

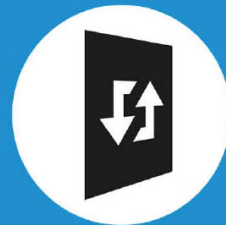
praxisnah
& kompetent

Das HANDBUCH

Microsoft

Exchange Server 2019

Von der Einrichtung
bis zum reibungslosen Betrieb



Thomas Joos



O'REILLY®

Inhalt

Cover

Titel

Impressum

Inhalt

Vorwort

Teil A Einstieg und Installation

1 Neuerungen und Grundlagen

 Neuerungen im Überblick

 Änderungen der Serverrollen im Überblick

 Edge-Transport, Koexistenz und Datenbankverfügbarkeitsgruppen

 Systemvoraussetzungen im Überblick

 Öffentliche Ordner und Exchange Admin Center

 Clientanbindung und Hochverfügbarkeit

 Outlook im Web – Die neue Outlook Web App

 Das bleibt in Exchange 2019 unverändert

 Outlook 2019 mit Exchange 2019

 ReFS und Database Divergence Detection

 Grundlagen zur Installation von Exchange 2019

 Editionen von Exchange Server 2019

 Exchange 2019 lizenzieren

 Zusammenfassung

2 Installation und Grundeinrichtung

 Active Directory für Exchange 2019 vorbereiten

 Funktionsebenen von Gesamtstrukturen und Domänen verstehen

 Schemamaster – Active Directory erweitern

Voraussetzungen an Domänencontroller und IPv6

 Softwarevoraussetzungen für Exchange 2019

Betriebssystem für Exchange vorbereiten

Tools und Voraussetzungen installieren

 Active Directory und Domänen vorbereiten

 Installation von Exchange 2019 durchführen

Exchange Server 2019 auf Core-Servern installieren

Aufgaben nach der Installation und Troubleshooting

Installation in der grafischen Benutzeroberfläche durchführen

Automatische Installation oder Deinstallation über die Eingabeaufforderung

Installation von Exchange 2019 delegieren

Rollup Packages und kumulative Updates installieren

Exchange-Sprachpakete installieren

Exchange-Verwaltungstools installieren

Exchange 2019 deinstallieren

 Erste Schritte nach der Installation

Installation in der Exchange Management Shell überprüfen und Fehler beheben

Microsoft Exchange Analyzer nutzen

Product Key eingeben

Exchange-Zertifikate konfigurieren

E-Mail-Versand und -Empfang konfigurieren

Virtuelle Verzeichnisse konfigurieren

 Fehlerbehebung während der Installation

Exchange-Server mit ADSI-Edit aus Active Directory entfernen

Neuinstallation durch Setupfehler oder falsche Uhrzeit

Exchange-Reparaturinstallation durchführen

System-Benutzerpostfächer verschieben und neu erstellen

Exchange und Domänencontroller – Probleme bei der Zusammenarbeit beheben

Virtualisierung von Exchange 2019

Allgemeine Hinweise zu virtuellen Exchange-Servern

Integrationsdienste und Zeitsynchronisierung beachten

Automatisches Starten und Herunterfahren

Snapshots und Datensicherungen für virtuelle Server

Daten von virtuellen Servern aus Hyper-V auslesen

Zusammenfassung

3 Erste Schritte

Erste Schritte mit Exchange 2019

Das Exchange Admin Center verstehen

Exchange-Organisation verwalten

Exchange-Server verwalten

Empfänger verwalten

Einführung in die Exchange Management Shell

Clientzugriff testen

User Principal Name und E-Mail-Domänen anpassen

Dienstpunkte und virtuelle Verzeichnisse verstehen und überprüfen

Nachrichtenfluss konfigurieren

Sendeconnector erstellen

E-Mail-Domänen konfigurieren

E-Mail-Adressenrichtlinien verwalten

E-Mail-Größen definieren

Allgemeine Informationen zu Serverrollen und Serverdiensten

Systemdienste von Exchange 2019

Ordnerstruktur von Exchange 2019

Den Pickup-Ordner für selbst erstellte E-Mails verwenden

Die Funktion des Replay-Ordners

Active Directory-Replikation überprüfen

Zusammenfassung

Teil B Einrichtung und Verwaltung

4 Nachrichtenfluss und Connectors

Informationen zum E-Mail-Routing in Exchange 2019

Routing über verschiedene Server und Exchange-Versionen

Zustellungsgruppen, Routingziele und Transportdienste verstehen

Sendeconnectors erstellen und verwalten

Neue Sendecollectors erstellen

Sendeconnectors in der Exchange Management Shell erstellen

Sendeconnectors verwalten

Eigenschaften eines Sendecollectors mit der Exchange Management Shell konfigurieren

Empfangsconnectors erstellen und verwalten

Neue Empfangsconnectors erstellen

Sicherheit von Empfangsconnectors verwalten

Relaying für Applikationsserver erlauben

Direkte Verbindung von Transportservern mit dem Internet

E-Mail-Fluss testen

Zustellungs-Agents und Transport-Agents

Zustellungs-Agents und -Connectors

Transport-Agents für ältere Versionen

Transport-Agents verwalten

Allgemeine Einstellungen für Exchange-Transportserver

Transportserver konfigurieren

Nachrichtengröße beschränken

Akzeptierte Domänen und Remotedomänen

- Remotedomänen verstehen
- Remotedomänen konfigurieren
 - Warteschlangen (Queues)
- Erster Einblick in die Warteschlangenanzeige
- Warteschlangentypen in Exchange 2019
- Warteschlangen verwalten
- Warteschlangendatenbank verwalten
 - Nachrichtenverfolgung (Message Tracking)
- Nachrichtenverfolgung konfigurieren
- Nachrichtenverfolgung verwenden
 - SMTP für Fortgeschrittene
 - Transportregeln für den Nachrichtenfluss erstellen
- Transportregeln verstehen
- Erste Schritte mit Transportregeln
- Transportregel in der Exchange Management Shell erstellen
 - Zusammenfassung
 - 5 Exchange-Datenbanken verstehen
 - Einführung in die Datenbankstruktur
 - Postfachdatenbanken erstellen und verwalten
- ReFS verwenden
- Neuen Postfachspeicher anlegen
- Datenbanken verschieben
- Postfachdatenbanken verwalten
 - Dateien aus Exchange-Datenbanken in .pst-Dateien exportieren
- Postfächer in Exchange 2007 exportieren
- Berechtigung für den Export in Exchange 2016/2019 erteilen
- .pst-Dateien in ein Postfach importieren
- Postfächer in .pst-Dateien exportieren

Microsoft PST Collection Tool nutzen

Transaktionsprotokolle verwalten

Grundlagen zu Transaktionsprotokollen

Prüfpunktdatei (.chk) verstehen

Umlaufprotokollierung verstehen

Probleme mit schnell anwachsenden Transaktionsprotokollen beheben

Exchange-Datenbankfehler beheben

Prüfung bei Serverausfall

Datenbanken auf Konsistenz überprüfen

Datenbanken mit der Exchange Management Shell reparieren

Offlinedefragmentierung einer Exchange-Datenbank

Datenbanken und Verbindungen in der Exchange Management Shell testen

Zusammenfassung

6 Clientanbindung an Exchange

Übersicht zur Clientanbindung

Exchange-Clientzugriff in der Management Shell testen

Funktionen in Outlook zusammen mit Exchange

Verbindungsprobleme in Outlook und anderen Office-Programmen finden und beheben

Autodiscover und AutoConnect mit Outlook

Allgemeine Informationen zur automatischen Anbindung an Exchange

Autodiscover in der Exchange Management Shell testen

DNS-Eintrag für Autodiscover erstellen

Autodiscover mit Office 365 und Exchange

Autodiscover in Hybrid-Umgebungen

Autodiscover mit Exchange und Lync/Skype

Startoptionen zur Fehlerbehebung von Outlook 2019

Outlook Web App (OWA) konfigurieren

OWA-Zugriff für Benutzerkonten aktivieren und deaktivieren

Bedienung von Outlook Web App

Offlinemodus in Outlook Web App nutzen

Virtuelle Ordner von Outlook Web App verwalten

Outlook Web App-Richtlinien

GZIP-Komprimierung konfigurieren

Outlook Web App-Dienste überprüfen und Fehler beheben

- Mailtips in Exchange 2019 konfigurieren
- E-Mail-Verschlüsselung mit Exchange 2019 und Outlook

Voraussetzungen für die E-Mail-Verschlüsselung

Zertifikate installieren und in Outlook einbinden

E-Mails mit Outlook verschlüsseln

S/MIME in Outlook Web App

E-Mail-Verschlüsselung mit Office 365

- Smartphones und Tablets mit Exchange ActiveSync (EAS) anbinden

Direct Push-Grundlagen

Benutzerverwaltung für Exchange ActiveSync

Exchange ActiveSync-Postfachrichtlinien

ActiveSync-Gerätezugriffsregeln

- Zertifikatbasierte Authentifizierung mit ActiveSync und OWA

Funktionsweise der zertifikatbasierten Authentifizierung

Voraussetzungen für den Einsatz der zertifikatbasierten Authentifizierung

UPN und E-Mail-Domänen anpassen

Server für zertifikatbasierte Authentifizierung konfigurieren

Clients für Zertifikatsauthentifizierung konfigurieren

OWA mit zertifikatbasierter Authentifizierung nutzen

- POP3 oder IMAP4 für den mobilen Verbindungsaufbau verwenden

POP3 versus IMAP4

POP3 und IMAP4 aktivieren

POP3 und IMAP4 konfigurieren

Zusammenfassung

7 Empfänger, Gruppen und Kontakte verwalten

Einführung in die Benutzerverwaltung

Postfächer erstellen

Freigaben – Shared Mailboxes

Raum- und Gerätepostfächern erstellen und verwalten

Ressourcen-Postfach erstellen

Rechte für Raumpostfächer verwalten

Raumlisten erstellen und verwalten

Postfächer konvertieren

Moderierter Transport – Nachrichtengenehmigung

Postfächer verwalten

Benutzerdaten, E-Mail-Adressen und Postfachnutzung

Erweiterte Postfachfunktionen steuern – Smartphones anbinden

Berechtigungen zur Verwaltung an Anwender zuweisen

Kalender und Besprechungen konsistent halten (Calendar Repair Assistant)

Postfächer löschen und deaktivieren

Postfächer erneut verbinden

Postfachberechtigungen – Anwendern Zugriff auf andere Postfächer erteilen

Anmeldung von Postfächern überwachen

Postfächer verschieben

Postfächer innerhalb der Exchange-Organisation verschieben

Postfächer zwischen Organisationen verschieben

Besprechungsanfragen erstellen und verwalten

Neue Besprechungsanfrage erstellen

Besprechungen bearbeiten oder absagen

Besprechungsanfragen beantworten und Kalender verwalten

- Kontakte und E-Mail-aktivierte Benutzer anlegen und verwalten
- Verteilergruppen erstellen und verwalten

Neue Verteilergruppe anlegen

Benennungsrichtlinie für Verteilergruppen erstellen

Verteilergruppen verwalten – Moderation und Mitgliedschaftsgenehmigung

Nachrichtenmoderation für Verteilergruppen

Gruppenmitgliedschaften mit der Mitgliedschaftsgenehmigung verwalten

Dynamische (abfragebasierte) Verteilergruppen

Verteilergruppen-Verwaltung delegieren

- Adresslisten und Adressbuchrichtlinien verwalten

Neue Adresslisten erstellen und verwalten

Adressbuchrichtlinien definieren

Offlineadresslisten verwenden

- Zusammenfassung
- 8 Teamwork mit Exchange und Office 365
- Öffentliche Ordner verwenden

Grundlagen und wichtige Fragen zu öffentlichen Ordnern in Exchange 2019

Möglichkeiten der öffentlichen Ordner

Öffentliche Ordner mit OWA und Outlook 2019

Öffentliche Ordnern aktivieren

Öffentliche Ordner erstellen und verwalten

Öffentliche Ordner in Outlook anlegen

Öffentliche Ordner verwalten

- Öffentliche Ordner zu Office 365-Gruppen migrieren

Office 365-Gruppen als Ersatz für öffentliche Ordner nutzen

Office 365-Gruppen erstellen und konfigurieren

Unterschiede von Office 365-Gruppen zu öffentlichen Ordnern

Migration von öffentlichen Ordnern zu Office 365-Gruppen durchführen
Migration in der Praxis durchführen
Microsoft Teams für die Zusammenarbeit von Gruppen nutzen
 Freigegebene Postfächer
Freigegebene Postfächer verstehen
Freigegebenes Postfach erstellen
Benutzerpostfach in ein freigegebenes Postfach konvertieren
 Websitepostfächer – Exchange und SharePoint gemeinsam betreiben
Grundlagen zu Websitepostfächern
Websitepostfächer in der Praxis
Websitepostfach in der Praxis nutzen
Neuerungen in SharePoint 2019
Websitepostfächer und Office 365
 Zusammenfassung

Teil C Compliance

 9 Richtlinien und Archivierung
 Grundlagen zur Archivierung
 Archiv aktivieren und anpassen
Archivpostfach aktivieren
Archivpostfach verwenden
Archivierung deaktivieren, Aufbewahrungszeiten festlegen und erneut verbinden
Archivrichtlinien ändern
Kontingente für das Archiv konfigurieren
E-Mail-Archivierung mit Exchange 2019-Bordmitteln in der Praxis
 Messaging-Datensatzverwaltung
Aufbewahrungsrichtlinien verstehen und einsetzen
Aufbewahrungstags (Retention Tags) erstellen
Aufbewahrungsrichtlinien (Retention Policies) erstellen

Assistent für verwaltete Ordner konfigurieren
Gesetzliche Aufbewahrungspflicht (Legal Hold)
 Compliance-Archiv
Grundlagen zur Archivierung
Compliance-Archiv verstehen
Compliance-Archiv erstellen
Compliance-Archiv entfernen
Compliance-eDiscovery
Die Compliance-Suche nutzen
 Journale nutzen
Journal verwalten
Journal für Postfachdatenbanken aktivieren oder deaktivieren
 Zusammenfassung
 10 Data Loss Prevention (DLP) und Überwachung
 DLP in Exchange 2019 nutzen
DLP-Richtlinie aus einer Vorlage erstellen
DLP-Richtlinien verwalten
Richtlinientipps verwalten
Dokumentfingerabdrücke erstellen
Informationsrechte verwalten
Grundlagen und erste Schritte zu IRM
Transportschutzregeln einsetzen
Outlook-Schutzregeln mit Outlook verwenden
Transport- und Journalentschlüsselung
Verwaltung von Informationsrechten aktivieren oder deaktivieren
Informationsrechte in Outlook Web App verwalten
Informationsrechten in Exchange ActiveSync verwalten
IRM für interne E-Mails aktivieren oder deaktivieren

Protokollierung der Verwaltung von Informationsrechten aktivieren oder deaktivieren

Postfachüberwachungsprotokollierung

Postfachüberwachungsprotokollierung aktivieren

Postfachüberwachungsprotokollsuche erstellen

Administratorüberwachungsprotokollierung

Überwachungsprotokoll verstehen

Administratorüberwachungsprotokollierung verwalten

Änderungen in der Ereignisanzeige anzeigen

Definierte Berechtigungen anzeigen

Zusammenfassung

Teil D Sicherheit und Hochverfügbarkeit

11 Edge-Transport-Server

Edge-Transport mit Exchange 2019

Exchange 2019 Edge-Transport-Server installieren

Installation überprüfen und lizenzieren

Edge-Server mit der Organisation verbinden

Edge-Abonnement verstehen

Address Rewriting Agent verwalten

Address Rewriting Agent aktivieren und deaktivieren

Address Rewriting Agent konfigurieren

Zusammenfassung

12 Viren- und Spamschutz

Integrierten Virenschutz verwalten

Virenschutz testen

Virenschutz aktualisieren

Virenschutz deaktivieren oder umgehen

Exchange Online Protection und Exchange 2016/2019

Standardrichtlinie für Antischadsoftware konfigurieren

Wichtige Einstellungen für Virens Scanner auf Dateisystemebene

Spamschutz und E-Mail-Sicherheit mit Exchange

Spamschutzfunktionen installieren

Spam Confidence Level (SCL) im Überblick

Spamfilter in Exchange konfigurieren

Spamserver aussperren – Verbindungsfilter konfigurieren

Spamabsender gezielt blockieren – Absenderfilterung konfigurieren

Schüsse ins Blaue verhindern – Empfängerfilterung konfigurieren

Absender vor der Zustellung überprüfen – Sender-ID verwenden

Spam-E-Mails nach ihrem Inhalt entlarven – Inhaltsfilterung verwenden

Antispameinstellungen für Postfächer konfigurieren

Spamsender entdecken – Absenderzuverlässigkeitsfilterung verwenden

Transportregeln für Spam-E-Mails erstellen

Sicherheit und Virenschutz mit Outlook 2016/2019

Bilder automatisch herunterladen

Datenschutzoptionen in Outlook festlegen

Anlagenbehandlung – Dateianlagen absichern

Einstellungen für Makros und Add-Ins konfigurieren

Office 2016/2019 mit Richtlinien steuern

Junk-E-Mail-Filter in Outlook – Schutz vor Phishing und Spam

Zusammenfassung

13 Berechtigungen verstehen und einrichten

Client Access Rules – Zugriff auf das Exchange Admin Center steuern

Verwaltungsrollengruppen und Verwaltungsrollen verstehen

Geteilte und gemeinsame Active Directory-Verwaltung verstehen und aktivieren

Grundlagen zu Verwaltungsrollengruppen

Pflege von Verwaltungsrollengruppen delegieren

Verwaltungsrollen im Detail

Verwaltungsrolleneinträge bearbeiten

Verwaltungsrollenbereiche verwalten

Verwaltungsrollenbereiche erstellen und verwalten

Verknüpfte Rollengruppen verwalten

Vertrauensstellungen zwischen Active Directory-Gesamtstrukturen erstellen

Verknüpfte Rollengruppe erstellen

Verwaltung von Rollengruppen überwachen

Endbenutzerrollen – Zuweisungsrichtlinien für Verwaltungsrollen

Rollenzuweisungsrichtlinien hinzufügen, entfernen und verwalten

Verwaltungsrollen zu einer Zuweisungsrichtlinie hinzufügen, entfernen und anzeigen

Definierte Berechtigungen anzeigen

Zusammenfassung

14 Datensicherung und Wiederherstellung

Grundlagen zur Exchange-Sicherung

Onlinesicherung einer Exchange-Datenbank verstehen

Grundlagen zur Onlinesicherung

Exchange-Datensicherung mit der Windows Server-Sicherung

Exchange-Daten mit dem Sicherungsprogramm wiederherstellen

Offlinesicherung der Exchange-Datenbanken

Offlinesicherung wiederherstellen

Probleme beim Offlinebackup

Erweiterte Wiederherstellungsmöglichkeiten

Wiederherstellungsdatenbanken nutzen

Exchange-Komponenten auf einem Server wiederherstellen

Datenbankportabilität verwenden

Dial Tone-Wiederherstellung

Aufbewahrungszeit für gelöschte Elemente konfigurieren
Single Item-Recovery für Exchange
Getrennte Postfächer erneut verbinden
 Outlook reparieren und wiederherstellen
Gelöschte E-Mails mit Outlook wiederherstellen
Daten aus OST-Dateien wiederherstellen
Profileinstellungen und E-Mail-Konten sichern
Outlook reparieren und Probleme lösen
Outlook startet nicht, weil ein Prozess noch aktiv ist
Add-Ins untersuchen und deaktivieren
Datendateien wiederherstellen
 Kompletten Server mit dem Sicherungsprogramm wiederherstellen
 Betriebssystem reparieren
Problemaufzeichnung – Fehler in Windows nachvollziehen und beheben
Bootprobleme beheben
Windows-Abstürze analysieren und beheben
 Zusammenfassung
 15 Hochverfügbarkeit mit Exchange 2019
 Datenbankverfügbarkeits-Gruppen verstehen
Einstieg in DAG
Mehr zu DAG, Clusterdienst und dem Active Manager
Grundlagen zur Erstellung und Verwendung einer DAG
 Datenbankverfügbarkeits-Gruppe erstellen und löschen
DAG erstellen
DAG konfigurieren
Mitglieder zu einer DAG hinzufügen, entfernen und reparieren
AutoReseed für eine Database Availability Group konfigurieren
Mitgliedsserver einer Datenbankverfügbarkeits-Gruppe wiederherstellen

Service Packs und Updates auf Mitgliedern einer Datenbankverfügbarkeits-Gruppe installieren

