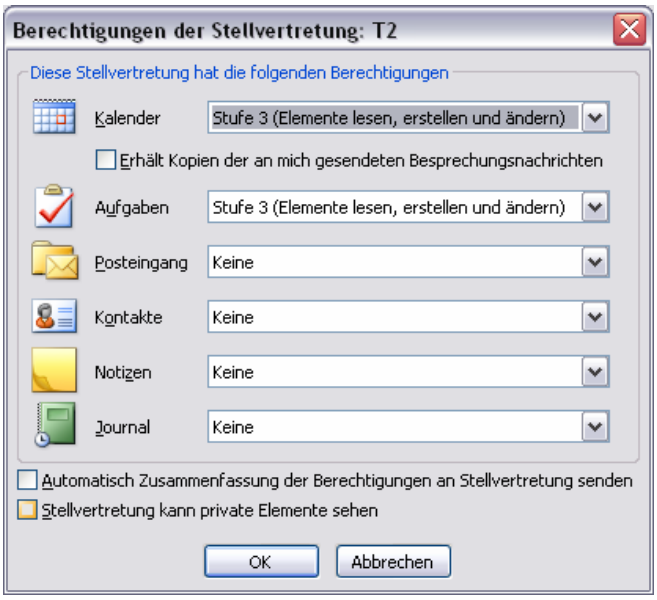


Abb. Stellvertreterberechtigungen in Outlook einzurichten

Wenn es erforderlich ist, das komplette Postfach durch einen anderen Anwender nutzen zu lassen, oder dieses bei einem Anwender mit eingebunden werden soll, dann ist ein Administrator mit Exchangeberechtigungen erforderlich. Mit dem Verwaltungstool Active Directory Benutzer und Computer, muss auf dem Postfach, auf das zugegriffen werden soll, dass entsprechende neue Benutzerkonto als berechtigt eintragen werden.
Während der Exchange Installation auf einem Server Computer werden parallel zur Exchange Applikation auch Verwaltungstools wie der Exchange System Manager und eben auch eine Erweiterung des Actice Directory Standardverwaltungstool Active Directory Benutzer und Computer auf diesem Server installiert. Dieses Verwaltungstool ist ausschließlich auf Servern und Arbeitsstationen vorhanden auf denen die Exchange Verwaltungstools explizit installiert wurden.

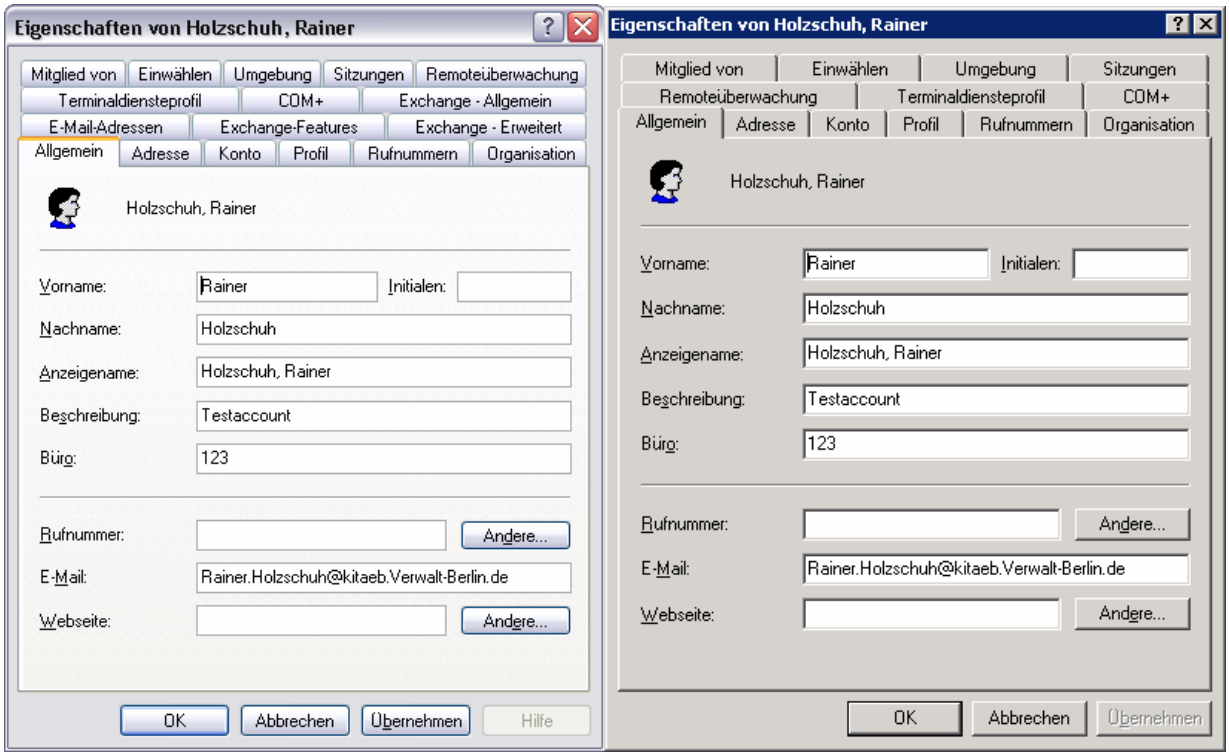


Abb. Active Directory Benutzer und Computer, mit und ohne Exchangeerweiterungen

Auf Servern, wie z.B. Domänencontrollern oder anderen Mitgliedsservern der Domäne sind die Erweiterungen des Exchangeverwaltungstools Active Directory Benutzer und Computer nicht vorhanden, dementsprechend können Exchange relevante Benutzerattribute nicht ohne weiteres durch Domänen Administratoren geändert werden. Exchangeattribute werden durch die Register „Exchange-Allgemein", „Exchange-Erweitert", „Exchange-Feature" und E-Mail-Adressen" verwaltet.

