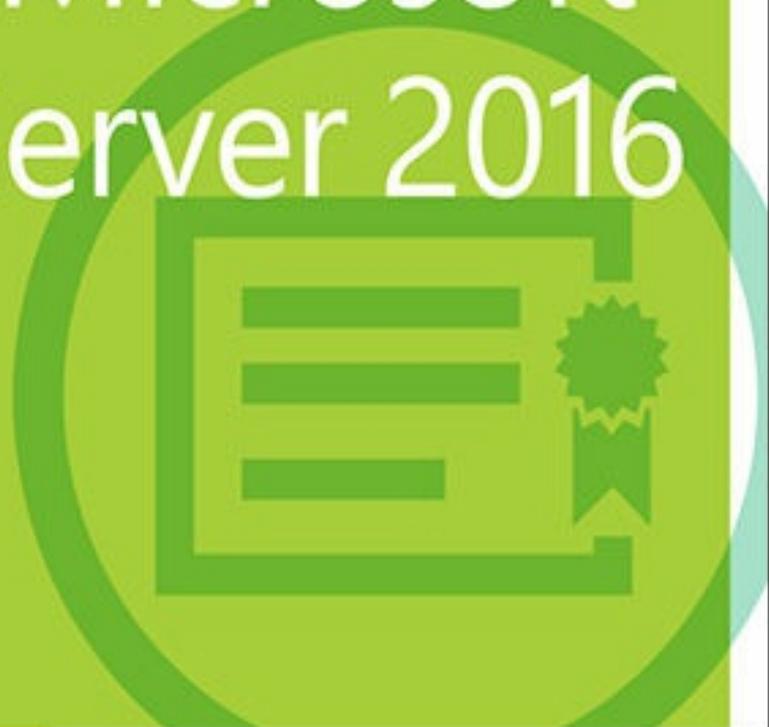




# Designing and Deploying Microsoft Exchange Server 2016



**Exam Ref 70-345**

Paul Cunningham  
Brian Svidergol

# **Exam Ref 70-345 Designing and Deploying Microsoft Exchange Server 2016**

**Paul Cunningham  
Brian Svidergol**



**PUBLISHED BY**

Microsoft Press

A division of Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052-6399

Copyright © 2016 by Paul Cunningham & Brian Svidergol

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Control Number: 2015956897

ISBN: 978-1-5093-0207-9

Printed and bound in the United States of America.

**First Printing**

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Support at [mspinput@microsoft.com](mailto:mspinput@microsoft.com). Please tell us what you think of this book at <http://aka.ms/tellpress>.

This book is provided “as-is” and expresses the author’s views and opinions. The views, opinions and information expressed in this book, including URL and other Internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

Microsoft and the trademarks listed at <http://www.microsoft.com> on the “Trademarks” webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

**Acquisitions Editor:** Karen Szall

**Developmental Editor:** Karen Szall

**Editorial Production:** Troy Mott, Ellie Volckhausen

**Technical Reviewer:** Bob Dean : Technical Review services provided by Content Master, a member of CM Group, Ltd.

**Copyeditor:** Rachel Jozsa

**Indexer:** Julie Grady

**Cover:** Twist Creative • Seattle



# Contents at a glance

[Introduction](#)

[Preparing for the exam](#)

[CHAPTER 1 Plan, deploy, manage, and troubleshoot mailbox databases](#)

[CHAPTER 2 Plan, deploy, manage, and troubleshoot client access services](#)

[CHAPTER 3 Plan, deploy, manage, and troubleshoot transport services](#)

[CHAPTER 4 Plan, deploy, and manage Exchange infrastructure, recipients, and security](#)

[CHAPTER 5 Plan, deploy, and manage compliance, archiving, eDiscovery, and auditing](#)

[CHAPTER 6 Implement and manage coexistence, hybrid scenarios, migration, and federation](#)

[Index](#)

# Contents

## Introduction

[Organization of this book](#)

[Microsoft certifications](#)

[Acknowledgments](#)

[Free ebooks from Microsoft Press](#)

[Microsoft Virtual Academy](#)

[Quick access to online references](#)

[Errata, updates, & book support](#)

[We want to hear from you](#)

[Stay in touch](#)

[Important: How to use this book to study for the exam](#)

## Chapter 1 Plan, deploy, manage, and troubleshoot mailbox databases

[Skill 1.1: Plan, deploy, and manage mailbox databases](#)

[Plan for database size and storage performance requirements](#)

[Plan mailbox database capacity and placement](#)

[Plan archive mailboxes capacity and placement](#)

[Plan modern public folder capacity and placement](#)

[Plan for storage architecture \(SAN, DAS, RAID, JBOD\)](#)

[Plan file system requirements](#)

[Plan for auto reseed](#)

[Plan for virtualization requirements and scenarios](#)

[Validate storage design by running Jetstress](#)

[Create and configure mailbox databases](#)

[Manage mailbox databases](#)

[Configure transaction log properties](#)

[Summary](#)

[Skill 1.2: Plan, deploy, and manage high availability solutions for mailbox databases](#)

[Identify failure domains](#)

Plan a solution that meets SLA requirements around scheduled downtime

Plan for software updates and server maintenance

Create, configure, and manage Database Availability Groups (DAG)

Create, configure, and manage DAG networks

Create, configure, and manage proper placement of a File Share Witness (FSW)

Create and configure mailbox database copies

Create, configure, and manage Azure DAG members

Summary

Skill 1.3: Plan, deploy, and manage a site-resilient Database Availability Group (DAG)

Plan, create, and configure cross-site DAG configuration

Plan, deploy, and configure Datacenter Activation Coordination (DAC)

Configure and manage proper placement of an alternate File Share Witness (FSW)

Test and perform site recovery

Summary

Skill 1.4: Monitor and troubleshoot mailbox databases

Monitor mailbox database replication and content indexing

Troubleshoot mailbox database replication and replay

Troubleshoot mailbox database copy activation

Troubleshoot mailbox database performance

Troubleshoot database failures

Resolve quorum issues

Summary

Skill 1.5: Plan, deploy, and manage backup and recovery solutions for mailbox databases

Plan most appropriate backup solution that meets SLA requirements of RPO/RTO

Recover an Exchange server

Recover a mailbox database

Recover a mailbox

Recover a mail item

Recover a public folder

Recover the public folder hierarchy

[Perform a dial tone restore](#)

[Deploy, configure, and manage lagged mailbox database copies](#)

[Summary](#)

[Thought experiment](#)

[Thought experiment answer](#)

## **[Chapter 2 Plan, deploy, manage, and troubleshoot client access services](#)**

[Skill 2.1: Plan, deploy, and manage Client Access services](#)

[Plan namespaces for client connectivity](#)

[Plan proxy and redirection requirements](#)

[Plan and deploy certificates](#)

[Plan and configure authentication](#)

[Plan, deploy, and configure Autodiscover, Outlook Anywhere, Outlook MAPI over HTTP, Exchange Web Services, Outlook on the web, Exchange Admin Center, Exchange ActiveSync, POP3, and IMAP4](#)

[Plan, deploy, and configure Office Online Servers](#)

[Plan, create, and configure Offline Address Book](#)

[Plan, create, and configure hierarchical address lists](#)

[Plan, deploy, and configure address book policies](#)

[Summary](#)

[Skill 2.2: Plan, deploy, and manage mobility solutions](#)

[Plan, deploy, and configure OWA for Devices, Outlook on the web policies, and mobile device mailbox policies](#)

[Plan, deploy, and configure ABQ](#)

[Plan, deploy, and configure Office Apps](#)

[Summary](#)

[Skill 2.3: Plan, deploy, and manage load balancing](#)

[Configure namespace load balancing](#)

[Plan for differences between layer seven and layer four load balancing methods](#)

[Summary](#)

[Skill 2.4: Monitor and troubleshoot client connectivity](#)

[Troubleshoot Outlook Anywhere connectivity](#)

[Troubleshoot Outlook MAPI over HTTP connectivity](#)

[Troubleshoot Exchange Web Services](#)

[Troubleshoot Outlook on the web](#)

[Troubleshoot POP3 and IMAP4](#)

[Troubleshoot authentication](#)

[Troubleshoot Autodiscover](#)

[Troubleshoot Exchange ActiveSync](#)

[Troubleshoot proxy and redirection issues](#)

[Summary](#)

[Skill 2.5: Plan, deploy, and manage a site-resilient client access services solution](#)

[Plan site-resilient namespaces](#)

[Configure site-resilient namespace URLs](#)

[Perform and test steps for site failover and switchover](#)

[Plan certificate requirements for site failovers](#)

[Manage expected client behavior during a failover and switchover](#)

[Summary](#)

[Thought experiment](#)

[Thought experiment answer](#)

## [Chapter 3 Plan, deploy, manage, and troubleshoot transport services](#)

[Skill 3.1: Plan, deploy, and manage transport services](#)

[Plan a solution that meets SLA requirements around message delivery](#)

[Plan inter-site mail flow](#)

[Plan inter-org mail flow](#)

[Plan, deploy, and configure redundancy for intra-site scenarios](#)

[Plan and configure for Safety Net](#)

[Plan and configure for shadow redundancy](#)

[Plan and configure for redundant MX records](#)

[Plan, create, and configure transport-related tasks](#)

[Summary](#)

[Skill 3.2: Troubleshoot and monitor transport services](#)

[Interpret message tracking logs and protocol logs](#)

[Troubleshoot a shared namespace environment](#)

[Troubleshoot SMTP mail flow](#)

Given a failure scenario, predict mail flow and identify how to recover  
Troubleshoot TLS

Troubleshoot the new transport architecture  
Summary

Skill 3.3: Plan, deploy, and manage message hygiene

Plan and configure malware filtering

Plan and configure spam filtering

Plan and configure connection filtering

Plan and configure recipient filtering

Plan and configure Sender Policy Framework

Plan and configure Spam Confidence Level (SCL) thresholds

Summary

Skill 3.4: Plan, deploy, and manage site resilient transport services

Plan, create and configure MX records for failover scenarios

Manage resubmission and reroute queues

Plan, create, and configure Send/Receive connectors for site resiliency

Test and perform steps for transport failover and switchover

Summary

Thought experiment

Thought experiment answer

## Chapter 4 Plan, deploy, and manage Exchange infrastructure, recipients, and security

Skill 4.1: Plan and configure Active Directory Domain Services for Exchange and Organizational settings

Plan the number of domain controllers

Plan placement of Global Catalog

Plan and configure DNS changes required for Exchange

Plan for schema changes required for Exchange

Prepare AD for Exchange

Prepare domains for Exchange

Plan and configure Active Directory site topology

Plan and configure throttling policies

## Summary

### Skill 4.2: Create and configure mail-enabled objects

Create and configure mailboxes

Create and configure resource mailboxes and scheduling

Create and configure shared mailboxes

Create and configure mail-enabled users and contacts

Create and configure distribution lists

Configure moderation

Create and configure linked mailboxes

Create and configure modern public folders

Summary

### Skill 4.3: Manage mail-enabled object permissions

Determine when to use Send As and Send On Behalf permissions

Configure mailbox folder permissions

Configure mailbox permissions

Set up room mailbox delegates

Configure auto-mapping

Create and configure public folder permissions

Summary

### Skill 4.4: Plan, deploy, manage, and troubleshoot Role Based Access Control

Determine appropriate RBAC roles and cmdlets

Limit administration using existing role groups

Evaluate differences between RBAC and Active Directory split permissions plan and configure a custom-scoped role group

Plan and configure delegated setup

Plan and create unscoped top-level roles

Troubleshoot RBAC

Plan and configure user assignment policies

Summary

### Skill 4.5: Plan an appropriate security strategy

Plan and configure BitLocker

Plan and configure S/MIME

Summary

## Skill 4.6: Plan, deploy, manage, and troubleshoot IRM

Plan and configure Information Rights Management (IRM) in Exchange

Create an RMS template

Plan and create transport protection rules

Plan and create Outlook protection rule

Plan and configure journal report decryption

Plan and configure IRM for eDiscovery

Plan and configure pre-licensing for client access

Troubleshoot failed IRM protection

Summary

Thought experiment

Thought experiment answer

## Chapter 5 Plan, deploy, and manage compliance, archiving, eDiscovery, and auditing

### Skill 5.1: Plan and configure Data Loss Prevention (DLP) solutions

Plan a DLP solution to meet business requirements

Plan and configure pre-built rules

Plan and create custom rules

Plan and configure DLP fingerprinting

Plan and configure custom DLP policies

Summary

### Skill 5.2: Plan, configure, and manage Archiving and Message Records Management (MRM)

Plan and configure archive and retention policies

Plan, create, and configure custom tags

Assign policies to users

Plan and configure the Managed Folder Assistant

Remove and delete tags

Plan and configure in-place archiving

Plan and configure online archiving (Office 365)

Summary

### Skill 5.3: Plan, configure, and perform eDiscovery

[Plan and delegate RBAC roles for eDiscovery](#)

[Perform multi-mailbox searches in Exchange admin center \(EAC\) and Exchange Management Shell](#)

[Perform a query-based in-place hold](#)

[Enable a legal/litigation hold](#)

[Integrate in-place federated search with Microsoft SharePoint Discovery center](#)  
[Summary](#)

#### [Skill 5.4: Plan, configure, and manage a compliance solution](#)

[Plan and configure MailTips](#)

[Plan, create, configure, and deploy message classifications](#)

[Plan and configure transport rules to meet specified compliance requirements](#)

[Plan and configure journaling](#)

[Summary](#)

#### [Skill 5.5: Plan, manage, and use mailbox and administrative auditing](#)

[Plan and configure mailbox audit logging](#)

[Plan and configure administrative audit logging](#)

[Summary](#)

[Thought experiment](#)

[Thought experiment answer](#)

## [Chapter 6 Implement and manage coexistence, hybrid scenarios, migration, and federation](#)

#### [Skill 6.1: Plan, deploy and troubleshoot coexistence with Office 365 \(Exchange Online\)](#)

[Plan, deploy, and manage hybrid configuration](#)

[Evaluate limitations of the Hybrid Configuration Wizard](#)

[Plan and manage hybrid deployment OAuth-based authentication](#)

[Troubleshoot transport with Exchange Online](#)

[Troubleshoot client access with Exchange Online](#)

[Troubleshoot directory synchronization](#)

[Summary](#)

#### [Skill 6.2: Plan, deploy, manage, and troubleshoot Exchange federation](#)

[Plan, create, and manage federation trusts with Microsoft federation gateways](#)

[Manage sharing policies](#)

[Manage organization relationships](#)

[Plan and create certificate and firewall requirements for federation](#)

[Troubleshoot Exchange federation trust and organization relationships](#)

[Troubleshoot cross-forest availability](#)

[Summary](#)

[Skill 6.3: Plan, deploy, and troubleshoot on-premises coexistence with earlier supported versions of Exchange](#)

[Plan, create, and configure namespaces for coexistence](#)

[Plan and configure proxy redirect](#)

[Plan firewall configurations for coexistence](#)

[Plan and configure for mail flow requirements](#)

[Plan for mailbox migrations](#)

[Troubleshoot transport in coexistence](#)

[Troubleshoot client access in coexistence](#)

[Summary](#)

[Skill 6.4: Migrate from earlier supported versions of Exchange](#)

[Determine transition paths to Exchange](#)

[Migrate mailboxes](#)

[Troubleshoot Mailbox Replication Services](#)

[Plan for discontinued features](#)

[Transition and decommission servers](#)

[Summary](#)

[Thought experiment](#)

[Thought experiment answer](#)

**What do you think of this book? We want to hear from you!**

**Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:**

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)



# Introduction

Many Exchange Server books take the approach of teaching you every detail about the product. Such books end up being huge and tough to read. Not to mention that remembering everything you read is incredibly challenging. That's why those books aren't the best choice for preparing for a certification exam such as the Microsoft Exam 70-345, "Designing and Deploying Microsoft Exchange Server 2016." For this book, we focus on your review of the Exchange Server skills that you need to maximize your chances of passing the exam. Our goal is to cover all of the skills measured on the exam, while bringing a real-world focus to the information. This book shouldn't be your only resource for exam preparation, but it can be your primary resource. We recommend combining the information in this book with some hands-on work in a lab environment (or as part of your job in a real-world environment).

The 70-345 exam is geared toward administrators that have a minimum of three years of experience working with Exchange Server. That doesn't mean you can't take and pass the exam with less experience, but it probably means that it will be harder. Of course, everyone is different. It is possible to get the knowledge and skills required to pass the 70-345 exam in fewer than three years. But whether you are a senior-level Exchange Server administrator or just a couple of years into your Exchange Server journey, we think you'll find the information in this book valuable as your primary exam prep resource.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the "Need more review?" links you'll find in the text to find more information and take the time to research and study the topic. Great information is available on MSDN, TechNet, and in blogs and forums.

## Organization of this book

This book is organized by the "Skills measured" list published for the exam. The "Skills measured" list is available for each exam on the Microsoft Learning website: <http://aka.ms/examlist>. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

## Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

### More Info: All Microsoft Certifications

For information about Microsoft certifications, including a full list of available certifications, go to <http://www.microsoft.com/learning>.

## Acknowledgments

**Paul Cunningham** I would like to thank Hayley, William, and Abby for their patience and support during the writing of this book, and for making everything in my life possible. I would also like to thank Tony Redmond, Orin Thomas, and my other fellow Microsoft MVPs for their friendship, help, and advice over the last several years. Finally, thanks to all of you around the world who make it so enjoyable being a part of the Exchange and Office 365 communities.

**Brian Svidergol** I would like to thank my wife Lindsay, son Jack, and daughter Leah for their continued love and support throughout these projects—I couldn't do it without you guys! I would also like to thank my mom, Pam, who enabled me to develop a passion for computers back in the bulletin board system (BBS) days, spending massive amounts of time on the computer tying up the phone line. I remember routinely going to the book store with mom and coming out with new computer books every time. That always made my day.

## Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

<http://aka.ms/mspressfree>

Check back often to see what is new!

## **Microsoft Virtual Academy**

Build your knowledge of Microsoft technologies with free expert-led online training from Microsoft Virtual Academy (MVA). MVA offers a comprehensive library of videos, live events, and more to help you learn the latest technologies and prepare for certification exams. You'll find what you need here:

<http://www.microsoftvirtualacademy.com>

## **Quick access to online references**

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these addresses (also known as URLs) can be painstaking to type into a web browser, so we've compiled all of them into a single list that readers of the print edition can refer to while they read.

Download the list at <http://aka.ms/ER345/downloads>.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

## **Errata, updates, & book support**

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

<http://aka.ms/ER345/errata>

If you discover an error that is not already listed, please submit it to us at the same page.

If you need additional support, email Microsoft Press Book Support at [mspinput@microsoft.com](mailto:mspinput@microsoft.com).

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to <http://support.microsoft.com>.

## **We want to hear from you**

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

<http://aka.ms/tellpress>

We know you're busy, so we've kept it short with just a few questions. Your answers go directly to the editors at Microsoft Press. (No personal information will be requested.) Thanks in advance for your input!

## **Stay in touch**

Let's keep the conversation going! We're on Twitter: <http://twitter.com/MicrosoftPress>.

## **Important: How to use this book to study for the exam**

Certification exams validate your on-the-job experience and product knowledge. To gauge your readiness to take an exam, use this Exam Ref to help you check your understanding of the skills tested by the exam. Determine the topics you know well and the areas in which you need more experience. To help you refresh your skills in specific areas, we have also provided “Need more review?” pointers, which direct you to more in-depth information outside the book.

The Exam Ref is not a substitute for hands-on experience. This book is not designed to teach you new skills.

We recommend that you round out your exam preparation by using a combination of available study materials and courses. Learn more about available classroom training at <http://www.microsoft.com/learning>. Microsoft Official Practice Tests are available for many exams at <http://aka.ms/practicetests>. You can also find free online courses and live events from Microsoft Virtual Academy at <http://www.microsoftvirtualacademy.com>.

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list for each exam is available on the Microsoft Learning website: <http://aka.ms/examlist>.

Note that this Exam Ref is based on this publicly available information and the author’s experience. To safeguard the integrity of the exam, authors do not have access to the exam questions.

# Chapter 1. Plan, deploy, manage, and troubleshoot mailbox databases

The Exchange Server 2016 mailbox server role hosts the mailbox databases for an organization. Mailbox databases host user and shared mailboxes, as well as the mailboxes for meeting rooms and equipment resources. Mailbox databases also host the contents of public folders and the public folder hierarchy in public folder mailboxes, which are also known as modern public folders. This method of public folder data storage was first implemented in Exchange Server 2013 and is different from Exchange Server 2010 and earlier, which used dedicated public folder databases. Hosting public folders in mailbox databases allows public folders to use the same high availability architecture, the Database Availability Group (DAG), as other types of mailboxes.

## Important: Have you read page xix?

It contains valuable information regarding the skills you need to pass the exam.

The architecture of Exchange Server 2016 is designed to deliver high performance and reliability for mailbox services at a lower cost. To achieve those goals, Microsoft has heavily invested in storage engine improvements aimed at reducing the input/output per second (IOPS) requirements for the storage hosting mailbox databases and removing the need for complex redundant array of independent disk (RAID) configurations. Exchange 2016 also includes managed availability, which is an intelligent self-monitoring and self-healing system that is able to detect issues and take corrective actions to maintain service availability. Many of the improvements in Exchange 2016 have come from Microsoft engineering, and from operating Exchange Online, the cloud-based Exchange that is part of Microsoft's Office 365 service. Code that has been tested at cloud-scale is now able to be implemented on-premises in customer datacenters. A well-designed Exchange 2016 mailbox server can perform well on its own, and when configured for high availability, can be resilient to a wide range of failure scenarios.

## Skills in this chapter:

- [Plan, deploy, and manage mailbox databases](#)
- [Plan, deploy, and manage high availability solutions for mailbox databases](#)
- [Plan, deploy, and manage a site-resilient Database Availability Group \(DAG\)](#)
- [Monitor and troubleshoot mailbox databases](#)
- [Plan, deploy, and manage backup and recovery solutions for mailbox databases](#)

## Skill 1.1: Plan, deploy, and manage mailbox databases

Deploying Exchange 2016 mailbox servers takes planning to ensure that the server and storage infrastructure used to host mailbox databases is able to meet the performance requirements of the environment. Installing an Exchange server without properly planning for the placement of database files and transaction logs, or choosing the wrong underlying storage technology, can lead to performance and stability issues that impact services, as well as the ability to recover from failures without data loss.

### This section covers how to:

- [Plan for database size and storage performance requirements](#)
- [Plan mailbox database capacity and placement](#)
- [Plan archive mailboxes capacity and placement](#)
- [Plan modern public folder capacity and placement](#)
- [Plan for storage architecture \(SAN, DAS, RAID, JBOD\)](#)
- [Plan file system requirements](#)
- [Plan for auto reseed](#)
- [Plan for virtualization requirements and scenarios](#)
- [Validate storage design by running Jetstress](#)
- [Create and configure mailbox databases](#)
- [Manage mailbox databases](#)
- [Configure transaction log properties and file placement](#)

### Plan for database size and storage performance requirements

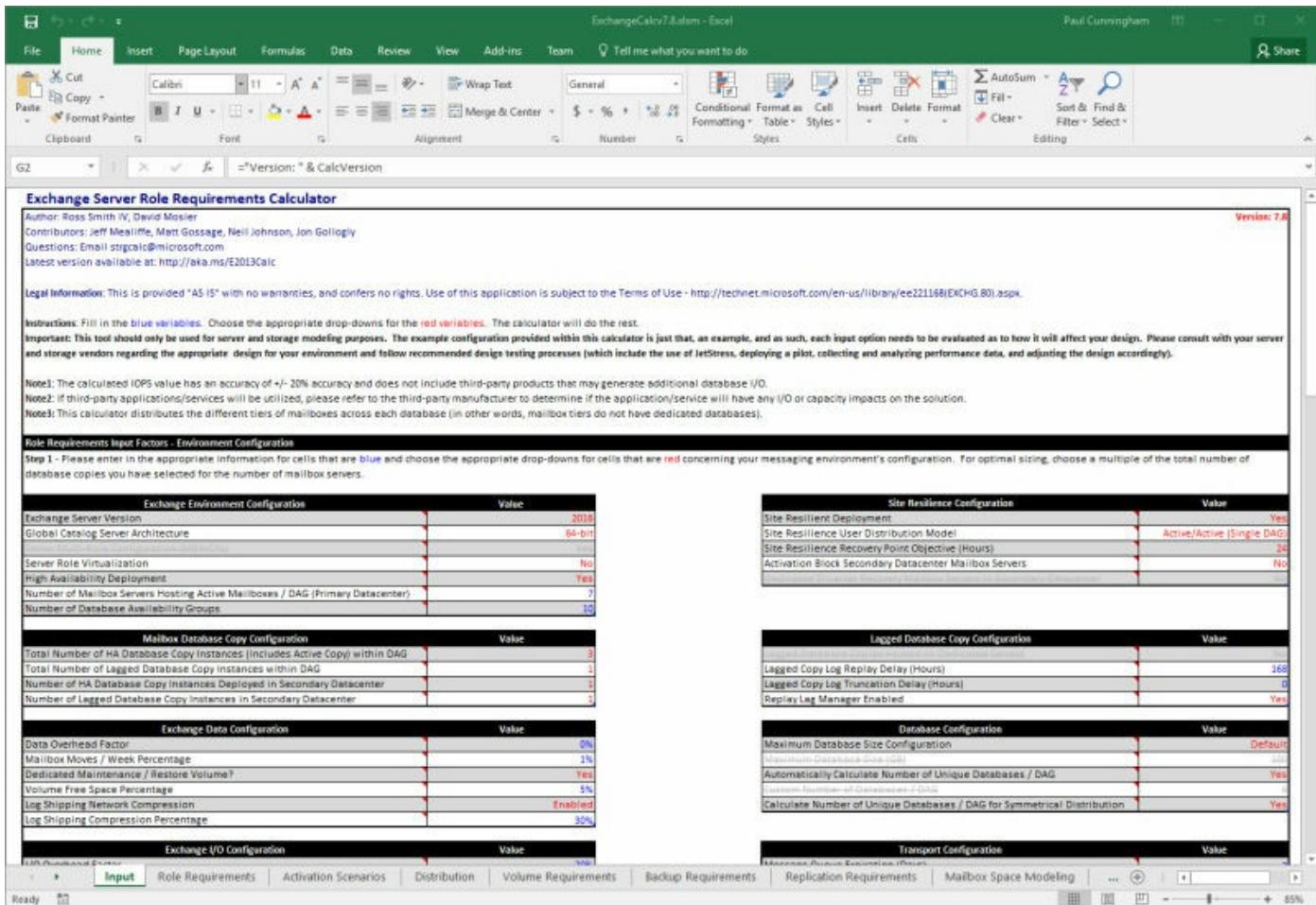
The database engine used by Exchange 2016 mailbox servers is capable of hosting databases up to 16 terabytes (TB) in size. That is a theoretical maximum because the capacity of disks available today is not large enough to store a 16-TB database file with another several terabytes of free space as well. Should disk capacities increase in the near future, there is still the issue of whether running a 16-TB database is recommended. Placing such a large amount of mailbox data in a single database carries the risk of extended recovery times if the database ever needs to be restored from a backup. Similarly, an extremely large database file requires an extended amount of time to seed or reseed between Database Availability Group members.

Such a large quantity of data also implies a very large number of mailbox users. Consider that even in the modern era of large mailboxes, a typical mailbox size is still around 2 gigabytes (GB), with extreme cases of 25 GB or more in some organizations. Considering an average mailbox size of 2 GB in a 1000 seat organization, the total

mailbox size can be estimated at 2 TB, with some extra allowances on top of that for database overheads. These overheads include the mailbox contents that each user can see, as well as the recoverable deleted items and other mailbox folders that are hidden from the user. The recoverable delete items folder has a default quota of 20 GB and can easily grow to that size if a mailbox is configured with a legal hold or an in-place hold.

Although the mailbox database engine is fully capable of running a 2-TB database file, placing the mailbox data for 1000 users within a single database concentrates the user load and the risk into a single point of failure. A more sensible approach is to separate mailbox data into multiple, smaller databases of approximately 200 GB in size, which distributes the risk of a long database restore or recovery time by reducing the size of the database files. This approach also allows the user load to be distributed across multiple storage volumes if necessary. For mailbox databases that are not replicated to multiple DAG members, a 200 GB maximum database size is considered best practice. The suggested best practice is purely a design and operational guideline and there are no technical limitations that prevent a non-replicated database from growing larger. Databases that are replicated to multiple DAG members can be sized up to 2 TB each within the best practice recommendations. Database replication, however, only reduces the risk of a long database restore or recovery operation by having multiple database copies available.

The size of the database is one important factor to consider when planning to deploy Exchange 2016 mailbox servers. You also need to consider the load caused by large numbers of users utilizing the same database hosted on a single underlying storage volume. Although Microsoft has invested heavily in reducing the storage IOPS requirements for mailbox databases, you still need to perform the necessary I/O calculations to plan for disks with sufficient performance. Microsoft provides a server sizing calculator for Exchange 2016 in the form of an Excel spreadsheet that contains formulas and macros to estimate disk performance requirements for your scenario, shown in [Figure 1-1](#). The calculator is regularly updated to ensure that it aligns with the latest sizing guidance and takes into account any changes in the Exchange 2016 codebase that have a performance impact on servers. You can download the calculator at <https://gallery.technet.microsoft.com/Exchange-2013-Server-Role-f8a61780>. Despite the URL containing the words “Exchange 2013,” the calculator applies to Exchange 2016. Use the calculator for all server sizing exercises to avoid performance issues caused by under-sized storage.



**FIGURE 1-1** The Exchange Server Role Requirements Calculator

## Plan mailbox database capacity and placement

When you have estimated the size of the mailbox databases to deploy in your environment, you can then plan the capacity of the storage volumes to host them. Database volumes need to be capable of hosting the estimated database file size, as well as the content indexing data that is used for mailbox searches by Outlook on the web users and for eDiscovery searches. In addition to existing data, the growth in mailbox data over time also needs to be taken into account to determine the size of the storage volumes. The Exchange Server Role Requirements Calculator does provide you with an estimated size for storage volumes, but keep in mind that the calculator takes into account data growth over several years, so the volume sizes can seem excessively large at first. Some organizations prefer to initially deploy a minimum amount of storage capacity and plan to expand it later as the Exchange databases grow. From that perspective, adding 20 percent to the current estimated database size should be sufficient.

The files for each mailbox database consist of the database and content index files, and also a set of transaction log files. Placement of the database and transaction log files depends on if you plan to replicate multiple copies of a database among DAG

members. For non-replicated databases it is recommended to place the database files on one volume and the transaction log files on a different volume. The two volumes should be backed by separate physical disks, mitigating the risk of a single physical disk failure that could cause the simultaneous loss of both the database and transaction log files, resulting in permanent data loss. Isolating the database and log files from failures allows for a database to be recovered to the point in time when the disk failure occurred, rather than only being able to recover the database to the point in time when the last backup was taken.

---



### Exam Tip

For standalone mailbox servers, always place the mailbox database and transaction log files on separate volumes backed by separate physical disks. Avoid any database placement that puts both the database files and the log files at risk of data loss from a single underlying disk failure.

---

For mailbox databases with multiple copies replicated in a DAG, the database and transaction log files can be co-located on the same volume. If a storage failure on one DAG member causes both the database and transaction log files to be lost, copies of the database and log files still exist on one or more other DAG members, so no permanent data loss is incurred. Even within a DAG, it is suggested to separate the database and log files onto different volumes to avoid potential data loss.

Exchange 2016 supports placing multiple databases on the same volume or separating databases onto their own dedicated volumes. The approach you take depends on the performance requirements of the databases. You should avoid overloading a single disk with more databases than it can handle the I/O requests for.

Carefully consider sizing the volumes that host the transaction log files. Transaction log files are generated by database operations, such as mailbox items being created, modified, or deleted. You can expect to see transaction logs being generated for any change within the database. Under conditions where there is a high rate of change, a large amount of transaction logging is generated. The volumes hosting log files, regardless of if they are co-located with the database files, must have enough free disk space to account for the maximum amount of transaction logging that occurs on a day to day basis.

## **Plan archive mailboxes capacity and placement**

In addition to normal user mailboxes, Exchange 2016 can also host archive mailboxes within its mailbox databases. Archive mailboxes are associated with a mailbox user who has been enabled for archiving. Mailbox items are moved from the primary mailbox to the archive mailbox based on retention policies that are configured and applied to mailbox users.

From a design perspective, there is no defined best practice for archive mailbox placement. Microsoft's recommendation, based on its experience operating Exchange Online, is to place an archive mailbox in the same database as the primary mailbox for that user. This ensures that both mailboxes are subject to the same service availability conditions. For example, by placing the mailboxes together, it avoids confusion for the user if one mailbox is available yet the other is not.

Some organizations prefer to place the primary and archive mailboxes for a user on separate mailbox databases. The reasons for this vary. In some cases, the intention is to use a different mailbox density for archive mailboxes than primary mailboxes. For others, it is to apply a different backup schedule to the archive mailbox than is applied to the primary mailbox. Keeping the mailboxes together, keeping them apart on different databases, or even keeping them on entirely different servers is supported in either scenario.

You must also consider the size of the archive mailboxes as part of the overall capacity planning. The archive mailboxes grow as the Managed Folder Assistant moves items from the primary mailbox in accordance with the retention policy assigned to the mailbox user. Assuming that the rate of new items being received or created in the primary mailbox is the same as the rate of items being moved to the archive mailbox, the primary mailbox remains at a fairly static size while the archive mailbox grows. In an environment where archive mailboxes are placed in separate databases to primary mailboxes, most of the database growth occurs in the archive mailbox databases. The primary mailbox databases remain fairly static in size. This inconsistent growth must be taken into account when you plan for the size of your storage volumes. It is also one of the reasons Microsoft recommends co-locating primary and archive mailboxes in the same database, so that the databases in the environment all grow at a more consistent and predictable rate.

## Plan modern public folder capacity and placement

In Exchange 2010 and earlier versions, public folders were stored in dedicated public folder databases. An Exchange server could host one public folder database and the public folder hierarchy. Content could then be replicated to other public folder databases in the organization. This multi-master replication allowed administrators to place public folder databases close to the users who needed them and configure replicas for the folders that users in multiple locations needed. This architecture did have its disadvantages. Public folder databases could not leverage the improvements in high availability that were developed for mailbox databases, namely the Database Availability Group. Also, public folder replication could be slow and unreliable at times, and the multi-master nature of it could cause replication conflicts to occur when users made changes to the same content in different replicas.

In Exchange 2013, Microsoft changed the public folder architecture to use public folder mailboxes instead. The public folder mailboxes are hosted in the same type of database as other mailbox types. This change removes the problems of the multi-master topology and allows public folders to take advantage of Database Availability Groups for high availability. These changes however, introduce new issues that need to be handled correctly when designing public folders in Exchange 2016.

The public folder hierarchy is stored in the first public folder mailbox created in the organization. This mailbox is referred to as the primary hierarchy mailbox and hosts the only writeable copy of the public folder hierarchy. Other than this feature, it is no different than other public folder mailboxes. Other public folder mailboxes can host a read-only copy of the hierarchy and are considered secondary hierarchy mailboxes. You can determine which public folder mailbox is the primary hierarchy mailbox by running Get-OrganizationConfig to retrieve the GUID of the RootPublicFolderMailbox. Next, compare it to the ExchangeGuid for the public folder mailboxes in the organization, as shown in [Listing 1-1](#). The RootPublicFolderMailbox value is empty if no public folder mailboxes have been created.

### LISTING 1-1 Locating the primary public folder hierarchy mailbox

[Click here to view code image](#)

```
[PS] C:\>Get-OrganizationConfig | Select-Object RootPublicFolderMailbox  
RootPublicFolderMailbox  
-----  
612fd5f2-1e50-4280-bce4-dd4b0791744d  
[PS] C:\>Get-Mailbox -PublicFolder | Where {$_.ExchangeGuid -eq "612fd5f2-  
1e50-4280-  
bce4-dd4b0791744d"}
```

Name	Alias	ServerName
ProhibitSendQuota	-----	-----
-----	-----	-----
PFMailbox01	PFMailbox01	ny-exch01
		Unlimited

---

Any additional public folder mailboxes in the environment are able to host a secondary copy of the public folder hierarchy. When a public folder mailbox is created, it needs some time to synchronize its copy of the hierarchy from the primary hierarchy mailbox. This delay means that any users connecting to the secondary hierarchy mailbox see an incomplete public folder hierarchy until the synchronization has finished. For that reason, it is recommended to exclude new public folder mailboxes from serving the hierarchy until the synchronization is complete. When you run the New-Mailbox cmdlet to create a public folder mailbox, use the IsExcludedFromServingHierarchy parameter to prevent the mailbox from serving the hierarchy before it has fully synchronized.

After creating the new public folder mailbox, you can monitor the IsHierarchyReady attribute until it shows a value of True. The synchronization of the hierarchy occurs every 15 minutes if any users are connected to the public folder mailbox. Synchronization occurs every 24 hours if no users are connected, which is the case for a new public folder mailbox that doesn't yet contain any public folder content. After the hierarchy has synchronized, you can configure the mailbox to permit it to serve the public folder hierarchy to clients, shown in [Listing 1-2](#).

## LISTING 1-2 Creating a new public folder mailbox, and managing the serving of the public folder hierarchy

[Click here to view code image](#)

---

```
[PS] C:\>New-Mailbox -PublicFolder -Name PFMailbox02 -  
IsExcludedFromServingHierarchy  
$true
```

Name	Alias	ServerName
ProhibitSendQuota	-----	-----
-----	-----	-----
PFMailbox02	PFMailbox02	ny-exch01
		Unlimited

```
[PS] C:\>Get-Mailbox -PublicFolder PFMailbox02 | Select IsHierarchyReady  
IsHierarchyReady : True
```

```
[PS] C:\>Set-Mailbox -PublicFolder PFMailbox02 -  
IsExcludedFromServingHierarchy $false
```

---

When a user is connected to a secondary hierarchy mailbox and makes a change, such

as adding a new folder under an existing folder, the request is proxied to the primary hierarchy mailbox. It is proxied to this location because only the primary hierarchy mailbox has a writeable copy of the hierarchy.

For accessing public folder contents, users connect to the public folder mailbox hosting that particular public folder. There are two things you should keep in mind for user access to public folder content:

- Public folder content isn't replicated to multiple public folder mailboxes. The mailboxes themselves can be replicated in a Database Availability Group, but only the mailbox in the active database is online and accessible to users. This makes the placement of public folders throughout your network something requiring careful planning to avoid poor Outlook performance. Poor performance could occur if there is high network latency between the user and the public folder. Public folder content should be located in mailboxes hosted within databases that are close to where the users are who need that content. You can also ensure that a user connects to a specific public folder mailbox by using Set-Mailbox to configure the DefaultPublicFolderMailbox property for their mailbox.
- Heavily used public folders can cause a significant load of client traffic on a single public folder mailbox. This also causes a heavy load on the mailbox database hosting that mailbox. It is recommended to separate heavily used public folders into their own public folder mailbox, and disabling those mailboxes from serving the public folder hierarchy.

You can move public folders between mailboxes by creating public folder move requests with the New-PublicFolderMoveRequest cmdlet. A public folder move request only moves a specific public folder, not including sub-folders. To move a public folder and all of its sub-folders, use the Move-PublicFolderBranch.ps1 script provided in the scripts folder of the Exchange 2016 installation.

Another consideration when placing public folders is folder size. Now that public folders are stored in mailboxes, they inherit the mailbox storage quotas configured on the mailbox database and defined by the IssueWarningQuota, ProhibitSendQuota, and ProhibitSendRecieveQuota properties of the database. By default, the storage quotas are:

- Issue warning quota—1.9 GB
- Prohibit send quota—2 GB
- Prohibit send and receive quota – 2.3 GB

You can configure higher quota thresholds at the database level using the Set-MailboxDatabase cmdlet if the mailbox database only hosts public folder mailboxes. If public folder mailboxes are inter-mingled with other mailbox types in a database, you can use Set-Mailbox cmdlet to set different quotas for that particular mailbox. When a

mailbox is configured with storage quotas that differ from the database it is located in, you must also set the UseDatabaseQuotaDefaults attribute to False for that mailbox. Database-level quotas continue to apply without these changes.

### Note: Public Folder Limits in Exchange 2016

Exchange 2016 has limits for public folders that include the total number of public folder mailboxes, the total number of folders in the hierarchy, the maximum sub-folder depth, the maximum public folder size, and many more. The limits are not always hard limits of the technology, but primarily exist for support or performance reasons. The limits change over time as Microsoft makes engineering investments in public folders. You can find the latest details about public folder limits in Exchange 2016 on TechNet: [https://technet.microsoft.com/library/dn594582\(v=exchg.160\).aspx](https://technet.microsoft.com/library/dn594582(v=exchg.160).aspx).

## Plan for storage architecture (SAN, DAS, RAID, JBOD)

Exchange 2016 supports a variety of storage architectures. This allows customers to choose storage that meets their performance requirements, fits into their budgets, and aligns with existing storage investments within their datacenters. Direct-attached Storage (DAS) is the recommended practice as it is the least complex, most reliable, and most predictable method of connecting storage to Exchange servers.

Customers who already have a Storage Area Network (SAN) can also use it for Exchange servers. SAN includes both iSCSI and fibre channel connected storage. When SAN volumes are used to host Exchange application data, the following recommendations are given:

- Do not share the physical disks that make up the SAN volumes for Exchange data with any other applications also using the SAN for storage. This prevents disk contention issues from impacting Exchange performance.
- For iSCSI connected storage, use dedicated storage networks. This involves the installation of additional 1 gigabit per second (Gbps) or 10 Gbps network interfaces on the Exchange servers connected to the iSCSI storage network.
- Use multiple storage network paths to avoid any single points of failure with the storage connectivity.
- For SANs that support tiers of data storage, in which the most accessed files are automatically moved by storage controllers to higher speed disks within the SAN enclosure, it is recommended to disable tiers for Exchange data.

## **Important: Beware of Unsupported Storage Types**

Network-Attached Storage (NAS) is generally not supported for Exchange 2016, nor is any storage that is not block-level storage. This includes any form of network file system (NFS) storage, no matter how robust or enterprise-grade the storage vendor claims it to be. NFS storage presented by a hypervisor to a virtualized Exchange server as a virtual SCSI device is also unsupported. The exception to these rules is Server Message Block (SMB) 3.0 storage that aligns with Microsoft's virtualization support guidelines for Exchange. Any form of data deduplication is also unsupported for Exchange application data.

Microsoft's recommendation in "The Exchange 2016 Preferred Architecture" (<https://blogs.technet.microsoft.com/exchange/2015/10/12/the-exchange-2016-preferred-architecture/>) is to use "just a bunch of disks" (JBOD) for storing mailbox databases. JBOD eliminates the configuration complexity and performance overheads of a redundant array of independent disks (RAID) storage configuration. Data stored on RAID-backed storage volumes is protected from permanent loss of data in the event that a single physical disk fails because the data is striped or mirrored across multiple physical disks. RAID makes perfect sense for the volume that hosts an Exchange server's operating system and application files. It is also recommended for use on those volumes no matter how many servers or database copies are being deployed. A RAID-1 volume is suitable for that task. RAID is suitable for all of the storage volumes on standalone mailbox servers that host non-replicated databases as well.

When a database is replicated to multiple DAG members, there are multiple copies of the database files. These files are isolated from each other in the different storage locations connected to each DAG member. Therefore, the database copies are protected from the failure of a single physical disk because another server has a copy of the database files. One situation to avoid is when a single failure reduces the number of database copies to one. Permanent data loss could occur if the last remaining database copy is hosted on a non-RAID volume and the physical disk it is stored on fails. For this reason, it is only recommended to use JBOD to store mailbox databases when at least three copies of the database are hosted by DAG members.

The disks allocated to an Exchange server can be configured as either basic disks or dynamic disks. Best practice is to use basic disks, meaning the volumes are contained on a single disk. Dynamic disks allow a volume to span multiple disks, or can be used to create striped, mirrored, or RAID-5 volumes. Although dynamic disks are supported, they are not recommended. Consider breaking up the mailboxes into multiple, smaller databases if you have databases that exceed the maximum volume size you can configure.

on a basic disk. The volumes created on the disks can be either GUID partition table (GPT) or master boot record (MBR) volumes. Although both GPT and MBR are supported, it is best practice to use GPT partitions because they can be up to 256 TB in size, well beyond the size required for an Exchange server. In contrast, MBR partitions only have a maximum size of 2 TB, which is suitable for some environments but too small for others. GPT is the best choice considering you can't convert an MBR partition to a GPT partition later without data loss.

## Plan file system requirements

Exchange 2016 supports both NTFS file system (NTFS) and Resilient File System (ReFS) for any volumes on the server that host operating system or application files. Although NTFS is a supported file system, some features of NTFS are not supported for Exchange server, namely NTFS compression and the NTFS Encrypting File System (EFS).

For Exchange 2016 the recommended file system for volumes hosting mailbox database and transaction log files is ReFS. ReFS is engineered to provide enhanced data verification and auto-correction and is more resilient to file system corruption. ReFS is not supported for the operating system volume however, or for volumes containing the Exchange application binaries themselves. When configuring a volume, it is best practice to disable the data integrity features of ReFS for the entire volume. Disabling the integrity features does not remove all of the benefits of ReFS for Exchange data, but avoids performance problems associated with the ReFS integrity stream for Exchange servers.

To format a volume for ReFS, use the PowerShell disk management cmdlets. The disk number for the disk that you want to format for ReFS volume can be identified using the Get-Disk cmdlet, followed by running a series of PowerShell cmdlets demonstrated in [Listing 1-3](#).

### LISTING 1-3 Running PowerShell storage management cmdlets to format an ReFS volume

[Click here to view code image](#)

---

Number	Friendly Name Style	OperationalStatus	Total Size	Partition
2	Microsoft Virtual Disk	Online	100 GB	GPT
1	Microsoft Virtual Disk	Online	100 GB	GPT
3	Microsoft Virtual Disk	Online	100 GB	RAW
0	Virtual HD ATA Device	Online	95 GB	MBR

```

PS C:\> Get-Disk 3 | Initialize-Disk -PartitionStyle GPT -PassThru | New-Partition
-UseMaximumSize | Format-Volume -FileSystem ReFS -NewFileSystemLabel
Volume3
-SetIntegrityStreams $false

Confirm
Are you sure you want to perform this action?
Warning, all data on the volume will be lost!
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):

Y

DriveLetter FileSystemLabel FileSystem DriveType HealthStatus
----- ----- -----
Volume3 ReFS Fixed Healthy

```

---

The mount points assigned to volumes formatted for Exchange depend on the mailbox database layout approach that you use.

- For single mailbox servers where the database and log files are placed on separate volumes, you can use drive letters to mount the volumes, such as F:\ or G:\. It is possible to run out of drive letters if you have a large number of mailbox databases on the server. In that case, you can mount the volumes in folders instead.
- For mailbox servers that are DAG members, it is recommended to mount the volumes in folders instead of drive letters, for example C:\ExchangeDatabases\DB01. This configuration simplifies mount point management for servers in the DAG, as well as being a foundational component of auto reseed.

## Plan for auto reseed

Auto reseed is a feature of Exchange 2016 allowing a mailbox server that is a member of a DAG to automatically detect and recover from storage failure scenarios. With auto reseed, the members of an Exchange 2016 DAG are pre-configured with one or more storage volumes that do not host any data and are available as spares. When a disk currently in use by Exchange fails, Managed Availability initiates a recovery workflow that automatically replaces the failed disk and reseeds the failed database copy back onto the new disk. This automated recovery eliminates the manual steps required in Exchange 2010 for an operator to replace failed storage before a database copy could be reseeded. With auto reseed, the resiliency of the DAG is automatically restored and the only operator intervention comes after the service has recovered. The only manual step is to replace the failed disk with a new one and configure it as a spare for future disk failure recoveries.

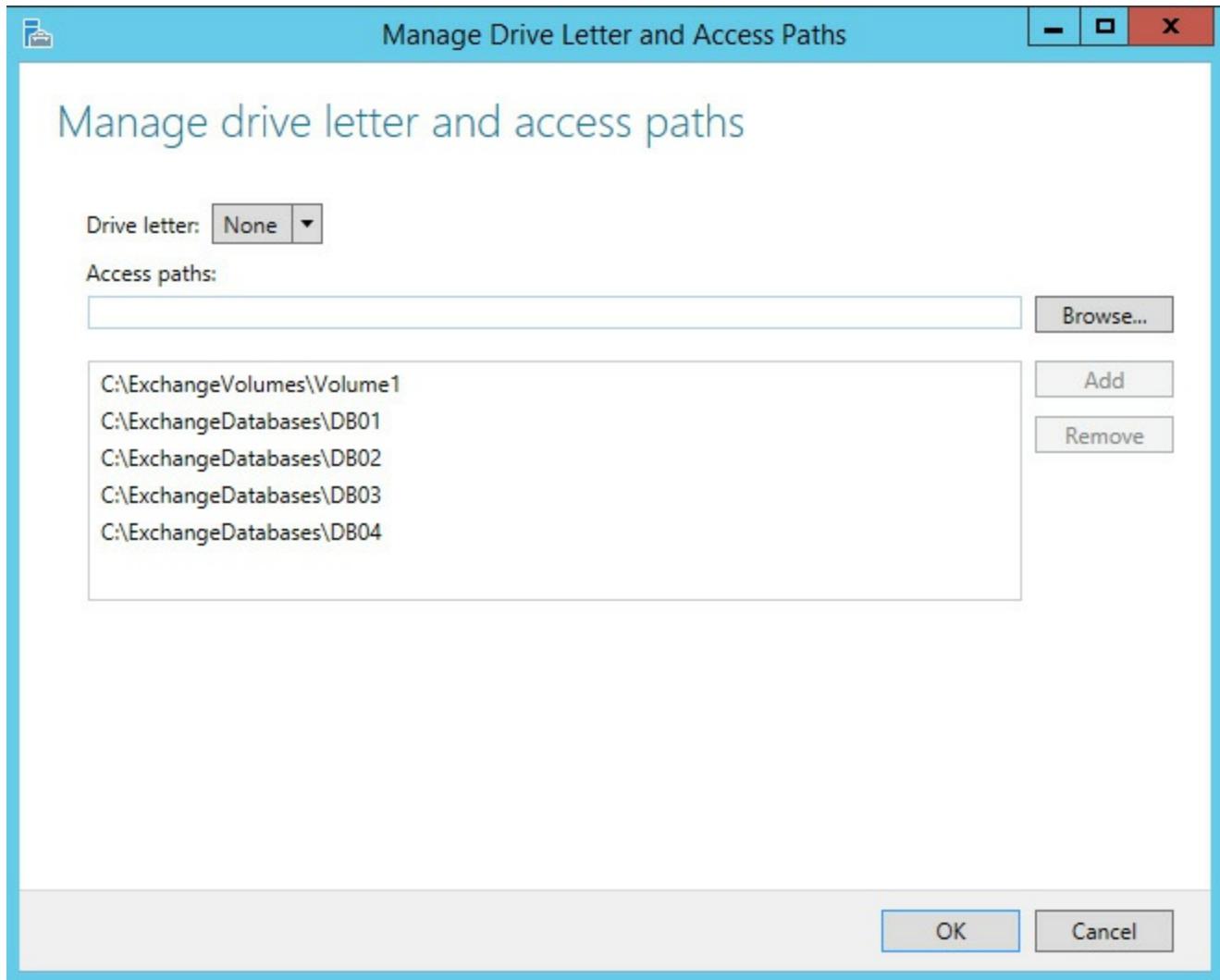
Laying the foundation for auto reseed involves the right planning and configuration of the underlying storage for the mailbox server:

- JBOD storage should be used for database and transaction log volumes. Remember that JBOD is only recommended when more than two copies of the database are replicated within the DAG. Using auto reseed is not practical when only two database copies exist because the underlying storage would be a RAID volume resilient to the type of failures that trigger the auto reseed recovery process.
- Multiple databases per volume should be used to improve the speed that failed database copies are reseeded when a disk has been replaced. The limiting factor for reseed performance is the speed of the disk hosting the database that is being used as a seeding source. One large database reseeding from a single disk is slower than four smaller databases reseeding from four different disks. The recommended number of databases per volume is equal to the number of copies of each database. For example, in a DAG with four copies of each database, four databases should be placed on the same volume.
- Co-locate the database and transaction log files on the same volume. Separating the database and log files is not required when more than two database copies exist because the databases are replicated to multiple copies within the DAG. Auto reseed requires the database and log files to be co-located on the same volume. If they are not co-located, recovery is not initiated for that database.

An Exchange 2016 DAG has two properties that define the root folder paths for volumes involved in the auto reseed process. They are the `AutoDagDatabasesRootFolderPath`, which defaults to `C:\ExchangeDatabases`, and the `AutoDagVolumesRootFolderPath`, which defaults to `C:\ExchangeVolumes`. You can modify the paths if you like, but it is not recommended and there is no advantage in doing so.

Consider a scenario in which a DAG has four databases, each with four copies hosted by the four DAG members. For each of the DAG members, the volumes hosting the mailbox databases and transaction log files are first mounted into sub-folders of the `AutoDagVolumesRootFolderPath`, for example, `C:\ExchangeVolumes\Volume1`.

Next, the same volumes are configured with additional mount paths that coincide with the names of the mailbox databases. For example, if you have four databases named DB01, DB02, DB03, and DB04, the same names must be used for the folder names in the mount paths, as shown in [Figure 1-2](#). An example folder name would be, `C:\ExchangeDatabases\DB01`.



**FIGURE 1-2** Configuring the access paths for Exchange volumes

Finally, within each database folder, two additional folders are created to host the database and transaction log files. The names of these folders must also align with the names of the mailbox databases. For a database named DB01, the two subfolders are therefore named DB01.db and DB01.log. The outcome of this configuration is a predictable storage layout for auto reseed to use when the recovery workflow is initiated. The workflow begins with the detection of a failed volume. Failed volumes are detected by periodically checking for database copies that have a status of FailedAndSuspended for more than 15 minutes. Three attempts are made to resume the failed database copies. The underlying storage has failed if after three attempts all of the database copies on a volume still have a FailedAndSuspended status. The server then attempts to replace the failed volume with a spare volume. The server can make up to five attempts, one per hour, to replace the volume. If the spare volume is successfully assigned, the server attempts to reseed the failed database copies to the new volume, again making up to five attempts, one attempt per hour. The operators can replace the failed disk with another spare if the recovery workflow is successful. If the recovery

workflow is unsuccessful, the server waits three days and if the database copies are still FailedAndSuspended the server attempts the recovery workflow again.

---

### **Note: Auto Reseed Recovery Actions are Not Instantaneous**

The timing of the recovery stages is intended to ensure that Exchange doesn't take corrective action too quickly when minor issues occur. Recovery actions are taken only after a level of confidence is reached that a storage failure has occurred. Recovery actions are also repeated at intervals to ensure that intermittent factors don't cause the whole workflow to fail. A successful recovery workflow might take as little as an hour to complete or anywhere up to 12 hours.

---

## **Plan for virtualization requirements and scenarios**

Virtualization is widely used in customer datacenters of all sizes. Many customers take a virtualization first approach to server deployments, and therefore prefer to deploy Exchange 2016 on virtual machines as well. Exchange 2016 servers support virtualization, but there are strict guidelines that you should adhere to so that you remain within the boundaries of what is supported.

Exchange 2016 can be virtualized using the Hyper-V server role of Windows Server or the dedicated Hyper-V server product. Third party hypervisors are also supported as long as they have first been validated under the Windows Server Virtualization Validation Program. Even on supported hypervisors, you must take care to ensure that you do not use virtualization features that are not supported.

Virtualization is a commonly used way of achieving maximum resource utilization by sharing hardware resources with multiple virtual machines. This type of sharing, however, introduces the risk of resource contention. Resource contention occurs when two or more virtual machines fight for the same CPU or memory resources. Exchange 2016 doesn't respond well when it can't get access to the hardware resources it requires. Performance can degrade and errors can surface that lessen the user experience. As such, Exchange 2016 virtual machines should not be placed on highly oversubscribed hosts. The maximum supported level for virtual CPU to logical CPU for all virtual machines on the host is a ratio of 2:1, although 1:1 is recommended. The Exchange VMs must also have a fixed memory allocation with no memory overcommitment on the host. Virtual machines should be sized using the same Exchange Server Role Requirements Calculator used to size physical servers. The calculator prompts you as to whether server role virtualization is being used and if so, adds an appropriate amount of overhead to the recommended CPU sizing for the server.

## **Important: Exchange Virtual Machines and Dynamic Memory**

The ability to assign a variable amount of memory to virtual machines has many names. In Hyper-V it is referred to as dynamic memory. The idea is that a VM is allocated the minimum amount of memory at startup, and can then increase and decrease the amount of memory in use depending on the application workload at the time. This doesn't work well for Exchange, which allocates a static amount of available memory to each of the worker store processes hosting a mounted database on the server. If the initial memory allocation is limited by the hypervisor, each worker store receives far less memory than it requires. Also, the worker stores cannot dynamically increase the memory during heavy workloads. As a result, Exchange server performance suffers, and you can expect to see a variety of errors and crashes due to a lack of resources.

The storage allocated to Exchange 2016 VMs has the same support requirements as the physical machines discussed earlier and must also be of a fixed size. Virtualization platforms usually have built-in features available that can be used to "thin provision" the virtual disks allocated to a VM. This way the disks only take up approximately as much space on the host machine as the data within the VM requires. In other words, the free disk space the VM's operating system sees inside of a virtual disk is not actually used on the host machine until the VM uses that space to store data. In fact, the free space that a VM sees could well exceed the actual capacity of the host machine. Storage over commitment creates a risk of Exchange trying to perform write operations on a mailbox database and failing because no more physical disk space is available for the database to grow. This type of scenario can cause database corruption and should be avoided. As such, it is required that any virtual disks allocated to an Exchange 2016 VM be of a static size and not be thin provisioned or dynamically expanding.

Many virtualization platforms have high availability features that allow the hypervisor to move a running VM from one host to another without shutting down the VM. This functionality is not supported for Exchange 2016. An Exchange VM can't be moved between hosts unless it is brought online on the second host as a cold boot. In other words, any time a VM is moved to another host, you should shut down the VM before you move it. The exception to that rule is Hyper-V Live Migration, which is fully supported for moving a running VM between Hyper-V hosts.

Disaster recovery planning for virtual machines is also important. Some hypervisors include disaster recovery features that can replicate running VMs to a separate datacenter, where they are kept as a cold standby in case of a major disaster at the primary datacenter. For Exchange 2016 VMs, no form of VM replication is supported. It

is recommended to use a Database Availability Group to provide site resiliency for Exchange 2016.

A final point about virtualized Exchange 2016 servers is that snapshots of the VMs are not supported for recovery, which means there is little benefit in taking snapshots at all. This is often a point of confusion because virtual machine backup products utilize hypervisor snapshots to make a point in time backup of the running VM. While snapshot-based backup products are often supported, the recovery process from those products does not involve reverting a running VM to a previous snapshot. Instead, the snapshots are used temporarily to create the backup. Other methods are then used to restore the data from within the backed up mailbox databases when necessary.

### **Important: Exchange 2016 Does Not Support Time Travel**

Rolling back an Exchange VM to a previous point in time is not supported under any circumstances. This action can cause irreparable harm to your Exchange and Active Directory environments. In any situation where you would consider a rollback, the correct course of action is to perform a recovery install of Exchange onto a new server of the same name. To avoid significant recovery related downtimes, deploy Database Availability Groups instead, which allows service availability to continue when a single Exchange server has an unrecoverable failure.

## **Validate storage design by running Jetstress**

Despite the investment by Microsoft in reducing the IOPS requirements for mailbox databases in Exchange 2016, deploying storage for Exchange is not simply a matter of attaching a bunch of disks and running your production databases on them. Before any production data is placed on the disks and before the Exchange 2016 software is even installed, you should test the performance of the storage. Testing the storage ensures it can meet the performance requirements estimated by the Exchange Server Role Requirements Calculator.

Microsoft provides the Jetstress tool for verifying the performance and stability of your storage by simulating disk I/O loads that would be produced by a given number of users. In doing so, Jetstress tests the disk hardware itself, as well as the storage firmware, storage controllers, and the file system. The effectiveness of the Jetstress test depends on the input values you provide. As long as you are able to provide accurate user profile information to Jetstress then the test results should be a true and accurate reflection of how well you can expect the storage to perform under the anticipated load.

## **Important: Jetstress Can't be Used on Running Exchange Servers**

Jetstress is designed to be run before you install Exchange 2016 on the server. It is too late to perform Jetstress tests if you already have Exchange installed. In this scenario, you should uninstall Exchange, run Jetstress, and then reinstall Exchange when the tests are complete.

The Jetstress testing scenarios you run should accurately represent the variety of operational scenarios that could occur in your environment. For instance, you would need to run Jetstress to validate both a healthy and a degraded RAID volume if you've configured RAID storage volumes for Exchange. Otherwise, when a disk in a RAID volume inevitably fails, you run the risk of subjecting users to poor performance while the RAID volume is repaired. There are a lot of shared resources involved that need to be validated if you are virtualizing your Exchange servers. Therefore, you should run Jetstress during peak load periods to verify that the Exchange VMs are able to perform at any time of day.

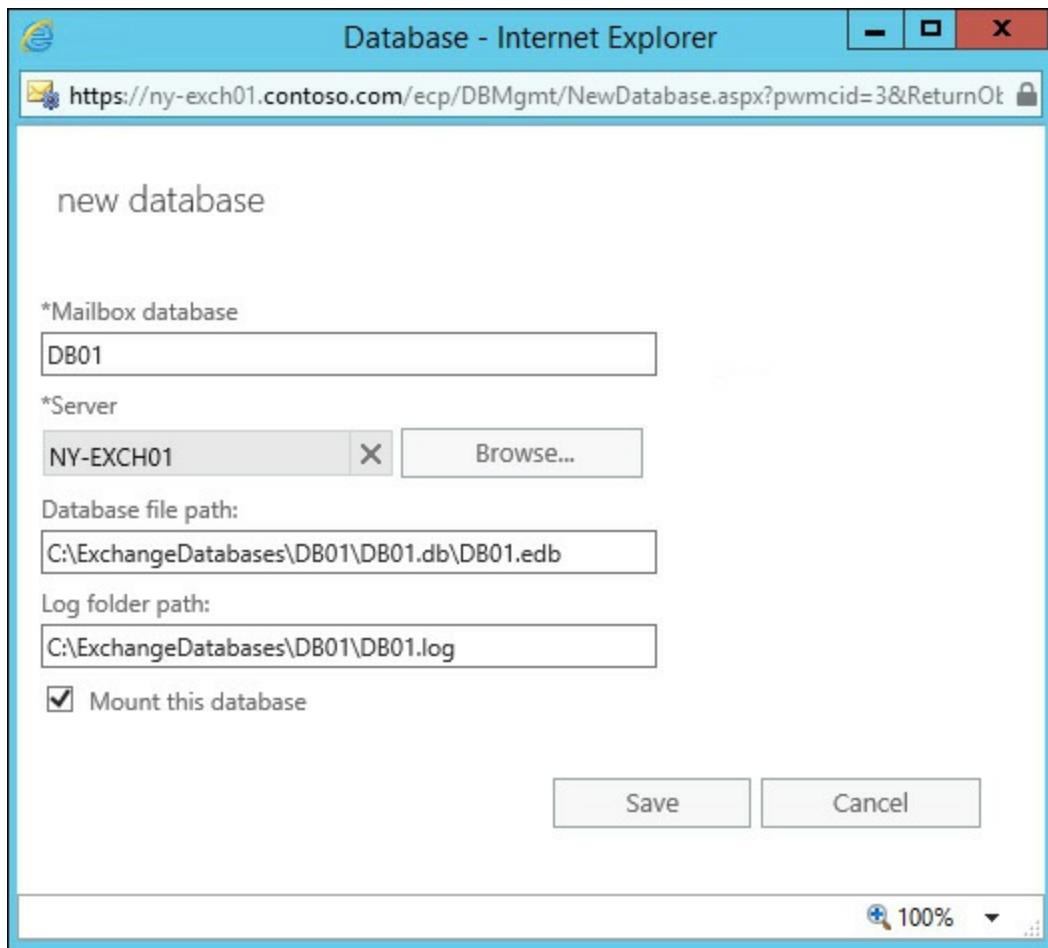
Interpreting Jetstress results is an interesting exercise. A failed test does not mean that the Jetstress tool itself has failed. Instead, it means that Jetstress determined the storage subsystem was not able to perform to the level you required based on the user load you specified. Assuming that you provided accurate numbers to Jetstress at the beginning of the test, you can remediate a failed test by looking at your storage subsystem. Performance problems can be caused by out of date firmware, hardware faults, or simply by poorly chosen components. Changing the Jetstress numbers to "fake" a successful test result only backfires when you put the under-performing system into production.

## **Need More Review? The Jetstress Field Guide**

Reference the Jetstress Field Guide, located in the TechNet Gallery at <https://gallery.technet.microsoft.com/Jetstress-2013-Field-Guide-2438bc12>, for more information about how Jetstress storage testing is performed.

## Create and configure mailbox databases

Mailbox databases are created by logging in to the Exchange admin center and navigating to servers and then databases. Click the New button to create a new mailbox database. A New Database Wizard appears in the browser window, as shown in [Figure 1-3](#). The Mailbox Database name you choose must be unique within the entire Exchange organization. Use a simple naming convention that is easy for you to use in PowerShell commands. You also need to choose which mailbox server to create the database on and specify the paths for the database and transaction log files. You can choose to mount the database immediately, or leave it dismounted after creation and manually mount it later.



**FIGURE 1-3** Creating a new mailbox database using the Exchange admin center

Mailbox databases can also be created by running the `New-MailboxDatabase` cmdlet.

[Click here to view code image](#)

```
#Creating a mailbox database in the Exchange management shell
```

```
[PS] C:\>New-MailboxDatabase -Name DB01 -Server NY-EXCH01 -EdbFilePath C:\ExchangeDatabases\DB01\DB01.db\DB01.edb -LogFolderPath C:\ExchangeDatabases\DB01\DB01.log
```

Name	Server	Recovery	Replication Type
DB01	NY-EXCH01	False	None

### Note: Restarting the Information Store for New Databases

When you create a new mailbox database, Exchange prompts you to restart the Information Store service on the server. The restart of the store service makes Exchange re-evaluate the memory allocations for each database instance, ensuring an equal distribution of available resources across all databases. Because a restart of the store service causes existing databases to dismount, you should schedule the task during a suitable outage window.

The maximum number of databases the server can host is determined by the edition of Exchange 2016 licensed for that server. There are two types of licensed editions, standard and enterprise. A standard edition Exchange 2016 license allows up to five mounted databases to be hosted on the server. An enterprise edition license allows up to 100 mounted databases per server. Microsoft defines a mounted database as “an active mailbox database that is mounted for use by clients, or a passive mailbox database that is mounted in recovery for log replication and replay”

([https://technet.microsoft.com/library/bb232170\(v=exchg.160\).aspx](https://technet.microsoft.com/library/bb232170(v=exchg.160).aspx)). A recovery database does not count as one of the mounted databases on the server. You can create more than five databases on a server, but only the maximum number of databases can be mounted at any given time. If you attempt to mount any more databases, the operation fails and an error message is logged in the Application event log on the server.

### Important: Where to Place Database and Log Files for New Databases

As you discovered earlier in this chapter, the decision as to whether database and log files should be separated on different volumes or co-located on the same volume depends on the number of database copies you plan to configure. Although each database starts with just one copy, you should only co-locate the database and log files on the same volume when you plan to add two or more additional copies of the database before it hosts any mailbox data.

After creating a new mailbox database, review the default configuration settings and make changes if needed. In the Exchange admin center, click the Edit button to open the database properties. Although the default values are suitable for many organizations, you have the option to configure the storage quota limits applied to mailboxes hosted on the database and the retention periods for deleted items and deleted mailboxes. You can

also configure the offline address book (OAB). If no offline address book is configured on a database, the mailboxes uses the default OAB for the organization. The database configuration can also be changed using the Set-MailboxDatabase cmdlet.

## Manage mailbox databases

A database must be mounted in order for it to be available to service user requests. When an Exchange 2016 mailbox server starts up, the Information Store service starts. The service mounts each mailbox database that has a MountAtStartup value of True and that was in a mounted state when the service last stopped. If a database was in a dismounted state when the service last stopped, the Information Store leaves the database dismounted at next startup whether the MountAtStartup attribute is set to True or False. This prevents the Information Store from automatically mounting a database that the administrator intended to leave dismounted. Administrators can mount databases by running the Mount-Database cmdlet and dismount databases with the Dismount-Database cmdlet.

You can also have the database files, log files, or both types of files for a mailbox database moved to new locations by running the Move-DatabasePath cmdlet. This process is often performed for the first mailbox database created on the server by Exchange setup. The first mailbox database is located in a sub-folder of the Exchange installation path, in C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\ by default. A sub-folder matching the database name is used to host both the database and log files. The first mailbox database is named “Mailbox Database” followed by 10 digits that are uniquely generated. As part of the process of moving a mailbox database to a new location, you can also rename the database to match your naming convention by running the Set-MailboxDatabase cmdlet, as shown in [Listing 1-4](#).

### LISTING 1-4 Renaming and moving a mailbox database

[Click here to view code image](#)

```
[PS] C:\>Set-MailboxDatabase "Mailbox Database 0135571303" -Name DB05
[PS] C:\>Move-DatabasePath -Identity DB05 -EdbFilePath
C:\ExchangeDatabases\DB05\DB05.
db\DB05.edb -LogFolderPath C:\ExchangeDatabases\DB05\DB05.log
Confirm
Are you sure you want to perform this action?
Moving database path "DB05".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"):
Y
Confirm
```

```
To perform the move operation, database "DB05" must be temporarily
dismounted, which
will make it inaccessible to all users. Do you want to continue?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [?] Help (default is "Y"):
Y
```

---

### **Important: Moving Mailbox Databases**

When a mailbox database hosting active mailboxes needs to be moved, the move process causes an outage for those mailbox users. The outage timeframe can last for a few hours, which is unacceptable for most businesses, if the mailbox database is very large. To avoid downtime, create a new mailbox database in the new location you want the database to be stored in, and then perform the mailbox move. Mailbox moves do not incur a lengthy outage for the users. Users can continue to use their mailboxes until the final cutover to the new database, which only requires a few minutes of interruption.

## **Configure transaction log properties**

Exchange 2016 uses a transactional database engine for mailbox databases. For each change or transaction that occurs within a mailbox database, information is written to the database's log stream. The log stream consists of a series of individual log files 1,024 KB in size each. In general, you can expect to see about 1 GB of log files written for each 1 GB of data that changes within the database. For example, if you move 50 GB of mailboxes to a database, approximately 50 GB of transaction logs are created.

The log stream is written until either a full or incremental backup of the database is successfully created, which then triggers log truncation. When log truncation occurs, any log files written leading up to the point in time the backup started are deleted from the disk. Taking regular backups of the databases prevents the size of the transaction log file data from growing indefinitely. Transaction log data would eventually fill all of the available disk space on the transaction log volume and cause the database to dismount unless you create a backup or use circular logging.

Circular logging is enabled or disabled for a mailbox database by running the Set-MailboxDatabase cmdlet to set the CircularLoggingEnabled attribute to a value of True or False. When circular logging is enabled, the log stream automatically truncates log files after the transactions are committed to the database. When circular logging is enabled, only a small number of transaction log files are visible on the transaction log volume. This prevents the transaction logs from consuming more than a few megabytes of disk space. The downside of this method is if the database experiences a failure, it can only be restored to the point in time of the last backup. This is because the full log

stream of transactions that occurred after the last backup is not available to roll forward in the database, preventing it from being recovered to the point in time the failure occurred. The exception to this is when circular logging is enabled for databases in a Database Availability Group that have more than one database copy.

## Summary

- Exchange 2016 mailbox servers do not require expensive, high speed disks. Exchange 2016 is supported on a wide range of storage configurations. You must carefully choose the storage to be used for storing Exchange data to ensure it provides the required performance, capacity, and resilience to failure.
- Placement of Exchange 2016 mailbox databases depends on whether a Database Availability Group is being deployed, and how many database copies are being configured.
- Modern public folders require additional considerations beyond those of other mailbox types to ensure the optimal placement of public folder data.
- Virtualization of Exchange 2016 mailbox servers is supported, but not all features of virtualization platforms are supported by Microsoft. Some virtualization vendors still support or recommend features that Microsoft does not. In deployment using third party platforms, customers need to make decisions about which of Microsoft's virtualization support guidelines they're prepared to deviate from based on the advice of the virtualization vendor. For exam scenarios, only the supported solution is the correct answer.
- Mailbox server storage should always be validated using Jetstress to ensure it meets the requirements of the scenario.

## Skill 1.2: Plan, deploy, and manage high availability solutions for mailbox databases

Mailbox databases that have a single copy hosted on one Exchange 2016 mailbox server are susceptible to downtime if any of the server infrastructure components fail. To reduce the risk of downtime due to single points of failure, mailbox databases can be made highly available by deploying a Database Availability Group (DAG). The DAG is the high availability model for Exchange 2016. An organization can have any number of DAGs deployed.

An Exchange 2016 DAG consists of up to 16 mailbox servers that are capable of replicating database copies between each member of the DAG. DAGs provide high availability by protecting the databases from software failures, corruption, failures of server infrastructure, and other dependencies within the datacenter. Each Exchange 2016 mailbox server can be a member of only one DAG. All members of the DAG must

be running Exchange 2016. You can't use different versions of Exchange within the same DAG. This means if you are migrating from an Exchange 2013 DAG, you need to create a new DAG for Exchange 2016. When the new Exchange 2016 DAG is created, you can configure new mailbox databases and migrate the mailboxes to the new DAG with mailbox move requests.

No special installations of Exchange 2016 or interruptions to existing mailbox database operations are required for a DAG to be created and for mailbox servers to be added as members. This is referred to as incremental deployment, which permits a single Exchange 2016 mailbox server to be scaled out to a 16 member DAG over time without the need to redeploy or drastically reconfigure anything.

An Exchange 2016 DAG is not a clustered application, but it does make use of an underlying Windows failover cluster. The failover cluster is automatically created and configured when you add the first member to the DAG. Failover clusters operate using the concept of quorum, which is a voting process by the members of the DAG to determine whether the resources of the DAG (the mailbox databases) should remain online. If a majority of votes cannot be obtained, quorum is not achieved and the DAG goes offline. To ensure that a majority of votes is possible, the DAG operates in one of two quorum modes:

- **Node Majority quorum mode** Used by DAGs with an odd number of members. Each member of the DAG is given a vote in the quorum voting process. Cluster quorum data is stored on the local disk of each DAG member.
- **Node and File Share Majority quorum mode** Used by DAGs with an even number of members. An additional server known as the File Share Witness (FSW) server is used as a tie-breaker in the quorum voting process.

When mailbox databases are made highly available in a Database Availability Group, the active database copy can switch over or failover between the DAG members that host a copy of the database. A switch over is an administrator-driven action involving a deliberate move of the active database copy to another DAG member. Switchovers can be targeted, meaning the administrator manually chooses a database copy to activate. Switchovers can also be targetless, meaning the administrator allows the DAG to select a database copy to activate. Failovers are automatic actions performed by the DAG in response to a failure. For example, the DAG activates another copy of any databases that go offline due to a server or disk failure.