DAG-Netzwerke erstellen und verwalten

Postfachdatenbankkopien für DAG einrichten

Grundlagen von Postfachdatenbankkopien

Postfachdatenbankkopie erstellen

Transaktionsprotokolle verzögert schreiben

Postfachdatenbankkopien verwalten

Serverswitchover und Rechenzentrumswitchover

Zusammenfassung

16 Exchange mit Office 365

Microsoft Exchange Hybrid Agent

Hybrid Agent für Exchange Server nutzen

Microsoft Hybrid Agent für die Migration von Exchange 2010 nutzen

Hybridbereitstellungen – Voraussetzungen beachten

DNS-Einstellungen und Zertifikate konfigurieren

Exchange Online mit der PowerShell verwalten

Computer an die Cloud anbinden

Lokale Einstellungen der PowerShell setzen

PowerShell Core für die Verwaltung nutzen

Verbindung zu Exchange Online aufbauen

Visual Studio Code mit der PowerShell nutzen und Exchange Online verwalten

Exchange Online mit der PowerShell in Visual Studio Code verwalten

Office 365 mit der PowerShell gemeinsam verwalten

Überblick zum Office 365-Abonnement in der PowerShell

Office 365-Benutzer in der PowerShell verwalten

Azure Cloud Shell: Azure und Office 365 mit der PowerShell verwalten

Office 365 mit der Azure Cloud Shell verwalten

- Eigene Domänen in Office 365 anbinden und verwalten
- Domänen in Office 365 hinzufügen
- Domänen endgültig an Office 365 anbinden
 - Migration zu Office 365
 - Office 365 gemeinsam mit Exchange betreiben
- Tools für Office 365 in Verbindung mit Exchange
- OneDrive for Business in Exchange 2016/2019 einbinden
- Mail Protection Reports for Office 365
- Mit Office 365 E-Mails verschlüsseln
- Multi-Faktor-Authentifizierung in Office 365
- Client Access Policy Builder – Richtlinien für Office 365 erstellen und umsetzen
- Office 365 Mobile Device Management
- Smartphones und Tablets verbinden
 - Zusammenfassung

Teil E Migration und Überwachung

- 17 Migration und Planung
 - Planung einer Exchange 2019-Infrastruktur
 - Änderungen der Serverrollen im Überblick
 - Vorgehensweise bei der Planung von Exchange 2019
 - Festplatten-Speicher planen
 - Transaktionsprotokolle bei der Planung berücksichtigen
 - WAN-Leitungen planen
 - Migration zu Exchange Server 2019
 - Vorbereitung für die Migration – Schema-Erweiterungen
 - Exchange Server 2019-Installation durchführen
 - MAPI-HTTP aktivieren
 - Installation überprüfen und Migration vorbereiten
 - Exchange-Datenbanken für die Migration vorbereiten

Connectors anpassen
URLs, Zertifikate und Webzugriffe steuern
Transportregeln und mehr migrieren
System-Postfächer migrieren
Empfänger-Postfächer verschieben
Fehlerhafte Elemente in Postfächern berücksichtigen
Öffentliche Ordner migrieren
Öffentliche Ordner und Exchange 2010
Discovery-Mailbox und AuditLog verschieben
Checkliste für das Entfernen von Exchange-Servern
Fehlerbehebung und früheren Exchange-Server entfernen
 Allgemeine Hinweise zur Migration nach Exchange 2019 und Exchange 2010
Vollhybride Migration zu Office 365 durchführen
 Zusammenfassung
 18 Überwachung und Leistungsverbesserung
 Grundlagen des Active Directory-Zugriffs von Exchange
LDAP-Lesezugriffe mit der Leistungsüberwachung messen
 Überwachen von Exchange-Servern und Postfachzugriffen
 Exchange-Administratoren überwachen
Änderungen in der Ereignisanzeige anzeigen
 Exchange mit kostenlosen Zusatztools überwachen
Exchange Reporter – Berichte regelmäßig per E-Mail versenden
Aktivieren eines öffentlichen Ordners für E-Mail
TechNet-Gallery: Generate Exchange Environment Reports using Powershell
Modern Exchange Environment Report with Health Checks
Exchange Monitor
ManageEngine Exchange Health Monitor 3.0

Leistungsprobleme beheben: Hohe CPU-Last in den Griff bekommen

Microsoft Sysinternals Process Explorer verwenden

Exchange-Dienste verursachen eine hohe CPU-Last

Prozessorauslastung messen und optimieren

Aus der PowerShell E-Mails für Systembenachrichtigungen schreiben

Zusammenfassung

Index

Kapitel 4

Nachrichtenfluss und Connectors

In diesem Kapitel:

Informationen zum E-Mail-Routing in Exchange 2019

Sendeconnectors erstellen und verwalten

Empfangsconnectors erstellen und verwalten

Direkte Verbindung von Transportservern mit dem Internet

E-Mail-Fluss testen

Zustellungs-Agents und Transport-Agents

Allgemeine Einstellungen für Exchange-Transportserver

Akzeptierte Domänen und Remotedomänen

Warteschlangen (Queues)

Nachrichtenverfolgung (Message Tracking)

SMTP für Fortgeschrittene

Transportregeln für den Nachrichtenfluss erstellen

Zusammenfassung

In Kapitel 2 und 3 haben wir Ihnen bereits gezeigt, wie Sie Exchange so konfigurieren, dass der Versand und Empfang von E-Mails funktionieren. In diesem Kapitel gehen wir ausführlicher auf den Nachrichtenfluss und die Möglichkeiten der Connectors ein. Haben Sie Exchange 2019 installiert und angepasst, bestehen die weiteren Aufgaben darin, den E-Mail-Fluss von Exchange 2019 zu konfigurieren.

Bevor Sie sich also mit diesem Kapitel beschäftigen, sehen Sie sich die Konfiguration in Kapitel 3 erneut an. In diesem Kapitel gehen wir die

notwendigen Konfigurations- und Verwaltungsaufgaben durch, die zum Transportieren von E-Mails gehören. Exchange 2019 nutzt für den Versand von E-Mails ins Internet sowie zwischen verschiedenen Active Directory-Standorten das SMTP-Protokoll. Auch Exchange 2019 kann, wie seine Vorgänger, keine E-Mails per POP3 abholen, sondern unterstützt ausschließlich die Zustellung per SMTP (Simple Mail Transfer-Protokoll).

Viele Unternehmen haben jedoch für ihre Mitarbeiter keine einzelnen POP3-Postfächer, sondern ein Sammel-POP3-Postfach, in dem alle E-Mails des Unternehmens zugestellt werden. Ein POP3-Connector holt dann die E-Mails aus dem Postfach ab und stellt diese dem Exchange-Server zu, der wiederum die E-Mails auf Basis der E-Mail-Adressen verteilt. Das Abholen von E-Mails per POP3 kann allerdings nur für sehr kleine Unternehmen empfohlen werden und ist selbst dann nicht optimal und stabil. Größere Unternehmen sollten auf jeden Fall auf SMTP setzen.

Der erste Schritt bei der Konfiguration des E-Mail-Flusses besteht darin, dass Sie festlegen, welche E-Mail-Domänen die Exchange-Server entgegennehmen und welche über die diversen Connectors nach extern versendet werden. Bevor Sie Connectors erstellen oder Richtlinien konfigurieren, müssen Sie die SMTP-Namensräume festlegen, die die Exchange-Server Ihrer Organisation entgegennehmen.

Diese Domänen werden akzeptierte Domänen genannt (siehe Kapitel 3). Standardmäßig wird während der Installation als erste SMTP-Domäne der FQDN der Active Directory-Gesamtstruktur festgelegt. Hierbei handelt es sich allerdings nur in Ausnahmefällen auch um die E-Mail-Domäne des Unternehmens, daher müssen Sie hier zunächst Anpassungen vornehmen. Wie das geht, zeigten wir Ihnen in Kapitel 3.

Tipp

Arbeiten Sie mit einem externen Exchange-Server, zum Beispiel einem Edge-Transport-Server, der direkt mit dem Internet verbunden ist und die E-Mails über den MX-Eintrag der Domäne erhält, können Sie über die Seite <https://mxtoolbox.com> die MX-Einträge Ihrer E-Mail-Domänen überprüfen. Sie sehen hier, welche MX-Einträge vorhanden sind und welche IP-Adressen für das Zustellen der E-Mails verwendet werden.

Informationen zum E-Mail-Routing in Exchange 2019

In Exchange 2019 verschicken Postfachserver die E-Mails (siehe Kapitel 1, 2 und 3). Hub-Transport-Server gibt es seit Exchange 2013 nicht mehr. Der Edge-Transport-Server ist in Exchange 2019 verfügbar. Sie können weiterhin vorhandene Exchange 2016-Edge-Transport-Server verwenden oder diese sofort auf Exchange 2019 aktualisieren.

Ein Exchange 2010-Edge-Transport-Server erfordert eine Verbindung mit einem Hub-Transport-Server. In Exchange 2019 befindet sich der Transportdienst auf dem Postfachserver. Daher verläuft der Internetnachrichtenfluss zwischen dem Transportdienst auf dem Postfachserver und dem Edge-Transport-Server.

Sie müssen das EdgeSync-Abonnement nicht neu erstellen, wenn Sie die vorhandene Exchange 2010-Organisation auf Exchange 2019 aktualisieren. Die Verfahren zur Bereitstellung eines neuen Edge-Transport-Servers in der Exchange 2019-Organisation gleichen denen früherer Versionen von Exchange. Alle Verfahren, die auf dem Hub-Transport-Server ausgeführt werden, führen Sie in Exchange 2019 auf dem Postfachserver aus.

Bei Exchange 2019 wartet immer der sendende Server darauf, dass der empfangende Server die E-Mail entweder in ein Postfach oder einen weiteren Transport-Server zugestellt hat. Stellt der sendende Server fest, dass sich eine E-Mail auf dem Empfangsserver nicht zustellen lässt, versucht Exchange 2019 eine Zustellung auf einem alternativen Weg. Diesen Transportcache behandeln wir in den folgenden Abschnitten dieses Kapitels noch ausführlicher.

Benutzer haben die Möglichkeit, eine E-Mail bis zum Erreichen des Empfängers zu verfolgen. Mit der Nachrichtenverfolgung in Outlook Web App (OWA) können alle Benutzer Nachrichten verfolgen.

Exchange 2019 kennt mehr Filter und Aktionen beim Erstellen von neuen Transportregeln. Die Cmdlets *New-TransportRule* und *Set-TransportRule* bieten die Möglichkeit, alle Aktionen mit einem einzigen Befehl festzulegen.

Außerdem lassen sich in Exchange 2019 Regeln auf Basis eines ADRMS-Schutzes (Active Directory Rights Management Services, Active Directory-Rechteverwaltungsdienste) erstellen. Mehr zu diesem Thema erfahren Sie in Kapitel 10. Empfangsconnectors überwachen die Nachrichtenübermittlungen nach Benutzer und IP-Adresse.

Sie können direkt im Exchange Admin Center als Administrator Transport- und Journalregeln erstellen. Das Exchange Admin Center erreichen Sie über <https://<Servername>/ecp>. Über den Link *Nachrichtenfluss/Regeln* stehen Ihnen verschiedene Optionen zur Verfügung, um Transportregeln und Journalregeln zu erstellen.

Eine Komponente des Transportdienstes ist der Categorizer. Dieser entscheidet für jede E-Mail, ob sie intern zugestellt werden kann oder ins Internet zu einem Smarthost oder per MX (Mail Exchange) direkt zum Zielsystem zugestellt wird (siehe Kapitel 3). Der Ablauf beim Versenden von E-Mail ist folgender:

1. Ein Anwender verschickt über Outlook eine E-Mail. Diese E-Mail legt der Client im Postausgang ab.
2. Der Postfachserver des Anwenders erkennt die Nachricht und überträgt die E-Mail aus dem Postfach.
3. Der Transportdienst erhält die Nachricht, kategorisiert diese, wendet Nachrichtenrichtlinien an und stellt die Nachricht an einen Server am Standort des Empfängers über SMTP zu. Dabei erfolgen im Detail folgende Vorgänge.
4. Die Nachricht wird in die Submission Queue auf dem Server aufgenommen.
5. Ist auf dem Server ein Virusschutzprogramm aktiv, überprüft der Agent für den Virenschutz die E-Mail.
6. Haben Sie Journalregeln erstellt, wendet der Agent diese als nächste an.
7. Der Categorizer versucht, die Empfängeradresse in Active Directory aufzulösen, oder entscheidet auf dieser Basis, ob es sich um einen internen oder externen Empfänger handelt, auch auf Basis der verwendeten Domänen zu den E-Mail-Empfängern.
8. Anhand dieser Erkenntnis berechnet der Server die beste Route zum Empfänger und stellt die Servernamen und die IP-Adressen der nächsten Hops fest.
9. Bevor der Server die E-Mail an den nächsten Hop weiterschickt, formatiert er die Nachricht so, dass der Inhalt für den Empfänger lesbar ist. Dabei wandelt er die Mail von MIME oder UUENCODE zu Base64 um und konvertiert auch den Text entsprechend.
10. Als Nächstes wendet der Server Transportregeln an und nochmals die Journalregeln. Die Journalregel überprüft zum Beispiel nach dem

Transport-Agent, ob eine Änderung der Nachricht eine neue Journalanforderung rechtfertigt.

11. Als Nächstes stellt der Server die E-Mail in die Übermittlungswarteschlange zum nächsten Server.
12. Anschließend wird die E-Mail per SMTP an das Zielsystem gesendet.
13. Der Server überträgt die Nachricht in Form einer RPC-Verbindung zum Postfachserver des Empfängers.

Routing über verschiedene Server und Exchange-Versionen

E-Mails stellt Exchange 2019 auf Basis der Replikationsverbindungen zwischen Active Directory-Standorten zu. Dazu verwendet Exchange automatisch erstellte Connectors, die die verschiedenen Active Directory-Standorte miteinander verbinden.

Nachfolgend beschreiben wir auch die Vorgänge in Zusammenarbeit von Exchange 2010/2013/2016 mit Exchange 2019 und in Infrastrukturen, in denen nur Exchange 2019 im Einsatz ist.

Nachrichtenversand beim parallelen Einsatz von Exchange 2010/2013/2016 und 2019

In Exchange 2010 hat Microsoft Techniken integriert, um den Ausfall von Hub-Transport-Servern abzufangen und den Versand von E-Mails sicherzustellen, indem der Quellserver diese erneut versendet. In Exchange 2010 wartet immer der sendende Server darauf, dass der empfangende Server die E-Mail entweder in ein Postfach zugestellt oder an einen weiteren Transport-Server weitergeleitet hat. Stellt der sendende Server fest, dass eine E-Mail auf dem Empfangsserver nicht zugestellt werden kann, versucht Exchange 2010 eine Zustellung auf einem alternativen Weg.

Server A schickt eine Mail an Server B, der die E-Mail zwar entgegennimmt, aber aufgrund von Netzwerkproblemen nicht an Server C weiterleiten kann. Server A hat die E-Mail zwar erfolgreich an Server B zugestellt, diese aber noch nicht gelöscht. Stellt Server A fest, dass Server B die E-Mail nicht an Server C weitersenden kann, versucht Server A auf einem alternativen Weg, zum Beispiel über Server D, die E-Mail an Server C zuzustellen. Auch hier behält Server A die E-Mail weiterhin auf dem Server, bis sichergestellt ist, dass Server D die E-Mail an

Server C zugestellt hat. Geht die Kette weiter, übernimmt Server D die Überwachung, ob Server C die Mail an Server E weitergeleitet hat und so weiter.

Exchange überwacht nicht nur die Zustellung an den nächsten Server, sondern auch an den übernächsten. Die Kommunikation für diese Technik erfolgt mit den beiden SMTP-Befehlen *XSHADOW* und *XQDISCARD*. Haben Sie auf einem Server die beiden Rollen *Postfach* und *Hub-Transport* installiert, versucht Exchange auch bei einer lokalen Zustellung von E-Mails, diese an einen weiteren Hub-Transport-Server zu senden, bevor eine direkte Zustellung erfolgt. Sinn dieser Technik ist, dass eine E-Mail immer auf zwei Transportservern liegen muss, um sicherzustellen, dass sie nicht verloren geht.

In Einzelfällen kann es durchaus passieren, dass E-Mails einem Anwender mehrfach zugestellt werden. Allerdings ist das sicher besser als ein Totalverlust der E-Mail. Damit diese Technik funktioniert, muss der empfangende Server dem sendenden Server mit *XSHADOW* mitteilen, dass er diese Technik auch beherrscht. Die Meldung wird beim Senden von EHLO an den sendenden Server übertragen. Mit dem SMTP-Befehl *XQDISCARD* fragt der sendende Server beim empfangenden Server ab, welche E-Mails er an weitere Server übertragen hat und der sendende Server daher löschen kann.

Erst wenn sich der sendende Server beim empfangenden Server authentifiziert hat und er dann die *XSHADOW*-Meldung erhält, legt er eine spezielle Warteschlange an, in der er die E-Mails, die er an den empfangenden Server sendet, zwischenspeichern kann. Vorher werden die E-Mails ganz normal behandelt.

Nach der erfolgreichen Übertragung von *XSHADOW* fragt der sendende Server immer wieder mit *XQDISCARD* beim sendenden Server nach, ob die E-Mail versendet ist und aus der Cachewarteschlange entfernt werden kann. Das Intervall dazu sind fünf Minuten, in denen der Server jeweils dreimal mit *XQDISCARD* nachfragt. Erhält der sendende Server innerhalb dieser Zeit keine Antwort, versucht er die Zustellung an andere Transportserver der Organisation. Insgesamt testet der Server bis zu sieben Tage eine mögliche Zustellung, bevor die E-Mail als nicht zustellbar erkannt wird und der Absender einen Nichtzustellbarkeitsbericht erhält.

Über das Internet kann diese Technik nur dann Einsatz finden, wenn sich der sendende Server am empfangenden Server authentifiziert. Erst nach der Authentifizierung findet die *XSHADOW*-Abfrage statt.

Der Transportcache ist standardmäßig nach der Installation von Exchange 2019 bereits aktiviert. Sie können den Status über die Exchange Management Shell anzeigen lassen, indem Sie den Befehl *Get-TransportConfig* eingeben. Den Status finden Sie im Bereich *ShadowRedundancyEnabled*. Am schnellsten überprüfen Sie den Status mit *Get-TransportConfig |fl *Shadow**.

```
[PS] C:\WINDOWS\system32>Get-TransportConfig |fl *Shadow*

ShadowRedundancyEnabled           : True
ShadowHeartbeatTimeoutInterval    : 00:15:00
ShadowHeartbeatRetryCount         : 12
ShadowHeartbeatFrequency          : 00:02:00
ShadowResubmitTimeSpan            : 03:00:00
ShadowMessageAutoDiscardInterval : 2.00:00:00
RejectMessageOnShadowFailure      : False
ShadowMessagePreferenceSetting    : PreferRemote
MaxRetriesForLocalSiteShadow      : 2
MaxRetriesForRemoteSiteShadow     : 4
```

Abbildung 4.1: Anzeigen der Transportkonfiguration eines Servers in der Exchange Management Shell

Mit dem Befehl *Set-TransportConfig -ShadowRedundancyEnabled \$true* aktivieren Sie den Transportcache, der Befehl *Set-TransportConfig -ShadowRedundancyEnabled \$false* deaktiviert die Technik.

Mit den Optionen *ShadowHeartbeatTimeoutInterval* (Standardwert ist 15 Minuten) und *ShadowHeartbeatRetryCount* (Standardwert ist 12) des Cmdlets *Set-TransportConfig* konfigurieren Sie das Intervall. Die Option *ShadowMessageAutoDiscardInterval* steuert den maximalen Verbleib in der Cache-Warteschlange.

Ein Beispielaufruf für die Änderung auf zehn Minuten und acht Versuche sieht so aus:

```
Set-TransportConfig -ShadowHeartbeatTimeoutInterval 00:10:00 -
ShadowHeartbeatRetryCount 8
```

Senden Sie mit Outlook oder Outlook Web App eine E-Mail, stellt der Client diese in den Postausgang. Anschließend holt sich ein Hub-Transport-Server die E-Mail ab, wenn Sie mit Exchange 2010 arbeiten. Der Client bemerkt das und kopiert die E-Mail in den Ordner für gesendete Objekte. Kann der Hub-Transport-Server die E-Mail nicht zustellen, bemerkt das der Postfachserver und veranlasst, dass

ein weiterer Hub-Transport-Server die E-Mail aus den gesendeten Objekten abholt und zustellt.

Setzen Sie Exchange 2010/2013/2016/2019 zusammen mit Exchange 2003/2007 ein, erhält ein Transport-Server keine Antwort durch *XSHADOW*, da die älteren Exchange-Versionen diese Technik nicht beherrschen. In diesem Fall sendet Exchange die Nachricht dennoch, verwendet aber nicht den Transportcache.

Dies bedeutet, bei gemischten Umgebungen kann der Versand von E-Mails nicht sichergestellt werden. Das gilt auch, wenn Exchange die Nachricht an ein externes System versendet, das den Cache nicht unterstützt. Auch hier funktioniert der Empfang, ist aber nicht durch den Cache abgesichert.