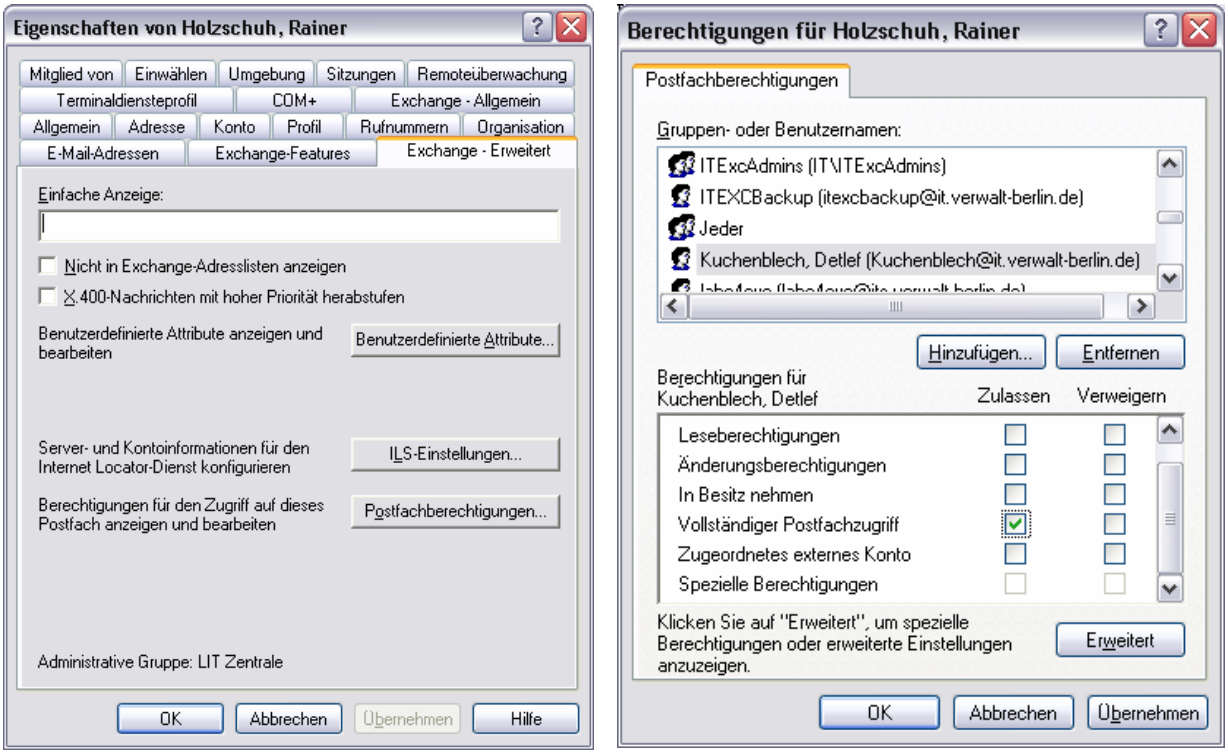


Abb. Berechtigung „Vollständiger Postfachzugriff"

Diese Berechtigungseinstellung kann der eigentliche Besitzer des Postfachs nicht sehen oder ändern, sondern werden vom Administrator vergeben. Diese Einstellung kann jeder Vornehmen, der Administrator über das Benutzerobjekt im Active Directory ist und der Zugriff auf die Exchange Verwaltungstools hat. Allerdings wird hiermit kein Zugriff auf die private Key Informationen des Postfachs eingerichtet und ohne weitere Schritte können keine signierten Mails versendet werden.

Benutzerbezogene Aufgaben

In der Exchange-Organisation müssen Exchange-Administratoren bestimmte allgemeine Aufgaben im Zusammenhang mit Benutzer Objekten durchführen können.

- Aktivieren des Postfachs für Benutzerobjekte
- Verschieben von Postfächern
- Deaktivieren des Postfachs eines Benutzerobjektes
- Aktivieren von E-Mail-Funktionen für Benutzerobjekte
- Deaktivieren von E-Mail-Funktionen für Benutzerobjekte
- Entfernen von Exchange-Attributen

Exchange Administratoren können diese Aufgaben mit dem Assistenten für Exchange-Aufgaben im Exchange- aktivierten Verwaltungstool „Active Directory-Benutzer und –Computer" durchführen.

Anlage B5 : Schulungskonzept

Grundsätzlich ist für die Mehrzahl der Nutzer eines Nachrichtenverarbeitungssystems die jeweilige Client Komponente ausschlaggebend für die tägliche Arbeit. Insofern besteht erstrangig ein Aus- und Fortbildungsbedarf für Nutzer der Microsoft Office Produkte. Die Verwaltungstools der Exchange Organisation selbst, sind nicht Bestandteil von Nutzeroberflächen, sondern Vielmehr ein im Hintergrund zur Nutzung bereitstehender, vom Anwender unabhängiger, Dienst innerhalb des Active Directory.
Für den Anwender besteht kein Schulungsbedarf in der Verwaltung der Exchange Organisation. Die vom Anwender unabhängige Arbeitsweise der Exchange Umgebung ist nur für administratives Personal zugänglich.
Für administratives Personal ist vor allem die Aus- und Fortbildung im Exchange Systemmanager zu schulen.