Moving the active database copy to another DAG member does not involve moving the actual databases files. The database copies are kept in sync by the continuous replication process. Moving the active database copy involves dismounting the active copy and mounting one of the passive copies. The passive copy then becomes the active copy. This is also referred to as activating a database copy. The whole process can take

just a few seconds, and with Outlook clients operating in cached mode, the switchover or failover process usually occurs without any impact to the user.

Database Availability Groups require careful planning and configuration to ensure they meet the high availability requirements of the environment.

---

## This section covers how to:

- [Identity failure domains](#)
  - [Plan a solution that meets SLA requirements around scheduled downtime](#)
  - [Plan for software updates and server maintenance](#)
  - [Create, configure, and manage Database Availability Groups \(DAG\)](#)
  - [Create, configure, and manage DAG networks](#)
  - [Create and configure mailbox database copies](#)
  - [Create, configure, and manage Azure DAG members](#)
- 

## Identify failure domains

A failure domain is any component of your overall infrastructure or solution that has the potential to fail. Failure domains can be physical, such as server hardware components, or they can be logical, such as an application service or database. To deploy a high availability solution resilient to failures, you must identify all of the failure domains that exist in your environment and mitigate the risk of those failures with your solution design.

Mitigating failures is a balancing act of achieving the level of service availability that you require, without incurring an excessively large cost in doing so. It's possible to design a "gold plated" solution that protects from failures that are extremely unlikely to occur. It is also possible that some failure scenarios can be considered an acceptable risk by the organization.

To identity all of the possible failure domains in your environment, you need to consider all of the components that exist between the user and the Exchange servers, including network links, routers, and switches. You also need to consider the components in and around the servers themselves, such as processors, memory, power supplies, power feeds into server racks, and even the physical datacenter itself.

A core principle of Microsoft's Preferred Architecture for Exchange 2016 is to reduce complexity and increase predictability of failures. That principle seems to contradict the idea of mitigating the risk of individual failure domains. What the Preferred Architecture advises, however, is to address failure domains with a simple building block approach. This approach uses the DAG itself rather than increase

complexity by adding components such as teamed network interfaces or RAID-backed storage to the environment. In doing so you achieve a more predictable response to failures. For example, deploying a teamed network interface means installing special drivers and running additional network cables to separate switches connected to separate power feeds and datacenter networks. A greater number of variables exist in that solution when trying to predict how the server responds to network failures. That type of solution is much more complex than adding an additional database copy to another DAG member located in a different rack and connected to a different switch. No matter what type of network failure occurs, the response is always the same, the active database copy fails over to another DAG member.

## **Plan a solution that meets SLA requirements around scheduled downtime**

Unplanned failure is not the only reason to deploy a Database Availability Group. The Exchange 2016 environment needs to be designed to be able to meet the availability requirements of the organization for failure scenarios and for planned downtime.

Scheduled maintenance of servers, network infrastructures, and datacenters is a normal part of IT operations and should occur as often as monthly in order to keep up with the security updates Microsoft releases each month. Regular maintenance such as updating firmware in servers, replacing end of life networking equipment, or power testing in the datacenter must also occur.

You can design a solution to meet a specific target if a service level agreement (SLA) is in place for the environment. For example, if the SLA requires 99 percent availability for email services, that only allows for 43.8 minutes of downtime per month. A single patching cycle can easily take up that much time, leaving no room for other maintenance tasks or unplanned outages.

As an alternative example, assume the SLA allows for 2 hours of scheduled downtime in a calendar month and the datacenter operators are planning a 4-hour power outage to conduct repairs. You cannot meet the SLA obligations without being able to switch over your Database Availability Group databases to a secondary datacenter.

As you can see, a clear SLA is important when considering an Exchange 2016 solution. Designing a solution that provides an arbitrary level of availability is neither cost effective nor is it guaranteed to satisfy the requirements of the organization.

## **Plan for software updates and server maintenance**

Regular maintenance of Exchange servers is to be expected. Windows operating systems need security updates and other bug fixes on a monthly basis, and new firmware updates are released often for server hardware to resolve performance and stability issues.

A Database Availability Group allows Exchange administrators to maintain service availability while maintenance is being performed on individual DAG members. Consider the scenario of monthly security patches being released by Microsoft for the Windows operating system. By switching the active database copies within a DAG away from one DAG member, that member can be taken out of operation temporarily for patching without any interruption to users. When the patching is complete, the member is put back into operation for the DAG. This process is repeated until all DAG members have received that month's security patches. The same concepts apply when installing cumulative updates for Exchange 2016 or for any maintenance activity on the server hardware.

Performing this type of maintenance on a DAG member involves putting the server into what is known as maintenance mode. Maintenance mode effectively means that the server is considered non-operational by other Exchange servers in the environment. While a server is in maintenance mode, database copies do not try to activate on that server, nor do other servers try to route email messages to the server. This is achieved by setting server component states to an offline status on the server.

There are several steps required to place a DAG member into maintenance mode. To begin, the HubTransport server component needs to be emptied of any email messages currently queued for delivery, as shown in [Listing 1-5](#). Setting the server component to a draining state prevents new email messages from being added to the queue, but some email messages already in the queue might be stuck there waiting for the destination server to become available. These messages can be redirected to another mailbox server in the organization so that the other server can continue to retry delivery.

## LISTING 1-5 Draining transport queues in preparation for server maintenance

[Click here to view code image](#)

---

```
[PS] C:\>Set-ServerComponentState NY-EXCH01 -Component HubTransport -State Draining  
-Requester Maintenance  
[PS] C:\>Redirect-Message -Server NY-EXCH01 -Target EX2016SRV2.exchangeservername.net
```

---

Because DAG members are also members of the underlying Windows failover cluster, the cluster needs to be made aware of the server status so that it does not try to take any corrective action while you are performing maintenance. You can achieve this by suspending the cluster node.

[Click here to view code image](#)

```
#Suspending a cluster node for maintenance
```

```
[PS] C:\>Suspend-ClusterNode -Name NY-EXCH01
```

During the maintenance period, the DAG needs to be prevented from trying to activate any of the database copies on the server where maintenance is being performed. To prevent this, you can configure two properties of the DAG member. The first is the DatabaseCopyActivationDisabledAndMoveNow attribute, which should be set to True during the maintenance period. This attribute doesn't prevent database copies from activating on the server, but it does automatically move any active database copies to other DAG members as long as another healthy database copy can be located for activation. You can consider this option to be a soft approach to preventing database copy activation on the server.

[Click here to view code image](#)

```
#Setting the DatabaseCopyActivationDisabledAndMoveNow attribute
```

```
[PS] C:\>Set-MailboxServer -Identity NY-EXCH01 -  
DatabaseCopyActivationDisabledAndMoveNow  
$true
```

The second property allows each DAG member to be configured with an automatic activation policy for database copies hosted on that server. This is controlled using the DatabaseAutoActivationPolicy attribute, which has three possible settings:

- **Unrestricted** The DAG member is not prevented from activating its database copies.
- **IntrasiteOnly** The DAG member can only activate its database copies if they are failing over from another DAG member located within the same Active Directory site.
- **Blocked** The DAG member is prevented from automatically activating its database copies, but you can still manually activate the database copies if necessary.

During the maintenance period the DatabaseAutoActivationPolicy should be set to blocked. But first, use Get-MailboxServer to determine the current setting, so that you can return the server's configuration to that setting again at the end of the maintenance period.

[Click here to view code image](#)

```
#Setting the database auto activation policy
```

```
[PS] C:\>Set-MailboxServer -Identity NY-EXCH01 -  
DatabaseAutoActivationPolicy Blocked
```

Performing these two steps should result in no active database copies being hosted by the DAG member. Even so, it is always possible that some other health condition within

the DAG is preventing the database copies from switching over to another DAG member. Always check that the server you're about to perform maintenance on has no active database copies before you proceed any further. The following command should return no results if there are no active database copies on the server.

[Click here to view code image](#)

```
#Checking for active database copies on the server
```

```
[PS] C:\> Get-MailboxDatabaseCopyStatus -Server NY-EXCH01 | Where  
{$_.Status -eq  
"Mounted"}
```

When all of the preparation steps have been completed and there are no active database copies on the server, you can finally place all server components on the DAG member to an inactive state. An inactive state takes the server completely out of operation for the organization.

[Click here to view code image](#)

```
#Taking server components offline for maintenance
```

```
[PS] C:\> Set-ServerComponentState NY-EXCH01 -Component ServerWideOffline  
-State  
InActive -Requester Maintenance
```

### Important: Maintaining Service Availability During Maintenance

There's more to service availability than just the mailbox databases. The client access and transport services are also critical to the continued function of the Exchange environment while you are performing maintenance on a server. As such, it's important to have a suitable load-balancing solution in place for client traffic and to have multiple connectors configured so that mail flow can continue to function.

At the end of your planned maintenance, the DAG member can be placed back into operation by running commands in the reverse order that they were used to put the server into maintenance mode, as shown in [Listing 1-6](#).

### LISTING 1-6 Taking a DAG member out of maintenance mode

[Click here to view code image](#)

```
[PS] C:\>Set-ServerComponentState NY-EXCH01 -Component ServerWideOffline -  
State Active  
-Requester Maintenance  
[PS] C:\>Resume-ClusterNode -Name NY-EXCH01
```

```
[PS] C:\>Set-MailboxServer NY-EXCH01 -DatabaseCopyAutoActivationPolicy  
Unrestricted  
[PS] C:\>Set-MailboxServer NY-EXCH01 -  
DatabaseCopyActivationDisabledAndMoveNow $false  
[PS] C:\>Set-ServerComponentState NY-EXCH01 -Component HubTransport -State  
Active -  
Requester Maintenance
```

---

Database Availability Groups fit rather neatly into the change management processes of most organizations. A key principle of the change management process is risk management. In a perfect world all changes that are planned for an Exchange 2016 environment are thoroughly tested within a separate test environment configured to match the production environment. In reality, many organizations simply do not have the resources to provide such a test environment for their Exchange administrators to use.

Fortunately, DAGs are able to help an organization manage risk by using their high availability features to maintain service availability while changes are rolled out. Take the example of the Windows security patches that Microsoft releases a monthly basis. In a single-server Exchange environment, the security patches can be deployed to other Windows servers in the environment first. Without a dedicated test environment however, there's no way to be sure that the patches do not pose a significant impact on the Exchange 2016 server application itself until you install them on the Exchange server. At that point, any problem that does occur is a production impacting issue. A further service disruption is required to uninstall the security patches and return the server to its previous state if the problem can't be remediated and a roll back is needed. A similar risk exists for installing Exchange 2016 cumulative updates. If for some reason the update process fails, you're left with a non-functioning server and a service disruption for your users while you resolve the problem.

In comparison, the nature of DAGs allows changes to be deployed to a single DAG member initially, enabling any impacts to be assessed before rolling the same changes out to the remaining DAG members. If an issue occurs with an update, there is no service disruption because the active database copies can continue to be hosted by a healthy DAG member while you resolve the issues with the unhealthy DAG member.

Given the DAG's capability to avoid service disruptions when changes are being made, it's sensible to incorporate those capabilities into any change management plans for your organization.

## Create, configure, and manage Database Availability Groups (DAG)

A new Database Availability Group has no members when it is first created. A DAG can have one member or as many as 16 members. In order for a mailbox database to be considered highly available, it needs at least two copies. This means that any DAG consisting of fewer than two members is not considered a high availability solution.

To prepare for creating a DAG, install the Exchange 2016 mailbox server role onto multiple servers with the same hardware specifications, including the same storage layouts and sizing. In order for a database copy to replicate to another DAG member, both DAG members must have the same storage paths available on them. For example, assume a database on one DAG member is stored in the E:\DB01 folder. The same E:\DB01 folder must exist for all DAG members who are hosting a copy of that database.

Prior to Exchange 2013 SP1 it was required to pre-stage a Cluster Network Object (CNO) before creating a DAG. The CNO is a computer account in Active Directory that is manually created and disabled, and is then associated in DNS with the cluster administrative access point (CAAP) IP address. In effect this allows other management tools and applications to connect to the underlying Windows failover cluster, and the DAG itself, for integration tasks such as performing DAG-aware backups. The CNO and CAAP are no longer required with Exchange 2016, and in fact an Exchange 2016 is created without a CNO and associated IP address by default. This simplifies administration and removes one potential failure domain by no longer needing to allocate and manage an IP address for the DAG.

---

#### Note: Why Did Microsoft Remove the Requirement for a DAG IP Address?

The motivation to adopt IP-less clusters for Exchange DAGs came from Microsoft's experience running Exchange Online in Office 365. By changing to completely IP-less DAGs in Exchange Online, Microsoft support and engineering teams eliminated all of the issues caused by problems such as IP address conflicts for the DAG IPs. Unless you have a specific requirement to deploy a DAG with an IP address, such as a backup product that doesn't support IP-less DAGs, then you should adopt the principle of least complexity by accepting the default configuration of an IP-less DAG.

---

To create the new DAG using the Exchange management shell you can run the New-DatabaseAvailabilityGroup cmdlet. Each DAG must be given a unique name. You also need to provide the name of a server to assign as the File Share Witness server. The File Share Witness can be another Exchange server that is not going to be a member of the DAG, or it can be a non-Exchange server. The DAG filesystem also needs to be configured if you have used ReFS for the volumes on your Exchange servers. This configuration ensures that the auto reseed workflow knows which file system to reformat volumes with when it is performing its recovery workflow.

[Click here to view code image](#)

```
#Creating a new database availability group
```

```
[PS] C:\>New-DatabaseAvailabilityGroup -Name DAG01 -WitnessServer NY-  
DC01.contoso.com  
-FileSystem ReFS
```

---



### Exam Tip

Using any current version of Windows Server as the File Share Witness server is supported, which at this time means Windows Server 2008 R2 or later. This also includes using a domain controller for the File Share Witness, although that is not recommended for security reasons. The domain controller method would require adding the Exchange Trusted Subsystem group as a member of the Administrators group for the entire Active Directory domain. It is not supported to use a Windows client operating system, or any non-Windows file share such as a Linux SAMBA file share, as the File Share Witness.

---

A newly created DAG does not have any members yet. When you add the first DAG member, Exchange automatically installs the Windows failover clustering components on the server, creates the underlying cluster, and configures the File Share Witness. You can add a single mailbox server to the DAG initially, or you can choose to add multiple mailbox servers at one time.

[Click here to view code image](#)

```
#Adding an Exchange 2016 server as a DAG member
```

```
[PS] C:\>Add-DatabaseAvailabilityGroupServer -Identity DAG01 -  
MailboxServer NY-EXCH01
```

To add more Exchange 2016 mailbox servers to the DAG use the Add-DatabaseAvailabilityGroup cmdlet again. After adding a new member to the DAG, you can view the current status of the DAG member servers by running the Get-DatabaseAvailabilityGroup cmdlet with the -Status switch. Next, pipe the output to Format-List so you can view all of the properties of the DAG. The WitnessServer and WitnessDirectory attributes show you where the File Share Witness is located.

[Click here to view code image](#)

```
#Command to view all properties of a DAG
```

```
[PS] C:\>Get-DatabaseAvailabilityGroup -Identity DAG01 -Status | Format-  
List
```

## Create, configure, and manage DAG networks

When mailbox servers are added as members of an Exchange 2016 Database Availability Group, a DAG network is automatically configured for each IP subnet that any DAG member has a network interface connected to, as shown in [Figure 1-4](#). DAG members require at least one network interface, and for a DAG with both members located on the same IP subnet, a single DAG network is configured. This network is automatically configured for client MAPI traffic, as well as for database replication traffic between DAG members.

The screenshot shows the Exchange admin center interface. The top navigation bar includes links for Enterprise, Office 365, and Administrator. The main title is "Exchange admin center". Below the title, there's a breadcrumb trail: recipients > servers > databases > **database availability groups** (which is highlighted). On the left sidebar, under the "servers" category, the "Database Availability Groups" link is also highlighted. The main content area displays a table for managing Database Availability Groups. The table has columns: NAME, WITNESS SERVER, and MEMBER SERVERS. A single row is selected, showing DAG01 as the name, ny-dc01.contoso.com as the witness server, and SF-EXCH01, SF-EXCH02, NY-EXCH02, NY-EXCH01 as member servers. To the right of the table, detailed information is provided for DAG01:

- DAG01
- Member Servers:
  - SF-EXCH01
  - SF-EXCH02
  - NY-EXCH02
  - NY-EXCH01
- Witness Server:
  - ny-dc01.contoso.com
- DAG Network:
  - MapiDagNetwork

At the bottom of the table area, it says "1 selected of 1 total".

**FIGURE 1-4** A Database Availability Group with auto-configured DAG network

In previous versions of Exchange, it was recommended to configure multiple DAG networks so that dedicated replication networks could be used. This recommendation has changed because datacenter networking is typically a lot faster now than it was in the Exchange 2010 era. Gigabit and 10-gigabit networks are common in modern datacenters and are capable of handling the database replication traffic for most DAG deployments. The current recommendation is to use a single DAG network for both MAPI and replication traffic, which is the least complex approach and therefore the simplest to configure and support. Additional network interfaces and DAG networks

can be considered when very high volumes of database replication traffic occur. Another scenario where you can consider using multiple DAG networks is when multiple redundant networks paths exist between DAG members, for example, across a WAN with multiple paths. In this situation, replication traffic would not compete for WAN bandwidth with other network traffic. If two datacenters communicate across a single WAN link however, there is nothing to gain from configuring multiple DAG networks.

### Note: Do Multiple Networks Help with DAG Resiliency?

When multiple DAG networks exist, the failure behavior for the DAG depends on which network is experiencing an issue. If a dedicated replication network fails, the DAG continues replicating over the MAPI network. If the MAPI network fails, however, the DAG member is considered to be offline and active database copies on that DAG member failover to other healthy DAG members. This inconsistent response to failure is one of the reasons why a simpler, single network approach is recommended.

The Database Availability Group automatically configures DAG networks based on the properties of the network interfaces. The MAPI network interface for each DAG member must be configured with:

- A static IP address
- A default gateway
- At least one DNS server
- An enabled “Register this connection’s address in DNS” checkbox

Any network interfaces intended for use on a replication network must be configured with:

- A static IP address
- No default gateway
- No DNS servers
- A disabled “Register this connection’s address in DNS” checkbox
- Static routes, if the network spans multiple subnets

The DAG network auto-configuration risks potential failure if those conditions are not met. You can also expect to see misconfigured subnets listed in the output of Get-DatabaseAvailabilityGroupNetwork if the conditions aren’t met. To resolve the misconfigured subnets, revisit the network interface configurations and adjust them to align with the requirements previously mentioned. After correcting the network interface

configurations, run the Set-DatabaseAvailabilityGroup cmdlet with the ManualDagNetworkConfiguration parameter, setting the value to True.

[Click here to view code image](#)

```
#Command to enable manual DAG network configuration

[PS] C:\>Set-DatabaseAvailabilityGroup -Identity DAG01 -
ManualDagNetworkConfiguration
$true
```

The DAG reassesses the network interface configuration and, assuming you have configured them correctly, adjusts the DAG networks. After the adjustments, the misconfigured subnets no longer appear. You can set the DAG back to using network auto-configuration if the issue has been resolved.

[Click here to view code image](#)

```
#Command to enable automatic DAG network configuration

[PS] C:\>Set-DatabaseAvailabilityGroup -Identity DAG01 -
ManualDagNetworkConfiguration
$false
```

Even when you don't plan to configure more than one DAG network, it's common for modern server hardware to ship with multiple network interfaces. Windows can detect and automatically configure these new network interfaces. When Exchange 2016 DAG members have other network interfaces that should not be used for any DAG networking functionality, such as dedicated backup networks, management ports, or iSCSI storage networks, those network interfaces should be disabled from use by the DAG. You can disable those interfaces by configuring the DAG to ignore them.

[Click here to view code image](#)

```
#Command to ignore a DAG network

[PS] C:\>Set-DatabaseAvailabilityGroupNetwork
"DAG01\ReplicationDagNetwork01"
-IgnoreNetwork $true
```

### **Note: Naming Database Availability Group Networks**

Exchange 2016 automatically names the DAG networks that it creates with names such as “MAPIDagNetwork” and “ReplicationDagNetwork01.” The DAG network names have no impact on their functionality, nor are they seen by your users. In that sense, the names are not particularly important. From an administrative simplicity point of view, however, renaming networks can make their purposes clearer, especially networks configured to be ignored by the DAG. You can use the Set-DatabaseAvailabilityGroup cmdlet with the Name parameter to rename a DAG network.

## **Create, configure, and manage proper placement of a File Share Witness (FSW)**

When you are deploying a Database Availability Group, an important part of the solution design is the File Share Witness server. All DAGs have a witness server and witness share defined, but only DAGs with an even number of members operate in Node and File Share Majority quorum mode. These modes allow the DAG to utilize the witness server during any situation in which quorum voting needs to occur. For example, a two-member DAG needs one of the members to be taken offline for server hardware maintenance. With only one out of two DAG members still online (50 percent of the total DAG membership), a majority cannot be formed based on the existing DAG members online. The witness server is therefore used as a tie-breaker, providing an additional vote for the online DAG members so that it can maintain quorum and keep the DAG resources online.

The File Share Witness is important to the quorum voting process, but is otherwise not required to be online during regular DAG operations. This means it is possible for administrators to perform maintenance on the witness server when necessary, as long as quorum is still maintained by having a majority of DAG members online. The witness server is also not required to be highly resilient. It might seem like a good idea to cluster the witness share, or protect it by configuring a Distributed File Share (DFS), but those solutions only add more complexity to the environment. More complexity creates less predictable failure behaviors and complicates troubleshooting.

Although the DAG member can be another Exchange server, it can't be an Exchange server that is also a member of the same DAG. The same server can be the witness server for multiple DAGs, so if you have an environment with multiple DAGs, you do not necessarily need to deploy multiple witness servers. Each DAG, however, does need its own witness directory that is separate from the others. When you allow the New-DatabaseAvailabilityGroup cmdlet to automatically name the witness directory for you, it names the directory according to the DAG name, therefore providing a unique

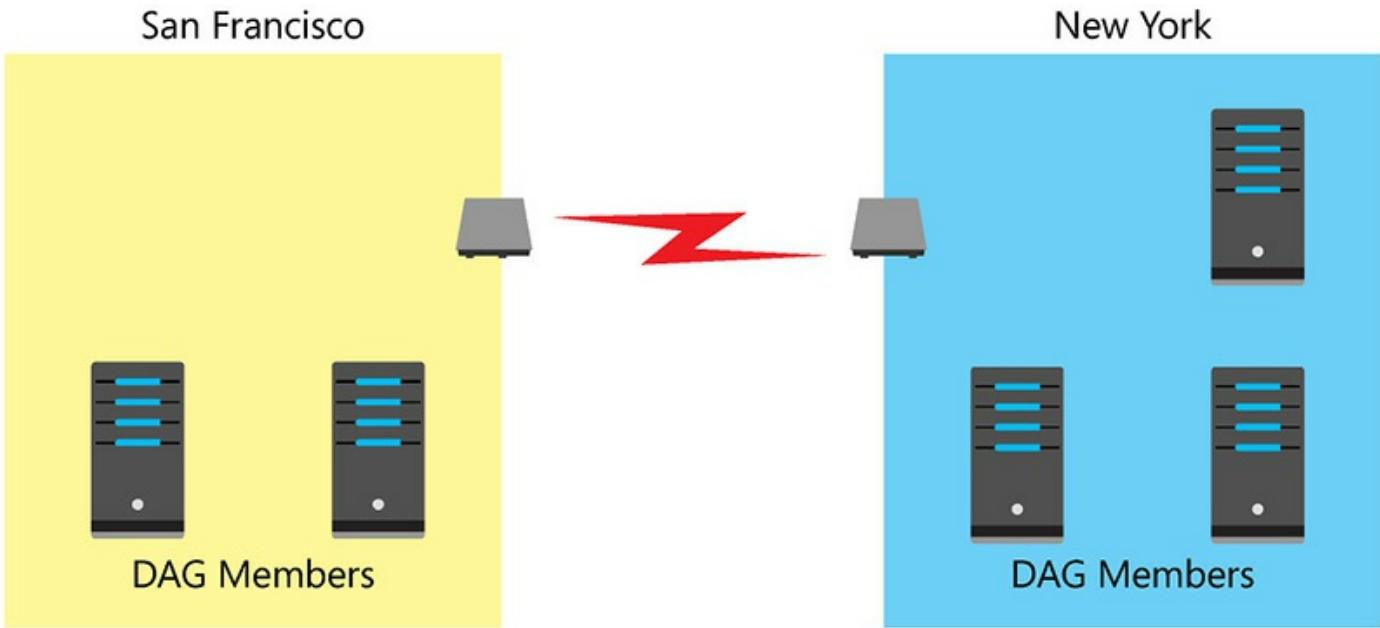
witness directory name for each DAG.

### **Important: Using Domain Controllers as File Share Witness Servers**

Microsoft supports the use of a domain controller as a File Share Witness, however, they do not recommend it. One of the requirements for the File Share Witness is that the Exchange Trusted Subsystem group in Active Directory must have local administrator rights on the witness server. Because domain controllers have no local administrator group, it is necessary to add Exchange Trusted Subsystem to the domain Administrator group. This is a significant elevation of privileges for the Exchange server computer accounts, which raises security concerns if one of the servers becomes compromised by an attacker. When possible, do not use domain controllers as witness servers.

Considering the critical role that the witness plays in the quorum voting process, give careful consideration to the location of the witness server. For DAGs hosted within a single datacenter, you should keep the failure domains in your datacenter in mind. Place the File Share Witness server where a single failure is unlikely to isolate both the DAG members and the witness server from each other at the same time. Quorum cannot be maintained if both DAG members are unable to connect to each other and are also unable to connect to the witness server.

For DAGs that span multiple datacenters, the File Share Witness server should be located in the datacenter that you consider the primary site. In other words, if a WAN failure occurred, consider which of the two datacenters would you prefer be able to maintain. Also consider which DAG resources you want to remain online. The datacenter you choose would be the primary site where you should place the File Share Witness server. As shown in [Figure 1-5](#), The New York datacenter is the primary site.



**FIGURE 1-5** Placing the file share witness in the primary datacenter

Another potential location to place the File Share Witness is a third datacenter location, which is supported for Exchange 2016 DAGs. The requirement in this scenario is that each of the datacenter locations has independent network connectivity to the other two datacenters. This placement ensures that the failure of a single WAN connection does not isolate multiple datacenters at the same time. Using a third datacenter location for the File Share Witness permits automatic site failover to occur when either the primary or secondary datacenter fails. Quorum can still be maintained when either of the datacenters hosting DAG members goes offline. Without the FSW in a third site, the loss of the primary datacenter causes a loss of quorum which also causes the entire DAG to go offline. In the event of such a disaster, manual administrator intervention is required to perform a datacenter switchover to the secondary datacenter.



### Exam Tip

Automatic site failovers is an attractive sounding capability, but it comes at a cost. A third datacenter is required to host the File Share Witness, as well as additional WAN connectivity to ensure that no single network connection can result in a loss of quorum. This means that it might not be the most cost effective solution for an organization. The most cost effective solution is not to deploy a third datacenter and supporting network infrastructure solely to host the FSW if the SLA allows for the time required to perform a manual datacenter switchover.

---

When a third datacenter is not available for use as a File Share Witness location, but

the organization would still like to have their witness server in a third site, a supported option is to host the witness share on a virtual machine running in Microsoft Azure. Independent network connectivity between all of the sites is still required. This configuration is made possible thanks to Microsoft adding multi-site VPN support to Azure, so that multiple datacenters can connect to the same Azure virtual network. Don't be confused by the existence of an Azure service called Azure Cloud Witness. This service can't be used as a witness server for an Exchange 2016 DAG. Instead, you must use an Azure virtual machine running a Windows Server operating system. This also means that the Azure virtual network must contain at least one domain controller, so at least two Azure VMs are necessary if you are using this configuration. As mentioned earlier in this section, it is not recommended to use a domain controller as a witness server even though it is supported.

#### Need More Review? Placing a File Share Witness in Microsoft Azure

You can find more information about using a Microsoft Azure VM as an Exchange 2016 DAG witness server on TechNet at  
[https://technet.microsoft.com/library/dn903504\(v=exchg.160\).aspx](https://technet.microsoft.com/library/dn903504(v=exchg.160).aspx).

## Create and configure mailbox database copies

When an Exchange 2016 mailbox server is added to a Database Availability Group, each of the mailbox databases hosted by that mailbox server become databases in the DAG. The databases however still only have a single database copy within the DAG. In order for the databases to be made highly available, they need database copies added to other DAG members.

Each of the DAG members hosting a copy of a given mailbox database must have the exact same storage paths available on it. You should configure each of your DAG members with the same storage layout to permit them to host copies of each database.

To add a copy of a mailbox database to another DAG member, use the Add-MailboxDatabaseCopy cmdlet, and specify the name of the mailbox server you want to host the new database copy. When the database is added, a process called seeding is initiated which copies the database and transaction log files from the active database copy to the server hosting the new copy.

[Click here to view code image](#)

```
#Adding a new database copy to another DAG member
```

```
[PS] C:\> [PS] C:\>Add-MailboxDatabaseCopy -Identity DB01 -MailboxServer NY-EXCH02
```

The automatic seeding process is usually fine, but in some scenarios you might prefer

to delay the seeding of a database to a different time, such as a weekend. Delay the process if you think initial seeding traffic might cause a network bandwidth problem. In such a scenario, use the `-SeedingPostponed` parameter with a value of `$True` when running the `Add-MailboxDatabaseCopy` cmdlet.

When you add a new database copy, the new copy is assigned an Activation Preference (AP) number. You can view the AP value for the copies of a database by running the `Get-MailboxDatabaseCopyStatus` cmdlet.

[Click here to view code image](#)

#### #Viewing the mailbox database copy status

```
[PS] C:\>Get-MailboxDatabaseCopyStatus DB01 | Select  
Name, Status, ActivationPreference, Co  
pyQueueLength  
Name           Status ActivationPreference CopyQueueLength  
----  
DB01\NY-EXCH01 Mounted                      1              0  
DB01\NY-EXCH02 Healthy                     2              0
```

#### Note: The Active Database Copy

The active database copy is the one that has a status of Mounted. Passive database copies that have a status of Healthy are in good working order and if their copy queue length is low, they can generally be considered to be replicating successfully.

The initial database is given an AP of 1, and the first copy of a database is automatically given an AP of 2, and so on. Up to 16 total database copies can exist, including 1 active copy and up to 15 passive copies. The AP number is an administrator assigned preference for which database copy should be the preferred target of a target-less switchover or failover. Both of these processes occur without the administrator choosing a database copy to activate. AP numbers are automatically assigned, but can be adjusted by the administrator if necessary. You can modify the Activation Preference for a database copy by running the `Set-Mailbox-DatabaseCopy` cmdlet.

[Click here to view code image](#)

#### #Configuring the Activation Preference for a mailbox database copy

```
[PS] C:\>Set-MailboxDatabaseCopy -Identity DB02\NY-EXCH02 -  
ActivationPreference 1
```

## Create, configure, and manage Azure DAG members

As organizations move to a cloud-first model, and in particular the infrastructure-as-a-service (IaaS) approach, it's natural to consider placing one or more of the members of a Database Availability Group in Microsoft Azure. Hosting Exchange 2016 servers, including DAG members, in Azure is a supported solution, however there are some specific requirements that must be met. Hosting Exchange servers in a cloud service provider raises a few technical issues as well.

IaaS is commonly used to provision applications in an elastic model where capacity expands and shrinks according to the demand on the workload at the time. A web application can scale out to multiple, load-balanced front end servers during peak usage, and then scale in to just one or two servers during off-peak times. This approach simply does not work for Exchange 2016 mailbox servers. Instead, you must provision virtual machines in Azure that meet the sizing requirements calculated using the Exchange Server Role Requirements Calculator. As previously mentioned, Exchange does not work with dynamic memory in virtual machines, so the full server specification of resources needs to be permanently allocated and available at all times.

Storage requirements are another area of concern when running Exchange 2016 on Azure. Typical IaaS workloads can take advantage of lower tiers of storage because the performance demands are not very high and the applications can be architected to scale in and out when necessary to meet performance requirements. Exchange 2016 VMs in Azure are required to use Azure Premium Storage to ensure there are no storage performance and contention issues. This might seem to contradict the idea that Exchange 2016 has lower IOPS requirements than previous versions of Exchange, and can run on less expensive, lower speed hard disks. While this is true, there is a difference between the enterprise-grade SATA disks you would install in your Exchange 2016 mailbox servers on-premises, which would be dedicated to the task of running Exchange workloads, and those used in Azure. The underlying storage in Azure is shared across multiple customers and workloads, so a consistent level of IOPS is not able to be guaranteed. Azure Premium Storage uses solid state drives (SSDs), and is designed for consistent high performance and low latency, which is necessary to run workloads such as Exchange mailbox databases.

The performance of the VM and its attached storage in Azure is just one part of the solution though. Connecting the Azure virtual network to your on-premises environment is also necessary. Each member of an Exchange 2016 DAG must have route trip network latency of no more than 500 milliseconds. A slower network has a detrimental effect on the replication of data between active and passive database copies. Latency is just one metric to be conscious of. The network also needs to have sufficient bandwidth to handle day to day replication, full database copy reseeds when necessary, and client traffic if there are times when active database copies failover to the DAG members.

hosted in Azure.

Network connectivity from the Azure VMs to the Internet must also be taken into account. The IP address space used by Azure VMs is not suitable for running a mail service. Other email servers on the Internet are highly likely to block any SMTP connections coming from that IP address space. As such, it is necessary to route email through a smart host or cloud service, such as Exchange Online Protection.

## Summary

- Planning a Database Availability Group that meets an organization's service availability requirements involves identifying the failure domains in the environment, understanding the service level agreement (SLA) in place for Exchange services, and then designing a DAG that is resilient to the identified failures in order to meet those availability requirements.
- Deploying a DAG involves creating the DAG, adding DAG members, configuring DAG networks, and then configuring database copies within the DAG.
- The placement of the File Share Witness server is critical to ensuring that quorum can be maintained under a variety of possible failure conditions. The DAG has not been adequately designed for the environment if a single failure can cause quorum to be lost.
- Mailbox database copies are added to DAG members to make the databases highly available. Administrators can specify their preferred order of activation during a failover situation by configuring the Activation Preference on each database copy, however Active Manager still makes its own decision about which database copy is the best one to activate.

## Skill 1.3: Plan, deploy, and manage a site-resilient Database Availability Group (DAG)

Site resilience involves extending a highly available Exchange 2016 Database Availability Group across multiple physical datacenter locations. The purpose of site resilience is to be able to maintain service availability when there is a complete datacenter outage.

Stretching a DAG across multiple sites requires further design consideration than a DAG located within a single datacenter. First, it's important to ensure that round trip network latency between DAG members is no greater than 500 milliseconds. Network bandwidth must also be adequate to support database replication and client traffic loads as well.

When using multiple datacenters, it is recommended to configure each datacenter as a separate Active Directory Site. This requires that the IP subnets in each datacenter are

different. Stretching an IP subnet across two datacenters makes both locations part of the same Active Directory Site, which makes it impossible for Exchange to make site-aware decisions. One of the important site-aware decisions that Exchange makes is the use of shadow redundancy to store copies of messages currently in transit on multiple mailbox servers in different sites. Similarly, Safety Net and Shadow Safety Net ensure that copies of messages that have been successfully delivered to mailboxes are kept on at least one mailbox server in each site. In doing so, the Exchange 2016 DAG ensures that if a complete site failure occurs requiring messages to be recovered from shadow redundancy or Safety Net, that both copies of the messages are not lost in the single datacenter outage.

By default, an Exchange 2016 DAG is also configured by default to compress replication traffic between DAG members located in different IP subnets. If the DAG spans multiple sites but uses a stretched IP subnet, the DAG can be reconfigured to compress all replication traffic so that the cross-site network traffic received the performance benefits of compression.

---

### This section covers how to:

- [Plan, create, and configure cross-site DAG configuration](#)
  - [Plan, deploy, and configure Datacenter Activation Coordination \(DAC\)](#)
  - [Configure and manage proper placement of an alternate File Share Witness \(FSW\)](#)
  - [Test and perform site recovery](#)
- 

## Plan, create, and configure cross-site DAG configuration

As described earlier in this chapter, quorum is the voting process used to determine whether to keep the Exchange 2016 DAG online when a failure occurs. In a single datacenter there are two possible outcomes, the DAG stays online or it goes offline. When you add site resiliency to the equation, there's an additional consideration of which datacenter the DAG should fail over to, or remain online in when a failure occurs.

Consider an organization that has mailbox users located in San Francisco and New York. To achieve site resiliency, the organization has configured a four-member DAG across the two datacenters with two members in San Francisco and two in New York. Active database copies for San Francisco mailboxes are located on San Francisco DAG members, and vice versa for New York mailbox users. This topology is referred to as an Active-Active DAG.

When the WAN connection between the two locations experiences an outage, quorum

can only be maintained in the datacenter that hosts the File Share Witness. In this case, that datacenter is New York. The San Francisco mailbox users are now unable to connect to their mailboxes because the WAN connection between the two sites is offline, even though the San Francisco datacenter is still online. In effect, only half of the organization has benefited from site resiliency with this design. In order to provide site resiliency to both groups of mailbox users, two Database Availability Groups must be deployed. Each DAG is configured with a File Share Witness located in the datacenter where quorum should be maintained during a WAN outage. This topology is referred to as an Active-Passive DAG and is shown in [Figure 1-6](#).

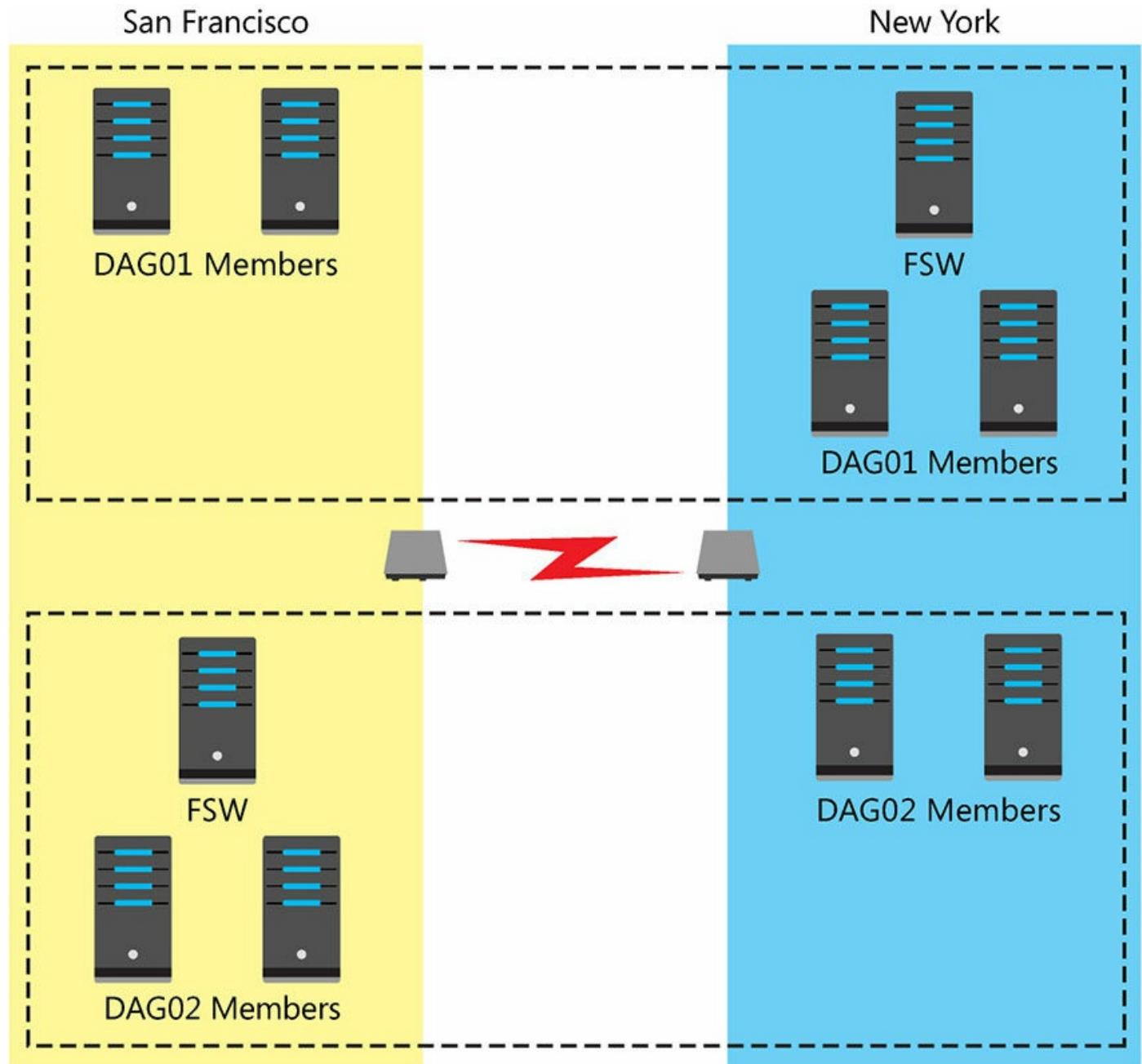


FIGURE 1-6 Two Active-Passive DAGs deployed across two datacenters

The examples provided apply to organizations that have wide geographic coverage. Some organizations only need a secondary datacenter in the event that their primary datacenter experiences a failure. The organization can then invoke their disaster recovery processes and perform a manual datacenter switchover to the secondary datacenter, bringing the DAG online until the primary datacenter becomes available again. In this scenario, the File Share Witness is located in the primary datacenter. Either an Active-Active DAG, which is able to run out of either datacenter at any time, or an Active-Passive DAG which only runs out of the secondary datacenter during a disaster, would be suitable for the organization.

As long as you have not enabled manual DAG network configuration when the first DAG member in a separate site is added to the existing DAG, the DAG networks are automatically reconfigured to include the additional IP subnets for the new DAG member locations. DAG network auto-configuration collapses the subnets into a single network. For example, the IP subnets for MAPI interfaces are collapsed into a single MAPI DAG network. This ensures the DAG understands which IP subnets and network interfaces for the DAG are related to each other. An example scenario would be to ensure the DAG knows that members should not attempt to connect from their MAPI network interface to the replication network interface of another DAG member. When you run Get-DatabaseAvailabilityGroupNetwork, you might notice multiple DAG networks configured for IP subnets that should be collapsed into a single network. In this instance, DAG network auto-configuration was not able to determine which network interfaces should belong in the same DAG network. The most likely cause of this issue is a misconfiguration on the network interfaces themselves. Refer to the DAG network planning section for the details on how each network interface should be configured.

## **Plan, deploy, and configure Datacenter Activation Coordination (DAC)**

Datacenter Activation Coordination (DAC) Mode is a property of Database Availability Groups designed to prevent split brain conditions from occurring. A split brain is a condition in which two different copies of the same database are active at the same time, for instance on two different DAG members in different datacenters. If such a condition were to occur, the result would be divergence of the data within the two copies of the database, which is a catastrophic outcome.

A split brain condition is actually a greater risk than you might think at first, especially in multi-site DAGs. Consider a scenario in which a power outage has taken the primary datacenter offline. The organization makes the decision to perform a manual datacenter switchover, bringing the DAG online and activating the database copies in the secondary datacenter. When power is restored to the primary datacenter, it's

determined that the power fault shorted out the WAN router. The WAN connectivity remains offline, but the servers in the primary datacenter are able to power on. Because the primary datacenter hosts the File Share Witness, the DAG members in the primary datacenter are able to achieve quorum and bring the DAG online, activating their database copies in the process. A split brain condition has now occurred.

DAC Mode enables a protocol called Datacenter Activation Coordination Protocol (DACP). DACP uses an in-memory bit that is set to 0 on startup. DACP prevents DAG members from mounting their databases until the DACP bit is set to 1, even if quorum is able to be achieved. The DACP bit can only change to 1 if:

- The DAG member can communicate with at least one other DAG member that has a DACP bit of 1.
- The DAG member can communicate with every other DAG member.

DACP acts as a safety catch to ensure that split brains cannot occur by requiring DAG members to be fully aware of the state of the DAG before they automatically activate their database copies. To enable DAC Mode, use the Set-DatabaseAvailabilityGroup cmdlet.

[Click here to view code image](#)

**#Enabling DAC Mode for a Database Availability Group**

```
[PS] C:\>Set-DatabaseAvailabilityGroup -Identity DAG01 -  
DatacenterActivationMode DagOnly
```

DAC Mode is recommended for any DAG that has more than one member, including DAGs that are located within a single datacenter. Even within a datacenter there are failure scenarios that could result in split brain, such as networking or power outages that isolate DAG members from each other in different server racks. Even if the risk is minimal, it's still recommended to enable DAC Mode. The only exception is when a third party hardware replication solution is being used for the DAG.

## **Need More Review? Datacenter Activation Coordination Mode**

DAC Mode is also applicable for two-member DAGs, but operates slightly differently than in larger DAGs by comparing the boot time of the File Share Witness server to the time when the DACP bit was set to 1.

Enabling DAC Mode also enables the use of built-in site resilience cmdlets used to perform datacenter switchovers. Without these cmdlets, a manual datacenter switchover requires running cluster management commands against the underlying Windows Failover Cluster directly.

You can find more information about DAC Mode on TechNet at  
[https://technet.microsoft.com/library/dd979790\(v=exchg.160\).aspx](https://technet.microsoft.com/library/dd979790(v=exchg.160).aspx).

## **Configure and manage proper placement of an alternate File Share Witness (FSW)**

For Database Availability Groups that span multiple datacenters there is an additional consideration of the alternate File Share Witness. The role of the alternate FSW is to serve as a witness server when a manual datacenter switchover to the secondary datacenter has occurred.

The alternate FSW does not need to be pre-configured on the DAG, it can be configured at the time the manual datacenter switchover is being performed. It's a good idea to have an alternate FSW ready and available when the time comes to do a datacenter switchover, so that your disaster recovery operation is not delayed by having to deploy a witness server first. Because every site requires domain controllers, you could consider using a domain controller at the secondary datacenter for the alternate FSW. As mentioned earlier, however, this is not recommended due to the security implications.

A common myth with the alternate FSW is that it provides redundancy for the witness server. This is not actually the case. At no time does the witness server role dynamically switch between the FSW and the alternate FSW, even when the FSW is offline for routine maintenance.

Because the alternate FSW is needed for datacenter switchovers, it needs to be located where the DAG members in the secondary datacenter can connect to it. The ideal location is within the secondary datacenter itself. There are no advantages to placing the alternate FSW elsewhere.

## Test and perform site recovery

When an Exchange 2016 Database Availability Group has been deployed with site resiliency, at some stage you should perform a manual datacenter switchover. Even if no disasters occur in the primary datacenter, the switchover is a process that should be tested and documented for your environment so that in the event of a real disaster, you have a well-rehearsed and tested process to follow. A manual datacenter switchover involves terminating the primary datacenter and then activating the DAG members in the secondary datacenter.

To terminate the primary datacenter, use the Stop-DatabaseAvailabilityGroup cmdlet with either the MailboxServer parameter to specify the servers to stop, or the ActiveDirectorySite parameter to stop all DAG members within an Active Directory Site boundary. Use the ConfigurationOnly switch if the mailbox servers are already offline, due to power failure for example, to make the change in Active Directory without needing to connect to the mailbox servers themselves. Ideally the mailbox servers should also be powered off and prevented from powering back on before you're ready, if the nature of the datacenter failure allows it.

[Click here to view code image](#)

```
#Terminating the DAG in a failed datacenter
```

```
[PS] C:\>Stop-DatabaseAvailabilityGroup -Identity DAG01 -  
ActiveDirectorySite NewYork  
-ConfigurationOnly
```

After stopping the servers in the primary datacenter, the DAG is then activated in the secondary datacenter by running the Restore-DatabaseAvailabilityGroup cmdlet. This process shrinks the DAG to only those servers used in the secondary datacenter, adjusting the quorum requirements accordingly. For DAGs without an alternate FSW already configured, use the AlternateWitnessServer parameter to configure a witness server for the DAG to use.

[Click here to view code image](#)

```
#Restoring the DAG in the secondary datacenter
```

```
[PS] C:\>Restore-DatabaseAvailabilityGroup -Identity DAG01 -  
ActiveDirectorySite  
SanFrancisco -AlternateWitnessServer SF-DC01
```

The database copies in the secondary datacenter should automatically activate if they are healthy, passive copies, and if there are no automatic activation blocks on the mailbox servers or the database copies themselves. If necessary, you can manually activate the mailbox database copies using the Move-ActiveMailboxDatabase cmdlet.

For Database Availability Groups that were not configured with DAC Mode enabled,

the datacenter switchover process involves manually running cluster management commands instead. The quorum mode for the cluster is manually adjusted to suit the number of available mailbox servers in the secondary datacenter. The alternate FSW is configured using Set-DatabaseAvailabilityGroup for quorum voting if necessary.

The switchover of the DAG to a different datacenter is only part of the overall process. For a fully site resilient solution to work, clients need to be able to connect to the Exchange servers and mail flow needs to work in and out of the secondary datacenter. As such, the datacenter switchover process also involves updating the DNS records for client access namespaces and ensuring that MX records and send connectors are adjusted for mail flow.

### Need More Review? Performing Datacenter Switchovers

The full process for performing datacenter switchovers for Exchange 2016

Database Availability Groups is available on TechNet at

[https://technet.microsoft.com/library/dd351049\(v=exchg.160\).aspx](https://technet.microsoft.com/library/dd351049(v=exchg.160).aspx).

## Summary

- Site resilience extends a high availability solution across multiple locations, enabling an Exchange 2016 DAG to be resilient to the failure of an entire datacenter.
- Multi-site DAGs can be designed for Active-Active scenarios, or Active-Passive scenarios, to meet the requirements of the organization's mailbox users so they can connect to their mailboxes when a datacenter is unavailable.
- DAC Mode prevents split-brain conditions from occurring when DAG members in different datacenter locations are isolated from each other due to a network failure.
- The datacenter switchover process is a critical part of an organization's disaster recovery plan, which should be documented thoroughly and tested regularly.

## Skill 1.4: Monitor and troubleshoot mailbox databases

Exchange 2016 has a built-in, intelligent health monitoring and recovery system called Managed Availability. Thanks to Managed Availability, many of the problems that occur in normal operation of an Exchange server are automatically detected and repaired. Despite the existence of Managed Availability, it's still necessary for the Exchange 2016 mailbox servers and databases to be monitored. Manual intervention by administrators is still required to troubleshoot and resolve problems.

---

## This section covers how to:

- [Monitor mailbox database replication and content indexing](#)
  - [Troubleshoot mailbox database replication and replay](#)
  - [Troubleshoot mailbox database copy activation](#)
  - [Troubleshoot mailbox database performance](#)
  - [Troubleshoot database failures \(e.g. repair, defrag, recover\)](#)
  - [Resolve quorum issues](#)
- 

## Monitor mailbox database replication and content indexing

The mailbox databases in a DAG are replicated between DAG members using a process called continuous replication. Continuous replication operates in two different modes:

- **File Mode** During the initial seeding process, and at any time where replication is catching up from a delay or outage, continuous replication runs in file mode. While running in file mode, a full transaction log file is written on the server hosting the active database copy. When the transaction log reaches 1 MB in size, the full log file is closed off and copied to the DAG members hosting passive database copies. The other DAG members then replay the log file into their passive copies, bringing it up to date with the changes that were logged to that transaction log file.
- **Block Mode** When seeding has finished and database replication is healthy, the DAG members switch to block mode continuous replication. While running in block mode, transaction log data is written to the log buffer stored in the memory of the server hosting the active database copy. The log data is also replicated to the log buffer stored in the memory of the servers hosting the passive database copies. When the log buffer is full, DAG members construct their own transaction log files on disk. Block mode replication allows DAG members to be kept more up to date with changes occurring on the active database copy, rather than needing to wait for a full log file to be shipped across the network.

Mailbox database replication health can be monitored using two methods. The first method is the `Test-ReplicationHealth` cmdlet, which reports the replication health of a DAG member. The health items reported by `Test-ReplicationHealth` include the cluster service, quorum resources, whether any database copies are failed or suspended, and whether the continuous replication process is copying and replaying logs fast enough.

[Click here to view code image](#)

```
#Using Test-ReplicationHealth to monitor Exchange 2016 DAG members
```

```
[PS] C:\>Test-ReplicationHealth -Server NY-EXCH01
```

Server	Check	Result
NY-EXCH01	ClusterService	Passed
NY-EXCH01	ReplayService	Passed
NY-EXCH01	ActiveManager	Passed
NY-EXCH01	TasksRpcListener	Passed
NY-EXCH01	TcpListener	Passed
NY-EXCH01	ServerLocatorService	Passed
NY-EXCH01	DagMembersUp	Passed
NY-EXCH01	MonitoringService	Passed
NY-EXCH01	ClusterNetwork	Passed
NY-EXCH01	QuorumGroup	Passed
NY-EXCH01	FileShareQuorum	Passed
NY-EXCH01	DatabaseRedundancy	Passed
NY-EXCH01	DatabaseAvailability	Passed
NY-EXCH01	DBCopySuspended	Passed
NY-EXCH01	DBCopyFailed	Passed
NY-EXCH01	DBInitializing	Passed
NY-EXCH01	DBDisconnected	Passed
NY-EXCH01	DBLogCopyKeepingUp	Passed
NY-EXCH01	DBLogReplayKeepingUp	Passed

The second method is to run the `Get-MailboxDatabaseCopyStatus` cmdlet. This cmdlet returns the health status of the database copies on a mailbox server, including the copy queue length and the replay queue length. Under normal, healthy conditions, the copy and replay queue lengths for a passive database copy should be close to zero unless the database copy is configured as a lagged copy.

[Click here to view code image](#)

```
#Using Get-MailboxDatabaseCopyStatus to monitor database replication
```

```
[PS] C:\>Get-MailboxDatabaseCopyStatus
```

Name	Status	CopyQueueLength	ReplayQueueLength	ContentIndexState
DB01\NY-EXCH01	Mounted	0	0	Healthy
DB02\NY-EXCH01	Healthy	0	0	Healthy
DB03\NY-EXCH01	Healthy	0	0	Healthy
DB04\NY-EXCH01	Healthy	0	0	Healthy

The status of a mailbox database copy can be one of the following:

- **Mounted** An active database copy that is serving client requests.
- **Healthy** A passive database copy that is successfully copying and replaying transaction log files from the active database copy.
- **DisconnectedAndHealth** A passive database copy that was previously in a

healthy state, but that has lost connectivity to the active database copy and can no longer participate in replication. Often this status is caused by a loss of network connectivity or DNS name resolution.

- **Suspended** A passive database copy that has been suspended from replication by an administrator.
- **Resynchronizing** A passive database copy for which the server has detected a divergence from the active database copy. The server automatically attempts to locate and resolve the issue.
- **ServiceDown** A database copy hosted on a server that has a stopped Microsoft Exchange Replication Service, or that is completely offline.
- **Failed** A database copy that is unable to copy or replay transaction log files. The server retries operations on this database copy at regular intervals attempting to return it to a non-failed state.
- **FailedAndSuspended** An underlying issue exists that has caused the database copy to fail. The server does not automatically retry operations on this database copy. The server does however, attempt auto reseed if it is configured in the environment. Usually this status requires manual intervention to resolve the underlying issue, such as replacing a failed disk, even if auto reseed is successful.

Get-MailboxDatabaseCopyStatus also returns the health of the content indexes for the database copies. Exchange 2016 maintains an index of mailbox contents, allowing users and administrators to perform searches to locate items. The search service indexes the contents of email items and attachments, including Microsoft Office files, PDFs, HTML, and plain text. One content index is maintained for each of the mailbox database copies. Content indexes in a Failed state cause users who are running Outlook in online mode, or who are using Outlook on the web, to be unable to search their mailboxes. Users who are running Outlook in cached mode are unaffected because their locally stored cache is indexed by their operating system and doesn't rely on the server-side indexing.

Databases that host journaling mailboxes are susceptible to the failed indexes because the journal mailbox captures all of the email traffic within the entire organization. As such, it is common to disable the content index on databases hosting journal mailboxes by running the Set-MailboxDatabase cmdlet to set the JournalingEnabled attribute to \$False.



## Exam Tip

Failed content indexes can be reseeded from another database copy in a DAG by running the `Update-MailboxDatabaseCopy` cmdlet with the `CatalogOnly` switch. For databases with only one copy, or where all copies have failed indexes, the only solution is to rebuild the index from scratch.

Content indexes display a state of Failed if the database is dismounted. If the database is mounted and the index is still Failed, there are two likely causes.

- Conflicts with the antivirus software installed on the server that is performing real-time scanning of the file system.
- A very high volume of changes within a mailbox database that the indexing service can't keep up with.

## Need More Review? Running Windows Antivirus Software on Exchange 2016 Servers

Antivirus software provides important protection for Windows servers. Even so, it does cause performance and stability problems for Exchange 2016 servers if it is not configured correctly. Microsoft's recommendations for setting exclusions for antivirus programs running on Exchange servers are published on TechNet at

[https://technet.microsoft.com/library/bb332342\(v=exchg.160\).aspx](https://technet.microsoft.com/library/bb332342(v=exchg.160).aspx).

## Troubleshoot mailbox database replication and replay

The output of `Get-MailboxDatabaseCopyStatus` reveals if there are replication or replay issues with a database copy by allowing you to see the copy and replay queue lengths. High copy queue lengths could indicate that network bandwidth is not sufficient to allow the transaction logs to be shipped from the active copy to the passive copies. It's common to see high copy queue lengths when a mailbox server has been offline for a period of time, such as during hardware maintenance. In these instances, the server is still catching up with all of the database changes that occurred while it was offline.

A high copy queue length could also mean a database copy has been suspended from replication because the `Suspend-MailboxDatabaseCopy` cmdlet has been used. Administrators can use the `SuspendComment` parameter to add comments so that other administrators know why the database copy has been suspended.

[Click here to view code image](#)

## #Viewing the reason for a suspended database copy

```
[PS] C:\>Get-MailboxDatabaseCopyStatus | Select Name, Status, SuspendComment
```

Name	Status	SuspendComment
DB01\NY-EXCH01	Mounted	
DB02\NY-EXCH01	Healthy	
DB03\NY-EXCH01	Suspended	Performing disk maintenance
DB04\NY-EXCH01	Healthy	

One of the reasons to suspend a database copy is so that it can be reseeded from another copy within the DAG. When a database copy's replication falls too far behind or diverges too much from the other database copies, the database copy fails and needs to be reseeded. Reseeding a database effectively means that the files for the database copy are deleted from the server, and are then copied across the network from another database copy. This process is similar to when the initial seeding process occurs for a new database copy. You can reseed a database copy by running the Update-MailboxDatabaseCopy cmdlet, and using the DeleteExistingFiles parameter to force the server to delete any existing database, log, or content index files that already exist on the disk.

[Click here to view code image](#)

## #Reseeding a mailbox database copy

```
[PS] C:\>Update-MailboxDatabaseCopy DB03\NY-EXCH01 -DeleteExistingFiles
```

For database copies that do not need to be reseeded, but were merely suspended for some other reason, then you can resume database replication by running the Resume-MailboxDatabaseCopy cmdlet.

Problems with database copies can cause transaction log files to accumulate on the DAG members, which runs the risk of eventually filling up all available disk space. The reason for this is that the DAG members do not remove transaction logs, even after a successful backup, until that log file has been successfully replayed into all of the passive database copies. The transaction logs are retained in case they need to be copied from a server during the activation of another database copy during the Best Copy and Server Selection (BCSS) process. The BCSS process, further explained in the next section, involves a step called Attempt Copy Last Logs (ACLL), which attempts to copy missing log files from the server that was hosting the active database copy before the failure occurred. The purpose of ACLL is to attempt to reduce the size of the copy queue length for a passive database copy. Copy queue length is a factor in determining which passive database copy is activated after a failure, which is also explained in the next section.

This risk exists even when circular logging is enabled. Circular logging operates differently for databases in a DAG that have more than one copy. Normal circular logging continually overwrites the log stream, resulting in only a small number of log files existing on disk at any given time. In a DAG, circular logging is called Continuous Replication Circular Logging (CRCL). The log files are only overwritten in CRCL when they have been confirmed to be copied and replayed into the other database copies.

## Troubleshoot mailbox database copy activation

During a target-less switchover or a failover scenario, the DAG's decision-making brain, called Active Manager, uses a process called Best Copy and Server Selection (BCSS) to choose which database copy is activated. BCSS takes into account more variables than just the Activation Preference value when choose a copy to activate.

Mailbox servers and database copies can be blocked from automatic activation, excluding them from the BCSS process. Mailbox servers are configured with a DatabaseCopyAutoActivationPolicy, which by default is set to Unrestricted. The policy is configured by running the Set-MailboxServer cmdlet. The other available configurations are:

- **Blocked** All database copies on the server are prevented from automatically activating. Administrators can still choose to manually activate the database copies if required. Mailbox servers in a secondary datacenter only used for disaster recovery purposes are sometimes configured with this setting to prevent unplanned failovers to that datacenter.
- **IntraSiteOnly** The database copies on the server can only activate automatically if the previously active database copy was located within the same Active Directory Site. This policy is only effective if the Active Directory Site boundaries are defined correctly.

In addition to the activation policies, mailbox servers can be configured for a maximum number of active databases by running the Set-MailboxServer cmdlet and using the MaximumActiveDatabases parameter. By default, there is no maximum number configured. In environments with a very large number of databases hosted within a DAG, a server can be sized for a certain number of active mailbox databases with the rest of the database copies on the server being passive or lagged. This opens up the possibility that too many database copies can activate on the server, causing a performance problem. Therefore, for larger environments, consider limiting the number of active databases per mailbox server to align with the sizing of the server and to ensure that the workload is balanced across the available DAG members. The potential downside of this is that Active Manager might not be able to automatically activate a database copy if all available DAG members have reached their maximum count.

Database activation policies configured at the mailbox server-level are sometimes not appropriate for an organization. When lagged database copies are configured, the lagged copies are often suspended from activation so they can only be manually activated by an administrator. Suspending a database copy from automatic activation is performed by running the `Suspend-MailboxDatabaseCopy` cmdlet and specifying the `-ActivationOnly` switch, which allows the database copy to continue participating in database replication.

#### Note: Automatic Activation Blocks

Preventing automatic activation of database copies by using mailbox server policies is not necessarily a fault. The configuration itself can be valid and perfectly justifiable for that organization. Blocking automatic activation of database copies however, does reduce the number of options the DAG has to maintain service availability by failing over to another database copy.

The `AutoDatabaseMountDial` settings for each mailbox server in the DAG are also taken into consideration. The `AutoDatabaseMountDial` setting configures the threshold for the number of missing transaction log files for a database copy that would qualify it as un-mountable. The missing log files are indicated by the copy queue length, which is the number of log files yet to be copied across the network from the server active database copy. There are three possible settings for `AutoDatabaseMountDial`:

- **GoodAvailability** This is the default setting and allows a database copy to be activated by Active Manager if it has a copy queue length of six or less.
- **BestAvailability** Allows a database copy to be activated by Active Manager if it has a copy queue length of 12 or less.
- **Lossless** Allows a database copy to be activated by Active Manager only if there are no missing log files.

#### Note: Missing Log Files Don't Necessarily Mean Data is Lost

Although it seems that **Lossless** is the logical choice, the potential data loss from the missing log files is mitigated by Safety Net. Active Manager can activate a mailbox database copy that is missing some log data, and then request the missing email items to be resubmitted from Safety Net, which maintains a cache of email messages that have already been delivered to mailboxes.

For any mailbox servers in the DAG that have an `AutoDatabaseMountDial` setting of **Lossless**, the Active Manager sorts the available database copies being considered for

activation in ascending order of their Activation Preference values. For the mailbox servers in the DAG configured with an AutoDatabaseMountDial setting of GoodAvailability or BestAvailability, the Active Manager sorts the available database copies by their copy queue length in order of shortest to longest. The AP value is used as a tie breaker if two database copies have the same copy queue length.

Active Manager then makes further assessment of the database replay queue length, which is the number of transaction log files copied from the server hosting the active copy, but have yet to be replayed into the passive database copy. Active Manager also looks at the health of the passive database copy and its content indexes, as well as the health of server components such as the client access protocol endpoints on the server. All of this assessment in the BCSS process is intended to ensure that during any failover situation, a healthy, up to date database copy hosted by a healthy mailbox server, is the database copy that is activated.

The net result of this is that under normal, healthy DAG conditions, the Activation Preference is the order in which database copies are activated during a failover. This order is not guaranteed however, so you should not assume that databases always failover to the next most preferred copy. If necessary, an administrator can manually activate a database copy by running the Move-ActiveDatabaseCopy cmdlet.

[Click here to view code image](#)

```
#Activating a database copy
```

```
[PS] C:\>Move-ActiveMailboxDatabase -Identity DB03 -ActivateOnServer SF-EXCH02
```

### Note: Balancing Database Availability Groups

To maintain a balanced I/O load across all of the disks hosting database copies, it is recommended to evenly distribute the Activation Preferences so that under normal conditions each server and disk is running approximately the same number of active, passive, and lagged database copies. Activation Preference values can be automatically balanced by running the RedistributeActiveDatabases.ps1 script provided with Exchange 2016. For more information, see

<http://exchangeserverpro.com/powershell-scripts-for-balancing-database-availability-groups>.

## Troubleshoot mailbox database performance

Even when a mailbox server has been appropriately sized using the Exchange Server Role Requirements Calculator, there can be cases where mailbox databases are not performing adequately, which results in slow email delivery and a poor user experience.

Database performance can be affected by storage hardware failure, memory exhaustion, low disk space, or an unexpectedly high load on the server. To isolate the cause of a problem, you must review event logs and collect performance data from the server. Event logs show alerts from Exchange 2016 when it detects issues such as delayed writes to the database. Performance data helps identify issues such as memory exhaustion and high load.

Performance data is only useful when it can be compared against a known, good baseline. As such, it is necessary to either collect performance data on a permanent, ongoing basis using a monitoring tool or periodically take a baseline of performance data for comparison purposes.

### Need More Review? Exchange 2016 Performance Counters

Microsoft publishes a detailed list of performance counters and their expected thresholds for good performance to monitor for Exchange. The performance counters for Exchange 2016 are largely the same as those for Exchange 2013 due to the similarities in the codebase of the two versions.

The full list is available on TechNet at

[https://technet.microsoft.com/library/dn904093\(v=exchg.160\).aspx](https://technet.microsoft.com/library/dn904093(v=exchg.160).aspx).

## Troubleshoot database failures

Exchange 2016 mailbox databases can become un-mountable due to corruption within the database itself, or due to missing transaction log files. Databases can be in a Dirty Shutdown state if the mailbox server experienced an unexpected restart, for example after the loss of power. When the mailbox server starts up again, the store service attempts to automatically recover the database to a mountable state. The store service checks the transaction log files against the database checkpoint and replays any log files for transactions that were still in the server's log buffer in memory and hadn't yet been committed to the database. This process relies on all of the database and log files being present and undamaged. You can perform a recovery using ESEUtil, or restore a previous version of the database from backup instead if any files are missing or damaged.

Despite Exchange 2016's ability to auto-recover un-mountable databases, there are times when a database still isn't able to be mounted automatically, or even manually

when you issue the Mount-Database command. Databases in this situation are often found to be in a state known as Dirty Shutdown. This can be determined by running the ESEUtil tool against the database file using the /mh switch, which examines the database header. In the output of ESEUtil, review the State attribute that is displayed.

[Click here to view code image](#)

```
#Using ESEUtil to determine the database state
```

```
C:\>eseutil /mh C:\ExchangeDatabases\DB01\DB01.db\DB01.edb
```

A database file in a Dirty Shutdown state requires a soft recovery to be performed using ESEUtil with the /r switch. To perform a soft recovery, you need to know:

- The log file name prefix. This can be retrieved by running the Get-MailboxDatabase cmdlet, and has a value similar to E00, E01, etc.
- The path to the transaction log files, for use with the /l switch.
- The path to the database file, for use with the /d switch.

For example, to perform a soft recovery on a database stored in E:\DB01, with logs in the F:\DB01 directory, and a log file prefix of E01, the ESEUtil command is:

[Click here to view code image](#)

```
#Soft repair of a mailbox database with ESEUtil
```

```
C:\>eseutil /r E01 /d E:\DB01 /l F:\DB01
```

After running the soft recovery, you can re-run ESEUtil /mh to check whether the database is still in a Dirty Shutdown state, or if the recovery successfully brought the database to a Clean Shutdown state. Mount the database if it is in a Clean Shutdown state by running the Mount-Database cmdlet.

Databases that fail soft recovery and that can't be restored another way, such as from a recent backup, can be considered for a hard recovery instead by running ESEUtil with the /P switch. Hard recovery is a potentially destructive process because it removes any corrupt database pages, which results in some data loss. The amount of data loss is impossible to predict. A hard recovery might result in a 200-GB database ending up as a 190-GB file with minimal data loss, or a 50-GB file with severe data loss. Due to the potential for data loss, you should only perform a hard repair of a mailbox database as a last resort, preferably under the direction of Microsoft Support and only after making a backup copy of the database file.

## Need More Review? Exchange Server Database Utility Guide

ESEUtil is a well-documented tool that has changed very little over the last 10 years. Microsoft has published extensive guidance on TechNet describing how to use ESEUtil in various modes for recovery purposes at [https://technet.microsoft.com/library/aa996953\(v=exchg.65\).aspx](https://technet.microsoft.com/library/aa996953(v=exchg.65).aspx).

## Resolve quorum issues

The most important element of any Database Availability Group that you need to consider when predicting failure response is quorum. When you are thinking about a failure condition, consider how and where quorum can be maintained, if at all. [Table 1-1](#) summarizes the quorum requirements for Exchange 2016 DAGs and includes the possible number of DAG members in each scenario. You must be careful performing normal maintenance to ensure that you do not inadvertently take down too many servers, causing a loss of quorum.

Number of DAG Members	QUORUM Requirement	File Share Witness Used
1	1 DAG member	No
2	1 DAG member	Yes
3	2 DAG members	No
4	2 DAG members	Yes
5	3 DAG members	No
6	3 DAG members	Yes
7	4 DAG members	No
8	4 DAG members	Yes
9	5 DAG members	No
10	5 DAG members	Yes
11	6 DAG members	No
12	6 DAG members	Yes
13	7 DAG members	No
14	7 DAG members	Yes
15	8 DAG members	No
16	8 DAG members	Yes

TABLE 1-1 Quorum requirements for Database Availability Groups of all sizes

Exchange 2016 can be deployed on Windows Server 2012 and Windows Server 2012 R2 operating systems. Each of those versions of Windows Server supports a feature called Dynamic Quorum. For Windows Failover Clusters on those operating systems, Dynamic Quorum is enabled by default. Dynamic Quorum allows the cluster to automatically adjust the quorum voting requirements when sequential failures occur, as long as quorum has been maintained in the failure scenario. For example, a four-member DAG requires at least three votes to remain online, which is achievable with a minimum of two DAG members plus the File Share Witness. If one DAG member fails, quorum is still maintained, and the cluster dynamically adjusts the number of votes required for quorum down to two. If another failure occurs, the cluster adjusts the voting requirement down again, all the way to a “last man standing” scenario.

In contrast, if a four-member DAG experiences a failure of two DAG members plus the File Share Witness simultaneously, when a datacenter fails for example, quorum is immediately lost and Dynamic Quorum has no effect. Therefore, Dynamic Quorum should be considered just one part of the overall high availability solution, and should not be relied upon to protect the DAG from every possible failure scenario that might cause a loss of quorum.

## Summary

- Mailbox databases must be monitored in your Exchange 2016 environment to ensure they are still mounted, healthy, and replicating successfully to any other database copies.
- Activation of database copies by Active Manager relies on the Best Copy and Server Selection Process, which takes into account multiple variables including the health of database copies and mailbox servers. It also takes into account whether automatic activation has been blocked by a policy on the server or database copy.
- Mailbox database failures can result in data loss if not managed correctly. Database recovery is attempted automatically by the Exchange server at startup, or can be performed manually using the ESEUtil tool.
- Understanding how the quorum voting process works is key to ensuring that an Exchange 2016 DAG is able to maintain service availability in a variety of failure scenarios.

## **Skill 1.5: Plan, deploy, and manage backup and recovery solutions for mailbox databases**

Much like designing a high availability solution to meet service level agreement (SLA) requirements, backup solutions should also be designed to meet a defined SLA. For backup solutions, the most important metrics are:

- **Recovery Point Objective (RPO)** Defines the point to which data must be restored, or in other words, how much data loss the organization is willing to accept in a recovery scenario. For example, the RPO could be stated as 24 hours if an organization is willing to lose one day's worth of email.
- **Recovery Time Objective (RTO)** Defines the amount of time in which the recovery must be completed. For example, data must be restored in less than 4 hours to meet the SLA if an organization has an RTO of 4 hours.

Without an RPO and RTO to aim for, the backup solution is simply a best effort approach, which might not satisfy the organization in every situation where a data restore is required. The purpose of the backup solution guides the types of backups that are performed.

---

### **This section covers how to:**

- [Plan most appropriate backup solution that meets SLA requirements of RPO/RTO](#)
  - [Deploy, configure, and manage lagged mailbox database copies](#)
  - [Recovery an Exchange server, mailbox database, mailbox, public folder, or mail item](#)
  - [Recovery the public folder hierarchy](#)
  - [Perform a dial tone restore](#)
- 

### **Plan most appropriate backup solution that meets SLA requirements of RPO/RTO**

There are four backup types that can be undertaken using most of the backup solutions available on the market today:

- **Full** A complete copy of the data on a server, volume, or file system. For Exchange 2016 backups, a full backup is often referred to as a “VSS full” or “application aware” backup due to the use of the Volume Shadow Service to take application-consistent backups of Exchange data. Full backups of mailbox databases include a complete backup of the database files and the transaction log files up to the current checkpoint. When the backup is completed, the log files

prior to the checkpoint are truncated, or in other words, removed from the server. A full backup can be used to restore mailbox databases on its own as it contains a complete set of data.

- **Incremental** A partial copy of the data on a server, volume, or file system. An incremental backup includes the data that changed after the last full or incremental backup. For mailbox databases this means that the transaction logs generated after the last backup are included, but not the database file itself. Successful incremental backups also initiate log truncation. Because there is a smaller amount of data being backed up, incremental backups are generally much faster than full backups. In a restore scenario however, the last full backup plus all of the subsequent incremental backups are required to complete the data restore, which tends to slow down the recovery process.
- **Differential** Similar to an incremental backup, however a differential backup does not initiate log truncation, nor does it mark data as having been backed up. This means that differential backup sets get larger and larger as more time passes after the last incremental or full backup. In a restore scenario however, only the last full backup and the most recent differential backup are required to complete the data restore, which can be faster than an incremental strategy but still slower than a full backup strategy.
- **Copy** Similar to a full backup, however, a copy backup does not initiate log truncation. Furthermore, copy backups are not supported for production recovery scenarios. A copy backup can only be used to make a copy of the Exchange database that you can take into a separate environment, such as a testing environment.

Each backup type has pros and cons and a different level of administrative complexity involved. The most important thing is still the RPO and RTO, and whether a given type of backup, or a mixture of several types of backups, is able to meet these goals. The size of the data to be backed up is also a factor you must consider in your backup strategy. For instance, it is not feasible to run a full backup every single day if a full backup of all databases on a server takes 26 hours to complete. Instead, you would consider using incremental backups on most days of the week, and only perform a full backup on the weekend.