Mit der Option *MaxAcknowledgementDelay* des Cmdlets *Set-ReceiveConnector* konfigurieren Sie die maximale Verzögerung, die der Empfangsconnector beim Empfang von Systemen ohne Unterstützung des Transportcache auf eine SMTP-Bestätigung wartet. Standardmäßig ist für den Empfangsconnector eine Bestätigungsverzögerung von bis zu 30 Sekunden eingestellt.

Für Exchange 2010/2013 empfiehlt Microsoft ausdrücklich, Clientzugriffsserver nicht in der DMZ (demilitarisierten Zone) zu betreiben. Alle E-Mails, auch interne E-Mails zwischen verschiedenen Postfachservern, leitet Exchange 2016/2019 immer über den Transportdienst. Dies hat den Vorteil, dass hinterlegte Transportregeln immer auf alle E-Mails angewendet werden.

Haben Sie die akzeptierten E-Mail-Domänen festgelegt, können Sie Connectors erstellen, um den Nachrichtenfluss Ihrer Exchange-Organisation zu steuern (siehe auch Kapitel 3). Die Basis der Connectors sind die akzeptierten Domänen (siehe Kapitel 3). Unter Exchange 2019 gibt es Sende- und Empfangsconnectors. Diese müssen auf den einzelnen Servern konfiguriert sein, damit der Nachrichtenfluss funktioniert.

Empfangsconnectors legt Exchange bereits bei der Installation an, Sendeconnectors müssen Sie manuell erstellen (siehe Kapitel 3). Sie müssen keinerlei Connectors erstellen oder konfigurieren, um den Nachrichtenfluss zwischen Servern innerhalb des Unternehmens zu steuern, auch nicht zwischen Active Directory-Standorten. Die notwendigen Connectors und Verbindungen richtet Exchange automatisch ein.

Während der Installation von Exchange 2019 erstellt Exchange automatisch Connectors, die den Transport zwischen Servern steuern. Diese Connectors basieren auf den Standorten von Active Directory.

E-Mail-Routing in Exchange 2019

Die wichtigste Verbesserung der Shadow-Redundanz seit Exchange 2013 ist, dass der Transport-Server eine redundante Kopie aller empfangenen Nachrichten erstellt, bevor dem sendenden Server der Empfang der Nachricht bestätigt wird. Diese Technik hat Microsoft auch in Exchange 2016/2019 übernommen.

Ob der sendende Server die Shadow-Redundanz unterstützt oder nicht, spielt keine Rolle mehr. So wird sichergestellt, dass von allen Nachrichten eine redundante Kopie erstellt wird, während sie übermittelt werden. Falls Exchange 2019 feststellt, dass die ursprüngliche Nachricht während der Übertragung verloren gegangen ist, wird die redundante Kopie der Nachricht übermittelt. Diese Funktion ist in Exchange 2019 standardmäßig aktiv.

Wenn eine Nachricht von einem Transport-Server innerhalb der Transportgrenze für Hochverfügbarkeit empfangen wird, versucht Exchange, zwei redundante Kopien der Nachricht auf den Transport-Servern innerhalb der Grenze beizubehalten. Wenn eine Nachricht die Transportgrenze für Hochverfügbarkeit überschreitet, behält Exchange die redundanten Nachrichtenkopien nicht mehr bei.

E-Mails, die vom Transportdienst auf einem Postfachserver erfolgreich verarbeitet oder an einen Postfachempfänger übermittelt wurden, werden in das Sicherheitsnetz verschoben.

Sie können Exchange 2019 so konfigurieren, dass eine Nachricht zurückgewiesen wird, auch wenn keine redundante E-Mail-Kopie erstellt wurde. Verwenden Sie dafür das Cmdlet *Set-TransportConfig* mit der Option *RejectMessageOnShadowFailure*. Die E-Mail wird mit einem vorübergehenden Fehler zurückgewiesen, der sendende Server kann die Nachricht jedoch erneut übertragen. Der SMTP-Antwortcode lautet *451 4.4.0 Message failed to be made redundant*. Sie sollten Exchange so konfigurieren, dass Nachrichten, von denen keine redundante Kopie erstellt werden kann, nur dann zurückgewiesen werden, wenn Ihre Organisation über mehrere Exchange 2019-Postfachserver verfügt.

Tipp Das Cmdlet *Set-TransportConfig* mit der Option *ShadowRedundancyEnabled \$true* aktiviert die Shadow-Redundanz auf allen Transport-Servern in der Organisation. Mit *\$false* wird die Shadow-Redundanz auf allen deaktiviert.

Über das Cmdlet *Set-TransportConfig* mit der Option *RejectMessageOnShadowFailure \$false* legen Sie fest, dass die primäre Nachricht trotzdem von den Transport-Servern in der Organisation akzeptiert wird. Mit *\$true* werden Nachrichten von keinem Transportserver akzeptiert oder bestätigt, bis eine Schattenkopie der Nachricht erstellt wurde. Wenn keine Schattenkopie der Nachricht erstellt werden kann, wird die primäre Nachricht mit einem vorübergehenden Fehler zurückgewiesen.

Sie sollten diesen Wert nur dann auf *\$true* festlegen, wenn Sie über mehrere Exchange 2019-Postfachserver in einer Datenbankverfügbarkeitsgruppe (Database Availability Group, DAG) oder an einem Active Directory-Standort verfügen. Diese Option ist nur von Bedeutung, wenn die Option *ShadowRedundancyEnabled* auf *\$true* festgelegt ist.

Das Hauptziel der Shadow-Redundanz besteht darin, immer über zwei Kopien einer Nachricht innerhalb einer Transportgrenze für Hochverfügbarkeit zu verfügen, während die Nachricht übermittelt wird. Bei einer Transportgrenze für Hochverfügbarkeit kann es sich um Folgendes handeln:

- Eine DAG für Postfachserver, die Mitglieder einer DAG sind. Hierzu gehören auch DAGs, die sich über mehrere Active Directory-Standorte erstrecken.
- Ein Active Directory-Standort für Postfachserver, die zu keiner DAG gehören.

Die Shadow-Redundanz verfolgt nie Shadow-Nachrichten über eine Transportgrenze für Hochverfügbarkeit hinweg. Wenn eine Nachricht die Transportgrenze für Hochverfügbarkeit überschreitet, beginnt die Shadow-Redundanz oder wird neu gestartet. Dadurch wird der Datenverkehr durch Shadow-Nachrichten reduziert und verhindert, dass Shadow-Nachrichten über die Transportgrenze für Hochverfügbarkeit hinweg erneut gesendet werden. Hub-Transport-Server in Exchange 2010 sind ein Sonderfall.

Wenn der Transportdienst auf einem Exchange 2019-Postfachserver eine Nachricht von einem Absender außerhalb der Transportgrenze für Hochverfügbarkeit empfängt, spielt es für den Postfachserver keine Rolle, ob der sendende Server die Shadow-Redundanz unterstützt oder nicht. Solange die Shadow-Redundanz aktiviert ist, erstellt der Postfachserver, der die Nachricht empfängt, eine redundante Kopie der Nachricht auf einem anderen

Postfachserver innerhalb der Transportgrenze für Hochverfügbarkeit und bestätigt danach dem sendenden Server den Empfang der Nachricht.

Wenn ein Exchange 2019-Transport-Server eine Nachricht an einen Empfänger außerhalb der Transportgrenze für Hochverfügbarkeit überträgt und der SMTP-Server auf der anderen Seite den Empfang der Nachricht bestätigt, verschiebt er die Nachricht, wie alle anderen erfolgreich verarbeiteten Nachrichten, in das Sicherheitsnetz. Die Nachricht kann aus dem Sicherheitsnetz nicht erneut übermittelt werden.

Hinweis Wenn ein Hub-Transport-Server in Exchange 2010 eine Nachricht an einen Exchange 2019-Postfachserver am gleichen Active Directory-Standort überträgt, kündigt er in Exchange 2010 über den *XSHADOW*-Befehl Unterstützung für die Shadow-Redundanz an, der Postfachserver jedoch nicht. Dies verhindert, dass der Hub-Transport-Server in Exchange 2010 eine Schattenkopie der Nachricht auf einem Exchange 2019-Postfachserver erstellt.

Wenn der Transportdienst auf einem Exchange 2019-Postfachserver eine Nachricht an einen Exchange 2010-Hub-Transport-Server am gleichen Active Directory-Standort überträgt, erstellt der Exchange 2019-Postfachserver eine Schattenkopie der Nachricht für den Exchange 2010-Hub-Transport-Server.

Nachdem der Exchange 2019-Postfachserver die Bestätigung vom Exchange 2010-Hub-Transport-Server über den Empfang der Nachricht erhalten hat, verschiebt er die erfolgreich verarbeitete Nachricht in das Sicherheitsnetz.

Wenn der primäre Server die Nachricht erfolgreich an den nächsten Hop übertragen und dieser Hop den Empfang der Nachricht bestätigt hat, aktualisiert er den Löschstaus der Nachricht in *Übertragung abgeschlossen*. Der Shadow-Server ermittelt den Löschstaus der Shadow-Nachrichten in den Shadow-Warteschlangen, indem der primäre Server abgefragt wird.

Wenn der Shadow-Server eine SMTP-Sitzung mit dem primären Server öffnet, führt er den Befehl *XQUERYDISCARD* aus, um den Löschstaus der primären Nachrichten zu ermitteln. Wenn er innerhalb eines konfigurierten Zeitintervalls keine SMTP-Sitzung mit dem primären Server geöffnet hat, öffnet er eine SMTP-Sitzung mit dem primären Server und führt den *XQUERYDISCARD*-Befehl aus.

Das Zeitintervall wird über das Cmdlet *Set-TransportConfig* mit der Option *ShadowHeartbeatFrequency* gesteuert. Nachdem der Shadow-Server eine SMTP-

Sitzung mit dem primären Server geöffnet hat, antwortet der primäre Server mit den Löschenbenachrichtigungen für Nachrichten, die für den abfragenden Shadow-Server relevant sind.

Hinweis In Exchange 2019 werden Löschenbenachrichtigungen nicht im Arbeitsspeicher, sondern auf einem Datenträger gespeichert. Aus diesem Grund bleiben die Löschenbenachrichtigungen nach einem Neustart des Microsoft Exchange-Transportdienstes erhalten.

Nach dem Start des Dienstes stehen die Informationen zu erfolgreich verarbeiteten Nachrichten sowohl dem primären Server als auch dem Shadow-Server weiterhin zur Verfügung.

Die Shadow-Redundanz minimiert den Nachrichtenverlust aufgrund von Serverausfällen. Wenn ein Transportserver nach einem Ausfall wieder online geschaltet wird, gibt es zwei Möglichkeiten:

1. Der Server wird mit einer neuen Transportdatenbank online geschaltet. In diesem Szenario kann die Transportdatenbank aufgrund von Datenbeschädigung oder eines Hardwarefehlers nicht wiederhergestellt werden.

Da der Transportserver in diesem Fall über eine neue Datenbank-ID verfügt, wird er von den anderen Transportservern in der Organisation als neue Route erkannt. Dies gilt auch für Situationen, in denen ein Server nicht wiederhergestellt werden kann und als Ersatz ein neuer Server bereitgestellt wird.

2. Der Server wird mit derselben Transportdatenbank online geschaltet. In diesem Szenario ist der betreffende Transportserver nicht ausgefallen, sondern war so lange offline, bis der Shadow-Server den Besitz für die Nachrichten übernommen und diese erneut übermittelt hat. Dieses Szenario kann beispielsweise durch einen Netzwerkkartenfehler oder eine längere Wartung des Servers verursacht werden.

Im folgenden Beispiel wird angenommen, dass es sich bei dem ausgefallenen Server um den Server *Mailbox01* handelt:

1. *Mailbox01* wird mit einer neuen Datenbank wieder online geschaltet.
2. Wenn *Mailbox01* nicht mehr verfügbar ist, übernimmt jeder Server, der Shadow-Nachrichten für *Mailbox01* in die Warteschlange eingereicht

hat, den Besitz für diese Nachrichten und übermittelt sie erneut. Die Nachrichten werden an ihre Ziele übermittelt.

3. Die maximale Verzögerung für Nachrichten entspricht dem Wert der Option *ShadowHeartbeatFrequency* im Cmdlet *Set-TransportConfig*. Der Standardwert beträgt zwei Minuten.

Ein weiteres Beispiel:

1. *Mailbox01* wird mit derselben Datenbank wieder online geschaltet:
2. Anschließend übermittelt der Server die Nachrichten in seiner Warteschlange, die bereits von denjenigen Servern übermittelt wurden, auf denen Schattenkopien der Nachrichten für *Mailbox01* gespeichert sind. Dies führt zur doppelten Zustellung dieser Nachrichten. Exchange-Postfachbenutzer erhalten aufgrund der Funktion zur Erkennung von Nachrichtenduplikaten keine doppelten Nachrichten. Empfänger in anderen Messagingsystemen als Exchange erhalten jedoch möglicherweise Duplikate ihrer Nachrichten.
3. Die maximale Verzögerung für Nachrichten entspricht dem Wert der Option *Shadow-ResubmitTimeSpan* im Cmdlet *Set-TransportConfig*. Der Standardwert ist drei Stunden.

Sicherheitsnetz in Exchange 2019

In Exchange 2019 ist der primäre Mechanismus für hohe Verfügbarkeit von Postfächern die Datenbankverfügbarkeitsgruppe (Database Availability Group, DAG). In Exchange 2010 schützt der Transportdumpster vor Datenverlusten. Dazu wurde eine Warteschlange erfolgreich zugestellter Nachrichten beibehalten, die noch nicht in passiven Postfachdatenbankkopien in der DAG repliziert wurden. Wenn aufgrund eines Ausfalls einer Postfachdatenbank oder eines Servers eine veraltete Kopie der Postfachdatenbank höhergestuft werden musste, wurden die Nachrichten im Transportdumpster automatisch an die neue aktive Kopie der Postfachdatenbank erneut übermittelt.

Der Transportdumpster in Exchange 2019 heißt Sicherheitsnetz. Das Sicherheitsnetz ist eine Warteschlange, die mit dem Transportdienst auf einem Postfachserver verbunden ist. In dieser Warteschlange werden Kopien von Nachrichten gespeichert, die vom Server erfolgreich verarbeitet wurden.

Sie können angeben, wie lange das Sicherheitsnetz Kopien der erfolgreich verarbeiteten Nachrichten speichert, bevor sie ablaufen und automatisch gelöscht werden. Das Sicherheitsnetz erfordert keine DAGs. Für Postfachserver,

die zu DAGs gehören, speichert das Sicherheitsnetz Kopien zugestellter Nachrichten auf anderen Postfachservern am lokalen Active Directory-Standort.

Das Sicherheitsnetz ist redundant. Wenn das primäre Sicherheitsnetz für mehr als zwölf Stunden nicht verfügbar ist, werden Anforderungen zur Neuübermittlung zu Anforderungen zur Shadow-Neuübermittlung, und Nachrichten werden aus dem Shadow-Sicherheitsnetz erneut übermittelt. Für die Shadow-Redundanz wird eine redundante Kopie der Nachricht gespeichert, während die Nachricht übertragen wird. Das Sicherheitsnetz bewahrt eine redundante Kopie einer Nachricht auf, nachdem die Nachricht erfolgreich verarbeitet wurde. Das Sicherheitsnetz setzt also da ein, wo die Shadow-Redundanz endet.

Das primäre Sicherheitsnetz befindet sich auf dem Postfachserver, auf dem die primäre Nachricht vorhanden war, bevor sie erfolgreich vom Transportdienst verarbeitet wurde. Nachdem der primäre Server die primäre Nachricht verarbeitet hat, wird die Nachricht von der aktiven Warteschlange in das primäre Sicherheitsnetz auf demselben Server verschoben.

Das Shadow-Sicherheitsnetz befindet sich auf dem Postfachserver, auf dem die Shadow-Nachricht vorhanden war. Sobald der Shadow-Server ermittelt, dass der primäre Server die primäre Nachricht erfolgreich verarbeitet hat, verschiebt er die Shadow-Nachricht aus der Shadow-Warteschlange in das Shadow-Sicherheitsnetz auf demselben Server.

Zustellungsgruppen, Routingziele und Transportdienste verstehen

Das Routing in Exchange 2019 bietet eine vollständige Unterstützung für Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAG). In Exchange 2019 hosten alle Postfachserver den Transportdienst.

Hinweis Der Transportdienst auf einem Postfachserver kommuniziert nie direkt mit einer Postfachdatenbank, sondern mit dem Postfachtransportdienst auf dem Postfachserver.

Nur der Postfachtransportdienst kommuniziert mit der Postfachdatenbank auf dem lokalen Postfachserver. Wenn der Postfachserver Mitglied einer DAG ist, akzeptiert nur der Postfachtransportdienst auf dem Postfachserver, auf dem die

aktive Kopie der Postfachdatenbank gespeichert ist, eine Nachricht für den Zielempfänger.

Der Postfachtransportdienst verwendet RPC (Remote Procedure Call), um Nachrichten an die lokale Postfachdatenbank zu senden oder von dieser zu empfangen. Wenn der Postfachserver Mitglied einer DAG ist, verwendet der Postfachtransportdienst RPC nur zur lokalen Kommunikation mit den aktiven Kopien der Postfachdatenbanken. RPCs werden daher nie für die serverübergreifende Kommunikation verwendet. Stattdessen kommunizieren der Postfachtransportdienst und die Transportdienste auf anderen Postfachservern über SMTP.

Für das Routing in Exchange 2019 wurden Routingziele und Zustellungsgruppen eingeführt. Das endgültige Ziel einer Nachricht wird als *Routingziel* bezeichnet. Postfachdatenbanken sind das Routingziel für jeden Empfänger mit einem Postfach in der Exchange-Organisation.

Hinweis Das Routen von Nachrichten an Empfänger in öffentlichen Ordnern funktioniert in Exchange 2019 genauso wie das Routen von Nachrichten an Postfachempfänger.

Ein Zustellungs-Agent-Connector oder ein fremder Connector wird als Routingziel für Nachrichten verwendet, die nicht über SMTP gesendet werden. Das können zum Beispiel auch Fax-Connectors sein.

Ein Server für die Aufgliederung der Verteilergruppen kann ebenfalls ein Routingziel sein, wenn eine Verteilergruppe über einen eigenen Server verfügt, der für die Aufgliederung der Mitgliedsliste der Gruppe zuständig ist. Ein Server für die Aufgliederung der Verteilergruppen ist immer ein Hub-Transport-Server oder ein Exchange 2019-Postfachserver.

Jedes Routingziel in Exchange 2019 verfügt über einen Transportserver, der für die Zustellung von Nachrichten an dieses Routingziel zuständig ist. Es kann sich dabei auch um eine Sammlung von Servern handeln. Diese Sammlung von Transportservern wird als Zustellungsgruppe bezeichnet. Bei einem Transportserver kann es sich um einen Exchange 2019-Postfachserver oder einen Exchange 2010-Server handeln, auf dem die Hub-Transport-Serverrolle installiert ist. Wenn das Routingziel eine Postfachdatenbank ist, müssen die Transportserver in der Zustellungsgruppe mit der gleichen Exchange-Version installiert sein wie die Postfachdatenbank. Wenn das Routingziel ein Connector oder ein Server für die Aufgliederung der Verteilergruppen ist, kann die

Zustellungsgruppe sowohl Exchange 2019-Postfachserver als auch Exchange 2010-Hub-Transport-Server umfassen.

Wenn der Quelltransportserver sich in der Zielzustellungsgruppe befindet, ist das Routingziel selbst der nächste Hop für die Nachricht. Die Nachricht wird vom Quelltransportserver an die Postfachdatenbank oder den Connector auf einem Transportserver in der Zustellungsgruppe gesendet.

Wenn sich der Quelltransportserver außerhalb der Zielzustellungsgruppe befindet, wird die Nachricht über den kostengünstigsten Routingpfad an die Zielzustellungsgruppe weitergeleitet. Es gibt bei diesen Vorgängen verschiedene Arten von Zustellungsgruppen:

Routingfähige DAGs sind eine Sammlung von Exchange 2019-Postfachservern, die zu einer gemeinsamen DAG gehören. Die Postfachdatenbanken in der DAG sind die Routingziele, die von dieser Zustellungsgruppe verwaltet werden. Wenn eine Nachricht vom Transportdienst auf einem Postfachserver empfangen wurde, leitet der Transportdienst die Nachricht an den Postfachtransportdienst auf dem Postfachserver in der DAG weiter, auf dem derzeit die aktive Kopie der Zielpostfachdatenbank gespeichert ist. Der Postfachtransportdienst auf dem Zielpostfachserver sendet die Nachricht anschließend an die lokale Postfachdatenbank.

Eine Postfachzustellungsgruppe ist eine Sammlung von Exchange-Servern der gleichen Version, die sich am selben Active Directory-Standort befinden. Der Active Directory-Standort stellt die Grenze der Zustellungsgruppe dar. Die Postfachdatenbanken auf Exchange 2010-Postfachservern werden von den Exchange 2010-Hub-Transport-Servern am Active Directory-Standort bedient.