Schwerpunkt dieser Schulungen ist:

- Active Directory Benutzer und Computer
- Datensicherung und Wiederherstellung von Exchange Installationen
- Virenschutzmechanismen
- Exchange Verwaltungstools

Die Exchange Installation stellt auch eine Vielzahl von neuen und erweiterten Managementwerkzeugen zur Verfügung, deren Handhabung einen Lern- und Trainingsprozess erfordern. Diese Aufgabe kann unterstützend durch fachlich ausgebildetes Administrationspersonal des ITDZ in Form von InHouse – Schulungen bei der Einführung des neuen Nachrichtenverarbeitungssystemes vermittelt werden. Ist dies nicht gewünscht, kann auch der Besuch von offiziell angebotenen Kursen bei Drittanbietern den erforderlichen Wissenstand vermitteln.

Anlage C 1 : Antwort auf Anfrage des Berliner DSB

GB I 2 Sw 17.5.05

Vermerk:

Anfrage des Berliner Beauftragten für Datenschutz und Informationsfreiheit zur datenschutzrechtlichen Bewertung administrativer Konten im Active Directory und im Exchange Verbund der Berliner Verwaltung.

GeschZ 45.438.1 Bearbeiterein Fr. Zabel Datum:29.April 2005

Fachliche und Technische Stellungnahme zum o.g. Schreiben

1. Fachlich technische Grundlagen des Active Directory Services

Active Directory Service ist der Verzeichnisdienst, der seit Einführung des Microsoft Betriebssystem Windows 2000 Server, von Servercomputern mit Domänen Controllern (DC) Funktionalität, zur Verwaltung von Strukturen in Netzwerken genutzt wird.

Das Serverbetriebssystem benutzt hierbei einen Ablageort (Verzeichnis) auf einem oder mehreren DC zum Speichern von Informationen über relevante Objekte. Der Verzeichnisdienst beinhaltet demnach Informationen über nachgeordnete Domänen, in einem Tree und in einem Forest.

Der Verzeichnisdienst stellt Mechanismen für einen sicheren Zugriff auf diese Objekte zur Verfügung und verhindert einen nichtautorisierten Zugriff auf diese Objekte (keine Nutzerdaten).

Dieser Verzeichnisdienst ist ein hierarchischer Namensraum von Objekten, Domänen sind die Basis Containerobjekte im Active Directory.

Active Directory Domänen stellen einen Sicherheitsbereich oder eine -partition dar, weil Zugriffsrechte und Berechtigungen nicht in oder aus diesen Domänen heraus gelöst werden können.

Innerhalb einer Domäne haben Domänen Administratoren (Mitglieder der Gruppe der Domänen-Admins) nicht nur Vollzugriff durch Standardeinstellung, sondern sie haben auch das Recht, den Besitz jedes beliebigen Objektes innerhalb der Domäne zu übernehmen. Es gibt keine Möglichkeit, innerhalb einer Domäne einem Mitglied der Gruppe Domänen Admins oder einem Built-In Administrator daran zu hindern den Besitz an Objekten zu übernehmen. Kein Enterprise Admin kann diese Aufgaben ausführen.

Ein wirkungsvolles Active Directory ist vom Einführen einer OU-Struktur innerhalb der Domäne abhängig, in der durch Delegierung administrativer Zugriff und durch Einsatz effektiver Richtlinien (GPO's) ein administrierbares Domänenumfeld geschaffen wird.

Ein Tree innerhalb des Active Directory ist eine Zusammenfassung von Domänen, die durch Vertrauensverhältnisse verbunden sind und einen einheitlichen Namensraum teilen. Ein Forest ist eine Zusammenfassung von Domänen, die durch Vertrauensverhältnisse verbunden sind, aber einen unterschiedlichen Namensraum verwenden. Im Land Berlin wurde ein Forest aufgebaut.

Im Active Directory ist die erste erstellte Domäne die Root Domäne. Diese Domäne verfügt über die Root Domänen Controller mit dem globalen Katalog, dem Schema und der Konfiguration für das Active Directory.

In der Forest Root Domäne steuern zwei vordefinierte Sicherheitsgruppen (Organisations Admins und Schema Admins) die Zugriffsberechtigungen für den gesamten Forest.

Organisations Admins sind autorisiert Änderungen im gesamten Forest innerhalb von Active Directory durchzuführen. Ebenfalls ist diese Gruppe berechtigt untergeordnete Domänen hinzuzufügen.

Schema Admins sind autorisiert Änderungen am Active Directory Schema vorzunehmen, die im gesamten Forest wirksam werden.

Während der Erstellung einer neuen Domäne in einem Forest, erzeugt Active Directory automatisch eine 2-Wege transitive Vertrauensstellung zwischen der Root Domäne und der neuen Domäne.

Active Directory beginnt nach dem Erstellen und konfigurieren aller Domänen Controller automatisch damit Replikate des globalen Kataloges, des Schema und der Konfiguration unter den Domänen Controllern auszutauschen oder zu verteilen.

Innerhalb einer Domäne werden hierbei große Teile dieser Datenbanken ausgetauscht. Zwischen den Domänen werden nur die Änderungen oder die Updates ausgetauscht.