Not all restore scenarios require that you restore data from a backup. As discussed later in this section, mailboxes and mailbox items can often be recovered using other mechanisms without the need to restore a full database from previous backups.

## Recover an Exchange server

When a full server failure occurs for Exchange Server 2016 it's important that you do not attempt to restore the entire server from a previous backup. Restoring a full server, even from a traditional backup, is similar to rolling back a virtual machine to a previous snapshot. As mentioned earlier in this chapter, Exchange 2016 does not support time travel. Do not attempt a recovery method that would revert the server to a previous state.

Often the failure of an Exchange Server 2016 mailbox server leaves the data volumes intact, only requiring the operating system and Exchange application to be restored. In some cases, it might also be necessary to restore the most recent database backups as well.

To recover a failed server, you must install a server of the same specifications as the one that failed. It can be a virtual machine or a physical server, as long as it has the same performance characteristics of the server it is replacing. The server also needs the same storage layout available.

After reinstalling the operating system for the server, giving it the same name as the old server, and joining it to the domain, you can then perform a recovery install of Exchange 2016. This is performed by running the Exchange setup process with the /m:RecoverServer command line parameters. Exchange setup retrieves configuration settings for the server from Active Directory and sets up the new server with those same settings.

### Important: Not all Settings are Stored in Active Directory

While most of an Exchange 2016 server's configuration is stored in Active Directory, there are still some important configuration items that are only stored locally on the server. Most notably, the SSL certificates installed on the previous server needs to be reimported or reissued for the new server. Similarly, any customizations in IIS, local config files, or the registry needs to be reapplied.

When the recovery install is complete and if the database and transaction log volumes are still intact and mounted in the same drive letters or folder paths, the server is once again operational.

For Exchange 2016 mailbox servers that are members of a DAG, the recovery process is slightly different. Firstly, thanks to the replication of databases within the DAG, the failure of one DAG member should not cause a loss of service availability. This means that the server recovery process is not required to meet any RPO or RTO on its own. Even so, it is still best to recover the server quickly and re-add it to the DAG.

so that it can add resiliency to your environment again.

For the failed DAG member, any database copies hosted on that server need to be removed from the DAG's configuration. This is achieved by running the Remove-MailboxDatabaseCopy cmdlet, and because the mailbox server is unavailable, also by using the ConfigurationOnly switch to make the change in Active Directory. The failed DAG member also needs to be removed from the DAG by running the RemoveDatabaseAvailabilityGroupServer cmdlet, again with the ConfigurationOnly switch to force the change in Active Directory. Finally, the Remove-ClusterNode cmdlet is used to forcibly evict the failed DAG member, which requires the use of the Force switch.

After a failed DAG member has been forcibly removed from the DAG you can proceed with the Exchange 2016 recovery install. At that point, the recovered server is back to being a functional mailbox server, but still needs to be manually re-added to the DAG and have database copies re-added to the server before it can be fully returned to service.

### **Important: Clean Removal of Exchange Servers**

In some environments, a failed Exchange server is simply abandoned by the administrators and a new Exchange server is deployed to replace it.

While the new server might provide the functionality the organization needs, the Active Directory objects for the failed server are still present and can cause issues over time. Other servers can "see" that the failed server still exists, but cannot connect to it. To resolve this situation, you should perform a recovery install of the failed server, followed by an uninstall of the Exchange server software to cleanly remove the server from the organization.

## **Recover a mailbox database**

The precise steps to recovering a mailbox database depends on the backup software you're using in your environment. Regardless of the software being used, there are some decisions that you must make as you work through the restore process.

The first decision is whether you plan to restore over the existing database or restore to an alternative location. In a situation where a database has failed and you are using a previous backup to restore the database, you would restore over the existing database. A second decision then needs to be made. Do you restore to the point in time of the last backup, therefore losing any changes made to the mailbox data after the backup? Or do you allow the backup software to use the transaction log files available on your server to "roll forward" the database up to the point in time the failover occurred? The answer

depends on your RPO, and the goal you're trying to achieve by restoring the database. In cases where corruption is suspected, such as a virus attack, then rolling forward the database using the transaction logs would risk reintroducing the corruption to the restored database.

If you decide to restore to an alternative location, the existing database is left untouched and you can use the restored database files to mount a recovery database. A recovery database is a mailbox database that contains mailbox data, but is not associated with users in the organization. You can extract data from the recovery mailbox by creating mailbox restore requests, but users can't log on to mailboxes in the recovery database, nor can they connect to it with Outlook or other clients.

To create a recovery database, run the New-MailboxDatabase cmdlet and use the Recovery switch. Restore the database and transaction log files to an alternative location, ensuring that the file paths match the EdbFilePath and the LogFolderPath for the recovery database. The database file is in a Dirty Shutdown state that requires a soft recovery to be performed using ESEUtil. When the database file is in a Clean Shutdown state, the recovery database can be mounted using the Mount-Database cmdlet. After mounting the database, run Get-MailboxStatistics with the Database parameter specifying the recovery database name to see the available mailboxes in the recovery databases.

## Recover a mailbox

Not all mailbox recovery scenarios require you to restore a full mailbox database from backup. Mailbox databases are configured with retention settings for deleted items and deleted mailboxes. By default, a mailbox database retains deleted mailboxes for 30 days. If a mailbox has been inadvertently disabled, it remains in the database as a disconnected mailbox for the deleted mailbox retention period before it is purged completely from the database.

While a mailbox is in this disconnected state in the database, it can be reconnected to an Active Directory user object. This is performed by running the Connect-Mailbox cmdlet. To connect a mailbox back to the original user object it was associated with, the following command is used.

[Click here to view code image](#)

```
#Reconnect a disconnected mailbox
```

```
[PS] C:\>Connect-Mailbox -Identity "Kim Akers" -Database DB01 -User "Kim Akers"
```

Use a mailbox restore request instead if the user already has a mailbox. Mailbox restore requests are also used to restore mailboxes from recovery databases. You can create a mailbox restore request using the New-MailboxRestoreRequest cmdlet. The

restore is then processed by the Exchange server as a background task.

[Click here to view code image](#)

```
#Create a mailbox restore request  
  
[PS] C:\>New-MailboxRestoreRequest -Name "Kim Akers restore" -  
SourceDatabase RecoveryDB  
-SourceStoreMailbox "Kim Akers" -TargetMailbox "Kim Akers"
```

When you need to restore a mailbox to a different user object than it was originally connected to, including if you have recreated the user object with the same name, you must include an additional AllowLegacyDNMismatch switch in the New-MailboxRestoreRequest command. You can also perform a redirection of the restored data to a specific folder in the mailbox by adding the TargetRootFolder parameter.

## Recover a mail item

A lot of restore scenarios do not require the entire mailbox to be restored. In many cases, the user is asking for specific items or folders to be restored to their mailbox, possibly due to accidental deletion.

Similar to the mailbox retention period, deleted items are retained by a mailbox database for 14 days by default. This makes it possible for users to recover deleted items for up to 14 days using Outlook or Outlook on the web. The exception to this is when the user purges their recoverable deleted items prior to the full retention period lapsing, which causes the items to be permanently deleted from the database before the full retention period. This can be a compliance concern for some organizations because it can be used by a user to try to remove evidence of an email that they have sent or received. To ensure that your full deleted item retention period is maintained, you can enable Single Item Recovery for a mailbox. When Single Item Recovery is enabled, even if the user purges their recoverable deleted items, the item is still retained until the full retention period has lapsed. If it is enabled however, the user can no longer recover the items themselves. Instead, the items can be recovered only by an administrator by running the Search-Mailbox cmdlet, which can return up to 10,000 results per mailbox, or by using the New-MailboxSearch cmdlet. Alternatively, the In-Place eDiscovery & Hold console in the Exchange Administration Center can be used to perform searches and recover deleted items.

To enable a mailbox for Single Item Recovery, use the Set-Mailbox cmdlet.

[Click here to view code image](#)

```
#Enabling a mailbox for Single Item Recovery
```

```
[PS] C:\>Set-Mailbox -Identity "Kim Akers" -SingleItemRecoveryEnabled  
$true
```

After deleted mailbox items have been purged from the database, a restore of a previous backup into a recovery database is required before you can recover the missing items. Mailbox items are then restored using mailbox restore requests, as with full mailbox restores demonstrated in the previous section. For mailbox item recovery you can use the `IncludeFolders` parameter to define the folders that should be included in the restore. For example, the following command restores the sent items folder for a mailbox.

[Click here to view code image](#)

#### #Restoring a specific mailbox folder

```
[PS] C:\>New-MailboxRestoreRequest -Name "Kim Akers sent items" -  
SourceDatabase RecoveryDB -SourceStoreMailbox "Kim Akers" -TargetMailbox  
"Kim Akers" -IncludeFolders  
"#SentItems#"
```

### Need More Review? Granular Mailbox Restore Requests

Mailbox restore requests can be configured in a very granular fashion to only include or exclude specific folders, date ranges, or even items matching specific keywords. You can find more information about mailbox restore requests on TechNet at

[https://technet.microsoft.com/library/ff829875\(v=exchg.160\).aspx](https://technet.microsoft.com/library/ff829875(v=exchg.160).aspx).

## Recover a public folder

Public folder content is stored in public folder mailboxes, which are contained in mailbox databases and protected by the same backup and recovery solutions you use for other types of mailboxes hosted in Exchange databases. Therefore, public folders can be restored using the same mailbox restore requests that you would use for other mailbox types.

Deleted public folder mailboxes that are still retained by the mailbox database can also be reconnected to an Active Directory user object. The user objects associated with public folder mailboxes should not be modified or deleted, but if they have been you can recover the deleted user object using your Active Directory recovery processes or recreate the user object with the same name.

Public folder mailboxes that are mail-enabled are not able to receive new email messages after being reconnected to the Active Directory user object. To get this working again you need to:

1. Make a backup or take note of the SMTP addresses on the public folder mailbox.
2. Mail-disable the public folder mailbox.

3. Mail-enable the public folder mailbox again.
4. Re-apply any missing SMTP addresses for the public folder mailbox.

## Recover the public folder hierarchy

Although public folder mailboxes use the same recovery processes as regular mailboxes, the primary hierarchy public folder mailbox requires a different approach in some cases. Remember that the primary hierarchy mailbox contains the only writeable copy of the public folder hierarchy.

You can reconnect a deleted public folder mailbox to an Active Directory user by running the Connect-Mailbox cmdlet if the mailbox is still retained within the mailbox database. The recovery process does introduce some risks if the deleted primary hierarchy mailbox has been purged from the mailbox database. By restoring the primary hierarchy mailbox from a previous backup, the hierarchy from the backup replicates to the secondary hierarchy mailboxes, causing any newly created public folders in the hierarchy to disappear. As such, it is recommended to protect the primary hierarchy mailbox from accidental deletion by setting the “Protect object from accidental deletion” checkbox on the Active Directory user object.

## Perform a dial tone restore

In some disaster situations, the recovery time requires that email services be recovered before any data has actually been restored. This is referred to as a dial tone restore, and involves mounting an empty mailbox database to replace the failed database. Users connect to the database and gain access to an empty mailbox. Using this method, they can begin sending and receiving emails while the data recovery efforts continue behind the scenes. The dial tone database can be hosted on the same server with the same database name as before, or it can be hosted on a different server with a different database name. To re-home the mailboxes to the dial tone database, run the Set-Mailbox cmdlet with the Database parameter.

The administrators can restore the failed mailbox databases to recovery databases, and mount them ready to activate for the users. At this stage a mailbox restore request is not the most efficient course of action. Consider a scenario in which a dial tone restore has been performed and a small amount of mailbox database content has been generated in the dial tone mailboxes. Meanwhile, several hundred gigabytes of mailbox content are stored in the recovery database. It is much more efficient to merge the small amount of new mail items from the dial tone database into the restored database than it is to merge in the other direction.

To merge the data, an outage needs to be arranged so that the databases can be dismounted. After dismounting the databases, swap the database and log files for the

dial tone database with those for the recovered database. As a precaution, you should make another copy of the dial tone database as well.

After swapping the files, the databases are mounted again. This time the mailbox users are connecting to their mailboxes in the restored database. The new mail items created in the dial tone database are not immediately available to users. At this point, you can run mailbox restore requests to restore the smaller amount of data in the dial tone database back into the users' mailboxes.

## Deploy, configure, and manage lagged mailbox database copies

A lagged database copy is a passive database copy in a DAG that has a delayed transaction log replay configured. Log files are shipped to the server hosting a lagged database copy, inspected to ensure their integrity, and then the server waits for the replay interval to pass before replaying the log data into the passive database copy. The purpose of a lagged copy is to provide the ability to recover the database from an earlier point in time if a corruption or error occurs in the other active and passive database copies.

### Note: Native Data Protection

Lagged database copies are one part of the overall Native Data Protection capability of Exchange 2016, which eliminates traditional backups in favor of multiple database copies combined with data retention settings. Native Data Protection is used by Microsoft in Exchange Online, the cloud-hosted Exchange service that is part of Office 365. No traditional backups of Exchange Online databases are performed by Microsoft.

Although Native Data Protection is recommended by Microsoft as part of the Preferred Architecture for Exchange 2016, it takes a high degree of technical accuracy and operational efficiency to make it feasible to run an on-premises Exchange organization without traditional backups.

The replay lag interval for a database copy is configured using the Set-MailboxDatabaseCopy cmdlet, with the value in the format of “days.hours:minutes:seconds.” You can configure a maximum lag interval of 14 days.

[Click here to view code image](#)

```
#Configuring a 7-day replay lag
```

```
[PS] C:\>Set-MailboxDatabaseCopy -Identity DB04\SF-EXCH02 -ReplayLagTime  
7.0:0:0
```

When you configure a replay lag interval, the Exchange server warns you that Safety

Net must also be configured with a hold time that is the same or greater than the replay lag time. This ensures that during some lagged copy activation scenarios, Safety Net can be used to resubmit missing email messages that would otherwise be lost as part of the activation process.

### Note: Storage Requirements for Lagged Copies

Lagged database copies accumulate a large number of transaction log files on disk. As such, it is important to plan for this in your storage design and provision large log volumes to accommodate the increased volume.

Lagged database copies are good candidates to suspend from automatic database activation. There are some concerns with automatically activating a lagged copy, such as:

- The activation process can take a very long time because all of the transaction log files that have not yet been replayed into the database need to be replayed prior to mounting the database.
- Automatic activation replays all available transaction log files, which might include the transactions that caused the logical corruption of other database copies.
- The lagged copy can no longer be used for recovery to a point in time, until it returns to being a lagged, passive copy.

To block a lagged database copy from automatic activation, use the Suspend-MailboxDatabaseCopy cmdlet with the ActivationOnly switch.

[Click here to view code image](#)

#Configuring a 7-day replay lag

```
[PS] C:\>Suspend-MailboxDatabaseCopy -Identity DB04\SF-EXCH02 -ActivationOnly
```

Lagged database copies can be used in a variety of recovery scenarios.

- **Roll forward all available log files** The lagged database copy can be brought up to date by committing all of the available log files for the database that are in the replay queue. The lagged database copy is first suspended by running Suspend-MailboxDatabaseCopy, so that a backup of the lagged database and log files can be taken. You can simply copy the files to an alternative location, or run a file-level backup. After resuming the database copy, use the MoveActiveMailboxDatabase cmdlet to activate the database copy, using the SkipLagChecks switch to force the lagged copy to activate. You must then wait for all of the queued log files to replay into the database.

- **Activate to a specific point in time** In this scenario, some of the transaction log files are removed from the server to prevent them from being replayed into the database copy. As with the previous approach, suspend the database copy and make a backup before you proceed. Next, use the timestamps of the transaction log files to locate the log files generated after the point in time you’re recovering to. Remove those folders from the server and delete the checkpoint (.chk) file from the log folder. A soft recovery is then performed using ESEUtil. When the database is in a Clean Shutdown state, copy it to another location to mount. For example, you can copy it to a location where a corrupted database copy was previously located. When the database copy is mounted you can resume the lagged database copy as well.
- **Activate a lagged copy using Safety Net** In this scenario, all of the transaction log files except for those required to mount the database are removed from the log folder. As always, suspend the lagged copy and make a backup first. You can then use ESEUtil to identify the hexadecimal value of the last log file that is required for the database to be mountable. Remove all other log files created after that log file. After stopping the Microsoft Exchange Replication service on any other DAG members hosting copies of that database, you can then run MoveActiveMailboxDatabase with the MountDialOverride, SkipActiveCopyChecks, SkipClientExperienceChecks, SkipHealthChecks, and SkipLagChecks switches. The database copy mounts and requests all missing mail items to be resubmitted from Safety Net.

#### **Important: Use Caution When Activating Lagged Database Copies**

The lagged copy activation procedures involve precise steps be followed to ensure that the database activates in the manner you require. For all of the lagged copy activation scenarios, make sure that you back up the original database and log files before you make any changes or remove any files from the log folder.

After activating a lagged database copy there are additional tasks you should perform to ensure the continued high availability of your mailbox databases:

- Use Get-MailboxDatabaseCopyStatus to monitor the health of your database copies, and remediate any that are no longer healthy.
- Move active database copies back to your most preferred server in order to rebalance the load on your DAG members.
- Re-apply the lagged copy configuration so you have another lagged copy ready for future recovery scenarios.

## Summary

- Backup solutions can't be designed in a vacuum. They must be designed to meet the specific RPO and RTO requirements of the organization.
- A backup and recovery strategy can contain a mixture of different backup types, database retention settings, and lagged database copies. With multiple capabilities available, you can choose the most appropriate restore technique for each scenario.
- Failed Exchange servers should be restored by performing a recovery install of Exchange onto the repaired server, or onto another server of similar performance characteristics. A failed server must be recovered first and then have a clean uninstall performed if it is to be decommissioned entirely.
- Mailboxes and mailbox items, including public folder content, can be restored from recovery databases using mailbox restore requests.
- Protecting the primary hierarchy mailbox is critical to ensuring that changes to the public folder hierarchy are not overwritten by restoring the primary hierarchy mailbox.
- Lagged database copies have the flexibility to provide a variety of recovery capabilities when database corruption occurs.

## Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find the answer to this thought experiment in the next section

Contoso, Ltd. has offices in New York and San Francisco, and wants to ensure its Exchange 2016 environment is highly available and able to be accessed by all staff when the WAN connection between the two cities is interrupted, as has happened in the past when construction work has resulted in the fibre cable being dug out of the ground.

The company has virtualization infrastructure available at each site, with both SAN and NAS storage available. Company directors have previously been frustrated by long recovery times when they accidentally delete emails and want to see faster restores of individual items. Because of the critical nature of email to the business, they also require that email services be unavailable for no more than 4 hours.

1. What type of high availability solution should be deployed?
2. Which storage type should be used for the mailbox servers?
3. What backup and recovery solution should be implemented to meet the directors' requirements?

## Thought experiment answer

This section contains the solution to the thought experiment.

1. An Exchange 2016 Database Availability Group should be deployed for New York and San Francisco. Two DAGs in total should be deployed in Active-Passive configuration, with the File Share Witness for each city's DAG located within that city's datacenter. This ensures that each DAG is able to achieve quorum and stay online in the datacenter closest to the mailbox users in that city in the event that the WAN connection goes offline.
2. The Exchange 2016 mailbox servers should use the SAN storage if it can meet the IOPS requirements for the environment. Alternatively, additional direct-attached-storage (DAS) can be purchased for the DAG members. The NAS storage should not be used.
3. Regular backups of the mailbox databases should be taken. A combination of full and incremental backups would be acceptable if daily full backups are not able to fit in the required backup window. To facilitate deleted item recovery, the deleted item retention period should be increased to 30 days. In a serious disaster where full databases restores are deemed necessary, dial tone recovery can be used to resume email service while the database restore tasks are performed behind the scenes.

# **Chapter 2. Plan, deploy, manage, and troubleshoot client access services**

As an administrator managing Exchange Server 2016, you have to manage a wide variety of technologies. Some of the technologies are backend technologies, which are invisible to your users. For example, users are unconcerned with the volumes where you store your mailbox databases as long as there is ample free space and the performance is good. Other services are client-facing, meaning that your users are directly impacted if there is a misconfiguration or if a service is unavailable. For example, if the certificate you use for client access expires, users are immediately impacted. Outlook might notify the user that there is a problem with the certificate, which often means users submit helpdesk tickets or call the IT department for a solution. To minimize user disruption, you need to properly plan, deploy, and manage all of the client access services.

## **Skills in this chapter:**

- [Plan, deploy, and manage client access services](#)
- [Plan, deploy, and manage mobility solutions](#)
- [Plan, deploy, and manage load balancing](#)
- [Monitor and troubleshoot client connectivity](#)
- [Plan, deploy, and manage a site-resilient client access services solution](#)

### **Skill 2.1: Plan, deploy, and manage Client Access services**

Client access services is an area that covers all of the technologies facilitating the client's ability to use Exchange-related services, such as email. Client access services include a fairly long list of technologies. Some technologies are important for all deployments, such as certificates. Other technologies are used less frequently and are simpler, such as POP3 and IMAP4. For the exam, you need to be familiar with all of them. In Exchange Server 2016, the Mailbox server role takes on its traditional duties, mailbox database management for example, along with the duties of the Client Access server role which handles client access services. There is no longer a dedicated Client Access server role in Exchange 2016. This section covers the planning, deploying, and managing of technologies that make up client access services.

---

## This section covers how to:

- [Plan namespaces for client connectivity](#)
  - [Plan proxy and redirection requirements](#)
  - [Plan and deploy certificates](#)
  - Plan and configure authentication, including forms-based authentication (FBA), Basic, NTLM, and Kerberos
  - [Plan, deploy, and configure Autodiscover, Outlook Anywhere, Outlook MAPI over HTTP, Exchange Web Services, Outlook on the web, Exchange Admin Center, Exchange ActiveSync, POP3, and IMAP4](#)
  - [Plan, deploy, and configure Office Online Servers \(OOS\)](#)
  - [Plan, create, and configure Offline Address Book \(OAB\)](#)
  - [Plan, create, and configure hierarchical address lists](#)
  - [Plan, deploy, and configure address book policies](#)
- 

## Plan namespaces for client connectivity

To enable users to access Exchange Server services, you need to configure Exchange services with names and URLs. When you see the word “namespace,” you should know that it refers to the URLs and fully qualified domain name (FQDNs) that are associated with Exchange services. For example, users who connect to Outlook on the web need a URL. The URL is part of your Exchange namespace. When Outlook runs, it attempts to use Autodiscover to locate Exchange services. Autodiscover is also part of your Exchange namespace. There are several services that require URLs and FQDNs to function, such as Autodiscover, Outlook Anywhere, Outlook MAPI over HTTP, Exchange Web Services, Outlook on the web, Exchange Admin Center, Exchange ActiveSync, POP3, and IMAP4.

You have a few primary options for your namespace. The first option is to use a unified namespace, sometimes referred to as an unbound deployment. With a unified namespace, all services use the same URLs and FQDNs without regard to their datacenter location and mailboxes are spread out across datacenters. A unified namespace simplifies your Exchange environment, however users might end up being serviced by a Mailbox server outside of their closest datacenter. In environments where you have two datacenters with low latency and high bandwidth connectivity between them, the user experience remains good regardless of which server services their requests. In environments with two datacenters with high latency connectivity, such as datacenters located far away from each other, the user experience is likely to be insufficient. In such a scenario, consider using a dedicated namespace for each

datacenter.

Using a dedicated namespace for each datacenter, sometimes referred to as a bound deployment, is a bit more complex than using a unified namespace. You have to manage multiple names and the names need to be part of your certificates. Be aware that having multiple certificates and a complicated set of names in a certificate add administrative overhead. If you have an Exchange environment spread out among datacenters with high latency connectivity, you should consider a dedicated namespace to improve the end user experience and reduce administrative overhead.

You must also consider internal versus external connectivity because in almost all environments, the path internal and external users use to connect to services is different. Your design goal should be to simplify this area as well. The simplest configuration uses a single namespace for internal and external connectivity. For example, your Outlook on the web URL can be <https://mail.contoso.com/owa> for internal and external users. To facilitate this, you need to have “split-brain” DNS, often referred to as “split DNS.” Split DNS occurs when you have Domain Name System (DNS) services for your internal local area network (LAN) separate from your DNS services for your externally facing resources. While each DNS services hosts a DNS zone for your domain, the IP addresses associated with the FQDNs is different. For example, the internal DNS for mail.contoso.com resolves to a private IP address on your LAN, such as 10.136.50.22, while the external DNS for mail.contoso.com resolves to a public IP address, such as 38.96.29.10. In both cases, the IP addresses can be Mailbox servers or load balancers that load balance traffic to your Mailbox servers, or for external connectivity, the IP might be attached to a firewall or reverse proxy server. Namespaces also impact other parts of your configuration such as certificates. Certificates are discussed later in this section.

### Need More Review? Namespace Planning in Exchange 2016

To find more information about planning for namespaces, see

<https://blogs.technet.microsoft.com/exchange/2015/10/06/namespace-planning-in-exchange-2016/>.

## Plan proxy and redirection requirements

When you first see proxy, you might be thinking about reverse proxy, which is a widely used application in Exchange deployments to securely connect Internet users to internal Exchange Server services. But in this case, the exam covers the proxying capabilities built into Exchange Server. Proxying, along with redirection, are specifically called out as some of the skills you need to know for the exam.

## Proxying

As previously mentioned, the Mailbox server is now responsible for the client access services. This is why proxying and redirection are handled by the Mailbox server. To facilitate this, client access services and the traditional mailbox services, hereby referred to as backend services, are separate and distinct services on the Exchange server. This is where proxying comes in. To understand proxying, it often helps to see a diagram showing it in action. [Figure 2-1](#) illustrates a user connecting to an Exchange Server 2016 Mailbox server. Based on where the user's mailbox is located, the client access services proxy the connection to the backend services, whether locally on the server or on a remote server.

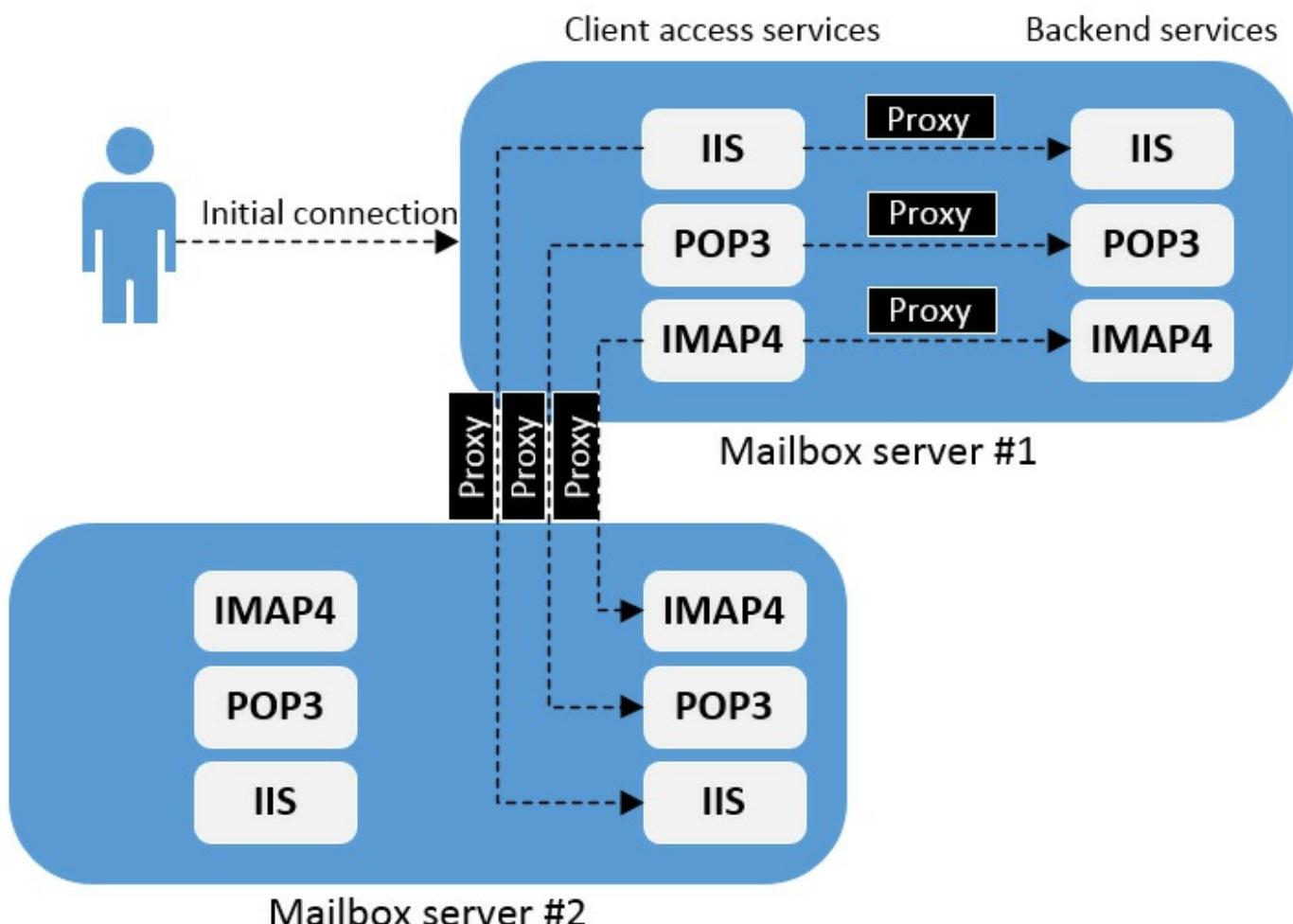


FIGURE 2-1 How proxying works in Exchange Server 2016

## Redirection

If you have worked with Exchange Server for a long time, you have probably configured redirection in Exchange Server so that users can get to Outlook on the web without remembering a special URL. While your actual Outlook Web App (OWA) URL might be <https://mail.contoso.com/owa>, redirection enables users to go to <https://mail.contoso.com> and automatically connect to OWA. Using redirection improves the user experience. But beyond the redirection to the URL with /owa, redirection can also be used to automatically redirect users from HTTP to HTTPS. For example, if a user tries to go to <http://mail.contoso.com/owa>, the user is redirected to <https://mail.contoso.com/owa>, which can also improve the user experience. There are a few points to keep in mind about redirection:

- Exchange Server 2016 automatically redirects requests to /owa. Automatic redirection is also part of Exchange 2013 Cumulative Update 6 and later. For Exchange implementations using older versions, an administrator must manually configure redirection.
- Redirection from HTTP to HTTPS must be configured by an administrator. You can configure the redirection by using an IIS custom error page. Configure an error page for the 403.4 status code, and then have the error page respond with a 302 direct to your URL with HTTPS, as shown in [Figure 2-2](#).

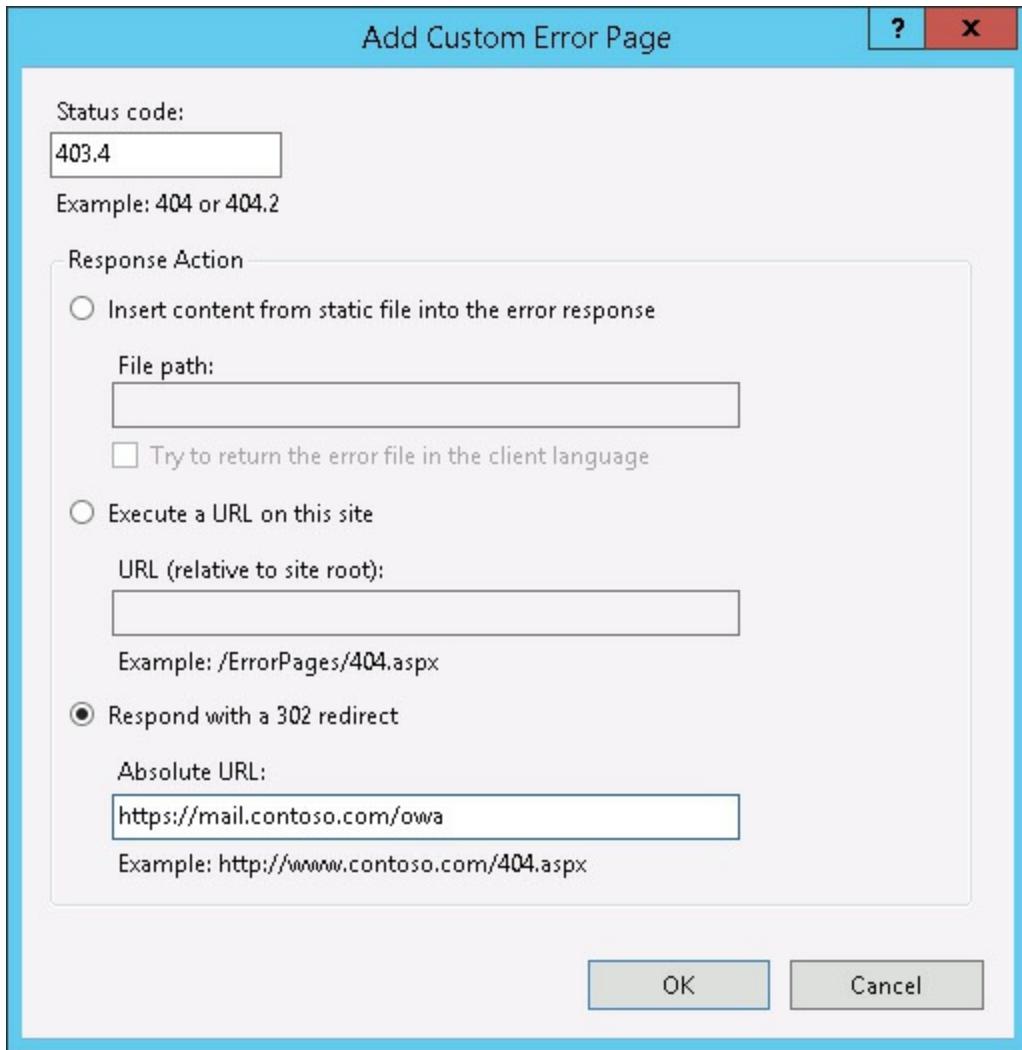


FIGURE 2-2 An IIS custom error page



### Exam Tip

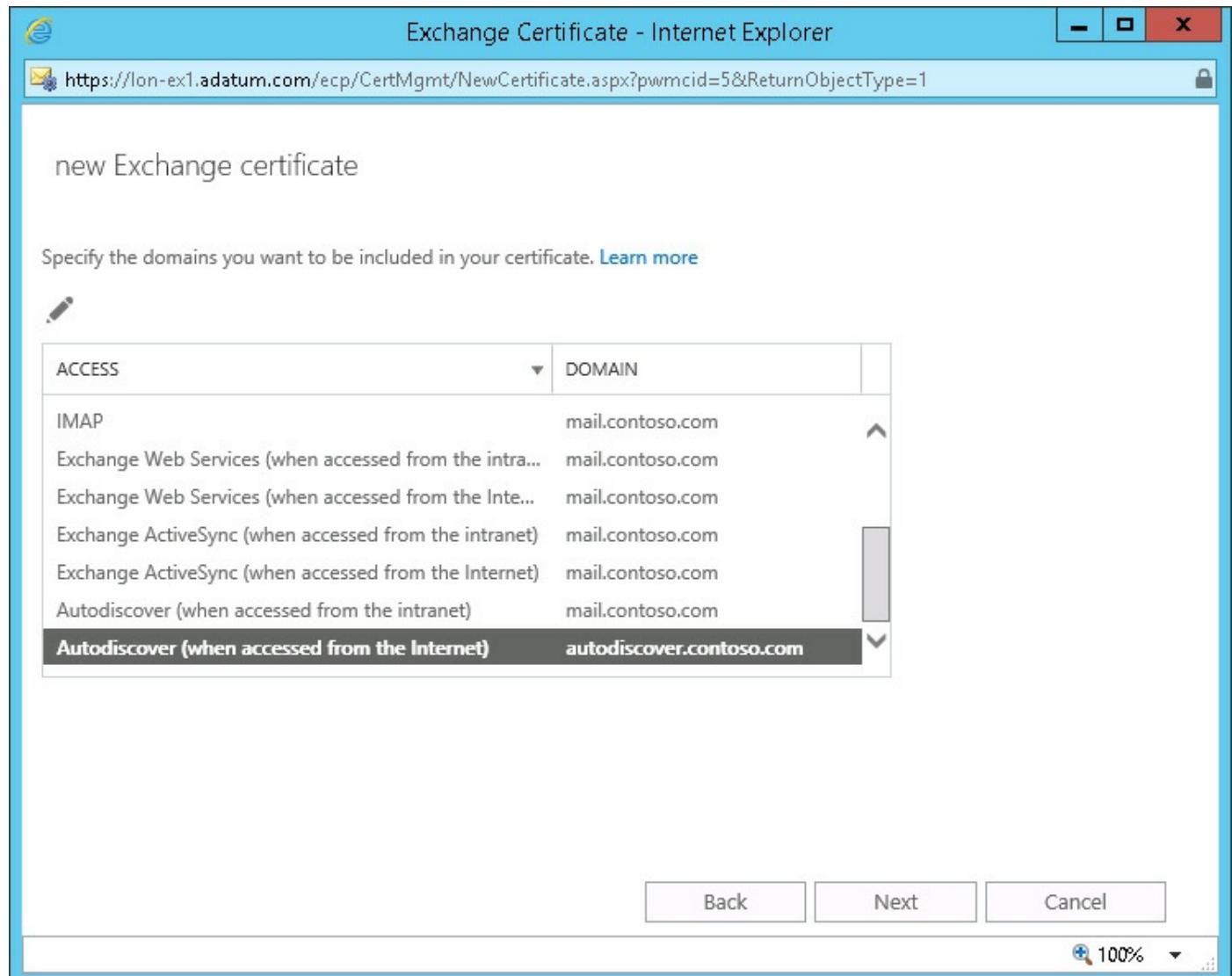
To prepare for the exam, consider implementing the HTTP to HTTPS redirection. It is quick and easy and helps cement the information into memory.

## Plan and deploy certificates

Certificates are a critical element of your Exchange Server implementation. When certificates aren't properly configured, users might get alarming warning messages in Outlook or in Outlook on the web. In some cases, Exchange Server functionality is degraded or non-functional when certificates are misconfigured. By default, self-signed certificates are created during the installation of Exchange Server. For backend mailbox services, self-signed certificates are sufficient, but for Client Access services, self-signed certificates should be swapped out for third-party certificates.

Planning for certificates is closely related to planning for namespaces, as discussed earlier in this section. Because certificates are tied to all of the fully qualified domain names (FQDNs) that you use in your environment, you can't obtain certificates until you know all of the FQDNs that will use SSL. The following scenarios look at certificate use in a simple configuration and a complex configuration:

- **Simple configuration** In a simple configuration, use one Autodiscover FQDN and one other FQDN for everything else. Using this configuration, you can obtain a single certificate containing two FQDNs (following the [contoso.com](#) examples earlier, [autodiscover.contoso.com](#) and [mail.contoso.com](#)). This configuration is viable if you use split DNS and all clients go to the same FQDNs, regardless of their network location. In this configuration, a single certificate can be used across all of your Exchange servers. In [Figure 2-3](#), the certificate wizard is configured to use two FQDNs.



**FIGURE 2-3** The configuration of FQDNs during a new certificate request

- **Complex configuration** In a complex configuration, your environment requires multiple FQDNs. A complex configuration can be the result of one or more factors such as the lack of split DNS, multiple domain names being used for email services, country/region-specific domain names, hybrid or mixed environments, and environments in the middle of a migration. In a complex configuration, it is often necessary to obtain multiple certificates. You are often required to use different certificates on different Exchange servers, depending on their location and version. Not only is the initial planning for a complex configuration time consuming, but the implementation and ongoing maintenance is as well. Certificates must be renewed occasionally and the more you have, the more time consuming it is to maintain them.

One method to simplify certificate management is to use a wildcard certificate. A wildcard certificate can be used for all FQDNs in a single domain. For example, if you use a wildcard certificate for \*.contoso.com; it would also handle requests to [autodiscover.contoso.com](#), [mail.contoso.com](#), and any other FQDN for the contoso.com domain. The downside of this method is that wildcard certificates can potentially be misused by a malicious person if they gain access to your Exchange servers. For example, a malicious person could reuse the wildcard certificate for a malicious website and use your domain and certificate to trick visitors into believing the website is legitimate.

When planning for certificates, remember the following good practices:

- Use a third-party certificate authority for your certificates. These certificates are widely trusted, quickly available, and you get support if issues arise.
- Use a single certificate for everything, when possible. To reduce the administrative overhead of managing your Exchange Server environment, you should use a simple configuration that requires less administrative management. You should reduce your total host name list as part of this configuration. Having two FQDNs is ideal.
- Obtain certificates that expire in a few years. To reduce administrative overhead, obtain certificates that expire in three to five years. Having certificates that expire in one year increases administrative overhead. Performing certificate maintenance and/or renewal every year also puts your organization at an elevated risk for an outage or degradation of services during maintenance periods.
- Use a Subject Alternative Name (SAN) certificate so you can have multiple FQDNs on a single certificate. This helps to simplify your configuration and reduces administrative overhead.

After you've finished planning your certificate strategy, you need to know how to deploy certificates. The high-level process for deploying certificates is straight

forward:

1. Create a new certificate request. You can do this through the Exchange Admin Center (EAC) or through PowerShell. Many administrators find the EAC simpler for certificate requests.
  2. Send the certificate request to a third-party certificate provider and purchase a SAN certificate.
  3. Download the SAN certificate from the third-party vendor.
  4. Install the certificate on all applicable Exchange servers.
  5. Enable the certificate for the appropriate services on the servers.
- 



### Exam Tip

Certificates are a complex topic. But to prepare for the exam, stick to learning only what you need to deploy an Exchange environment in various scenarios.

---

---

### Need More Review? Digital Certificates and Encryption in Exchange

You can find more information about how digital certificates and encryption work in Exchange Server 2016 on TechNet at

[https://technet.microsoft.com/library/dd351044\(v=exchg.160\).aspx](https://technet.microsoft.com/library/dd351044(v=exchg.160).aspx).

## Plan and configure authentication

Whether you are using Outlook or a web browser, authentication must occur when you connect to Exchange services. The authentication type used is based on the location of the client computing device, whether the client computing device has connectivity to the domain's domain controllers, and the configuration of Internet Information Services (IIS) depending on which service is being used.

Outlook uses two authentication methods, Kerberos and NTLM. Here are the situations when each is used:

- **Kerberos** Kerberos is the default protocol. Outlook uses this option when the client computing device is joined to the domain where the Exchange Server resides and when the device has connectivity to the domain's domain controllers.
- **NTLM** NTLM is often used when Kerberos doesn't work and can be considered as a fallback plan for Kerberos. Also, NTLM doesn't offer as much scalability as Kerberos.

When you use a browser to access Exchange services, such as Outlook on the web, you are often presented with forms-based authentication (FBA). This type of authentication requires you to manually type your credentials to sign in. There are other variations of forms-based authentication as well:

- **Integrated authentication** This type of authentication enables users to automatically sign in if they are already signed in to the internal domain. Integrated authentication is rarely used for Outlook on the web because most organizations need to provide users with access to Outlook on the web even when they are using a personal computer or are outside of the domain. Integrated authentication does not work in these scenarios.
- **Basic authentication** This type of authentication uses HTTP. You should use SSL any time you use basic authentication. One downside to Basic authentication is that browsers can cache credentials. Users need to be aware of credential caching and avoid using that feature if they use a shared computer, such as a public computer at an airport or library.
- **Digest authentication** This type of authentication is similar to Basic authentication but sends hashed passwords instead of plain text passwords. Unlike Basic authentication, this type of authentication requires passwords to be stored with reversible encryption in Active Directory. Reversible encryption is considered insecure. Therefore, you should not use Digest authentication, even with SSL.

Authentication for Exchange is straightforward in a simple environment, but when you start adding reverse proxy servers, authentication begins to become more complex, especially during initial setup and during troubleshooting later on. For the exam, you should know that if you use a reverse proxy for Outlook on the web or Outlook Anywhere, you should configure IIS for Basic authentication. This is because Kerberos and NTLM do not work if the reverse proxy examines the communication or modifies it in any way. Another scenario where you should configure IIS for Basic authentication is when you use pre-authentication with a reverse proxy. Pre-authentication is when a reverse proxy, or similar solution, authenticates users with the intention of sending their credentials to whichever backend services they use thereafter. In that situation, you should also configure IIS for basic authentication. By doing so, you ensure that users only need to authenticate once. If you don't use basic authentication, users must authenticate twice. For example, without Basic authentication, users attempting to access Outlook on the web receive FBA from the reverse proxy and FBA from Outlook on the web.

# **Plan, deploy, and configure Autodiscover, Outlook Anywhere, Outlook MAPI over HTTP, Exchange Web Services, Outlook on the web, Exchange Admin Center, Exchange ActiveSync, POP3, and IMAP4**

This section covers a wide variety of technologies. They are grouped together for the exam skills because their configuration and troubleshooting aspects are similar. They each have URLs, they each depend on certificates, and they are each tied to client connectivity or administrative connectivity. For each of these technologies, you must understand the impacts of namespaces and certificates and how to manage internal and external availability. You must take these key planning considerations into account when designing your Exchange environment. This section covers key information regarding Autodiscover, Outlook Anywhere, Outlook MAPI over HTTP, Exchange Web Services, Outlook on the web, Exchange Admin Center, Exchange ActiveSync, POP3, and IMAP4.

## **Plan, deploy, and configure Autodiscover**

When working with Autodiscover, you will work with your namespaces and certificates. However, you already reviewed those facets earlier in this chapter. By now, you know that you need to have an FQDN for Autodiscover such as [autodiscover.contoso.com](https://autodiscover.contoso.com). And you know that you need to have a valid SSL certificate that has your Autodiscover FQDN as one of the names on the certificate. In addition to these requirements, there are other facets of Autodiscover you need to be aware of:

- There is a Service Connection Point (SCP) containing the Autodiscover URLs. When there is more than one SCP, and therefore more than one Autodiscover URL, the SCP for the server in the same Active Directory Domain Services (AD DS) site, or nearest site, is given priority.
- By default, the SCP for the first Exchange server contains an Autodiscover URL tied to the server's hostname. For example, a server named ex01.contoso.com would register an SCP for Autodiscover using <https://ex01.contoso.com/Autodiscover/Autodiscover.xml>. This naming convention isn't ideal, especially if you have more than one Exchange server and you plan to do load balancing. It is considered a good practice to use a URL that isn't associated with a specific server, such as <https://autodiscover.contoso.com/Autodiscover/Autodiscover.xml>. Use the Set-ClientAccessServer cmdlet to update the SCP.
- For external clients, such as computers outside your network and not joined to your domain, you need to understand how they locate your Exchange environment. Imagine a scenario where your organization uses the contoso.com domain. By default, the Outlook client tries to find the Autodiscover service by using

<https://contoso.com/autodiscover.xml>. If the Outlook client doesn't find it, it tries <https://autodiscover.contoso.com/autodiscover/autodiscover.xml>. The client is not able to connect if it cannot find the Autodiscover service at either URL.

---



### Exam Tip

If you are configuring Outlook for the first time on a computer and Outlook is not able to automatically configure the email settings, there is probably a configuration issue with Autodiscover.

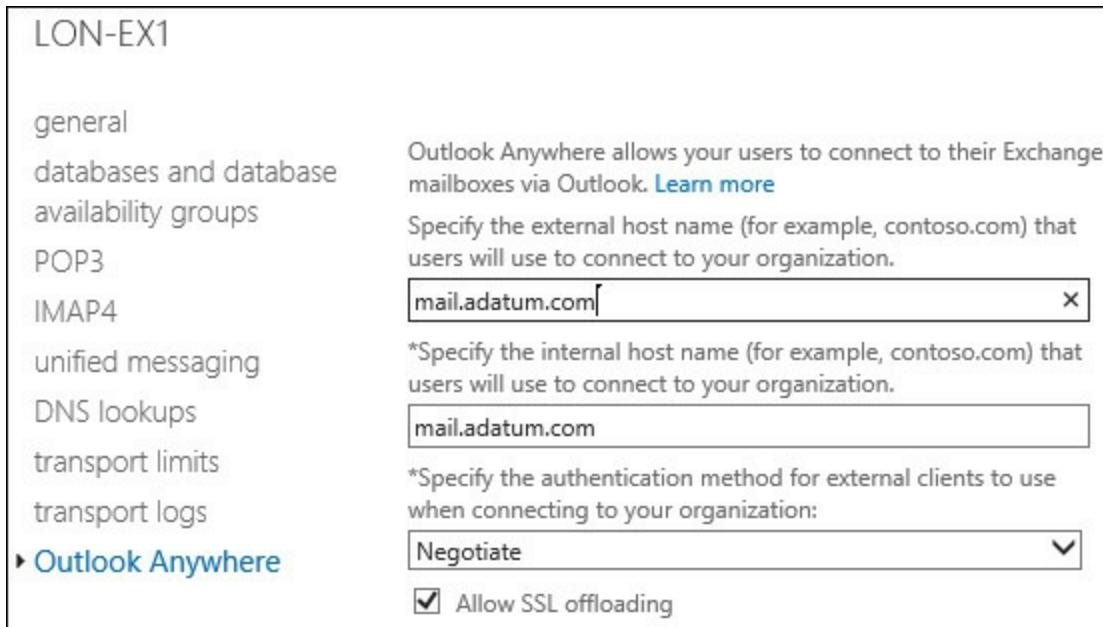
---

## Plan, deploy, and configure Outlook Anywhere

Outlook Anywhere allows users to use Outlook and connect to their Exchange server from outside of the company network, such as over the Internet. To effectively deploy and manage Outlook Anywhere, you must be aware of the planning components involved, such as network considerations, deployment considerations, and configuration options:

- Outlook Anywhere communication uses RPC over HTTP/HTTPS, meaning that RPC communication is encapsulated in standard HTTP/HTTPS. This greatly simplifies a firewall configuration because only TCP port 443 needs to be opened.
- When you deploy and configure Outlook Anywhere, use the `Test-OutlookConnectivity` cmdlet to test communication for Outlook Anywhere. This test is also helpful when troubleshooting Outlook Anywhere connectivity.
- In Exchange Server 2013, Outlook Anywhere was the default communication method used by Outlook, regardless of the client's location.
- By default, in Exchange Server 2016, Outlook uses MAPI over HTTP. Use RPC over HTTP, Outlook Anywhere, if MAPI over HTTP doesn't work.
- You can configure an internal and external FQDN for Outlook Anywhere. Use the same FQDN if you have split DNS. You must specify different FQDNs in the configuration if you don't have split DNS.

[Figure 2-4](#) illustrates the configuration of Outlook Anywhere.



**FIGURE 2-4** The configuration of Outlook Anywhere

Also remember that RPC over HTTP is equivalent to Outlook Anywhere.

### Quick check

- What would the URLs for an internal and external configuration be in an environment that uses split DNS?

### Quick check answer

- The URLs for split-DNS can be the same, [mail.adatum.com](mailto:mail.adatum.com) for external clients and [mail.adatum.com](mailto:mail.adatum.com) for internal clients.

## Plan, deploy, and configure Outlook MAPI over HTTP

While MAPI over HTTP is the default protocol for Outlook in an Exchange Server 2016 environment, there are some key details that you need to know for the exam:

- If you implement Exchange Server 2016 in an existing environment that has Exchange 2013, MAPI over HTTP is not enabled by default.
- If you upgrade your Exchange 2010 environment (all servers) to Exchange 2016, MAPI over HTTP is enabled.
- MAPI over HTTP can be enabled at the organization level (all mailboxes) or at the individual mailbox level. This is important to know, especially for troubleshooting scenarios.
- To configure MAPI over HTTP, you must configure the following items:
  - **Virtual directories** There is an internal URL and an external URL for the MAPI

virtual directory. Outlook uses these URLs to connect to Exchange. Use the Set-MapiVirtualDirectory cmdlet to configure the virtual directories.

- **Network devices** If you use a reverse proxy, load balancer, or firewall, you might need to configure them to enable communication to the MAPI over HTTP virtual directory.

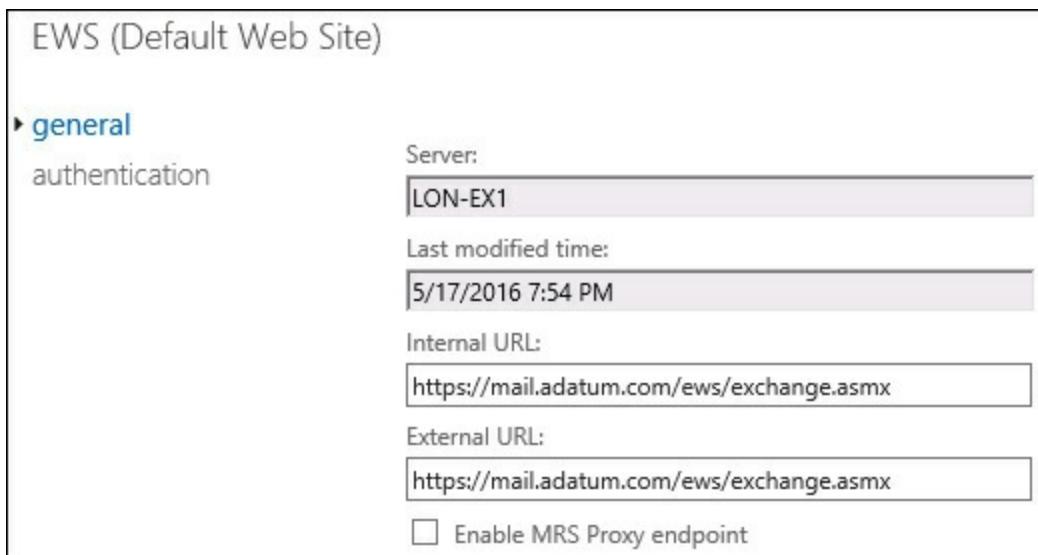
When your environment is ready for MAPI over HTTP, run the following command to enable it:

[Click here to view code image](#)

```
Set-OrganizationConfig -MapiHttpEnabled $True
```

## Plan, deploy, and configure Exchange Web Services

Managing Exchange Web Services (EWS) should not be time intensive, but there are a few things to keep in mind. Like many other Exchange services, EWS has internal and external URLs. You need to configure the URLs depending on your environment. For most environments, it is considered a good practice to use the same namespace across all of the services. The domain names you use for EWS also need to be on the SSL certificate you are using. [Figure 2-5](#) illustrates the EWS URLs in use.



**FIGURE 2-5** The configuration of FQDNs for EWS

Use the Set-WebServicesVirtualDirectory cmdlet to set your URLs. For example, to set your internal and external URLs to use <https://mail.adatum.com/ews/exchange.asmx> for a server named EX-01, run the following command:

[Click here to view code image](#)

```
Set-WebServicesVirtualDirectory -Identity EX-01\EWS (Default Web Site) -  
ExternalUrl  
https://mail.contoso.com/EWS/exchange.asmx -InternalUrl  
https://mail.contoso.com/EWS/  
exchange.asmx
```

## **Plan, deploy, and configure Outlook on the web**

Outlook on the web also has virtual directories. These directories should be configured and should also use domain names that are part of your SSL certificate. You also have the option to configure the authentication type. Forms-based authentication is set by default, but you can switch to Integrated Windows authentication, Digest authentication for Windows domain servers, or Basic authentication.

Some lesser used configuration items are from the features and file access options.

- You can enable or disable features that are available for Outlook on the web users. Features include items like instant messaging, text messaging, and email filtering. All of these features are enabled by default.
- You can configure attachment access based on whether users are connecting from a private computer or a public computer. For example, you can disable attachment access for public computers.
- One of the initial configuration steps is to configure the external URL for Outlook on the web. This enables users to access the service from any network.

## **Plan, deploy, and configure Exchange Admin Center**

For the Exchange Admin Center (EAC), you need to configure the internal and external URL, as well as the authentication type. When configuring URLs, it is considered a good practice to use a single URL for internal and external use. It simplifies the administrative experience. The default authentication for EAC is forms-based authentication. This authentication is sufficient for most organizations, however you can switch the authentication type to Integrated Windows authentication, Digest authentication for Windows domain servers, or Basic authentication.

## **Plan, deploy, and configure Exchange ActiveSync**

In addition to considering internal URLs, external URLs, and authentication, there are other aspects of Exchange ActiveSync (EAS) to keep in mind.

You should be familiar with the following information and tasks:

- **Control device access** You can dictate which mobile devices can connect to Exchange ActiveSync by using device access rules. For mobile devices specified in a rule, you can allow access, block access, or quarantine the device and enable an administrator to decide. In the example shown in [Figure 2-6](#), the Exchange ActiveSync access settings are set to allow access to all devices, to email the administrator when devices are quarantined, and to send a customized message to quarantined devices.

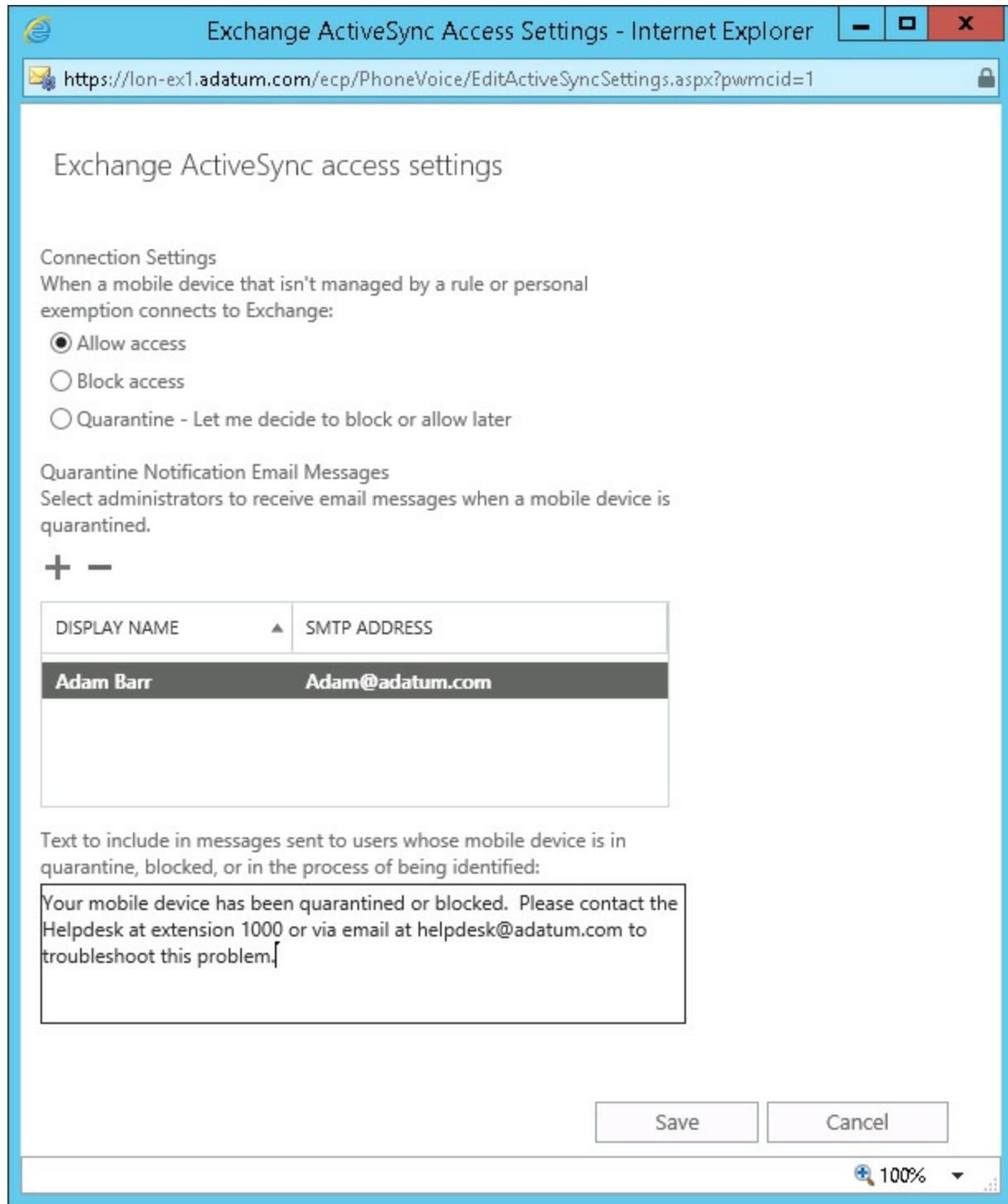


FIGURE 2-6 The configuration of the Exchange ActiveSync access settings

- **Control quarantined devices** When devices are quarantined, you can use EAC to block or allow them. You can also create a rule based on the device type.
- **Create security policies for ActiveSync devices** Email and calendar data often contains information meant only for internal use. To help protect access to email and calendar data, you can create a variety of security policies to enhance the security on ActiveSync mobile devices. The following options are available:

- **Require a password or do not require a password** In the vast majority of environments, it is considered best practice to require a password.
- **Enable or disable simple passwords** For moderate and high security environments, disable simple passwords.
- **Require an alphanumeric password** This is a good practice to increase the security of your mobile devices.
- **Specify a minimum password length** Longer minimum password lengths ensure a higher level of security for your mobile devices. In many environments six characters is sufficient. For high security environments, 10 characters is typical.
- **Configure Exchange to wipe devices after a specified number of failed logon attempts** Configure this setting so that users only have a limited number of attempts to enter the correct password. Be careful when determining the attempt threshold because if you set the threshold too low, a legitimate user might wipe a device by accident. It isn't uncommon for someone's child to be playing with a phone and wipe the device without realizing it. Your helpdesk might get extra support requests if the number is too low.
- **Require user sign-in for idle devices based on the number of minutes idle** This is an important setting, especially for devices that are lost or stolen. For example, if you set your mobile device down in a coffee shop and it is stolen, extended idle time might allow the thief to gain access to your data. In high security environments, configure this setting to minimize the number of idle minutes. One minute is common.
- **Set a maximum password age** The maximum password age is often set at 90 days or 180 days. Anything less and the user experience is degraded without much benefit to the overall security of the environment.
- **Set password history so users cannot reuse a specific number of their old passwords** Use password history to prevent users from reusing recently expired passwords. This helps maximize mobile device security.
- **Remotely wipe mobile devices to clear email data from the device** This setting is important if a device is lost or stolen. Remotely wiping devices is a common task as it helps minimize data loss for lost or stolen devices. This setting should be enabled in all environments.
- **Run reports to show ActiveSync usage and devices** It is recommended to track which devices are connecting to your environment, especially if you have a support policy only allowing specific device types and models. If a security issue is reported for specific device types or versions, reports can help you locate

impacted devices and work with the users to mitigate the issue.

[Figure 2-7](#) shows a mobile device mailbox policy with security settings chosen for an environment with moderate security requirements.

The screenshot shows a web-based configuration interface for a mobile device mailbox policy. The title bar reads "Mobile Device Mailbox Policy - Internet Explorer". The URL in the address bar is <https://lon-ex1.adatum.com/ecp/PhoneVoice/EditMobileDeviceMailboxPolicy.aspx?pwmcid=3&ReturnObjectType=1&id=06c>. The left sidebar has a tree view with "Default" at the top, followed by "general" and "security". The "security" node is expanded, showing several configuration options with checkboxes and input fields:

- Require a password
- Allow simple passwords
- Require an alphanumeric password
  - Password must include this many character sets:  
3
- Require encryption on device
- Minimum password length:  
6
- Number of sign-in failures before device is wiped:  
15
- Require sign-in after the device has been inactive for (minutes):  
5 minutes
- Enforce password lifetime (days):  
90 days
- Password recycle count:  
5

At the bottom right are "Save" and "Cancel" buttons. A status bar at the bottom right shows "100%" and a zoom control.

**FIGURE 2-7** The configuration of a mobile device mailbox policy

## Plan, deploy, and configure POP3

You configure POP3 settings at the server level. Each server has its own set of POP3 settings. For the exam, the primary information you need to know is:

- By default, only secure TLS connections are allowed. Optionally, you can use Basic authentication or Integrated Windows authentication, but that means the

username and password is sent over the network in plain text.

- By default, POP3 listens on TCP port 110, which is not secured, and TCP port 995, which is SSL secured. These settings reflect the industry standard POP3 ports. You can change the default settings, but it is best to maintain the default ports. POP3 clients automatically try the default ports. Firewalls and other security software flag TCP port 110 and TCP port 995 as POP3 traffic, which is helpful for initial setup and troubleshooting.

Even though this option is available, it is a good practice to eliminate POP3 in your environment. POP3 is an inefficient protocol and you don't have many options for controlling the data.

## Plan, deploy, and configure IMAP4

You configure IMAP4 settings at the server level, each server has its own IMAP4 settings. For the exam, the primary information you need to know is:

- By default, Exchange 2016 allows IMAP4 connections over a secure TLS connection. Optionally, you can change the default and use Basic authentication or Integrated Windows authentication, but that means the username and password is sent over the network in plain text.
- By default, IMAP4 listens on TCP port 143, which is not secured and TCP port 993, which is SSL secured, and is considered to be the industry standard for IMAP4 ports. You can change these default settings, but it is best to maintain the default ports because IMAP4 clients automatically try the default port while firewalls and other security software flag default ports as IMAP4 traffic, which is helpful for initial setup and troubleshooting.

Like POP3, it is a good practice to eliminate IMAP4 in your environment. IMAP4 is an inefficient protocol and you don't have many options for controlling the email data.

## Plan, deploy, and configure Office Online Servers

Office Online Server (OOS) is an optional component of your Exchange environment. It enables users to view supported email attachments in Outlook on the web without having to download the attachments or use a locally installed application. This feature is helpful for users that use personal devices where they might not have applications installed to view certain types of attachments.

For the exam, be aware of the following information:

- OOS is available for volume licensing customers only. From an exam perspective, obtaining volume licensing could be a first step in a scenario involving OOS.
- You can configure OOS at the organization level or at the server level. If you are

in a mixed environment with older versions of Exchange Server running alongside Exchange 2016, you must configure OOS at the server level to avoid issues with older versions of Exchange Server using OOS.

- Like other Exchange services, OOS has an internal and an external URL.
- If you deploy multiple OOS servers, each server requires its own FQDN. This is unlike the other Exchange services, so expect the exam to tie this into some scenarios.

Later in this chapter, we discuss some planning and deployment information for OOS with regard to namespace planning and load balancing.

## **Plan, create, and configure Offline Address Book**

The Offline Address Book (OAB) is a copy of an address book, often referred to as the Global Address List, downloaded by Outlook clients so that address book information can be used by clients even when they are not connected to an Exchange server. In Exchange Server 2016, Exchange generates an updated OAB every 8 hours. For most environments, the default OAB generation of every 8 hours is sufficient. You might need to reconfigure your environment so that the OAB generates more often, such as every 4 hours, if you regularly have a large number of new workers starting at or departing from the company.

There is an internal URL and an external URL that you can configure for distributing the OAB over HTTP/HTTPS. You must set these URLs up as part of the initial deployment and configuration. The names you use must match your certificate's namespace.

## **Plan, create, and configure hierarchical address lists**

A hierarchical address book (HAB) is an address list based on your organization's hierarchy. It is also customizable based on your organization's requirements. For example, you can set up a hierarchical address book based on your organization's departments, such as Sales, Engineering, and Finance. From there, you can use a seniority index to organize people in the departments based on their seniority. In this instance, the person running the sales department would be at the top of the sales hierarchy, sales managers are in the middle, and salespeople are at the bottom. A hierarchical address book is an optional address list and must be manually configured to make it usable.

The following steps outline the process to enable and configure an HBA. In this example, the company name is A. Datum Corporation, but you would use your own company name in your environment. In a typical organization, you might have several parent groups, child groups, and even child groups of child groups. The following steps

create a parent group named Engineering with one child group named Software.

1. Create an organizational unit (OU) named HAB. The location isn't relevant. It is a good idea to have it underneath an OU that stores distribution groups to keep the root OU structure simple.

2. Run the following command to create the root level HAB.

[Click here to view code image](#)

```
New-DistributionGroup -Name "Adatum, Inc" - DisplayName "Adatum" - Alias  
"AdatumRoot" - OrganizationalUnit "adatum.com/HAB" - SamAccountName  
"AdatumRoot"  
- Type "Distribution"
```

3. Run the following command:

[Click here to view code image](#)

```
Set-OrganizationConfig - HierarchicalAddressBookRoot "Adatum" command
```

This enables HABs for the organization and sets the distribution group with a display name of "Adatum" as the HAB root. This is usually the company name or the top-level name of a hierarchy.

4. Run the following command to create a new distribution group that you can use as a departmental top-level hierarchy:

[Click here to view code image](#)

```
New-DistributionGroup - Name "Engineering" - DisplayName "Engineering" -  
Alias  
"Engineering" - OrganizationalUnit "adatum.com/HAB" - SamAccountName  
"Engineering"  
- Type "Distribution"
```

5. Run the following command to configure the new distribution group to be part of the hierarchical structure:

[Click here to view code image](#)

```
Set-Group - Identity "Engineering" - IsHierarchicalGroup $True
```

6. Run the following command to create the Software name:

[Click here to view code image](#)

```
New-DistributionGroup - Name "Software" - DisplayName "Software" - Alias  
"Software"  
- SamAccountName "Software"
```

7. Run the following command to add the Software distribution group as a member of the Engineering hierarchy:

[Click here to view code image](#)



### Exam Tip

Think about HABs if you are presented a situation that calls for simplifying the address list or helping users locate people in the address list.

---

## Plan, deploy, and configure address book policies

Sometimes you need to configure your environment so that certain users see one view of an address book while other users see a different view. You can achieve this by using Address Book Policies (ABPs). ABPs do not change the actual address lists, but instead show the target of the ABP a filtered view of the global address list. An ABP is an alternative to creating multiple global address lists. For many administrators, an ABP is simpler and easier to work with than multiple global address lists.

---



### Exam Tip

The exam might not use the term address book policies. Instead, it might use global address list segmentation or global address list segregation.

---

When you create a policy, you must specify the following items:

- A global address list
- An offline address book
- A room list
- Address lists related to the policy

To complement an ABP, turn on the Address Book Policy Routing agent, which is a transport agent that dictates how email recipients are resolved. This enables you to ensure that recipients not in an ABP are not viewable like other internal recipients. In other words, the organization information is not viewable and the recipients are displayed in a manner similar to an external user.

## Summary

- A unified namespace simplifies your environment but could degrade the user experience if some of your data centers are connected with high latency and/or low bandwidth connectivity.
- A dedicated namespace requires more administrative overhead to manage more

names and more certificates, but it can improve the user experience if your environment has some data centers with high latency and/or low bandwidth connectivity.

- You can use a multi-name digital certificate for your Exchange environment or a wildcard certificate. Certificates should be purchased through a third-party certificate authority that is well-known and trusted.
- Kerberos is the default protocol that Outlook uses for Exchange Server connectivity. However, HTML is sometimes used when Kerberos isn't functioning.

## Skill 2.2: Plan, deploy, and manage mobility solutions

In most environments today, using Exchange services on a mobile device is just as important as it is on a primary device such as a desktop or laptop computer. Many users switch back and forth between devices and device types and they expect to have the same positive experience no matter how they choose to access Exchange services. As the administrator, you need to be familiar with the technologies that can help make a mobile solution a success.

### This section covers how to:

- [Plan, deploy, and configure OWA for Devices, Outlook on the web policies, and mobile device mailbox policies](#)
- [Plan, deploy, and configure Allow Block Quarantine \(ABQ\)](#)
- [Plan, deploy, and configure Office Apps](#)

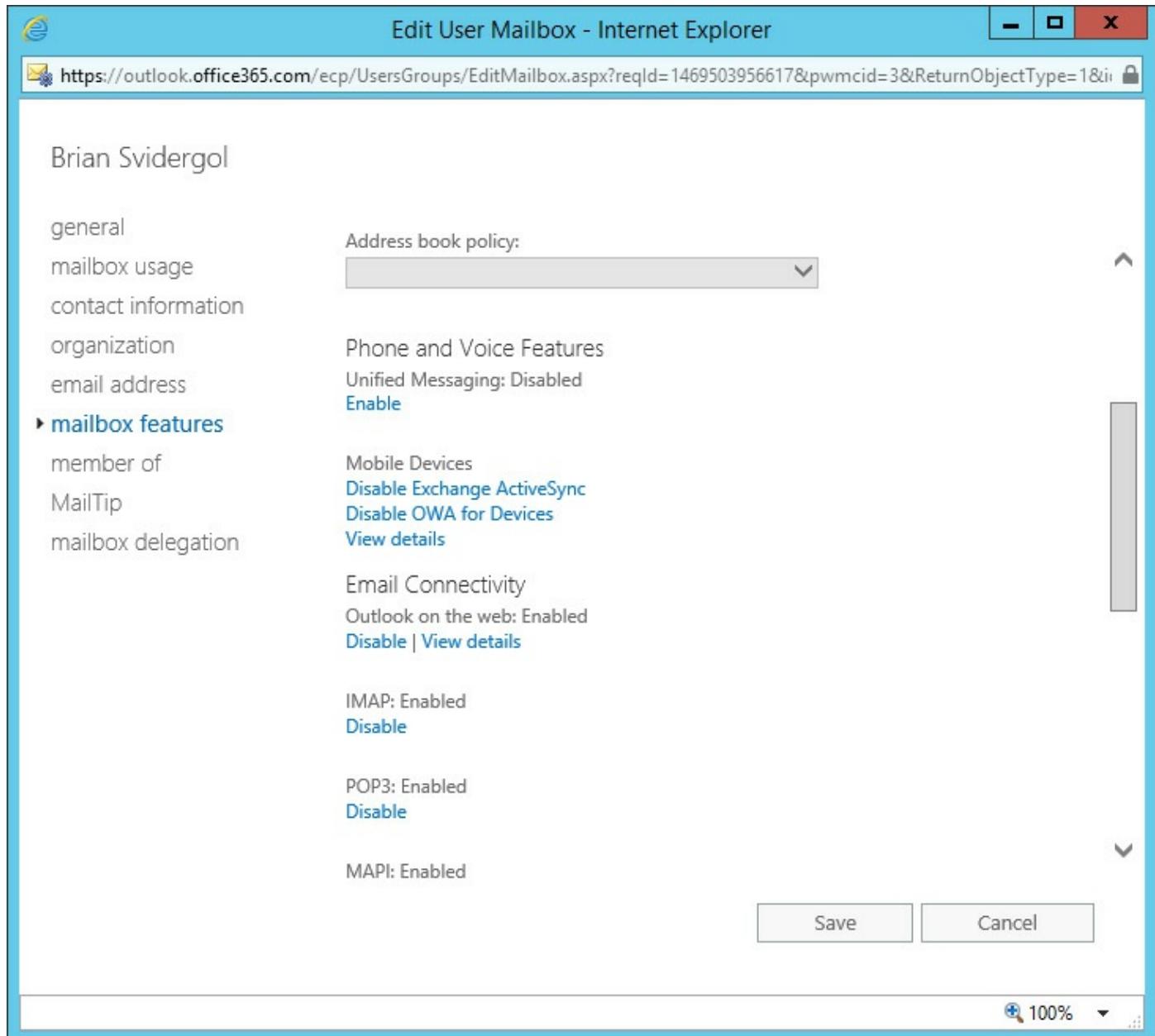
## Plan, deploy, and configure OWA for Devices, Outlook on the web policies, and mobile device mailbox policies

Managing mobile devices with Exchange Server can be as simple or as complex and restrictive as you need it to be. For example, a small business might enable all of their employees to use any device without restrictions and without requiring a device password. A large enterprise might enable employees to bring their own devices, but often requires a screen lock after idle time and a complex passphrase to unlock a device.