Die Postfachdatenbanken auf Exchange 2019-Postfachservern am Active Directory-Standort, die zu keiner DAG gehören, werden vom Transportdienst auf Exchange 2019-Postfachservern am Active Directory-Standort bedient.

Wenn eine Nachricht auf dem Zielpostfachserver am Active Directory-Zielstandort empfangen wurde, leitet der Transportdienst die Nachricht unter Verwendung von SMTP an den Postfachtransportdienst weiter. Der Postfachtransportdienst sendet die Nachricht dann mit RPC an die lokale Postfachdatenbank.

In Exchange 2010 wird die Nachricht einem zufälligen Exchange 2010-Hub-Transport-Server am Active Directory-Zielstandort zugestellt. Dieser verwendet RPC, um die Nachricht in die Postfachdatenbank zu schreiben.

Eine Mitgliedschaft in mehreren Zustellungsgruppen ist möglich. Zum Beispiel kann ein Exchange 2019-Postfachserver, der Mitglied einer DAG ist, auch der Quellserver eines Sendecollectors mit Bereich sein.

Wenn ein Server eine Nachricht an eine Remotezustellungsgruppe senden muss, muss ein Routingpfad für die Nachricht ermittelt werden. Exchange 2019 berechnet den kostengünstigsten Routingpfad, indem die Kosten der IP-Standortverknüpfungen addiert werden, die zum Erreichen des Ziels durchlaufen werden müssen. Wenn das Ziel ein Connector ist, werden die dem Adressraum zugewiesenen Kosten zu den Kosten addiert, die zum Erreichen des Connectors erforderlich sind. Sind mehrere Routingpfade möglich, verwendet Exchange den Routingpfad mit den geringsten Gesamtkosten. Wenn mehrere Routingpfade die gleichen Gesamtkosten aufweisen, wird der Routingpfad mit der geringsten Anzahl von Hops verwendet.

Exchange verwendet den Routingpfad, der dem Ziel am nächsten ist und in der alphanumerischen Reihenfolge am niedrigsten ist. In Exchange 2019 kann sich eine Zustellungsgruppe über mehrere Active Directory-Standorte erstrecken. Außerdem kann es mehrere Routingpfade zu mehreren Active Directory-Zielstandorten geben. Exchange legt einen einzigen Active Directory-Standort in der Zielzustellungsgruppe als primären Standort fest.

Der Front-End-Transportdienst wird auf allen Clientzugriffsservern ausgeführt und fungiert als Proxy für den eingehenden und ausgehenden externen SMTP-Datenverkehr für die Exchange 2019-Organisation. Für ausgehende Nachrichten verwendet der Transportdienst Sendecollectors zur Kommunikation mit dem Front-End-Transportdienst auf einem Clientzugriffsserver.

Ausgehende Nachrichten werden per Proxy über den Front-End-Transportdienst weitergeleitet, wenn der Parameter *FrontEndProxyEnabled* des Sendecollectors auf *\$true* festgelegt ist oder wenn in den Eigenschaften des Sendecollectors im Exchange Admin Center die Option *Proxy über Clientzugriffsserver* ausgewählt ist. Exchange verwendet einen beliebigen Front-End-Transportserver am lokalen Active Directory-Standort. Nur der Transportdienst auf dem Postfachserver verfügt über Sendecollectors.

Der Transportdienst lädt Routingtabellen basierend auf Informationen aus Active Directory und verwendet Zustellungsgruppen, um die Weiterleitung von Nachrichten festzulegen. Der Front-End-Transportdienst wird nicht als Mitglied einer Zustellungsgruppe betrachtet, auch wenn der Postfachserver und der

Clientzugriffsserver auf dem gleichen Server installiert sind. Daher kann der Front-End-Transportdienst nur mit dem Transportdienst kommunizieren.

Die Routingtabellen enthalten keine Sendecconnectorrouten, aber eine spezielle Liste mit Postfachservern am lokalen Active Directory-Standort, damit ein Failover möglich ist. Beim Routing im Front-End-Transportdienst werden die Namen der Nachrichtempfänger in den Postfachdatenbanken aufgelöst. Der Front-End-Transportdienst sucht für jede Postfachdatenbank die Zustellungsgruppe und die zugehörigen Routinginformationen.

Für Nachrichten, die an einen Empfänger gerichtet sind, wird ein Postfachserver in der Zielzustellungsgruppe ausgewählt. Dabei wird der Postfachserver bevorzugt, der dem Active Directory-Standort am nächsten gelegen ist. Für Nachrichten, die an Empfänger mit mehreren Postfächern gerichtet sind, werden die ersten 20 Empfänger verwendet, um einen Postfachserver in der am nächsten gelegenen Zustellungsgruppe auszuwählen.

Der Postfachtransportdienst wird auf allen Postfachservern ausgeführt und besteht aus zwei getrennten Diensten: dem Dienst für die Postfachtransportübermittlung und dem Dienst für die Postfachtransportzustellung. Bei eingehenden Nachrichten empfängt der Dienst für die Postfachtransportzustellung SMTP-Nachrichten vom Transportdienst und stellt über einen RPC eine Verbindung mit der lokalen Postfachdatenbank her, um die Nachricht zuzustellen. Bei ausgehenden Nachrichten stellt der Dienst für die Postfachtransportübermittlung über einen RPC eine Verbindung mit der lokalen Postfachdatenbank her, um die Nachrichten abzurufen, und übermittelt die Nachrichten per SMTP an den Transportdienst. Der Postfachtransportdienst ist zustandslos und stellt keine Nachrichten in die lokale Warteschlange.

Ebenso wie der Transportdienst lädt der Postfachtransportdienst Routingtabellen basierend auf Informationen aus Active Directory und verwendet Zustellungsgruppen, um die Weiterleitung von Nachrichten festzulegen.

Der Postfachtransportdienst weist jedoch einige einzigartige Routingaspekte auf: Da sich der Transportdienst und der Postfachtransportdienst auf demselben Exchange 2019-Postfachserver befinden, gehört der Postfachtransportdienst immer zur selben Zustellungsgruppe wie der Postfachserver. Diese Zustellungsgruppe wird als lokale Zustellungsgruppe bezeichnet.

Der Dienst für die Postfachtransportübermittlung sendet Nachrichten nicht automatisch an den Transportdienst auf dem lokalen Postfachserver oder auf

anderen Postfachservern in der eigenen lokalen Zustellungsgruppe. Der Dienst für die Postfachtransportübermittlung greift auf die gleichen Informationen zur Routingtopologie zu wie der Transportdienst und kann daher Nachrichten an den Transportdienst auf Postfachservern außerhalb der Zustellungsgruppe senden. Die Postfachserver in der lokalen Zustellungsgruppe werden als Fallbackoptionen genutzt und zur Zustellung an Empfänger ohne Postfach verwendet.

Der Postfachtransportdienst kommuniziert nur mit dem Transportdienst auf dem lokalen Exchange 2019-Postfachserver. Er kommuniziert niemals mit Postfachdatenbanken auf anderen Postfachservern. Wenn ein Benutzer eine Nachricht aus dem Postfach sendet, löst der Dienst die Namen der Nachrichtempfänger auf. Wenn der Dienst für die Postfachtransportzustellung eine Nachricht vom Transportdienst empfängt, kann er die Zustellung der Nachricht an eine lokale Postfachdatenbank akzeptieren oder ablehnen.

Der Dienst für die Postfachtransportzustellung kann die Nachricht zustellen, wenn sich der Empfänger in einer aktiven Kopie einer lokalen Postfachdatenbank befindet. Ist dies nicht der Fall, kann er die Nachricht nicht zustellen und muss dem Transportdienst einen Unzustellbarkeitsbericht senden.

Sendeconnectors erstellen und verwalten

Sendeconnectors verwalten Sie im Exchange Admin Center über den Menüpunkt *Nachrichtenfluss* auf der Registerkarte *Sendeconnectors*. Im Gegensatz zu Empfangsconnectors legt Exchange während der Installation keinen Sendecconnector an. Sie müssen manuell mindestens einen Connector anlegen, damit Exchange E-Mails versenden kann. Mehr zu diesem Thema lesen Sie auch in Kapitel 3.

Hinweis Standardmäßig legt Exchange 2019 zwar Empfangsconnectors zum Empfangen von E-Mails an, allerdings keine Sendecconnectors. Um E-Mails mit Exchange zu versenden, müssen Sie also immer auch Sendecconnectors erstellen.

Sendeconnectors speichert Exchange in Active Directory als Konfigurationsobjekt. Erhält ein Server eine E-Mail, überprüft er in Active Directory, welcher Sendecconnector für die E-Mail-Domäne zuständig ist, und stellt die E-Mail entsprechend zu. Dazu sind im Connector die Server hinterlegt, die die E-Mails zustellen können.

Sind für einen Sendecconnector mehrere Server zuständig, verteilt der Connector die E-Mails lastabhängig. Durch diese Konfiguration erhalten Sie eine Ausfallsicherheit, da die E-Mail erst zugestellt wird, wenn der empfangende Server auch tatsächlich zur Verfügung steht. Diese Ausfallsicherheit gilt aber nur für die Server, die für einen einzelnen Connector konfiguriert sind. Legen Sie mehrere Connectors für denselben Adressraum an, wird diese Lastverteilung außer Funktion gesetzt. Sendecconnectors stellen logische Gateways dar, um den Nachrichtenfluss innerhalb und nach beziehungsweise von außerhalb der Organisation zu steuern.

Neue Sendecconnectors erstellen

Wie bereits erwähnt, erstellt Exchange bei der Installation standardmäßig keine Sendecconnectors. Sie müssen mindestens einen Sendecconnector manuell erstellen und konfigurieren, wenn die Server in Ihrem Unternehmen eine direkte Verbindung zum Internet haben sollen (siehe Kapitel 3). Sie benötigen im Unternehmen mindestens einen Sendecconnector, auf dem hinterlegt ist, welche E-Mail-Domänen über welche Server ins Internet versendet werden.

Sie müssen keine Sendecconnectors zwischen den Exchange-Servern Ihrer Organisation untereinander erstellen. Nur Connectors, die ins Internet oder zu anderen E-Mail-Systemen Nachrichten übermitteln, müssen Sie manuell erstellen. Haben Sie den Assistenten zur Erstellung eines neuen Sendecconnectors aufgerufen, legen Sie auf der ersten Seite zunächst einen Namen fest.

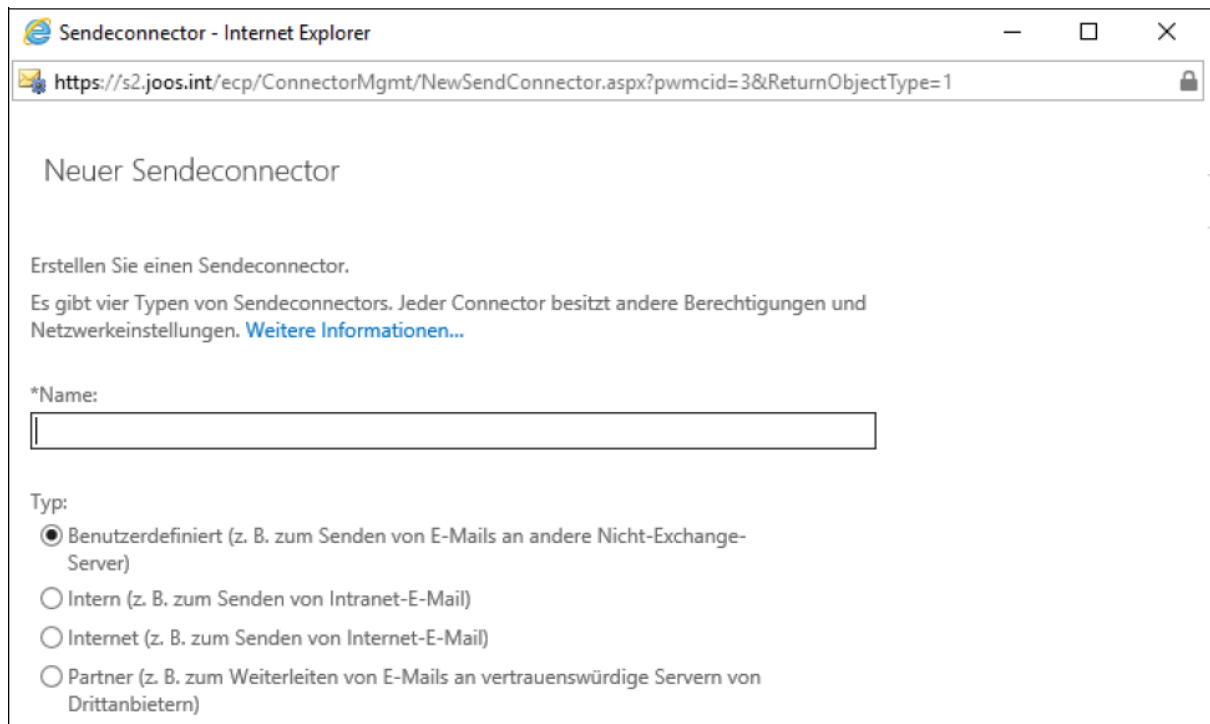


Abbildung 4.2: Erstellen eines neuen Sendconnectors

Auf der ersten Seite legen Sie auch die Verwendung des Connectors fest. Durch die Auswahl des Verwendungstyps bestimmen Sie die Authentifizierung für den Connector. Sie müssen allerdings nicht zwingend einen Verwendungstyp auswählen, sondern können die Auswahl auch auf *Benutzerdefiniert* belassen. Alle Möglichkeiten zur Authentifizierung lassen sich auch nachträglich festlegen:

- **Intern** Erstellen Sie einen Sendconnector für den internen Versand innerhalb Ihrer Organisation, wählen Sie als Verwendungstyp *Intern* aus. Dies kann zum Beispiel sinnvoll sein, wenn Sie zwischen zwei Servern spezifische Connectors, auch auf Basis von Domänen, erstellen wollen.
- **Internet** Wollen Sie über den Connector E-Mails ins Internet zustellen, dann verwenden Sie diese Option.
- **Partner** Diese Art von Connector verwenden Sie, wenn Sie E-Mails zwischen verschiedenen Organisationen oder E-Mail-Systemen im Unternehmen oder zwischen Partnern versenden wollen. Bei dieser Art von Connector können Sie beispielsweise mit TLS-Verschlüsselung (Transport Layer Security) auf Basis von SSL (Secure Sockets Layer) und Zertifikaten arbeiten. Dieser Connector wird so konfiguriert, dass er nur Verbindungen zu Servern zulässt, die sich mit TLS-Zertifikaten authentifizieren und die in der Liste der Domänen enthalten sind. Verwenden Sie zur Konfiguration das Cmdlet *Set-TransportConfig* mit der Option *TLSSendDomainSecureList*.

Auf der nächsten Seite legen Sie fest, wohin die E-Mails gesendet werden sollen, die über diesen Connector verschickt werden. Sie können an dieser Stelle entweder eine IP-Adresse, einen FQDN oder die Auflösung über MX-Einträge verwenden.

Wählen Sie die direkte Zustellung per MX-Eintrag, müssen Sie zuvor sicherstellen, dass Ihre Exchange-Server Internetadressen über DNS auflösen können und auch das Recht haben, zu den einzelnen Empfangsservern direkt E-Mails zu senden. Sie müssen dazu Ihre internen DNS-Server so konfigurieren, dass auch externe Internetadressen aufgelöst werden können.

Neuer Sendeconnector

Ein Sendeconnector kann E-Mails direkt über das DNS weiterleiten oder zu einem Smarthost umleiten. [Weitere Informationen...](#)

*Netzwerkeinstellungen:
Geben Sie an, wie mit diesem Connector E-Mails gesendet werden.

Mit der Empfängerdomäne verbundener MX-Eintrag
 E-Mail über Smarthosts weiterleiten

+ ✎ -

SMARTHOST

Die Einstellungen für externes DNS-Lookup auf Servern mit Transportrollen verwenden

Abbildung 4.3: Festlegen des Ziels eines Sendeconnectors

Die direkte Zustellung bietet sich eigentlich nur für größere Firmen an. Das Problem ist, dass viele E-Mail-Server im Internet nicht von allen Servern E-Mails annehmen, sondern nur von großen und bekannten Providern, deren Server eine statische IP-Adresse besitzen. Haben Sie keine statische IP-Adresse im Internet, sondern arbeiten Sie mit einer dynamischen IP-Adresse (haben also zum Beispiel einen typischen DSL-Anschluss), werden Sie mit vielen E-Mail-Servern Schwierigkeiten haben.

Wählen Sie in dem Fall zur Sicherheit die Zustellung zu Ihrem Provider aus, der auch den DNS-Server für Ihre Domäne verwaltet. Dieser sendet die E-Mails weiter. Die notwendigen Daten dieses Smarthosts erhalten Sie von Ihrem Provider.

Um einen neuen Smarthost hinzuzufügen, klicken Sie auf das Plus-Zeichen. Aktivieren Sie zusätzlich noch die Option *Die Einstellungen für externes DNS-Lookup auf Servern mit Transportrollen verwenden*, wenn Sie, statt der hinterlegten DNS-Server im Netzwerkadapter, eigene DNS-Server für den Connector hinterlegen wollen, die die Namensauflösung für den Connector durchführen. Dadurch können Sie die herkömmliche Namensauflösung von Windows von der DNS-Auflösung für E-Mails trennen. Diese Einstellung ist aber nur optional.

Sie finden diese DNS-Server über das Cmdlet *Set-TransportService* oder über das Menü *DNS-Lookups* in den Eigenschaften des Servers im Exchange Admin Center bei *Server*. Die Einstellung können Sie jederzeit anpassen, auch nach der Erstellung des Sendeconnectors.

Auf der nächsten Seite des Assistenten zum Erstellen neuer Sendeconnectors legen Sie den Adressraum fest, der über diesen Connector versendet werden soll. Wollen Sie alle E-Mail-Domänen über diesen Connector versenden, wählen Sie als Domäne den Platzhalter * aus.

Hinweis Sie können beim Anlegen von neuen Sendeconnectors für einzelne E-Mail-Domänen einen eigenen Connector erstellen. Findet Exchange keinen passenden Connector für eine spezielle Domäne, wird automatisch der Connector mit dem Adressraum * verwendet. Wird ein passender Connector gefunden, verwendet Exchange diesen auch dann, wenn ein Connector mit dem Adressraum * vorhanden ist.



Abbildung 4.4: Festlegen eigener DNS-Server für die Namensauflösung

Haben Sie zum Versenden einen Smarthost eingetragen, geben Sie auf der nächsten Seite die Authentifizierungsdaten für ihn ein. Unterstützt der empfangende E-Mail-Server das Transport Layer Security-Protokoll (TLS), können Sie die Option *Standardauthentifizierung erst nach dem Start von TLS anbieten* aktivieren. In diesem Fall wird die Authentifizierung verschlüsselt. Allerdings unterstützen nicht alle E-Mail-Server standardmäßig TLS.

Bei der TLS-Verschlüsselung handelt es sich um eine besondere Art der SSL-Verbindung. Im Gegensatz zur normalen Übertragung ist es bei TLS nicht mehr möglich, den Datenverkehr zwischen zwei SMTP-Servern abzuhören. Benötigt der empfangende E-Mail-Server keine Authentifizierung, können Sie die Einstellung auf *Keine* belassen. Wenn Sie mehrere Smarthosts angeben, müssen alle Smarthosts den gleichen Benutzernamen und das Kennwort akzeptieren.

Konfigurieren Sie die Smarthostauthentifizierung. [Weitere Informationen...](#)

Smarthostauthentifizierung:

Keine

Standardauthentifizierung

Standardauthentifizierung erst nach dem Start von TLS anbieten

*Benutzername:

*Kennwort:

Hinweis: Alle Smarthosts müssen denselben Benutzernamen und dasselbe Kennwort akzeptieren.

Exchange-Serverauthentifizierung

Extern gesichert (z. B. mit IPSec)

Abbildung 4.5: Konfigurieren der Authentifizierung für den Smarthost

Zusätzlich haben Sie an dieser Stelle noch zwei weitere Möglichkeiten zur Authentifizierung:

- **Exchange-Serverauthentifizierung** Bei dieser Art wird eine Exchange-interne Authentifizierung wie TLS oder Kerberos verwendet.
- **Extern gesichert** Bei dieser Einstellung können Sie zum Beispiel IPsec oder ein VPN (virtuelles privates Netzwerk) für die Verbindung verwenden. Bevor der Connector nach einem Verbindungsaufbau E-Mails zu senden versucht, wird auf die Authentifizierung gewartet. Diese wird allerdings nicht durch den Exchange-Server gesteuert.

Alternativ können Sie auch einen eigenen Connector für einzelne E-Mail-Domänen erstellen. Exchange verwendet immer den Connector mit der hinterlegten E-Mail-Domäne zum Versenden und erst dann Connectors mit dem Platzhalter. Mit der Deaktivierung der Option *Sendconnector mit Bereich* kann der Connector standardmäßig von allen Servern in der Exchange-Organisation verwendet werden. Aktivieren Sie diese Option, kann der Connector nur von Servern verwendet werden, die am selben Active Directory-Standort positioniert sind.