2. Fachlich technische Grundlagen der Exchange Organisation (Koexistenz von Exchange 5.5 und Exchange 200x Server)

Microsoft Exchange in der Version ab 200x ist hinsichtlich der Bereitstellung von Verzeichnisdiensten vollständig abhängig von Active Directory. Im Gegensatz zu früheren Versionen von Exchange (z.B. Exchange 5.5) mit eigenen unabhängigen Verzeichnisstrukturen und -diensten, erweitert Exchange 200x die Anzahl von Objektklassen und Attributen, die Objekten (wie z.B. Benutzern oder Gruppen) zugeordnet sind, in Active Directory.

Wenn bereits vor Einführung von Active Directory eine Bereitstellung von Exchange Server 5.5 stattgefunden hat, d.h. eine Exchange Organisation bereits besteht, dann ist mit Bereitstellung von Active Directory auch eine Koexistenz zwischen den Exchange Server 5.5 und Exchange 200x Server einzurichten. Es entsteht eine Exchange Organisation im gemischten Modus

Eine Verbindung des Exchange 5.5 Verzeichnisses mit Active Directory erfolgt über einen Active Directory Connector (ADC). Der ADC ist ein Modul für Replikation und Attributzuordnung, das Informationen aus einem LDAP-basierten Verzeichnis (Exchange 5.5.) entnimmt und mit einem anderen (Active Directory) synchronisiert. Dieser Vorgang ist in beide Richtungen möglich. Dadurch ist die Zusammenarbeit zwischen Exchange 4.4 und Exchange 200x Systemen möglich.

Solange in der bestehenden Exchange Organisation Exchange 5.5 Server vorhanden sind, besteht die Notwendigkeit, sowohl das Exchange 5.5 Verzeichnis als auch Active Directory zu verwenden und mithilfe des ADC Informationen zwischen beiden Verzeichnisdiensten zu synchronisieren.

Die im Active Directory bestehenden und die zusätzlich hinzu gekommenen Informationen, aus der ADC- Replikation, benutzt Exchange 200x Server, unter zu Hilfenahme eines global Katalogserver zur Bildung der globalen Adressliste (GAL) der Exchange Organisation.

Da die GAL alle Messaging- und E-Mail-fähigen Objekte der Active Directory Gesamtstruktur enthält, kann eine Exchange Organisation nur genau eine Active Directory Gesamtstruktur umfassen.

3. Fachlich und technische Umsetzung der allgemeinen Grundlagen des Active Directory Verzeichnisdienstes in der Gesamtstruktur der Berliner Verwaltung

Das ITDZ betreibt im Auftrag der Berliner Verwaltung die Active Directory Gesamtstruktur.

Dazu hat das ITDZ die Forest Root Domäne erstellt und administriert diese eigenverantwortlich entsprechend eines eigenen Organisationskonzeptes.

Bestandteil des Active Directory Organisationskonzeptes sind unter anderem verstärkte Sicherheitsmechanismen zur Administration der Root Domäne und zum Umgang mit den gesamtstrukturweiten Sicherheitsgruppen Organisations-Admins und Schema-Admins:

- Die Forest Root Domäne wird physikalisch im Hochsicherheitsrechenzentrum (HSRZ) des ITDZ betrieben.
- Die Forest Root Domäne dient ausschließlich der Administration der Gesamtstruktur,
- Die Kennwortrichtlinie dieser Domäne entspricht den Vorgaben der Berliner Verwaltung.
- Objektzugriffe und Anmeldeereignisse in der Domäne werden ständig in der Ereignisanzeige der Server protokolliert.
- Die Built-In Administrator Kennung ist umbenannt und wird verschlossen aufbewahrt,
- Kein Benutzerkonto ist standardmäßig Mitglied der Gruppe der Schema-Admins für die Gesamtstruktur.
- Anzahl der Benutzerkonten in der Gruppe der Organisations-Admins ist auf eins beschränkt.

Der Active Directory Verzeichnisdienst stellt in einem entsprechenden Sicherheitskontext, ohne erforderlichen Nutzereingriff, in der Gesamtstruktur notwendige Mechanismen bereit, erst wenn Änderungen und Fehler innerhalb des Verzeichnisdienstes auftreten ist ein Nutzereingriff erforderlich.

Der Einsatz eines Schema Administrator ist immer der Standort der Forest Root Domäne, hier befindet sich der DC mit der Schema-Master Funktion,

Der Einsatz eines Organisations Administrators erfolgt ausschließlich für strukturbildende Maßnahmen und vor allem aber für die Fehlersuche und -Behebung innerhalb der Gesamtstruktur.

Das Active Directory Organisationskonzept des ITDZ regelt jeweils den erforderlichen Einsatz von Schema- und Organisations- Administratoren im Normalfall und in Ausnahmesituationen.

4. Fachlich technische Umsetzung der allgemein Grundlagen einer Exchange Organisation im produktiven Exchange Verbund (Verwalt-Berlin)

Die Exchange Organisation (Verwalt-Berlin) wird im Auftrag der Berliner Verwaltung durch das ITDZ betrieben.

Dazu hat das ITDZ einen Active Directory Connector Server und die zentralen Exchange Server der Organisation (Verwalt-Berlin) erstellt und betreibt diese Organisation eigenverantwortlich innerhalb einer Active Directory Domäne. Diese Domäne ist Teil der Gesamtstruktur, sie ist aber nicht die Forest Root Domäne.

Exchange ist eine Applikation, die im Gegensatz zu einem Verzeichnisdienst nicht Mechanismen bereitstellt, sondern vor allem die bereitgestellten Mechanismen des Verzeichnisdienstes nutzt, insofern gelten für Exchange grundsätzlich

Mechanismen zur Administration einer Applikation und nicht vordergründig die gleichen Mechanismen wie zur Administration einer Domäne.