## **OWA for Devices**

Microsoft offers several methods to access email, calendar, and contacts from a mobile device. OWA for Devices refers to the OWA app for mobile operating systems such as iOS and Android. However, the OWA app has been replaced with the newer Outlook app, also available for iOS and Android. The Outlook app is now the primary method for accessing email data on a mobile device. The Outlook app functions as an ActiveSync client, requiring the appropriate configuration on the Exchange servers to function properly. By default, Exchange ActiveSync and OWA for Devices are enabled on Exchange servers. For the OWA app, think of it as an OWA wrapper and not an ActiveSync client, although it does support mobile device policies.

After you've decided to enable mobile device access, you can enable or disable access on a per-user basis from the mailbox features page of a user's mailbox, as shown in [Figure 2-8](#).



**FIGURE 2-8** Mailbox features at the mailbox level

Alternately, Exchange ActiveSync and OWA for Devices can be configured on individual mailboxes by using the Set-CASMailbox cmdlet. For example, to disable OWA for Devices for Marc's account, run the following command:

[Click here to view code image](#)

```
Set-CASMailbox -Identity Marc -OWAforDevicesEnabled $False
```

The OWA application functions more like Outlook on the web and requires the Office 365 push notification proxy to be configured, even if the Exchange organization is on-premises. To configure the push notification proxy from Exchange Server 2016 in the adatum.com domain, run the following command:

[Click here to view code image](#)



### Exam Tip

You need to configure OAuth authentication between your on-premises environment and Office 365 to ensure that push notifications function.

---

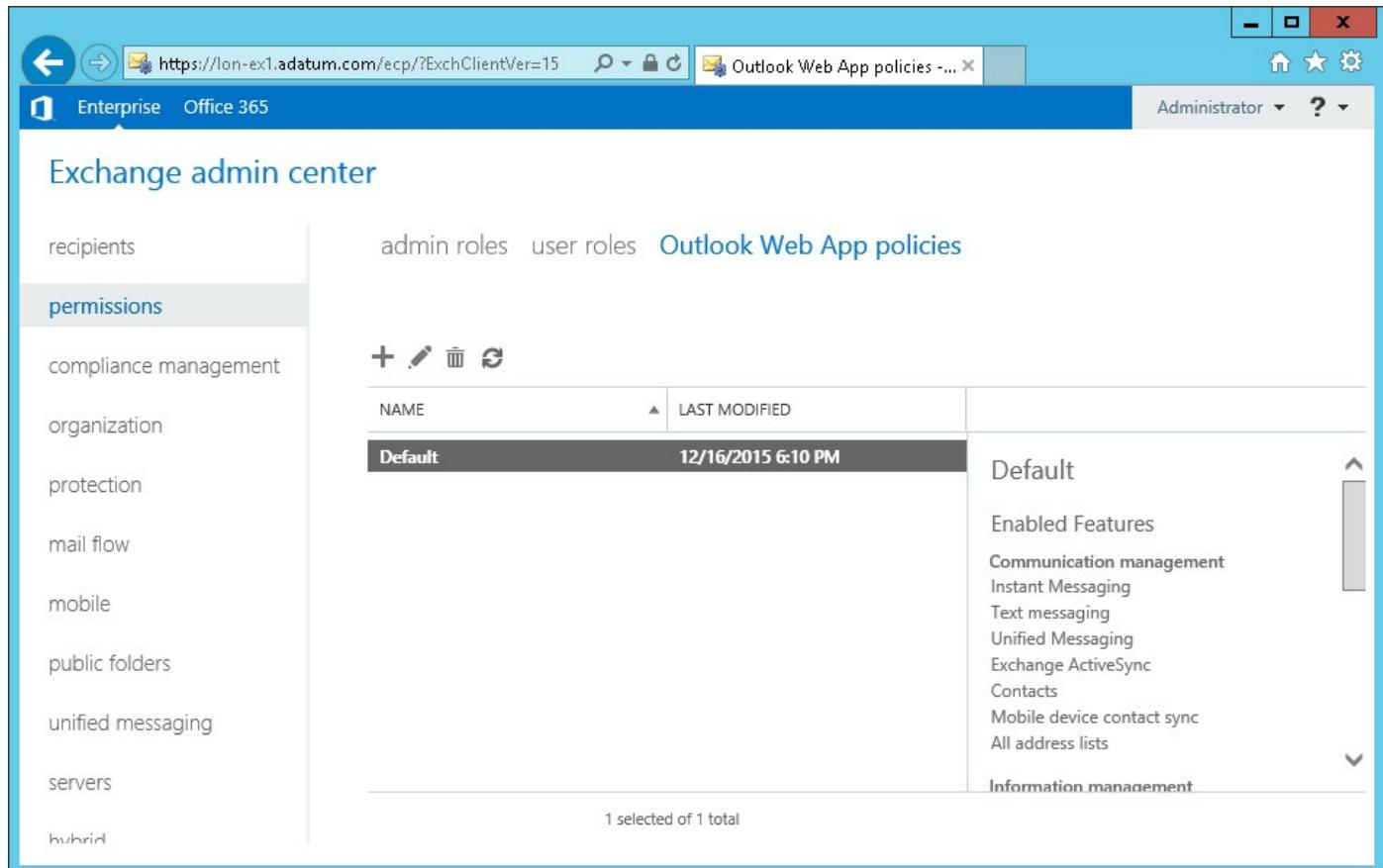
For this configuration to work, the organization must also be enrolled in Office 365 for business. After configuring the notifications, you can also test and monitor them by using the Invoke-MonitoringProbe cmdlet. For example, to test this on a server named EX01 in the adatum.com domain, run the following command:

[Click here to view code image](#)

```
Invoke-MonitoringProbe PushNotifications.Proxy\  
PushNotificationsEnterpriseConnectivityProbe -Server EX01.adatum.com
```

### Outlook on the web policies

By default, Outlook on the web is enabled for all mailboxes in an organization. All of the features and capabilities are also enabled per the default policy that is defined and applied. [Figure 2-9](#) shows the Outlook Web App policies page in the Exchange Admin Center.



**FIGURE 2-9** Outlook Web App policies and enabled features

Some categories of features that can be enabled or disabled by using an OWA policy include:

- Communication management
- Information management
- Security
- User experience
- Time management

As the administrator, you have the ability to enable or disable any of the features you want. For example, if you wanted to disable the user's ability to change passwords from Outlook on the web, modify the Security settings of a policy and then assign the policy to a mailbox. To disable password changes for an existing policy named NoPasswordChange, run the following command:

[Click here to view code image](#)

```
Set-OwaMailboxPolicy -Identity NoPasswordChange -ChangePasswordEnabled $False
```

After you have created or modified a policy and are ready to use the policy, you need to assign the policy to a mailbox. To assign a policy to a mailbox, use the Set-

CASMailbox cmdlet. For example, to assign the NoPasswordChange policy to Marc's mailbox, run the following command:

[Click here to view code image](#)

```
Set-CASMailbox -Identity Marc -OwaMailboxPolicy:NoPasswordChange
```

Assigning a policy through the EAC isn't as intuitive as it seems. A configured policy can be assigned to a mailbox under the Email Connectivity section in the Mailbox Features page, as shown in [Figure 2-10](#).

The screenshot shows the 'User Mailbox - Internet Explorer' window. The URL in the address bar is <https://lon-ex1.adatum.com/ecp/UsersGroups/EditMailbox.aspx?pwmcid=4&ReturnObjectType=1&id=0d432627-6b16-48c5-8>. The main content area displays the 'Administrator' mailbox features. On the left, a sidebar lists general mailbox settings: general, mailbox usage, contact information, organization, email address, and a expanded 'mailbox features' section. Under 'mailbox features', there are links for member of, MailTip, and mailbox delegation. The right side of the screen shows detailed configuration for various connectivity protocols and policies. For 'Email Connectivity', it shows 'Outlook on the web: Enabled' with 'Disable | View details' options. Other sections include 'Phone and Voice Features' (Unified Messaging: Disabled, Enable link), 'Mobile Devices' (Disable Exchange ActiveSync, Disable OWA for Devices, View details), 'IMAP: Enabled' (Disable link), 'POP3: Enabled' (Disable link), 'MAPI: Enabled' (Disable link), and 'Litigation hold: Disabled' (Enable link). At the bottom right are 'Save' and 'Cancel' buttons, and a status bar at the bottom right shows '100%'.

**FIGURE 2-10** Mailbox Features page

To configure an Outlook Web App policy for a specific mailbox, click the View Details link under Email Connectivity. This opens a pop-up window where you are able to browse the available policies in your organization. [Figure 2-11](#) shows an OWA

policy named NoPassword selected for a mailbox.

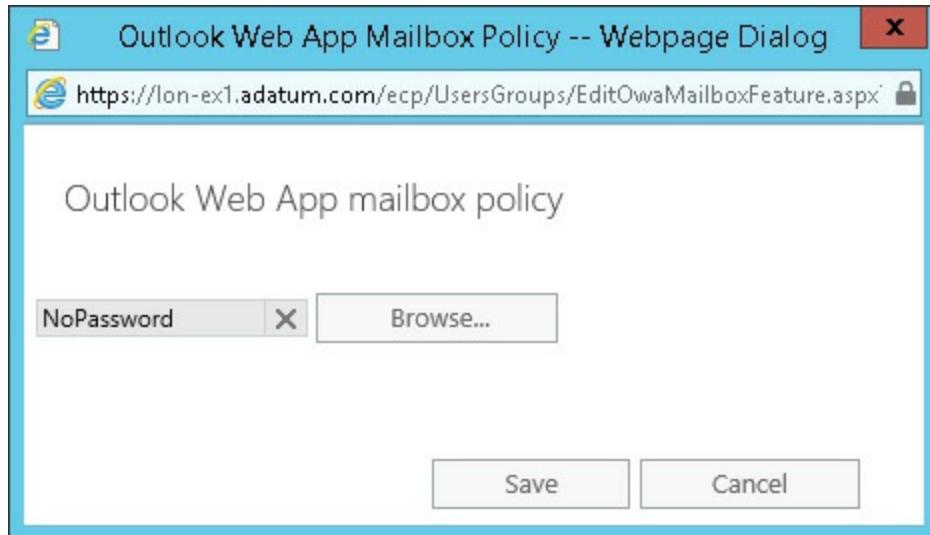
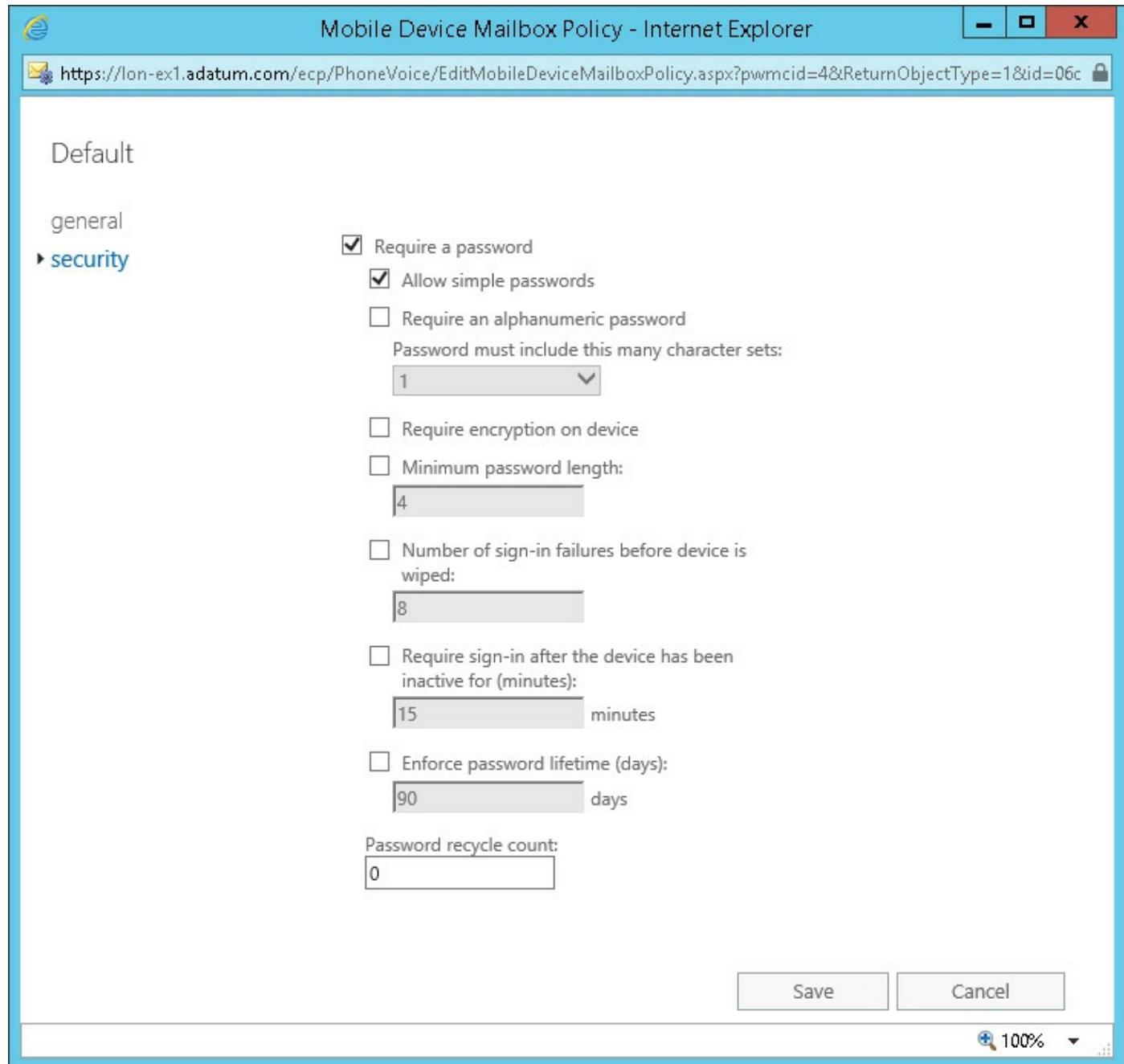


FIGURE 2-11 Selecting an Outlook Web App mailbox policy for a mailbox

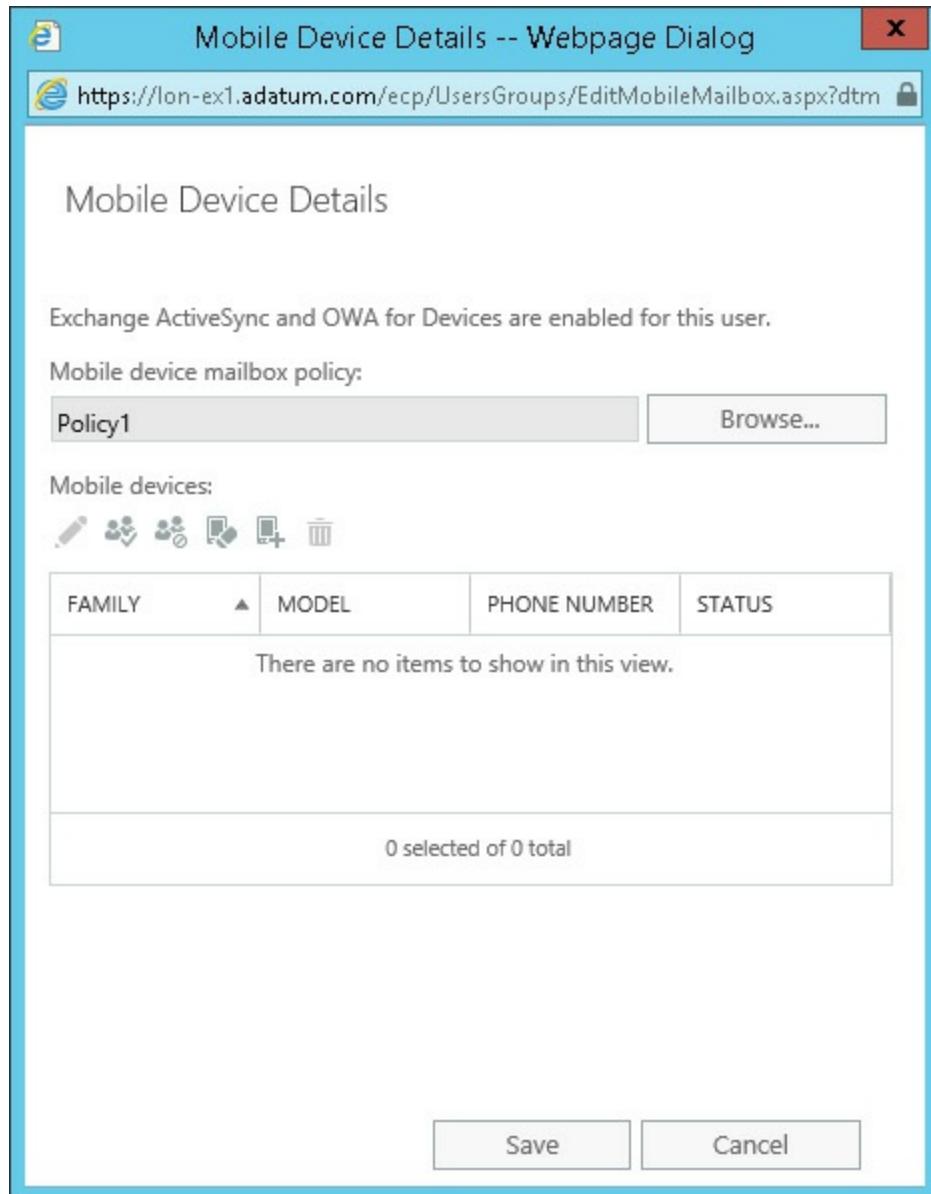
## Mobile device policies

Mobile devices can be managed from an Exchange environment by using a mobile device policy. A mobile device policy can require specific password lengths or types, encryption, lock screen timeouts, and more. [Figure 2-12](#) shows the security settings that can be defined by using a mobile device policy.



**FIGURE 2-12** Security settings available in a mobile device mailbox policy

Similar to OWA policies, mobile device policies can be applied to individual mailboxes. [Figure 2-13](#) shows a policy named Policy1 being applied to a specific mailbox.



**FIGURE 2-13** A mobile device Details page shows existing mobile devices associated with a user along with any associated mobile device mailbox policies

You can create a mobile device policy from PowerShell by using the New-MobileDeviceMailboxPolicy cmdlet. For example, to create a policy named Policy2 that allows simple passwords, run the following command:

[Click here to view code image](#)

```
New-MobileDeviceMailboxPolicy -Name Policy2 -AllowSimplePassword $True
```

When creating a new policy, you also have the option to allow or block devices that don't support the policies that are defined. With dozens of devices supporting ActiveSync, some devices might not support the security requirements of a policy. For example, this could happen if you require device encryption on a device that doesn't support encryption.

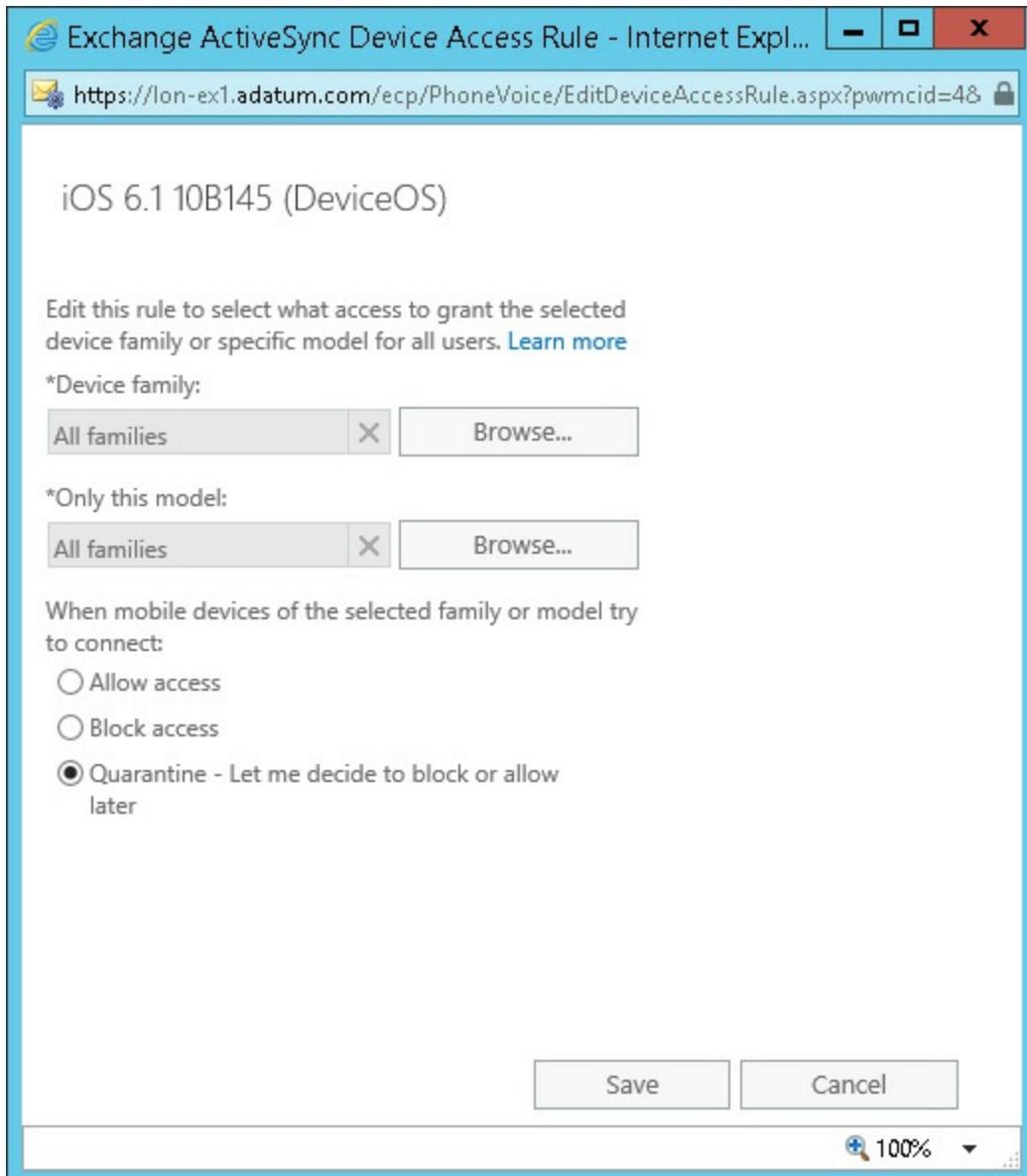
After you have a policy configured and ready, you can assign it to a mailbox by using PowerShell. For example, to assign Policy2 to Marc's mailbox, run the following command:

[Click here to view code image](#)

```
Set-CASMailbox -Identity Marc -ActiveSyncMailboxPolicy Policy2
```

## Plan, deploy, and configure ABQ

In addition to the policies for devices and web access, you can also prevent or quarantine devices that connect to the Exchange organization based on the device family or model type. It is helpful to limit devices to a specific family or model to simplify support and keep users informed of security updates and other important device information. [Figure 2-14](#) shows creating a device access rule to quarantine a device. To save the policy, you must select both the family and model types. Models only appear in the list of available devices after the devices attempts to connect to the server.



**FIGURE 2-14** A device access rule limits access to ActiveSync based on the family and model of the device

Device access rules can also be configured from PowerShell by using the New-ActiveSyncDeviceAccessRule cmdlet. For example, to block iOS devices running version 7.0.2, run the following command:

[Click here to view code image](#)

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceOS -QueryString "iOS 7.0.2 11A501" -AccessLevel Block
```

As you might notice in the command, the device specific information is required as part of the rule to block or quarantine the device. To retrieve this information from a device that has already connected to the organization, run the Get-MobileDevice cmdlet, and look for the DeviceOS, DeviceModel, and DeviceType fields.

## [Click here to view code image](#)

```
Get-MobileDevice | Format-List DeviceOS,DeviceModel,DeviceType
```

In our example, we used the DeviceOS characteristic that matched the specific version for iOS devices running 7.0.2. It is common to have multiple device operating systems for a single version. For example, you might find eight different versions of iOS 7.0.

## Plan, deploy, and configure Office Apps

Microsoft Office 2016 includes updated applications for Office, including Outlook 2016. All of the primary Office applications have been updated, and a deployment guide for each version can be found on TechNet at

<https://technet.microsoft.com/library/cc303401%28v=office.16%29.aspx>.

This section focuses on Outlook 2016 because it is most closely related to the 70-345 exam. Consider the following planning and deployment requirements for Outlook 2016:

- Clients must be running Windows 7 or later
- Autodiscover must be configured in the Exchange environment
- Client antivirus should not scan Outlook files, such as .pst, .ost, .oab, and .srs files

When you're ready to deploy Office 2016, it can be performed in one of two ways:

- Using the Click-2-Run setup
- Using the MSI installer with volume licensing

The most customizable method, however, is to use the Office Customization Tool (OCT) to configure settings to use during and after deployment. To launch the OCT, run the following command at the root of the installation media:

```
setup.exe /admin
```

---



### Exam Tip

Make sure you know how to customize the setup for Office 2016 and be familiar with the prerequisites.

---

## Summary

- Mobile devices can use ActiveSync, OWA for Devices, or the Outlook app to access an Exchange environment.
- Outlook on the web settings can be assigned by using a policy.

- Mobile device capabilities can be required by using a policy.
- Specific brands, types, and versions of mobile devices can be blocked from connecting.
- Office applications can be deployed automatically with Click-2-Run or MSI deployments.

## Skill 2.3: Plan, deploy, and manage load balancing

As an email administrator, you must routinely manage load balancing. In most enterprise implementations of Exchange Server, load balancing is one of the key components to bring highly available Exchange services to clients. It is important to understand how load balancing integrates with and enhances your email environments. It is also important to understand the various skills for planning, deploying, and managing load balancing. This section should help you prepare for complex exam scenarios.

---

### This section covers how to:

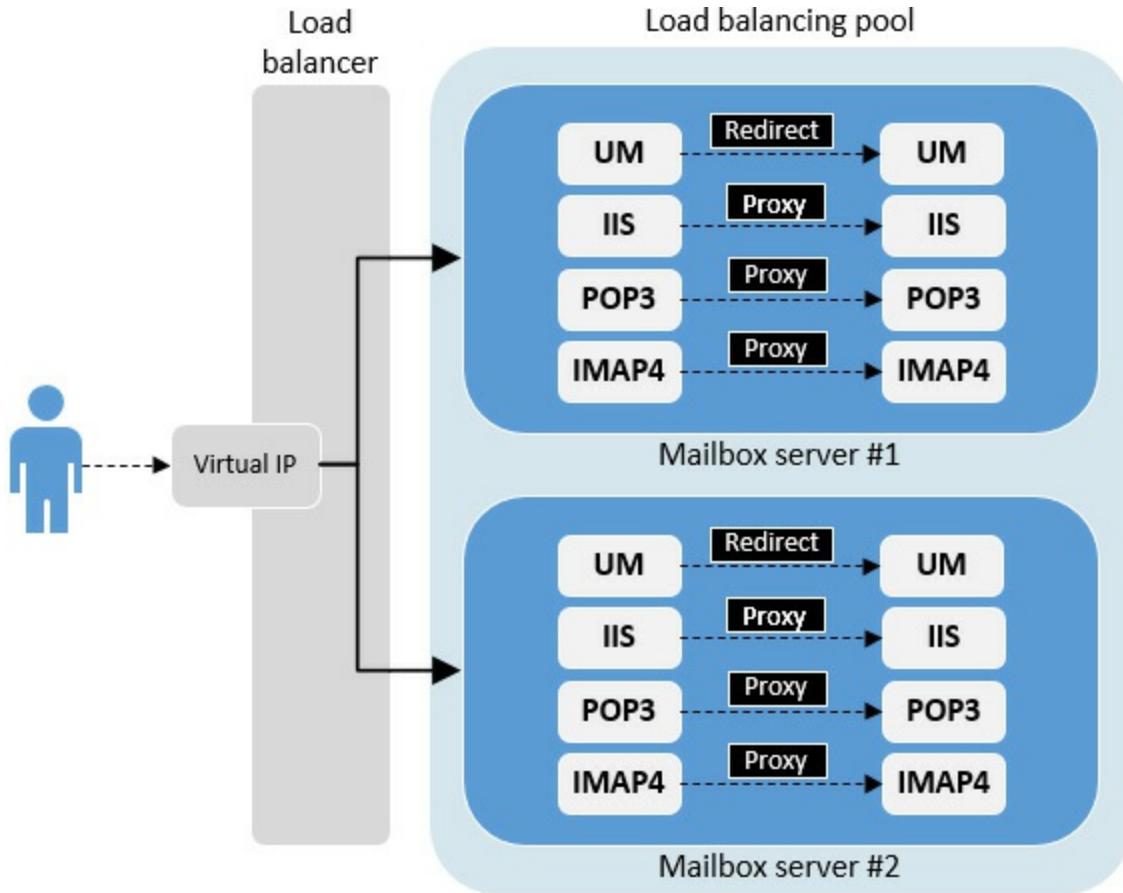
- [Configure namespace load balancing](#)
  - [Plan for differences between layer seven and layer four balancing methods](#)
- 

## Configure namespace load balancing

As mentioned previously, Microsoft Exchange 2016 uses namespaces for clients to connect to the Exchange environment. As part of your planning for load balancing, you need to include your namespaces. For environments that use load balancing, there are six steps that occur when a client connects to a load-balanced resource:

1. A client requests a connection to the namespace, and the namespace resolves to a virtual IP address on the load balancer.
2. The load balancer assigns the client connection to an appropriate Mailbox server in the pool of available servers.
3. The client access services running on the Mailbox server authenticates the request and performs a service discovery through Active Directory.
4. The service discovery locates the mailbox version and the mailbox location information, including which Mailbox server and database the user's mailbox resides on.
5. The client access services determine which Mailbox server has an active copy of the database.
6. The client access services either proxies or redirects the request to the server that has the active copy of the database.

Similar to Exchange Server 2013, Exchange Server 2016 does not require session affinity for the load balancing layer. This means that regardless of where a connection originates, it always connects, either directly or by proxy, to the Mailbox server that has an active copy of the database where that user's mailbox is located. This is true for most protocols, as shown in [Figure 2-15](#).



**FIGURE 2-15** Protocol connections in Exchange 2016 are redirected or proxied



### Exam Tip

SIP and RTP sessions do not use a proxy to establish a connection. They are redirected to the mailbox server with the active database copy.

Because the load balancers do not keep session affinity, they do not require client traffic to be decrypted and re-encrypted when traversing the load balancers. The load balancers simply use the layer 4 information:

- DNS namespace
- IP address
- Protocol and port number

The load balancer in these scenarios uses a variety of methods to select the target server. Two of the most common load balancing methods are:

- **Round robin** Each inbound request is sent to the next server in the list of servers.
- **Least-connection** Each inbound request is sent to the server with the least amount of current connections.

## Load balancing with health monitoring

Layer 4 load balancing presents a challenge because the layer 4 information does not provide any information on the health status of the destination Mailbox server. Exchange 2016 builds on Exchange 2013's Managed Availability feature, which is a built-in health monitoring solution. This feature now includes an offline responder for load balancers. This means that a server with a problem, such as a service that is down, can be removed from service. To use this feature, the load balancers must be configured to check the <virtualdirectory>/healthcheck.htm page to determine the health status of the target Mailbox server. The healthcheck.htm page does not actually exist in the virtual directory, but is automatically generated in memory based on the health of the protocol. [Figure 2-16](#) shows a status page showing that a service is healthy.



**FIGURE 2-16** Successful OWA health check request

If the load balancer receives a 200 status code from the Mailbox server, the protocol is working. If the load balancer receives any other status code, Managed Availability has marked the protocol as down for that Mailbox server. The load balancer should then be configured to remove the Mailbox server from its list of available servers until the issue has been resolved. You can also manually remove a service or protocol for maintenance or other reasons by using the Set-ServerComponentState cmdlet. For example, to disable the OwaProxy protocol on a Mailbox server named EX01, run the following command:

[Click here to view code image](#)

```
Set-ServerComponentState EX01 -Component OwaProxy -Requestor Maintenance -  
State Inactive
```

If the load balancer does not use the healthcheck.htm service, it is not able to dynamically remove or re-add a Mailbox server from its list of servers. In this scenario, a load balancer can direct a client request to a Mailbox server that has been marked for maintenance or is offline, which can result in a degraded client experience.

## SIP load balancing

Unified messaging uses a variety of port numbers for connections and communications, as shown in [Table 2-1](#).

Port Number	Use
5060	Unencrypted communications for IP PBX, VoIP Gateway, and SBC
5061	Encrypted SIP connections
5062	Unsecured SIP communications
5063	Secured SIP communications
5065	Unsecured UM worker process
5066	Secured UM worker process
5067	Unsecured UM worker process
5068	Secured UM worker process

TABLE 2-1 Unified messaging port numbers

The client access service that runs on a Mailbox server receives the SIP traffic from load balancers or a client, and redirects the request to the Mailbox server that has the active copy of the database where the user's mailbox is located.

The connection between the client and the Mailbox server either uses real-time transport protocol (RTP) or secure real-time transport protocol (SRTP). Only the TCP ports 5060 and 5061 between the SIP clients and the Mailbox server need to be load balanced. The SIP traffic does not require session affinity to be configured, as the SIP client establishes the RTP or SRTP connections directly with the Mailbox server.

## Windows Network Load Balancing (Windows NLB)

Windows NLB is a feature built-in to the Windows Server operating system. It is a free and commonly used method for an Exchange load balancing solution. An exception to this however, is that Windows NLB cannot be deployed with Windows Failover Clustering. When an Exchange environment is deployed with DAGs, and therefore Failover Clustering, Windows NLB cannot be deployed on the same servers that Exchange is running on.

Windows NLB is not service-aware. For example, if a service fails that is part of the cluster, the client connection requests can be directed to a server that is offline. Windows NLB can also result in port flooding, which can disrupt network switches with subnet broadcasts. This can cause a negative impact not only to the Exchange environment but also to any other devices running on the same subnet.

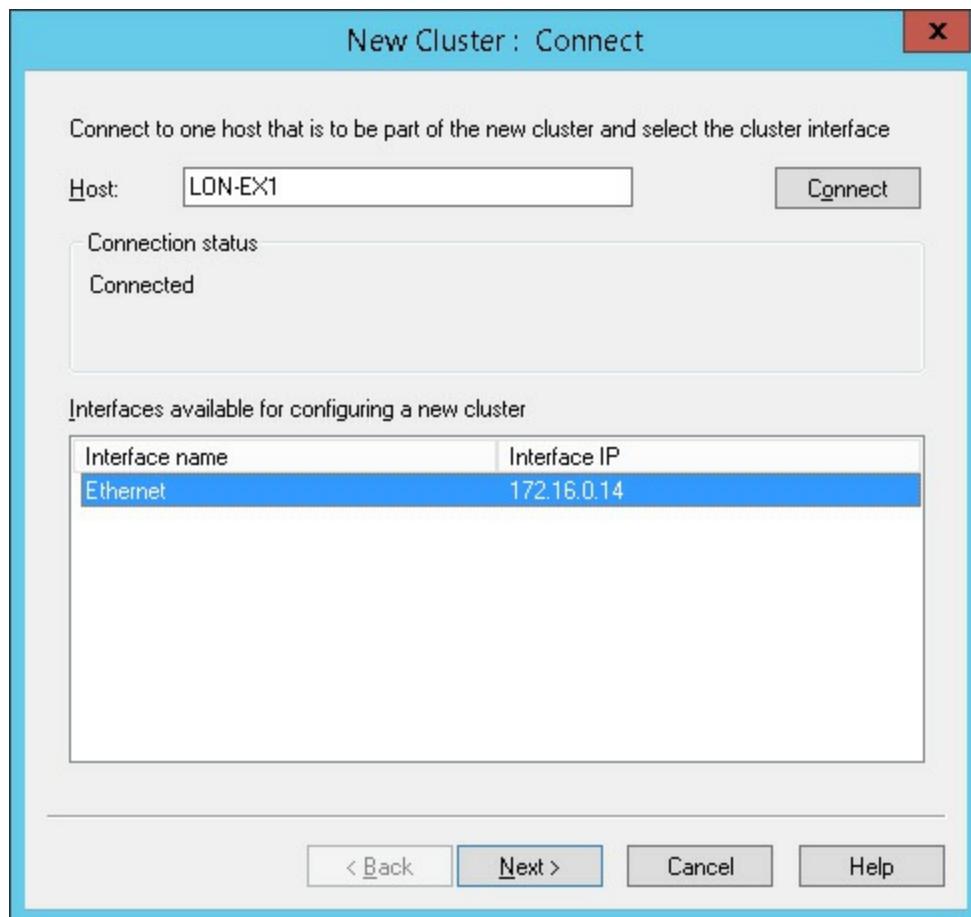
With these limitations in mind, it is possible to deploy Windows NLB with Exchange 2016. When using Windows NLB it is recommended to configure a dedicated

management adapter that isn't shared with any networks that clients will use. To create a Windows NLB cluster, use the Add Roles and Features Wizard or the Add-WindowsFeature cmdlet to add the feature and tools. You can run the following command to install the feature:

[Click here to view code image](#)

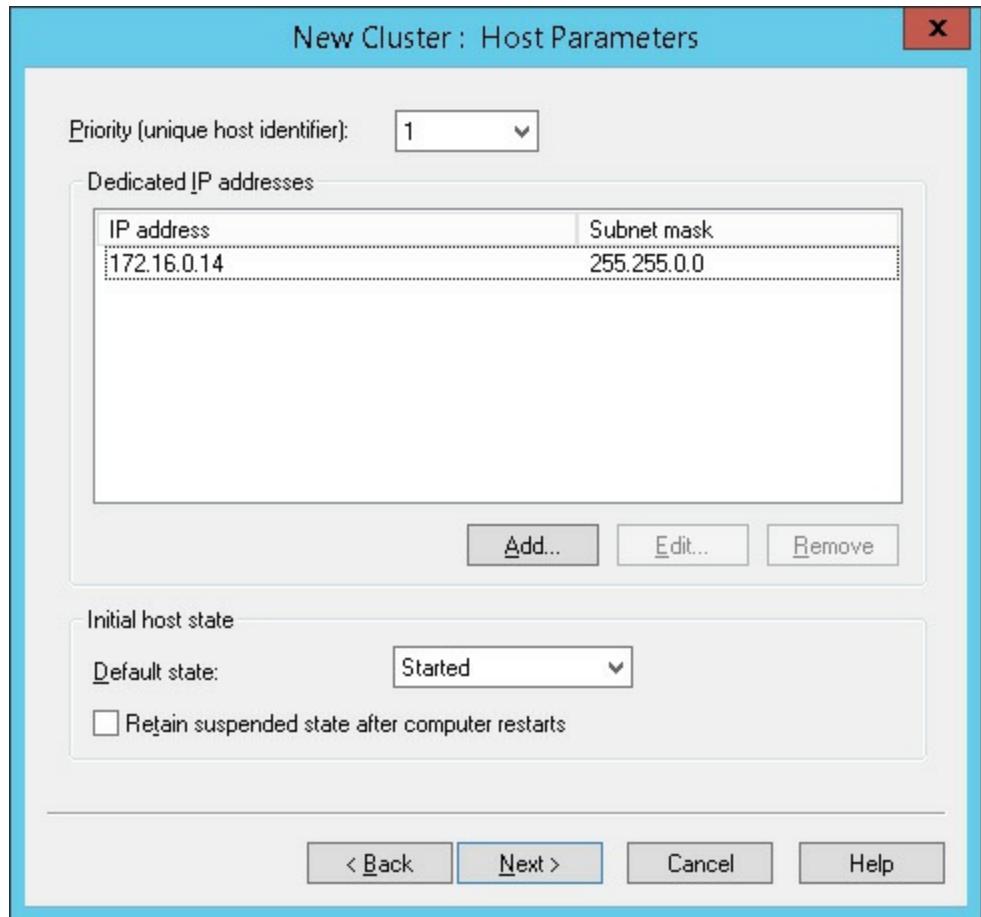
```
Add-WindowsFeature -Name NLB -IncludeManagementTools
```

After you install the feature, configure it by adding the first host to the Windows NLB cluster. [Figure 2-17](#) shows how to add the first host to a new cluster from the Windows NLB management tool.



**FIGURE 2-17** Creating a new cluster

After clicking Connect to connect to the host, the next step of the wizard is to configure the parameters for the new host. One of the options is the host priority, which is a numerical value between 1 and 32. This value must be unique for each host in the cluster. You can configure other parameters, including a dedicated IP address. [Figure 2-18](#) shows the New Cluster Wizard's Host Parameters page.



**FIGURE 2-18** Host configuration parameters

The Cluster IP Addresses page configures the IP address used for cluster communications. This is the IP address that clients use to connect to the load balanced cluster. If necessary, you can configure more than one IP address on this page. If more than one IP address is defined, the first IP address is used for the cluster heartbeat. [Figure 2-19](#) shows the IP address configured for the cluster, in this example, 172.16.0.99.

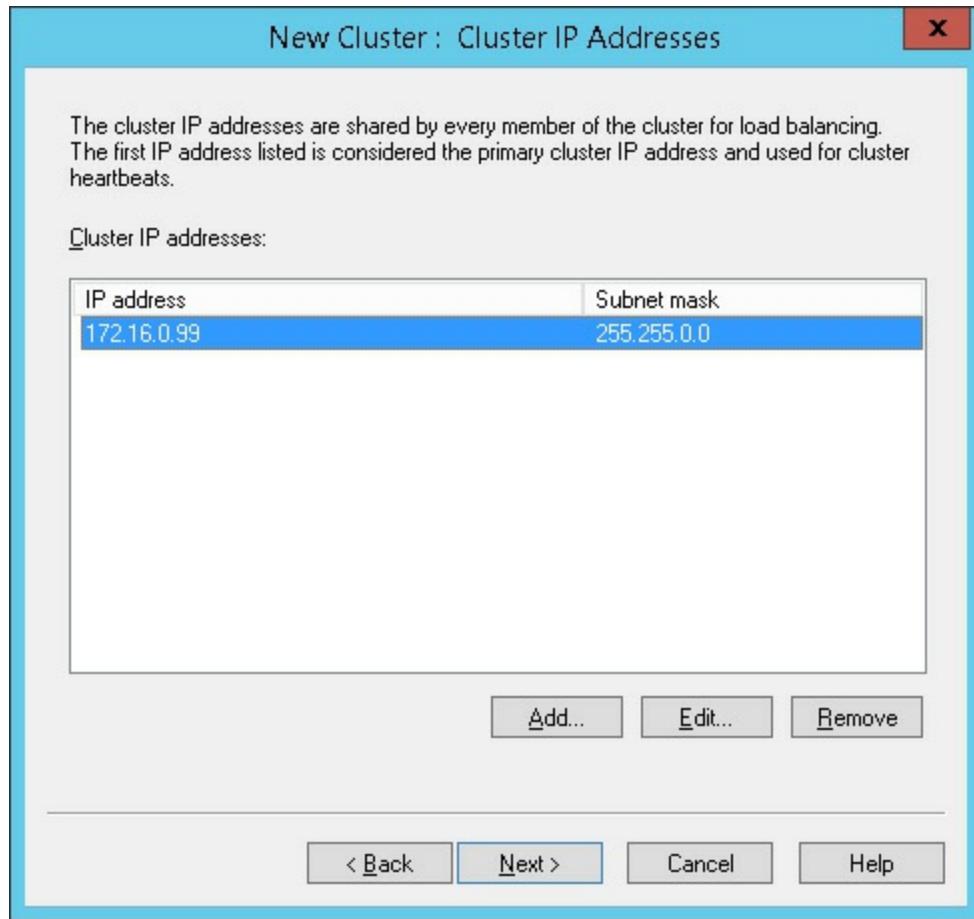
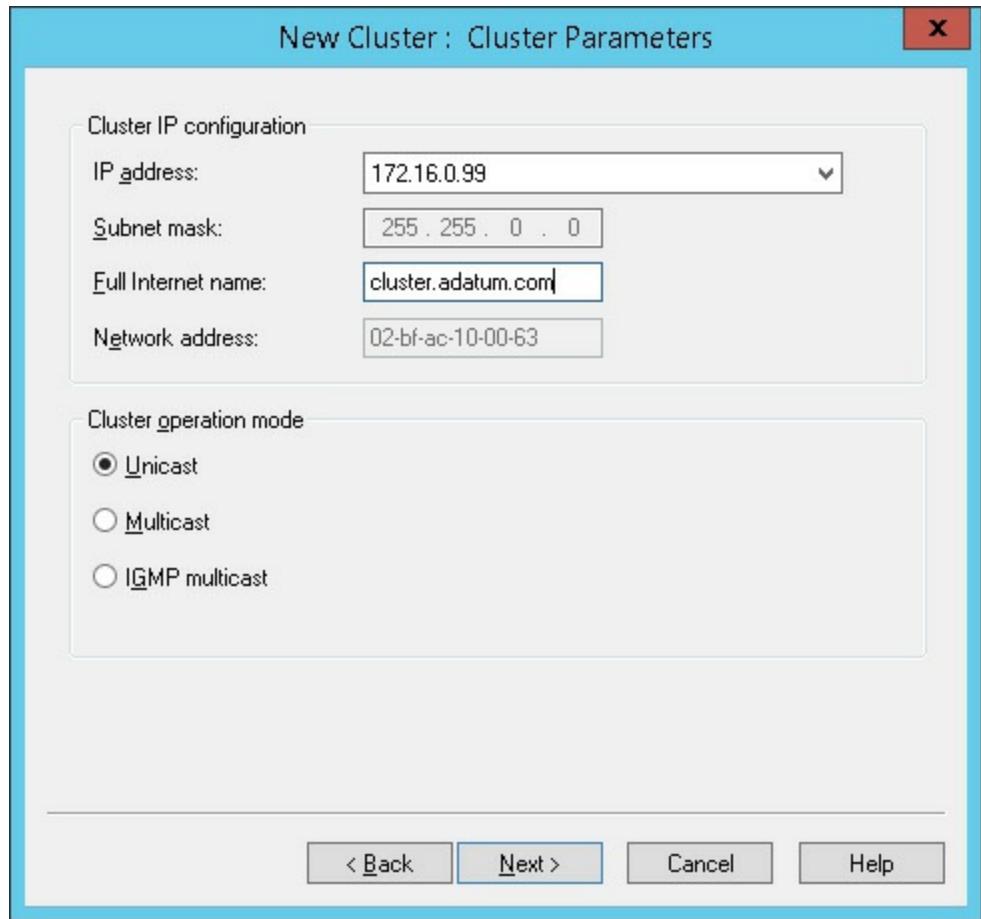


FIGURE 2-19 Cluster IP address

On the Cluster Parameters page shown in [Figure 2-20](#), you assign the FQDN of each IP address configured in the previous step. This is also required to configure the cluster operation mode, which by default is set to Unicast. Another option, Multicast, changes the cluster MAC address to the multicast address. Internet Group Management Protocols (IGMPs) limit the amount of switch flooding by only sending traffic to ports registered to Windows NLB instead of all ports. You must plan carefully and diligently if you plan to use Multicast or IGMP modes.



**FIGURE 2-20** Cluster parameters

The final page of the wizard configures the port rules for the cluster, as shown in [Figure 2-21](#). These rules enable you to configure which ports and protocols the Windows NLB cluster responds to. If you have configured multiple IP addresses, you can configure the port ranges for each IP address that is defined.

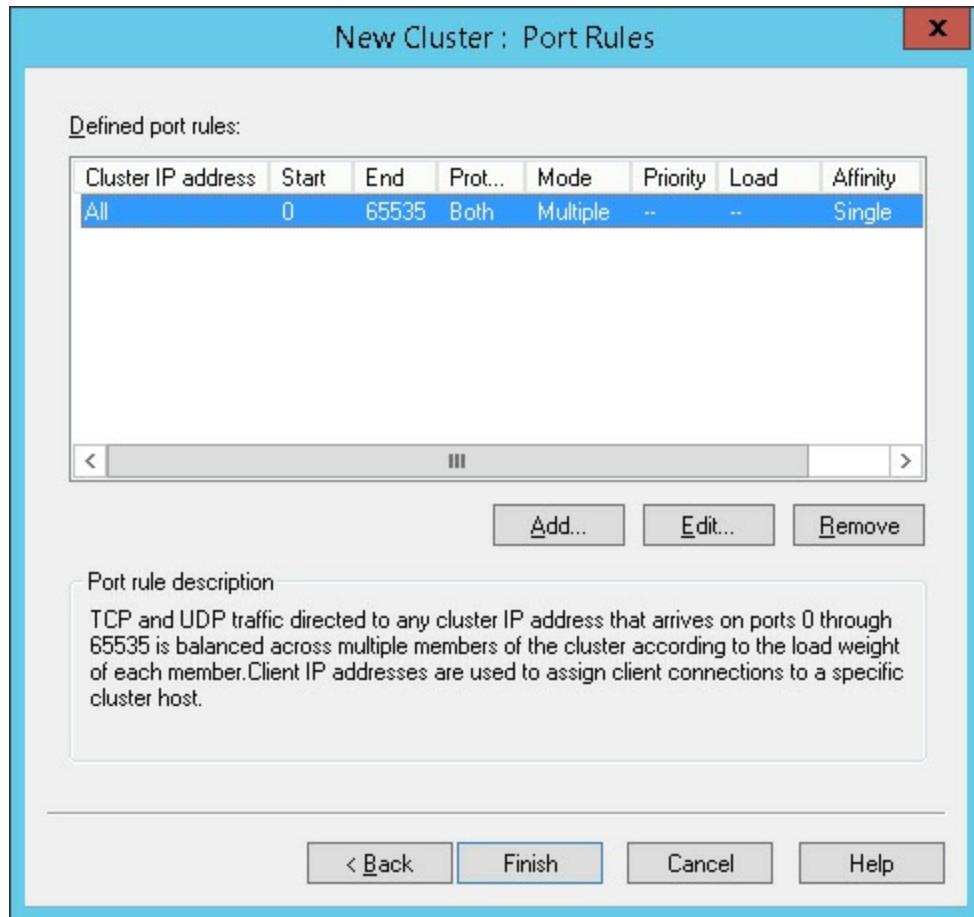


FIGURE 2-21 Cluster port rules

## Plan for differences between layer seven and layer four load balancing methods

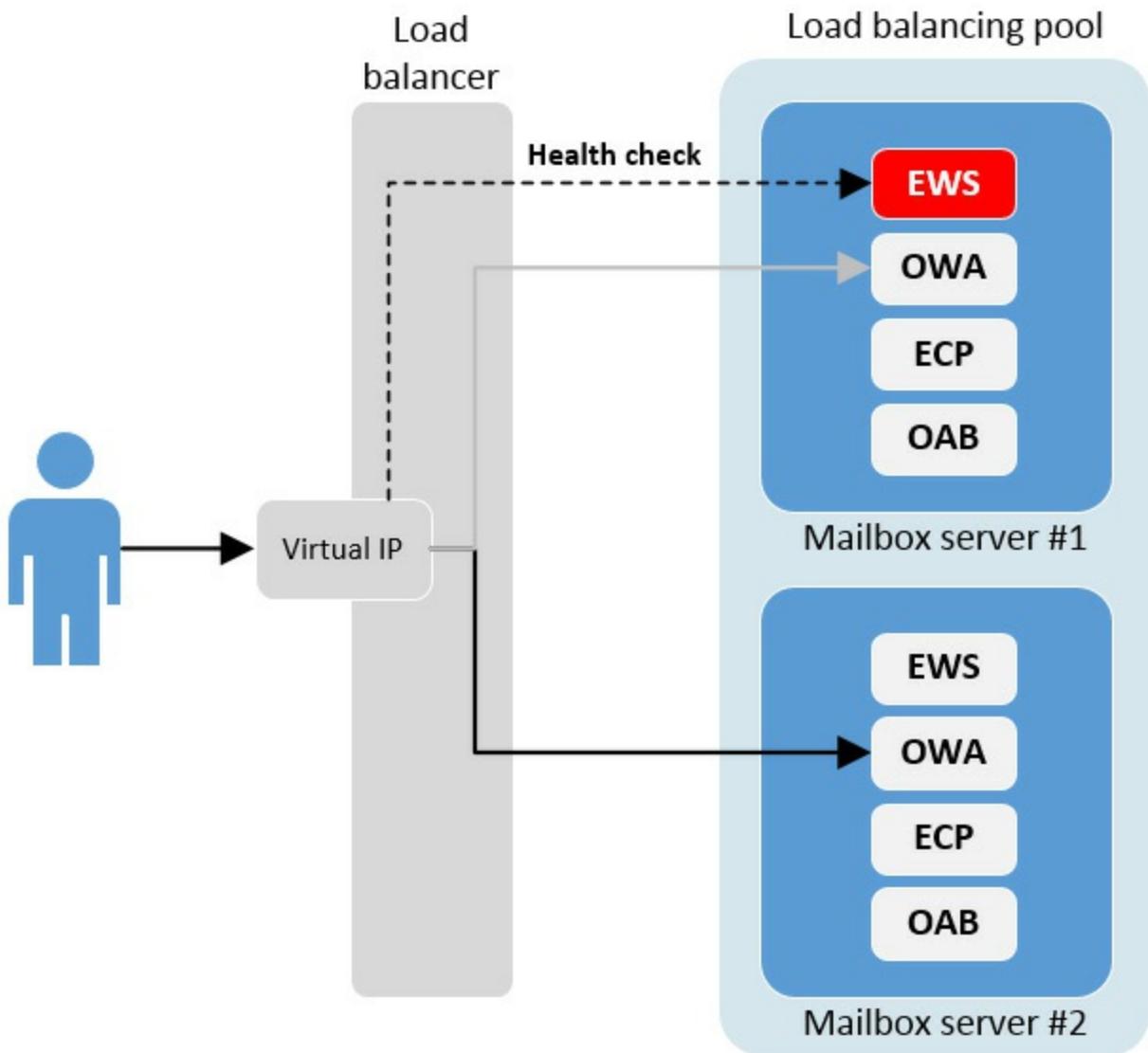
As we discussed earlier in this section, Exchange 2016 does not require session affinity for load balancing. Session affinity can still be configured when using load balancing at layer 7. This section looks at four scenarios for load balancing:

- Single namespace using layer 4 load balancing without session affinity
- Single namespace using layer 7 load balancing without session affinity
- Single namespace using layer 7 load balancing with session affinity
- Multiple namespaces without session affinity

## **Single namespace using layer 4 load balancing without session affinity**

In this scenario, the load balancing solution is using layer 4 to distribute client connection traffic. Although it is operating at layer 4, the load balancer can still be configured to check the health of the Exchange server. The load balancer can validate only one of the virtual directories running on the Exchange server because it is using a single namespace. In this scenario, configure the health check on a virtual directory that is used frequently, such as OWA. Note that OWA is still the name of the virtual directory, even though administrators now know OWA as Outlook on the web.

Provided that the health check response is successful, the load balancer proxies or redirects requests to each available Mailbox server in its resource list. If the health check fails at any point, that Mailbox server is removed from the list of available servers. It is important to note that the health check is from the perspective of the load balancer, not the rest of the network. When using a single namespace, that also means the health check simply checks the server, not the protocol. Therefore, if one protocol fails, the load balancer assumes all protocols are offline. [Figure 2-22](#) illustrates a client connection with a layer 4 load balancing solution that has failed a health check.



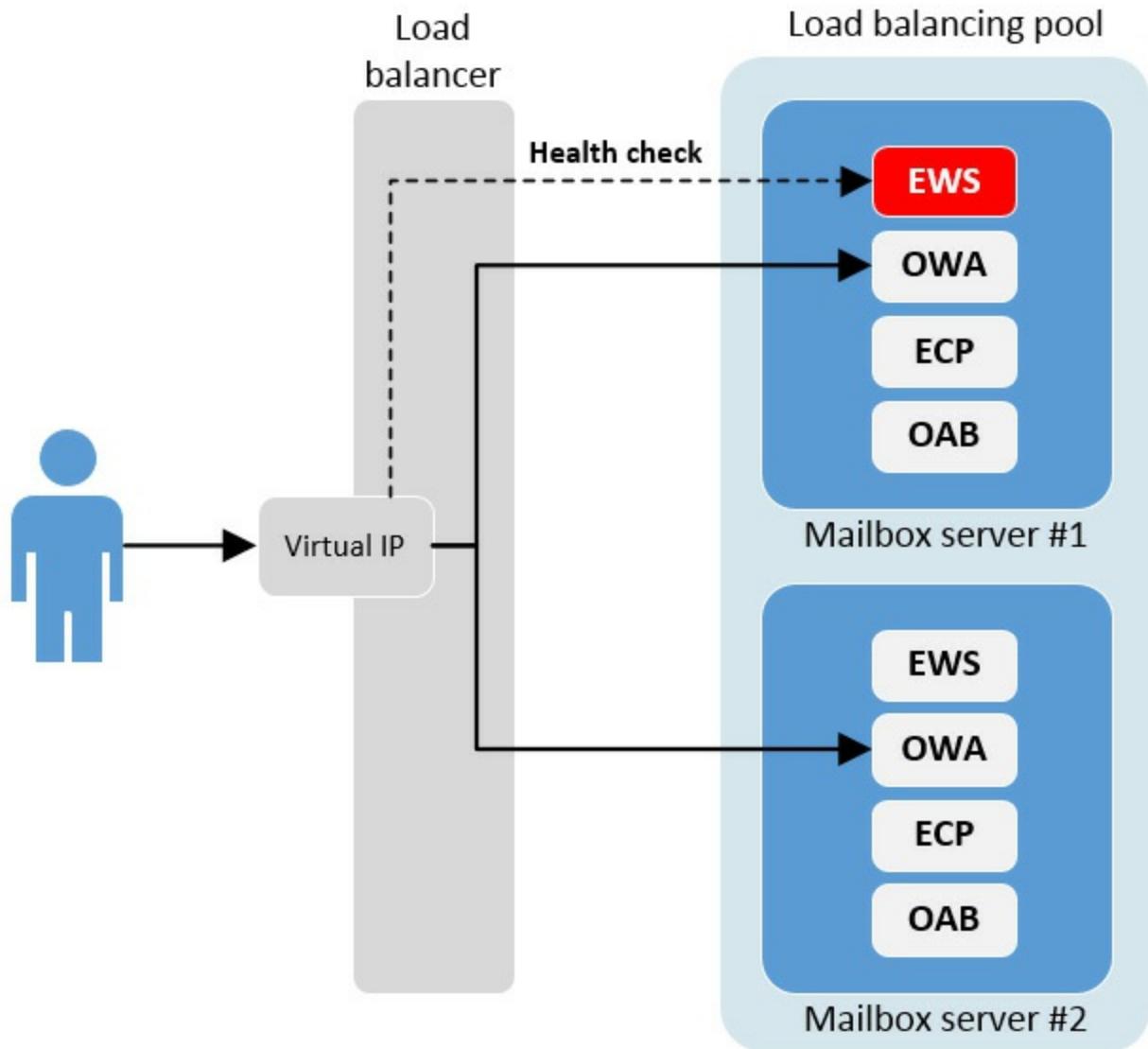
**FIGURE 2-22 Failed health check on layer 4**

### Single namespace using layer 7 load balancing without session affinity

This scenario is similar to the previous one, in that we have a single namespace that is not using session affinity. The difference in this scenario is that the load balancer is using layer 7, which enables it to be more application aware. In this type of scenario, the client connection's SSL connections end at the load balancer, which knows the target URL of the Mailbox server. Because the load balancer is now aware of the destination, it can be configured to check the health of each individual virtual directory being used. If a single virtual directory is not responding, the load balancer redirects requests only for that virtual directory to another server. Other virtual directories that are operational still receive requests from the load balancer.

This enables the load balancing solution to be aware on a protocol basis, rather than just for a single server. [Figure 2-23](#) illustrates how the health check is performed on a per-protocol basis. Configuring a single namespace that uses a layer 7 load balancer

without session affinity is the recommended load balancing solution for Exchange Server 2016.



**FIGURE 2-23 Failed health check on layer 7**



### Exam Tip

A layer 7 load balancing solution does not need session affinity to be application-aware. Each protocol and virtual directory is checked with Managed Availability by using a layer 7 load balancing solution.

## **Single namespace using layer 7 load balancing with session affinity**

Similar to other scenarios, this scenario uses a single namespace for load balancing, however, session affinity with the layer 7 load balancing is now included. As with the previous scenario, using layer 7 makes the load balancer application-aware for each of the virtual directories on the Exchange server.

Enabling session affinity causes the load balancer to use additional memory and CPU processing. This is because the load balancer now tracks additional cookies or SSL session-IDs for each session, which is not necessary for Exchange server connections. Therefore, it is not recommended to deploy a load balancing solution that uses session affinity with Exchange 2016.

### **Quick check**

- How does layer 7 load balancing use Managed Availability to verify a destination server is responding to requests?

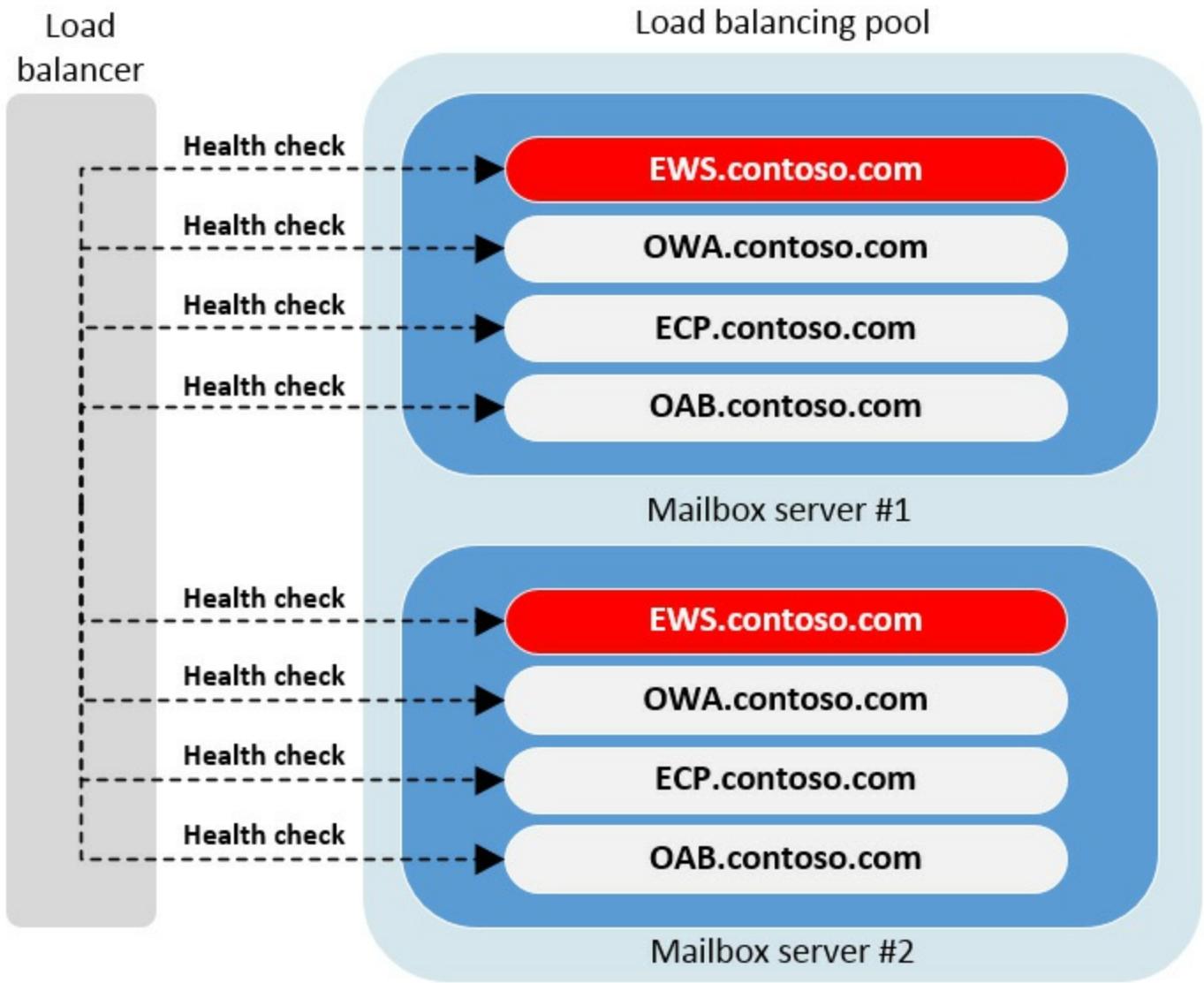
### **Quick check answer**

- Managed Availability at layer 7 checks each individual virtual directory to ensure it is responding to requests on the destination server.

## **Multiple namespaces without session affinity**

A scenario with multiple namespaces and without session affinity appears on the surface to be less complex, but does require more load balancing configuration. In this scenario, rather than have all load balancing traffic use a single namespace, such as [mail.adatum.com](mailto:mail.adatum.com), each virtual directory can be configured individually at the load balancing level.

Because each namespace is configured separately, each virtual directory's health can be checked without using layer 7 load balancing. [Figure 2-24](#) illustrates having each virtual directory configured as a separate namespace in the load balancing configuration.



**FIGURE 2-24** The impacts of a singled failed service are only for the failed service

At its core, load balancing is a relatively straight forward concept where you balance incoming connections to even out the workload across multiple servers. Things become much more complex, and require additional planning, when you have multiple sites and geographic regions to take into account.

### Need More Review? Load Balancing in Exchange 2016

You can find more information about load balancing in Exchange Server 2016 on TechNet at

<https://blogs.technet.microsoft.com/exchange/2015/10/08/load-balancing-in-exchange-2016/>.

## **Summary**

- Exchange 2016 does not require session affinity for load balancing. It is not recommended to configure session affinity with Exchange 2016.
- Most connections use a proxy or redirect from a load balancer to Exchange, except for SIP and RTP. SIP and RTP always redirect and do not proxy.
- Managed Availability enables virtual directory health checks which helps to ensure that functional services remain available through a load balancer even if another service is down.
- Load balancing for SIP is only required on ports 5060 and 5061.
- Windows NLB is not supported on a server with the Failover Clustering feature.
- A single namespace with layer 7 load balancing is recommended for Exchange 2016.

## **Skill 2.4: Monitor and troubleshoot client connectivity**

Maintaining client access within Exchange 2016 involves monitoring and troubleshooting client connectivity. Even the simplest environment needs to be monitored and surveyed for connectivity issues. When problems are discovered, it is important to understand which tools are at your disposal and what methods are most effective for troubleshooting different situations.

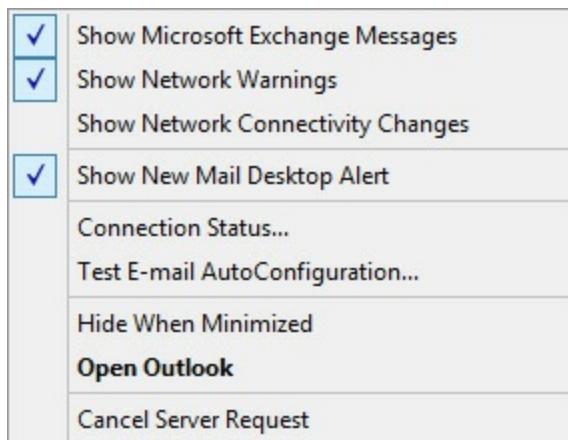
---

### **This section covers how to:**

- [Troubleshoot Outlook Anywhere connectivity](#)
  - [Troubleshoot Outlook MAPI over HTTP connectivity](#)
  - [Troubleshoot Exchange Web Services \(EWS\)](#)
  - [Troubleshoot Outlook on the web](#)
  - [Troubleshoot POP3 and IMAP4](#)
  - [Troubleshoot authentication](#)
  - [Troubleshoot Autodiscover](#)
  - [Troubleshoot Exchange ActiveSync](#)
  - [Troubleshoot proxy and redirection](#)
-

## Troubleshoot Outlook Anywhere connectivity

There are many different methods to troubleshoot and identify connectivity issues with Outlook Anywhere. The primary method of testing Outlook Anywhere is from within the Outlook application itself. When Outlook is running, press the CTRL key and right-click the Outlook icon in the notification area to reveal additional options in the menu, as shown in [Figure 2-25](#).



**FIGURE 2-25** Outlook context menu

One of the options in the advanced context menu is Outlook Connection Status. The connection status tool shows the following for the active configuration:

- Server name
- Status
- Protocol
- Encryption
- Interface
- Version

[Figure 2-26](#) shows the Outlook Connection Status window with multiple Exchange accounts defined, in this example Office 365 accounts.

Outlook Connection Status

General Local Mailbox

Activity

Server name	Status	Pro...	Authn	E...	R...	Type	Re...	A...	A...	Sess	Type	Int...	Conn	Notif	RPC	Version	Network...
https://outlook.office365.com...	Established	HTTP	Clear*	SSL		Exchange Mail	43/3	518	40	Background	Wi-Fi			Async	Async	15.1.501.11	Unrestri...
https://outlook.office365.com...	Established	HTTP	Clear*	SSL		Exchange Mail	87/2	405	22	Cache	Wi-Fi			Async	Async	15.1.501.11	Unrestri...
https://outlook.office365.com...	Connecting	HTTP	Error*	SSL		Exchange Mail				Cache						---	
https://outlook.office365.com...	Established	HTTP	Clear*	SSL		Exchange Mail	91/2	472	31	Cache	Wi-Fi			Async	Async	15.1.497.21	Unrestri...
https://outlook.office365.com...	Connecting	HTTP	Error*	SSL		Exchange Mail				Background						---	
https://outlook.office365.com...	Established	HTTP	Clear*	SSL		Exchange Mail	68/4	566	42	Background	Wi-Fi			Async	Async	15.1.497.21	Unrestri...
https://outlook.office365.com...	Established	HTTP	Clear*	SSL		Exchange Mail	484/3			Cache	Wi-Fi			Async	Async	15.1.497.21	Unrestri...
https://outlook.office365.com...	Established	HTTP	Clear*	SSL		Exchange Mail	25/3			Background	Wi-Fi			Async	Async	15.1.497.21	Unrestri...

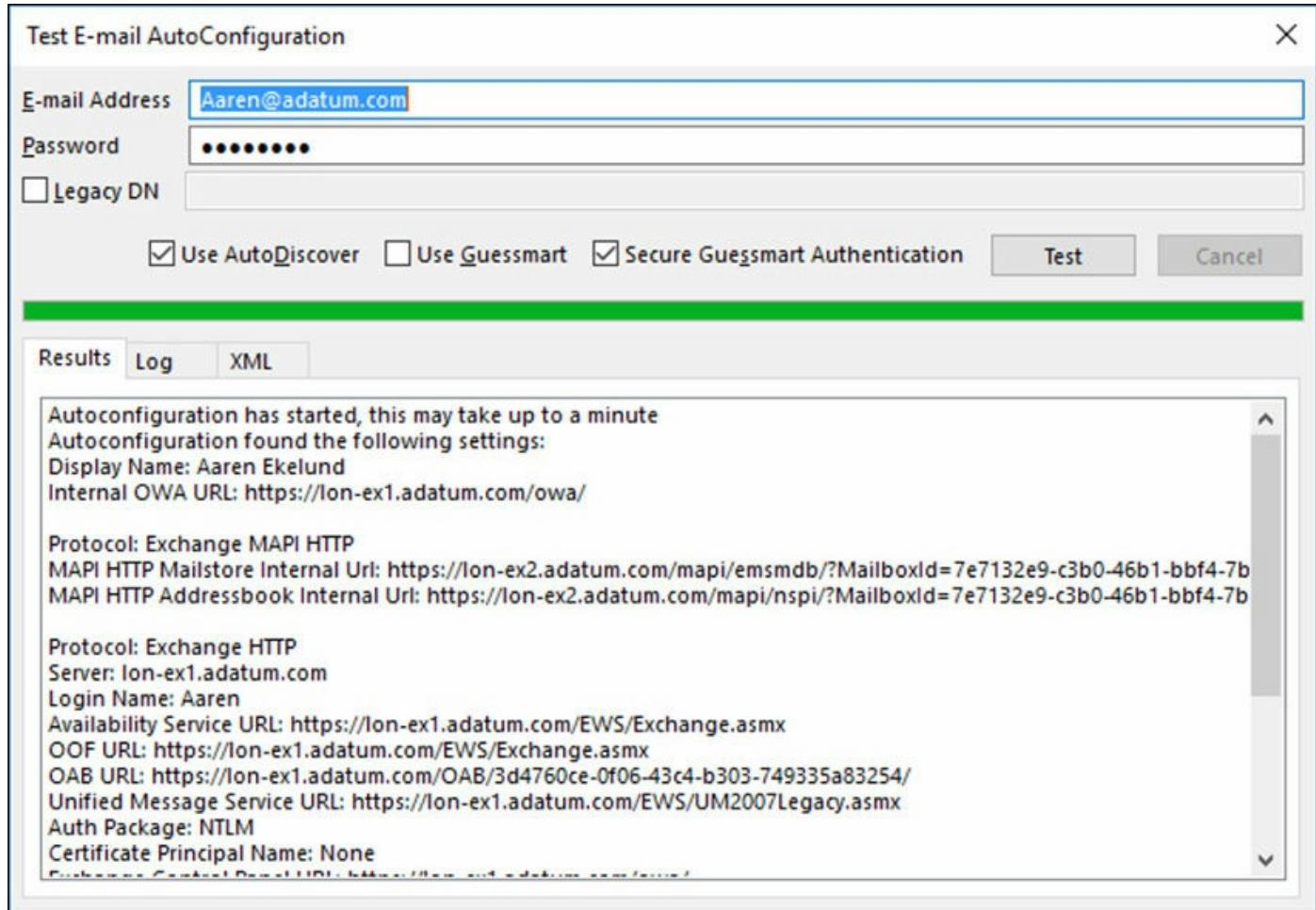
< >

Reconnect

Close

FIGURE 2-26 Outlook Connection Status tool

The other built-in tool is the Test E-Mail AutoConfiguration tool. This tool ensures that Outlook can contact the Exchange server to retrieve the configuration necessary for the client. The Test E-Mail AutoConfiguration tool is shown in [Figure 2-27](#).

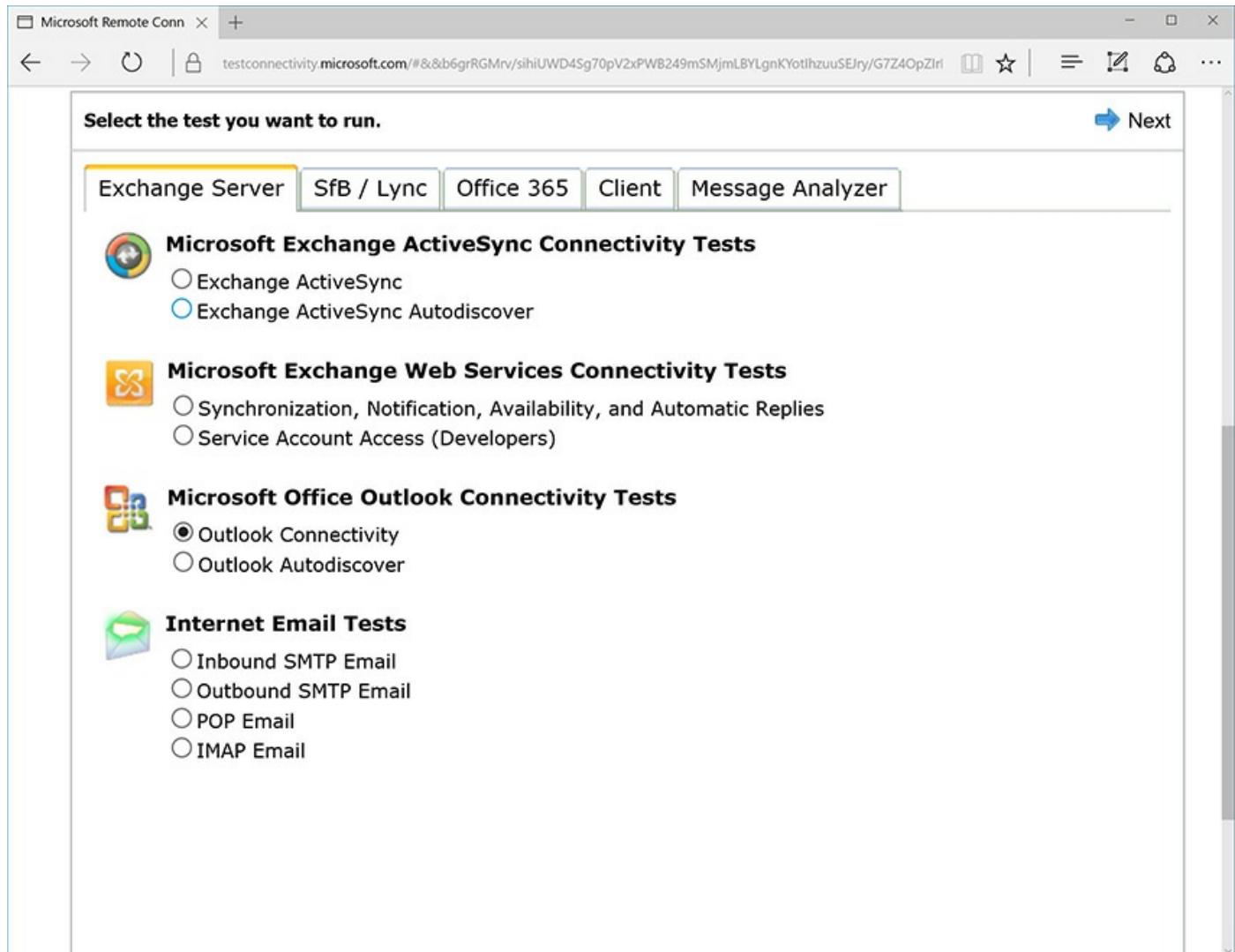


**FIGURE 2-27** Outlook’s Test E-Mail AutoConfiguration tool

If errors are discovered during the test, you can use the information shown in the Test E-mail AutoConfiguration results to correct any configuration issues.

## Troubleshoot Outlook MAPI over HTTP connectivity

The Remote Connectivity Analyzer provides methods to troubleshoot connectivity to Exchange. The tools available in the Remote Connectivity Analyzer are shown in [Figure 2-28](#) and are available at <https://testconnectivity.microsoft.com>.



**FIGURE 2-28** Remote Connectivity Analyzer

Another tool that can be used to troubleshoot Outlook connectivity is the Microsoft Support and Recovery Assistant for Office 365. While the tool sounds like it requires Office 365, it works to identify and troubleshoot Outlook for clients that connect to on-premises Exchange environments as well. [Figure 2-29](#) shows the Outlook troubleshooting options from the Support and Recovery Assistant.

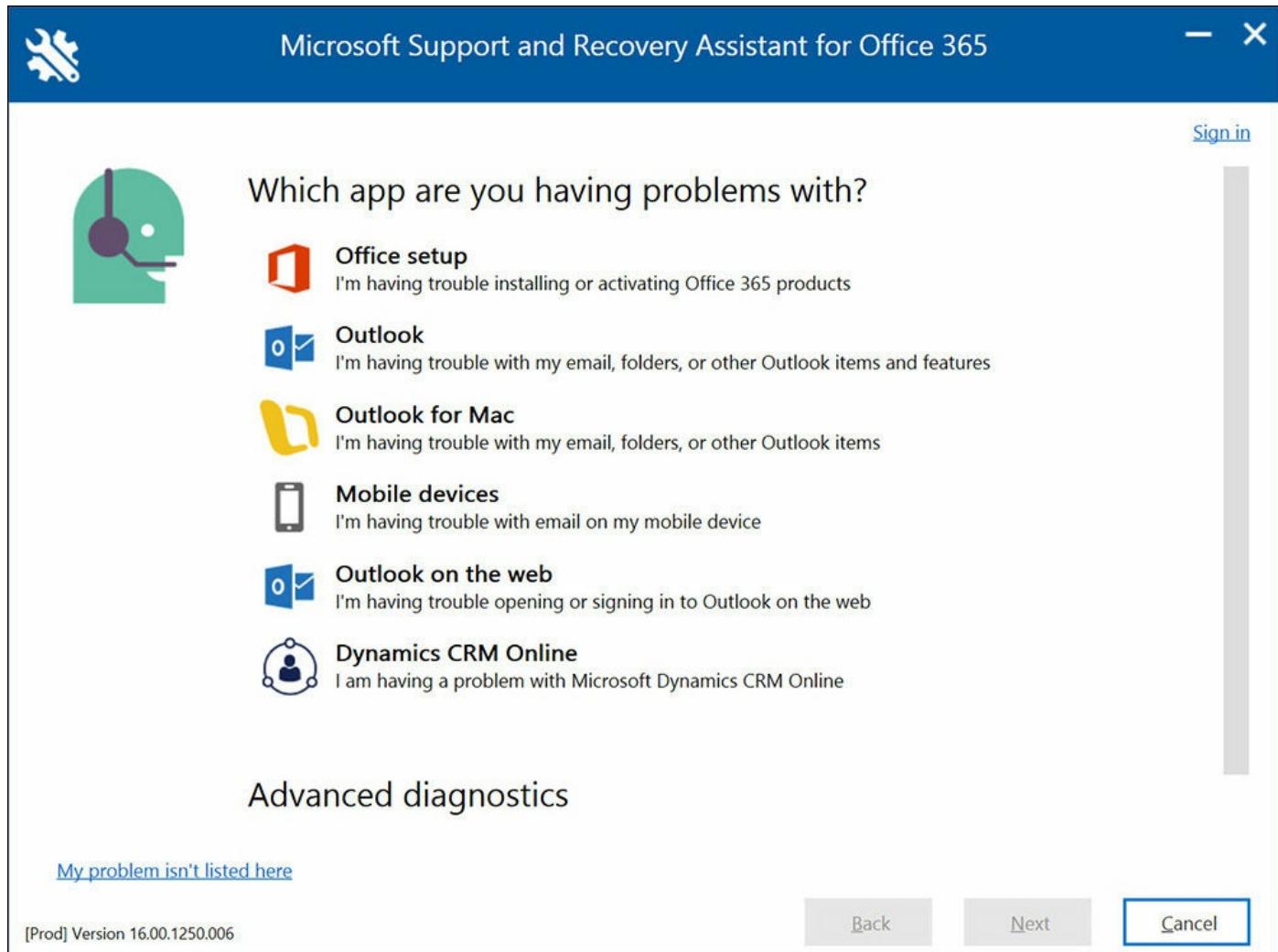


FIGURE 2-29 Microsoft Support and Recovery Assistant

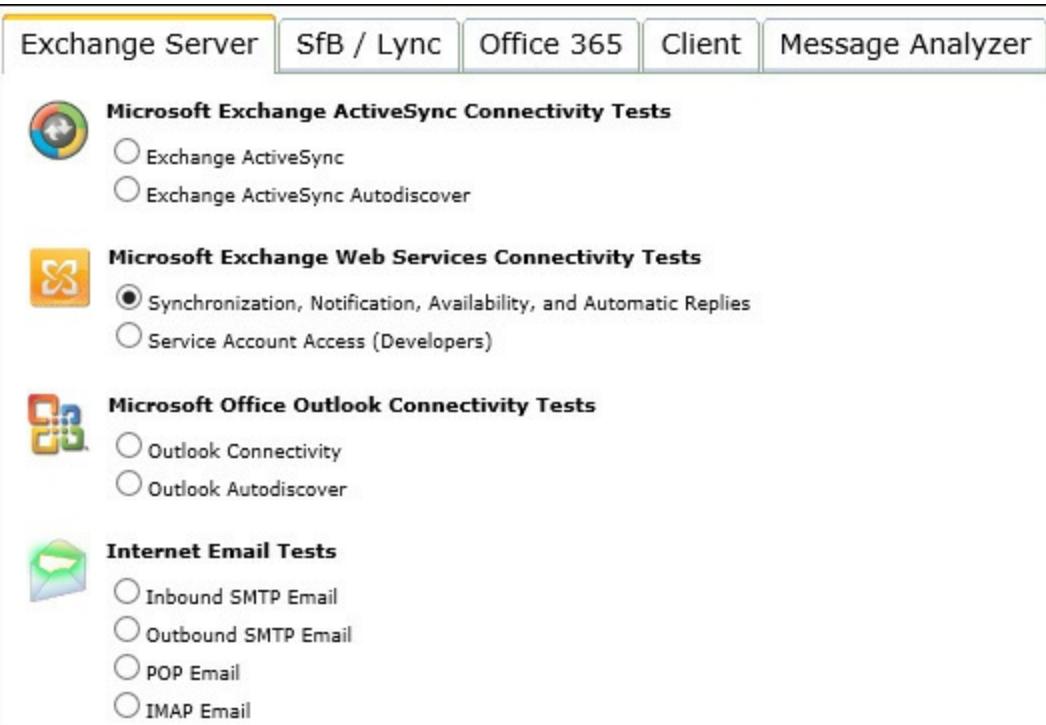
For most options within the Support and Recovery Assistant, the tool requires the credentials of the user account that is having trouble. Additionally, most tasks require that they be run directly from the computer that is experiencing the problem.

## Troubleshoot Exchange Web Services

The Microsoft Remote Connectivity Analyzer can troubleshoot EWS issues. There are two EWS tests that the tool can perform:

- **Synchronization, Notification, Availability, and Automatic Replies** This test performs some EWS-related tasks to find out if EWS is functional.
- **Service Account Access (Developers)** This test mimics a service account that performs actions in a mailbox, such as deleting items.

The testing menu for the Remote Connectivity Analyzer is shown in [Figure 2-30](#) with one of the EWS tests selected.



**FIGURE 2-30** Remote Connectivity Analyzer's available tests

After supplying valid credentials in the tool, you can perform the tests. The results of a successful EWS test (Synchronization, Notification, Availability, and Automatic Replies) are shown in [Figure 2-31](#).

 Exchange Web Services synchronization, notification, availability, and Automatic Replies.  
Tests of all Exchange Web Services tasks completed successfully.

▷ Additional Details

▲ Test Steps

- ✓ The Microsoft Connectivity Analyzer is attempting to test Autodiscover for brian@svidergol.com.  
Autodiscover was tested successfully.
  - ▷ Additional Details
  - ▷ Test Steps
- ✓ Creating a temporary folder to perform synchronization tests.  
Temporary folder created successfully.
  - ▷ Additional Details
  - ▷ Test Steps
- ✓ Creating and deleting items in a test folder to confirm synchronization changes.  
Synchronization changes were confirmed successfully.
  - ▷ Additional Details
  - ▷ Test Steps
- ✓ Items are being created and deleted in a test folder to confirm notification events.  
The Microsoft Connectivity Analyzer received the expected notification events for the actions performed in the test.
  - ▷ Additional Details
  - ▷ Test Steps
- ✓ Appointments are being created and deleted in the user's calendar to confirm the user's availability.  
User availability was confirmed successfully.
  - ▷ Additional Details
  - ▷ Test Steps
- ✓ Setting and retrieving user OOF settings.  
The user's Automatic Replies (OOF) settings were set and retrieved successfully.
  - ▷ Additional Details
  - ▷ Test Steps

FIGURE 2-31 Successful EWS test results

## Troubleshoot Outlook on the web

The troubleshooting tools discussed previously aren't applicable to Outlook on the web. Instead, you need to use other methods. First, as with most troubleshooting, you need to find out if you actually have a problem and where the problem is located. You can use the Get-ServerHealth cmdlet to check your entire server or a specific service for issues. To look at the current health of Outlook on the web on a server named EX01, run the following command:

[Click here to view code image](#)