Anschließend wählen Sie aus, welche Transportserver dieser Connector verwenden darf, um seine E-Mails zu versenden. Wählen Sie an dieser Stelle mehrere Server aus, verteilt der Connector das Versenden der E-Mails auf Basis der Last der Server. Ist ein Server nicht verfügbar, verwendet der Connector einen anderen hinterlegten Quellserver.

Der Connector wird im Anschluss im Exchange Admin Center angezeigt. Klicken Sie ihn doppelt an oder rufen Sie seine Eigenschaften auf, können Sie alle konfigurierten Einstellungen nachträglich anpassen.

Sendeconnectors in der Exchange Management Shell erstellen

Mit dem Cmdlet *New-SendConnector* *-Name* <Connectorname> *-AddressSpaces* <Adressraum> <Optionale Parameter> erstellen Sie Connectors auch in der Exchange Management Shell von Exchange:

```
New-SendConnector -Name "Microsoft" -Usage Custom -
AddressSpaces "*.microsoft.com;1","*.fabrikam.com;2" -
DNSRoutingEnabled $false -SmartHosts 192.168.178.95 -
MaxMessageSize 20MB
```

- *Name*: Microsoft
- *Verwendungstyp*: Benutzerdefiniert
- SMTP-Adressraum *microsoft.com* und alle Unterdomänen
- Die Adressraumkosten sind 1. Exchange verwendet immer den Connectorweg mit den niedrigsten Gesamtkosten, also der Summe aller verwendeten Connectors.
- Der Connector sendet außerdem noch E-Mails an die Domäne *fabrikam.com*, ebenfalls mit allen Unterdomänen. Die Adressraumkosten zu diesem Namensraum sind 2.
- Der Connector verwendet den Smarthost 192.168.178.95.
- Für diesen Connector gilt eine maximale Nachrichtengröße von 20 MB. Größere E-Mails verweigert der Connector und informiert den Absender darüber.

Die Option *IsCoexistenceConnector* wird in Exchange 2016/2019 nicht mehr unterstützt. Wenn Sie eine Hybridumgebung konfigurieren, in der die Postfächer zum Teil lokal und zum Teil in der Cloud gehostet werden, empfiehlt sich die Verwendung des Assistenten für die Hybridkonfiguration.

Ebenfalls nicht mehr unterstützt wird die Option *LinkedReceiveConnector*. Diese wurde zum Beispiel in Exchange 2010 zum Erstellen von Connectors verwendet, die Nachrichten an den Antispamdienst eines Drittanbieters routen konnten. In Exchange 2019 werden E-Mails an den Antispamdienst unter Verwendung des MX-Eintrags geroutet, und verknüpfte Connectors sind nicht erforderlich.

Die standardmäßige maximale Nachrichtengröße, die durch die Option *MaxMessageSize* angegeben wird, wurde erhöht. Die Option *TlsCertificateName* wurde in Exchange 2013 hinzugefügt und wird zum Authentifizieren des lokalen Zertifikats für ausgehende Verbindungen verwendet.

Sendecollectors verwalten

Rufen Sie die Eigenschaften von Sendecollectors auf, können Sie alle Einstellungen, die Sie beim Erstellen angeben, über verschiedene Menüs ändern. Die Optionen haben wir in den vorangegangenen Abschnitten behandelt. Im folgenden Abschnitt gehen wir auf die Möglichkeiten ein, die sich nicht aus den vorangegangenen Abschnitten ergeben.

Internet-Sende-Connector

► **Allgemein**
Zustellung
Bereichsdefinition

*Name:
Internet-Sende-Connector

Connectorstatus:
 Aktivieren
 Proxy über Clientzugriffsserver

Kommentar:

Protokolliergrad:
 Keine
 Ausführlich

*Maximale Größe für gesendete Nachricht (MB):
35

Abbildung 4.6: Verwalten der Eigenschaften eines Connectors

Sie können über den Aktionsbereich rechts im Exchange Admin Center einen Connector auch zeitweise deaktivieren. Ein deaktivierter Connector kann jederzeit wieder aktiviert werden, sodass er für den E-Mail-Verkehr wieder zur Verfügung steht. Die Konfiguration des Connectors geht während der Deaktivierung nicht verloren. Sie deaktivieren einen Connector, indem Sie ihn

mit einem Mausklick im Exchange Admin Center markieren und im Aktionsbereich auf den Link *Deaktivieren* klicken.

Auf der Registerkarte *Allgemein* in den Eigenschaften können Sie nachträglich den Namen des Connectors anpassen:

- **Connectorstatus** Zeigt an, ob der Connector aktiviert oder deaktiviert ist. Den Status können Sie an dieser Stelle ebenfalls ändern.
- **Protokolliergrad** Wählen Sie hier aus, welche Bereiche Exchange bezüglich des Connectors protokollieren soll.
- **Maximale Größe für gesendete Nachricht (MB)** Geben Sie hier einen Wert in Megabyte ein, wenn Sie für die Nachrichten, die über diesen Connector gesendet werden, eine maximale Nachrichtengröße festlegen wollen. Der gültige Eingabebereich liegt zwischen 0 und 2.096.128 MB. Um alle Einschränkungen aufzuheben, aktivieren Sie die Option *unlimited*.

Eigenschaften eines Sendecollectors mit der Exchange Management Shell konfigurieren

Mit dem Cmdlet *Set-SendConnector* können Sie Einstellungen für einen vorhandenen Sendecollector anpassen. Ein Beispiel wäre

```
Set-SendConnector "Verbindung zu Contoso.com" -MaxMessageSize 50MB -ProtocolLoggingLevel Verbose
```

Über dieses Cmdlet können Sie auch Parameter konfigurieren, die in der GUI nicht zur Verfügung stehen, zum Beispiel den Wert *ForceHELO*, mit dem Sie die Verwendung des älteren SMTP-Befehls *HELO* statt des neueren *EHLO* erzwingen können. Dies kann notwendig sein, wenn Sie mit einem Postfachserver kommunizieren wollen, der den neuen Befehl nicht versteht.

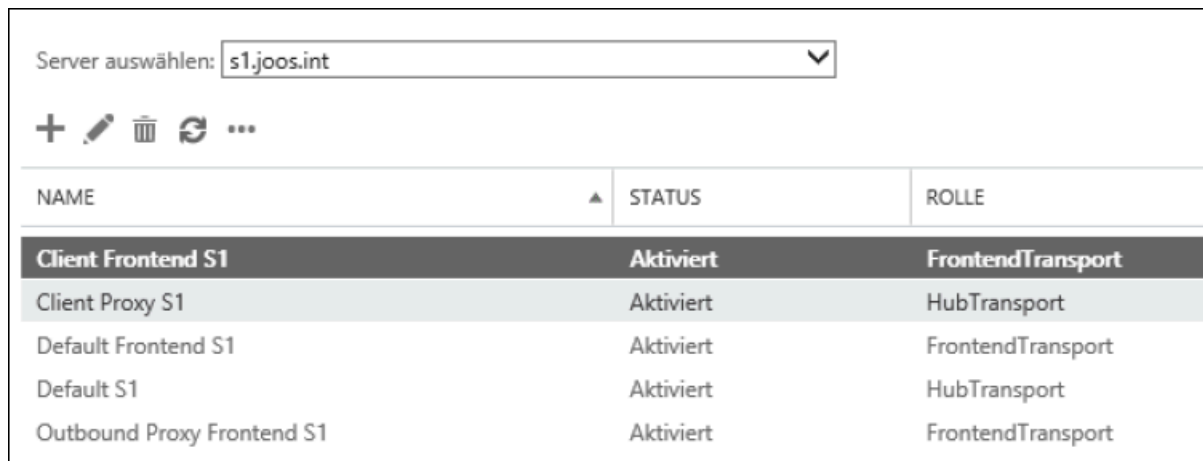
Zudem können Sie für spezielle Netzwerkumgebungen den Parameter *Port* angeben, falls die Kommunikation mit dem anderen Server auf einem anderen Port als dem standardmäßigen Port TCP/25 erfolgen soll.

Empfangscollectors erstellen und verwalten

Empfangscollectors werden direkt für einzelne Exchange-Server auf Serverebene erstellt. Diese Collectors bilden auf Exchange-Servern den SMTP-Endpunkt, zu dem andere Server Verbindungen aufbauen und E-Mails senden.

Ohne einen Empfangsconnector kann ein Exchange 2019-Transportserver keine E-Mails empfangen.

Während der Installation von Exchange 2019 erstellt der Assistent automatisch Empfangsconnectors, die Sie aber nachträglich bearbeiten oder anpassen können. Der Connector *Default Frontend <Servername>* ist bereits so konfiguriert, dass er E-Mails aus dem Internet empfangen kann.



NAME	STATUS	ROLLE
Client Frontend S1	Aktiviert	FrontendTransport
Client Proxy S1	Aktiviert	HubTransport
Default Frontend S1	Aktiviert	FrontendTransport
Default S1	Aktiviert	HubTransport
Outbound Proxy Frontend S1	Aktiviert	FrontendTransport

Abbildung 4.7: Verwalten der Exchange-Empfangsconnectors

Wenn Sie einen Empfangsconnector erstellen, wird er in Active Directory als untergeordnetes Objekt des Servers gespeichert.

Neue Empfangsconnectors erstellen

Sie finden die Konfiguration von Empfangsconnectors im Exchange Admin Center über *Nachrichtenfluss/Empfangsconnectors*. Die angelegten Empfangsconnectors werden im Ergebnisfenster der Konsole im unteren Bereich angezeigt. Über das Pluszeichen erstellen Sie einen neuen Connector.

Bereits nach der Installation von Exchange sind standardmäßige Empfangsconnectors angelegt, allerdings keine Sendeconnectors. Für beide Standardconnectors ist keine Konfiguration erforderlich, da beide bereits korrekt eingestellt sind. Sie können die Namen aber nachträglich in den Eigenschaften anpassen:

- **Client Frontend <Servername>** Dieser Connector dient dem Verbindungsaufbau von Nicht-MAPI-Clients, zum Beispiel der Verbindung über POP3 oder IMAP4. Der Connector nimmt über jede Netzwerkverbindung von allen IP-Adressen entsprechende Anfragen

entgegen. Er antwortet auf den Port 587 auf die Anfrage von Nicht-MAPI-Clients.

- **Default <Servername>** Dieser Connector nimmt Nachrichten von anderen Transportservern der Organisation auf Port 25 entgegen. Er akzeptiert ebenfalls Verbindungen von allen IP-Adressen. Dieser Connector ist zudem für den Empfang externer E-Mails zuständig.

Starten Sie den Assistenten für die Erstellung eines neuen Empfangsconnectors, haben Sie ähnliche Auswahlmöglichkeiten wie bei der Erstellung eines Sendeconnectors. Wenn Sie den Assistenten starten, müssen Sie auf der ersten Seite zunächst den Namen und den Verwendungszweck festlegen.

Neuer Empfangsconnector

Der Assistent erstellt einen Empfangsconnector.
Es gibt fünf Arten von Empfangsconnectors. Jeder Connector verfügt über andere Berechtigungen und Authentifizierungsverfahren. [Weitere Informationen...](#)

*Name:
[]

Server:
s1.joos.int

Rolle:
 Hub-Transport
 Front-End-Transport

Typ:
 Benutzerdefiniert (um z. B. Anwendungsrelays zuzulassen)
 Intern (z. B. zum Empfangen von Intranet-E-Mail)
 Internet (z. B. zum Empfangen von Internet-E-Mail)
 Partner (z. B. zum Weiterleiten von E-Mails von vertrauenswürdigen Servern von Drittanbietern)
 Client (z. B. zum Empfangen von E-Mails von Nicht-Outlook-Clients)

Weiter Abbrechen

Erstellen Sie einen aussagekräftigen, unterscheidbaren Namen.

Abbildung 4.8: Erstellen eines neuen Empfangsconnectors

Beim Verwendungszweck können Sie zwischen fünf Punkten auswählen, die hauptsächlich für die Konfiguration der Authentifizierung benötigt werden:

- **Benutzerdefiniert** Es ist nicht zwingend notwendig, die Authentifizierung bereits dann festzulegen, wenn Sie einen neuen

Connector für bestimmte Szenarien erstellen. In diesem Fall können Sie die Option *Benutzerdefiniert* verwenden.

- **Intern** Erstellen Sie einen Empfangsconnector für den internen Versand Ihrer Organisation oder einen Empfangsconnector zwischen verschiedenen Gesamtstrukturen innerhalb Ihres Unternehmens, wählen Sie als Verwendungstyp *Intern* aus.
- **Internet** Wählen Sie diese Option aus, kann der Connector Nachrichten aus dem Internet empfangen. Dazu wird die Authentifizierung deaktiviert, sodass der Exchange-Server auch anonyme Verbindungen entgegennimmt. Da die Authentifizierung nicht erlaubt ist, kann dieser Connector nicht von externen Clients mit Anmeldung als Relay verwendet werden.
- **Partner** Bei dieser Art von Connector können Sie, wie beim Sendecconnector, eine interne TLS-Verschlüsselung konfigurieren.
- **Client** Bei dieser Art von Connector nimmt der Connector E-Mails von Anwendern entgegen, die sich nicht mit Outlook (MAPI) oder Outlook Web App mit dem Server verbinden, sondern E-Mails per SMTP versenden.

Auf der nächsten Seite geben Sie die IP-Adressen des Servers an, bei denen er auf eine Verbindung warten soll. Standardmäßig hört der Connector auf Port 25 alle verbundenen IP-Adressen.

Jeder Empfangsconnector benötigt eine eigene Kombination aus IP-Adresse und Port, auf die er hören kann. Standardmäßig hören die bereits angelegten Empfangsconnectors auf alle verfügbaren IP-Adressen des Servers.

Haben Sie als Verwendungstyp *Benutzerdefiniert*, *Partner*, *Intern* oder *Client* ausgewählt, erscheint die Seite *Remotenetzwerkeinstellungen*. Geben Sie auf der Seite die IP-Adresse oder den IP-Adressbereich der Remoteserver ein, von denen der Connector eingehende Verbindungen akzeptiert.

Wenn Sie zum Beispiel die Adresse 192.168.1.1 eingeben, akzeptiert der Empfangsconnector nur Nachrichten von diesem Host. Geben Sie 192.168.1.0/24 an, akzeptiert der Empfangsconnector Nachrichten aus dem gesamten Klasse-C-Subnetz von 192.168.1.0. Sie können an dieser Stelle sowohl IPv4- als auch IPv6-Adressen angeben.

Tipp Mit dem Cmdlet *New-ReceiveConnector* erstellen Sie Empfangsconnectors in der Exchange Management Shell.

Sicherheit von Empfangsconnectors verwalten

Wie Sendecollectors können Sie auch bei Empfangsconnectors die Eigenschaften aufrufen, um deren Konfiguration zu ändern. Hierüber können Sie Collectors auch deaktivieren oder löschen.

Client Frontend S1

Allgemein

► **Sicherheit**

Bereichsdefinition

- Transport Layer Security (TLS)
 - Domänensicherheit aktivieren (Gegenseitige TLS-Authentifizierung)
- Standardauthentifizierung
 - Standardauthentifizierung erst nach dem Start von TLS anbieten
- Integrierte Windows-Authentifizierung
- Exchange-Serverauthentifizierung
- Extern gesichert (z. B. mit IPSec)

Berechtigungsgruppen:
Geben Sie an, wer eine Verbindung mit diesem Empfangsconnector herstellen darf.

- Exchange-Server
- Legacy-Exchange-Server
- Partner
- Exchange-Benutzer
- Anonyme Benutzer

Abbildung 4.9: Konfigurieren der Eigenschaften von Empfangsconnectors

Auf der Registerkarte *Sicherheit* können Sie nachträglich die Authentifizierung für Empfangsconnectors konfigurieren, also wie sich Clients an diesem Server anmelden müssen, damit der Connector E-Mails entgegennimmt. Dabei haben Sie sieben verschiedene Möglichkeiten:

- **Transport Layer Security (TLS)** Aktivieren Sie diese Option, verwendet der Server das *STARTTLS* in der *EHLO*-Antwort an SMTP-Server, die eine Verbindung herstellt, und wartet auf eine TLS-Authentifizierung. Die Datenübertragung ist ähnlich wie beim Zugriff auf eine HTTPS-Adresse über SSL verschlüsselt.

- **Domänensicherheit aktivieren (Gegenseitige TLS-Authentifizierung)** Aktivieren Sie diese Option, muss der Empfangsconnector sich mit TLS-Authentifizierung am Remoteserver genauso authentifizieren wie der Remoteserver sich am lokalen Server.
- **Standardauthentifizierung** Aktivieren Sie diese Option, verwendet der Connector *AUTH* in der *EHLO*-Antwort an SMTP-Server, die eine Verbindung herstellen. Der Server akzeptiert dann die Standardauthentifizierung. Da bei der Standardauthentifizierung der Benutzername und das Kennwort unverschlüsselt beziehungsweise nur Base64-codiert gesendet werden, sollten Sie zusätzlich mit TLS-Verschlüsselung arbeiten.
- **Standardauthentifizierung erst nach dem Start von TLS anbieten** Aktivieren Sie diese Option, startet der Connector zunächst TLS und bietet erst danach die Standardauthentifizierung an. In diesem Fall wird die Übertragung des Benutzernamens und des Kennworts verschlüsselt.
- **Integrierte Windows-Authentifizierung** Aktivieren Sie diese Option, verwendet der Connector NTLM und Kerberos für die Authentifizierung. Hierbei werden keine Kennwörter übertragen.
- **Exchange-Serverauthentifizierung** Aktivieren Sie diese Option, benutzt der Connector eine TLS-Vertrauensstellung oder Kerberos über TLS, die nur von Exchange-Servern für die interne Kommunikation verwendet wird. Unterstützt werden die Versionen Exchange 2003/2007/2010/2013/2019.
- **Extern gesichert (z. B. mit IPSec)** Bei dieser Option wird die Verbindung durch ein VPN oder über IPsec gesichert. Aktivieren Sie diese Option, kann Exchange diese Sicherung nicht überprüfen, da sie außerhalb der Exchange-Dienste stattfindet.

Bevor Sie jedoch diese Authentifizierungsmethode auswählen, sollten Sie zuerst die Option *Exchange-Server* im Bereich *Berechtigungsgruppen* wählen, damit die Kommunikation funktioniert. Hier steuern Sie über vordefinierte Sammlungen von Berechtigungen, wer E-Mails an diesen Empfangsconnector senden darf. Jeder Berechtigungsgruppe wird ein unterschiedlicher Satz von Berechtigungen erteilt. Folgende Optionen sind verfügbar:

- **Exchange-Server** Mitglieder der universellen Sicherheitsgruppe *Exchange-Servers* in der OU *Microsoft Exchange Security Groups* in Active Directory
- **Legacy-Exchange-Server** Mitglieder der universellen Sicherheitsgruppe *Exchange-LegacyInterop* in der gleichen OU in Active Directory

- **Partner** Benutzerkonten aus anderen Gesamtstrukturen, die an diese Organisation angebunden sind
- **Exchange-Benutzer** Authentifizierte Benutzerkonten
- **Anonyme Benutzer** Nicht authentifizierte Benutzer

Mit dem Cmdlet *Set-ReceiveConnector* können Sie Einstellungen für einen vorhandenen Empfangsconnector über die Exchange Management Shell anpassen.

Relaying für Applikationsserver erlauben

In vielen Unternehmen gibt es Server, zum Beispiel ERP-, CRM- oder auch SharePoint-Server, die für ihre Funktionen einen E-Mail-Server auf SMTP-Basis ansprechen müssen, um E-Mails zu senden. Dies gilt auch für Multifunktionsgeräte oder Scanner.

Aus Sicherheitsgründen blockiert Exchange E-Mails, die nicht von internen Anwendern kommen. Dabei ist es unerheblich, ob Exchange E-Mails intern zustellen oder über entsprechende Connectors nach extern versenden soll. Ist das Relaying für den Server deaktiviert, erhalten andere Server die Meldung *550 5.7.1 Unable to relay*. Die Lösung dieses Problems sollte sein, dem Server das Relaying zu erlauben. Sie finden diese Einstellungen im Exchange Admin Center über *Nachrichtenfluss/Empfangsconnectors*:

1. Rufen Sie die Einstellungen des Connectors *Default <Servername>* auf, sehen Sie bei *Sicherheit* und *Bereichsdefinition*, von welchen Servern der Connector E-Mails empfängt.
2. Wollen Sie weiteren Servern das Senden erlauben, sollten Sie einen neuen Empfangsconnector erstellen, der E-Mails von den entsprechenden Geräten entgegennimmt. Den Standardconnector sollten Sie möglichst nicht verändern.

Tipp Die Einstellung der aktuellen Empfangsconnectors können Sie auch in der Exchange Management Shell mit dem Befehl *Get-ReceiveConnector* anzeigen lassen.