In der Summe aller Applikationsinstallation von Exchange, in unterschiedlichen Domänen, innerhalb der Gesamtstruktur und in der Summe aller ADC - Verbindungsvereinbarungen zu Exchange 5.5 Standorten entsteht innerhalb der Active Directory Gesamtstruktur einen eigener Applikations- und Sicherheitskontext, der Exchange Verbund (Verwalt-Berlin).

Der Exchange Sicherheitskontext wird vollständig und ausschließlich von dem Objekt (Nutzer oder Gruppe) verwaltet, in dessen Kontext der erste Exchange Server im Exchange Verbund installiert wurde. Dieses Objekt ist in der o.g. Domäne des ITDZ angelegt worden.

Um den Exchange Applikationsbetrieb in seinem vollen Funktionsumfang in der Gesamtstruktur aufrecht erhalten zu können (ca. 19.000 Postfächer), besteht nur die Möglichkeit des Nutzens einer Delegierung von Teilverantwortlichkeiten innerhalb des Exchange Verbundes.

Diese Delegierung bedingt jedoch den zweifelsfreien Nachweis, der Fähigkeit und Fertigkeit, Exchange als Applikation innerhalb einer Teilstruktur administrieren zu können. Die Einrichtung einer Delegierung ohne diesen Nachweis birgt nicht nur die Gefahr eines Applikationsausfalls innerhalb einer Teilstruktur, sondern kann auch zu Stillstand oder Ausfall des gesamten Applikationsbetrieb innerhalb des Exchange Verbundes führen. Dies gilt es von Seiten des ITDZ, als Betreiber des Exchange Verbundes im Interesse aller angeschlossenen Verwaltungen, von vornherein aus zu schließen.

Es existiert nur ein Exchange Verbund, insofern steht es jedem Teilnehmer am Exchange Verbund frei, zu entscheiden in welchem Umfang eine zentrale Exchange Administration durch das ITDZ oder eine dezentrale Administration in der Verwaltung gewünscht wird. Für eine zentrale Administration sind Service Level Vereinbarungen erforderlich.

Für die Administration des Exchange Verbundes wurden eigene Festlegungen getroffen:

- Der Active Directory Connector (ADC) Dienst, ist eine Übergangslösung im Exchange Verbund und wird nach Umstellung des Verbundes auf Exchange 200x entfallen.
- Die Rolle des Administrator der Exchange Organisation ist auf wenige Mitarbeiter beschränkt und ist beim ITDZ, als dem Betreiber des Verbundes, angesiedelt. Der Administrator des Exchange Verbundes hat keinen Zugriff auf die einzelnen Exchange Server, sondern regelt die Administration der Verbindungsconnectoren und der Verzeichnisreplikation.
- Delegiert werden ausschließlich Rechte zur Verwaltung administrativer Gruppen innerhalb von Exchange.
- Zugriff auf Mitgliedsserver von Domänen auf denen die Exchange Applikation ausgeführt wird, haben nur Exchange Administratoren der einzelnen Verwaltungen.
- Das Einrichten neuer administrativer Gruppen ist Aufgabe des Administrator der Exchange Organisation.
- Die Installation eines Exchange Servers innerhalb administrativer Gruppen des Exchange Verbundes ist gemeinschaftliche Aufgabe des Administrator der Exchange Organisation und des Administrator der administrativen Gruppe.

Der Applikationsbetrieb innerhalb des Exchange Verbundes ist ein von permanenter Veränderung geprägter Prozess, dessen Überwachung und Früherkennung von Engpässen maßgeblich Einfluss auf die Funktionalität und Verfügbarkeit der Exchange Dienste im gesamten Active Directory hat.

5. Fachlich und technische Forderungen an Kunden der Active Directory Gesamtstruktur und des Exchange Verbundes

   Basis der Gespräche über die Aufnahme in die Active Directory Gesamtstruktur ist immer das Infrastruktur Konzept des Kunden. Dort wird geregelt wie sich der Kunde den Anschluss an das MAN und damit die zukünftige Struktur seiner IT-Landschaft vorstellt.

   Ebenso definiert das Sicherheitskonzept des Kunden Inhalte und Umfang von Zugriffsmöglichkeiten auf interne Strukturen.

   Erst dann haben Neukunden in der Active Directory Gesamtstruktur, sich vor Inbetriebnahme ihrer Domäne oder -partition, dem ITDZ gegenüber, zur Einhaltung der dann noch offenen Festlegungen des Active Directory Organisationskonzeptes betreffend zu verpflichten.

   Optional müssen gesonderte Vereinbarungen über Service Level Agreements zwischen dem Kunden und dem ITDZ abgeschlossen werden.

   Der Kunde hat sein bestätigtes Infrastruktur- und Sicherheitskonzept um zusetzten und dessen Einhaltung zu überwachen. Ist dies nicht gewährleistet kann die Verantwortlichkeit für nicht autorisierte Zugriffe auch nicht auf Andere verlagert werden.

Anlage C2 : Merkblatt über unerwünschte E-Mail

Unter SPAM versteht man unverlangte, zumeist unerwünschte und wiederholte Massen- bzw. kommerzielle E-Mail-Sendungen. Mit großem Abstand liegen den meisten SPAM-Exemplaren kommerzielle Interessen zugrunde. SPAM wird aber auch im Vorfeld von Wahlen oder Abstimmungen, zum Versand von Scherzmails und vieles mehr eingesetzt. Es handelt sich hingegen nicht um SPAM, wenn Sie von einer Firma deren Kunde Sie sind, hin und wieder E-Mails bekommen. Auch der Newsletter den Sie abonniert haben, stellt kein SPAM dar. Voraussetzung dafür ist jedoch, dass Sie diesen Sendungen zugestimmt haben.