```
Get-ServerHealth EX01 | where HealthSetName -eq "OWA" | FT Name,AlertValue  
-AutoSize
```

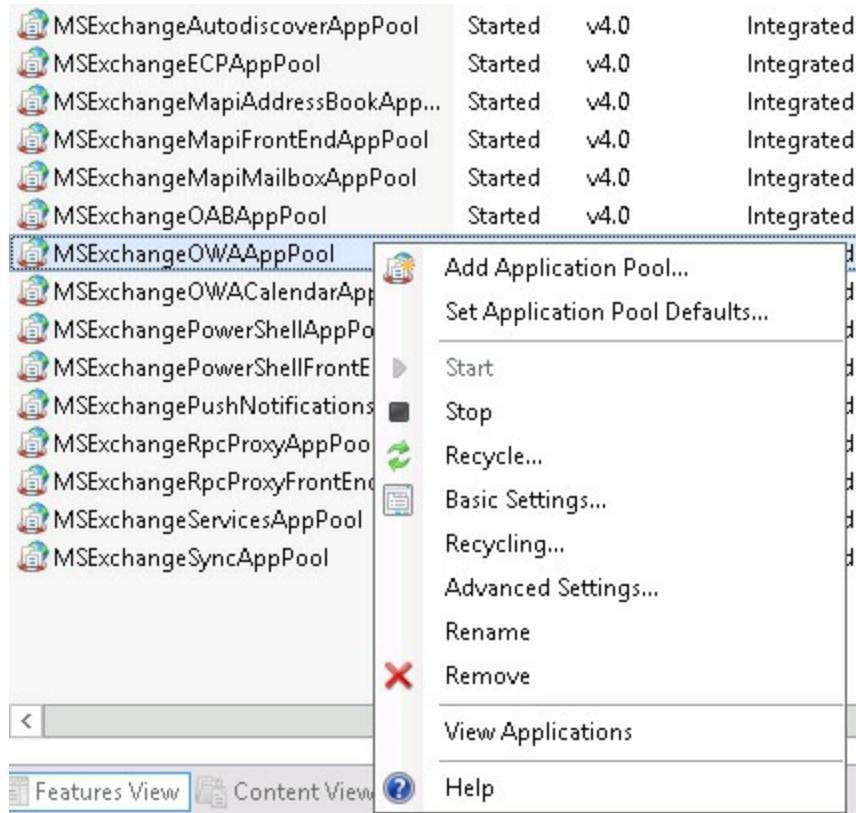
The output is shown in [Figure 2-32](#).

Name	AlertValue
MaintenanceFailureMonitor.OWA	Healthy
MaintenanceTimeoutMonitor.OWA	Healthy
P0_OwaStartPage_AllMonitor	Healthy
P1_OwaStartPage_AllMonitor	Healthy
P0_OwaLogoff_AllMonitor	Healthy
P1_OwaLogoff_AllMonitor	Healthy
P0_OwaServiceCommand_CreateItemMonitor	Healthy
P1_OwaServiceCommand_CreateItemMonitor	Healthy
OwaCtpMonitor	Healthy
CreateItem_CreateMessageForCompose_EXMonitor	Healthy
CreateItem_CreateMessageForComposeSend_EXMonitor	Healthy
CreateItem_CreateResponse_EXMonitor	Healthy
CreateItem_CreateResponseSend_EXMonitor	Healthy
CreateItem_MailComposeUpgrade_EXMonitor	Healthy
FindConversation_BrowseAll_EXMonitor	Healthy
FindConversation_BrowseNoClutterAll_EXMonitor	Healthy
FindConversation_BrowseNoClutterUnread_EXMonitor	Healthy
FindConversation_BrowseUnread_EXMonitor	Healthy
FindItem_BrowseAll_EXMonitor	Healthy
FindItem_BrowseNoClutterAll_EXMonitor	Healthy
FindItem_BrowseNoClutterUnread_EXMonitor	Healthy
FindItem_BrowseUnread_EXMonitor	Healthy
GetConversationItems_EXMonitor	Healthy
GetItem_GetMailItem_EXMonitor	Healthy
UpdateItem_UpdateMessageForCompose_EXMonitor	Healthy
UpdateItem_UpdateMessageForComposeSend_EXMonitor	Healthy
OwaTooManyWebAppStartsMonitor	Unknown

FIGURE 2-32 Successful OWA test results

The Get-ServerHealth cmdlet displays components as healthy, unhealthy, or unknown. For components that are unhealthy, you should investigate further to determine the root cause of the issue. The Microsoft Exchange logs in the Event Viewer are a good place to start.

If you identify trouble with Outlook on the web, you have a few actions that you can take to try to resolve the issue. First, you can recycle the primary IIS application pool for Outlook on the web. To do so, run the IIS Manager. Next, click Application Pools in the left pane, right-click MSEExchangeOWAAppPool in the right pane, and then click Recycle. [Figure 2-33](#) shows the IIS Manager screen with the right-click menu displayed.



**FIGURE 2-33** Recycle Outlook on the web IIS application pools

IIS provides the backend functionality for Outlook on the web. Sometimes, resetting IIS can resolve some issues. To reset IIS on an Exchange Mailbox server, without impacting current connections, run the following command:

```
iisreset /noforce
```

There are other steps you can take to try to resolve issues, including:

- Make sure all of the Exchange-related application pools are running.
- Make sure the default website is running.
- Make sure the World Wide Web Publishing Service is running.
- Check the most recent log file in  
%systemdrive%\inetpub\logs\LogFiles\W3SVC1.

If all else fails, you can reboot the server to try to resolve the issue. A reboot should be considered a last resort because it impacts your users.

## Troubleshoot POP3 and IMAP4

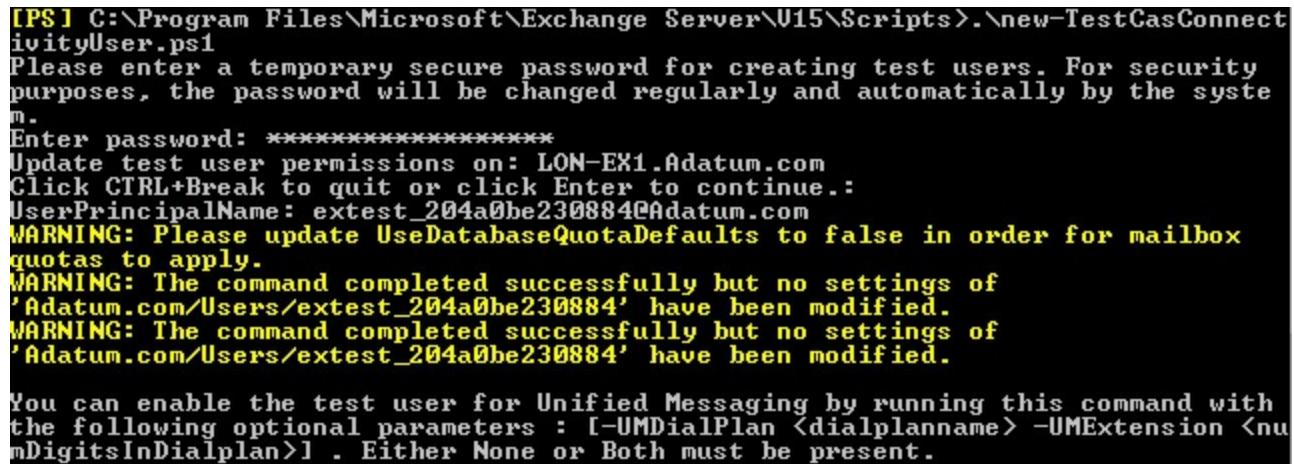
You can troubleshoot POP3 and IMAP4 by using built-in PowerShell cmdlets. The Test-PopConnectivity and Test-ImapConnectivity cmdlets can be used to test the POP3 and IMAP4 functionality in an Exchange environment. Both commands can be run similarly:

[Click here to view code image](#)

```
Test-PopConnectivity -ClientAccessServer EX01.contoso.com  
Test-ImapConnectivity -ClientAccessServer EX01.contoso.com
```

However, if you are running these commands for the first time you might receive an error if a test user does not exist. This is because the commands require a credential, either a test account or credentials that you specify in order to function properly. You can use the pipeline to specify credentials with the Get-Credential cmdlet, or you can set up a test user account.

By default, Exchange Server comes with several pre-defined scripts in the installation directory. In a default installation, the scripts folder is located at: %systemdrive%\Program Files\Microsoft\Exchange Server\V15\Scripts. One of the available scripts is named new-TestCasConnectivityUser.ps1 and it creates a test user that some of the client access troubleshooting cmdlets, such as Test-PopConnectivity and Test-ImapConnectivity, use automatically. When running the script, you are prompted to enter a password for the test user account. The password is changed by the system and updated at regular intervals without requiring input from an administrator. [Figure 2-34](#) shows creating a test user account by using the predefined script.



```
[PS] C:\Program Files\Microsoft\Exchange Server\V15\Scripts>.\new-TestCasConnectivityUser.ps1  
Please enter a temporary secure password for creating test users. For security purposes, the password will be changed regularly and automatically by the system.  
Enter password: *****  
Update test user permissions on: LON-EX1.Adatum.com  
Click CTRL+Break to quit or click Enter to continue.:  
UserPrincipalName: extest_204a0be230884@Adatum.com  
WARNING: Please update UseDatabaseQuotaDefaults to false in order for mailbox quotas to apply.  
WARNING: The command completed successfully but no settings of 'Adatum.com/Users/extest_204a0be230884' have been modified.  
WARNING: The command completed successfully but no settings of 'Adatum.com/Users/extest_204a0be230884' have been modified.  
You can enable the test user for Unified Messaging by running this command with the following optional parameters : [-UMDialPlan <dialplanname> -UMEExtension <numDigitsInDialplan>] . Either None or Both must be present.
```

FIGURE 2-34 Test user script

After the test user account has been successfully created, you can run both the Test-ImapConnectivity and the Test-PopConnectivity commands from the Exchange server.

Finally, the Remote Connectivity Analyzer can test IMAP and POP connectivity with an on-premises Exchange environment.



## Exam Tip

In addition to using the troubleshooting tools, you should check to see if the related Exchange services are running. POP3 has two services, Microsoft Exchange POP3 and Microsoft Exchange POP3 Backend, and IMAP4 has two services, Microsoft Exchange IMAP4 and Microsoft Exchange IMAP4 Backend.

By default, IMAP and POP3 aren't running. From a network perspective, you can test connectivity to the ports by using a network tool such as the Telnet client. POP3 uses TCP port 110 for unencrypted connections and TCP port 995 for encrypted connections. IMAP4 uses TCP port 143 for unencrypted connections and TCP port 993 for encrypted connections.

## Troubleshoot authentication

Authentication errors primarily occur at one of two points during the connection process:

- During the client connection
- At the IIS connection point

To begin troubleshooting authentication issues, you can use the event logs, Exchange Server logs, and IIS logs to identify specific services or accounts that might be causing authentication problems.

While authentication is a huge topic, you should focus on knowing the different authentication methods used in Exchange environments:

- **Basic authentication** Basic authentication prompts users for their usernames and passwords. The credentials are sent to Exchange Server in plain text. You can encrypt the communication, and therefore the credentials, by using an SSL certificate. You should never use basic authentication without SSL or TLS.
- **Integrated Windows authentication** Integrated Windows authentication is typically relegated to your local area network (LAN) because that is usually the location where users are signed into your domain. Internet users and users using personal devices cannot use Integrated Windows authentication. Some reverse proxy solutions support Integrated Windows authentication.
- **Forms-based authentication** Forms-based authentication is the default authentication for Outlook on the web and the Exchange Admin Center. Forms-based authentication requests credentials in a web-based form.

- **Kerberos** MAPI clients, such as Outlook, can use Kerberos authentication. Kerberos authentication is preferred over other authentication protocols because it offers enhanced performance without scalability concerns. To use Kerberos, you need an Alternate Service Account (ASA). There are a couple of key facts to understand about ASAs:
    - You use the `RollAlternateserviceAccountCredential.ps1` built-in script to create a new ASA.
    - You cannot share an ASA between different versions of Exchange. If you have Exchange Server 2016 and Exchange Server 2013, you need at least one ASA for each.
- 



### Exam Tip

The exam will not focus on troubleshooting authentication from an Active Directory Domain Services (AD DS) perspective.

---

## Troubleshoot Autodiscover

Autodiscover is a required component of Exchange Server configurations and must be configured correctly to enable Outlook and mobile clients to connect successfully. To test and troubleshoot Autodiscover, you can use the following tools:

- Microsoft Remote Connectivity Analyzer
- Microsoft Support and Recovery Assistant
- Test E-Mail AutoConfiguration tool

You can discover some additional tips for troubleshooting Autodiscover by looking at the tests the Remote Connectivity Analyzer tool performs when you run the Outlook Autodiscover test. The results for the svidergol.com domain are shown in [Figure 2-35](#).

The Microsoft Connectivity Analyzer is attempting to test Autodiscover for brian@svidergol.com. Autodiscover was tested successfully.

► Additional Details

▲ Test Steps

Attempting each method of contacting the Autodiscover service.

The Autodiscover service was tested successfully.

► Additional Details

▲ Test Steps

Attempting to test potential Autodiscover URL https://svidergol.com:443/Autodiscover/Autodiscover.xml

Testing of this potential Autodiscover URL failed.

► Additional Details

► Test Steps

Attempting to test potential Autodiscover URL https://autodiscover.svidergol.com:443/Autodiscover/Autodiscover.xml

Testing of this potential Autodiscover URL failed.

► Additional Details

► Test Steps

Attempting to contact the Autodiscover service using the HTTP redirect method.

The Autodiscover service was successfully contacted using the HTTP redirect method.

► Additional Details

▲ Test Steps

Attempting to resolve the host name autodiscover.svidergol.com in DNS.

The host name resolved successfully.

► Additional Details

Testing TCP port 80 on host autodiscover.svidergol.com to ensure it's listening and open.

The port was opened successfully.

► Additional Details

The Microsoft Connectivity Analyzer is checking the host autodiscover.svidergol.com for an HTTP redirect to the Autodiscover service.

The redirect (HTTP 301/302) response was received successfully.

► Additional Details

Attempting to test potential Autodiscover URL https://autodiscover-s.outlook.com/Autodiscover/Autodiscover.xml

Testing of the Autodiscover URL was successful.

► Additional Details

► Test Steps

**FIGURE 2-35** Remote Connectivity Analyzer Outlook Autodiscover test results

When troubleshooting, it is a good idea to start at the client level, especially if only a single user has reported an issue. For example, for Autodiscover, you would start by using the Test E-mail AutoConfiguration tool on the user's computer that is reporting a problem. If multiple users are reporting the same problem, you would start by using the Remote Connectivity Analyzer tool.

## Troubleshoot Exchange ActiveSync

There are multiple methods for troubleshooting Exchange ActiveSync. Four tools you can use to troubleshoot Exchange ActiveSync are:

- Microsoft Remote Connectivity Analyzer
- Microsoft Support and Recovery Assistant
- Windows PowerShell
- Mobile phone testing

The first two tools in the list have previously been discussed. The PowerShell cmdlet to troubleshoot Exchange ActiveSync is Test-ActiveSyncConnectivity. For example, to troubleshoot ActiveSync on a server named NYC-EX1 in the contoso.com domain, run the following command:

[Click here to view code image](#)

```
Test-ActiveSyncConnectivity -ClientAccessServer nyc-ex1.contoso.com
```

The Remote Connectivity Analyzer performs several tests as part of its ActiveSync troubleshooting test. [Figure 2-36](#) shows the results of an ActiveSync test against an Office 365 mailbox.

The screenshot displays the Microsoft Connectivity Analyzer interface. At the top, a green checkmark icon indicates that the Exchange ActiveSync test was successful. Below this, a summary message states: "The Microsoft Connectivity Analyzer is testing Exchange ActiveSync. Exchange ActiveSync was tested successfully." A "Test Steps" section follows, listing various tests with their outcomes:

- Attempting the Autodiscover and Exchange ActiveSync test (if requested). Autodiscover was successfully tested for Exchange ActiveSync.
  - Additional Details
  - Test Steps
- Validating Exchange ActiveSync settings. Exchange ActiveSync URL <https://outlook.office365.com/Microsoft-Server-ActiveSync> was validated successfully.
  - Additional Details
  - Test Steps
- Attempting to resolve the host name outlook.office365.com in DNS. The host name resolved successfully.
  - Additional Details
  - Test Steps
- Testing TCP port 443 on host outlook.office365.com to ensure it's listening and open. The port was opened successfully.
  - Additional Details
  - Test Steps
- Testing the SSL certificate to make sure it's valid. The certificate passed all validation requirements.
  - Additional Details
  - Test Steps
- Checking the IIS configuration for client certificate authentication. The test passed with some warnings encountered. Please expand the additional details.
  - Additional Details
- Testing HTTP Authentication Methods for URL <https://outlook.office365.com/Microsoft-Server-ActiveSync>. The HTTP authentication methods are correct.
  - Additional Details
  - Test Steps
- An ActiveSync session is being attempted with the server. Testing of an Exchange ActiveSync session completed successfully.
  - Additional Details
  - Test Steps

**FIGURE 2-36** Remote Connectivity Analyzer ActiveSync test results

Beyond the typical tools for troubleshooting, you can also use an ActiveSync client to troubleshoot issues. Often, setting up a client for ActiveSync provides clues that help you locate problems.

## Troubleshoot proxy and redirection issues

Exchange Server 2016 proxies or redirects a client request, depending on the requesting protocol and connection type. Troubleshooting these layers of Exchange can require additional insight into the event log and log files from the Exchange server environment. It is important to review these logs in the event of an error when you suspect a proxy or redirection issue might arise.

The most common error that can occur from proxy or redirection requests is if the server that is forwarding the request does not know that the destination is offline. If a different server is hosting an active copy of the database, the originating server that received the request might forward the request to a server that is offline. This is only temporary, and can be solved by configuring a DAG.

## Summary

- Numerous tools can be used to troubleshoot components of Exchange
  - Windows PowerShell
  - Microsoft Remote Connectivity Analyzer
  - Microsoft Support and Recovery Assistant
  - Pre-defined scripts
  - Outlook Connection Status
  - Test E-Mail AutoConfiguration Tool
- Create a test user by using a predefined script

## Skill 2.5: Plan, deploy, and manage a site-resilient client access services solution

This section focuses on planning, deploying, and managing a site-resilient configuration for Exchange 2016. Exchange 2016 provides many benefits and functionality for site-resilient configurations, especially compared to previous versions of Exchange. Namespace requirements, DAG configuration, and certificates are all discussed in this section, and how they relate to planning and deploying a site-resilient solution.

## This section covers how to:

- [Plan site-resilient namespaces](#)
- [Configure site-resilient namespace URLs](#)
- [Perform and test steps for site failover and switchover](#)
- [Plan certificate requirements for site failovers](#)
- [Manage expected client behavior during a failover and switchover](#)

## Plan site-resilient namespaces

Earlier versions of Microsoft Exchange required several namespaces, especially for a site-resilient configuration. A site-resilient configuration for Exchange 2010 might have been configured as follows:

- A primary datacenter namespace ([mail.adatum.com](#))
- A secondary datacenter namespace ([mail2.adatum.com](#))
- A primary datacenter OWA fallback namespace ([mailpri.adatum.com](#))
- A secondary datacenter OWA fallback namespace ([mailsec.adatum.com](#))
- A primary datacenter RPC Client Access namespace ([rpc.adatum.com](#))
- A secondary datacenter RPC Client Access namespace ([rpc2.adatum.com](#))
- A transport namespace ([mailsec.adatum.com](#))
- An Autodiscover namespace ([autodiscover.adatum.com](#))

In addition to numerous and complex namespace configurations, many of these namespaces also require certificates, further complicating the process.

Exchange 2013 introduced, and Exchange 2016 uses, a simplified namespace configuration, where the eight required namespaces from the Exchange 2010 configuration are reduced to only two required namespaces. As mentioned previously with load balancing, additional namespaces can be configured, but aren't necessary. The two required namespaces are:

- Client access ([mail.adatum.com](#))
- Autodiscover ([autodiscover.adatum.com](#))

One reason for the reduction in required namespaces is that Exchange 2016 does not use RPC for any client access. Therefore, the two RPC namespaces are not required in an Exchange 2016 environment. Another reason, as mentioned earlier in this chapter, is that client requests are proxied or redirected to the Mailbox server that has an active copy of the database where the user's mailbox is located. [Figure 2-37](#) illustrates the connection process for a user account that uses a single namespace across multiple

sites. Note that the user can connect through four possible paths. In all cases when a user initially connects to a Mailbox server that doesn't contain that user's mailbox, the connection is proxied to the server that does contain the mailbox.

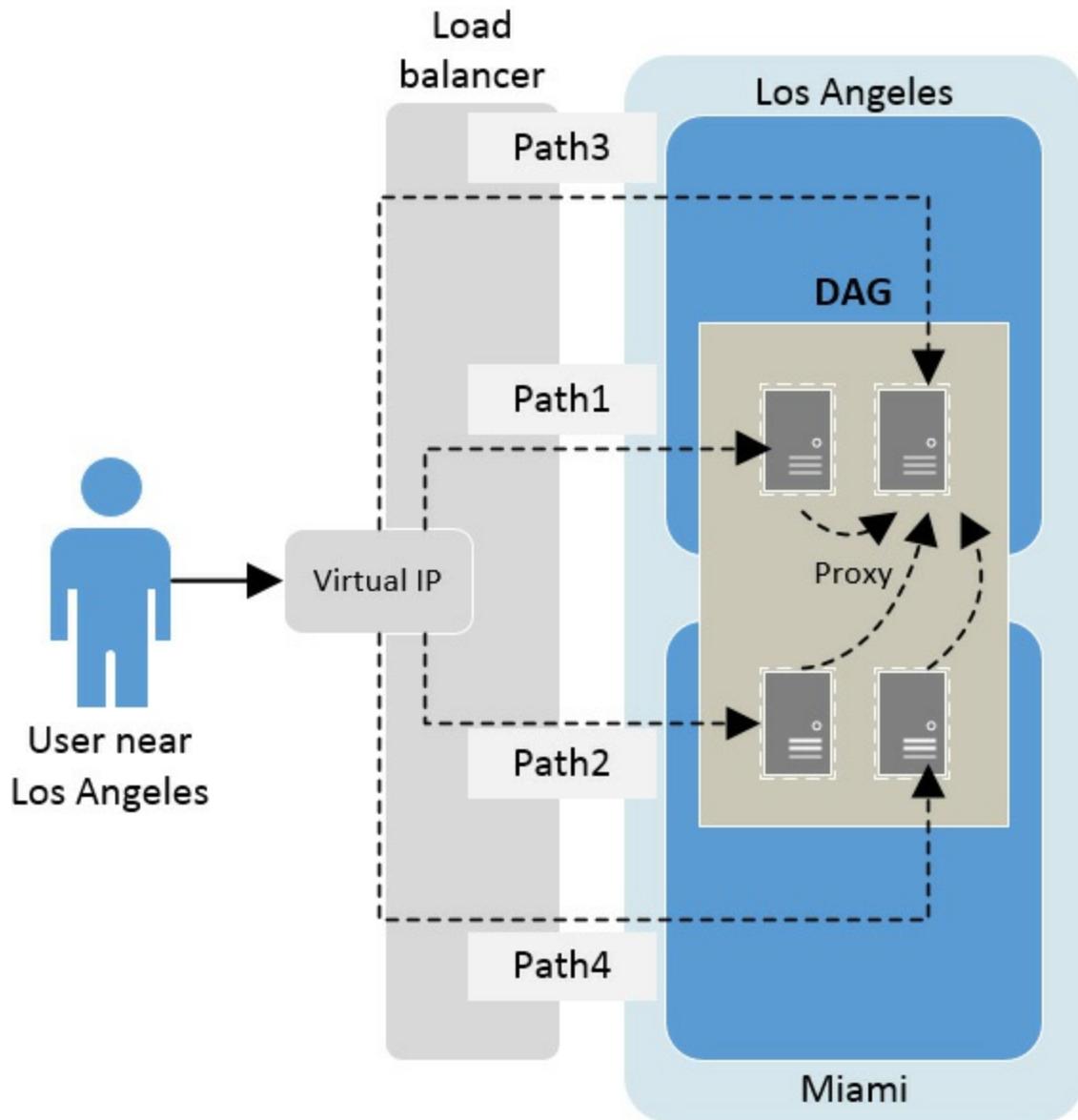


FIGURE 2-37 Single namespace across two sites with four possible paths

Typically, AD DS and Exchange objects are organized into sites. Unlike previous versions of Exchange Server, Exchange Server 2016 does not require that a namespace be dedicated or assigned to a specific AD DS site. This is because of how the proxy connection occurs, sending any client request to a server with an active database copy. Therefore, only one namespace is required for each site in the environment. This even means that DAGs can be spanned across multiple sites using a single namespace. This also reduces the number of namespaces that are required by not needing unique namespaces for each site and by eliminating the namespaces for DAG activation.

Given these scenarios with Exchange 2016, there are two models that can be used to

build an environment:

- Use a single namespace for a site-resilient configuration. This is the model shown in the [Figure 2-37](#). In this model, the downside is that clients might have a better user experience based on where they are initially connected. For example, if a user near Los Angeles is load balanced to Miami and then proxied back to Los Angeles, where the user's mailbox is located, the performance isn't as good as if the user is initially connected to a server in Los Angeles. This is a trade-off. The user experience might not vary if a user is centrally located between two datacenters or if the datacenters are fairly close and have high bandwidth, low latency connections to each other.
- Use dedicated namespaces for each site. This model ties users to specific sites for regular mailbox access. Users only connect to a separate site in a failover scenario. Failover to another site is a task performed by an administrator. In this model, you usually use multiple namespaces, especially if clients only have connectivity to one datacenter during normal operations.

The details of these approaches are discussed later in this section.

## Network requirements

To configure multi-site resiliency with DAGs and Exchange 2016, each DAG must have a MAPI network defined. The MAPI network is used to communicate with the other Exchange members of the DAG. Additionally, a replication network can be configured for log shipping and database seeding. These two networks can be combined into a single network.

It is possible to use two network adapters, one for each network as required, but note that each member of the DAG must have the same number of network connections defined. If a single network adapter is used on one server in the DAG, all members must be configured to use a single network. Additionally, each member can have only one MAPI network defined. However, more than one replication network can be defined, as needed.



### Exam Tip

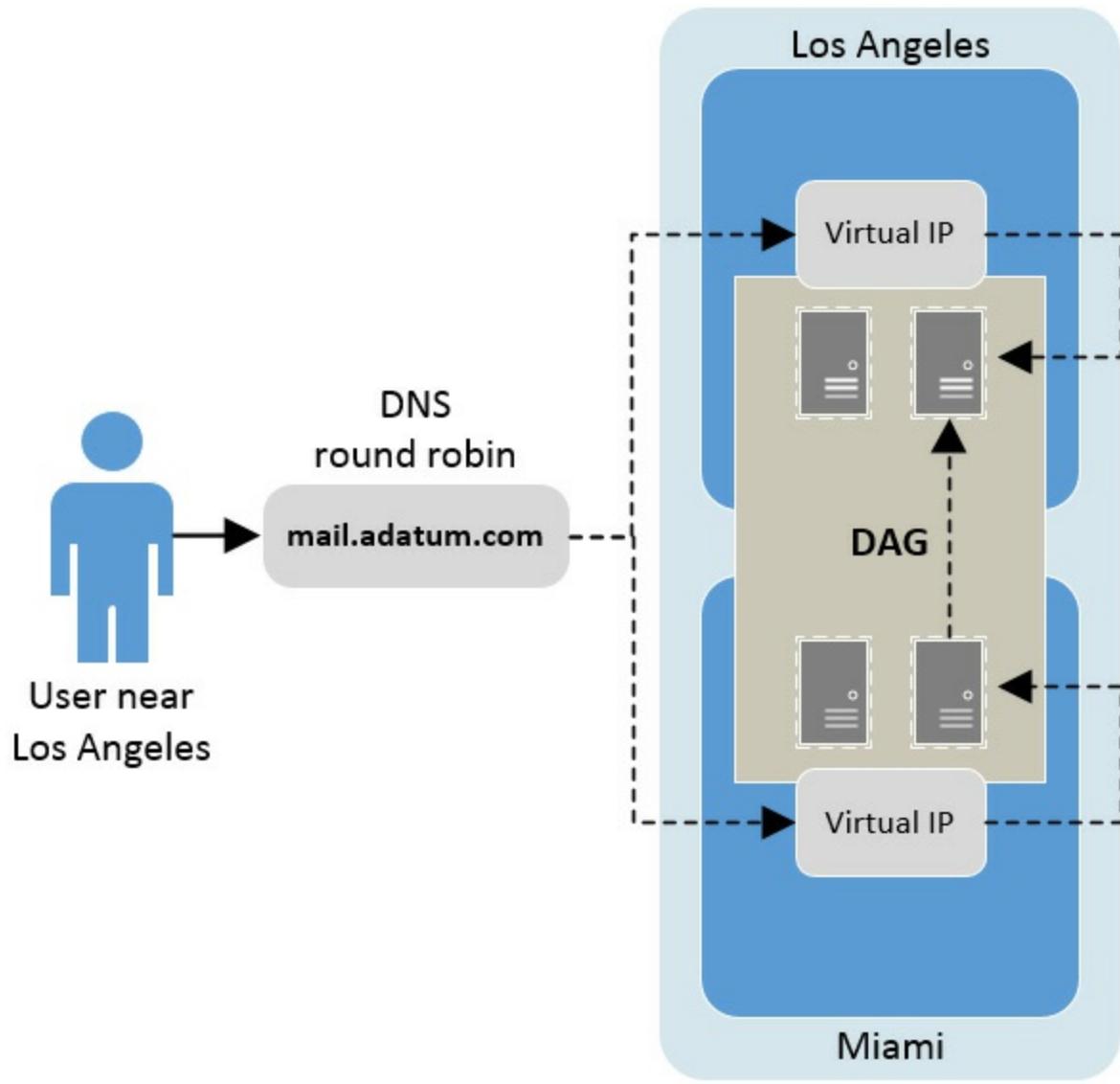
Round-trip latency must not exceed 500 milliseconds between each member of the DAG. Additionally, while IPv4 and IPv6 are supported when used together, an IPv6-only configuration is not supported.

---

## Single site-resilient namespace

In this scenario, you configure a single DAG that is used across the sites. This model is sometimes referred to as the unbound model because users are not bound to a specific site. The DAG has Mailbox servers in each site which often have all active copies of the database. Alternately, you can deploy a single DAG with active databases in one site and backup databases in the second site. With this configuration, an external client connection can be sent to the WAN of either of the sites, and a Mailbox server with an active copy of the database responds.

A single namespace is recommended for configuring a DAG across sites, so that either site can respond to a client access query. This enables you to create a load balancing configuration between sites, where the namespace simply resolves to the load balancing virtual IP addresses. [Figure 2-38](#) illustrates the concept of using load balancing across two sites with a single namespace. In this example, DNS round robin is used for the initial connection. Each site, Los Angeles and Miami, has local load balancing. Two of the four possible paths are shown. Note that you can opt to use a third-party geo-load balancing solution to direct users to their closest site based on their source IP address or other algorithm.



**FIGURE 2-38** Load balancing a single namespace across sites with load balancers at each site

### Dedicated namespaces for each site

A different approach to namespaces is to configure a dedicated namespace for each site. With this configuration, you are configuring a user preference for a specific site by having them use a specific site's namespace. In the event of a failover, the user uses the secondary site with a different namespace. Note that this scenario can also be accomplished by using a load balancer that performs health checks or has a weighted priority configuration.

In this scenario, each namespace would typically have its own DAG. Each DAG would contain a set of Mailbox servers and databases for that specific datacenter. By controlling which databases are mounted and active, you control how the connection requests are responded from. [Figure 2-39](#) illustrates how two namespaces can be configured in a site-resilient configuration. In this example, users connect to their

closest site because they are using site-specific FQDNs.

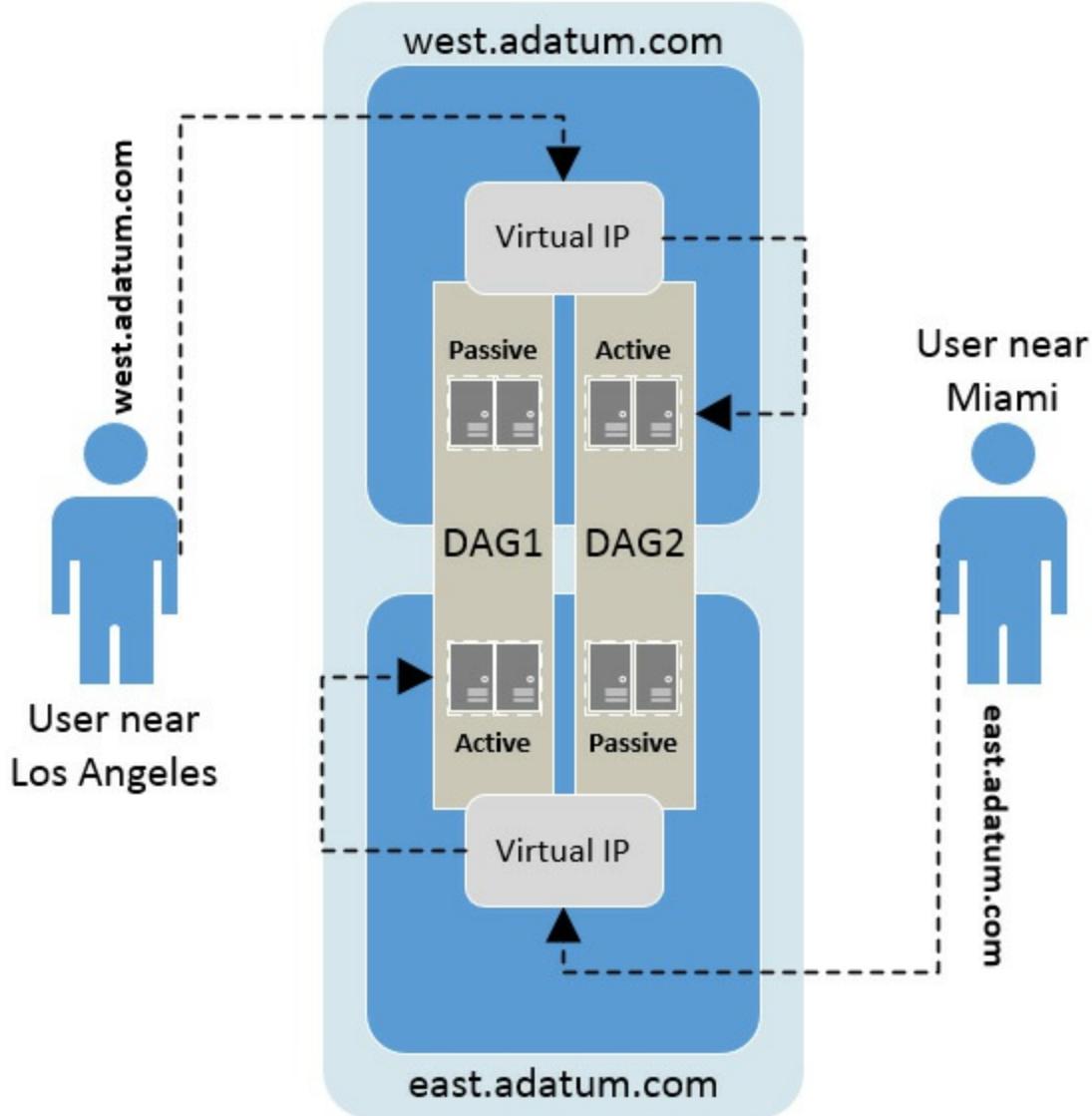


FIGURE 2-39 Two namespaces in a site-resilient configuration

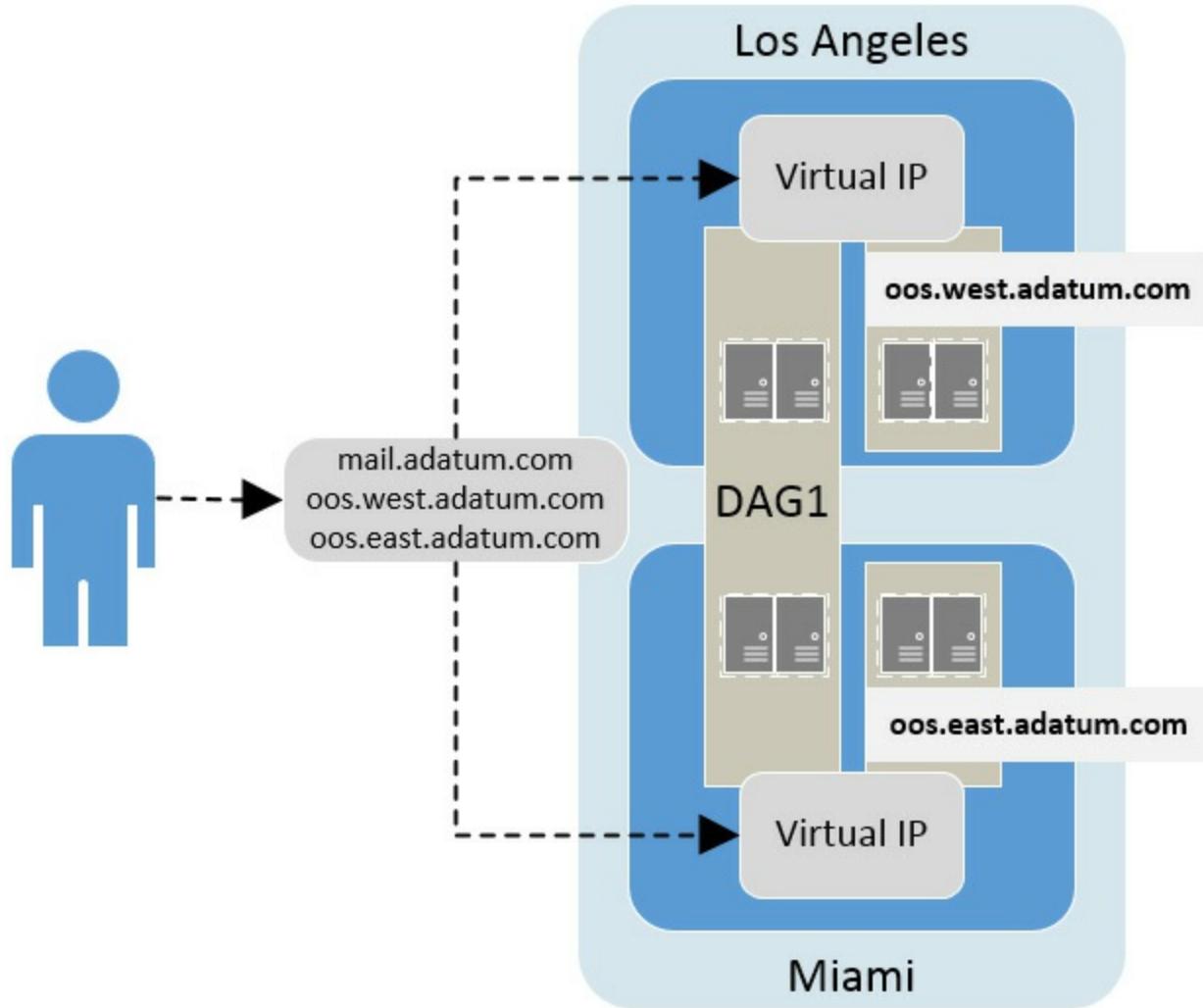
## Autodiscover

The only exception to either of the deployment scenarios previously discussed is for the Autodiscover service. Exchange 2016 uses Autodiscover for client configuration and a dedicated namespace must be configured, regardless of the site-resilient deployment method used.

## Site resiliency with document collaboration

Exchange 2016 introduces document collaboration features that can be used with Outlook on the web. To use these features, you must also have an Office Online Server. For site resilient deployments, you must have an Office Online Server in each site that is part of the namespace.

A dedicated namespace for each site must be configured for the Office Online Server configuration. This namespace is separate from the namespace that is used for the Exchange 2016 environment or the Autodiscover service. This also means that you can still use a single namespace for the multi-site Exchange configuration. [Figure 2-40](#) illustrates a single namespace for Exchange services, [mail.adatum.com](mailto:mail.adatum.com) in this example, and dedicated namespaces for Office Online Server, [oos.west.adatum.com](http://oos.west.adatum.com) and [oos.east.adatum.com](http://oos.east.adatum.com).



**FIGURE 2-40** Namespace configuration with Office Online Server

## Configure site-resilient namespace URLs

As discussed in the previous section, Exchange Server 2016 requires a minimal number of namespaces for core functionality. A basic namespace configuration can consist of the following FQDNs:

- Client access [mail.adatum.com](mailto:mail.adatum.com).
- Autodiscover [autodiscover.adatum.com](http://autodiscover.adatum.com).

Additional namespaces can be configured, if necessary. These include:

- Dedicated namespaces for each site ([west.mail.adatum.com](https://west.mail.adatum.com) and [east.mail.adatum.com](https://east.mail.adatum.com))
- Office Online Server ([oos.west.adatum.com](https://oos.west.adatum.com) and [oos.east.adatum.com](https://oos.east.adatum.com)).

Office Online Server is unique with Exchange 2016, because although Exchange does not require dedicated namespaces across multiple sites, Office Online Server does. The Office Online Server URL is configured at the Mailbox server level. Therefore, if an Exchange site fails, the Mailbox servers in the secondary site automatically use the necessary Office Online Servers located within the site. Exchange 2016 uses the Set-MailboxServer cmdlet to configure the local Office Online Server. For example, to configure an Exchange server named EX01 for a primary Office Online Server location, run the following command:

[Click here to view code image](#)

```
Set-MailboxServer EX01 -WACDiscoveryEndPoint  
https://oos.west.adatum.com/hosting/  
discovery
```

## Internal and External namespaces

Since Exchange 2007, the recommended namespace configuration is to use split-DNS. Split-DNS enables a different IP address to be returned for a DNS query, depending on the location of the client. Therefore, if the client is internal to the company's network, it receives the internal IP address of a load balancer for Exchange server. If the client is external, it receives a public IP address. This simplifies the namespace configuration, requiring only one namespace, such as [mail.adatum.com](https://mail.adatum.com), regardless of where the client initiates the connection. In addition to the client, it also simplifies the Exchange server configuration, as the InternalURL and ExternalURL parameters can be configured to the same value.

If split-DNS is not used in your environment, Exchange 2016 supports configuring separate URLs for internal and external access.



### Exam Tip

If split-DNS is configured, both internal and external access settings must be configured to use the same type of authentication. Outlook prioritizes internal settings over external settings. If the same namespace is used for both internal and external settings, regardless of the client's actual location, the internal authentication settings will be used.

---

## Location-based namespaces

Location-based namespaces provide a method of enabling users to connect to a Mailbox server that is located close to them geographically. In a global organization, it is common to have a site-resilient configuration strictly for one country/region, and a separate multi-site configuration for another country/region. In this example, you can have different namespaces for each configuration. [Figure 2-41](#) illustrates using different namespaces for the geographic locations. In this example, DNS round robin is used for the initial connection and each FQDN resolves to one of two geographic namespaces. Local load balancing is shown for each of the four sites.

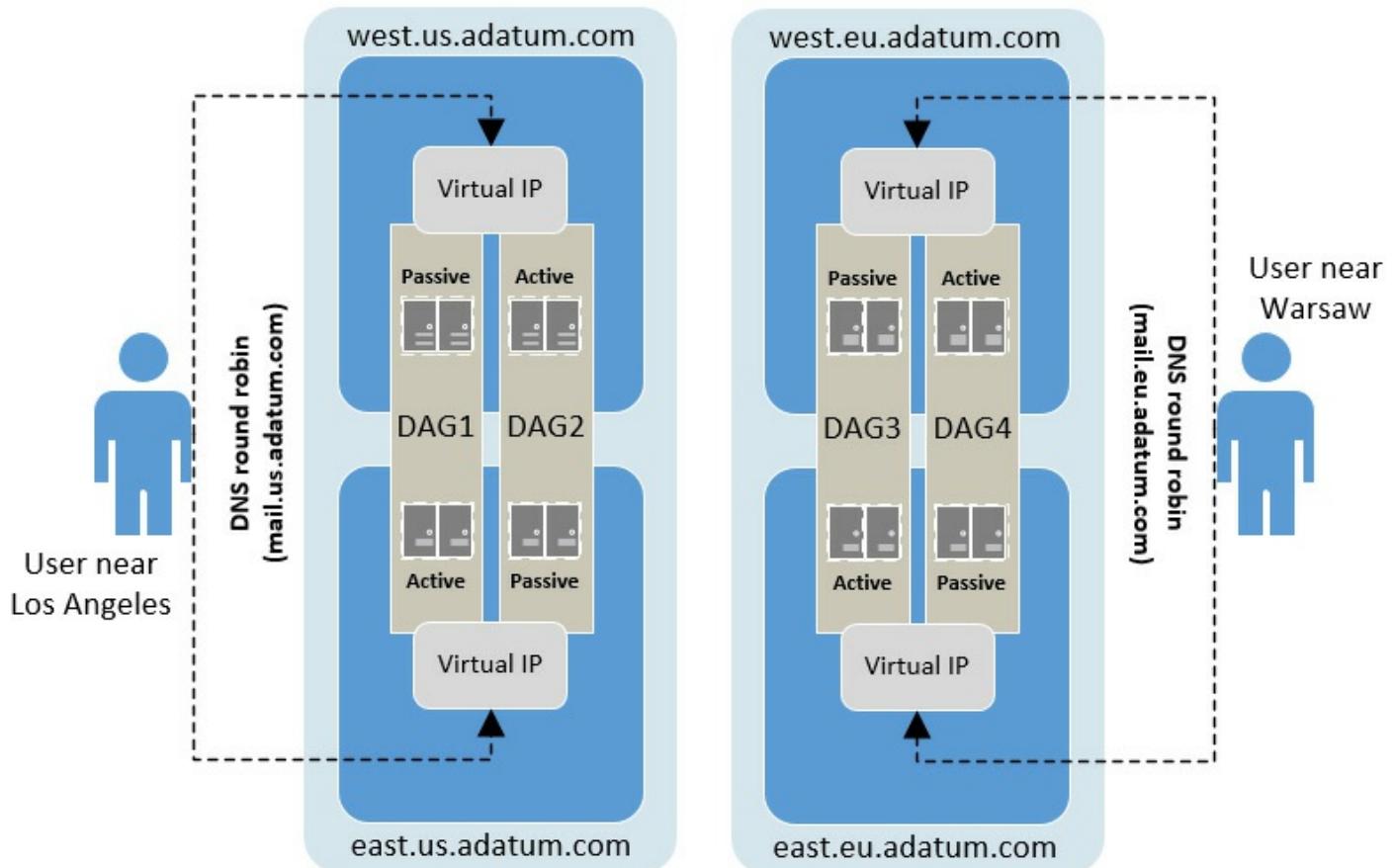


FIGURE 2-41 Location-based namespaces across different geographic regions

## Perform and test steps for site failover and switchover

The architecture Exchange 2016 uses provides for automatic failover when configured to use a single namespace. By having a single namespace across sites, client connections are always directed to a load balancer or edge connection for a DAG. At this point, the client connection is always redirected or proxied to a Mailbox server that has an active copy of the database. This process occurs regardless of which site is used, or where the client connection originated from. There are no specific actions you must take to perform a failover of an Exchange environment.

While namespaces and load balancing provides a method of automatic failover for client access, the Exchange servers themselves must provide failover as well. When using a DAG, the witness server is the key to providing automatic failover for individual database servers. A good practice is to place a witness server in a third location within the environment, segmented from possible network failures that would impact Exchange. If a third location is not available within the local environment, another option is to configure the witness in the public cloud, such as Microsoft Azure. Both options provide a method of database-level failover, regardless of which site experiences a failure. Note that one witness server can be used for multiple DAG configurations.

## Plan certificate requirements for site failovers

Exchange 2016 does not have any specific certificate requirements when deploying a DAG in a single datacenter environment. In a multi-site environment however, a certificate is required depending on the client services in use. Best practice is to use as few certificates as possible, one is optimal, while configuring subject alternative names for additional datacenters or namespaces. Thus, even with multiple regions and datacenters, you can obtain a single certificate as long as the certificate handles all of the names in use in your environment.

## Manage expected client behavior during a failover and switchover

The general concept behind providing automatic failover in a multi-site Exchange environment is to ensure that client connections are always serviced. If an automatic failover is implemented efficiently, a client should not even realize a failover has occurred. At most, a client's Outlook application might experience a slight delay if the user is expecting an email message. Otherwise, the client does not have any knowledge of any failover or fallback during normal operations. The client should be configured to use the global namespace, while the load balancing and DAG solutions take care of any backend failover that might need to occur. When using multiple namespaces and a manual site failover, it is important to notify users before a planned failover.

## Summary

- You should use a single namespace across DAGs. It simplifies the environment for administrators and for users. It is important to minimize administrative overhead and using a single namespace can do that.
- Dedicated namespaces can be used if necessary or for geographical reasons. In general, use dedicated namespaces only when you have to.
- Additional namespaces are required for document collaboration with Office Online Server. In complex environments, you often end up with more than one

namespace just for OOS.

- In the best possible configuration, Exchange clients should not be impacted during a site failover.

## Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find answers to this thought experiment in the next section.

You are the email administrator for Wingtip Toys, a leading toy developer and manufacturer specializing in virtual reality and interactive game content. The Wingtip Toys headquarters is located in Portland, Oregon. Its manufacturing plant is located in Boise, Idaho. Both locations have datacenters on-premises. There are 1,100 employees, with an expectation to grow 25 percent over the next year. All servers run Windows Server 2012 R2. All client computers in the domain run Windows 10 and Office 2016. The current email platform is Exchange Server 2010. The following challenges have been identified:

- **Email access differs based on location** Currently users must remember two separate URLs for web mail access depending on whether they are inside or outside of the corporate network. This has been causing confusion.
- **Support for personal devices is in demand** Employees continue to bring their personal devices to the office with an expectation for BYOT support. iOS devices in particular have been difficult to support due to the variety of operating system versions and corresponding issues with the existing email server.
- **Client connectivity is limited to a single Client Access Server** Even though the organization has more than one CAS server, all client connectivity goes to only one of them. This occasionally results in degraded performance.

The company has decided to upgrade to Exchange Server 2016. The company has identified the following requirements:

- **Simplify the user experience for email connectivity** Provide a solution that makes it easy for users to access their email, regardless of the network they are connected to.
- **Enable mobile device support** Configure operating system restrictions, limiting devices to those running iOS 9 or later.
- **Provide a solution that maximizes the efficiency of the email environment and improves overall reliability** The company wants to take advantage of having multiple Exchange servers by spreading the load across all applicable servers.

As the email administrator, you need to design and deploy an Exchange Server 2016 solution to meet the requirements. What should you do?

## Thought experiment answer

This section contains the solution to the thought experiment.

To simplify the user experience for email connectivity, you should implement a single namespace using [mail.wingtiptoys.com](http://mail.wingtiptoys.com). This enables users to utilize one FQDN for accessing Exchange services such as ActiveSync and Outlook on the web. Using a single namespace also reduces user confusion and simplifies the user experience. As part of using the single namespace, you should use split DNS. This enables you to direct internal users to internal IP addresses and direct external users to external IP addresses while all users use the same namespace.

For mobile device support, you should implement mobile device access rules that limit devices to those running iOS 9 or later. This prevents devices running unapproved versions of iOS from connecting to Exchange. As an additional measure, you should plan on running ActiveSync device reports on a routine schedule. This information is helpful in accessing the device types and operating systems that have been approved, as well as highlighting all devices attempting to gain access to Exchange.

To maximize the efficiency of the email environment and improve overall reliability, you should implement load balancing using layer 7. Add all applicable Exchange servers to the load balancer pool. This ensures all incoming connections are balanced evenly across the environment. This also fixes the problem in the current environment where a single server is being overloaded and exhibiting degraded performance.

# **Chapter 3. Plan, deploy, manage, and troubleshoot transport services**

As an email administrator, you deal with several technologies to provide all of the collaboration functionality in Exchange Server. One could argue, however, that none of the technologies are as important as the transport services. Transport services handle the movement of email data between components, servers, and organizations. For the exam, it is critical that you have a thorough understanding of email flow. You need to understand the planning aspects, the deployment methods and steps, and know how to manage and monitor the components. This chapter discusses how to plan, deploy, manage, and monitor transport-related services.

## **Skills in this chapter:**

- [Plan, deploy, and manage transport services](#)
- [Troubleshoot and monitor transport services](#)
- [Plan, deploy, and manage message hygiene](#)
- [Plan, deploy, and manage site resilient transport services](#)

### **Skill 3.1: Plan, deploy, and manage transport services**

Transport services make up all of the components that participate in email data transport. In Exchange Server 2016, transport services are split between two roles, the Edge Transport role and the Mailbox Server role. The Mailbox Server role provides client access, mailbox database services, and transport services. However, there is logical segmentation between the services. For the exam, you need to be intimately familiar with transport services, including being able to plan, deploy, manage, and troubleshoot the services in a variety of real-world scenarios.

## This section covers how to:

- [Plan a solution that meets SLA requirements around message delivery](#)
- [Plan inter-site mail flow](#)
- [Plan inter-org mail flow](#)
- [Plan, deploy, and configure redundancy for intra-site scenarios](#)
- [Plan and configure for Safety Net](#)
- [Plan and configure for shadow redundancy](#)
- [Plan and configure for redundant MX records](#)
- [Plan, create, and configure TLS transport, Edge transport, Send/Receive connectors, transport rules, accepted domains, email address policies, and Address Rewriting](#)

## Plan a solution that meets SLA requirements around message delivery

A service level agreement (SLA) is an agreement between a service provider, in this case the IT team responsible for Exchange Server, and the customer, in most cases all of an organization's employees who rely on Exchange Server for collaboration. In large organizations, an SLA is often in place for many aspects of an IT environment, including the Exchange environment. For the exam, this skill is focused on message delivery only.

When you plan your Exchange environment for message delivery, you need to factor in the SLA requirements. A typical SLA for email message delivery usually includes the following components:

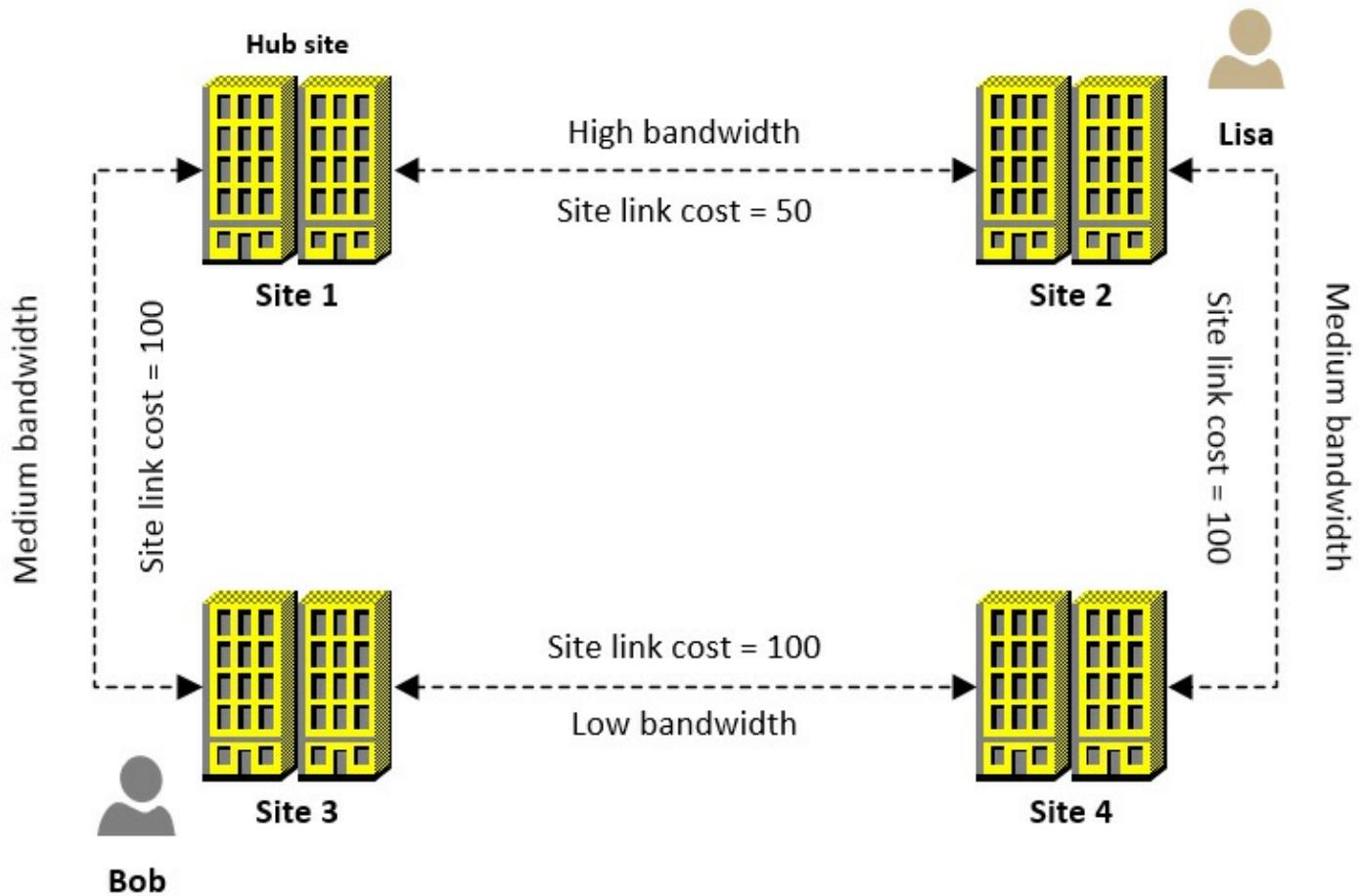
- **Performance** How long does it take an email message to be delivered to an internal or external destination? For most environments faster is better, but speed isn't the only factor. You also need to understand how to plan a solution around performance.
- **Uptime** The uptime dictates the availability of the email system for message delivery. Often, uptime is expressed in a percentage such as 99.9 percent. For many businesses, all critical services such as email need to be highly available.
- **Recoverability** In the event of] an outage, you need to bring email delivery services back up in an agreed upon amount of time, as documented in the SLA.

In this chapter, you are going to look at many of the transport components that can help you meet your SLA requirements.

## Plan inter-site mail flow

Inter-site mail flow is email delivery between different sites in your organization. For the exam, you need to be able to plan the email flow for an organization based on given scenarios. To do so, you must understand how email flows between sites. Exchange Server uses the Active Directory Domain Services (AD DS) sites and site links for message routing. Note that this is virtually unchanged since Exchange Server 2010, so if you have a pretty good understanding of it from earlier versions, you are well positioned for the topic on the exam.

[Figure 3-1](#) shows mail flow between two internal sites.



**FIGURE 3-1** Four sites and the AD DS site links connecting sites together

Imagine that you are the administrator for an organization with four sites, as shown in [Figure 3-1](#). Each site has a server that runs Exchange Server 2016. A user named Bob in Site 3 wants to send an email message to a user named Lisa in Site 2. How does Exchange Server transfer the email message from Site 3 to Site 2? In this scenario, there are two network paths:

- **Site 3 to Site 4 to Site 2** This path is one of two paths. Using this path, Exchange Server calculates the cost of the AD DS site links to see if this path has the lowest cost to Site 2. In this case, the total cost of the site links is 200.

- **Site 3 to Site 1 to Site 2.** This path is one of two paths. The AD DS site links add up to 150 for this path, which is lower, and therefore preferred, over the other path which has a site link cost of 200. This is the preferred path for routing the email.

In addition to looking for the lowest cost path, Exchange Server also figures out if there is a hub site along the lowest cost path. A hub site is a site you manually configure to be a hub site. In such a case, an Exchange server in the hub site always receives email destined for other sites. In the example, this means that email from Site 3 to Site 2 is handled by an Exchange Server in Site 1. Without such a hub site, the Exchange server in Site 3 delivers email directly to the Exchange server in Site 2, even if the network connectivity is configured to go through Site 1. To set a site named Site 1 as a hub site, run the following PowerShell command from the Exchange Management Shell:

[Click here to view code image](#)

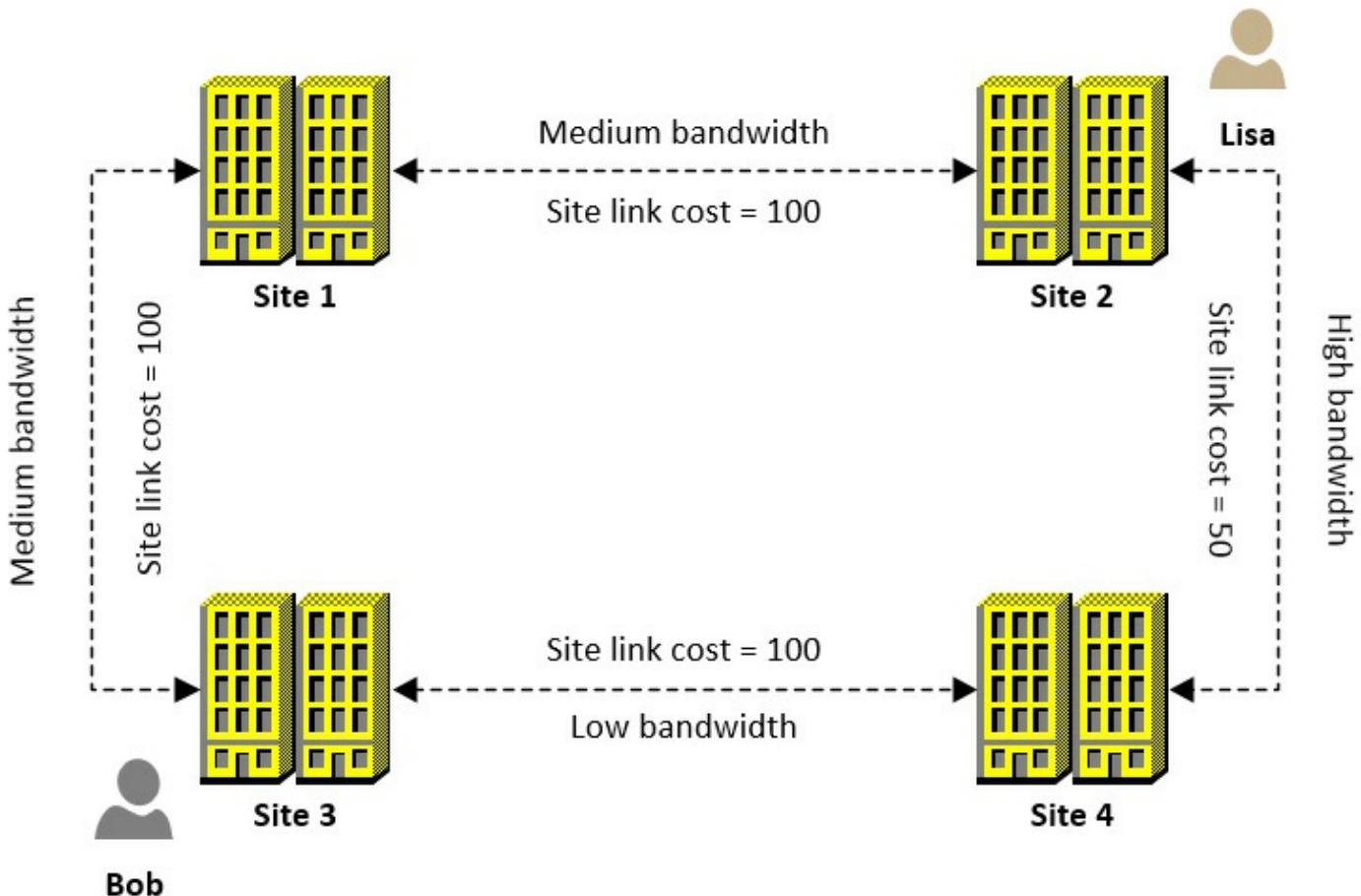
```
Set-AdSite "Site 1" -HubSiteEnabled $True
```

The example shown in [Figure 3-1](#) is just one of several network topologies. The following design principles were followed for this organization:

- **The bandwidth between Site 3 and Site 4 is low** You should avoid routing email over this connection if possible. The site link cost is 100, which is the default cost. To discourage use of the connection, you can adjust the site link to a higher cost, such as 200.
- **The bandwidth between Site 1 and Site 2 is high** You should use this segment to route email, because the AD DS site link cost has been set to 50, half of the default value of 100.
- **The network connections between Site 3 and Site 1 and between Site 4 and Site 2 are medium bandwidth** The AD DS site links have a default value of 100.
- **Designate Site 1 as a hub site to scan email messages for compliance before delivery** In some cases, organizations use hub sites for message compliance or message hygiene.

The main goal of your design should be to use the highest performing network segments to route email between sites. You can do that a number of different ways as long as the AD DS site link cost is lowest on the highest performing network path.

[Figure 3-2](#) shows an organization that has four sites and does not have a designated hub site.



**FIGURE 3-2** Four sites and the AD DS site links connecting sites together

Imagine that you are the administrator for the organization with four sites, depicted in [Figure 3-2](#). Bob in Site 3 sends an email to Lisa in Site 2. Which route does the email take? The email should travel from Site 3 to Site 4 to Site 2 because that is the lowest cost path based on the AD DS site link costs. As the email administrator however, you are concerned about the low bandwidth between Site 3 and Site 4. You are worried that email messages with large attachments might be delayed by using the lowest cost path. You can have the AD DS team adjust the site link costs to change the email route from Site 3 to Site 2, but the AD DS site link costs might be set with their current values for other reasons, such as to control the AD DS replication. In such situations, Exchange Server provides a separate way to control the email route. You can set Exchange-specific costs for an AD DS site link. These costs do not interfere with AD DS site link costs. To ensure that email routes from Site 3 through Site 1 on the way to Site 2, you can configure Exchange-specific costs on one or more of the AD DS site links. You need the site link total cost to be less than 150, which is the cost of the current lowest cost path. In this case, you can set the Exchange-specific cost of the site link between Site 3 and Site 1, named “Site3-Site1”, to 25 by running the following command:

[Click here to view code image](#)