Um einen neuen Connector zu erstellen, der das Relaying erlaubt, gehen Sie folgendermaßen vor:

1. Starten Sie das Exchange Admin Center.

2. Klicken Sie auf *Nachrichtenfluss/Empfangsconnectors*.
3. Erstellen Sie einen neuen Connector.
4. Weisen Sie dem Connector einen Namen zu und wählen Sie im darunter befindlichen Listenfeld den Eintrag *Benutzerdefiniert* aus.
5. Entfernen Sie auf der nächsten Seite den vorhandenen Eintrag der hinterlegten IP-Adressen und klicken Sie auf *Hinzufügen*.
6. Tragen Sie die IP-Adresse des Exchange-Servers ein und bestätigen Sie mit *Speichern*.
7. Auf der nächsten Seite *Remotenetzwerkeinstellungen* löschen Sie den Eintrag und klicken auf *Hinzufügen*. Geben Sie hier die IP-Adressen aller Geräte ein, die zu diesem Connector E-Mails senden sollen.
8. Schließen Sie die Erstellung des Connectors ab.
9. Rufen Sie anschließend die Eigenschaften des Connectors auf.
10. Wechseln Sie zur Registerkarte *Sicherheit*.
11. Aktivieren Sie das Kontrollkästchen *Anonyme Benutzer*.
12. Überprüfen Sie alle Einstellungen der restlichen Registerkarten und bestätigen Sie dann das Fenster mit *Speichern*.
13. Öffnen Sie die Exchange Management Shell und geben Sie den folgenden Befehl ein:

```
Get-ReceiveConnector "<Empfangsconnector>" | Add-ADPermission -User "ANONYMOUS-ANMELDUNG" -ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"
```

Sie können die hier durchgeführten Aufgaben aber auch in der Exchange Management Shell durchführen:

```
New-ReceiveConnector -Name "Relay" -RemoteIPRanges ("10.0.0.54","10.0.0.55") -TransportRole "FrontendTransport"&nbsp; -Bindings ("0.0.0.0:25") -Usage "Custom" -Server "<Server>"
```

```
Get-ReceiveConnector "<Servername>\Relay" | Add-ADPermission -User "ANONYMOUS-ANMELDUNG" -ExtendedRights "Ms-Exch-SMTP-Accept-Any-Recipient"
```

Direkte Verbindung von Transportservern mit dem Internet

Sie können Transportserver auch ohne Edge-Transport-Server direkt mit dem Internet verbinden. In diesem Fall muss ein Sendecorrelator erstellt werden, der direkt eine Verbindung zum Internet aufbauen kann. Gehen Sie bei der Erstellung eines Sendecorrelators für die Internetanbindung eines Servers genauso vor wie in diesem Kapitel und in Kapitel 3 beschrieben. Geben Sie als Adressraum den Platzhalter * ein, damit dieser Connector alle E-Mails ins Internet versenden kann, für die es noch keinen anderen Connector gibt.

Damit ein Server über das Internet erreichbar ist (wenn Sie SMTP-Gateway verwenden), sollten Sie einen neuen Empfangsconnector erstellen und diesem als Verwendungstyp *Internet* zuweisen. Achten Sie darauf, diesem Connector eine eindeutige IP-Adresse zuzuweisen.

Auch bei den bereits angelegten Connectors sollten Sie den IP-Bereich anpassen, damit keine Überschneidungen entstehen. Erstellen Sie einen Empfangsconnector mit dem Verwendungstyp *Internet*, lässt dieser auch anonyme Verbindungen zu. Aus diesem Grund sollten Sie möglichst die Verbindung von Internet und internen E-Mails voneinander trennen.

Am besten ist es, wenn Sie für die Internetanbindung eine eigene Netzwerkkarte mit eigener IP-Adresse in den Server einbauen und diese IP-Adresse für den Empfangsconnector für Internetmails verwenden. Zwischen den Netzwerkkarten können Sie mit einer Firewall, zum Beispiel auch der Windows-Firewall, eine sichere Kommunikation ermöglichen.

E-Mail-Fluss testen

Sie können in der Exchange Management Shell auch den E-Mail-Fluss testen. Dazu verwenden Sie das Cmdlet *Test-Mailflow -SourceMailboxServer <Postfachserver>*. Sie erhalten auch hier das passende Ergebnis und können feststellen, ob der E-Mail-Fluss auf dem entsprechenden Postfachserver funktioniert.

Zusammen mit dem E-Mail-Fluss auf den Exchange-Servern sollten Sie auch die Abarbeitung der Warteschlangen auf den Transportservern überprüfen. Auch hier stehen Cmdlets in der Exchange-Verwaltungsshell zur Verfügung: *Get-TransportServer | Get-Queue*.

Die einzelnen Ports auf den Servern sollten Sie ebenfalls testen. Dazu verwenden Sie das Cmdlet *Test-NetConnection* und den entsprechenden Port:

```
Test-NetConnection -ComputerName <Servername> -Port  
<Portnummer>
```

Vor allem die Ports 25 (Transportserver), 135 (Clientzugriff-Server und Postfachserver), 443 (Clientzugriff-Server), 587 (Transportserver) müssen offen sein und kommunizieren können.

Laden Sie sich von der Seite <https://www.frankysweb.de> das PowerShell-Skript *.\Test-Mail-Domain.ps1* herunter. Mit diesem können Sie testen, ob die eigenen oder andere E-Mail-Domänen optimal von Exchange erreicht werden können. Falls erforderlich, müssen Sie vorher über *Set-ExecutionPolicy* die Ausführung des Skripts erlauben.

Die Syntax ist:

```
.\Test-MailDomain.ps1 -Domainname <Domäne>
```

Zustellungs-Agents und Transport-Agents

Für die Zusammenarbeit mit Drittherstellerprodukten, die Exchange zum Austauschen von E-Mails nutzen, spielen Zustellungs-Agents und Transport-Agents eine wichtige Rolle. Wir gehen nachfolgend auf diese Connectors ein.

Zustellungs-Agents und -Connectors

Ein Zustellungs-Agent kann Nachrichten aus Ihrer SMTP-Exchange-Serverumgebung an ein System zustellen, in dem das SMTP-Protokoll nicht verwendet wird, zum Beispiel ein Fax-Connector. Jeder Zustellungs-Agent ist einem Zustellungs-Agent-Connector zugeordnet. Der Connector reiht an den Zustellungs-Agent weitergeleitete Nachrichten für die Verarbeitung an das Nicht-SMTP-Gerät weiter oder in eine Warteschlange ein.

Die Vorteile dieses Systems sind, dass Sie die Warteschlangenverwaltung für Nachrichten verwenden können, keine Dateiübertragung an einen Ablageordner notwendig ist und Sie die Nachrichtenzustellung überprüfen können.

Ein Zustellungs-Agent ist eine im Transportdienst eines Postfachservers installierte Software, die eine Verbindung an das fremde System für die Nachrichtenzustellung herstellen kann. Die Software ist in der Lage, Nachrichten aus den Warteschlangen auf den Postfachservern abzurufen und an das fremde

System zuzustellen. In der Regel werden Zustellungs-Agents von Drittanbietern zur Verfügung gestellt. Achten Sie beim Einsatz aber auf Kompatibilität zu Exchange 2019.

Zum Lieferumfang von Exchange 2019 gehört ein Zustellungs-Agent-Connector für Textnachrichten. Installieren Sie den entsprechenden Zustellungs-Agent im Transportdienst auf den Postfachservern, die als Quellserver für die Zustellungs-Agent-Connectors dienen.

Ein Zustellungs-Agent-Connector leitet Nachrichten weiter, die an fremde Systeme ohne SMTP-Protokoll gerichtet sind. Wenn eine Nachricht an den Zustellungs-Agent-Connector weitergeleitet wird, führt der zugeordnete Zustellungs-Agent die Inhaltskonvertierung und die Nachrichtenzustellung durch.

Sie können Zustellungs-Agent-Connectors nicht im Exchange Admin Center erstellen. Sie verwenden dazu die Exchange Management Shell und das Cmdlet *New-DeliveryAgentConnector*. Die Zustellungs-Agent-Connectors bearbeiten Sie mit *Set-DeliveryAgentConnector*. Sie können über die Option *SourceTransportServers* einen oder mehrere Postfachserver für den Connector angeben.

Sie können den Zustellungs-Agent-Connector für Textnachrichten zum Weiterleiten von Nachrichten an mobile Geräte wie Smartphones nutzen. Führen Sie auf dem Exchange-Server das Cmdlet *Get-DeliveryAgentConnector | fl* aus, um den Connector und alle zugehörigen Optionen anzuzeigen.

Transport-Agents für ältere Versionen

Exchange 2019 unterstützt Transport-Agents, die mit Microsoft .NET Framework entwickelt wurden. Zum Aktivieren der Unterstützung älterer Transport-Agents muss die entsprechende XML-Anwendungskonfigurationsdatei geändert werden:

```
%ExchangeInstallPath%Bin\EdgeTransport.exe.config,  
%ExchangeInstallPath%Bin\MSExchangeTransport.exe.config
```

Die Unterstützung für ältere Transport-Agents wird über Schlüssel in den Anwendungskonfigurationsdateien festgelegt (standardmäßig sind keine Schlüssel vorhanden):

- **useLegacyV2RuntimeActivationPolicy** Dieser Schlüssel aktiviert oder deaktiviert die Unterstützung für ältere Transport-Agents. Gültige Werte für

diesen Schlüssel sind *true* oder *false*. Wenn dieser Schlüssel nicht angegeben wird, lautet der Standardwert *false*.

- **supportedRuntime version** Dieser Schlüssel gibt die Version von Microsoft .NET Framework an, die für den Agent erforderlich ist.

Wenn Sie mehrere Werte angeben wollen, verwenden Sie separate Einträge des Schlüssels `supportedRuntime version`. Änderungen an Anwendungskonfigurationsdateien werden aber erst nach dem Neustart des entsprechenden Dienstes angewendet:

- *Microsoft Exchange-Front-End-Transport (MSEExchangeFrontendTransport)*
- *Microsoft Exchange-Transport (MSEExchangeTransport)*

Beim Neustart der Dienste wird die Nachrichtenübermittlung auf dem Server vorübergehend unterbrochen. Gehen Sie folgendermaßen vor, um die Unterstützung für ältere Transport-Agents zu aktivieren:

1. Führen Sie den folgenden Befehl aus, um die entsprechende Anwendungskonfigurationsdatei im Editor zu öffnen:

```
Notepad %ExchangeInstallPath%Bin\<<AppConfigFile>
```

2. Navigieren Sie zum Schlüssel `</configuration>` am Ende der Datei und fügen Sie davor die folgenden Schlüssel ein:

```
<startup useLegacyV2RuntimeActivationPolicy="true">  
  <supportedRuntime version="v4.0" />  
  <supportedRuntime version="v3.5" />  
  <supportedRuntime version="v3.0" />  
  <supportedRuntime version="v2.0" />  
</startup>
```

3. Speichern und schließen Sie die Anwendungskonfigurationsdatei. Führen Sie den folgenden Befehl aus, um den zugehörigen Windows-Dienst zu starten:

```
Net stop <Dienst> && Net start <Dienst>
```

Transport-Agents verwalten

Sie können die Transport-Agents im Front-End-Transportdienst nicht mit Exchange Admin Center verwalten. Sie müssen Exchange-Cmdlets in die Windows PowerShell-Sitzung importieren:

1. Öffnen Sie auf dem Server die PowerShell und führen Sie dann den folgenden Befehl aus:

```
Add-PSSnapin  
Microsoft.Exchange.Management.PowerShell.SnapIn
```

2. Führen Sie den folgenden Befehl aus, um die Transport-Agents im Front-End-Transportdienst auf einem Server anzuzeigen:

```
Get-TransportAgent -TransportService FrontEnd
```

Wenn Sie einen Transport-Agent installieren, registriert Exchange nur die *.dll*-Dateien, die ihm zugeordnet sind. Sie müssen sicherstellen, dass alle Dateien, Registrierungsschlüssel und anderen Objekte, von denen der Transport-Agent abhängig ist, ordnungsgemäß installiert und konfiguriert sind.

Transport-Agents haben Vollzugriff auf alle gefundenen E-Mail-Nachrichten. Exchange 2019 schränkt das Verhalten eines Transport-Agents nicht ein. Aus diesem Grund sollten Sie nur Transport-Agents installieren, die vertrauenswürdig sind und vollständig in einer Testumgebung getestet wurden.

Transport-Agents werden in deaktiviertem Zustand installiert, um sicherzustellen, dass der Nachrichtenfluss von noch nicht konfigurierten Transport-Agents unbeeinträchtigt bleibt. Nach der Installation müssen Sie den Transport-Agent aktivieren:

```
Install-TransportAgent -Name <Name> -TransportAgentFactory  
<"TransportAgentFactory"> -AssemblyPath <Pfad>
```

Beispiele:

```
Install-TransportAgent -Name "Contoso Transport Agent" -  
TransportAgentFactory "vendor.exchange.  
ContosoTransportAgentfactory" -AssemblyPath "C:\Program  
Files\Vendor\TransportAgent\ContosoT-transportAgentFactory.dll"
```

Enable-TransportAgent "Contoso Transport Agent" (Aktiviert den Agent)

Disable-TransportAgent "Contoso Transport Agent" (Deaktiviert den Agent)

Get-TransportAgent "Transport Rule Agent" | Format-List (Zeigt Informationen zum Agent an)

Transport-Agents mit einer hohen Priorität (1 ist am höchsten) verarbeiten E-Mails zuerst. Führen Sie den folgenden Befehl aus, um die Priorität eines vorhandenen Transport-Agents zu ändern:

```
Set-TransportAgent <TransportAgentIdentity> -Priority <Zahl>
```

Beispiel:

```
Set-TransportAgent "Contoso Transport Agent" -Priority 3
```

Woher wissen Sie, dass dieses Verfahren erfolgreich war? Geben Sie den folgenden Befehl ein, um die Eingabe zu überprüfen:

```
Get-TransportAgent | Format-List Name,Priority
```

Mit dem folgenden Befehl lassen sich die Agents wieder deinstallieren:

```
Uninstall-TransportAgent -Identity <TransportAgentIdentity>
```

Allgemeine Einstellungen für Exchange-Transportserver

Neben den Einstellungen für Sende- und Empfangsconnectors auf Transportservern können Sie im Exchange Admin Center und der Exchange Management Shell auch Einstellungen vornehmen, die die allgemeine Konfiguration von Transportservern betreffen, also des E-Mail-Flusses als Ganzes.

In der Exchange Management Shell verwenden Sie das Cmdlet *Get-TransportService*, um die Konfiguration der Transportserver in der Organisation anzuzeigen.

Ausführliche Informationen erhalten Sie mit *Get-TransportService |fl*, wie bei allen *Get*-Cmdlets.

Transportserver konfigurieren

Über den Befehl *Set-TransportServer* oder *Set-TransportService* passen Sie Konfigurationen der Transportserver in der Exchange Management Shell an. Neben den Einstellungen für die Connectors finden Sie im Exchange Admin Center über den Menüpunkt *Server* sämtliche Transportserver der Organisation.

Doppelklicken Sie zunächst auf den Server, dessen Konfiguration Sie überprüfen wollen. Es öffnet sich ein neues Fenster, über das Sie einige Einstellungen für

den Transportserver anpassen können. Zur Verwaltung des E-Mail-Transports stehen Ihnen verschiedene Registerkarten zur Verfügung.

Auf der Registerkarte *Allgemein* finden Sie Informationen über die Edition, die Produkt-ID und die installierten Rollen auf dem Server. Wenn der Product Key für den Server noch nicht eingegeben ist, finden Sie einen Hinweis, dass die Exchange Server-Software noch nicht lizenziert ist.

Auf der Registerkarte *DNS-Lookups* können Sie unabhängig von der DNS-Konfiguration der Netzwerkkarten spezielle DNS-Server eintragen, die für die interne und externe Namensauflösung für E-Mails verwendet werden. Die DNS-Namensauflösung im Netzwerk ist für den erfolgreichen Betrieb von Exchange 2019 extrem wichtig.

Sie können entweder zur Namensauflösung alle eingebauten Netzwerkkarten verwenden (diese Einstellung ist Standard) oder eine einzelne Karte auswählen, wenn mehrere verbaut sind. Außerdem können Sie über die Option *Benutzerdefinierte Einstellungen* andere DNS-Server für die Namensauflösung eintragen, als das Betriebssystem für sonstige Abfragen verwendet.

Auf der Registerkarte *Transportgrenzwerte* stellen Sie für verschiedene Funktionen des Nachrichtenflusses Zeitgrenzen ein, die ausschließlich die Verarbeitung von Nachrichten betreffen. Auf dieser Registerkarte definieren Sie keine Grenzwerte für die Benutzer Ihrer Exchange-Organisation. Hauptsächlich geht es bei diesen Grenzwerten um die Wiederholungsversuche, die der Exchange-Server bei erfolglosem Nachrichtenfluss starten kann, um die Nachricht doch noch zuzustellen. Die einzelnen Optionen sind selbsterklärend. Normalerweise müssen Sie hier keine Änderungen vornehmen.

S2

Allgemein	Intervall für Wiederholungsversuche bei Fehlern ausgehender Verbindungen (Sekunden):
Datenbanken und Database Availability Groups	<input type="text" value="600"/>
POP3	Intervall für Wiederholungsversuche bei vorübergehenden Fehlern (Sekunden):
IMAP4	<input type="text" value="5"/>
Unified Messaging	Wiederholungsversuche bei vorübergehenden Fehlern:
DNS-Lookups	<input type="text" value="6"/>
► Transportgrenzwerte	Nachrichtenablauf
Transportprotokolle	Maximale Dauer seit Übermittlung (Tage):
Outlook Anywhere	<input type="text" value="2"/>
	Benachrichtigungen
	Absender bei Verzögerung der Nachricht benachrichtigen nach (Stunden):
	<input type="text" value="4"/>
	Einschränkungen für ausgehende Verbindung
	Maximale Anzahl von gleichzeitigen Verbindungen:
	<input type="text" value="1000"/> ▼

Abbildung 4.10: Transportgrenzwerte in Exchange 2019 konfigurieren

- **Intervall für Wiederholungsversuche bei Fehlern ausgehender Verbindungen (Sekunden)** Sie sollten den Standardwert nur ändern, wenn Sie aufgrund von Timeouts auf Firewalls oder Proxyservers keine andere Wahl haben.
- **Intervall für Wiederholungsversuche bei vorübergehenden Fehlern (Sekunden)** Hier legen Sie das Intervall zwischen den einzelnen Verbindungsversuchen fest, die bei der Option *Wiederholungsversuche bei vorübergehenden Fehlern* angegeben sind. Der Standardwert ist fünf Sekunden.
- **Wiederholungsversuche bei vorübergehenden Fehlern** Hier legen Sie die maximale Anzahl von Wiederholungsversuchen fest, wenn ein Verbindungsfehler mit einem Remoteserver auftritt. Der Standardwert ist 6. Legen Sie diesen Wert auf 0 fest, versucht der Server nicht sofort, wieder eine Verbindung herzustellen.

- **Maximale Dauer seit Übermittlung (Tage)** Hier konfigurieren Sie den Ablaufzeitraum für eine Nachricht. Ist eine Nachricht länger als der angegebene Zeitraum in der Warteschlange, wird sie als andauernd fehlerhaft an den Absender zurückgeschickt. Die Standardeinstellung beträgt zwei Tage.
- **Absender bei Verzögerung der Nachricht benachrichtigen nach (Stunden)** Hier steuern Sie, wie lange der Server wartet, bevor er eine Benachrichtigung über den Zustellungsstatus (Delivery Status Notification, DSN) an den Absender der E-Mail verschickt. Der Standardwert ist vier Stunden.
- **Maximale Anzahl von gleichzeitigen Verbindungen** Hier legen Sie die maximale Anzahl ausgehender Verbindungen fest. Erreicht der Server das Verbindungslimit, baut er keine neuen Verbindungen auf. Der Standardwert ist 1000.
- **Maximale Anzahl von gleichzeitigen Verbindungen pro Domäne** Hier geben Sie die maximale Anzahl gleichzeitiger Verbindungen für eine einzelne Domäne an. Der Standardwert ist 20.

Hinweis

Die beiden letzten Angaben beeinflussen die Geschwindigkeit, mit der Ihr Server anstehende E-Mails versenden möchte. Nehmen wir an, Ihr Server möchte 1.000 E-Mails versenden. In diesem Fall kann er über den Wert *Maximale Anzahl von gleichzeitigen Verbindungen* dazu gebracht werden, dass er versucht, alle diese E-Mails gleichzeitig zu versenden, indem 1.000 Verbindungen parallel aufgebaut werden.

Sind unter diesen 1.000 E-Mails jedoch beispielsweise 500 Empfänger in der Domäne *hotmail.com*, greift der zweite Wert *Maximale Anzahl von gleichzeitigen Verbindungen pro Domäne*, sodass er nur 20 gleichzeitige Verbindungen zu Hotmail aufbaut. Bei der Einstellung der Werte muss immer auch daran gedacht werden, mit welcher Bandbreite der Server mit dem Internet verbunden ist.