Beschaffung von E-Mail Adressen durch den Spammer

Spammer beschaffen sich E-Mail-Adressen mittels leistungsfähiger Suchmaschinen, sog. Harvester, aus Mitgliederverzeichnissen verschiedenster Dienste von Online-Anbietern wie z.B. Foren, Newsgroups und Chats. Spammer kaufen oder tauschen Adresslisten von Unternehmen, die das Sammeln von Adressen zu ihrem Hauptgeschäft gemacht haben. Spammer können jedoch die Adressen auch selber zusammenfügen, indem sie Namenslisten und häufige Domains kombinieren.

Die wichtigsten Konsequenzen für die betroffenen Personen

Der Spammer gibt den betroffenen Personen keine Möglichkeit, die unerwünschten Zusendungen abzubestellen. Postfächer werden mit unerwünschten Sendungen überfüllt. Das Selektieren zwischen unerwünschten und „richtigen“ Sendungen ist mühsam und zeitraubend. Der Inhalt der Sendungen stellt oftmals einen erheblichen unerwünschten Eingriff in den privaten Lebensbereich dar. Die Netzinfrastruktur (z.B. Mailserver) werden übermäßigen Belastungen ausgesetzt, unnötige Verbindungskosten und Netzlasten entstehen.

Schutzmaßnahmen gegen SPAM

Seien Sie vorsichtig bei der Verwendung Ihrer E-Mail-Adresse im Internet. Sie kann auch ohne Ihre Kenntnis und Einwilligung durch unberechtigte Dritte erfasst werden, sobald sie auf einer Webseite bekannt gegeben wird (z. B. bei der Teilnahme an Diskussionsforen oder Bestellung von Newsletters, bei Online-Geschäften oder beim Ausfüllen von Online-Formularen).

Mit folgenden präventiven Maßnahmen können Sie sich gegen SPAM schützen:

Transparenz über die Weiterverwendung Ihrer E-Mail-Adresse im Internet: Vergewissern Sie sich vor der Erfassung Ihrer E-Mail-Adresse in einem Internet-Formular, dass Angaben über die weitere Verwendung der Adresse gemacht werden. Dadurch können Sie das Risiko einer unerwünschten Weiterverwendung Ihrer E-Mail-Adresse (z. B. zu Marketingzwecken) reduzieren.

Mehrere E-Mail-Adressen benutzen: Schaffen Sie sich für Ihre Internetgeschäfte, Ihre Teilnahme an Diskussionsforen und Newsletter bestimmte persönliche E-Mail-Adressen. Damit können Sie Ihre dienstliche E-Mail-Adresse, die Sie ausschließlich für berufliche Tätigkeit benutzen, weitgehend vor SPAM schützen.

Liste der Empfänger Ihrer E-Mail-Adresse: Daten (Einschreibedatum, E-Mail-Inhalt, Passwort), die Sie beim Abonnement von Newsletter, bei der Öffnung von Konten oder Online-Zahlungen angeben, sollten Sie ausdrucken und aufbewahren. Desgleichen sollten Sie eine Liste jener Webseiten führen, auf welchen Sie Ihre E-Mail-Adresse bekannt gegeben haben.

Schutz von E-Mail-Adressen Dritter: Wenn Sie eine Sendung an mehrere Empfänger vornehmen, benutzen Sie die Funktion „versteckte Kopie“ (BCC) Ihrer E-Mail-Software.

Damit schützen Sie die Adressen Ihrer Korrespondenzpartner. Verbergen Sie die Adressen auch in Newsgroups und anderen Verteilerlisten.

Einwilligung der betroffenen Personen: Geben Sie E-Mail-Adressen von Drittpersonen ohne deren Einwilligung nicht bekannt.

Öffentliche Verzeichnisse: Vermerken Sie beim Eintrag in ein öffentliches Verzeichnis (z. B. elektronische Telefonverzeichnisse), sofern möglich, dass Sie keine unaufgeforderte Werbung erhalten möchten.

Mit folgenden präventiven Maßnahmen schützt Sie das ITDZ gegen SPAM:

SPAM-Filter: Der SPAM-Problematik lässt sich momentan mittels Header- und Inhalts-Analyse entgegenwirken. Die eingegangenen Sendungen werden nach bestimmten Merkmalen untersucht und gefiltert. Damit sind jedoch nicht alle Probleme beseitigt. Erstens können auch erwünschte Sendungen im Filter hängen bleiben. Im Allgemeinen rechnet man mit einer Fehlerquote von mindestens 10% (falsch positive und falsch negative Treffer). Zweitens wird das eigentliche Problem nicht gelöst: SPAM wird trotzdem verschickt. Insgesamt ist die tägliche Anzahl der vom zentralen SPAM-Filter des ITDZ abgewiesenen bzw. als [SPAM] gekennzeichneten Sendungen doppelt so hoch, wie die Anzahl der „richtigen„ Sendungen.