```
Set-AdSiteLink -Identity Site3-Site1 -ExchangeCost 25
```

After you set the Exchange-specific cost, the lowest cost path is now Site 3 to Site 1 to Site 2 with a total cost of 125.

---



### Exam Tip

A hub site is only used if it is on the lowest cost path to the destination site.

Watch for scenarios on the exam that use a hub site that is not on the lowest cost path.

---

Now, you should understand how email flows internally, but that is just part of the email flow. Next, you look at planning for email flow between different organizations.

## Plan inter-org mail flow

Inter-org mail flow is email delivery between different organizations. For the exam, you need to be able to plan the email flow for external mail delivery to other organizations. You also need to be comfortable recommending designs and solutions based on a given scenario. To do that, you need to understand how inter-org email flows and which components are involved. In the diagram shown in [Figure 3-3](#), two organizations are represented. Each organization has a single Mailbox server and a single Edge Transport server. This configuration helps to simplify the diagram and provides an email flow overview. Fabrikam, Inc. is the sending organization and a user named Roman is the sender. Contoso, Ltd. is the receiving organization. Roman is sending an email to a Contoso, Ltd. user named Vivian.

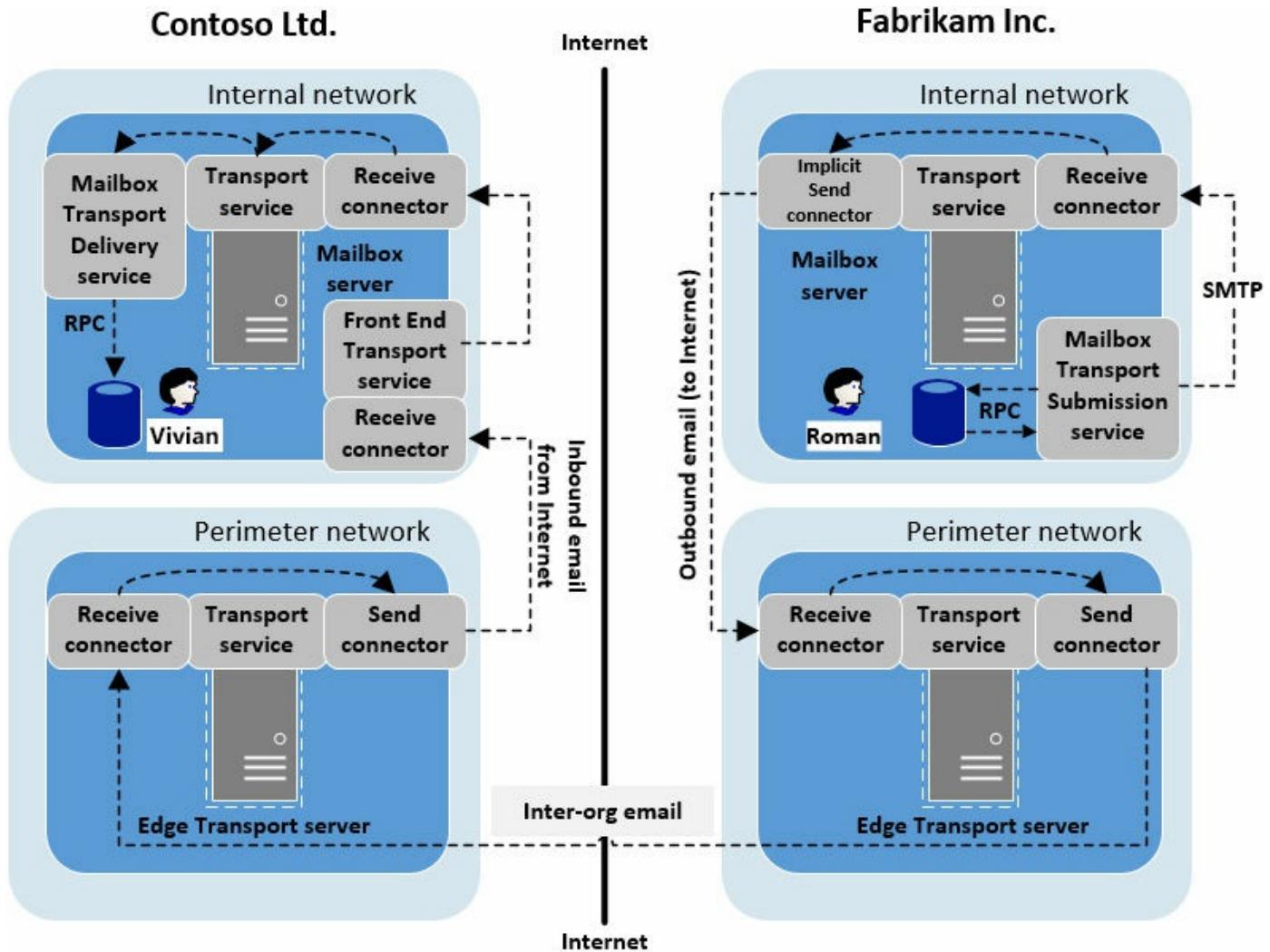


FIGURE 3-3 Email from Fabrikam, Inc. to Contoso, Ltd

Figure 3-3 shows two organizations, Contoso, Ltd. and Fabrikam, Inc. Let's walk through the email flow step-by-step.

1. Roman at Fabrikam, Inc. sends an email from Outlook 2016 to Vivian at Contoso, Ltd.
2. The Mailbox Transport Submission service on Fabrikam's mailbox server where Roman's mailbox is located, uses RPC to check for outbound messages in the mailbox database.
3. The Mailbox Transport Submission service uses SMTP to send the email message to the Receive connector on the local mailbox server.
4. The Transport service, which contains the Receive connector, uses the implicit Send connector, also part of the Transport service, on the local server to send the email message to Fabrikam's Edge Transport server's Receive connector. The Receive connector is part of the Transport service on the Edge Transport server. Note that you can't look at the implicit Send connector as it is not displayed in the Exchange Admin Center (EAC) but it is there to send email between Exchange

servers in the same Exchange organization.

5. The Transport service on the Edge Transport server sends the email message to the Receive connector on Contoso's Edge Transport server.
6. Contoso's Edge Transport server's Transport service sends the email message to the Send connector on the local Edge Transport server.
7. The Send connector sends the email message to the Mailbox server which is in the subscribed AD DS site. The Receive connector in the Front End Transport service receives the email messages.
8. The Front End Transport service sends the email message to the Receive connector in the Transport service on the local Mailbox server.
9. The Transport service sends the email message to the Mailbox Transport Delivery service.
10. The Mailbox Transport Delivery service uses RPC to put the email message in the local mailbox database for the recipient.

What happens if Contoso, Ltd. and Fabrikam, Inc. don't have Edge Transport servers? In such cases, email flows through the Mailbox servers. In the diagram shown in [Figure 3-4](#), Fabrikam, Inc. is the sending organization and Contoso, Ltd. is the receiving organization.

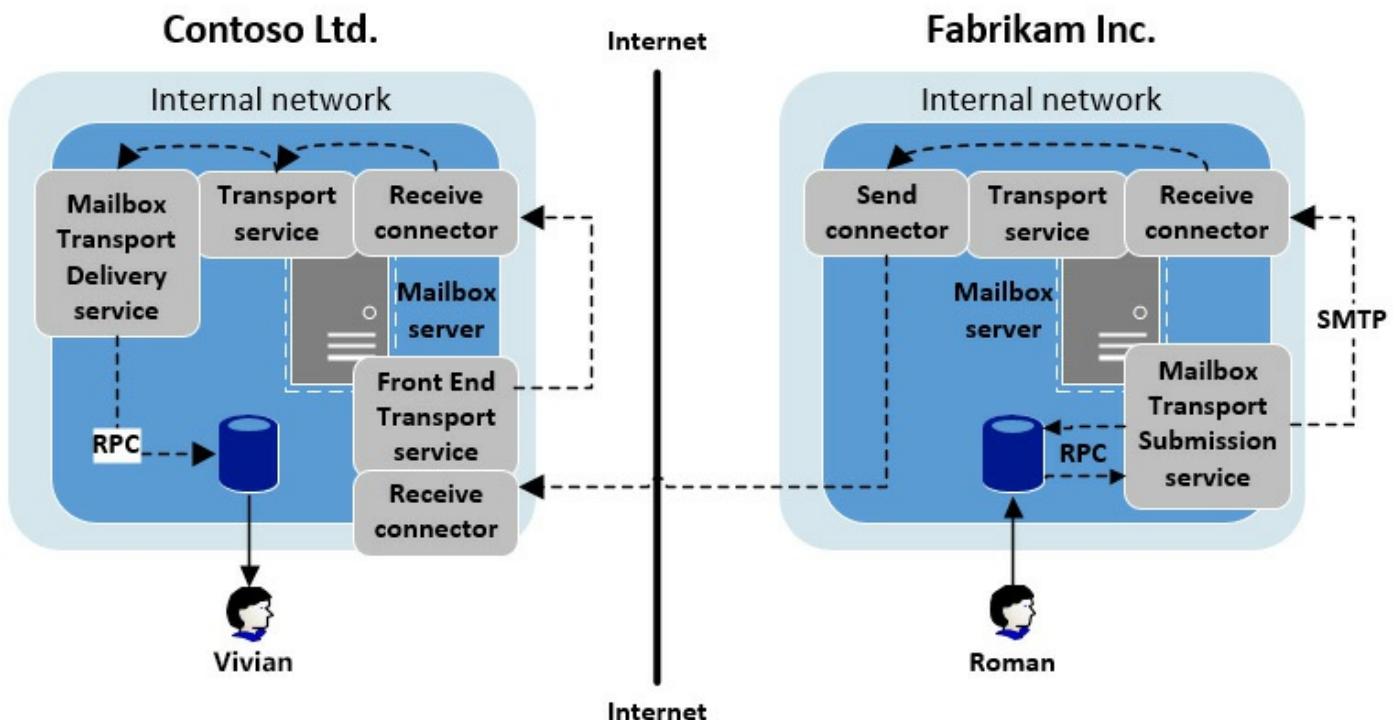


FIGURE 3-4 Email from Fabrikam, Inc. to Contoso, Ltd

[Figure 3-4](#) shows Fabrikam, Inc. sending email to Contoso, Ltd. all without the use of Edge Transport servers. The following steps describe the email flow.

1. Roman at Fabrikam, Inc. sends an email from Outlook 2016 to Vivian at Contoso, Ltd.
2. The Mailbox Transport Submission service, located on Fabrikam's mailbox server where Roman's mailbox is located, uses RPC to check for outbound messages in the mailbox database.
3. The Mailbox Transport Submission service uses SMTP to send the email message to the Receive connector on the local mailbox server.
4. The Transport service, which contains the Receive connector, sends the email message to the Send connector for delivery to Contoso, Ltd.
5. The Send connector sends the email message to the Receive connector, which is part of the Front End Transport service, on Contoso's Mailbox server.
6. The Front End Transport service sends the email message to the Receive connector, which is also part of the Transport service.
7. The Transport service sends the email message to the Mailbox Transport Delivery service.
8. The Mailbox Transport Delivery service uses RPC to put the email message into the mailbox database where Vivian's mailbox is stored.

The overall email flow is similar for organizations that are using Edge Transport servers and organizations that are not using Edge Transport servers. Understanding the differences in email flow are key to being prepared for the exam. You should be comfortable with the following key points:

- Edge Transport servers provide benefits to sending and receiving organizations:
  - Mailbox servers do not communicate directly with the Internet for sending and receiving email.
  - Edge Transport servers provide additional security compared to just using Mailbox servers. Email communication, until it passes through an Edge Transport server, is restricted to the perimeter network. Also, distributed denial of service attacks do not usually impact these Mailbox servers and you can perform additional message hygiene in the perimeter network.
- Edge Transport servers require additional administrative overhead, including initial setup and configuration and ongoing maintenance.
- Edge Transport servers are optional and are often considered when security is important and/or high performance is important.
- Beyond using Edge Transport servers, you can use third-party solutions in the perimeter network. It is a good practice to use something to ensure that Mailbox servers remain unavailable through the Internet.

- For outbound email, you can opt to use a standard Send connector in the Transport service, as shown in [Figures 3-3](#) and [3-4](#), or you can opt to proxy outbound email through the Front End Transport service instead. Proxying through the Front End Transport service enables all inbound and outbound email to go through the Front End Transport service.

## Plan, deploy, and configure redundancy for intra-site scenarios

Intra-site mail delivery is delivery in a single site. For this exam topic, you need to be familiar with redundancy options to provide highly available services. For a single site, redundancy is provided by using more than one Mailbox server because each server can provide transport services for inbound and outbound email. This exam topic does not focus on Database Availability Groups (DAGs) because those were covered in [Chapter 1](#).

For the exam, you should be familiar with how the various transport components function and how having more than one provides redundancy. [Figure 3-5](#) shows a single site with two mailbox servers in the site. The concepts in the diagram, which are described in detail following the diagram, are applicable for sites with a large number of Mailbox servers. For simplicity, however, the diagram only shows two servers.

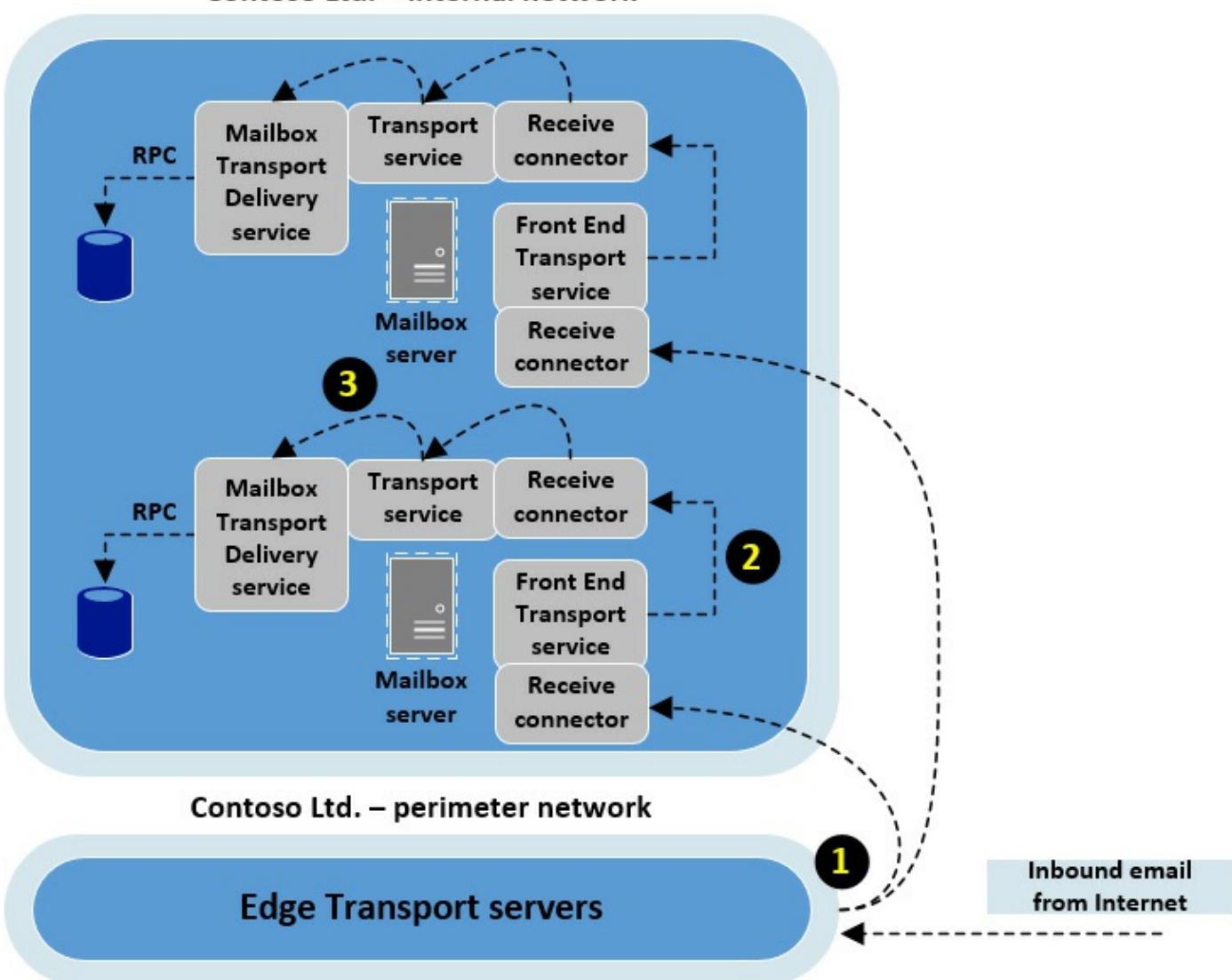


FIGURE 3-5 A single site with two Mailbox servers for redundancy

In [Figure 3-5](#), there are three specific areas that are redundant:

1. The communication from the Edge Transport servers, labeled as “1” in the diagram, can go to any Mailbox server in the subscribed AD DS site. In this case there are two available Mailbox servers. If one Mailbox server is down, the other server can accept all inbound email from the Edge Transport servers.
2. The communication from the Front End Transport service to a Receive connector in the Transport service, labeled as “2” in the diagram, has redundancy because the Front End Transport service can send email to the Receive connector on the local Mailbox server or on a remote Mailbox server.
3. The communication from the Transport service to the Mailbox Transport Delivery service, labeled as “3” in the diagram, has redundancy because the Transport service can send email messages to the Mailbox Transport Delivery service on the local Mailbox server or on a remote Mailbox server.



## Quick check

- How can you ensure that an Edge Transport server sends email to a specific internal site?

## Quick check answer

- You should subscribe the Edge Transport server to the site you want the server to send email to. Thereafter, the Edge Transport server can only use the subscribed AD DS site for sending email to the internal organization.

A key aspect of providing redundancy for an intra-site scenario is having multiple servers and enabling communication between all of the servers.

## Plan and configure for Safety Net

If you are an Exchange administrator without experience with Exchange Server 2013 or Exchange Server 2016, you might be wondering what “Safety Net” is. You might, however, remember the term “transport dumpster”. Transport dumpster was first introduced in Exchange 2007 and improved with Exchange 2010. As of Exchange 2013, Safety Net is the new name for the transport dumpster.

Safety Net, similar to the transport dumpster in Exchange 2010, maintains redundant copies of email messages that were successfully sent to the mailbox database. Safety Net was created to provide redundancy for recently delivered email messages. For example, imagine you have a Database Availability Group (DAG) with two servers and some new email messages haven’t replicated to the passive database copy yet when the active mailbox database server fails. If you activate the second server, those new email messages are lost, unless you use the Safety Net feature. With the Safety Net feature, the messages are resubmitted when the passive database is made active.

The following Safety Net characteristics are good to know for the exam:

- **You can customize how long Safety Net keeps copies of email messages** By default, Safety Net keeps message copies for two days. Note that you cannot control how much disk space Safety Net uses, except by adjusting the amount of time that email message copies are kept.
- **When you have a lagged copy of a mailbox database, you need to ensure that the amount of lag time for the database copy is equal to or less than the amount of time Safety Net keeps email copies** This ensures that you don’t lose email data.
- **You can make Safety Net redundant, which wasn’t possible with Exchange**

**2007 and Exchange 2010** To ensure Safety Net redundancy, you must have shadow redundancy enabled. Shadow redundancy is covered in the next topic. When you have redundancy with Safety Net, there is a primary Safety Net and a shadow Safety Net. The shadow Safety Net takes over if the primary Safety Net isn't available for 12 hours.

- You can use the Set-TransportConfig cmdlet with the SafetyNetHoldTime parameter to adjust the amount of time Safety Net keeps messages. The more messages you keep, the more disk space that you use.
- 



### Exam Tip

Watch for troubleshooting situations where email data is being lost. It might not be obvious at first, but Safety Net might be a potential fix. An item writer for this exam might explore such a situation involving a DAG. This is because Safety Net takes over some functionality from shadow redundancy for DAGs.

---

## Plan and configure for shadow redundancy

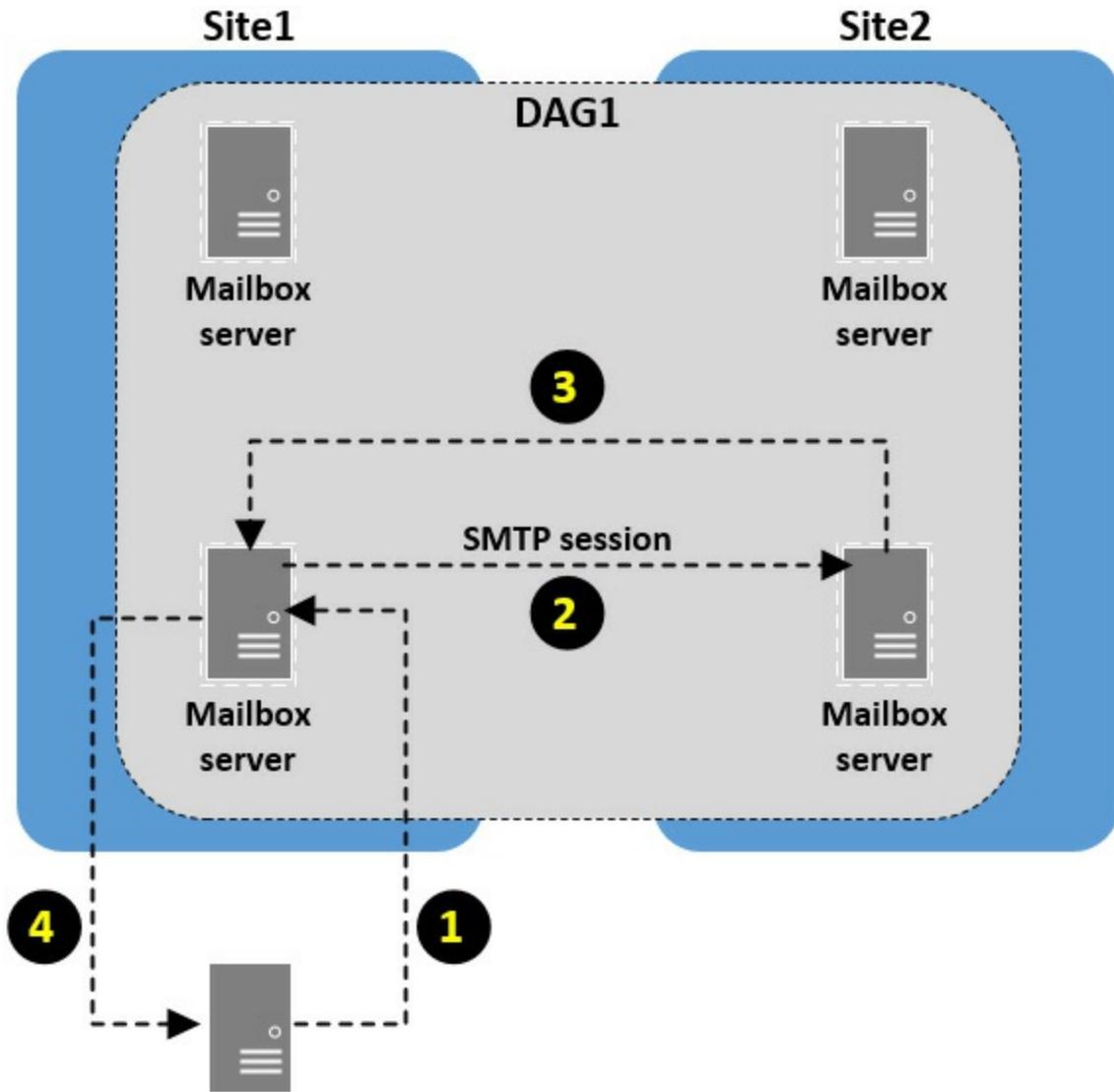
Shadow redundancy, an optional feature of Exchange Server, offers similar functionality as Safety Net. Shadow redundancy however, maintains copies of email messages before they are sent to mailbox databases. Enabled in Exchange Server 2013, shadow redundancy makes a copy of an incoming email message before it even acknowledges it received the message from the sending server. Shadow redundancy is enabled by default.

The following characteristics of shadow redundancy are helpful for planning for it:

- Shadow redundancy can't protect messages in transit when there is only a single server in the environment.
- Shadow redundancy works in conjunction with Safety Net to protect email messages in the transport pipeline.
- In environments where all messages must be placed in the shadow copy at all costs, you can configure Exchange Server to reject an incoming email message if it fails to be placed in the shadow copy.
- Shadow redundancy works within a DAG or within an AD DS site when servers are not part of a DAG. In such situations, the DAG is considered a transport boundary and an AD DS site is also considered a transport boundary.
- You can use the Set-TransportConfig cmdlet with the ShadowRedundancyEnabled parameter to enable or disable shadow redundancy by using a value of \$true or

\$false. To reject messages if shadow redundancy fails, you can use the Set-TransportConfig cmdlet with the RejectMessageOnShadowFailure parameter by using a value of \$true or \$false.

[Figure 3-6](#) shows the process for how shadow redundancy works.



### SMTP server on Internet

FIGURE 3-6 The process of how shadow redundancy works

The following steps describe the corresponding numbered steps in [Figure 3-6](#).

1. An SMTP server on the Internet on behalf of one organization, sends an email message to another organization. A Mailbox server in Site 1 receives the message. The Mailbox server in Site 1 is known as the primary server in shadow redundancy terms. The email message received is known as the primary email message.
2. The primary server, before acknowledging receipt of the email message to the SMTP server on the Internet, uses SMTP to send a copy of the message to the

Transport service on the Mailbox server in Site 2. The Mailbox server, by default, sends a copy of the message to a Mailbox server in a different site. While you can configure it to choose the local site instead, the remote site is better because it provides site resiliency to the email message. If there is not a DAG in place, the primary server sends a copy of the email message to another Mailbox server in its AD DS site.

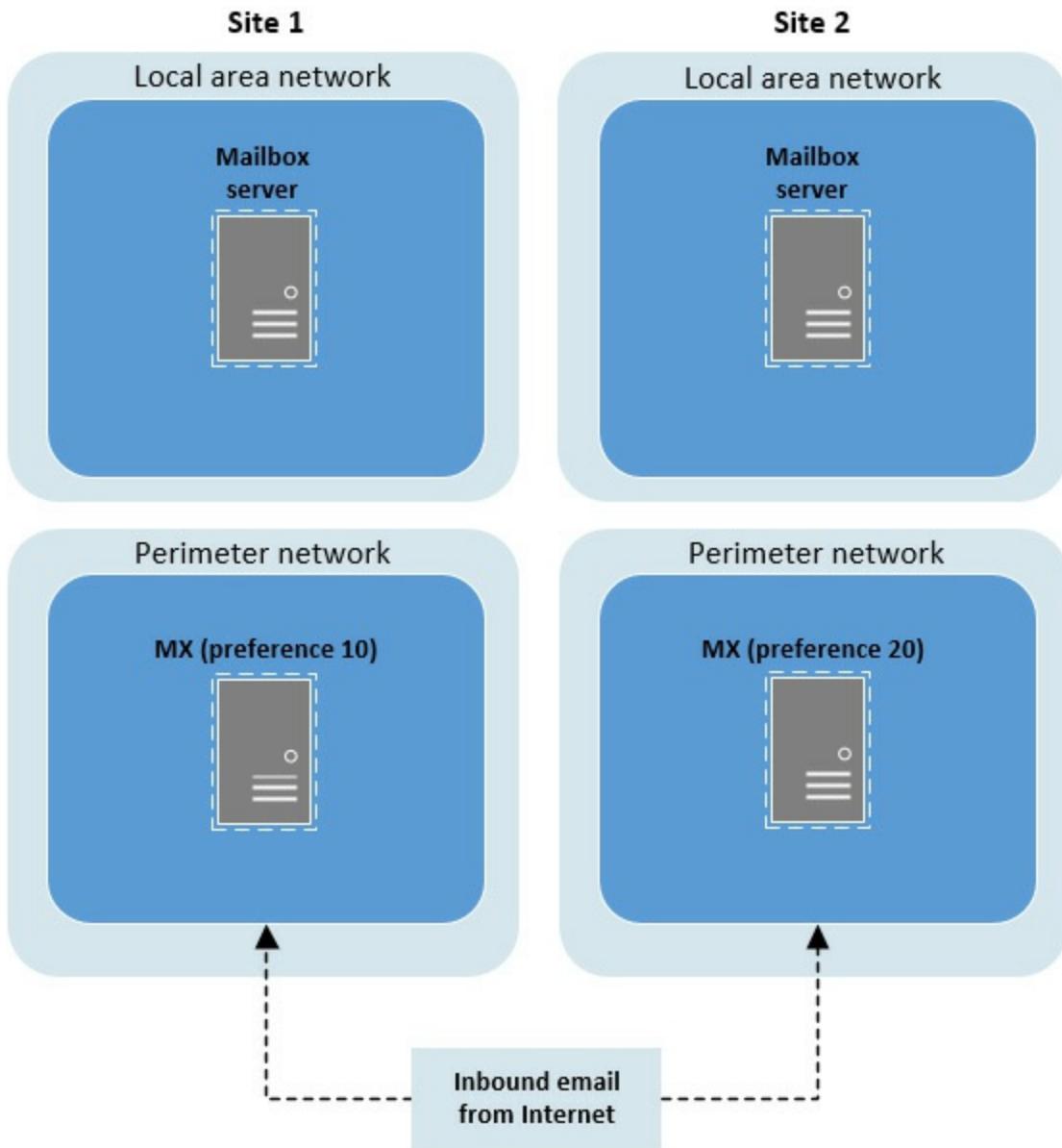
3. The server receiving the copy of the email message is known as the shadow server in shadow redundancy terms, and the email message that it holds a copy of is known as the shadow message. Upon successfully receiving the shadow message, the shadow server notifies the primary server that it got the message copy.
4. The primary server, after getting confirmation from the shadow server, notifies the SMTP server on the Internet that it received the email message. The SMTP server on the Internet is unaware of the shadow redundancy. This is important because it means other servers sending email to your organization do not need to support shadow redundancy or perform any steps to facilitate it.

For the exam, ensure that you understand how shadow redundancy works and how it differs from Safety Net.

## Plan and configure for redundant MX records

Mail exchange (MX) records are DNS records used by email servers to find other email servers for destination domains. For example, if a person at contoso.com wants to send email to a person at fabrikam.com, the contoso.com DNS servers look for the MX records for the fabrikam.com domain. Based on those records, the contoso.com email server connects to the fabrikam.com email server. These connections, however, can get a bit more complicated when an organization wants to have redundancy for the MX records.

[Figure 3-7](#) shows an organizational structure that has two MX records.



**FIGURE 3-7** The layout of the Exchange environment with redundant MX records

The organization shown in [Figure 3-7](#) has two MX records. One MX record has a preference of 10 and the other has a preference of 20. A preference is sometimes known as a mail server priority, or just priority. The lower the preference, the more preferred it is. Based on the RFC standard for SMTP, an email server must try to delivery email to the lowest preference MX record for a domain. If the lowest preference MX record points to a server that is down or unreachable, the next lowest preference MX record is used to attempt email delivery. The lowest preference you can use has a value of 0.

In a configuration where one MX record has a preference of 10 and one MX record has a preference of 20, the MX record with a preference of 20 is known as a backup server. This is because it never participates in inbound email unless the server for the MX record with a preference of 10 is down or unreachable. There is another option however. You can set both servers to have an MX preference of 10. In that case, it

works like DNS round-robin, or DNS load balancing, with both email servers handling inbound email.

---



### Exam Tip

If a domain does not have any MX records, an implicit MX record is presumed, with a preference of 0, pointing to the destination domain. For example, if the domain contoso.com does not have any MX records, email servers sending email to contoso.com attempt to send the email to the host “contoso.com.” If contoso.com resolves to an email server, the email goes through. For most organizations, however, the domain name resolves to the organization’s website. This implicit MX record is by design as documented in RFC 5321.

---

## Plan, create, and configure transport-related tasks

This skill covers a few administration tasks related to transport, such as TLS transport, Edge transport, Send/Receive connectors, transport rules, accepted domains, email address policies and Address Rewriting. Each of these topics are broken down into small sub-sections to make them easier to consume.

### Plan, create, and configure TLS transport

TLS transport is email transport over transport layer security (TLS). TLS replaces Secure Sockets Layer (SSL) for secure communications. TLS is enabled by default with Exchange Server 2013 and Exchange Server 2016. This means that any server that sends to Exchange Server can encrypt the SMTP session, and outbound communication from Exchange Server to other email servers on the Internet use TLS, when available.

While TLS is enabled by default, you might need to disable TLS in some scenarios. For example, if you have three sites and you use wide-area network (WAN) optimization controllers (WOCs), SMTP traffic is compressed. SMTP traffic cannot be compressed when it is encrypted. By disabling TLS, you can compress the SMTP traffic with WOCs and improve overall performance. You can disable TLS between sites by configuring the Receive connectors. For example, to disable TLS on a Receive connector named WAN1 on a server named SERVER1, run the following command:

[Click here to view code image](#)

```
Set-ReceiveConnector SERVER1\WAN1 -SuppressXAnonymousTLS $true
```

You can also use TLS for mutual authentication. In such a scenario, all email sent between organizations uses TLS. If TLS can't be used at any time, email is rejected.

Mutual authentication is mostly used between partner organizations, or sometimes between organizations belonging to the same parent company. You should be aware of the following requirements for mutual TLS:

- **Mutual TLS requires certificates** Most often, each organization uses an internal PKI.
- **Mutual TLS requires that each organization trust the other organization's root certification authority (CA)** Because of this, you should limit mutual TLS to closely trusted organizations, such as partners. Optionally, each side can use third-party certificate providers that are already trusted instead.
- **Mutual TLS provides an alternative to S/MIME or similar email security solutions** Mutual TLS and S/MIME are not mutually exclusive however. Organizations can use both.

## Plan, create, and configure Edge transport

In an Exchange organization, transport occurs across the entire environment. For the exam, you need to know how to work with transport at the edge, specifically with Edge Transport servers.

From a planning perspective, there are important considerations for Edge Transport servers:

- You should deploy Edge Transport servers in the perimeter network to maximize security and performance. This enables all message hygiene to occur outside of the local area network and outside of your AD DS domain.
- You should use servers that are not joined to your AD DS domain for your Edge Transport servers. This is because Edge Transport servers do not use AD DS for functionality and because you do not want to open up firewall ports, enabling servers in the perimeter network to join the AD DS domain on the local area network.
- You must have at least one Mailbox server in your Exchange organization before you can deploy an Edge Transport server.
- You cannot install an Edge Transport server on a Mailbox server.
- Edge Transport servers use Active Directory Lightweight Directory Services (AD LDS) to store Exchange configuration and recipient information.
- Edge Transport servers must be able to resolve the names of the Mailbox servers and the Mailbox servers must be able to resolve the names of the Edge Transport servers. You might have to open firewall ports, such as TCP/UDP port 53, if you are using different DNS servers for the perimeter network and the local area network.

Installing an Edge Transport is a fairly basic task: go through the installation wizard, select the Edge Transport role, and wait for it to complete. After the installation, you need to perform some post-installation tasks to enable the server to function. The following steps describe the prerequisite steps:

1. Ensure that you have configured authoritative domains and email address policies prior to starting the post-installation tasks for your Edge Transport server.
2. Ensure that TCP port 50636 is open on the firewall separating the perimeter network and the local area network. This enables secure LDAP communication. This communication is needed for EdgeSync.

The following steps describe the process of the post-installation tasks:

1. On the Edge Transport server, run the following command to create the edge subscription file. You can use any path and file name.

[Click here to view code image](#)

```
New-EdgeSubscription -FileName e:\temp\subscription.xml
```

2. Copy the .xml file to the Mailbox servers in the AD DS site that you plan on subscribing the Edge Transport server to.
3. Import the edge subscription file on the Mailbox servers. For example, to import a file named subscription.xml in the d:\temp directory and subscribe the Edge Transport server to an AD DS site named “HQ”, run the following command:

[Click here to view code image](#)

```
New-EdgeSubscription -FileData ([byte[]]$ (Get-Content -Path "d:\temp\subscription.xml" -Encoding Byte -ReadCount 0)) -Site "HQ".
```

4. Start the edge synchronization by running the Start-EdgeSynchronization command on a Mailbox server.



### Exam Tip

The edge subscription file contains sensitive information related to the credentials used during LDAP communication. To maximize security, you should securely delete the file from the Edge Transport server and the Mailbox server once edge synchronization is functional.

---

As part of preparing for the exam, you should add an Edge Transport server to your test environment so that you can gain some hands on experience, especially if you haven't worked with the Edge Transport role in the past.

## Plan, create, and configure Send/Receive connectors

Exchange Server 2016 creates some receive connectors by default during installation. For small organizations with minimal requirements, the default receive connectors are probably all that they need, even if they need to configure and maintain them. By default, there aren't any send connectors. You must have a send connector to send email to the Internet. This section looks at receive and send connectors, but first, you look at receive connectors.

### Receive connectors

A receive connector enables an Exchange server to receive email. Receive connectors can be created for one of two roles, the Hub Transport role and the Frontend Transport role. You can choose from five types of receive connectors:

- **Custom** Custom receive connectors are typically used in complex, cross-forest environments, or when you want to enable applications to send email through Exchange.
- **Internal** An Internal connector is used for email routing between Exchange servers in your organization.
- **Internet** The Internet connector is used to receive SMTP connections from the Internet.
- **Partner** The Partner connector is used when you want to establish email communication between your organization and a partner organization.
- **Client** The Client connector is used for email clients other than Outlook.

You can create new receive connectors in the EAC or by using EMS). The following high-level steps outline the EAC process for creating a new receive connector to receive email from the Internet.

1. Add a new receive connector in the EAC.
2. Type a name for the connector, choose the role, either Hub Transport or Frontend Transport, and choose the type.
3. Specify the IP addresses that the connector listens on. Also specify the port. For Internet email use port 25, which is the default.
4. Specify the IP address range(s) the receive connector accepts connections from. By default, it accepts email from 0.0.0.0 to 255.255.255.255, which covers any IPv4 address on the Internet.

In addition to using the EAC, you should be familiar with creating and managing receive connectors by using Windows PowerShell. You can use the New-ReceiveConnector cmdlet to create a new receive connector. You can use the Get-ReceiveConnector cmdlet to view existing receive connectors. You can use the Set-

ReceiveConnector cmdlet to configure an existing receive connector.

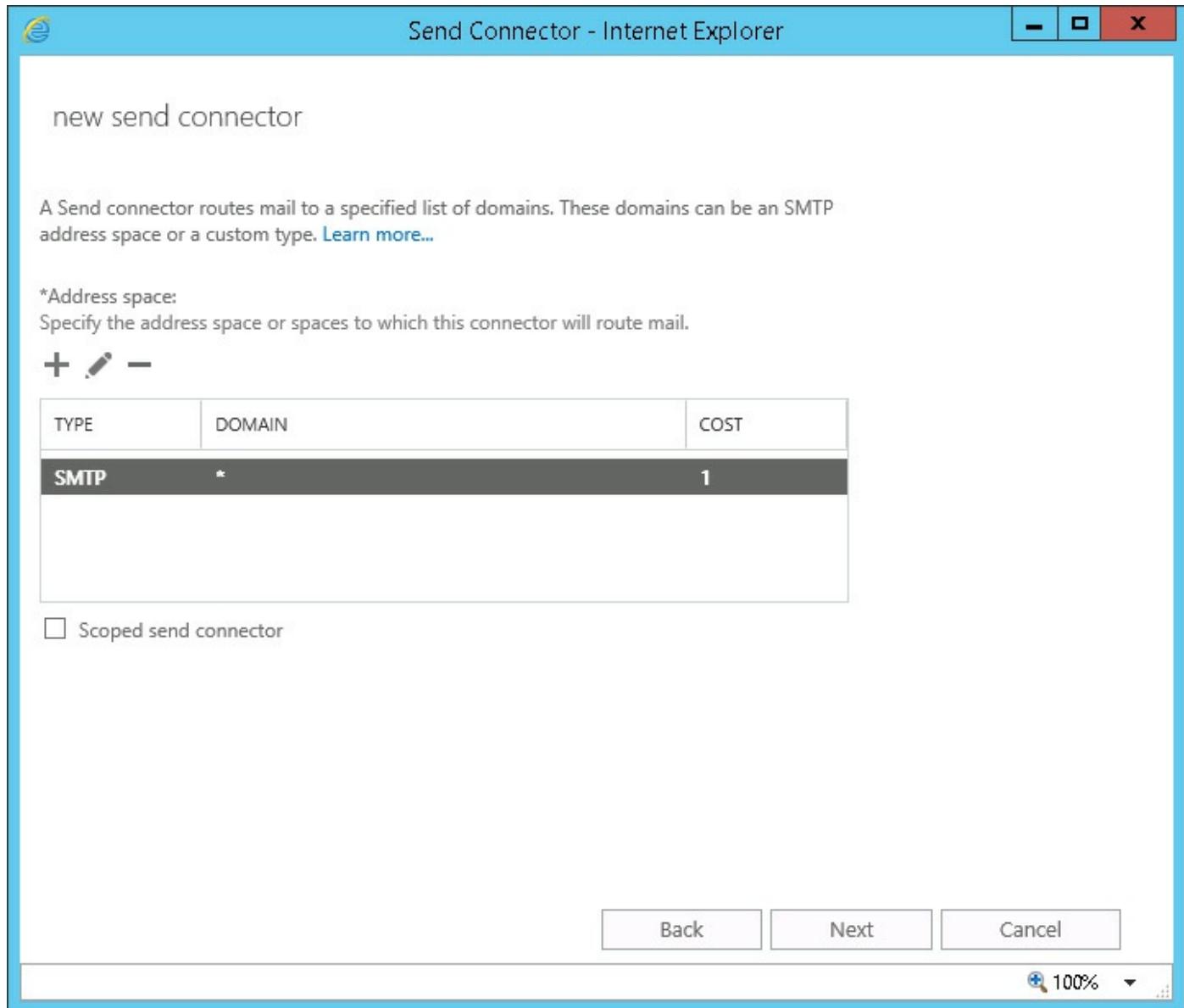
## Send connectors

A send connector enables an Exchange server to send email. Send connectors do not have any associated roles, but there are various types of send connectors:

- **Custom** A Custom connector is mostly used to send email to other email servers.
- **Internal** An Internal send connector enables email relay within your organization.
- **Internet** The Internet send connector enables you to send email to the Internet.  
Remember that by default, a newly deployed Exchange server cannot send email to the Internet, and that problem is fixed by creating a new Internet send connector.
- **Partner** A Partner connector is used to enable email communication between two partner organizations.

You can create new send connectors in the EAC or by using EMS. The following high-level steps outline the EAC process for creating a new send connector to send email to the Internet.

1. Add a new send connector in the EAC.
2. Type a name for the connector and choose the connector type. For this example, use the Internet type because the goal is to send email to the Internet.
3. Choose how the send connector routes email. You can use MX records, where the sending server looks up DNS MX records to ascertain where to send email. Or you can use a smart host, which is another email server that performs delivery on behalf of other email servers. Some organizations prefer to have their Mailbox servers use a smart host that resides in the perimeter network to prevent their Mailbox servers from directly going to the Internet.
4. Specify the domain you want the send connector to send email to. For a send connector used for the Internet, use an asterisk (\*) to represent all domains. [Figure 3-8](#) shows a send connector configured to send to all domains.



**FIGURE 3-8** The New Send Connector page

**5. Specify the servers that use the send connector. Often, the servers are Edge Transport servers or servers that send email to the Internet.**

You can also use Windows PowerShell to create and manage send connectors. You can use the `New-SendConnector` cmdlet to create a new send connector. You can use the `Get-SendConnector` cmdlet to view the existing send connectors. You can use the `Set-SendConnector` cmdlet to configure existing send connectors.

## Summary

- A service level agreement (SLA) is an agreement between a service provider, you and/or your IT department, and a customer, your company or your customers. This agreement documents the expectations of a service, such as email, from an availability and performance aspect.

- Inter-site email flow relies on AD DS site links, and optionally Exchange costs on AD DS site links, to efficiently route email between sites.
- Inter-org email, in a typical large enterprise environment, uses Edge Transport servers in a perimeter network to send and receive email from the Internet. Edge Transport servers are subscribed to an AD DS site as part of their configurations.
- Safety Net, similar to the transport dumpster in Exchange 2010, maintains a redundant copy of an email message that was successfully sent to the mailbox database. It was created to provide redundancy for recently delivered email messages. For example, imagine you have a DAG with two servers. Some new email messages haven't replicated to the passive database copy yet and then the active mailbox database server fails. If you activate the second server, those new email messages are lost, unless you use the Safety Net feature.
- Shadow redundancy, an optional feature of Exchange Server, offers similar functionality as Safety Net. Shadow redundancy maintains copies of email messages before they are sent to mailbox databases.
- You can use multiple MX records to provide redundancy for incoming email. The MX record with the lowest preference number is the server that receives incoming email. If it has a failure and becomes unavailable, the server with the next lowest MX preference number receives incoming email.

## Skill 3.2: Troubleshoot and monitor transport services

In the previous section, you looked at transport services and transport components. In this section, you build on that by looking at troubleshooting and monitoring those services and components. For the exam, you are expected to know how to plan, install, configure, monitor, and troubleshoot transport-related technologies.

---

### This section covers how to:

- [Interpret message tracking logs and protocol logs](#)
  - [Troubleshoot a shared namespace environment](#)
  - [Troubleshoot SMTP mail flow](#)
  - [Given a failure scenario, predict mail flow and identify how to recover](#)
  - [Troubleshoot TLS](#)
  - [Troubleshoot the new transport architecture](#)
-

## Interpret message tracking logs and protocol logs

When your environment has email flow issues or transport issues, you need to be able to use the tracking logs and protocol logs to troubleshoot and find the root cause. For the exam, you need to know how to work with the message tracking logs and protocol logs for a given troubleshooting scenario. Remember, the term “protocol logs,” like any other skill on the exam, is open to interpretation. Some might think that protocol logs are SMTP logs, while others might think of POP3 or IMAP4. For your exam preparation, think of any logs that handle any protocol. Many of the techniques you can use to review logs are the same, including knowing where the logs are, how to turn them on, and how to efficiently search them for problems.

### POP3 and IMAP4 protocol logs

By default, POP3 and IMAP4 services are not enabled. After being enabled, protocol logging is not turned on by default. When a problem arises, you should enable logging. You can turn on POP3 logging for a server named EX-03 by running the following command:

[Click here to view code image](#)

```
Set-PopSettings -Server EX-03 -ProtocolLogEnabled $True
```

You can turn on IMAP4 logging for a server named EX-03 by running the following command:

[Click here to view code image](#)

```
Set-ImapSettings -Server EX-03 -ProtocolLogEnabled $True
```



#### Exam Tip

After you enable POP3 or IMAP logging, logging does not start until the POP3 and IMAP4 services have been restarted.

In addition to turning on the logging, you can also configure some log file settings such as log file location, log file sizes, and log file rotation, which determines how often files are created. For example, files can be created at a rate of one file a day or one file an hour. By default, logs are stored at %SYSTEMDRIVE%\Program Files\Microsoft\Exchange Server\V15\Logging\Pop3 and %SYSTEMDRIVE%\Program Files\Microsoft\Exchange Server\V15\Logging\Imap. If you don't configure the log file location to a non-system volume, you run the risk of running out of disk space. It is a good practice to store the logs on a non-system volume to avoid disk spaces issues on the system volume.

When working with raw protocol logs, you are often looking at them because of a problem that occurred. Logs are not easy to look at, however, especially if you use Notepad or another pure text viewer. There are certain keywords you can search for that can be helpful for locating issues, such as:

- Fail
- Unknown
- Bad
- Denied

Let's take a look at a log to understand the general logic. The following example contains five entries from the POP3 protocol log and illustrates the logging messages written when a user connects to the server using POP3 and then tries a bad password:

[Click here to view code image](#)

```
2016-06-14T04:11:07.250Z,0000000000000009,0,  
[2601:101:c000:1503:998:4be:fa4c:371c]:995,[  
2601:101:c000:1503:458b:9fa2:446f:b825]:57837,,1,0,51,OpenSession,,,  
  
2016-06-14T04:11:07.265Z,0000000000000009,1,  
[2601:101:c000:1503:998:4be:fa4c:371c]:995,[  
2601:101:c000:1503:458b:9fa2:446f:b825]:57837,,1,4,37,capa,,R=ok,  
  
2016-06-14T04:11:07.265Z,0000000000000009,2,  
[2601:101:c000:1503:998:4be:fa4c:371c]:995,[  
2601:101:c000:1503:458b:9fa2:446f:b825]:57837,user2,1,10,5,user,user2,R=ok,  
  
2016-06-14T04:11:07.265Z,0000000000000009,3,[2601:101:c000:1503:998:4b  
e:fa4c:371c]:995,[2601:101:c000:1503:458b:9fa2:446f:b825]:57837,user2  
,2,10,56,pass,*****, "R=""-ERR Logon failure: unknown user name or bad  
password."";Msg=LogonFailed:LogonDenied;ErrMsg=LogonFailed:LogonDenied",  
  
2016-06-14T04:11:07.265Z,0000000000000009,4,  
[2601:101:c000:1503:998:4be:fa4c:371c]:995,[  
2601:101:c000:1503:458b:9fa2:446f:b825]:57837,user2,0,0,0,CloseSession,,,
```

In the POP3 log file listing, there are the following five entries:

1. In the first line, a connection to port 995, a secure POP3 port, is opened. Note that the initial connection writes “OpenSession” to indicate a new connection.
2. In the second line, there isn’t much to go on. The CAPA command is used to list the capabilities of the POP3 server.
3. In the third line, the user attempts to sign in as “user2.”
4. In the fourth line, the password, obfuscated because of the use of secure POP3, is sent but a failed logon message is generated.
- In the fifth line, a “CloseSession” message indicates that the session has been

closed.

As part of your exam preparation, you should enable all of the logs and review the log files.

## Message tracking logs

Message tracking logs are logs that capture information related to email flow. These logs are routinely used to diagnose mail flow issues. They are often your first stop, besides looking at queues. Message tracking logs are enabled by default and they are stored at %ExchangeInstallPath%\TransportRoles\Logs\MessageTracking. If your Exchange installation path is on the system volume, you should move the message tracking logs to a non-system volume to ease concerns with disk space and performance. You can use the Set-TransportService cmdlet to configure all aspects of message tracking. The two most important configurations are the log locations (use the MessageTrackingLogPath parameter) and the maximum amount of space that the logs can use (specified in days by using the MessageTrackingLogMaxAge parameter). You should set a maximum size to avoid having message tracking logs run a volume out of space.

The Get-MessageTrackingLog cmdlet can be used to track email in your Exchange environment which can help identify where a problem might have occurred. For example, when researching your issue, you might find that a sender used the wrong email address or had a typo in the address. Or if you don't find any records, it might lead you to look at the user's outbox and computer. The following example uses a command to search for email sent by [user1@contoso.com](mailto:user1@contoso.com). In this case, only a small amount of information is returned. This is because you are looking for a specific subject line.

[Click here to view code image](#)

```
Get-MessageTrackingLog -Server NYC-EX1 -Sender "user1@contoso.com" | FL
  Sender,Recipient
  s,MessageSubject,MessageId

  Sender      : User1@contoso.com
  Recipients   : {managers@adatum.com}
  MessageSubject : Tomorrow's meeting
  MessageId    : 2a48b06dce944de793134062ce912cd7@contoso.com
```

After finding the email message that you are looking for, you can return more information from the message tracking logs. The following example shows all of the information available for the specific email message with a message ID of [2a48b06dce944de793134062ce912cd7@contoso.com](mailto:2a48b06dce944de793134062ce912cd7@contoso.com).

[Click here to view code image](#)

```

Get-MessageTrackingLog -MessageID
"2a48b06dce944de793134062ce912cd7@contoso.com"
| FL

RunspaceId          : 06d04667-4a4d-4d07-b193-88f961f140cd
Timestamp           : 6/13/2016 8:39:08 PM
ClientIp            : 2601:101:c000:1503:998:4be:fa4c:371c
ClientHostname      : NYC-EX1.contoso.com
ServerIp            : 2601:101:c000:1503:998:4be:fa4c:371c
ServerHostname      : NYC-EX1
SourceContext        : 08D393FF7B4C6721;2016-06-14T03:39:07.959Z;0
ConnectorId         : NYC-EX1\Default NYC-EX1
Source              : SMTP
EventId             : RECEIVE
InternalMessageId   : 2847563317266
MessageId           : 2a48b06dce944de793134062ce912cd7@contoso.com
NetworkMessageId    : 0172c47b-949b-4388-76b2-08d3940570eb
Recipients          : {managers@adatum.com}
RecipientStatus     : {}
TotalBytes          : 7805
RecipientCount      : 1
RelatedRecipientAddress :
Reference           :
MessageSubject      : Tomorrow's meeting
Sender              : User1@contoso.com
ReturnPath          : User1@contoso.com
Directionality      : Originating
TenantId            :
OriginalClientIp    : 2601:101:c000:1503:458b:9fa2:446f:b825
MessageInfo          : 0cI:
MessageLatency      :
MessageLatencyType  : None
EventData           : {[FirstForestHop, NYC-EX1.contoso.com],,
[FromEntity,
[AccountForest,
contoso.com] }

```

Message tracking logs are helpful when troubleshooting. They often lead you to the place of trouble, which could be a specific Exchange server, a client computer, or similar. Next, look at using the EAC to track messages. You can use the delivery reports to view message tracking. [Figure 3-9](#) shows a delivery report. All messages sent by [Administrator@Adatum.com](mailto:Administrator@Adatum.com) are displayed.

rules **delivery reports** accepted domains email address policies receive connectors  
send connectors

specific person. You can narrow the search to messages with certain keywords in the subject.

\*Mailbox to search:

Administrator

Search for messages sent to:

Search for messages received from:

Search for these words in the subject line:

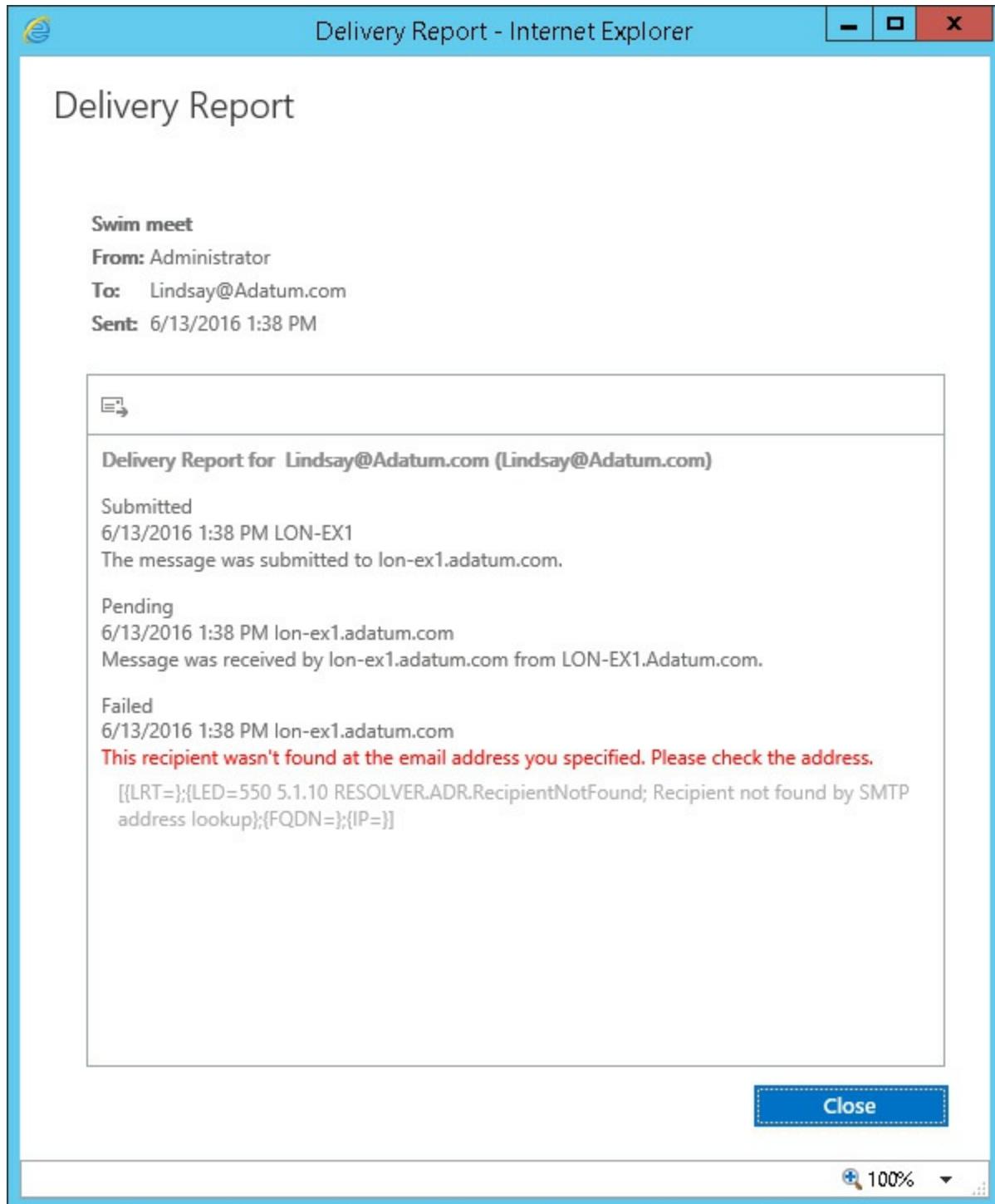
Search results

FROM	TO	SUBJECT	SENT TIME
Administrator	Lindsay@Adatum.com	Swim meet	6/13/2016 1:38 PM
Administrator	Jay Hamlin	Hiking trip	6/13/2016 12:49 PM
Administrator	brian@svideraol.com	Summer pool party	6/13/2016 12:40 PM

**FIGURE 3-9** A delivery report shows all sent messages from [Administrator@Adatum.com](mailto:Administrator@Adatum.com)

While administrators routinely use delivery reports in the EAC, users are also able to track their own messages by using Outlook on the web. In all cases, the information comes from the same place, message tracking log files.

When you have a list of search results, you can double-click a single email to show the delivery report which includes details about the email message. [Figure 3-10](#) shows a delivery report clearly stating that the email wasn't delivered because the email recipient wasn't found, meaning the recipient's email address is bad or no longer valid.



**FIGURE 3-10** An email delivery report

There are also other protocol logs that sometimes have helpful information in troubleshooting situations. You look at those next.

## Other protocol logs

As an Exchange administrator, one of the first things you discover is that Exchange Server, especially Exchange Server 2016, provides a great deal of logging. Some of it is enabled by default. Much of it isn't enabled by default but you can enable it to troubleshoot an issue. Every component that plays a part in message transport has associated log files. The following logs exist:

- SMTP send/receive for the Transport service
- SMTP send/receive for the Front End Transport service
- SMTP send/receive for the Mailbox Transport service (logs for submission and delivery components)

By default, all of these logs are disabled. You can enable logging for any of them, by configuring the associated connector. You can use the Set-ReceiveConnector cmdlet to enable logging. To enable SMTP logging for the Default Frontend receive connector for a server named EX-01, run the following command:

[Click here to view code image](#)

```
Set-ReceiveConnector -Identity 'EX-01\Default Frontend EX-01' -  
ProtocolLoggingLevel  
Verbose
```

In some cases, you might not know where the problem is. In such a case, you can enable logging on all of the receive connectors on a server. For example, to set all of the receive connectors on EX-01 to use verbose logging, run the following command:

[Click here to view code image](#)