Steht Ihnen nur eine geringe Bandbreite zur Übertragung der Daten zur Verfügung, kann diese bereits durch wenige gleichzeitige Verbindungen ausgelastet sein. Weitere Verbindungen könnten dann zwar noch aufgebaut werden, erhalten aber nur sehr wenige Daten. Dies kann dazu führen, dass die Verbindung vom gegenüberliegenden Server mit einem Timeoutfehler abgebrochen wird. Die beiden Werte und die

Bandbreite müssen deshalb immer gleichzeitig betrachtet werden.

Auf der Registerkarte *Transportprotokolle* aktivieren Sie die Nachrichtenverfolgung und die Konnektivitätsprotokollierung. Hier legen Sie auch den Speicherort der Protokolle fest. Standardmäßig ist die Nachrichtenverfolgung bei Exchange 2019 nach der Installation bereits aktiv. Basisordner aller Protokolle ist der Ordner *C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs*. Die einzelnen Protokolle werden in entsprechenden Unterordnern angelegt. Folgende Optionen stehen zur Verfügung:

- **Protokoll für Nachrichtenverfolgung aktivieren** Standardmäßig ist die Nachrichtenverfolgung auf Transportservern aktiviert. Hier können Sie die Funktion für einzelne Server deaktivieren.
- **Protokollpfad der Nachrichtenverfolgung** In diesem Feld wird der aktuelle Speicherort der Protokolle der Nachrichtenverfolgung angezeigt. Die Protokolle sind standardmäßig im Unterordner *MessageTracking* gespeichert.
- **Konnektivitätsprotokoll aktivieren** Hier aktivieren oder deaktivieren Sie die Protokollierung für die Serververbindungen des Exchange-Servers.
- **Konnektivitätsprotokollpfad** In diesem Feld wird der aktuelle Speicherort der Konnektivitätsprotokolle angezeigt. Sie werden standardmäßig im Unterordner *Connectivity* gespeichert.
- **Protokollpfad senden** In diesem Feld wird der aktuelle Speicherort der Sendeconnectorprotokolle angezeigt. Sie werden standardmäßig im Unterordner *Protocol-Log\SmtpSend* gespeichert. Alle Sendeconnectors, die auf dem Transportserver konfiguriert sind, verwenden die gleichen Protokolle.
- **Protokollpfad für Empfangsprotokoll** In diesem Feld wird der aktuelle Speicherort der Empfangsconnectorprotokolle angezeigt. Sie werden standardmäßig im Unterordner *ProtocolLog\SmtpReceive* gespeichert. Alle Empfangsconnectors, die auf dem Transportserver konfiguriert sind, verwenden die gleichen Protokolle.

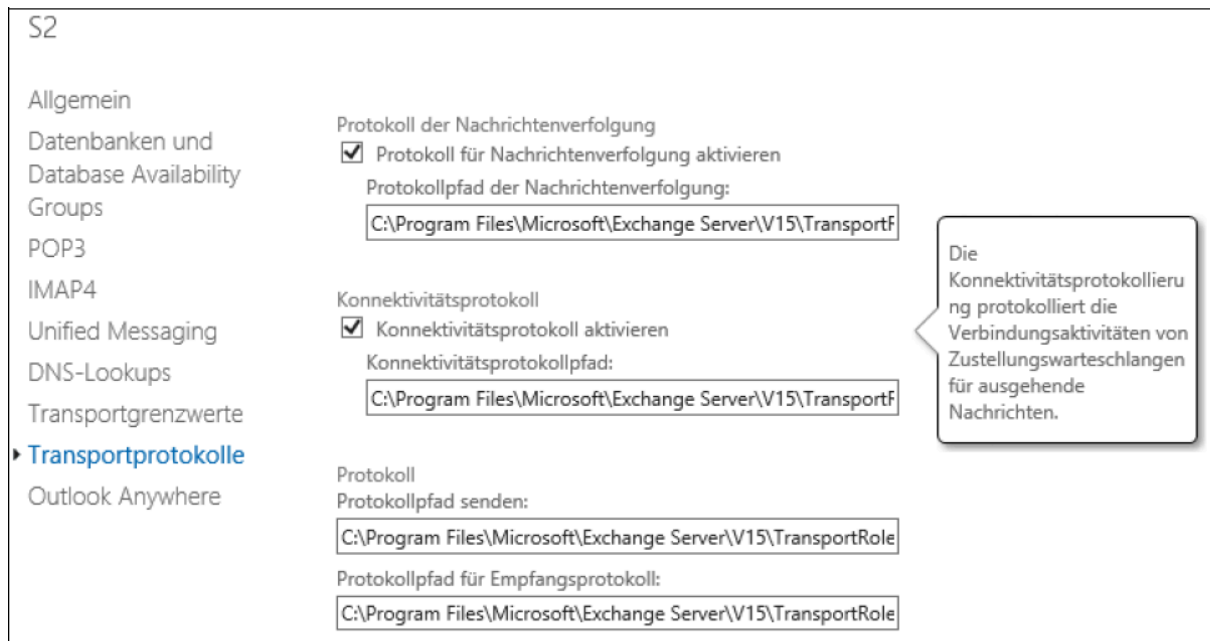


Abbildung 4.11: Konfigurieren der Protokollierung für einen Exchange-Server

Mit den Cmdlets *Set-TransportServer* oder *Set-TransportService* können Sie die Einstellungen in der Exchange Management Shell ändern. Hiermit können Sie insbesondere auch festlegen, wie groß die einzelnen Protokolldateien jeweils werden dürfen und nach welcher Zeit alte Dateien automatisch gelöscht werden sollen.

Tipp Auf einem Server im Produktiveinsatz sollten Sie die Lage der Protokolldateien verändern, damit diese nicht auf dem Systemlaufwerk abgelegt werden und dort gegebenenfalls Platz für wichtige Aktionen des Betriebssystems belegen.

Nachrichtengröße beschränken

Die maximale Größe für empfangene oder gesendete Nachrichten beträgt 10 MB. Sie steuern diese über das Cmdlet *Set-TransportConfig* und die Option *MaxReceiveSize*. Alternativ finden Sie diese Einstellungen im Exchange Admin Center über *Nachrichtenfluss/Empfangsconnectors/Mehr/Einstellungen für Organisationstransport/Grenzwerte/Maximale Größe für empfangene Nachricht*.

Einstellungen für Organisationstransport

Grenzwerte

Sicherheitsnetz

Zustellung

Maximale Anzahl von Empfängern:

Maximale Größe für empfangene Nachricht (MB):

Maximale Größe für gesendete Nachricht (MB):

Abbildung 4.12: Konfigurieren der Grenzwerte für Nachrichten

Die maximale Größe für gesendete Nachrichten steuern Sie auf derselben Seite. Das gilt dann auch für die Steuerung der maximalen Empfänger. In der Exchange Management Shell verwenden Sie das Cmdlet *Set-TransportConfig* mit der Option *MaxSendSize*.

Die maximale Anzahl von Empfängern pro Nachricht steuern Sie auch in der Exchange Management Shell mit dem Cmdlet *Set-TransportConfig* und der Option *MaxRecipient-EnvelopeLimit*.

Die maximale Anlagengröße von E-Mails legen Sie in Transportregeln fest, die für alle Postfachserver in der Organisation gelten. Dazu verwenden Sie die Cmdlets *New-TransportRule* und *Set-TransportRule* mit der Option *AttachmentSizeOver*.

Alternativ erstellen Sie eine neue Regel über *Nachrichtenfluss/Regeln*. Klicken Sie auf das Plus-Zeichen und wählen Sie den Eintrag *Nachrichten nach Größe filtern*. Legen Sie anschließend die Bedingung *Diese Regel anwenden, wenn/Mindestens eine Anlage/ist größer oder gleich* fest.



Abbildung 4.13: Konfigurieren einer neuen Regel zum Steuern der Größe von Anlagen

Die maximale Kopfzeilengröße durch einen Empfangsconnector beträgt 128 KB. Sie steuern diese mit den Cmdlets *New-ReceiveConnector* und *Set-ReceiveConnector* und der Option *MaxHeaderSize*.

Im Exchange Admin Center steuern Sie den Empfang und die Größe von Nachrichten über *Nachrichtenfluss/Empfangsconnectors/Bearbeiten* auf der Registerkarte *Allgemein* mit *Maximale Größe für empfangene Nachricht*.

Client Frontend S1

- ▶ Allgemein
- Sicherheit
- Bereichsdefinition

Version:
Version 15.2 (Build 464.5)

Connectorstatus:
 Aktivieren

Kommentar:

Protokolliergrad:
 Keine
 Ausführlich

Maximale Größe für empfangene Nachricht (MB):
36

*Maximale Anzahl von lokalen Hops:
5

*Maximale Anzahl von Hops:
60

Abbildung 4.14: Steuern der maximalen Größe für das Empfangen von Nachrichten

Wenn die Anzahl von Empfängern für einen anonymen Absender überschritten wird, wird die Nachricht für die ersten 200 Empfänger angenommen. Die Mehrzahl der SMTP-Messagingserver erkennt, dass eine Empfängerbeschränkung wirksam ist. Der SMTP-Messagingserver sendet die Nachricht auch weiterhin erneut in Gruppen von 200 Empfängern, bis die gesamte Nachricht allen Empfängern zugestellt wurde. Sie verwenden dazu *New-ReceiveConnector* und *Set-ReceiveConnector* mit der Option *MaxRecipientsPerMessage*

Die maximale Nachrichtengröße durch einen Sendconnector beträgt 10 MB. Sie steuern die Einstellung mit den Cmdlets *New-SendConnector* und *Set-SendConnector* und der Option *MaxMessageSize*.

Auch diese Einstellung finden Sie im Exchange Admin Center. Navigieren Sie dazu über *Nachrichtenfluss/Sendeconnectors/Bearbeiten* zur Registerkarte

Allgemein und legen Sie im Feld *Maximale Größe für gesendete Nachricht* einen Grenzwert fest.

Die maximale Nachrichtengröße durch einen Active Directory-Standortlink ist unbeschränkt. Sie legen diese mit dem Cmdlet *Set-AdSiteLink* und der Option *MaxMessageSize* fest.

Auch die maximale Nachrichtengröße durch einen Zustellungs-Agent-Connector ist unbeschränkt. Sie konfigurieren diese mit *New-DeliveryAgentConnector* und *Set-DeliveryAgentConnector* über die Option *MaxMessageSize*.

Die maximale Nachrichtengröße durch einen fremden Connector bestimmen Sie mit *Set-ForeignConnectorParameter* und *MaxMessageSize*.

Die maximale Kopfgröße für Nachrichten im *Pickup*-Ordner (siehe Kapitel 3) ist 64 KB. Sie steuern diese mit *Set-TransportService* und *PickupDirectoryMaxHeaderSize*.

Die maximale Anzahl von Empfängern pro Nachricht für Nachrichten im *Pickup*-Ordner ist 100 und wird mit *Set-TransportService PickupDirectoryMaxRecipientsPerMessage* gesteuert.

Sie können Größenbeschränkungen auch für einzelne Benutzer festlegen, nicht nur für die komplette Organisation oder einzelne Connectors. Dazu verwenden Sie die folgenden Cmdlets:

- *Set-DistributionGroup*
- *Set-DynamicDistributionGroup*
- *Set-Mailbox*
- *Set-MailContact*
- *Set-MailUser*
- *Set-MailPublicFolder*
- *Set-RemoteMailbox*

Die Option *MaxSendSize* steuert die maximale Größe von Nachrichten, die gesendet werden. Sie finden die Einstellungen auch im Exchange Admin Center im Abschnitt *Empfänger* über *Postfächer/Bearbeiten/Postfachfunktionen*.

Thomas Joos	
Allgemein	
Postfachnutzung	Archivierung: Deaktiviert Aktivieren
Kontaktinformationen	
Organisation	
E-Mail-Adresse	Nachrichtenfluss
► Postfachfunktionen	Zustelloptionen
Mitglied von	Die Zustelloptionen steuern die Weiterleitungs- und Empfängergrenzwerte.
E-Mail-Info	Details anzeigen
Postfachstellvertretung	Größeneinschränkungen für Nachrichten
	Größeneinschränkungen für Nachrichten steuern die maximale Größe der Nachrichten, die der Empfänger senden und empfangen kann.
	Details anzeigen
	Einschränkungen für die Nachrichtenzustellung
	Einschränkungen für die Nachrichtenzustellung definieren, welche Absender Nachrichten an diesen Empfänger senden können.
	Details anzeigen

Abbildung 4.15: Konfigurieren der Nachrichtengröße für einzelne Benutzer

Sie können verschiedene Nachrichtengrößenbeschränkungen auf verschiedenen Ebenen in der Exchange-Organisation festlegen. Beim Weiterleiten einer Nachricht durch die Transportinfrastruktur kann die Nachricht unterschiedlichen Beschränkungen der Nachrichtengröße unterliegen.

Beschränkungen der Nachrichtengröße für die Empfangsconnectors, die Nachrichten aus dem Internet empfangen, sollten kleiner als oder gleich den Beschränkungen der Nachrichtengröße sein, die Sie für Ihre interne Exchange-Organisation konfiguriert haben.

Hinweis Beschränkungen auf Benutzerebene haben Vorrang vor anderen Beschränkungen der Nachrichtengröße. Daher können Sie ein Benutzerkonto so konfigurieren, dass seine Beschränkungen die für Ihre Organisation festgelegten Standardbeschränkungen der Nachrichtengröße überschreiten.

Wenn eine Nachricht an einen Empfänger im Internet gesendet oder von diesem empfangen wird, werden die Organisationsbeschränkungen angewendet.

Index

.edb-Dateien 144, 159

.nk2-Dateien 183

.pst-Dateien 154, 315

A

Abgesicherter 485

Abschneideverzögerung 515

Absenderfilter-Agent 394, 401

Absenderzuverlässigkeits-Agent 411

Abwesenheits-Assistent 171

Abwesenheitsnachrichten 122

Active Directory-Berechtigungen 422

 geteilte 423

Active Directory-Domänen und Vertrauensstellungen 67

Active Directory-Gesamtstruktur 40

Active Directory-Rechteverwaltungsdienste 352

Active Directory-Zertifikatdienste 42

Active Directory Federation Services 352

ActiveDirectorySplitPermissions 423

ActiveSync 188, 199

 Benutzerverwaltung 199

 Gerätezugriffsregeln 202

 Postfachrichtlinien 200

ADFS *siehe* Active Directory Federation Services

ADRMS 89

ADRMS *siehe auch* Active Directory-Rechteverwaltungsdienste

Add-ADPermission 237

Add-ContentFilterPhrase 408
Add-DatabaseAvailabilityGroupServer 499
Add-DistributionGroupMember 228
Add-Ins 414, 481–482
Add-MailboxDatabaseCopy 502, 506
Add-MailboxPermission 237
Add-ManagementRoleEntry 430
Add-PSSnapin 114
Address Rewriting Agent 379
Add-RoleGroupMember 31, 338, 469
AdminDisplayVersion 35
Administrator Rollengruppenbericht 367
Administratorrollen 337, 420, 425
Administrator-Überwachungsprotokollierung 361
Adressbuch 186, 250
Adressbuchrichtlinie 264
Adressliste 60, 262
 globale 265
ADSI-Edit 46
ADSI-Editor 277, 466
Aktivierungseinstellungsnummer 507
Akzeptierte Domänen 72
Anhaltevorgang 128
Anlagenbehandlung 414
Anlagenfilter-Agent 394
Anlagenvorschau 414
Anonym 283
Antischadsoftware-Modul 387
Antispam 394
AntiSpamBypassEnabled 406
Antispameinstellungen 410
Antwortdatei 29
Anwendungs-Add-Ins 482
Anwendungsdatenbanken 457

Anwendungsereignisprotokoll 313
appwiz.cpl 34
Arbeitsspeicherbereich 486
Archiv 312, 471
Archivierung 13
Archivpostfach 223, 233, 311
Aufbewahrungseinstellungen 274
Aufbewahrungspflicht 330
Aufbewahrungsrichtlinien 316, 323, 326
Aufbewahrungstags 317
Aufbewahrungszeit 468
Aufbewahrungszeitraum 150, 325
Aufzeichnung 484
Authentifizierung 239
AutoConnect 176
AutoDatabaseMountDial 496
Autodiscover 66, 80, 176

B

Backupordner 459
Bare-Metal-Restore 483
Befehlszeile 29
Benachrichtigungen 390
Benennungsrichtlinie 256
Berechtigungen 238, 448
Berechtigungsstufe 239, 279
Bereichsfilter 434
Besitzer 279
Besprechung
 Raumsuche 250
 Zeitzone 250
Besprechungen 186
 Mit Vorbehalt 252
Besprechungsanfrage 242, 249

- beantworten 252
- erstellen 249
- Tastenkombinationen 249
- Besprechungsnachrichten 242
- Besprechungsserien 227
- Beweissicherungsverfahren 361
- Bluescreens 486
- BlueScreenView 487
- Bootprobleme 485
- bootrec 485
- Buchungsoptionen 226
- Buchungsvorlaufzeit 227

C

- CAL 13
- Calendar Repair Assistant 234
- Categorizer 89
- checkclient 182
- CheckDatabaseRedundancy.ps1 509
- CLC 353
- cleancategories 182
- cleanclientrules 182
- cleandmrecords 182
- cleanfinders 182
- cleanfreebusy 182
- Clean-MailboxDatabase 316, 464
- cleanreminders 182
- cleanroamedprefs 182
- cleanrules 182
- cleanserverrules 183
- cleansharing 183
- cleansniff 183
- cleansubscriptions 183
- cleanviews 183

ClientAccess 80
Clienteneinstellungen 152
Client-Lizenzgeberzertifikat 353
Clientzugriffslizenz 13
Clientzugriffsprotokolle 5
clussvc 518
Cluster 391, 517
Clusterknoten 498
COM-Add-Ins 482
Compliance 317
Compliance-Archive 318
Compliance-eDiscovery 300, 334–335
Computerreparaturoptionen 483
Connect-Mailbox 236, 471
Connectors 87, 233
Continuous Replication Circular Logging 507
Core-Modus 19
CRA *siehe* Calendar Repair Assistant
CRCL 507
Cutover-Migration 578

D

DAG 96, 149, 271, 489
DAG *siehe auch* Datenbankverfügbarkeitsgruppen
Data Loss Prevention, DLP 6, 138, 345
Database Availability Groups 96, 149, 271, 489
Dateifreigabemehrheit 493
Dateifreigaben 53
Dateisystem 145
Dateizugriff 189
Datenbankdatei 144
Datenbanken 59
Datenbankfehler 162
Datenbankhochverfügbarkeits-Gruppen 489

Datenbankkopien 492, 500
Datenbankportabilität 467
Datenbankverfügbarkeitsgruppen 7, 96
Datendateien 482
Datenschutzoptionen 414
Datensicherungskonzept 54
Datensicherungsprogramm 54, 159
Datenträger 483
Datenübermittlung 583
Datenverlust 346, 490
Dcdiag 46
dcdiag.exe 83
Debuginformationen 487
Debugmodus 485
Default Policy 73
Default Web Site 562
Definitionsdateien 388
Defragmentation 165
Deinstallieren 34
Dial Tone-Portabilität 467
Dienste 76
Differenzielle Sicherung 455
Digestauthentifizierung 184
Direct Push 199
Disable-Antimalwarescanning.ps1 388
Disable-JournalRule 342
Disable-Mailbox 464
Disable-TransportAgent 379–380, 402
Discovery Management 469
DiscoveryHold 333
Dismount-Database 65, 165, 468
DLP 6, 345
DLP *siehe auch* Data Loss Prevention
DLP-Richtlinie 350

Domänen, akzeptierte 72
Domänencontroller 16, 582
Domänenlokal 255
DoNotIncludeArchive 314
Dsmmod 466
dsquery 17

E

E00.chk 458
EAS *siehe* Active Sync
ecp 58
EDB-Datei 454
Edge-Abonnement 378
EdgeSync-Abonnement 372
Edge-Transport 394
Edge-Transport-Server 371, 405
EHLO 90
EICAR 387
Einbindung 150, 459
E-Mail-Adressenrichtlinien 44, 73
E-Mail-Autokonfiguration 178
E-Mail-Domänen 71
E-Mail-Fluss 71
Empfänger 59, 220
Empfängerdomäne 69
Empfängerfilter-Agent 394
Empfängerfilterung 403
Empfängerlesebereich 432
Empfängerrichtlinien 73
Empfängerschreibbereich 432
Empfangsconnectorprotokolle 118
Empfangsconnectors 44, 106
Enable-JournalRule 342
Enable-Mailbox 223