SPAM-Filter Stufe I Mail-Header Analyse: Bei jeder ankommenden Sendung erfolgt automatisch eine Abfrage top-aktueller Datenbanken im Internet, ob die Mail-Absender IP-Adresse als Spammer oder offenes Relay bekannt ist, wenn ja wird die Sendung abgewiesen. Seit dem 1.7.05 erfolgt zusätzlich eine Datenbankabfrage im Internet, ob die Sendung von einer temporär vergebenen IP-Adresse aus dem Internet abgesendet wurde. Ist dies der Fall erfolgt immer eine Abweisung der Sendung, weil die eindeutige Identität des Absenders nicht verifiziert werden kann. Ca. 70.000 Sendungen werden in Spitzenzeiten täglich von der Stufe I des ITDZ SPAM-Filter abgewiesen.

SPAM-Filter Stufe II Inhaltsanalyse: Eingehende Sendungen durchlaufen mehrere Filtermechanismen, die den Inhalt der Sendung untersuchen, Basis dieser Filtermechanismen sind ebenfalls Datenbanken im Internet, darüber hinaus sind diese Mechanismen selbstlernend. Jede eingehende Sendung erhält eine entsprechende Einstufung. Ergibt die Einstufung einen Wert, der unter 3 Punkten liegt, erfolgt keine Markierung als SPAM. Zwischen 3 und 4 Punkten erfolgt die Markierung nur im Header der Sendung und bei höherer Einstufung erfolgt eine zusätzliche Kennzeichnung als "[SPAM]" im Betreff. Die anschließende Weiterleitung an den Empfänger erfolgt aber in jedem Falle. Vom ITDZ SPAM-Filter der Stufe II werden täglich 3.000 eingehende Sendungen im Header als SPAM und weitere 7.000 zusätzlich im Betreff als [SPAM] gekennzeichnet. Beide SPAM-Filterstufen agieren vollautomatisch und werden vom ITDZ auch nicht durch zusätzliche Eintragungen von Betreffzeilen von Hand gepflegt.

Wenn Sie SPAM erhalten haben, sollten Sie sich an folgende Regeln halten:

Ungelesen löschen (Outlook Junk-E-Mail Ordner): Am besten löschen Sie SPAM-Sendungen, ohne sie zu öffnen. Auf keinen Fall sollten Sie Anlagen öffnen oder auf auffällige kommerzielle Angebote eingehen, egal wie interessant die Werbebotschaft aussehen mag.

SPAM nicht beantworten: Sie sollten SPAM nie beantworten. Eine Antwort bestätigt dem Spammer, dass Ihre E-Mail-Adresse gültig ist und benutzt wird. Eine automatische Weiterleitung eingehender Sendungen eines Postfachnutzers an Zieladressen im Internet, ist für den gesamten Exchange-Verbund deaktiviert, Ebenso wie die Deaktivierung der automatischen Weiterleitung, ist auch das Versenden von automatischen Antworten (Outlook-Abwesenheits-Assistent) an Zieladressen im Internet für den gesamten Exchange-Verbund deaktiviert.

Keine Überreaktionen: Überfluten Sie das Postfach des Spammer nicht mit großen Dateien. Der Spammer hat seine Sendungen mit hoher Wahrscheinlichkeit mit einer falschen Identitätsangabe signiert. Wahrscheinlich gehört die Adresse einem anderen SPAM-Opfer. Außerdem belasten Sie die Netzinfrastruktur unnötig.

Hypertext-Links im SPAM nicht anklicken: Hypertext-Links im SPAM sollten nicht angeklickt werden. Sie riskieren damit, dass Ihre E-Mail-Adresse z.B. via Cookies erfasst wird, womit der Spammer die Bestätigung hat, dass die Adresse benutzt wird.

Drohungen des Spammers melden: Werden Sie durch den Spammer bedroht (z. B. mit der Verbreitung von Botschaften mit pornographischem Inhalt in Ihrem Namen), melden Sie diesen Zustand auch ihrer zuständigen IT-Stelle.

Anlage E1 : Eingabehilfen für Personen mit Behinderungen

Microsoft® hat es sich zur Aufgabe gemacht, die Handhabung der Produkte und Dienste für jeden einfach zu gestalten. Diese Anlage enthält Informationen über Features, Produkte und Dienste, mit denen die Microsoft Windows Server™ 2003-Reihe, die Windows® 2000 Server-Reihe, Microsoft Exchange Server 2003 und Microsoft Office Outlook® Web Access 2003 für Personen mit Behinderungen einfacher einzusetzen sind. Es werden die folgenden Themen besprochen:

- Eingabehilfen in Microsoft Windows
- Anpassen von Microsoft-Produkten für Menschen, die Eingabehilfen benötigen
- Microsoft- Produktdokumentation in alternativen Formaten
- Microsoft-Dienste für Gehörlose oder Hörgeschädigte
- Spezifische Informationen über Exchange 2003 und Outlook Web Access 2003
- Andere Informationsressourcen für Personen mit Behinderungen

Hinweis: Weitere Informationen finden Sie auf der Microsoft-Website für Eingabehilfen unter (http://go.microsoft.com/fwlink/?LinkId=22008) .

Eingabehilfen in Microsoft Windows

Seit der Einführung von Windows 95 wurden bereits viele Eingabehilfen in das Betriebssystem Windows integriert. Diese Features sind für Personen konzipiert, die eine Tastatur oder Maus nur mit Schwierigkeiten bedienen können, blind oder sehbehindert, gehörlos oder hörgeschädigt sind. Die Features können beim Setup installiert werden.