```
Get-ReceiveConnector -Server EX-01 | Set-ReceiveConnector -  
ProtocolLoggingLevel Verbose
```

You can also enable verbose logging on send connectors. Instead of using the Set-ReceiveConnector cmdlet, you use the Set-SendConnector cmdlet.

## Troubleshoot a shared namespace environment

In [Chapter 2](#), you walked through namespaces, including the use of a single FQDN. Using a single FQDN is often referred to as a single namespace. A single namespace is similar to a shared namespace. Each can be used for client connectivity, across multiple organizations, or in a hybrid environment where some services are on-premises and some are in the public cloud. The primary difference between a shared namespace and a single namespace is a shared namespace is used across multiple organizations or environments, whereas a single namespace might or might not be.

Troubleshooting a shared namespace environment takes more time because there are more servers involved and more log files to look through. Otherwise, it is very similar

to troubleshooting standard email transport issues.

In many cases, a shared namespace is used for all external communication, but internally, more than one namespace is in use. For example, imagine that a toy company named Tailspin Toys buys another toy company named Wingtip Toys. Each company has their own domain names and Exchange organizations, but the company wants to present a unified company to the public. They decide to use the tailspintoys.com domain name for all email that goes to the Internet or that is received from the Internet. To accomplish this, you can use address rewriting. Address rewriting converts all inbound messages sent to [wingtiptoys.com](#) to [tailspintoys.com](#). It also converts all outbound messages to the Internet so that the sender uses [tailspintoys.com](#). Most often, you use Edge Transport servers to do the address rewriting. There is an Address Rewriting Inbound Agent and an Address Rewriting Outbound Agent that handle address rewriting. In a shared namespace environment, you might have to troubleshoot address rewriting. The following characteristics of address rewriting are important to know for troubleshooting:

- The domain you use as part of address rewriting must be configured as an authoritative accepted domain in Exchange Server.
- Email aliases must be unique across the domains. For example, if there is a [marc@tailspintoys.com](#) and a [marc@wingtiptoys.com](#), address rewriting would rewrite [marc@wingtiptoys.com](#) as [marc@tailspintoys.com](#), which already exists.
- You must add proxy addresses for all senders that have their email addresses rewritten.
- Address rewriting is compatible with signed, encrypted, and rights-protected, AD RMS or Azure RMS, messages.

## Troubleshoot SMTP mail flow

Earlier in this section, you looked at message tracking and protocol logs, both of which are helpful when troubleshooting SMTP mail flow issues. Before you get there, however, you often work with the queues. Queues hold email during and before transport. Sometimes, messages get stuck in queues for various reasons, such as a bad email address.

You can view queues through the Queue Viewer or through the EMS. [Figure 3-11](#) shows the output of the Get-Queue | Select Identity,Status,MessageCount command.

Identity	Status	MessageCount
LON-EX1\4	Retry	1
LON-EX1\Submission	Ready	1
LON-EX1\Unreachable	Ready	2

FIGURE 3-11 Command output in the Queue Viewer

In addition to looking at queues on individual servers with the Get-Queue cmdlet, you can use the Get-QueueDigest cmdlet to look across all servers in a DAG, in a specific AD DS site, or in the entire AD DS forest. This enables you to quickly find out the status of email deliveries in your organization. The following commands show the usage of Get-QueueDigest:

- **Get-QueueDigest –Dag DAG1** This command shows you the queues for all servers in the DAG named DAG1.
- **Get-QueueDigest –Forest** This command shows you all of the queues for servers in the forest.

Instead of looking at the queues from EMS, you can also use a GUI-based tool to view the queues. The Queue Viewer has been part of Exchange Server for a long time, but for Exchange administrators that haven't worked on a recent version of Exchange Server, the Queue Viewer might appear to have been removed from Exchange Server. It is still there however. It has been moved to a dedicated Microsoft Management Console (MMC) snap-in named "Exchange Toolbox." You can open a new MMC and add the snap-in. When the snap-in is added, you can find three tools, including the Details Template Editor, the Remote Connectivity Analyzer, and the Queue Viewer. This topic covers the Queue Viewer. [Figure 3-12](#) shows the Queue Viewer.

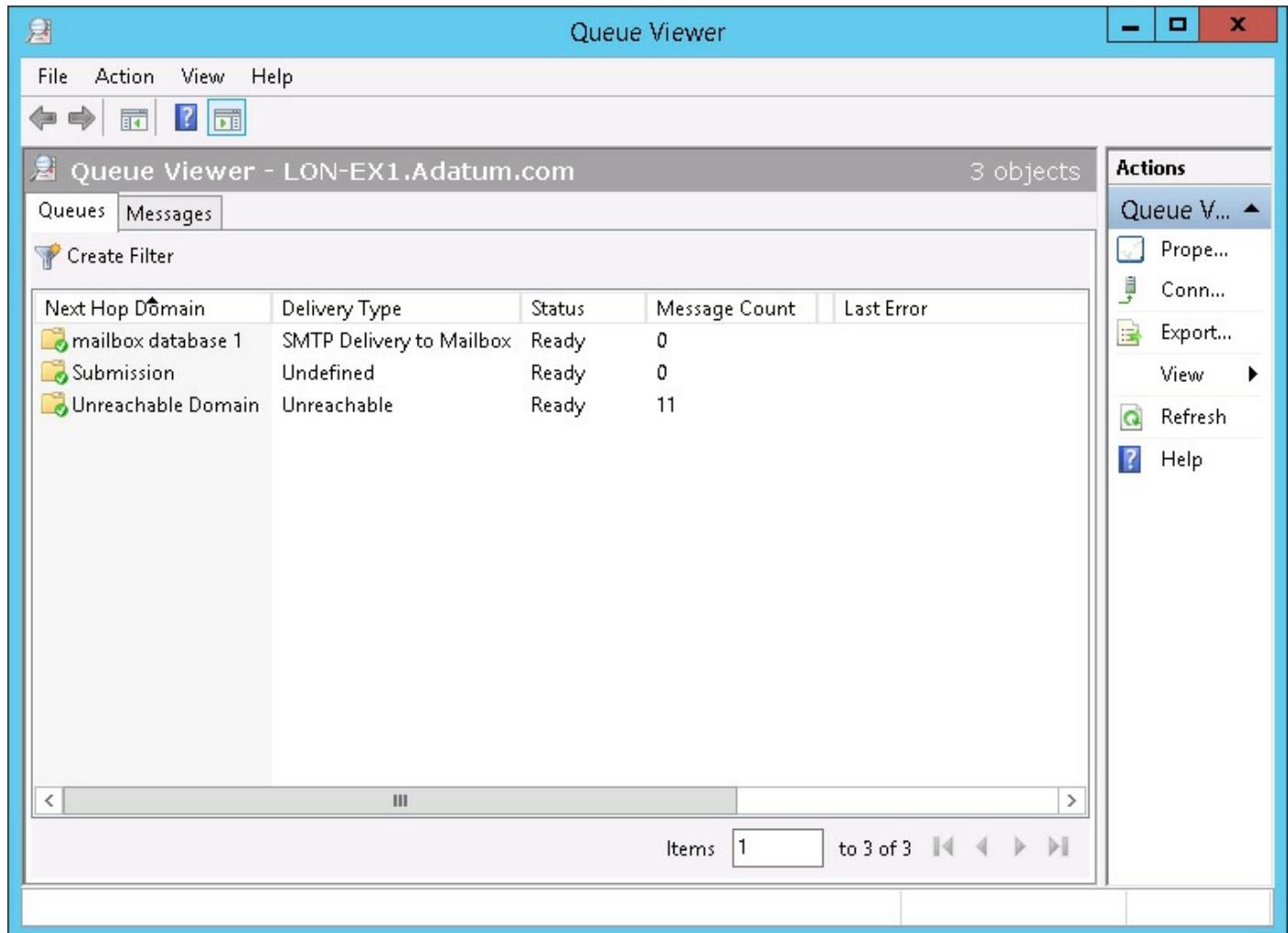


FIGURE 3-12 The Queues tab in the Queue Viewer tool

The Queue Viewer makes it easy to work with the queues and troubleshoot undeliverable messages. For example, [Figure 3-12](#) shows messages that are in an unreachable domain. You can right-click Unreachable Domain and view the messages. The result shows more information about the sender, the errors, and other message details, as shown in [Figure 3-13](#).

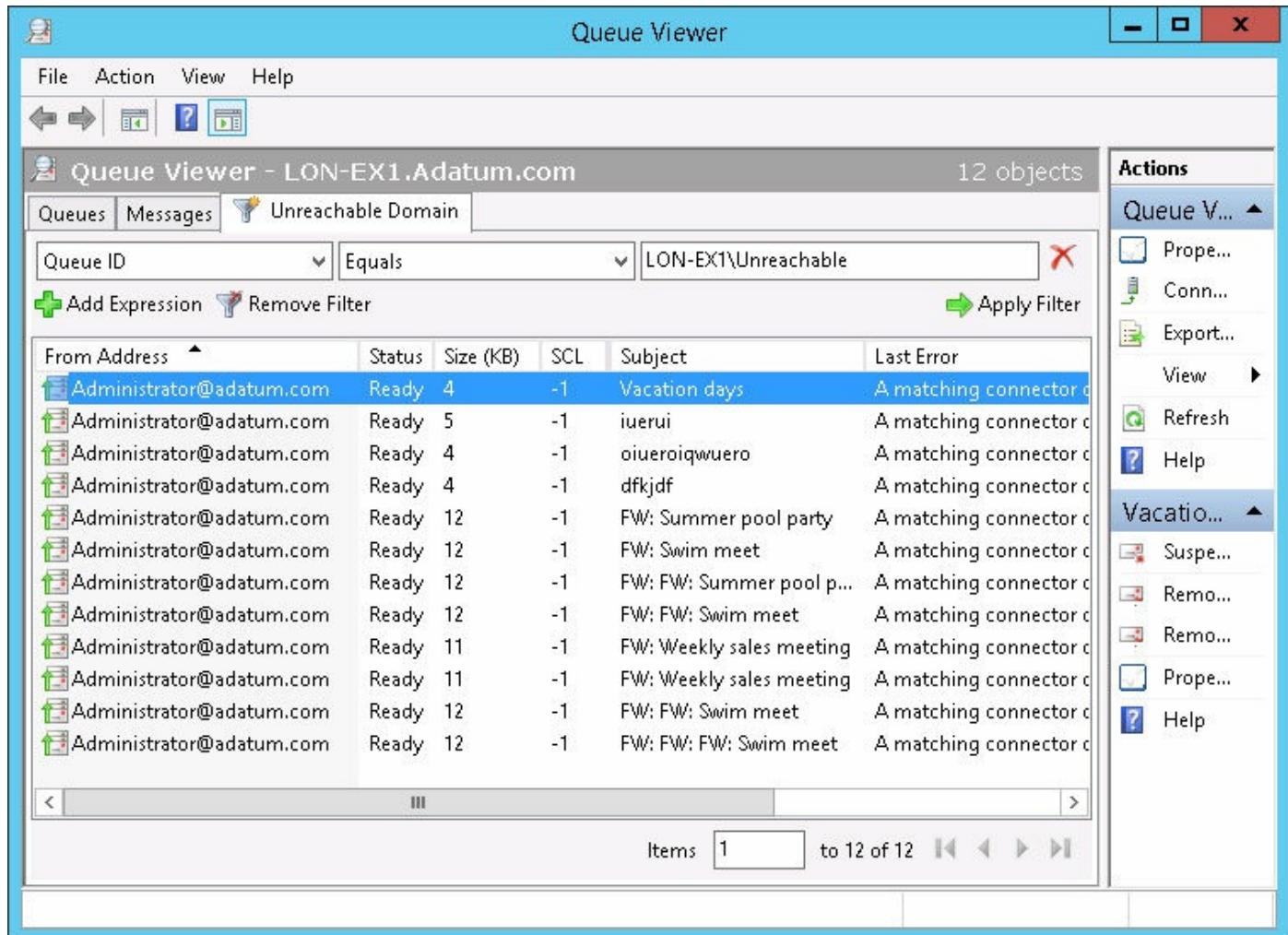


FIGURE 3-13 The details for a selected queue

From a troubleshooting perspective, the Queue Viewer is a great tool. It quickly shows you if queues are backing up and it shows you why. Then, from the Queue Viewer itself, you can take action to deal with messages in the queue, such as:

- **Suspend** Think of suspending a message as pausing delivery. The message remains in the queue until you resume it, removing it from suspension. You can right-click a message and choose to suspend it from the context menu.
- **Remove with NDR** You can remove messages in the queue by right-clicking them and choosing to remove them. When you remove with an NDR, the sender receives an NDR message. You might want to do this if you have a large number of messages being retried and you know that they will fail.
- **Remove without NDR** In some cases, you want to remove messages from a queue without notifying the sender. For example, if you are troubleshooting with a user and are having the user send test emails out, you might remove them without sending the user an NDR to minimize user confusion.
- **Resume** You can use the resume function to take messages out of suspension.

From that point, they resume their normal delivery processes.

### Quick check

- You have a DAG. You notice that one of the servers in the DAG has queues backing up. You want to quickly check all of the queues for all servers in the DAG. What should you do?

### Quick check answer

- You should use the Get-QueueDigest cmdlet specifying the DAG to return all of the queues for all servers in the DAG. For example, if your DAG name is DAG3, you can run the **Get-QueueDigest –Dag DAG3** command.

Besides working with the queues, SMTP mail flow can also be troubleshooted using some of the other tools and techniques described throughout this chapter, including some tools and techniques from upcoming topics.

## Given a failure scenario, predict mail flow and identify how to recover

The exam often presents scenarios to you. In some scenarios, you are in the planning stages. In other scenarios, you are troubleshooting. That's what this section covers. Walk through the following scenarios and try to figure out how to fix them.

- **Scenario 1: The disk drive is full and mail is not being sent from the Mailbox server** Back several years ago, it was thought that disk space would not be a problem after a few more years because disk space was becoming very inexpensive and disk drive sizes were dramatically increasing. It turns out that running out of disk space is still a major cause of Exchange problems. When you run out of disk space, the immediate thought is to add more disk space, but often that alone does not solve the problem. You might need to perform an offline defragmentation to free up space, especially if you aren't able to add more disk space to an Exchange server. Or, you might need to move the transaction logs to another disk drive. You might have to go through a soft recovery after adding disk space and you might also have to manually mount any offline databases.

- **Scenario 2: An internal server uses [SMTP.contoso.com](http://SMTP.contoso.com) for email delivery from an application** The FQDN points to two servers at the main office, Server1 and Server2. Server1 is unavailable and some email is not being delivered. What should you do? In this case, you can update the DNS record for [smtp.contoso.com](http://smtp.contoso.com) to just point to Server2 until Server1 is back up and running. To avoid this problem in the future, you can deploy a load balancer to replace DNS round robin. A load balancer detects that Server1 is down and automatically removes it

from the pool.

- **Scenario 3: Queues are filling up and appear to be stalled** In this situation, it is likely that the queues are going to get bigger and bigger. First, it is a good idea to figure out why the queues are filling up. Is email coming in so fast that the server can't keep up? This scenario isn't likely, but it is possible. Is spam and/or malware responsible? Which queues are being filled up? These are questions that you need to find answers to. One solution might be to fix an unavailable server. In the meantime, you might have to create a send connector or update AD DS site link costs or Exchange costs on AD DS site links. Other times, you might need to block malicious senders by adding their IP addresses to the IP Block list. Also don't forget about some of the core infrastructure which could be causing the problem. For example, DNS lookups might not be functioning properly or a network firewall might be blocking communication.
- **Scenario 4: A partner company sends an email to an internal user, but the email is never received** In this scenario, check the Edge Transport servers for issues. Check all filtering services, including anti-spam, anti-virus appliance, or service filtering, connection filtering, and the allow and block lists. Check message tracking logs on the Edge Transport servers to see if the email messages reached the organization. Check the queues at the Edge Transport server. Follow the message through the transport pipeline.

## Troubleshoot TLS

To effectively troubleshoot a ]technology, it is helpful to know how the technology works, what the prerequisites are, and information such as whether the service was already working or if it is a brand new configuration. Mutual TLS, whereby both servers use TLS for communication, is referred to as Domain Security in Exchange. The following list outlines the requirements for TLS with a focus on troubleshooting.

- **Certificates** When two organizations agree to use TLS for email communication between organizations, certificates are required. You can use Internal PKIs or third-party certificate providers. The most important thing is that the root certification authorities (CAs) are trusted by each organization. From a troubleshooting perspective, you need to check for revoked certificates, expired certificates, and for whether the root CAs are trusted. Additionally, you need to ensure the certificates are imported on the correct Exchange servers. For example, if you use Edge Transport servers, the certificates should be imported on them, since they would handle all inbound email.
- **Domain security configuration** After you have certificates covered, you need to look at the domain security configuration. During initial setup, the domain you send TLS email to is set and the domain you receive TLS email from is set. You

can use the Get-TransportConfig cmdlet without parameters to view the current setup. You should see both domains in the list with one populated in the TLSReceiveDomainSecureList property and the other in the TLSSendDomainSecureList property. If either is incorrect, you can fix them by using the Set-TransportConfig cmdlet and specifying the TLSReceiveDomainSecureList parameter or the TLSSendDomainSecureList parameter.

- **Send connectors** By default, send connectors are not enabled for Domain Secure. As part of the initial setup, you need to configure your send connector for it. For example, to configure a connector named Internet for Domain Secure, you can run the **Set-SendConnector Internet –DomainSecureEnabled:\$True** command. For troubleshooting, you can run the **Get-SendConnector Internet | FL** command to view the existing configuration. You need to look at whether Domain Secure is enabled. If it is enabled, the DomainSecureEnabled property's value should be True. You can also view the certificate used for TLS, the authentication used for TLS, and the TLS domain.
- **Receive connectors** Similar to send connectors, you also need to check the receive connectors. By default, receive connectors are not enabled for Domain Secure. You can use the Set-ReceiveConnector cmdlet with the DomainSecureEnabled parameter to enable a receive connector for Domain Secure. For troubleshooting, you should look at the existing configuration to ensure the receive connector handling inbound email is enabled for Domain Secure.

During a new configuration, you should look at the configuration first because it likely leads you to a resolution. For an existing mutual TLS configuration that was at one point functional, you should enable verbose protocol logging and examine the logs. You can enable logging on the receive and send connectors and then check the log files. Additionally, you can use the built-in performance counters. There is a performance category named MSExchange Secure Mail Transport that has a few counters related to Domain Secure:

- Domain-Secured Messages Received
- Domain-Secured Messages Sent
- Domain-Secured Outbound Session Failures

## Troubleshoot the new transport architecture

For the exam, the skills measured include this section titled “[Troubleshoot the new transport architecture](#).” This is a fairly generic topic that is partly covered by our earlier troubleshooting coverage. There are some important troubleshooting tips that you should be familiar with about earlier transport topics such as inter-site mail flow and, inter-org mail flow.

The first things to keep in mind is that email is routed using the lowest cost path. The cost is calculated by adding up the total cost of the AD DS IP site links along a chosen path. There are some additional details that you need to keep in mind for troubleshooting:

- You can also configure optional Exchange costs on AD DS site links. Imagine that you are troubleshooting email flow and find that email is taking a path that does not have the lowest total cost for the AD DS IP site links. What might cause that? Exchange costs are the likely culprit.
- Hub sites, mentioned earlier in this chapter, are also important in troubleshooting mail flow. Imagine that you are troubleshooting email flow between two sites. The sites are able to directly communicate through the headquarters site, but you find that email is not going directly from an Exchange server at one site to the Exchange server at the other site. What might cause this? A hub site. In this case, the headquarters site is a hub site. A hub site, when it is in the lowest cost path, always processes the email. You can check a site to see if it is a hub site by looking at the HubSiteEnabled property on the site. For example, to see if the site named London is a hub site, you can run the Get-AdSite ‘London’ command.
- Troubleshooting inter-org email is another area that might come up on the exam. Earlier in this chapter, you looked at planning inter-org email, walked through a typical configuration and walked through the step-by-step process. To prepare for the exam, you should look at the diagrams and study the step-by-step process. Imagine a scenario where you are sending email to an external organization, but the organization never gets the email. Which component in the transport architecture is the last one to deal with the email before it is sent to the external organization? If you are thinking the send connector on an Edge Transport server, great! If not, go back and review [Figure 3-3](#) and the associated mail flow steps. Now imagine a scenario where inbound email from the Internet is making it to your Edge Transport server, but the email never makes it to the mailboxes. Which component should you troubleshoot first? In such a scenario, you should look at the send connector on the Edge Transport server. You can also look at the receive connector in the Front End Transport service which receives the email from the send connector.

- Safety Net, the new name for the transport dumpster, is also part of the transport architecture. Troubleshooting Safety Net might come up on the exam. Safety Net is enabled by default. If you come across a scenario where Safety Net isn't functional, the first thing you need to do is check whether it is enabled and check the settings for how long it is holding email. You can run the **Get-TransportConfig | Select SafetyNetHoldTime** command to look at the existing configuration. If something is amiss, you can use the **Set-TransportConfig** cmdlet to fix it.
- Shadow redundancy is an optional feature that maintains copies of email messages before they are sent to mailbox databases and is enabled by default. To check if it is enabled, run the **Get-TransportConfig | Select ShadowRedundancyEnabled** command. Imagine a scenario where shadow redundancy isn't working, even though it is enabled. This scenario occurs in single-server Exchange environments. Shadow redundancy only works when there is more than one server in the environment.

The final topic to walk through for troubleshooting transport covers the Edge Transport role. The important things to know from a troubleshooting perspective are:

- Check if an edge subscription is configured. To check the configuration, run the **Get-EdgeSubscription** command on the Edge Transport server.
- Check firewalls, both the network firewall and Windows firewall, to ensure communication is enabled. Edge Transport servers listen on TCP port 50389 for standard LDAP and on TCP port 50636 for secure LDAP.
- An edge subscription file is valid for 24 hours. If you generate a file but don't finish the edge subscription process within 24 hours, you need to generate a new subscription file and start over.
- If you add a new mailbox server in a subscribed AD DS site and you want it to participate in EdgeSync synchronization, you need to re-subscribe the Edge Transport server.

Now that you have some troubleshooting knowledge for the exam, you are going to switch to look at a new topic: message hygiene. Message hygiene is a topic covering technologies to keep your environment safe, primarily from malware and spam.

## Summary

- Most Exchange logs need to be enabled before log files are generated. You can enable logging on send and receive connectors, in protocol settings, such as POP3 or IMAP, and on transport services, such as the Front End Transport service.
- When reviewing log files, you should look for key words that point to trouble

such as fail, unknown, bad, denied, and error.

- Address rewriting enables an organization to use a single domain name for all external communications while maintaining multiple domain names on the internal network. For example, a toy company with two divisions, Tailspin Toys and Wingtip Toys, could opt to use Tailspin Toys ([tailspintoys.com](http://tailspintoys.com)) for all external communication but maintain the two domains internally.
- You should use the Queue Viewer tool, the Get-Queue cmdlet, and the Get-QueueDigest cmdlet to troubleshoot email flow. You can quickly figure out if one or more servers have queues that are backing up. They can also help direct your efforts to the appropriate server or transport service.
- TLS and mutual TLS requires certificates and trusted root CAs, configuration of the Domain Security feature, and send and receive connectors to function. In a troubleshooting scenario with TLS, focus on those areas first.

### **Skill 3.3: Plan, deploy, and manage message hygiene**

This section focuses on planning, deploying, and managing message hygiene for incoming and outgoing messages. To run a successful email environment, you must plan for malware and spam to ensure that users do not receive the majority of malware and spam sent to them. To accomplish this, you can look at malware and spam filtering, connection filtering, recipient filtering, Send Policy Framework (SPF), and Spam Confidence Level (SCL) thresholds.

#### **This section covers how to:**

- [Plan and configure malware filtering](#)
- [Plan and configure spam filtering](#)
- [Plan and configure connection filtering](#)
- [Plan and configure recipient filtering](#)
- [Plan and configure Sender Policy Framework \(SPF\)](#)
- [Plan and configure Spam Confidence Level \(SCL\) thresholds](#)

### **Plan and configure malware filtering**

While this skill as a whole is for message hygiene, malware filtering itself can be broken up into two categories:

- Protecting the Exchange server itself
- Protecting clients from messages with malware

While this exam skill is focused on messages, there may be some questions on the

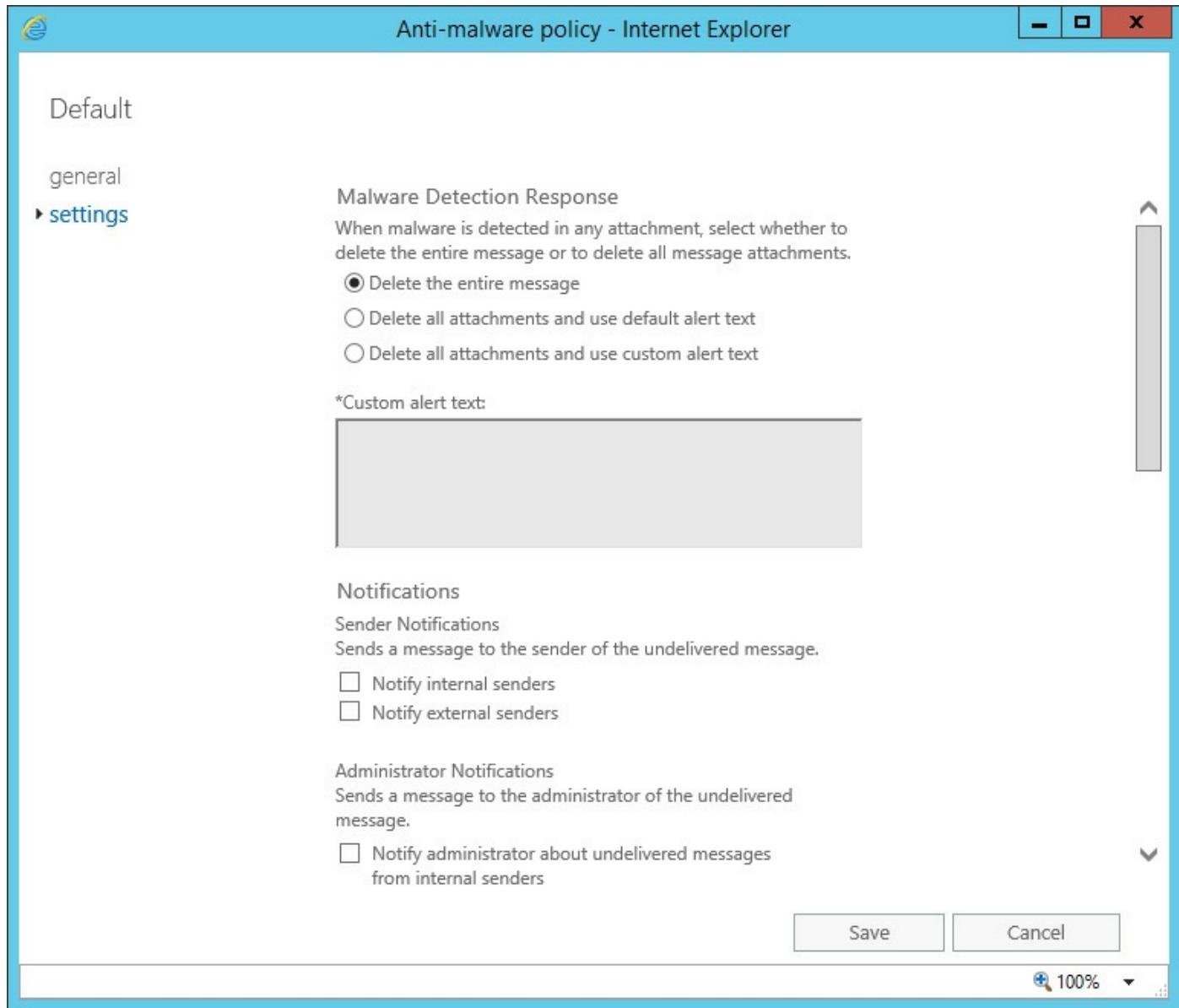
exam that relate to antivirus on the Exchange servers themselves. Traditional antivirus programs only detect malware that is running either in memory or stored in the file system. Therefore, these antivirus programs cannot detect malware that is in transport to a Mailbox server, or any malware that could have made its way to an Exchange database. It is important to configure local antivirus applications to exclude the Exchange database files on the server, as well as certain IIS directories if Outlook on the web is used on the server.

### **Need More Review? Folders to Exclude**

For a full list of recommended folders to exclude from antivirus scanning, see

<https://technet.microsoft.com/library/bb332342%28v=exchg.160%29.aspx>.

Focusing on malware filtering for messages, Exchange server has a built-in malware detection. By default, an anti-malware policy is enabled that deletes an entire message when malware is detected. You can customize the policies from the protection page within the EAC. [Figure 3-14](#) shows the default anti-malware policy.



**FIGURE 3-14** Anti-malware policy settings

If you need to configure an alert when deleting the malware message, you can use the default alert text or custom text. You can configure a malware policy to include notifications for internal and external senders as well as specific administrators.

As with most components in Exchange Server, you can configure malware policies and rules by using Windows PowerShell. You can manage three primary malware components by using PowerShell:

- MalwareFilteringServer
- MalwareFilterPolicy
- MalwareFilterRule

Each of the components have various cmdlets available in the form of \*-MalwareFilterPolicy. For a full list, run the following command from the EMS:

```
Get-Command *Malware*
```

For example, to create a new malware policy, use the New-MalwareFilterPolicy cmdlet. To create a new policy that deletes the malware attachment and then creates a default alert, run the following command:

[Click here to view code image](#)

```
New-MalwareFilterPolicy -Name Policy1 -Action  
DeleteAttachmentAndUseDefaultAlertText
```

Note that when using PowerShell to configure malware settings, creating a policy does not enable the policy or make it active. A rule must also be created by using the New-MalwarePolicyRule cmdlet that references the policy object. For example, to create a rule named Rule1 that uses the policy named Policy1 from the previous example, run the following command:

[Click here to view code image](#)

```
New-MalwareFilterRule -Name Rule1 -MalwareFilterPolicy Policy1 -  
RecipientDomainIs  
contoso.com
```

This command enables the policy that was created for messages that are destined for the contoso.com domain.

## Plan and configure spam filtering

Exchange Server offers several anti-spam agents that can be enabled on Mailbox or Edge Transport servers to assist in preventing spam from reaching user mailboxes. By default, these agents are not enabled. To enable anti-spam agents on an Edge Transport server, you must be a member of the local administrator's group on the server. Additionally, you must also be granted the Organization Management and Hygiene Management roles for the organization.

It is also important to note that anti-spam agents cannot be enabled through the EAC. Instead, there is a pre-defined script located in the installation directory of Exchange Server that enables the anti-spam agents. In the installation directory, in the Scripts folder, the script name is Install-AntiSpamAgents.ps1. If you successfully run the script, you see several warnings, stating that the PowerShell session and the Exchange Transport service must be restarted. [Figure 3-15](#) shows a successful result when running the built-in script.

```

[PS] C:\Program Files\Microsoft\Exchange Server\v15\Scripts>.\install-AntispamAgents.ps1
Creating a new session for implicit remoting of "Get-TransportService" command..
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport

Identity                           Enabled   Priority
Content Filter Agent              True      12
WARNING: The following service restart is required for the change(s) to take effect : MSExchangeTransport
WARNING: Please exit Windows PowerShell to complete the installation.

```

FIGURE 3-15 The Install-AntiSpamAgents.ps1 run results

When the agents are enabled, you must also specify the internal SMTP servers for the Exchange organization. The best method to do this is by using the Set-TransportConfig cmdlet. For example, to add an SMTP server with the IP address of 192.168.1.112, run the following command:

[Click here to view code image](#)

```
Set-TransportConfig -InternalSMTPServers @{Add="192.168.1.112"}
```

By using the Add function in this cmdlet, it does not modify or replace any of the existing values in the Transport configuration server configuration. [Figure 3-16](#) shows restarting the Microsoft Exchange Transport service and adding an SMTP server for the organization to the Transport server configuration.



```

Machine: NYC-EX1.contoso.com

[PS] C:\Program Files\Microsoft\Exchange Server\v15\Scripts>Restart-Service MSExchangeTransport
WARNING: Waiting for service 'Microsoft Exchange Transport (MSExchangeTransport)' to stop...
WARNING: Waiting for service 'Microsoft Exchange Transport (MSExchangeTransport)' to start...
WARNING: Waiting for service 'Microsoft Exchange Transport (MSExchangeTransport)' to start...
[PS] C:\Program Files\Microsoft\Exchange Server\v15\Scripts>Set-TransportConfig -InternalSMTPServers @{Add="192.168.1.112"}
[PS] C:\Program Files\Microsoft\Exchange Server\v15\Scripts>

```

FIGURE 3-16 Restarting and configuring the Transport service

After spam filtering has been enabled and configured, you can enable the individual components that spam filtering offers. These include:

- Content filtering
- Attachment filtering
- Safelist aggregation
- Spam confidence level threshold
- Sender filtering

- Sender ID
- Sender reputation

One aspect of anti-spam filtering is attachment filtering. Attachment filtering enables administrators to control the types of attachments that can be received in email messages, either by file name, file type, or MIME content type. For example, you can block users in the organization from receiving .exe or .reg files. MIME filtering is based on the content type, which is defined by <type>/<subtype>. For example, JPEG images are represented by image/jpeg.

After you define the file or MIME types to filter, you can decide what to do with the email message:

- **Block the message** Blocking the message notifies the sender that the content or file type cannot be delivered because of the attachment.
- **Remove the attachment** Removing the attachment allows the message to be delivered, but removes the attachment from the message. If other approved attachments are included with the message, those attachments are still delivered with the message.
- **Delete the message** Deleting the message simply drops it from the queue, without notifying the sender or the receiver.

It is important to note that if you combine removing an attachment from email messages that are digitally signed, encrypted, or protected by Rights Management Services, the signature of the message becomes invalid. Messages without a valid signature cannot be opened and are unreadable. For outgoing messages, this can be avoided by signing the messages only after they have been processed by the agent.

Another feature of anti-spam filtering you can use is the sender reputation level. The sender reputation level can be calculated and enabled at the Edge Transport server to block messages based on characteristics of the sender. Sender reputation is calculated by the Protocol Analysis agent of the anti-spam service. There are a number of characteristics that can be used to determine the sender reputation. These include:

- **HELO/EHLO analysis** Servers that send spam messages frequently forge the HELO/EHLO statement. By analyzing and comparing the IP addresses provided in these statements, fraudulent servers can be identified.
- **Reverse DNS lookup** Sender reputation can use the reverse DNS to check and see if the source IP address and domain name matches the reverse DNS. For example, if a sending server in the contoso.com domain has an IP address of 10.95.80.40 (A private IP address is used here only as an example. The IP address is usually a public IP address.) but the reverse DNS shows a server in the fabrikam.com domain, you can block messages from the server.

- **Spam confidence level** When the Content Filter agent processes a message, it also generates a spam confidence level based on the contents of the message. The spam confidence level uses a rating between zero and nine. The higher the number, the more confident the agent is that the message is spam.
- **Open proxy test** An open proxy is essentially an open relay, being a server that accepts connection requests from anyone and forwards the traffic as if it was local. This enables malicious users and spammers to hide their identities and send messages through the proxy server. You can block messages from open proxy servers.

Similar to the spam confidence level, the sender reputation level is also rated for each message from zero to nine. You can configure how the agent handles messages with certain levels. By default, messages rated with a seven or higher are blocked and the sender is blocked for 24 hours. Senders that have not had any messages analyzed start with a reputation of zero and begin receiving a rating after 20 messages have been received.

There are similar actions that can be taken for messages coming from a blocked sender:

- **Reject** The message is not delivered and a non-delivery report is sent to the sender.
- **Delete** The message is not delivered and no notification is sent to the sender or receiver.
- **Accept** The message is delivered, but is marked as coming from a blocked sender.

## Plan and configure connection filtering

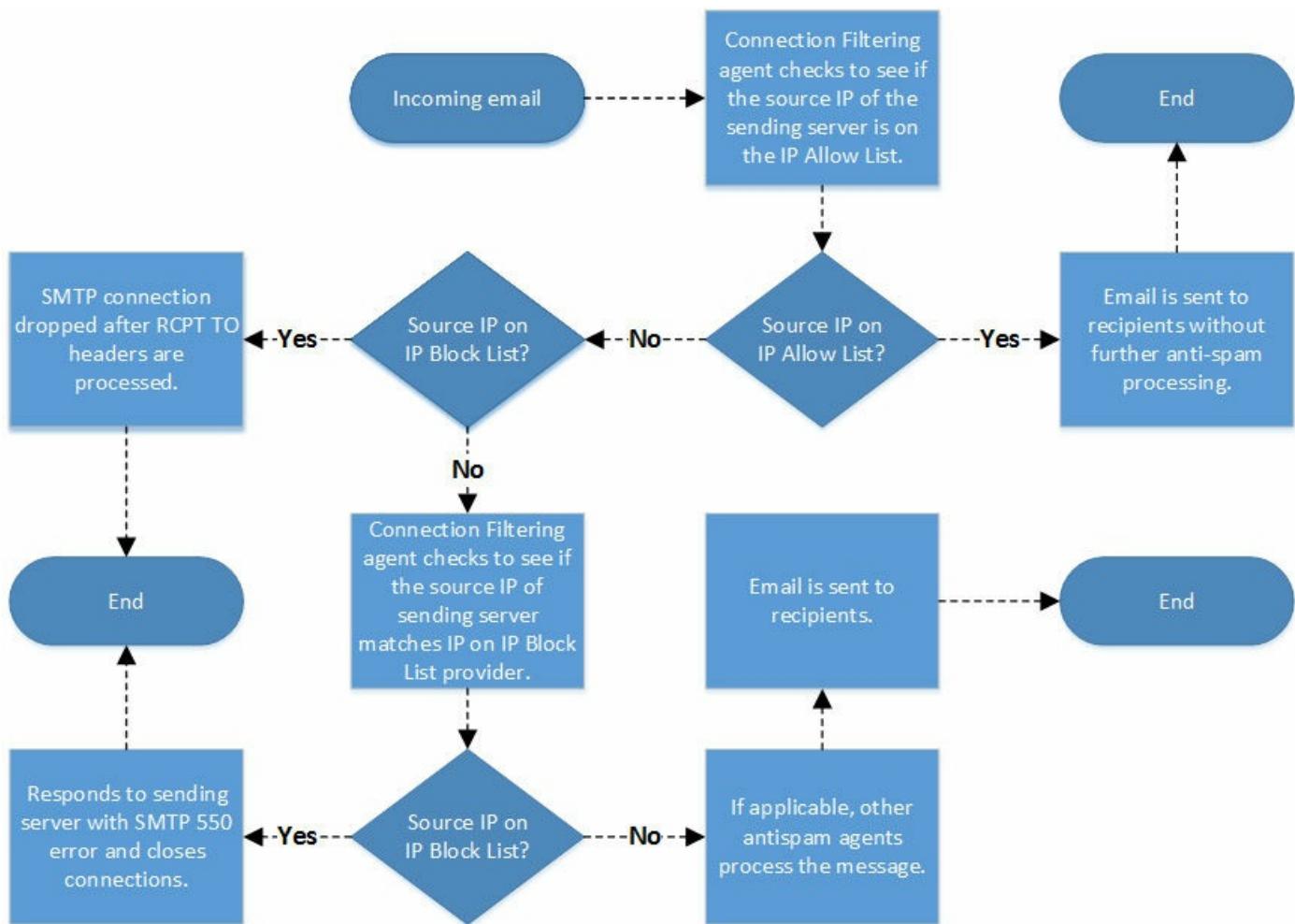
Connection filtering is a feature within the anti-spam component of Exchange Server. Connection filtering evaluates mail that is being received based on a few factors:

- IP Block list
- IP Allow list
- IP Block list providers
- IP Allow list providers

The IP Block and Allow lists are simply lists of configured IP addresses that are either explicitly allowed or blocked. As the Exchange administrator, you are responsible for maintaining IP addresses that are in either list. As part of maintaining these lists, you can also set expiration times for the IP addresses that are configured on either list. This automatically disables the block or allow for the configured IP address when the expiration time has been reached.

Specifically for the block list, IP addresses can be added automatically on the Sender Reputation feature of the Protocol Analysis agent.

Block list providers are often referred to as Real-time Block Lists (RBLs). RBLs are typically third-party services or systems that compile lists of IP addresses that are frequently reported as spam, or are open relays that are frequently used to send spam. This might also include dynamic IP addresses from certain Internet Service Providers. If an RBL has been configured in the Exchange environment, the connection filtering agent compares the source IP address against the RBL. If the IP address is found on an RBL, the Transport server processes the recipient headers and responds to the email with an SMTP 550 error. If the IP address is not found on an RBL, the message is handed off to the next agent on the Transport server. [Figure 3-17](#) shows the decision making process for Edge Transport servers as each mail message arrives.



**FIGURE 3-17** Incoming message process for anti-spam

The SMTP 550 error the Mailbox or Edge Transport server sends when a spam message is received can be customized to include the RBL the message was verified against. This helps in scenarios where a message is identified as spam, when in reality the message is from a legitimate sender. This enables the sending administrator to verify

their IP address or email configuration so that they are not on the RBL.

When a message is identified as spam from an RBL, the RBL typically includes a reason code through either a bitmask or data value. [Table 3-1](#) displays common values and reasons why a sender is on an RBL.

Value	Reason
1	The IP address is on an IP Block list.
2	The SMTP server is an open relay.
4	The IP address supports dial-up connections.
127.0.0.2	The IP address is a direct spam source.
127.0.0.4	The IP address is a bulk mailer.
127.0.0.5	The remote server sending the message supports multi-stage open relays.

TABLE 3-1 RBL reasons

IP Allow lists and IP Allow list providers are similar to block lists in the way that they are configured. Instead of blocking messages, however, messages are successfully passed to the next transport service without additional processing by the anti-spam agent. Therefore, it's recommended to only use an allow list for trusted partner organizations. Allow list providers act in a similar manner to an RBL, except that it is a white or safe list instead of a block list. Most organizations rarely use this feature, however, as the list is maintained by a third-party.

To verify that the Connection Filter agent is enabled, run the following command:

[Click here to view code image](#)

```
Get-TransportAgent "Connection Filtering Agent"
```

If the agent is disabled, you can enable it by using the Enable-TransportAgent cmdlet. For example:

[Click here to view code image](#)

```
Enable-TransportAgent "Connection Filtering Agent"
```

When the agent is enabled, you can add lists and providers by using one of the following cmdlets:

- Add-IPBlockListEntry
- Add-IPBlockListProvider
- Add-IPAllowListEntry
- Add-IPAllowListProvider

For example, to block message that originate from the 10.0.0.0/24 network, run the following command:

[Click here to view code image](#)

```
Add-IPBlockListEntry -IPRange 10.0.0.0/24
```

## Need More Review? Connection Filtering

For more information on enabling, disabling, adding, or removing connection filtering with Exchange 2016, visit

<https://technet.microsoft.com/library/bb124376%28v=exchg.160%29.aspx>

## Plan and configure recipient filtering

Recipient filtering is another feature of anti-spam with Exchange 2016. You can use recipient filtering to block messages sent to specific recipients or to recipients that don't exist in the organization. This functionality relies on the recipient header to determine which action needs to be taken. The Recipient Filter Agent in the Edge Transport service performs the action. The following examples describe how recipient filtering can assist in reducing spam:

- **Recipients that don't exist** This can prevent messages from being delivered to a Mailbox server when the recipient doesn't exist in the organization.
- **Internal distribution groups** This can prevent external email from being delivered to internal distribution groups that should only be used by organizational user for example, an executive-level distribution group.
- **Internal mailboxes** This can prevent external email from being delivered to mailboxes that should only be used internally. For example, a help desk mailbox.

The recipient block list is a list defined by Exchange administrators that includes the distribution groups or mailboxes that should not receive external email. To block messages for recipients that don't exist, the agent can use EdgeSync to query Active Directory to ensure that the account exists and has an associated mailbox.

Even though recipient filtering can be configured on a Mailbox server, it is not recommended to configure it there. Instead, recipient filtering should be configured on an Edge Transport server to prevent any legitimate messages from being blocked. Recipient filtering on a Mailbox server blocks the message to all recipients, even if only one of the recipients is invalid or blocked.

Recipient filtering is enabled by default, but does not have any lists or providers configured. To view the current configuration, use the Get-RecipientFilterConfig cmdlet. To enable the block list, run the following command:

[Click here to view code image](#)

```
Set-RecipientFilterConfig -BlockListEnabled $true
```

## Need More Review? Recipient Filters

For more information on configuring recipient filters with PowerShell, see <https://technet.microsoft.com/library/bb125187%28v=exchg.160%29.aspx>.

## Plan and configure Sender Policy Framework

The Sender Policy Framework (SPF) is a method used in conjunction with DNS to detect spoofing. A spoofed email message appears to be from a legitimate sender, when in reality, it is spam or malware from another sender. For example, a rogue DNS server might attempt to send email as [contoso.com](#) even though it doesn't have any affiliation with [contoso.com](#). With Sender ID in Exchange, the RECEIVED SMTP header within a message can be used to query the DNS record of the source domain to ascertain whether the domain name has been spoofed. Sender ID is enabled by default on Edge Transport servers, but it can also be enabled on Mailbox servers.

When Exchange receives a message, the Sender ID agent verifies the sender's IP address by using DNS for the sender's domain. This ensures the IP address that sent the message is an authorized sender for that domain. Administrators publish the Sender Policy Framework records by using TXT records in DNS and use these records to identify the authorized servers for a domain. If an SPF record is available in DNS, the Exchange server can verify that the source IP address is authorized to send on behalf of the domain.

[Table 3-2](#) outlines the possible evaluation results of an SPF record.

Result	Status
Pass	Allow the message to be sent
Fail	Block the message from being sent
SoftFail	Host is not allowed to send, but is being transitioned
Neutral	Nothing to confirm the validity
None	No SPF record exists
PermError	Permanent error, such as improperly formatted record
TempError	Temporary error

TABLE 3-2 SPF evaluation results

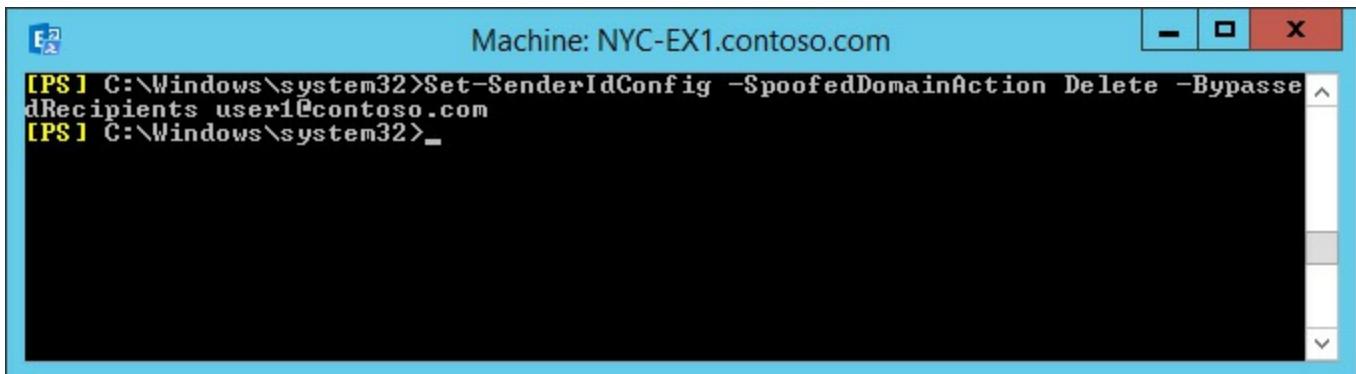
Note that if the header does not have a source IP address, Exchange processes the message without including a Sender ID status. The message is sent to the next agent, and an event is logged in the Event Log. The status of the SFP does not affect whether a message is flagged as spam within Outlook. Outlook uses the Sender ID status as part of the calculation for the spam confidence level.

Sender ID configuration on an Exchange server can be configured by using the Set-

SenderIdConfig cmdlet. For example, to delete email that has been spoofed, but exclude a mailbox with the SMTP address [user1@contoso.com](mailto:user1@contoso.com), run the following command. [Figure 3-18](#) shows the command output.

[Click here to view code image](#)

```
Set-SenderIdConfig -SpoofedDomainAction Delete -BypassedRecipients  
user1@contoso.com
```



```
[PS] C:\Windows\system32>Set-SenderIdConfig -SpoofedDomainAction Delete -BypassedRecipients user1@contoso.com  
[PS] C:\Windows\system32>_
```

FIGURE 3-18 Set-SenderIdConfig

### Need More Review? SPF and RFC 7208

The Sender Policy Framework is based on RFC 7208. For more information on the standard, visit [http://www.openspf.org/SPF\\_Record\\_Syntax](http://www.openspf.org/SPF_Record_Syntax).

## Plan and configure Spam Confidence Level (SCL) thresholds

Spam Confidence Level (SCL) has been mentioned a few times in this section. The SCL is calculated based on numerous email message characteristics. You can configure Exchange to reject, delete, or quarantine messages based on the SCL. These actions are performed by the Content Filter agent of the anti-spam service. Other aspects of the anti-spam service are absolute in whether a message is blocked or allowed. For example, the block and allow lists either block or allow the message. Using the SCL is slightly different because it rates a message based on numerous factors. You configure a threshold value for each action that can be taken and the Exchange server takes the action when a threshold is reached. The values should be monitored regularly, however, to ensure that legitimate messages are not being quarantined or rejected.

As mentioned previously, the SCL value can range from zero to nine, with the higher number representing a more of a likelihood that the message is spam. Each action can be configured with a different value:

- **SCL delete threshold** This SCL message value must be at this level or higher for the message to be deleted. By default, this value is set to nine. With this action, the

message is deleted with no notification.

- **SCL reject threshold** This SCL message value must be at the minimum value, but lower than the delete threshold for the message to be rejected. By default, this value is set to seven. With this action, messages are rejected and the sender is notified with a non-delivery report.
- **SCL quarantine threshold** The SCL message value must be at the minimum value, but lower than the reject threshold. This value is set to nine by default, but is disabled. With this action, messages are delivered to a specified quarantine mailbox. Administrators can then review the mailbox to ensure that legitimate email has not been sent to quarantine, or that the mailbox is not full of spam.
- **SCL Junk Email folder threshold** The SCL message value must be greater than the configured value to be moved to the Junk Email folder in Outlook. Note that this is the only action that requires the SCL value to be greater than the value set. By default, the threshold value is set to three. Therefore, only messages with a value of four or higher are moved to the Junk Email folder. A message with the value of three is delivered to the mailbox.

Each of these actions can be configured at different locations within an Exchange organization. Individual mailboxes can be configured differently than a server or organization. The Junk Email folder threshold can be set for an entire organization or each server can be configured individually for the delete, reject, and quarantine thresholds.

To configure SCL threshold levels, use the Set-ContentFilterConfig cmdlet. For example, to set the delete threshold to seven, run the following command:

[Click here to view code image](#)

```
Set-ContentFilterConfig -SCLDeleteEnabled $True -SCLDeleteThreshold 7
```

Note that to configure the delete threshold to a lower value than the default of 9, the reject threshold must be lowered before performing the configuration change. The service does not let you set the delete threshold to a value lower than or equal to the reject action value.

To configure the organization for the Junk Email folder threshold, use the Set-OrganizationConfig cmdlet. For example:

[Click here to view code image](#)

```
Set-OrganizationConfig -SCLJunkThreshold 4
```

[Figure 3-19](#) shows the configuration of the delete, reject, and Junk Email thresholds.

```
[PS] C:\Windows\system32>Set-ContentFilterConfig -SCLRejectThreshold 7  
[PS] C:\Windows\system32>Set-ContentFilterConfig -SCLDeleteThreshold 8  
[PS] C:\Windows\system32>Set-OrganizationConfig -SCLJunkThreshold 4  
[PS] C:\Windows\system32>Get-ContentFilterConfig  
  
RunspaceId : 99b9133a-3937-4d62-8ab4-f07ebb0fa342  
Name : ContentFilterConfig  
RejectionResponse : Message rejected as spam by Content Filtering.  
OutlookEmailPostmarkValidationEnabled : True  
BypassedRecipients : <>  
QuarantineMailbox :  
SCLRejectThreshold : 7  
SCLRejectEnabled : True  
SCLDeleteThreshold : 8  
SCLDeleteEnabled : True  
SCLQuarantineThreshold : 9  
SCLQuarantineEnabled : False
```

FIGURE 3-19 Configuring SCL settings and viewing the content filter configuration

Now that you have finished looking at message hygiene, turn your attention to site resilience for transport services in the next section.

## Summary

- Configure exceptions for local antivirus running on Exchange servers.
- You can configure malware policies by using the EAC and Windows PowerShell.
- You can enable spam filtering only through PowerShell. A built-in script is provided to enable the functionality.
- Connection filtering enables you to allow or block specific IP addresses.
- Recipient filtering prevents spam from reaching servers if a recipient is not valid.
- The Sender Policy Framework (SPF) helps prevent spoofing of domains.
- The Spam Confidence Level is used to delete, reject, quarantine, or move messages to the junk email folder based on the calculated rating of the message.

## Skill 3.4: Plan, deploy, and manage site resilient transport services

Besides just implementing and managing transport services, you also need to understand how to make those services site resilient. If one site becomes unavailable, how can you ensure that another site handles transport services? This section looks at making transport services site resilient.

## This section covers how to:

- [Plan, create and configure MX records for failover scenarios](#)
- [Manage resubmission and reroute queues](#)
- [Plan, create, and configure Send/Receive connectors for site resiliency](#)
- [Test and perform steps for transport failover and switchover](#)

## Plan, create and configure MX records for failover scenarios

Mail exchange (MX) records are how organizations determine where to send mail for a domain. For example, when someone sends an email to [aaren@adatum.com](mailto:aaren@adatum.com), the sending email servers perform a DNS lookup for the MX record of [adatum.com](http://adatum.com). Earlier in this chapter, you looked at how to use MX record for redundancy. These techniques can be used for failover scenarios as well. [Figure 3-20](#) shows the result of creating an MX record for the adatum.com domain.

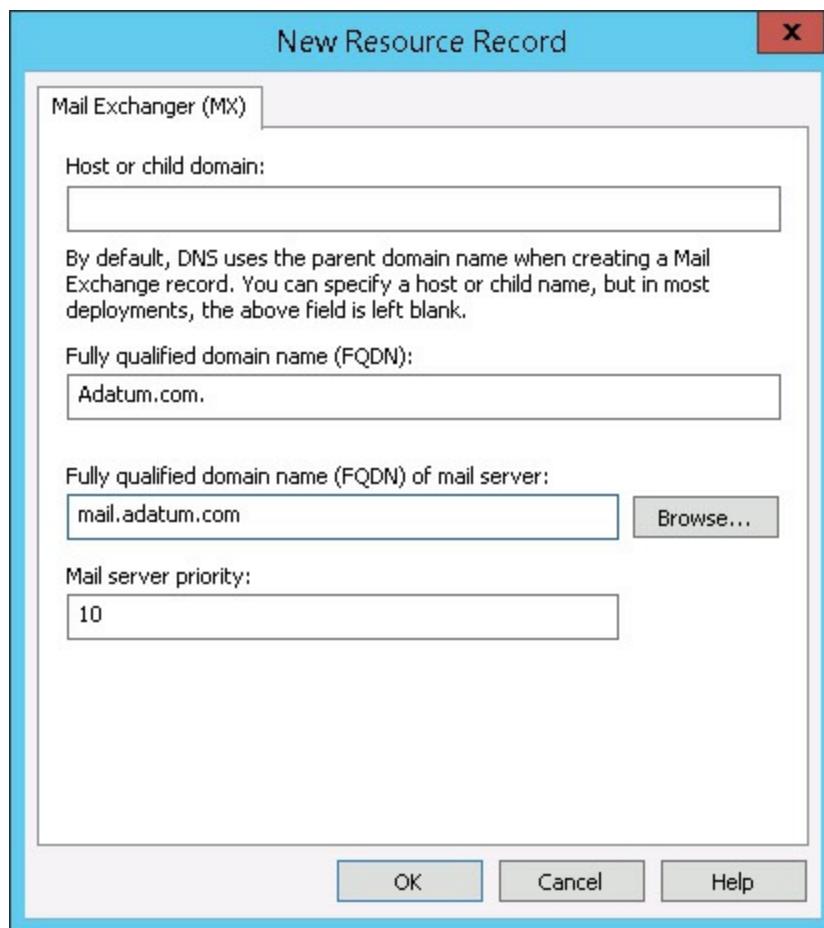


FIGURE 3-20 The MX record for [mail.adatum.com](mailto:mail.adatum.com)

A simple method of load balancing incoming SMTP connections is to assign multiple MX records with the same preference. When a sender queries DNS for the MX record, it receives both IP addresses with the same preference. Servers then alternate between

the IP addresses to send email messages.

The MX preference is defined by the receiving administrator in DNS. For most DNS providers, the mail server's priority is set to 10 by default. By using tiered mail servers with different MX preferences, you effectively create a simple failover scenario. An MX record configuration that uses multiple servers might look similar to [Table 3-3](#).

Priority	FQDN	IP address
10	mail1.contoso.com	10.10.10.100
20	mail2.contoso.com	10.20.20.100
30	mail3.contoso.com	10.30.30.100

TABLE 3-3 DNS MX records

In this scenario, all mail is routed to the server at [mail1.contoso.com](#). In the event that the server is unavailable, mail is then sent to [mail2.contoso.com](#). Finally, if both servers are unavailable, mail is sent to [mail3.contoso.com](#). Note that [mail3.contoso.com](#) only receives mail if the first two servers are unavailable.

## Manage resubmission and reroute queues

If a mail server is not responding or accepting mail, the sending server has several configuration options for retrying or resubmitting an email message before the message expires. A retry is defined as a continued attempt to connect to the destination server. Resubmitting a message is defined as moving an email message back in the process to the submission queue, so that it can be reprocessed as though it were new. Finally, when a message expires, a failed delivery notification is sent to the sender and the message is deleted from the queue.

### Automatic message retries

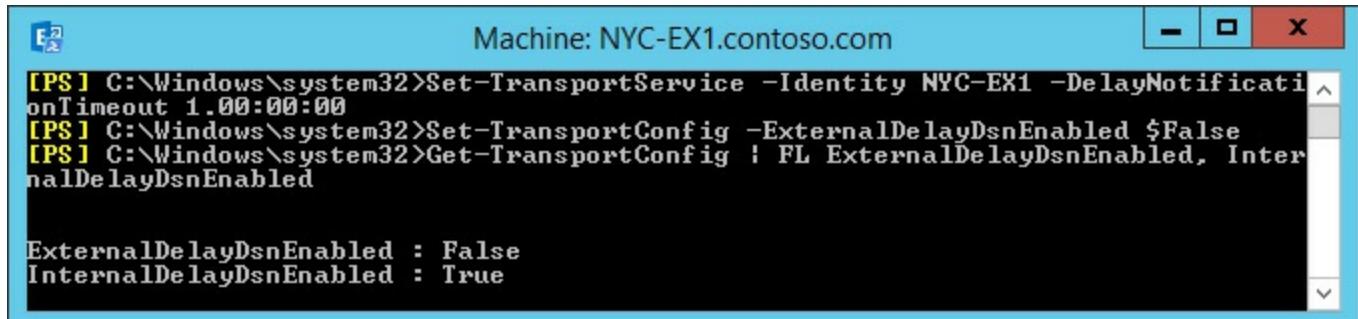
For email messages that fail to send, the first course of action is to use message retries. Retries are another attempt to send the email message. You can configure message retries by using the Set-TransportService cmdlet. For message retries, you can use the TransientFailureRetryCount parameter to set the number of connection attempts that the sending server should make to deliver a message. By default, this parameter is set to six, but you can set it to any number between 0 and 15. To set this parameter, run the following command:

[Click here to view code image](#)

```
Set-TransportService -TransientFailureRetryCount 10
```

When a message cannot be delivered, a delivery status notification message is queued to the original sender after the value in the timeout parameter has elapsed. You can configure the DelayNotificationTimeOut parameter by using the Set-TransportServer

cmdlet, but whether these messages are delivered is controlled by the Set-TransportConfig cmdlet. For example, [Figure 3-21](#) shows configuring the DelayNotificationTimeOut parameter to one day, but only enabling the delivery status notification message to internal senders. By default, both delivery status notification options are enabled.



```
Machine: NYC-EX1.contoso.com
[PS] C:\Windows\system32>Set-TransportService -Identity NYC-EX1 -DelayNotificationTimeout 1.00:00:00
[PS] C:\Windows\system32>Set-TransportConfig -ExternalDelayDsnEnabled $False
[PS] C:\Windows\system32>Get-TransportConfig : FL ExternalDelayDsnEnabled, InternalDelayDsnEnabled

ExternalDelayDsnEnabled : False
InternalDelayDsnEnabled : True
```

**FIGURE 3-21** Configuring an Edge Transport server's delivery status notifications

One of the parameters in the EdgeTransport.exe.config file is the MaxIdleTimeBeforeResubmit parameter. This parameter controls the interval for a message to be resubmitted. The parameter is set to 12 hours by default. Only messages in a delivery queue can be considered for automatic resubmission. Messages in the delivery queue can be resubmitted manually at any time, either by using the Queue Viewer or by using the Retry-Queue cmdlet.

Finally, the MessageExpirationTimeOut parameter defines the maximum amount of time that the Transport service has to attempt to deliver a message before removing it from the queue. By default, the value is set to two days. This parameter can be configured by using the Set-TransportService cmdlet, and can be configured for anything between 5 seconds and 90 days. Additionally, messages can be removed or exported from the queue at any time.

## Manual message retries

When an Exchange Server delivery queue has a status of Retry, you can try to manually force the message to be delivered by using the Queue Viewer. You can also use the Retry-Queue cmdlet in the EMS. Attempting to manually retry the message overrides the next scheduled retry. If the message cannot be delivered manually, the regularly scheduled retries begin again.

## Automatic message resubmission

The scheduled timer for automatic message resubmissions is controlled by the MaxIdleTimeBeforeResubmit parameter. This parameter is defined in the EdgeTransport.exe.config configuration file. The default value is 12 hours, defined as 12:00:00 in the file. You can specify a value by using the format dd.hh:mm:ss, where d = days, h = hours, m = minutes, and s = seconds.

## Manual message resubmission

Similar to retrying a message manually, you can also resubmit the message manually. You can resubmit messages that are in the following state:

- message queues that have a status of Retry and email messages that are not suspended
- messages that are in the unreachable queue and are not suspended
- messages that are in the poison message queue

You can manually resubmit messages before the MaxIdleTimeBeforeResubmit parameter has expired by using the `Retry-Queue` cmdlet. For messages that are in the poison queue, use the `Resume-Message` cmdlet or the Queue Viewer tool.

Another method to manually resubmit messages is to suspend the messages in the delivery or unreachable queues. Using PowerShell, you can export the email messages to text-based .eml files. The .eml files can then be copied to the Replay directory of a Mailbox or Edge Transport server. This causes the Exchange server to resubmit any of the messages that it finds in this directory. Because the messages have to be suspended, this method does not work for messages in the Submission queue. Also, exporting the messages does not delete them from the queue they were exported from. Therefore, to avoid duplicate deliveries, ensure that you delete the messages from the original queue before replaying them.

By default, the replay directory is located at `%ExchangeInstallPath%\TransportRoles\Replay`. The directory is scanned every five seconds for messages. To export all messages originating from a domain named contoso.com on a server named NYC-EX1, run the following command:

[Click here to view code image](#)

```
Get-Message -Filter {FromAddress -like "*@contoso.com"} -Server NYC-EX1 |  
ForEach-Object  
{$Temp="C:\ "+$__.InternetMessageID+".eml";$Temp=$Temp.Replace("<","_");$Temp=$Temp.  
Replace(">","_");Export-Message $_.Identity | AssembleMessage -Path $Temp}
```

## **Plan, create, and configure Send/Receive connectors for site resiliency**

This skill is a holdover from earlier versions of Exchange Server when there were dedicated hub transport servers. When there were dedicated hub transport servers, you had to take special actions to provide site resiliency, especially if some sites did not have direct Internet access. For example, there were times when you had to configure send/receive connectors for Internet connectivity at a secondary site if the Internet-connected site went down. With Exchange 2016, if you lose your transport servers, you lose your mailbox servers so you won't need to configure send and receive connectors to get to the other site. There are a couple of scenarios however, where you might need to configure connectors for site resiliency:

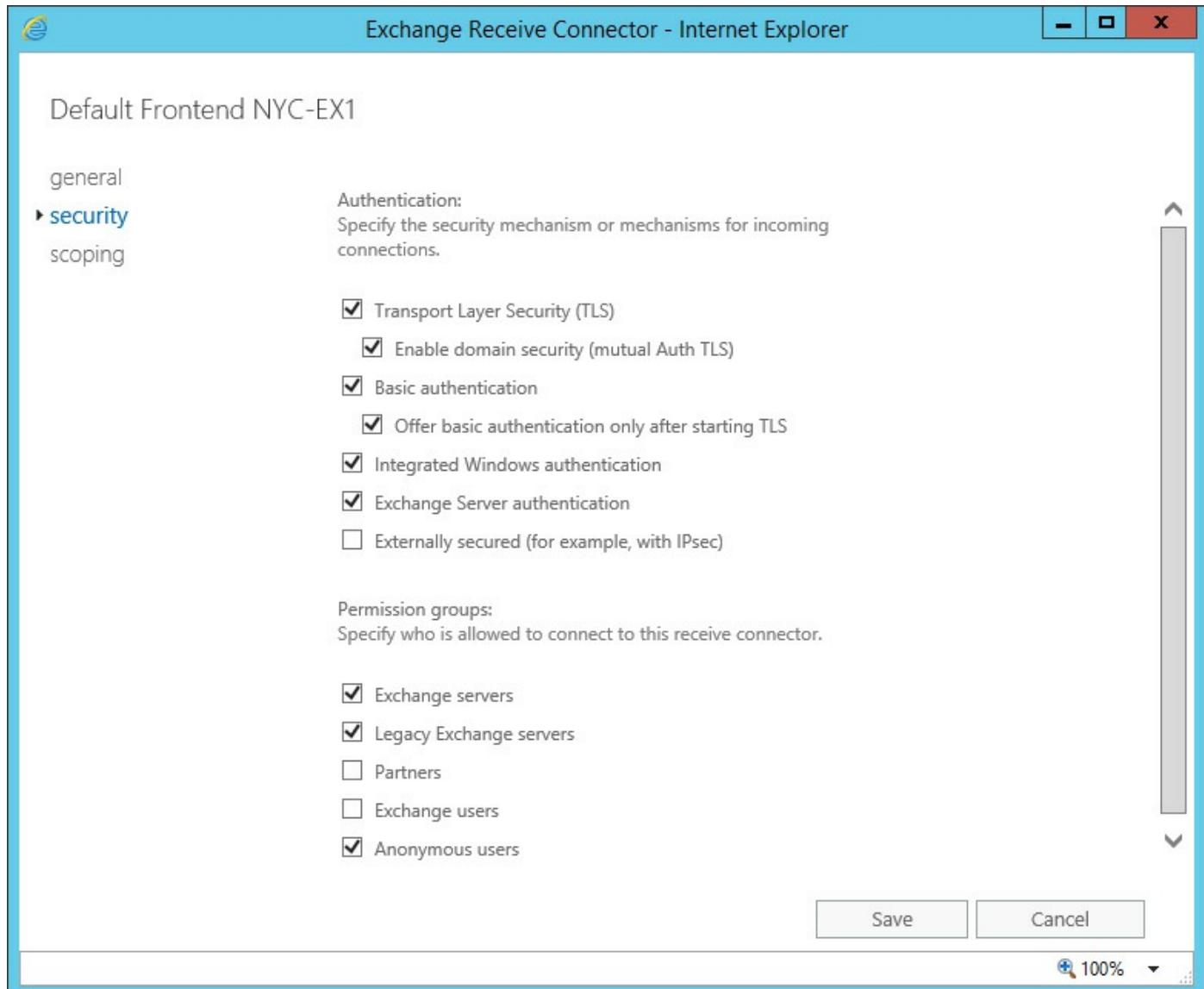
- **You have three sites with only Site 1 configured to send and receive email with the Internet** If Site 1 is down, you need to configure servers in one of the other sites to send and receive email with the Internet. In such a case, you can create the same send and receive connectors that you had in Site 1, albeit with different IP addresses.
- **You have multiple sites** You configure an Exchange server at each site to serve as an SMTP server, or relay server, for applications. The Exchange server in one site goes down, but the applications still need to relay email. You need to configure a receive connector, and possibly a send connector, to enable the applications to relay through a second site. While you might normally set this up ahead of time, the exam item writers craft up environments unlike your environment in order to test specific concepts.

Part of your exam preparation should be looking at the connectors in Exchange and becoming familiar with the roles they play. There are several default receive connectors in Exchange Server 2016, as outlined in [Table 3-4](#).

Name	Description	TCP Port Number	Permission groups	Serve Type
Client Frontend	Accepts connections from authenticated SMTP clients	587	ExchangeUsers	Front End Transport service on Mailbox servers
Default Frontend	Accepts anonymous connections from SMTP servers and is the most commonly used connector.	25	AnonymousUsers ExchangeLegacyServers ExchangeServers	Front End Transport service on Mailbox servers
Outbound Proxy	Accepts authenticated connections from the Transport service on Mailbox servers.	717	ExchangeServers	Front End Transport service on Mailbox servers
Client Proxy	Accepts authenticated client connections that are proxied from the Front End Transport service.	465	ExchangeServers ExchangeUsers	Transport server on Mailbox servers
Default	Accepts connections from: <ul style="list-style-type: none"><li>■ Front End Transport service</li><li>■ Transport service on remote Mailbox servers</li><li>■ Mailbox transport service</li><li>■ Edge transport servers</li></ul>	2525	ExchangeServers ExchangeUsers ExchangeLegacyServers	Transport server on Mailbox servers
Default internal receive connector	Accepts anonymous connections from external SMTP servers	25	AnonymousUsers ExchangeServers Partners	Transport service Edge Transport server
Mailbox delivery receive connector (Implicit)	Accepts authenticated connections from the Transport service	475	ExchangeServers	Mailbox Transport Delivery service on Mailbox servers

TABLE 3-4 Default receive connectors

By default, the Default Frontend receive connector accepts email messages from any remote IPv4 or IPv6 network, including from anonymous users. Therefore, site resiliency can primarily be handled by using MX records as previously discussed in this section. [Figure 3-22](#) shows the default security options for the Default Frontend NYC-EX1 receive connector.



**FIGURE 3-22** Exchange Receive Connector settings

For internal applications that connect directly to an Exchange server rather than use MX records, it is a good practice to configure the application to use an alias, or CNAME record, that points to a transport server, or an A record that points to multiple transport servers for DNS round robin.

## Test and perform steps for transport failover and switchover

For incoming connections to an Exchange environment, there are several options that can assist in redirecting that traffic to another server, including MX records or a load balancer with Managed Availability. This section covers transport failover and switchovers. First, let's define the two terms:

- **Failover** A failover refers to an unexpected scenario that causes unavailability of services or data. A failover requires activating a passive mailbox database to make it the active database. If a mailbox server cannot be found that can activate

the database, the database is dismounted.

- **Switchover** A switchover refers to a scheduled or planned move of an active database from one Exchange server to another in the same DAG. If another Mailbox server in the DAG cannot be loaded to host the database, the administrator receives an error. The database is still active and mounted on the original server.

## Failovers

Failovers can occur for a variety of reasons. A failover can have an impact on a single database, a server, or an entire datacenter. A common occurrence for a database failure is a loss of storage access, whereas a server or datacenter might lose power. By using DAGs and mailbox database copies, you can provide redundancy and recovery of both data and services for an Exchange organization.

When a database failover occurs, the following high-level steps are taken:

1. The Exchange Information Store service detects that a database is unavailable.
2. The Exchange Information Store writes failure events to the channel event log.
3. The Active Manager on the Exchange server detects the events and requests the status of the database from other Mailbox servers.
4. The other Mailbox servers return the status to the Active Manager.
5. The primary Active Manager begins moving the active database to another server in the DAG, and updates the database mount location in the cluster database.
6. The primary Active Manager changes to the new server to become the database master.
7. The newly selected database master uses the Exchange Replication service to copy the logs from the failed server. It also sets the mountable attribute for the database.
8. The Active Manager reads the maximum log generation number from the cluster database, and then mounts the new active database copy.

When a server failover occurs, the following actions are taken:

1. The Active Manager notifies the cluster service that a node is down or the MAPI network is down.
2. If the affected server is reachable, a notification is sent to immediately dismount the active database. For each database on the server, the following actions are taken:
  - A. The status of each database is requested and sent.
  - B. The best log source is selected from the servers that respond.

- C. Each server responds with the log generation number.
- D. The Active Manager retrieves the search index catalog status. Using the catalog status and log generation number, a new server is selected to activate the database.
- E. The active database location is set in the cluster database and a failover notification is sent to other servers.
- F. The Exchange Replication service is used to copy the most recent logs to the new server and set the mountable flag.
- G. The database is mounted on the new server.

## Switchovers

As with failovers, switchovers can occur for a database, server, or datacenter. Switchovers follow a different process because all server communication and functionality is expected to be working. A database switchover uses the following high-level steps:

1. An administrator begins the process to move the active database. The client that is being used makes an RPC call to the Exchange Replication services on a DAG member.
2. The DAG member refers the client to the Active Manager, and then the client initiates a session with the Exchange Replication service on that server.
3. The Active Manager reads and updates the database location in the cluster database, and contacts the new server.
4. The Exchange Replication service queries the DAG members to ascertain the best log source. The database is dismounted from the current server and logs are replicated to the new server.
5. The Exchange Replication service mounts the database on the new server and replays the log files.
6. The Active Manager queries the database status for the DAG and any error codes are reported to the administrator.

Server switchovers follow the same process as individual databases but are repeated for each database on the server.

### Need More Review? Switchovers and Failovers

To view a detailed process for each of these steps, or for more information on how to perform a switchover, see  
[https://technet.microsoft.com/library/dd298067\(v=exchg.150\).aspx](https://technet.microsoft.com/library/dd298067(v=exchg.150).aspx).

## Summary

- Address (A) records are used to define MX records in DNS.
- You can customize the retry attempts, resubmit attempts, and expirations settings for email messages.
- Exchange, by default, is configured to accept email from any remote IP address including from anonymous users.
- A failover is an unexpected failure of a server or other component in your environment that causes a server to become unavailable. A switchover is a planned cutover from one server or datacenter to another server or datacenter.

## Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find the answer to this thought experiment in the next section.

You are a systems administrator for Alpine Ski House, a luxury mountain sports provider with mountain lodging, recreational activities, and special events facilities and services. The company's primary location is in Jackson, Wyoming. Other locations are in Whistler, British Columbia, Canada, Vail, Colorado and Salt Lake City, Utah. Each location has a datacenter. The existing AD DS environment has site links with the default costs. The company uses a legacy third-party email system to provide email to the company. The company is planning to migrate to an on-premises Exchange Server 2016 environment. Currently, the company is in the planning stages.

You've met with the rest of the IT team and the management team and have identified the following concerns with the existing legacy email system:

- While the legacy email system has two servers in the Jackson, Wyoming datacenter, the datacenter lost power once during the year and the company lost email.
- The existing email system does not allow secure email communications with an Alpine Ski House supplier named Fabrikam, Inc.
- Due to the remoteness of the company's locations, all sites are only able to communicate directly with two other sites.

The management team has come up with the following requirements for the on-premises deployment:

- To meet security and compliance requirements, all email must flow through an email server in Jackson, Wyoming where the company maintains a third-party compliance system that scans all email messages. The only exception is in the case of a site outage.
- Secure email communication must be enabled for all email sent between Alpine

## Ski House and Fabrikam, Inc.

- Inbound email from the Internet must provide for site resilience so that in the event of a datacenter power outage, email is received at a secondary site.

You need to plan for a solution to meet the requirements. What should you do?

## Thought experiment answer

This section contains the solution to the thought experiment. While there are often multiple ways to meet requirements, read the solution to understand the thought process behind the answers.

To meet the security and compliance requirements, you should configure the Jackson, Wyoming site to be a hub site. Hub sites, when they are in the shortest path between a sender and the destination, receive and process all email.

To meet the secure email communication requirement between Alpine Ski House and Fabrikam, Inc., you should implement Domain Security. Domain Security, also known as mutual TLS, enables the organizations' servers to communicate securely. As part of the setup, you need to ensure that the organizations use certificates issued by trusted root CAs.

To meet the requirement of providing site resiliency for inbound email from the Internet, you should deploy Edge Transport servers to at least two sites and set up at least two MX records. One MX record, the primary record, should have a preference of 10 and point to the Jackson, Wyoming location because all email must flow through Jackson, Wyoming per the first requirement. A second MX record should have a preference of 20, or any number larger than 10, and point to a secondary site, such as the Salt Lake City site, or wherever you place the other Edge Transport servers.

# **Chapter 4. Plan, deploy, and manage Exchange infrastructure, recipients, and security**

As an email administrator, you routinely work with technologies directly related to email, such as recipients, distribution groups, and connectivity. However, you also need to know about closely related technologies that Exchange Server requires or that enhance the functionality of Exchange Server. For example, you need to have a solid understanding of Active Directory including how the site topology impacts email transport. Additionally, you need to be familiar with security-related settings and technologies such as digital rights management with Active Directory Rights Management Service and Azure Rights Management Services. This chapter discusses the integration of Exchange and Active Directory, mail-enabled objects, working with permissions, security, and digital rights management.

## **Skills in this chapter:**

- [Plan and configure Active Directory \(AD\) Domain Services for Exchange and Organizational settings](#)
- [Create and configure mail-enabled objects](#)
- [Manage mail-enabled object permissions](#)
- [Plan, deploy, manage, and troubleshoot Role Based Access Control \(RBAC\)](#)
- [Plan an appropriate security strategy](#)
- [Plan, deploy, manage, and troubleshoot IRM with Active Directory Rights Management Services \(AD RMS\) or Azure RMS](#)

### **Skill 4.1: Plan and configure Active Directory Domain Services for Exchange and Organizational settings**

Exchange Server stores all of its configuration information and recipient information in Active Directory. The Active Directory schema is extended to support the storing of Exchange-related information. Active Directory and Exchange Server are tightly integrated and Exchange Server has dependencies on Active Directory. You need to be intimately familiar with the requirements, planning concepts, and implementation tasks to prepare an Active Directory environment for Exchange Server.

## This section covers how to:

- [Plan the number of domain controllers](#)
- [Plan placement of Global Catalog](#)
- [Plan and configure DNS changes required for Exchange](#)
- [Plan for schema changes required for Exchange](#)
- [Prepare AD for Exchange](#)
- [Prepare domains for Exchange](#)
- [Plan and configure Active Directory site topology](#)

## Plan the number of domain controllers

In many environments, especially large environments, there is one team that manages Active Directory and/or directory services and another team that manages Exchange Server. Ultimately, the directory services team is responsible for providing Active Directory services to the company and all of the applications that depend on it. As an Exchange administrator, your primary goal in planning for the number of domain controllers is ensuring that the environment meets the minimum requirements along with the requirements you have for performance and availability. The following key factors should be considered when planning the number of domain controllers:

- **Read-only domain controllers (RODCs) are not used by Exchange Server** If you have RODCs in your environment, you should not count them as domain controllers for Exchange. Thus, you might need to add a read-write domain controller (RWDC) to a site to meet your requirements.
- **Exchange Server uses Global Catalog servers** If you have domain controllers that aren't also Global Catalog servers, you should not count them as domain controllers for Exchange. You can also plan to configure them as Global Catalog servers instead.
- **Exchange Server doesn't require the use of same-site domain controllers** If you want to maximize overall performance, you should use Global Catalog servers in every site where you have Exchange Server.
- **You should have one Global Catalog processor core for every eight Exchange Server processor cores** For example, if you have two Exchange servers and they each have two 8-core processors, you should have at least four Global Catalog processor cores.

The diagram in [Figure 4-1](#) shows a fictitious company's site layout of their existing domain controllers.

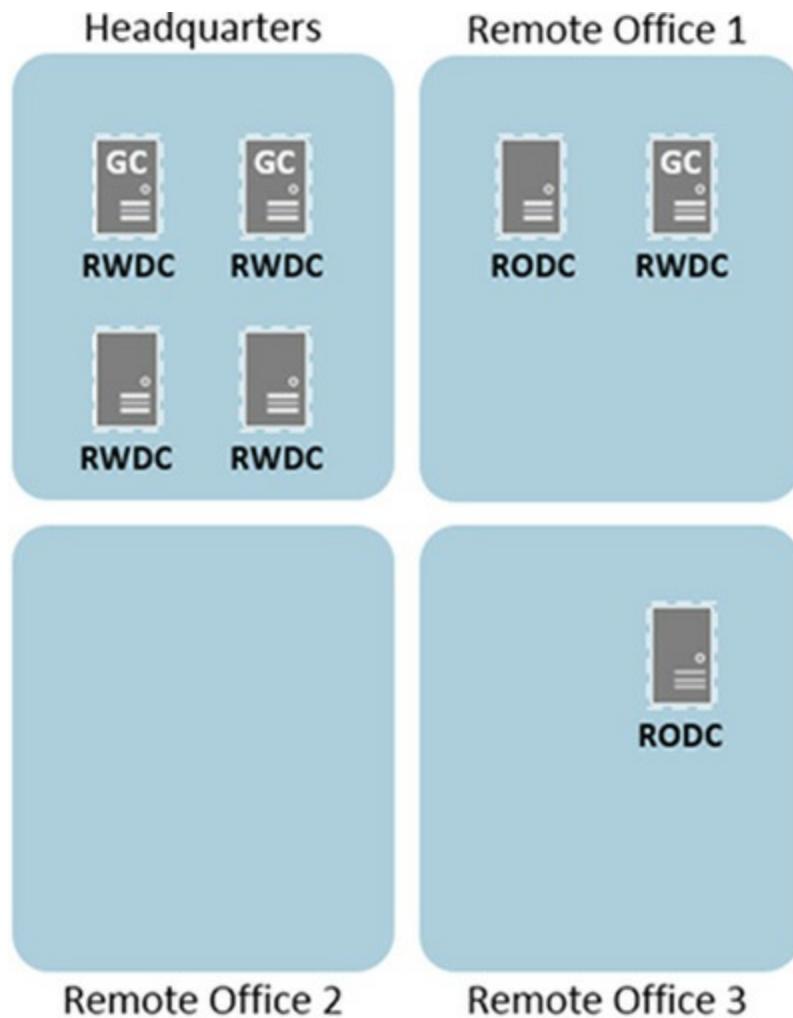


FIGURE 4-1 Company sites and the domain controllers in each site

Imagine that you are the Exchange Server administrator for the fictitious company whose sites are shown in [Figure 4-1](#). For the purposes of this walk-through, let's say that every domain controller has a single dual-core processor. The new Exchange servers have dual 8-core processors. You want to deploy Exchange Server and have two servers in each site. Which changes would you recommend for the domain controller layout? Some options for each site are as follows:

- **Headquarters site** The headquarters site has four RWDCs right now. Two of them are Global Catalog servers. Because each has a single quad-core processor, the headquarters site has four Global Catalog processor cores. The two Exchange servers have a total of 32 processor cores. From a processor core perspective, the headquarters site is OK as is, just meeting the minimum requirement. Thinking about high availability, having two Global Catalog servers in the site is sufficient. Thus, the headquarters site does not require any changes to support the deployment of Exchange Server.
- **Remote Office 1** The Remote Office 1 site has one RODC and one RWDC. The RWDC is a Global Catalog server. There are two Global Catalog processor cores

total. The two Exchange servers have a total of 32 processor cores. From a processor core perspective, the Remote Office 1 site does not meet the recommendation of having at least one Global Catalog process core for every eight Exchange Server processor cores. Additionally, from a high availability perspective, the site isn't highly available for Global Catalog services. If the RWDC becomes unavailable, Exchange Server must rely on Global Catalog services in a remote site, which impacts performance. In this scenario, you can replace the RODC with an RWDC that is also a Global Catalog server, or you can add a third server and make it an RWDC that is also a Global Catalog server.

- **Remote Office 2** There aren't any domain controllers in Remote Office 2. At a minimum, you should add two Global Catalog servers and at least four Global Catalog processor cores. You can provide high availability within the site for Global Catalog servers by having at least two servers.
  - **Remote Office 3** There is a single RODC in Remote Office 3, but RODCs are not used by Exchange Server. So effectively, Remote Office 3 is similar to Remote Office 2. The solution is also the same. You can deploy two new Global Catalog servers with at least a total of four Global Catalog processor cores. You can also opt to switch the RODC for an RWDC with Global Catalog and deploy one other Global Catalog server.
- 



### Exam Tip

Microsoft recommends one Global Catalog processor core for every eight Exchange Server Mailbox processor cores. This recommendation is not a prerequisite or a requirement and is specific to 64-bit processors. For 32-bit processors, the ratio is 1:4.

---

One final thought about Global Catalog servers. Exchange Server isn't the only application that relies on Global Catalog servers. Thus, as part of your planning work, you should factor in other applications that rely on the Global Catalog servers. If there are several other applications that rely on them, you might need to deploy more Global Catalog servers or processor cores than the minimum recommended for Exchange Server.

## Plan placement of Global Catalog

In addition to knowing how many Global Catalog servers you need for a given scenario, you also need to know in which datacenters to place them. The previous section covers some of that placement information. Instead of repeating that here, this section walks through the remaining Global Catalog placement information. The following placement information is important to know for the exam:

- **You might need Global Catalog servers from multiple domains** In a multi-domain forest, you often want to have Global Catalog servers from each domain in sites where Exchange Server is deployed.
- **In large organizations, you might need dedicated AD DS sites for Exchange** When you have substantial demand for Global Catalog services, you might need to use dedicated Active Directory Domain Services (AD DS) sites with dedicated Global Catalog servers for your Exchange environment.
- **If you have LAN connectivity and low latency, you might be able to get by without local Global Catalog servers** It is a good practice to have local Global Catalog servers wherever you have Exchange servers. In situations where that isn't feasible, you can use sites that are well connected, sites that have LAN connectivity and low latency.

## Plan and configure DNS changes required for Exchange

For this area of the exam skills, DNS changes are focused on the changes required to successfully deploy a new Exchange Server environment. The DNS changes required for the flow of email and for anti-spam are covered in [Chapter 3](#). For this exam skill, you should be familiar with the different DNS configurations supported by Exchange Server:

- **Contiguous** The vast majority of domains in use today are contiguous. Contiguous domains share the same root domain name. For example, you might have alpineskihouse.com as your forest root domain, and you might have corp.alpineskihouse.com and partner.alpineskihouse.com as child domains. Because all of these domains share the forest root domain name, the namespace is contiguous.
- **Noncontiguous** When you have a forest that uses unrelated domain names, you have a noncontiguous namespace. For example, imagine you have fabrikam.com as your forest root domain. Under that domain, you have tailspintoys.com and wingtiptoys.com. That is a noncontiguous namespace. It is more complex than a contiguous namespace and takes more administrative overhead to manage and maintain. In this configuration, you need to edit the msDS-AllowedDNSSuffixes attribute for the domain object in Active Directory. All of your DNS suffixes must

be added to the attribute.

- **Single label domains** A standard domain name has two parts: the top level portion to the right of the period and the name to the left of the period, for example, alpineskihouse.com. In a single label domain, there isn't a top level portion. In the example domain, the single-label version would be just ALPINESKIHOUSE. Starting with Windows Server 2008 R2, you cannot create a new Active Directory domain with a single-label name. One good option to consider is migrating to a new domain based on a standard DNS domain name.
- **Disjoint namespace** When domain-joined computers use a DNS suffix that does not match the domain they are joined to, a disjoint namespace occurs. For example, imagine that you have the alpineskihouse.com domain. It is the forest root domain. A child domain, named corp.alpineskihouse.com, is the primary domain for computers and services. Some computers have a DNS suffix of alpineskihouse.com even though they are joined to the corp.alpineskihouse.com domain. That is a disjoint namespace. You need to edit the msDS-AllowedDNSSuffixes attribute for the domain object in Active Directory. Both of your DNS suffixes must be added to the attribute. By default, the attribute is empty. Lastly, it is a good practice to use a Group Policy Object (GPO) to configure the suffix search order to include all of your domains.

The key point for DNS changes is that Exchange Server needs to be able to efficiently resolve DNS names across your entire environment. Otherwise, there are email flow problems. Clients also need to be able to resolve DNS names across your entire environment.

## Plan for schema changes required for Exchange

A prerequisite for installing Exchange Server 2016 is an AD DS schema that has been prepared for Exchange Server 2016. Exchange Server 2016, like previous versions of Exchange Server, requires a schema extension. The schema extension adds and updates objects in AD DS to support the storage of Exchange configuration information and recipient information.

As part of the preparation for the schema changes, you need to consider the two options for updating the schema:

- **Use the Exchange 2016 Setup Wizard** During the installation of your first Exchange 2016 server, the setup wizard can perform all of the necessary changes to your Active Directory environment. This makes the process quick and easy. The only requirement is that the account you use to install Exchange Server 2016 is a member of the Enterprise Admins group and the Schema Admins group. There are some downsides to using the setup wizard to perform the schema changes. First, if

you have a team that manages Active Directory, they often want to perform all schema updates. Second, if you work for an organization that strives to minimize the number of changes in a single night or change control window, the manual approach might be better because you can split all of the work across a few different days or change control windows.

- **Manually update the schema** If you have one team that manages Exchange and a separate team that manages Active Directory, the option to manually update the schema is usually the best choice. It enables the Active Directory team to own and manage the schema update while enabling the Exchange team to manage Exchange Server. It also enables you to methodically go through the schema changes one by one. You can individually validate each step of the process and allow the schema changes to be taken care of several days before the first Exchange server is installed.

In the next section, you walk through the detailed process of preparing Active Directory with the schema changes.

## Prepare AD for Exchange

While this section of the exam is mostly focused on the schema updates, you should also be aware of a general requirement to support Exchange Server 2016. First, the AD DS forest functional level must be Windows Server 2008 or higher. Thus, all domain controllers must run Windows Server 2008 or later.

To meet the schema requirements for Exchange Server 2016, you need to perform the following high-level steps, in order:

1. **Extend the schema** This is the initial schema preparation.
2. **Prepare Active Directory** This is the step when Active Directory is updated with containers and objects, and when the Exchange organization is created, if you don't currently have Exchange in the environment.
3. Prepare domains. This step occurs only when you have more than one domain. If you just have one domain, the preparation of Active Directory takes care of preparing the domain. The details of this step are covered in the next section.



## Exam Tip

Pay close attention to the group membership requirements. You need to be a member of the Enterprise Admins group and Schema Admins group to extend the schema. For preparing Active Directory and for additional domain preparation, you only need to be a member of the Enterprise Admins group. Watch out for references to the Domain Admins group because such references are almost certainly wrong.

## Prepare the schema for Exchange

Before you begin the schema preparation process, make sure that your account is a member of the Enterprise Admins group and the Schema Admins group. Then, perform the following steps:

1. Copy the Exchange Server 2016 installation files to the computer you are using to extend the schema.
2. Open an elevated command prompt and navigate to the location of the Exchange Server 2016 installation files.
3. Run the `Setup.exe /PrepareSchema /IAcceptExchangeServerLicenseTerms` command. Note that this command must be run once per forest.
4. Wait for AD DS replication to complete. Optionally, if you need to speed up the process, you can manually force replication.

## Prepare Active Directory

After you prepare the schema, you are ready to prepare Active Directory. For this step, you must be a member of the Enterprise Admins group. Perform the following steps:

1. Copy the Exchange Server 2016 installation files to the computer you are using to extend the schema.
2. Open an elevated command prompt and navigate to the location of the Exchange Server 2016 installation files.
3. Run the `Setup.exe /PrepareAD /OrganizationName:<organization name> /IAcceptExchangeServerLicenseTerms` command. Note that this command assumes you have a single-domain forest. If you have more than one domain, you need to specify the domain name as part of the command.
4. Wait for AD DS replication to complete. Optionally, if you need to speed up the

process, you can manually force replication.

## Prepare domains for Exchange

If you have a single-domain forest, you don't need to prepare any additional domains. Your work is done after you perform the steps in the previous section to prepare Active Directory. If you have a multi-domain forest and plan to use the domains for mail-enabled objects, you need to prepare all of the domains, but only if at least one of the following statements is true:

- You plan to install an Exchange server in the domain.
- You plan to have mail-enabled users in the domain.

At this point, you can prepare one domain at a time or you can prepare all additional domains in one command. To prepare all additional domains in one command, run the following command:

[Click here to view code image](#)