Enable-MailPublicFolder 280
Endbenutzerrollen 420
Enterprise-CAL 312
Ereignisanzeige, Aufruf 367
ESE-Datenbank 143
Eseutil 458, 463
Eseutil.exe 150, 163, 514
Eventvwr.msc 387
Exchange Admin Center 58
Exchange Install Domain Servers 24
Exchange Management Shell 8, 64
Exchange Server Administrators 248
Exchange Server-Authentifizierung 110
Exchange Trusted Subsystem 494
Exchange-Adressliste 237
Exchange-Datenbank 81
 Sicherheit 455
ExchangeLegacyInterop 110
Exchange-Organisationen 60
ExchangeSetup.log 34
ExchangeSetup.msilog 46
Exchange-Verwaltungskonsole *siehe* Exchange Admin Center
Exchange-Verwaltungsshell *siehe* Exchange Management Shell
Exchange-Verwaltungstools installieren 34
Exchange-Webdienste 188
Exchange-Windows-Permissions 495
ExchClientVer=15 566
Export-PublicFolderStatistics.ps1 573
Export-TransportRuleCollection 567

F

Failovercluster 493
Favoriten 274
Fax 272

Fehlerbehebung während der Installation 45

Filterabfrage 433

finder 183

FIPFS 388

fixmbr 485

Fpsdiag.exe 80

Front-End-Transport-Dienst 6

Fsutil.exe 144

Funktionsebene 16

G

GAL *siehe* Global Address List

Gerätepostfach 225

Gesamtstruktur 16

Gesamtstrukturvertrauensstellungen 440

Get-AcceptedDomain 404

Get-ActiveSyncMailboxPolicy 202

Get-ActiveSyncOrganizationSettings 202

Get-AddressList 264

Get-ADReplicationUpToDateVectorTable 83

Get-ClientAccessServer 168, 179

Get-Command 64

Get-Credential 248

Get-DatabaseAvailabilityGroup 501

Get-DeliveryAgentConnector 113

Get-DistributionGroup 193

Get-DistributionGroupMember 328

Get-DlpPolicy 349

Get-DynamicDistributionGroup 260

GetEffectiveUsers 443

Get-ExchangeServer 35, 374

Get-GlobalAddressList 264

Get-Help 164

Get-Mailbox 64, 154, 156, 235, 265, 276, 298, 300, 314, 406, 445, 467, 570

Get-MailboxDatabase 65, 166–167, 342, 391, 469, 570
Get-MailboxDatabaseCopyStatus 167, 503
Get-MailboxExportRequest 156
Get-MailboxExportRequestStatistics 156
Get-MailboxFolderStatistics 314
Get-MailboxImportRequest 155
Get-MailboxImportRequestStatistics 155
Get-MailboxRestoreRequest 476–477
Get-MailboxRestoreRequestStatistics 477
Get-MailboxSearch 335
Get-MailboxServer 168, 330
Get-MalwareFilteringServer 388
Get-ManagementRoleAssignment 367, 430, 443
Get-ManagementRoleEntry 429
Get-ManagementScope 436
Get-Message 398
Get-MobileDevice 204
Get-MoveRequest 570
Get-OfflineAddressBook 264
Get-OrganizationConfig 192, 257, 274, 573
Get-OutlookProtectionRule 355
Get-OwaVirtualDirectory 188
Get-PublicFolder 277
Get-PublicFolderItemStatistics 286
Get-PublicFolderMigrationRequest 573
Get-PublicFolderStatistics 271, 288
Get-Queue 112, 126
Get-ReceiveConnector 111
Get-RetentionPolicy 323, 328
Get-RetentionPolicyTag 325
Get-RMSTemplate 354
Get-RoleAssignmentPolicy 447
Get-RoleGroupMember 31, 338
Get-SenderFilterConfig 402

Get-SenderIDConfig 405
Get-SiteMailboxProvisioningPolicy 300
Get-TransportAgent 340, 353, 355, 380, 388
Get-TransportConfig 91, 396
Get-TransportRule 141
Get-TransportRuleAction 138
Get-TransportRulePredicate 138
Get-TransportServer 112, 115
Get-User 223, 474
Get-VM 55
Get-VMNetworkAdapter 55
Get-WMI-Object 55
Global Address List 265
Globale Adressliste 265
GrantSendonBehalf 298
Grenzwerte 231, 286, 469
Größenbeschränkungen 233
Größeneinschränkungen 285
Gruppenbenennungsrichtlinien 256
Gruppenmoderator 258
GZIP 190

H

HELO 134
Herunterfahren 53
Hub-Transport-Dienst 6
Hub-Transport-Server 90
Hyper-V 54
Hyper-V-Cluster 489

I

IAcceptExchangeServerLicenseTerms 22, 48
IIS 176, 392
IMAP4 78, 392
importnk2 183

Import-TransportRuleCollection 568
Informationsspeicher 78, 147
Inhaltsfilter-Agent 394
Inhaltsfilterung 406
Inhaltsindexdienste 515
Inkrementelle Sicherung 454
Installation 15
Install-TransportAgent 114
Integrationsdienste 53
IPv4 490
IPv6 19, 490
IP-Zulassungsentsprechung 400
IP-Zulassungsliste 400–401
IRM-Schutz 352
iSCSI-Speicher 52, 504
Isinteg 164

J

Jetstress 144
JET-Umlaufprotokollierung 507
Journale 340
Journalempfänger 150
Journalregeln 89
Junk-E-Mail 416

K

Kalender freigeben 242
Kalenderberechtigungen 242–243
Kapazität 226
Kennwort 201
Komprimierung 505
Konfigurationslesebereich 432
Konfigurationsschreibbereich 432
Konnektivitätsprotokollierung 117
Kontaktinformationen 230

Kontingentinformationen 151

Kontoeinstellungen 178, 243

Kopiedatenbank 508

Kopiewarteschlange 511

Kumulatives Update 31

L

LDAP 582

LDAP-Lesedauer 583

Legal Hold 312

Leistungsprobleme 581

Leistungsüberwachung 582

Lizenz 13

M

MAC-Adresse 54

Mailbox Delivery Queue 127

Mailbox Replication Service 244, 471

Mailtipps 192

Makros 414

ManagementScope 433

mapi 562

MapiHttpEnabled 561

Maximalgrößen 75

MaxReceiveSize 76

MaxSendSize 76

mdsched.exe 486

Memory.dmp 487

Message-ID 133

Messaging Records Management 322

Messaging-Datensatzverwaltung 313, 322

Microsoft Exchange Active Directory Topology 77

Microsoft Exchange EdgeSync 77

Microsoft Exchange Frontend Transport 77

Microsoft Exchange IMAP4 78

Microsoft Exchange POP3 78
Microsoft Exchange Replication 79
Microsoft Exchange Search Host Controller 78
Microsoft Exchange Server Extension for Windows Server Backup 78
Microsoft Exchange System Objects 24
Microsoft Exchange-Antispam Update 78
Microsoft.Exchange.Management.PowerShell.SnapIn 114
Migration 15, 40, 246, 553
MIME 82
Minidump 487
Mitgliedschaftsgenehmigung 257, 259
Mobile Geräte 204
Mobiltelefone 204
Moderation 257
Moderator 229
Mount-Database 147, 166, 468
Mountvol.exe 501
Move Mailboxes 248
Move-ActiveMailboxDatabase 516
Move-AddressList 263
Move-DatabasePath 147
MRM 322
MRS 471
MRS *siehe auch* Mailbox Replication Service
MSEExchange Management 367
MSEExchangeIS 584
MSEExchangeTransport 396
MsExchDefaultPublicFolderMailbox 277
msExchInstallPath 467

N

Nachrichtenfluss 44, 68, 107, 116, 138, 233, 412
Nachrichtengenehmigung 258
Nachrichten-ID 133

Nachrichtenkopien 93
Nachrichtentracking 125
Nachrichtenverfolgung 130, 185
Nachrichtenzustellung 233, 285
Namensuffixrouting 441
NDRs 123
Net time 48
Net-Befehl 84
Netlogon.dns 84
netsh 18
Netzwerkdienst 131
Netzwerkverbindungen 504
New-AddressBookPolicy 264
New-DatabaseAvailabilityGroup 495
New-DeliveryAgentConnector 113
New-DistributionGroup 228, 257
New-DynamicDistributionGroup 260
New-JournalRule 341
New-Mailbox 64, 221, 275, 422, 574
New-MailboxAuditLogSearch 361
New-MailboxDatabase 147, 502
New-MailboxExportRequest 156
New-MailboxImportRequest 155
New-MailboxRepairRequest 163
New-MailboxRestoreRequest 462
New-MailboxSearch 332, 469
New-MailContact 422
New-MailUser 422
New-ManagementRole 429, 431
New-ManagementRoleAssignment 155, 362
New-ManagementScope 433, 435
New-MobileDeviceMailboxPolicy 202
New-MoveRequest 246, 248, 570
New-OfflineAddressBook 267

New-OutlookProtectionRule 355
New-OwaMailboxPolicy 190
NewProvisionedServer 31
New-PublicFolder 278, 287
New-PublicFolderMigrationRequest 574
New-ReceiveConnector 120
New-RemoteMailbox 422
New-RetentionPolicyTag 325
New-RoleGroup 426, 437
New-SendConnector 104
New-SiteMailboxProvisioningPolicy 299
New-TransportRule 89, 141, 354
Nltest 84
Non-Delivery Reports 123
notepad 573
NTFS 144
NTLM 109

O

OAB 188
Office 365 388
Offlineadressbuch 152, 188, 391
Offlineadressliste 153, 266
Offlinedefragmentation 165
Offlinesicherung 457
Onlinesicherung 452–453
Open-Proxy-Test 411
optionalfeatures 134
Ordnerberechtigungen 238, 279
Ordnergröße 282
Ordnerkontaktperson 240
Ordnerstruktur 79
Organisation 60
Organisationseinheit 432

Organization Management 335

OST2PST 479

OST-Datei 479

Outlook 398, 409, 417, 477

 Fehlerbehebung 182

 Startoptionen 182

Outlook im Web *siehe* OWA

Outlook Web App 9, 170, 172

 Offlinemodus 187

Outlook Web App *siehe auch* OWA

Outlook Web App-Richtlinien 188

Outlook.exe 182

Outlook-Schutzregeln 354

OWA 66, 184, 273

P

PAM *siehe* Primary Active Manager

Perfmon.msc 582

pfx-Datei 40

Phishingmails 416

Pickup-Ordner 81

Point-in-Time-Wiederherstellung 460

Poison Message Queue 127

POP3 78

Postfach 230

 freigegebenes 296

 verbinden 470

 verschieben 244

 wiederherstellen 475

Postfachdatenbank 52, 223

 verschieben 245

Postfachdatenbankkopie 506

Postfächer 184

Postfachfunktionen 184, 200, 231, 314, 445

Postfachinhalt 334
Postfachreplikationsdienst 244, 471
Postfachrichtlinien 200
Postfachscanner 161
Postfachserver 94
Postfachstellvertretung 234, 237
Postfachtransportzustellung 99
Postfachüberwachungsprotokollierung 360
Postfachzugriff 361
Postfachzustellungsgruppe 97
PrepareAllDomains 423
PrepareMoveRequest.ps1 247
PrepareSchema 22
Primary Active Manager 492
Problemaufzeichnung 484
Problembehandlung 483
Product Key 38
Profileinstellungen 479
Protokollanalyse-Agent 394
Protokolliergrad 105, 583
Prozesse 392, 488
Prüfpunktdatei 160, 162, 452
psr 484
PublicFolderToMailboxMapGenerator.ps1 573

Q

Quelltransportserver 97
Quorumkonzept 493

R

RAC 353
Raumpostfach 225, 228
RBAC *siehe* Zugriffssteuerung
RBL 400
Realtime Blackhole Lists 400

Rechtekontozertifikat 353
Rechteschutz 354
Rechteverwaltung 13, 348
Recipient Management 425
RecipientRestrictionFilter 433
RecoverServer 466
Regeln 412
Registrierung 452
regsvr32 17
Relaying 110, 135
Remote Delivery Queue 127
Remotedomänen 122
Remove-AddressBookPolicy 265
Remove-DatabaseAvailabilityGroupServer 500
Remove-DlpPolicy 349
Remove-Mailbox 64, 236, 422, 464
Remove-MailboxDatabaseCopy 509
Remove-MailboxExportRequest 156
Remove-MailboxImportRequest 155
Remove-MailContact 422
Remove-MailUser 422
Remove-PublicFolder 278
Remove-PublicFolderMigrationRequest 573
Remove-RemoteMailbox 422
Remove-RetentionPolicyTag 326
Remove-RoleAssignmentPolicy 447
Remove-RoleGroup 427
Remove-RoleGroupMember 31
Remove-SiteMailboxProvisioningPolicy 300
Remove-StoreMailbox 464, 471
Remove-TransportRule 141
Repadmin.exe 83
Reparieren 178
Replikation 270

Replikationsverbindungen 90
Replikationsverfahren 504
Resilient File System 145
Ressourcen 221, 225
Ressourcenplanung 272
Ressourcen-Postfach 220
Restart-Computer 21
Restart-Service 396
Restore-DatabaseAvailabilityGroup 518
Resume-MailboxDatabaseCopy 511
Resume-MailboxExportRequest 156
Resume-MailboxImportRequest 155
Resume-MailboxRestoreRequest 477
Richtlinien 73, 312
Richtlinientipp 350
Richtlinientreue 317
RMS 348
Role Based Access Control 419
Rollengruppe 421
Rollengruppenbericht 443
Rollenmodell 61
Rollenzuweisungen 422, 432
Rollenzuweisungsrichtlinie 444
Rollforward-Wiederherstellung 457
Rollup Package 31
Routingpfad 98
Routingtabellen 98
Routingziel 97
rpcdiag 183

S

SAM *siehe* Standby Active Manager
Schadsoftwarefilter 389
Schadsoftwareschutz 386

Schema 17
Schemamaster 16
Schreibbereich 432
Schweregrad 140
SCL 128, 397
Scripts 431
Search-Mailbox 469
Search-MailboxAuditLog 361
Seeding 508
Sendeconnectorprotokolle 118
Sendeconnectors 44, 69, 98
Sender ID-Agent 394
Server Message Block-Protokoll 491
Serverdienste 36
Serverrollen 76
Serverswitchover 515
Serverzertifikat 39
services.msc 76
Set-AcceptedDomain 404
Set-ActiveSyncMailboxPolicy 202
Set-AddressBookPolicy 265
Set-AdminAuditLogConfig 363
Set-AutodiscoverVirtualDirectory 179
Set-CASMailbox 190, 232
Set-DatabaseAvailabilityGroup 493, 500, 517
Set-DistributionGroup 121, 193, 229
Set-DlpPolicy 349
Set-DynamicDistributionGroup 121, 260
Set-EventLogLevel 584
Set-ExchangeServer 35
Set-IRMConfiguration 356
Set-Mailbox 64, 121, 223, 254, 265, 271, 360, 410
Set-MailboxCalendarConfiguration 227
Set-MailboxDatabase 316, 342

Set-MailboxExportRequest 156
Set-MailboxImportRequest 155
Set-MailboxServer 131, 235, 330, 497
Set-MailContact 121
Set-MailPublicFolder 121
Set-MailUser 121
Set-MalwareFilteringServer 388
Set-ManagementScope 436
Set-OabVirtualDirectory 188
Set-OrganizationConfig 275, 561, 573
Set-OwaMailboxPolicy 187, 362
Set-OwaVirtualDirectory 187
Set-PublicFolder 286–287
Set-PublicFolderMigrationRequest 574
Set-ReceiveConnector 92, 110, 120
Set-RemoteDomain 124
Set-RemoteMailbox 121
Set-RetentionPolicyTag 317
Set-RoleAssignmentPolicy 445
Set-RoleGroup 426, 437
Set-RpcClientAccess 79
Set-SenderFilterConfig 402
Set-SenderIDConfig 405
Set-SiteMailboxProvisioningPolicy 300
Set-TransportAgent 115
Set-TransportConfig 76, 91, 396
Set-TransportRule 89, 141
Set-TransportServer 81
Set-TransportService 360
Setup.exe 28
ShadowHeartbeatFrequency 94
ShadowRedundancyEnabled 91
Shadow-Redundanz 92
SharePoint 11, 78, 110, 270

SharePointURL 300
Shortcut Trusts 438
Sicherheit 109
Sicherheitsgruppe 436
Sicherheitsnetz 93, 96, 491
Sicherung 451
 differenzielle 455
 inkrementelle 454
Sicherungs-Assistent 453
Sicherungsprogramm 454, 483
Signatur 415
SiteMailboxProvisioningPolicy 299
Smarthost 103
Smartphone 204
SMB 491
SMB 3.0 53
SMTP 92, 134
SMTP-Gateway 111
Snapshots 52
SoftDeleted 464
Soft-Recovery 160, 453
Spam Confidence Level 128, 397
Spamschutz 77, 395
Speicherabbild 487
Sperrlistenanbieter 400
Sprachpaket 33
SSL 39
Standardauthentifizierung 103, 216
Standardschreibbereich 432
Standardwarntext 389
Standby Active Manager 492
Standby-Rechenzentrum 517
Start-EdgeSynchronization 410
Start-ManagedFolderAssistant 330

Startprotokollierung 485
Stellvertreter 242
Stellvertretung 241
Stellvertretungen 226, 313
Stop-DatabaseAvailabilityGroup 517
Stoppaktion 53
Stop-Service 518
Submission 126
Suspend-MailboxDatabaseCopy 511
Suspend-MailboxExportRequest 156
Suspend-MailboxImportRequest 155
Suspend-MailboxRestoreRequest 476
Switchover 515
Systemeinstellungen 487
Systemfehler 486
Systemimage-Wiederherstellung 483
SystemMailbox 336
Systemsteuerung 487
Systemvoraussetzungen 7

T

Taktintervall 199
Task 488
Task-Manager 481
Taskmgr 481
Teamworkfunktionen 269
Telnet 214
Telnet.exe 134
Terminplanung 227
Terminplanungs-Assistent 249
Test 178
Test-ActiveSyncConnectivity 203
Test-ArchiveConnectivity 314
Test-EcpConnectivity 168, 171

Test-ImapConnectivity 168, 171
Test-Mailflow 112
Test-OutlookConnectivity 167, 171
Test-OwaConnectivity 168, 171
Test-PopConnectivity 168, 171
Test-ReplicationHealth 509, 515
Test-ServiceHealth 36
Testvirus 387
Test-WebServicesConnectivity 171
Timeout 216
TLS 103
Transaktionsprotokolldateien 452
Transaktionsprotokolle 146, 159, 460
Transport-Agents 114
Transportdienst 491
Transportdumpster 95, 491
Transportgrenzwerte 116
Transportprotokolleinstellungen 130
Transportregel-Agent 137, 412
Transportregeln 138, 345, 350, 386, 398, 412, 567
Transportrichtlinien 13
Transportschutzregeln 353
Transportserver 111
Treiber 484
Treibersignatur 485
Trust Center 412
Trusted 438
Trusting 438

U

Übermittlungswarteschlange 90
Überwachung 362, 367, 443
Überwachungen 360
Umlaufprotokollierung 149, 160

Unified-Messaging 5
Uninstall-TransportAgent 115
Unreachable Queue 127
UnscopedTopLevel 431
Unzustellbarkeitsbericht 123, 230
Update-AddressList 264
Update-MailboxDatabaseCopy 511
Update-MalwareFilteringServer.ps1 387
Update-Safelist 409
UPN 68

V

Verbindungsfilter 399
Verbindungsfilter-Agent 394
Verteilergruppe
 abfragebasierte 260
 anlegen 255
Vertrauensstellung
 bidirektionale 437
 unidirektionale 437
Vertrauensstellungen 437
Verwaltungsbereich 430
Verwaltungsrollen 429
Verwaltungsrolleneintrag 444
Verwaltungsrollengruppen 423, 437
Verwaltungsshell *siehe* Exchange Management Shell
VHDs 53
Viren 391
Virenschanner 161, 391
Virenschutz 386
Virtualisierungslösungen 52
Vollhybrid-Migration 579
Volume Shadow Copy Service 54
Volumeschattenkopie-Dienst 54

Voraussetzungen 18

vSphere 54

VSS 54

vssadmin.exe 514

W

Warnmeldung 151, 230

Warteschlange 490

 mail.que-Datei 130

Warteschlangen 125

Warteschlangendatenbank 130

Wartung 160

Wartungsarbeiten 151

Webfrontend 40

Webserverkomponente 176

Websitepostfach 220, 299

Weiterleitungsadresse 232

Weiterleitungsbenachrichtigungen 123

Wiedergabewarteschlange 511

Wiederherstellung 456, 500

Wiederherstellungsanforderungen 477

Wiederherstellungsdatenbank 461, 463

Wiederherstellungsserver 461

Wiederholungsintervall 117

Windows-Authentifizierung 109

Windows-Protokolle 387

Winrm 247

Wldap32.dll 581

X

XQDISCARD 90

XSHADOW 90

Z

Zeitsynchronisierung 53

Zertifikat 39, 179

Zertifikatimport-Assistent 179

Zertifizierungsstelle 179

Zeugenserver 493

Zugriffssteuerung 419

Zustellungs-Agent 112

Zuweisungen 422