Eingabehilfedateien zum Download

Eingabehilfedateien downloaden:

- Die Microsoft-Website für Eingabehilfen http://www.microsoft.com/enable/
- Die Website unter http://go.microsoft.com/fwlink/?LinkId=14898. Klicken Sie auf die Option **Knowledge Base Article ID Number Search**, geben Sie **165486** ein, und klicken Sie dann auf den Pfeil. In den Suchergebnissen wird der Knowledge Base-Artikel „Customizing Windows for Individuals with Disabilities“ angezeigt, der Hyperlinks zu Dokumenten über das Anpassen verschiedener Versionen von Microsoft Windows enthält.

  Klicken Sie zum Abrufen von weiteren Artikeln zu Eingabehilfen von der Website „Microsoft Help and Support“ auf die Option **Search the Knowledge Base**, wählen Sie **All Microsoft Products** aus, geben Sie unter **Search for** die Zeichenfolge **kbenable** ein, und klicken Sie dann auf **Go**.
- Microsoft-Internetserver unter ftp://ftp.microsoft.com/, in **softlib/MSLFILES**.

Anpassen von Microsoft-Produkten für Menschen die Eingabehilfen benötigen

Optionen und Features für Eingabehilfen sind in viele Microsoft-Produkte integriert, auch in das Betriebssystem Windows. Eingabehilfen sind für Personen hilfreich, die eine Tastatur oder eine Maus nur mit Schwierigkeiten bedienen können, blind oder sehbehindert, gehörlos oder hörgeschädigt sind.

Kostenlose, schrittweise aufgebaute Lernprogramme

Microsoft bietet eine Reihe von schrittweise aufgebauten Lernprogrammen an, in denen Sie das Anpassen der Optionen und Einstellungen des Computers für die Eingabehilfen erlernen können. Die kostenlosen Lernprogramme enthalten ausführliche Vorgehensweisen zum Anpassen von Optionen, Features und Einstellungen entsprechend ihren persönlichen Anforderungen an Eingabehilfen. Die Informationen über die Verwendung der Maus, der Tastatur, oder einer Kombination beider Geräte werden zu Ihrer Unterstützung seitenweise dargestellt.

Die neuesten schrittweise aufgebauten Lernprogramme finden Sie auf der Microsoft-Webseite „Microsoft Accessibility Step by Step Tutorials Overview“ (http://go.microsoft.com/fwlink/?LinkId=14899).

Unterstütze Produkte für Windows

Für die einfachere Verwendung von Computern für Menschen mit Behinderungen ist eine breite Palette an unterstützenden Produkten verfügbar.

Microsoft bietet auf der Webseite „Microsoft Overview of Assistive Technology“ (http://go.microsoft.com/fwlink/?LinkId=14901) einen durchsuchbaren Katalog von Unterstützungsprodukten an, die unter Microsoft Windows ausgeführt werden können.

Für die Betriebssysteme MS-DOS®, Windows und Microsoft Windows NT® sind beispielsweise folgende Produkte erhältlich:

- Programme zur Darstellung von Informationen am Bildschirm in Blindenschrift oder in synthetisch gebildeter Sprache für Blinde oder Personen mit Leseproblemen
- Hardware- und Softwaretools, die das Verhalten von Maus und Tastatur ändern
- Programme, die das Eingeben von Informationen mit der Maus oder per Spracheingabe ermöglichen
- Software zur Wort- oder Satzergänzung, die Personen für eine schnellere Eingabe mit weniger Tastenanschlägen verwenden können
- Alternative Eingabegeräte, wie zum Beispiel Einzelschaltergeräte oder Atem- und Schluckgeräte für Personen, die keine Maus oder Tastatur verwenden können

Microsoft Dokumentationen in alternativen Formaten

Neben den standardmäßigen Dokumentationsformaten sind viele Microsoft-Produkte auch in anderen Formaten erhältlich, um den Zugriff auf diese Produkte zu erleichtern.
Bei Sehstörungen oder Problemen im Umgang mit gedruckten Dokumentationen, können viele Microsoft-Veröffentlichungen auch über Recording for the Blind & Dyslexic, Inc. (RFB&D) bezogen werden. RFB&D vertreibt diese Dokumente an registrierte, berechtigte Mitglieder ihres Verteilerdienstes in einer Vielzahl von Formaten, z. B. auf Audiokassetten oder CDs. Das Angebot von RFB&D umfasst über 90.000 Titel, einschließlich Microsoft-Produktdokumentation und Bücher von Microsoft Press®. Viele Microsoft-Bücher können von der Website „Accessible Documentation for Microsoft Products“ unter (http://go.microsoft.com/fwlink/?LinkId=22007) gedownloadet werden.

Microsoft Dienste für Gehörlose oder Hörgeschädigte

Gehörlose oder Hörgeschädigte haben über einen „Teletype/Telecommunication device for the deaf(TTY/TDD)“-Dienst Zugriff auf alle Produkt- und Kundendienste von Microsoft.

Weitere Informationen über Eingabehilfen

Auf der Microsoft-Website für Eingabehilfen (http://www.microsoft.com/enable/) stehen Informationen für Menschen mit Behinderungen und deren Freunde und Verwandte sowie für Beratungsstellen, Bildungseinrichtungen und Anwälte zur Verfügung.
Durch Bezug eines kostenlosen monatlichen elektronischen Newsletters können Sie auf dem aktuellsten Stand der Entwicklung auf dem Gebiet der Eingabehilfen für Microsoft-Produkte bleiben. Wenn Sie den Newsletter abonnieren möchten, besuchen Sie die Webseite „Accessibility Update“ (http://go.microsoft.com/fwlink/?LinkId=14920).