```
Setup.exe /PrepareAllDomains /IacceptExchangeServerLicenseTerms
```



### Exam Tip

Watch for questions about preparing Active Directory because there are some key details that are tough to remember. Be sure to know that you must name the Exchange organization as part of the Active Directory preparation. Compare the command to prepare Active Directory and the command to prepare additional domains and be sure to know the difference for the exam.

## Plan and configure Active Directory site topology

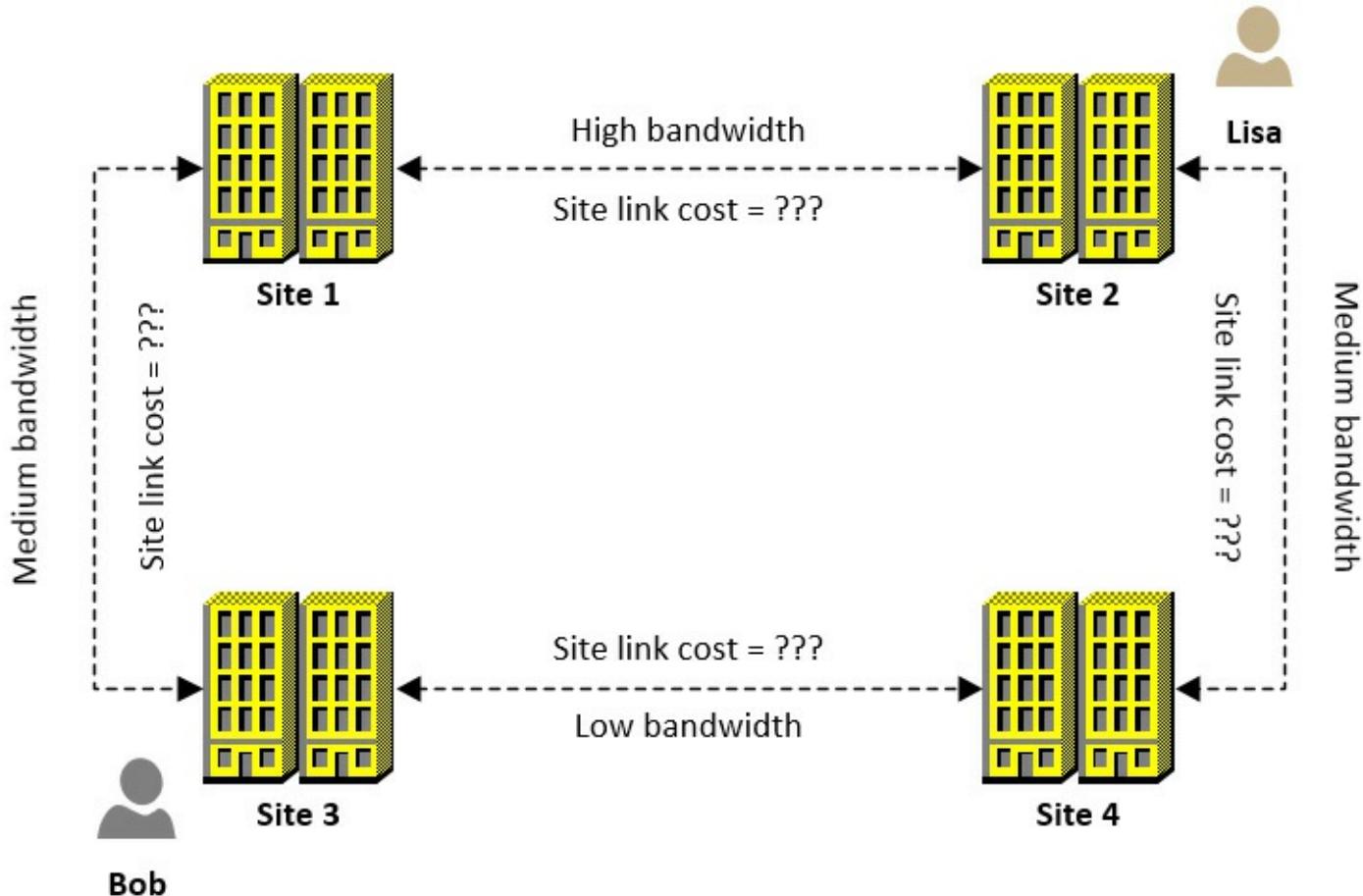
If you have an existing Exchange environment and you are planning to put Exchange Server 2016 servers in the same sites as existing servers, you might not need to change your Active Directory site topology. If you do not currently have Exchange in your environment or plan to change the sites that have Exchange servers, you might have to update your Active Directory site topology.

When you have Exchange servers in multiple sites, Exchange Server uses the site topology to figure out how to route email to other sites. [Chapter 3](#) covers email routing and looks at internal email flow. Here is a quick recap of key facts:

- **Exchange Server evaluates the potential routes from one site to another site**  
The path with the lowest total site link cost is used to route email.

- A hub site, when on the lowest cost path, always processes email A hub site is often used for compliance and security scans. Hub sites are optional.

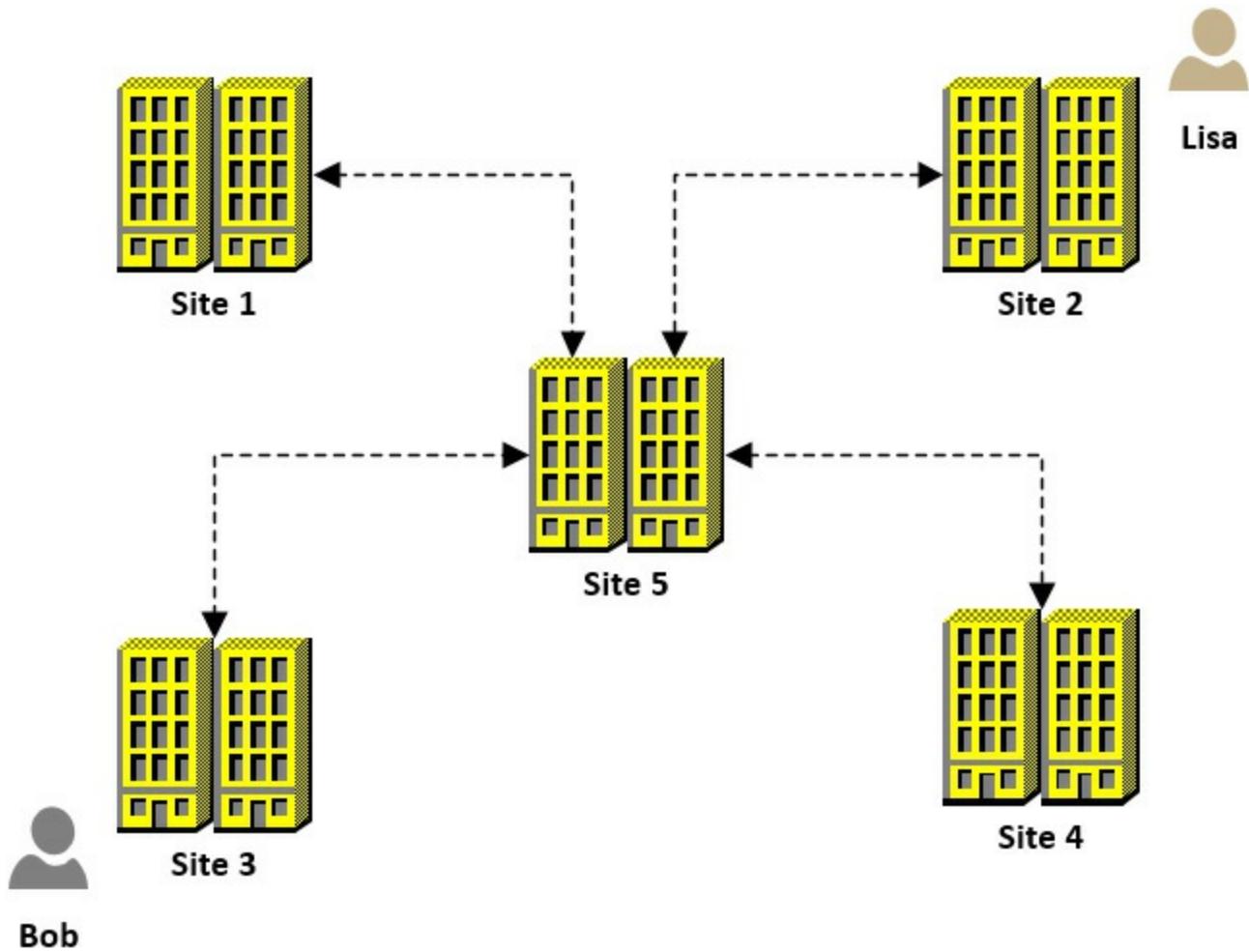
In this section, look at the following scenarios and work through planning and configuring site topologies. In this first scenario, you are planning to configure the site link costs for the site links shown in [Figure 4-2](#).



**FIGURE 4-2** An Active Directory site topology without the site link costs

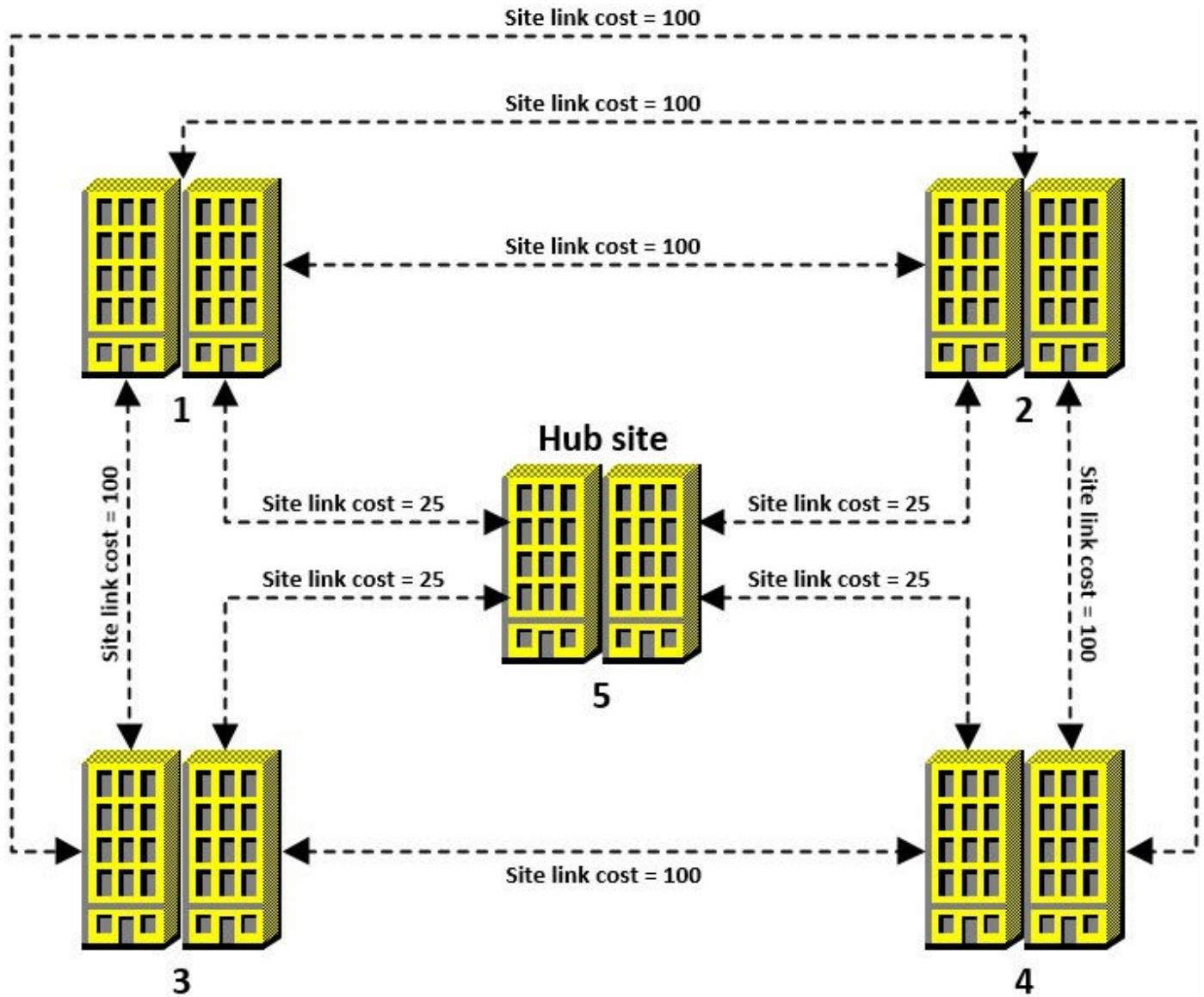
Look at the diagram in [Figure 4-2](#). If you wanted all email messages from Bob to Lisa to be processed by an Exchange server in Site 1, what would you do? If your answer is to configure Site 1 to be a hub site and adjust the site link costs so the total cost of the site links between Site 3/Site 1/Site 2 is lower than between Site 3/Site 4/Site 2, you are right!

Let's look at another scenario, shown in [Figure 4-3](#).



**FIGURE 4-3** An Active Directory site topology using a hub and spoke model

In [Figure 4-3](#), you have a hub and spoke topology. Site 5 is the headquarters location. All network connectivity between all of the sites goes through Site 5. Exchange servers are in every site. The management team asks that you have all email between all of the sites processed for compliance by a server in Site 5. What should you do? If you answered that you don't have to do anything since all network connectivity already goes through Site 5, you didn't get the question correct. That's because a server in Site 5 only processes email if Site 5 is a hub site and is in the shortest path. If you answered that you need to configure Site 5 to be a hub site, you got it right! Imagine instead that the network connectivity was a mesh network. All sites have direct connectivity to all other sites. Management still wants all email to be processed for compliance by a server in Site 5. You configure Site 5 as a hub site. What else do you need to do? You need to configure the site links so that the lowest cost path to other sites is through Site 5. [Figure 4-4](#) shows one way of doing this.



**FIGURE 4-4** An Active Directory site topology with a mesh network, a hub site, and site link costs

In [Figure 4-4](#), a mesh network is shown with each site being labeled as 1 for Site 1, 2 for Site 2, 3 for Site 3, 4 for Site 4, and 5 for Site 5 the headquarters site. Because the management team asked for all email between sites to be processed by a server in Site 5, you configured Site 5 as a hub site. Additionally, you must configure the site link costs so that the lowest cost path to all other sites goes through Site 5. You can use any costs that you want for the site links. The costs must be lowest through Site 5 so that the hub site is used and email is processed by a server in Site 5. Look through the costs in [Figure 4-4](#). For example, note that Site 3 has direct connectivity to Site 4 with a site link cost of 100. The path through Site 5 however, costs a total of 50, with the Site 3 to Site 5 cost at 25 and the Site 5 to Site 4 cost also at 25. Thus, Exchange uses that path as it is the lowest cost path.

## Plan and configure throttling policies

Imagine you have a user that is consuming excessive amounts of your Exchange server resources, such as CPU or Exchange database activities. The user is consuming so much that the user experience for other users is degraded. This isn't a good situation to be in. To avoid that, you can use throttling policies. Throttling policies minimize the chances of one or two users degrading the experience of other users by consuming excessive resources. Exchange Server 2016 has one default throttling policy named `GlobalThrottlingPolicy`. It applies globally to all users. When you want to customize the throttling settings, you should create new policies that have different settings than the default. Exchange Server 2016 provides the following controls for throttling:

- **Throttle a user for a short period of time** While a user is throttled, he or she can still use Exchange services. The performance is slightly reduced however. Often, users do not realize that they are being throttled because the performance remains adequate.
- **Temporarily block a user from using any resources** If a user reaches the maximum usage threshold, he or she is temporarily blocked from using Exchange services. You can configure the amount of time before a blocked user is unblocked by setting the recharge rate.
- **Create a throttling policy for a single user, a group of users, or all users** There is a default global policy that applies to all users. You can create a new global policy to apply to all users or you can create a scoped policy and associate one or more users to the policy.
- **Create a throttling policy for a single Exchange service** For example, you can create a policy for Outlook on the web or a policy for IMAP. You can define many parameters for each service and policy.

The following PowerShell examples show the throttling-related cmdlets and common commands for configuring throttling.

In the following command, you create a new throttling policy that applies to all users, existing and future. The policy limits concurrent Outlook on the web connections to five. The default is three.

[Click here to view code image](#)

```
New-ThrottlingPolicy -Name OWAConcurrency -OwaMaxConcurrency 5 -  
ThrottlingPolicyScope  
Organization
```

In the following command, an existing throttling policy named `PowerShellCmdlets` is adjusted so the maximum number of cmdlets that can be run in a 60 second period is 10.

[Click here to view code image](#)

```
Set-ThrottlingPolicy PowerShellCmdlets -PowerShellMaxCmdlets 10  
-PowerShellMaxCmdletsTimePeriod 60
```

## Need More Review? New-ThrottlingPolicy Cmdlet

For more information on throttling, see [https://technet.microsoft.com/en-us/library/jj150503\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj150503(v=exchg.150).aspx). For more information on the New-ThrottlingPolicy cmdlet, see [https://technet.microsoft.com/en-us/library/dd351045\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd351045(v=exchg.150).aspx).

## Summary

- RODCs are not used by Exchange Server, so you should not account for them when you plan your domain controller layout.
- You should have one Global Catalog processor core for every eight Exchange Server processor cores.
- You can use the Exchange Server 2016 setup program to update the Active Directory schema.
- You must prepare all Active Domains for Exchange if you install Exchange servers in the domain or have mail-enabled users in the domain.
- You can use custom throttling policies to ensure that users do not consume excessive resources on the Exchange servers.

## Skill 4.2: Create and configure mail-enabled objects

As an email administrator, you regularly create and configure new objects such as mailboxes, contacts, and distribution lists. For the exam, you need to be familiar with the process of creating and configuring mailboxes, contacts, and distribution lists. You must also be familiar with the different types of mailboxes, such as standard user mailboxes, resource mailboxes, shared mailboxes, and linked mailboxes. Plan to be familiar with PowerShell for these tasks too.

---

## This section covers how to:

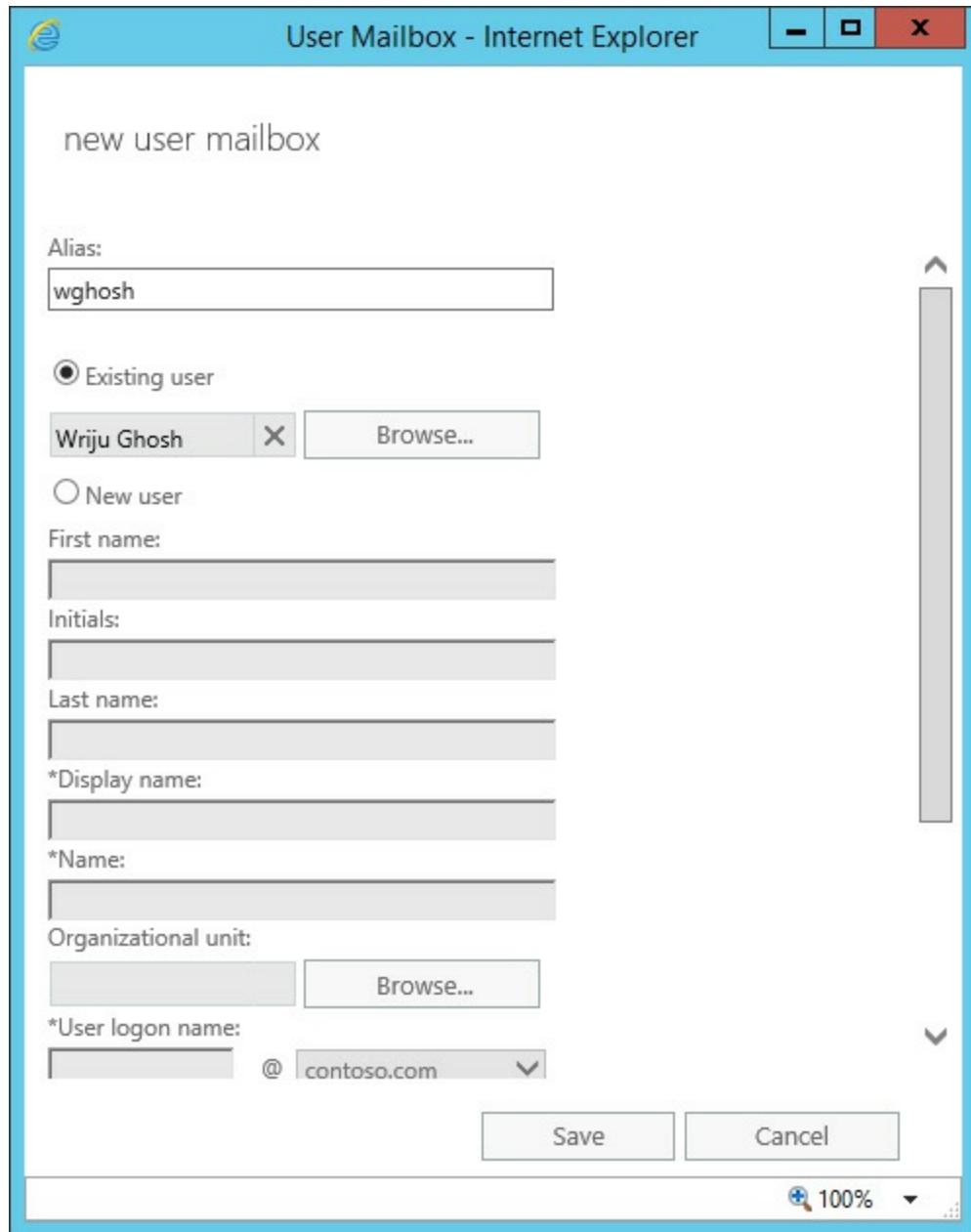
- [Create and configure mailboxes](#)
  - [Create and configure resource mailboxes and scheduling](#)
  - [Create and configure shared mailboxes](#)
  - [Create and configure mail-enabled users and contacts](#)
  - [Create and configure distribution lists](#)
  - [Configure moderation](#)
  - [Create and configure modern public folders](#)
- 

## Create and configure mailboxes

For the purposes of the exam, this section covers standard mailboxes such as a mailbox that you create for a user. Other mailboxes are covered in upcoming sections. There are two primary ways to create mailboxes, through Exchange Admin Center (EAC) and Exchange Management Shell (EMS).

To have a mailbox, you must have an Active Directory user account. In many environments, mailboxes are created after Active Directory user accounts. Often, the team that manages Active Directory is responsible for creating user accounts. A different team that manages Exchange Server, creates mailboxes.

To create a mailbox in the EAC for an existing user account, navigate to the recipient's workspace in the EAC, click the new object dropdown menu which is displayed with a plus symbol icon, and then click the user mailbox option. From there, you can give the user an alias and browse to the existing user account. Then, you can save the changes to create the mailbox. [Figure 4-5](#) shows the process of creating a mailbox for an existing user named Wriju Ghosh.



**FIGURE 4-5** A new user mailbox being created in the EAC

To create a new mailbox for an existing user named Brian Svidergol by using PowerShell, run the following command:

[Click here to view code image](#)

```
Enable-Mailbox -Identity "Brian Svidergol"
```

[Figure 4-6](#) shows the output of the command.

```

Machine: LON-EX1.Adatum.com
[PS] C:\>Enable-Mailbox -Identity "Brian Svidergol"
Name          Alias        ServerName   ProhibitSendQuota
----          ----        -----       -----
Brian Svidergol  bsvidergol  lon-ex1    Unlimited
[PS] C:\>_

```

**FIGURE 4-6** A new user mailbox being created in PowerShell

Notice how a mailbox database does not have to be specified in the command or in the EAC? This is because Exchange Server has a feature that automatically distributes mailboxes randomly across mailbox databases. Optionally, you can specify a database in PowerShell by using the **Database** parameter.

Beyond creating mailboxes, you also need to be familiar with configuring mailboxes. You can configure mailboxes during creation, for example by specifying the database to house the mailbox, or you can configure mailboxes after creation. The subsequent commands show some common mailbox configuration tasks.

The following command configures Wriju's mailbox so that it does not use an email address policy:

[Click here to view code image](#)

```
Set-Mailbox -Identity "Wriju Ghosh" -EmailAddressPolicyEnabled $False
```

The following command configures Wriju's primary SMTP address to be [wriju@adatum.com](mailto:wriju@adatum.com):

[Click here to view code image](#)

```
Set-Mailbox -Identity "Wriju Ghosh" -PrimarySmtpAddress wriju@adatum.com
```

The following command configures Wriju's mailbox for litigation hold:

[Click here to view code image](#)

```
Set-Mailbox -Identity "Wriju Ghosh" -LitigationHoldEnabled $True
```

### Need More Review? Set-Mailbox Cmdlet

For more information on the Set-Mailbox cmdlet, including the full syntax and list of parameters, see [https://technet.microsoft.com/en-us/library/bb123981\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/bb123981(v=exchg.160).aspx).

As part of your exam preparation, run through some of these tasks to create and configure mailboxes. This helps you remember cmdlets and parameters that are likely to appear on the exam.



## Exam Tip

Beware of the New-Mailbox cmdlet. It might appear to be the correct cmdlet to establish a new mailbox for an existing user, but it isn't. It is used to create a new Active Directory user and a mailbox in the same command. For example, to create a new Active Directory user account and mailbox for a user named Wriju Ghosh, you can run the following commands:

[Click here to view code image](#)

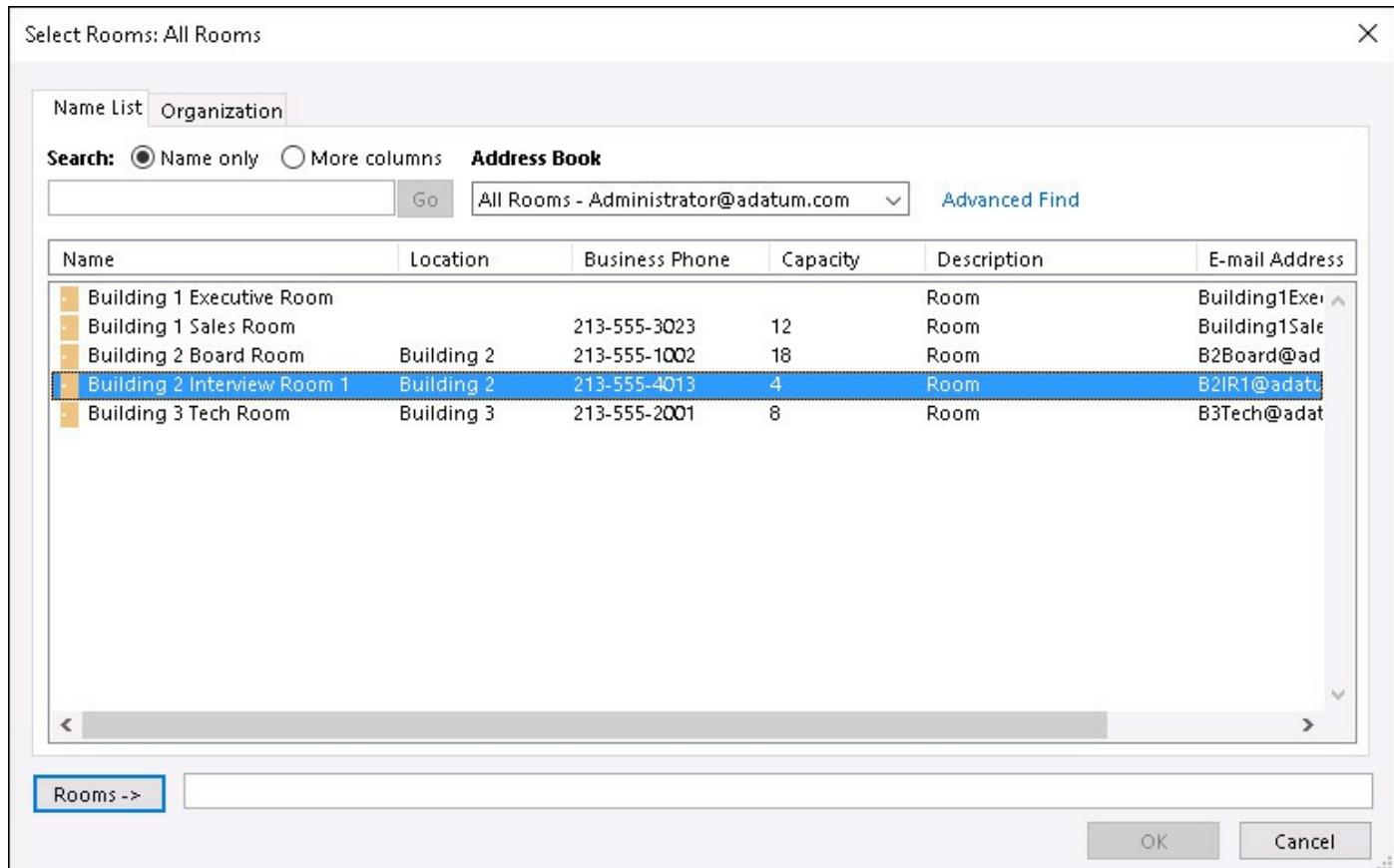
```
$password = Read-Host "Password?" -AsSecureString  
  
New-Mailbox -UserPrincipalName wghosh@adatum.com -Alias wghosh -Name  
wghosh  
-OrganizationalUnit CorpUsers -Password $password -FirstName Wriju -  
LastName  
Ghosh-DisplayName "Wriju Ghosh" -ResetPasswordOnNextLogon $true
```

## Create and configure resource mailboxes and scheduling

Resource mailboxes are mailboxes for rooms, such as conference rooms or meeting rooms, or for equipment, such as projectors or company vehicles. Resource mailboxes are in widespread use in organizations. Because they are specifically called out as an exam skill, you can be fairly certain that the exam tests your knowledge of them.

### Room mailboxes

In most companies, every meeting room has an associated room mailbox. This enables users to book the meeting rooms, since every mailbox has an associated calendar. To create a room mailbox, you only need to specify a room name and an alias. To make room mailboxes useful to your users however, you should also specify details about the rooms such as the location, the phone number, and the capacity of the room. [Figure 4-7](#) shows the rooms available and some of their properties. Notice that populating the location and capacity enables a person to find a room that matches their requirements quickly.



**FIGURE 4-7** A list of available rooms for meetings

The subsequent commands create and configure room mailboxes.

The following command creates a new room mailbox named “GTNP” with a capacity of 10 people and a phone number of 307-555-1299:

[Click here to view code image](#)

```
New-Mailbox -Room -Name "GTNP" -ResourceCapacity 10 -Phone "307-555-1299"
```

The following command configures an existing room mailbox named “Signal Mountain” to have a capacity of 12:

[Click here to view code image](#)

```
Set-Mailbox -Name "Signal Mountain" -ResourceCapacity 12
```

You can also expand the information about rooms by using custom properties. The methods are shown here so you are familiar with them for the exam. The following example adds custom properties named Projector, Smartboard, and Whiteboard to Exchange for room mailboxes:

[Click here to view code image](#)

```
$ResourceConfiguration = Get-ResourceConfig
$ResourceConfiguration.ResourcePropertySchema+=("Room/Projector")
```

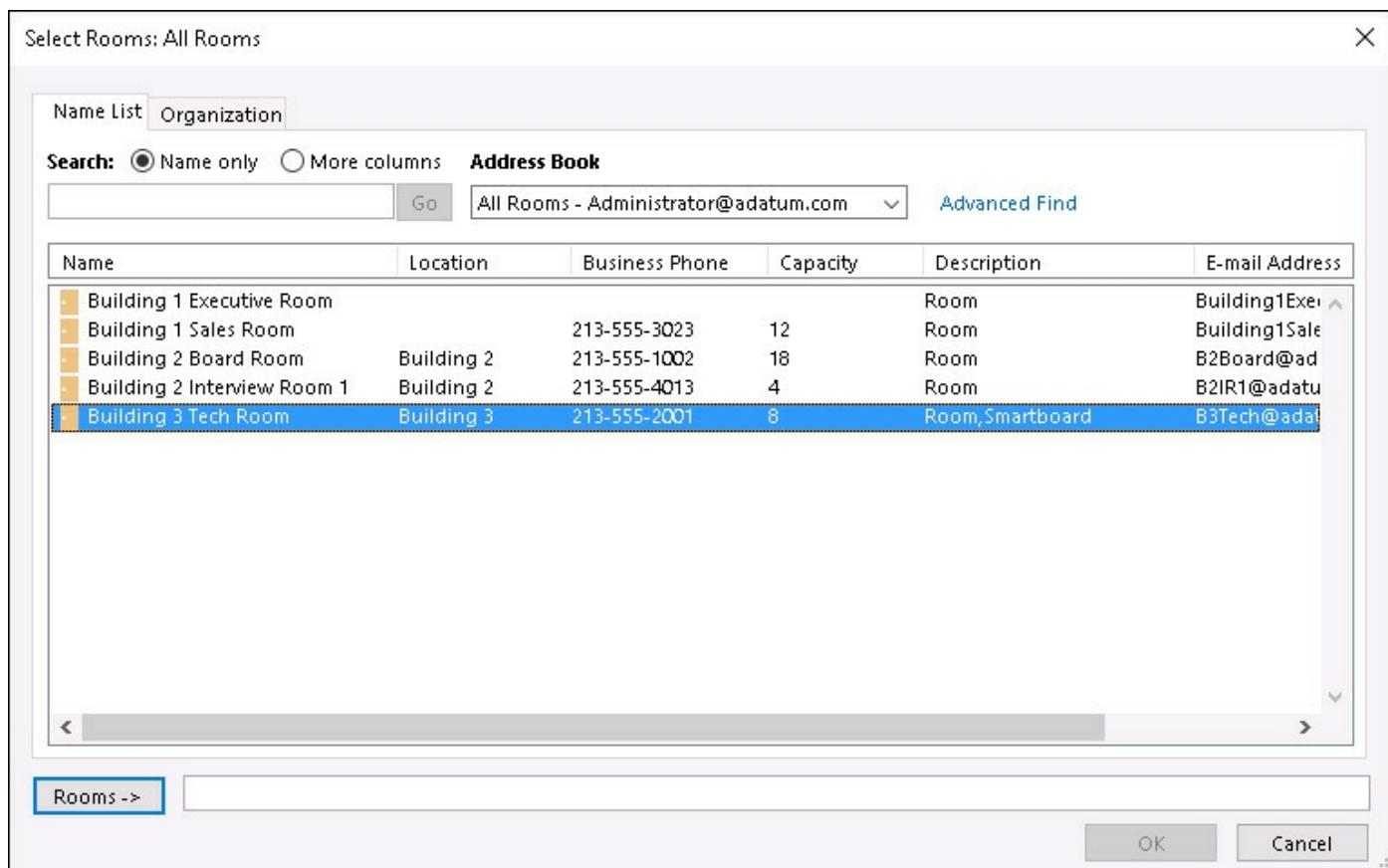
```
$ResourceConfiguration.ResourcePropertySchema.Add("Room/Smartboard")
$ResourceConfiguration.ResourcePropertySchema+=("Room/Whiteboard")
Set-ResourceConfig -ResourcePropertySchema
$ResourceConfiguration.ResourcePropertySchema
```

After you have custom properties, you can add the properties to mailboxes. In the following example, the Smartboard property is added to the Building 3 Tech Room mailbox:

[Click here to view code image](#)

```
$ResourceMailbox = Get-Mailbox -Identity "Building 3 Tech Room"
$ResourceMailbox.ResourceCustom.Add("Smartboard")
$ResourceMailbox | Set-Mailbox -ResourceCustom
$ResourceMailbox.ResourceCustom
```

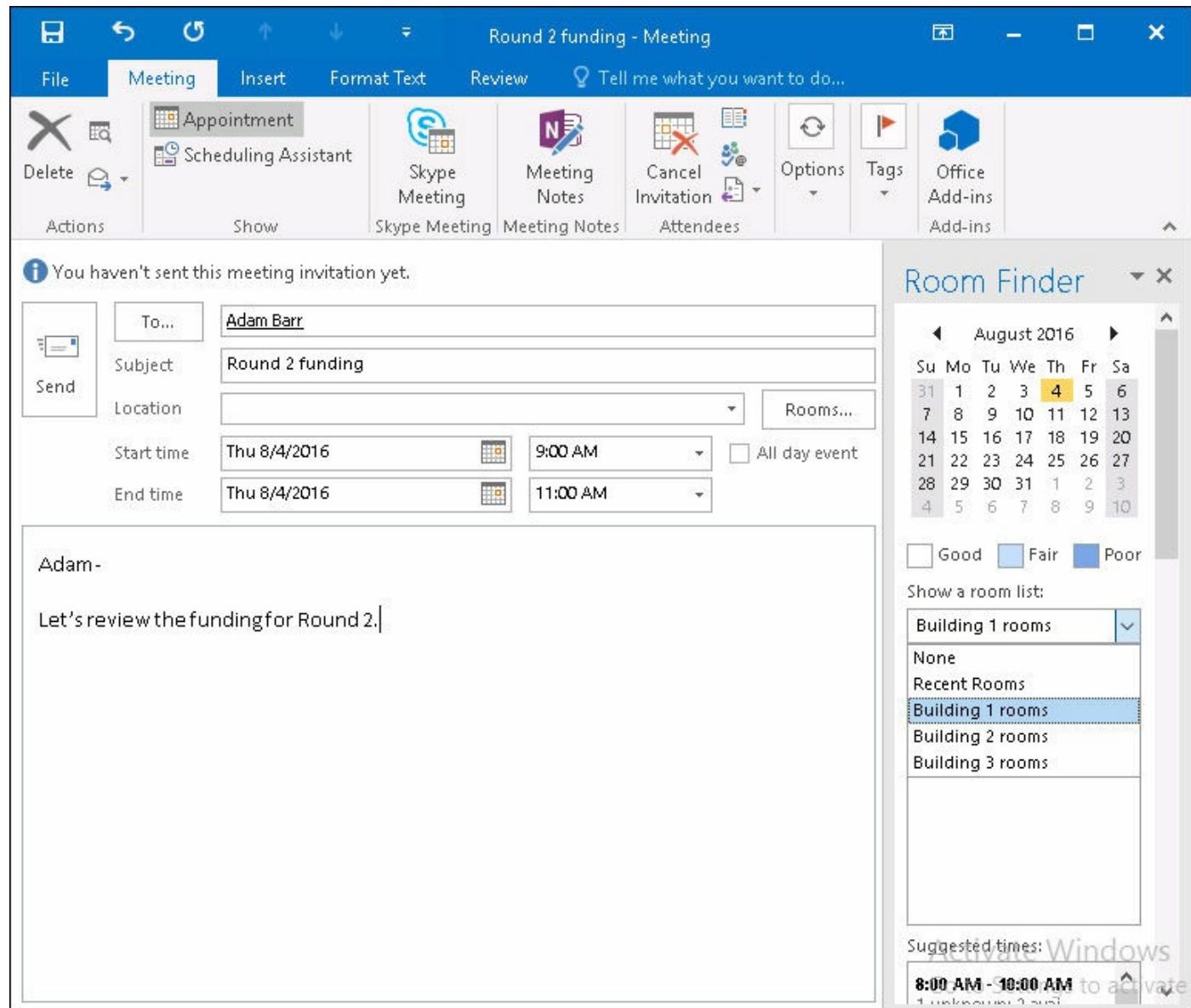
In [Figure 4-8](#), notice how the description of the room has been updated with the custom property of Smartboard. If you imagine all of your room mailboxes populated with pertinent information, you can quickly see the value of custom properties.



**FIGURE 4-8** A list of available rooms for meetings, one with a customer property

There is one final thing to be familiar with for room mailboxes. You can create a

distribution list that is a room list and then you can add your room mailboxes to the list. This greatly simplifies finding conference rooms for users because the Outlook Room Finder function displays the room lists and quickly finds an available room. For example, if you work on a campus with three large buildings and your preference is to locate a conference room in your own building, you can create a room list for the building and add the conference rooms to it. You can do the same for specific floors too. In [Figure 4-9](#), you can see a meeting being scheduled, with the Room Finder feature shown on the right. Notice that the room list shows a specific list for each building. You can select the appropriate list and look for rooms.



**FIGURE 4-9** A new meeting request with room lists displayed

You can also nest room lists into other room lists. For example, you could set up a room list for your corporate headquarters named HQ and place all of the room lists covering your headquarters into the HQ room list. If somebody was traveling to the

headquarters office and wanted to book a meeting room without a preference for a specific building, they can use the HQ room list to find a room in any building.

The setup process for room lists is shown in the following commands. Note that you must use PowerShell to configure this functionality.

In the following command, a room list is created for rooms in Building 1:

[Click here to view code image](#)

```
New-DistributionGroup -Name "Building 1 rooms" -OrganizationalUnit  
"adatum.com/Exchange/  
DLs" -RoomList
```

Next, add the existing room mailbox for rooms in Building 1 as a member of the new room list. Note that you would repeat this step for all applicable room mailboxes:

[Click here to view code image](#)

```
Add-DistributionGroupMember -Identity "Building 1 rooms" -Member "Building  
1 Sales Room"
```

## Equipment mailboxes

Although room mailboxes are the most popular type of resource mailbox, equipment mailboxes are just as useful. At a minimum, to create an equipment mailbox you need a name for the mailbox and an alias. You should also provide information about the equipment to make it easier for users to reserve the right equipment. For example, if you have two projectors that have equipment mailboxes, you should identify the projector that has wireless capabilities.

The following command creates a new equipment mailbox for a wireless projector:

[Click here to view code image](#)

```
New-Mailbox -Equipment -Name "Wireless projector"
```

## Create and configure shared mailboxes

A shared mailbox is a mailbox that is used by more than one person. Often, a shared mailbox is used by a department for communications. For example, a customer service department might use a shared mailbox to communicate with people about their warranty service. Instead of each person using their own mailbox, they can use a shared mailbox. This enables the entire team to participate in discussions or look up information related to warranty service that another customer service person initially handled. It also maintains the anonymity of the customer service representatives because the communications are through a shared mailbox.

A shared mailbox does not have an associated Active Directory user account. Thus, the only way for people to access a shared mailbox is by using their own credentials,

and that only works if the person has permissions to do that. You can use three permissions to grant access to a shared mailbox: Full Access, Send As, and Send On Behalf. When you grant somebody full access to a shared mailbox, you give them the permission to do just about everything except send email as the mailbox. For example, they can read the email, create meetings, and delete items.

Granting permissions is easily performed by using PowerShell. This section doesn't walk through the EAC method for the exam because it is similar to other tasks you walked through and you are not likely to be tested on the GUI aspects of the process.

To grant full access to the [Warranty@adatum.com](mailto:Warranty@adatum.com) mailbox for Kari, run the following command:

[Click here to view code image](#)

```
Add-MailboxPermissions -Identity "Warranty" -User "Kari" -AccessRights  
"Full Access"  
-InheritanceType all
```

Note the InheritanceType parameter. This parameter ensures that permissions are inherited down the mailbox.

For the details of granting Send As permissions and Send On Behalf permissions, see [Section 4.3](#) in this chapter.

## Create and configure mail-enabled users and contacts

A mail-enabled user and a contact are similar because both represent a user that has an external email address and appears in the global address list. The only difference between them is that a mail-enabled user has an Active Directory user account while a contact does not. Both are often used for consultants or contractors in an organization where they are working closely with team members, but maintain their own identities and email addresses at their company.

You can use the EAC or the EMS to create mail-enabled users and contacts. In the EAC, mail-enabled users and contacts are created in the Recipients workspace under the Contacts tab. The process is straight forward and similar to other Exchange objects so it isn't covered here to save space for covering it in PowerShell.

The subsequent commands show you how to create and configure mail-enabled users and contacts.

The following command creates a mail-enabled user for an existing Active Directory user account named Wriju with an email address of [wriju@contoso.com](mailto:wriju@contoso.com):

[Click here to view code image](#)

```
Enable-MailUser -Identity Wriju -ExternalEmailAddress wriju@contoso.com
```

The following command creates a mail contact for a new consultant named Marc with

an email address of [marc@contoso.com](mailto:marc@contoso.com):

[Click here to view code image](#)

```
New-MailContact -Name Marc -ExternalEmailAddress marc@contoso.com
```

The following command updates the existing mail-enabled user Wriju so his display name shows his company affiliations:

[Click here to view code image](#)

```
Set-MailUser -Identity Wriju -DisplayName "Wriju Ghosh (Contoso Ltd.)"
```

The following command creates a new Active Directory account and a mail-enabled user for Wriju Ghosh:

[Click here to view code image](#)

```
New-MailUser -Name "Wriju Ghosh" -ExternalEmailAddress wriju@contoso.com -  
Password  
(ConvertTo-SecureString -String 'Dr. Pepper had 20 ounces.' -AsPlainText -  
Force)
```

## Create and configure distribution lists

Distribution groups are a fairly large topic. The exam item writers have quite a bit of material to use when writing items to test your knowledge of distribution groups. This section covers the key points of importance for preparing you for the exam. If your knowledge of distribution groups is limited, you should also spend a little time reviewing the additional link at the end of this section.

This section outlines key information for distribution groups, mostly related to creation and configuration because that is what the exam skill covers. The following points provide information that might be covered in various exam scenarios.

- **New distribution groups, by default, do not accept email from anonymous sources** When you create a new distribution group, it only accepts mail from authenticated senders. Thus, only accepting mail from internal users. If you are creating a distribution group with the intention of it accepting email from the Internet, you must configure it specifically to do so.
- **Every distribution group has an owner** Whoever creates a group is the owner. Often, IT administrators create groups. A group owner can add and remove people from the distribution group. Imagine that Marc requests to have a group created for his team. After an IT administrator creates it, Marc cannot manage the group membership. Instead, Marc must be configured as the owner to enable him to manage the group membership.
- **You can configure different membership styles for a group** For joining a group, a group can be open, which means that anybody can join it. A group can also be

closed, which means only an owner or an IT administrator can add group members. Lastly, a group can be configured for owner approval whereby people that attempt to join must be approved by the group owner. You can also configure the disjoining style. A group can allow anybody to leave or you can configure a group so only members that have been approved by the owner can leave.

- **You can use moderation for groups** By default, new groups accept mail without requiring inbound email to be approved by a moderator. You can however, configure a group to have a moderator. In such a case, the moderator can approve or reject email messages to the group. Optionally, you can also configure specific people, such as the executive staff, to bypass moderation which enables them to send directly to a group.
- **You can use a MailTip for a group** You can configure a specific MailTip for a specific group. For example, if a group named “Information Technology” is not supposed to be used for trouble tickets, you can create a MailTip for the group to notify people that they should send an email message to Helpdesk for any troubleshooting situations.
- **You can create a distribution group naming policy for your company** With a naming policy, you can prepend or append words or symbols in front of or after a new distribution group name. For example, if a new group is created named “IT”, a naming policy could prepend Group\_ and append \_Users. Thus, the group name would be Group\_IT\_Users.

The following PowerShell commands outline some of the key creation and configuration tasks for distribution groups. In this first example, the command creates a new distribution group named “Azure Admins.” Notice how only a name is specified. That name, without the space, becomes the alias.

[Click here to view code image](#)

```
New-DistributionGroup -Name "Azure Admins"
```

In the following command, a new distribution group named Azure RMS Admins is created. It is hidden from email address lists, so users must type in the email address instead of finding it in the address book.

[Click here to view code image](#)

```
New-DistributionGroup -Name "Azure RMS Admins" -  
HiddenFromAddressListsEnabled $True
```

In the following command, an existing distribution group named “Canadian Sales” is modified so that anybody can join the group.

[Click here to view code image](#)

```
Set-DistributionGroup -Name "Canadian Sales" -MemberJoinRestriction Open
```



## Exam Tip

Be sure that you remember when a PowerShell parameter requires a Boolean value such as \$true or \$false and when a parameter requires a parameter-specific value such as “Open” or “Closed”, for example the MemberJoinRestriction parameter. On the exam, an answer choice that shows the command Set-DistributionGroup -Name “Canadian Sales” -MemberJoinRestriction \$False looks very compelling if you need to configure a group so anybody can join it, but it is wrong. As part of your exam preparation, you should use the commands outlined in this book to help you remember them.

### Need More Review? Creating and Configuring Distribution Groups

For more information on creating and configuring distribution groups, see [https://technet.microsoft.com/en-us/library/bb124513\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/bb124513(v=exchg.150).aspx).

From that webpage, you can find additional links to other supporting material too.

## Configure moderation

Earlier, this section defined what moderation is and now it looks at how to configure moderation.

In the following command, a new distribution group named Azure RMS Admins is created. It has moderation enabled, the moderator is Kari, and allows email from the Internet.

[Click here to view code image](#)

```
New-DistributionGroup -Name "Azure RMS Admins" -ModeratedBy "Kari" -  
ModerationEnabled  
$True -RequireSenderAuthenticationEnabled $False
```

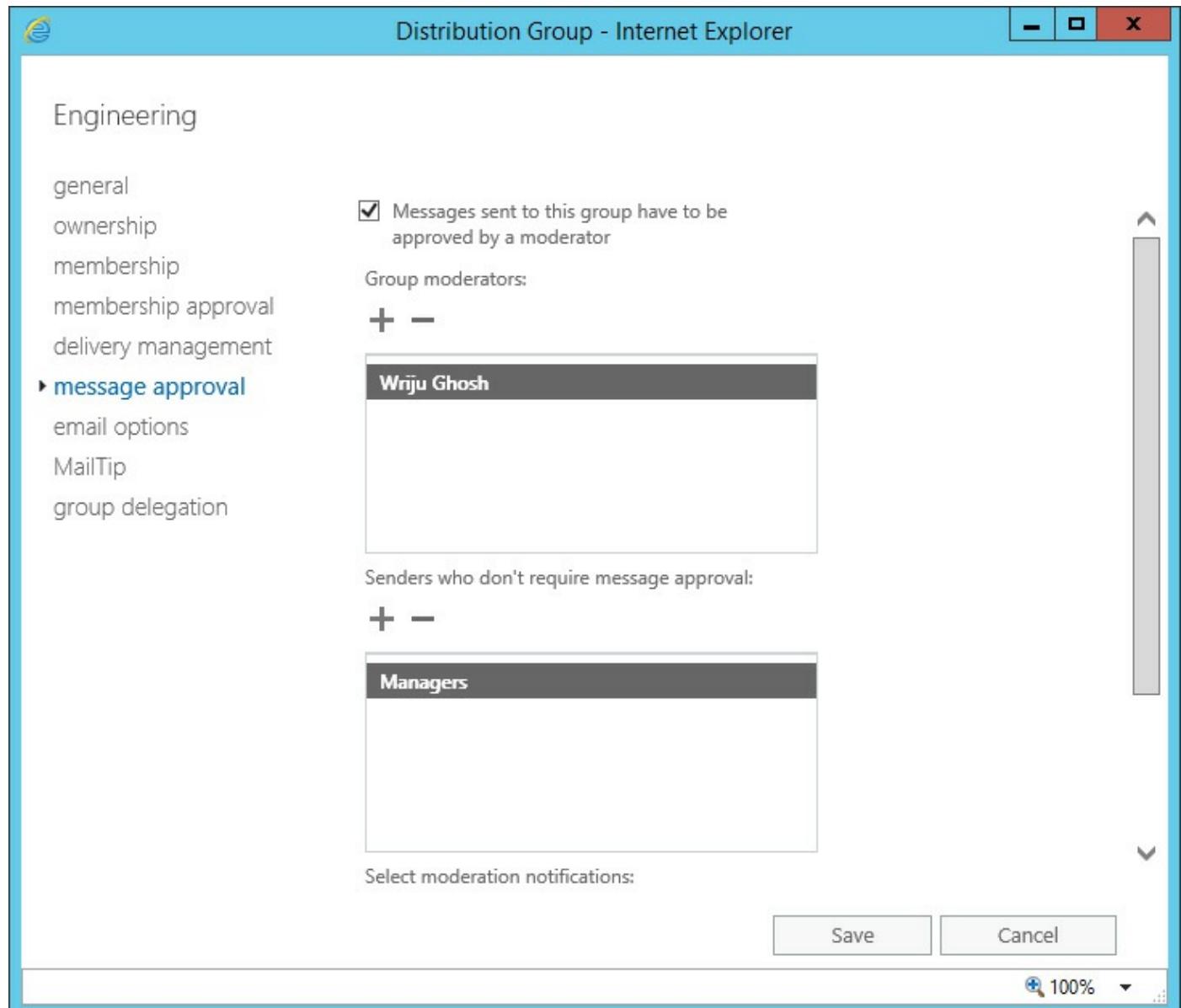
Let’s walk through a hypothetical exam scenario:

You are the email administrator for Tailspin Toys. A manager requests a distribution group named “Toy Designers.” The manager also requests to be the group owner. Finally, the manager needs to moderate email messages sent to the group. You need to configure the group while minimizing administrative overhead. What should you do? Choose all that apply.

This scenario might have several answer choices, including one answer choice to create the group, one answer choice to enable moderation, and another answer choice to

set the moderator to the group owner. You choose those three answers, but you get the question wrong or only partially right. Why? The reason is a small but key detail about moderation. A group owner is the moderator if moderation is enabled for a group and a specific moderator is not specified.

In addition to PowerShell, you can also use the EAC to configure moderation. Just modify a distribution group and go to the Message Approval tab. In [Figure 4-10](#), a distribution group named Azure Admins has moderation enabled. Wriju Ghosh is the moderator and members of the Managers group bypass moderation.



**FIGURE 4-10** A distribution group properties windows from the EAC

One final note about moderation. You can have somebody moderate specific messages without using moderation. To do this, you can use a mail flow rule. A mail flow rule can be configured to look for specific properties in a message and then send that email message to a moderator for processing. For example, a rule can look for a

specific keyword or phrase in the subject or body, such as “lawsuit,” and forward that message to a paralegal for moderation. If you come across an item on the exam that requires moderation, make sure to think through whether moderation or a mail flow rule is the solution.

## Create and configure linked mailboxes

A linked mailbox is a mailbox that exists in one forest or domain but has an associated user account that exists in a separate forest or domain. Linked mailboxes are commonly used in mergers and acquisitions, or in environments that have a separate forest for user accounts and mailboxes. A user account associated with a linked mailbox is known as a linked master account. You can create a linked mailbox by using the EAC or by using Windows PowerShell. In the following command, a new linked mailbox named Wriju is created for a user with “Wriju Ghosh” as the display name:

[Click here to view code image](#)

```
New-Mailbox -Name Wriju -LinkedMasterAccount "Wriju Ghosh" -  
LinkedDomainController  
"DC-01.tailspintoys.com" -LinkedCredential :(Get-Credential  
TAILSPINTOYS\ITAdmin)
```

## Create and configure modern public folders

You create public folders to provide users with a method of collaborating. Users often use public folders to store information and communications about a project. Companies often use public folders to hold company information, such as company calendars and benefits information.

Before you can begin creating public folders, you must create a public folder mailbox. The first public folder mailbox that you create is the writable public folder mailbox. The writable public folder mailbox is used when updates are made to the public folder hierarchy. If you plan to have thousands of concurrent public folder users, you should create additional public folder mailboxes to enhance performance. A public folder mailbox should be placed in a database that is close to the public folder users to maximize performance.

You can create a public folder mailbox by using the EAC or by using Windows PowerShell. To create a new public folder mailbox named PFMBX1, run the following command:

[Click here to view code image](#)

```
New-Mailbox -PublicFolder -Name PFMB1
```

You can also create a public folder mailbox in the EAC by going to the Public Folders workspace and then clicking the Public Folder Mailboxes tab in the right pane.

When you have a public folder mailbox, you can create and configure public folders. In the following command, a new public folder named Company Communications is created:

[Click here to view code image](#)

```
New-PublicFolder -Name "Company Communications"
```

Because the creation of a public folder is simple, the exam writers are likely to look for other ways to test your knowledge of public folders. Besides creating public folders, there are configuration components that administrators are expected to know for the exam. For example, you can configure a public folder to be mail-enabled. Then, it gets an email address. From there, you can add the public folder to a distribution group. You can also configure the deleted item retention for a public folder. You use the Set-PublicFolder cmdlet to configure a public folder.

As an administrator, you routinely configure permissions for public folders. In many organizations, administrators delegate the back end management of public folders to IT administrators and the management of individual public folders to users. This enables administrators to manage the back end and enables users to create, configure, and manage public folders without requiring the IT team. You can use the built-in role group named “Public Folder Management” for IT administrators. In the following command, Kari is added to the Public Folder Management group:

[Click here to view code image](#)

```
Add-RoleGroupMember -Identity "Public Folder Management" -Member Kari
```

The following command enables Kari to be a publishing editor for a public folder named HR:

[Click here to view code image](#)

```
Add-PublicFolderClientPermission -Identity "\Corporate\HR" -AccessRights PublishingEditor -User Kari
```

You look specifically at public folder permissions in the next section.

### Need More Review? Configuring Public Folder Client Permissions

For more information on the Add-PublicFolderClientPermission cmdlet, see [https://technet.microsoft.com/en-us/library/bb124743\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/bb124743(v=exchg.141).aspx).

## Summary

- You use the New-Mailbox cmdlet to create new mailboxes and the Set-Mailbox cmdlet to configure existing mailboxes.

- You can help users find meeting rooms by creating room mailboxes. Then, organize the room mailboxes by creating distribution lists for rooms, known as room lists. For example, you can create a room list for a specific office location or a room list that contains all large meeting rooms, such as rooms that hold more than 18 people.
- A shared mailbox is a mailbox used by multiple people. You can configure people to send email as the mailbox itself by using Send As permission. You can also configure people to send email on behalf of the shared mailbox by using Send On Behalf permission. Additionally, you can configure people to have Full Access to a mailbox so they can delete items and perform other management tasks. People with just Full Access cannot send email as the mailbox or on behalf of the mailbox. Instead, they need specific permission to do so.
- Distribution groups have an owner. The owner, by default, is the moderator when moderation is enabled.
- You can configure moderation for a distribution group by using the moderated option in the distribution group properties or by using a mail flow rule.
- Before you can create public folders, you need to create at least one public folder mailbox.

### Skill 4.3: Manage mail-enabled object permissions

While you've touched a little bit on object permissions during this chapter, you are now going to dive a further into the details. This section looks at how to manage permissions for mail-enabled objects. It focuses on Windows PowerShell methods because they are the least understood and often the primary method used to test your knowledge of permissions on the exam.

---

#### This section covers how to:

- [Determine when to use Send As and Send On Behalf permissions](#)
  - [Configure mailbox folder permissions](#)
  - [Configure mailbox permissions](#)
  - [Set up room mailbox delegates](#)
  - [Configure auto-mapping](#)
  - [Create and configure public folder permissions](#)
-

## Determine when to use Send As and Send On Behalf permissions

The last section talked about shared mailboxes, and that brought up a few permissions that you can use when you work with shared mailboxes. You have already seen how to grant full control to a shared mailbox, so now this section looks at the other two permissions so you can figure out when to use one over the other:

- **Send As** When you grant somebody Send As permissions, they can choose that specific mailbox as the sender. Recipients receive the email and it appears to come directly from the chosen mailbox. This permission is typically used with shared mailboxes when you want to maintain the anonymity of the senders.
- **Send on Behalf** The permission to send on behalf of somebody enables a person to send on behalf of a shared mailbox. Instead of the email appearing to come directly from the shared mailbox however, recipients clearly see that the email message was sent by a specific person, on behalf of the shared mailbox. You routinely use Send on Behalf permission for delegates. For example, you might grant an executive assistant Send on Behalf permission for her boss's mailbox. This enables the executive assistant to maintain her boss's calendar by sending out meeting invites.

To grant Send As permissions to a shared mailbox named Warranty for Kari, run the following command:

[Click here to view code image](#)

```
Add-ADPermission -Identity Warranty -User Kari -ExtendedRights "Send As"
```

To grant Send on Behalf permissions to the Warranty mailbox for Kari, run the following command:

[Click here to view code image](#)

```
Set-Mailbox -Identity Warranty@adatum.com -GrantSendOnBehalfTo  
Kari@adatum.com
```

## Configure mailbox folder permissions

You can grant users permissions to specific mailbox folders, such as the Inbox or user-created folders. Such permissions enable a user to only work with items in the specified folder. Doing this is more granular than granting mailbox access. For the exam, be aware of that. Watch for questions that have requirements to maximize security and adhere to the principle of least privilege.

[Table 4-1](#) highlights the available mailbox folder permissions.

Permission	Description
CreateItems	A user can create new items in a folder.
CreateSubfolders	A user can create a new subfolder in a folder.
DeleteAllItems	A user can delete any item in a folder.
DeleteOwnedItems	A user can delete items that they created in a folder.
EditAllItems	A user can edit all items in a folder.
EditOwnedItems	A user can edit items that they created in a folder.
FolderContact	The user is a contact for a public folder.
FolderOwner	The user is the owner of a folder and can view it, move it, or create subfolders in it.
FolderVisible	A user can see that a folder exists but cannot read items, edit items, or create items.
ReadItems	A user can read items in a folder.

TABLE 4-1 Mailbox folder permissions

In addition to working with individual folder permissions, which can be a bit tedious, you can also use the built-in roles that combine permissions for ease of assignment. [Table 4-2](#) shows the roles and role descriptions.

Role	Description
Author	A user can create items, delete their own items, edit their own items, see the folder, and read items.
Contributor	A user can see the folder and create items in it.
Editor	A user can create items, delete all items, edit all items, see the folder, and read items.
None	A user can see the folder.
NonEditingAuthor	A user can see the folder, read items, and create items.
Owner	A user can create items, create subfolders, delete all items, edit all items, see the folder, and read items. The owner is also the folder contact for a public folder.
PublishingEditor	A user can create items, create subfolders, delete all items, edit all items, see the folder, and read items.
PublishingAuthor	A user can create items, create subfolders, delete their owned items, edit their owned items, see the folder, and read items.
Reviewer	A user can see the folder and read items.
AvailabilityOnly	A user can see availability data. This is applicable to calendar folders only.
LimitedDetails	A user can view availability data and read items. This is applicable to calendar folders only.

TABLE 4-2 Mailbox folder roles

You do not have to memorize every action that a role has, which is tedious and not worth the investment of time. You should however, be familiar with the available roles,

their names, and their general capabilities.

Now that you've seen the permissions and the roles, let's walk through some examples of how to grant them.

The following command enables Marc to read items in Kari's HR folder:

[Click here to view code image](#)

```
Add-MailboxFolderPermission -Identity kari@adatum.com:\HR -User  
marc@adatum.com  
-AccessRights ReadItems
```

The following command enables Marc to be an author for Kari's Inbox folder:

[Click here to view code image](#)

```
Add-MailboxFolderPermissions -Identity kari@adatum.com:\Inbox -User  
marc@adatum.com  
-AccessRights Author
```

As you can see, whether you grant individual permissions or a role, the cmdlet is the same and the command syntax is the same.

## Configure mailbox permissions

Earlier when you looked at shared mailboxes, the permissions you can use for the shared mailboxes were briefly mentioned. That section also showed you how to configure full access to a shared mailbox. All of that information applies to regular mailboxes too. This section looks at the built-in permissions available at the mailbox level.

[Table 4-3](#) shows the access rights that you can use for the Add-MailboxPermission cmdlet.

Permission	Description
FullAccess	Full access to a mailbox except cannot send email messages.
ExternalAccount	Full access to a mailbox for a user in a separate forest and domain.
DeleteItem	Delete items from the mailbox.
ReadPermission	Read items in the mailbox.
ChangePermission	Change permissions on the mailbox.
ChangeOwner	Change the owner for the mailbox.

TABLE 4-3 Mailbox permissions

The following command grants ReadPermission for Brian's mailbox to Kari:

[Click here to view code image](#)

```
Add-MailboxPermission -Identity "Brian" -User "Kari" -AccessRights  
ReadPermission
```

## Set up room mailbox delegates

Earlier, this chapter introduced you to room mailboxes. This section shows you some options for configuring room mailboxes with delegates.

There are two options for room mailboxes to handle meeting requests:

- **Automatically process booking requests** In this scenario, if a time slot is open, the room mailbox automatically accepts a meeting invitation and books the room. If there is a scheduling conflict or the meeting violates the scheduling limits, such as a meeting lasting multiple days, the room mailbox automatically declines the meeting invitation.
- **Use a delegate to process booking requests** In this scenario, a person handles booking requests. The person is responsible for verifying that the requested date and time are available and that the meeting doesn't violate the scheduling limits. The person then accepts or declines the meeting. Some organizations use executive assistants and/or secretaries to process room mailbox scheduling requests.

The following commands show how to set up delegates and calendar processing.

The following command updates the Building 1 Sales Room so Kari is the delegate:

[Click here to view code image](#)

```
Set-CalendarProcessing -Identity "Building 1 Sales Room" -  
ResourceDelegates "Kari"
```

The following command updates the Building 2 Board Room so the maximum meeting length is 3 hours:

[Click here to view code image](#)

```
Set-CalendarProcessing -Identity "Building 2 Board Room" -  
MaximumDurationInMinutes 180
```

The following command configures the Building 3 Tech Room so the room does not automatically process meeting requests, such as if you are going to use a delegate instead:

[Click here to view code image](#)

```
Set-CalendarProcessing -Identity "Building 3 Tech Room" -  
AutomateProcessing None
```

## Need More Review? Configuring Calendar Processing

For more information about the Set-CalendarProcessing cmdlet, including the full syntax and list of parameters, see [https://technet.microsoft.com/en-us/library/dd335046\(v=exch.160\).aspx](https://technet.microsoft.com/en-us/library/dd335046(v=exch.160).aspx).

## Configure auto-mapping

When you give a user full access to another mailbox, Outlook automatically opens the other mailbox along with the user's primary mailbox. Auto-mapping is the name of the feature that enables Outlook to automatically open other mailboxes when a user has full access to them. It is convenient, but it is often undesired, especially if you have full access to several mailboxes.

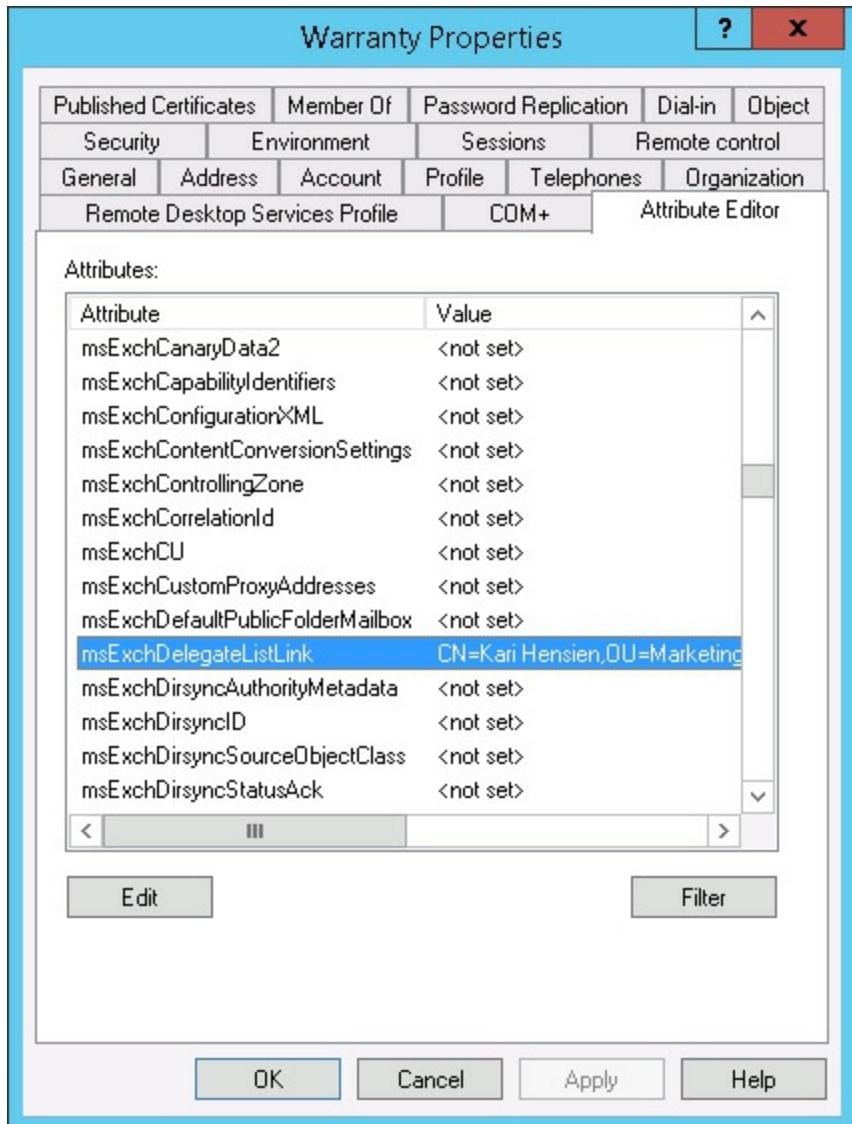
You configure auto-mapping when you grant full access to a mailbox. There is a dedicated parameter for turning on or turning off the auto-mapping feature. In the following command, Kari is given full access to the Warranty mailbox with auto-mapping disabled.

[Click here to view code image](#)

```
Add-MailboxPermission -Identity Warranty -User Kari -AccessRight  
FullAccess  
-InheritanceType All -Automapping $false
```

If you have a user that already has full access to a mailbox and you want to remove the auto-mapping feature, you can use the same command. In such a case, permissions remain the same and just the auto-mapping feature is removed. Alternatively, you can remove the access to the mailbox and add it back with the desired auto-mapping setting.

On the backend, the auto-mapping feature works because the mxExchDelegateListLink attribute is populated with the DNs of users that have full access to the mailbox, as shown in [Figure 4-11](#).



**FIGURE 4-11** The attributes of a mailbox

## Create and configure public folder permissions

We have covered many permissions-related topics in this chapter. Our final look at configuring permissions deals with public folder permissions. The good news is that the permissions used for public folders come from the same list as mailbox permissions. Similar to mailboxes, you can assign individual permissions for public folders, such as the ability to create new items, or you can use built-in roles, such as Publishing Editor, to assign rights. Refer to [Table 4-1](#) and [Table 4-2](#) to refresh your memory on the individual permissions and roles. In the following commands, you are able to see how to perform common public folder permission tasks.

The following command grants an HR employee named Kari the access to create items in the Corporate Communications public folder. Note that while Kari can create items, she can't delete or edit her own items. You have to individually assign the rights needed, or you can use a role instead.

### [Click here to view code image](#)

```
Add-PublicFolderClientPermission -Identity "\Corporate Communications" -  
User Kari  
-AccessRights CreateItems
```

The following command uses a role to grant Kari Author permissions for the Corporate Communications public folder. This enables Kari to create items, edit her own items, and delete her own items.

### [Click here to view code image](#)

```
Add-PublicFolderClientPermission -Identity "\Corporate Communications" -  
User Kari  
-AccessRights Author
```

One important concept to understand about public folder permissions is inheritance. Similar to NTFS inheritance, public folder permissions are inherited by child public folders by default. You can use inheritance to reduce administrative overhead. For example, imagine that you are going to create a new public folder structure for the HR department. You decide to create a top-level HR department public folder and several public folders under the HR top-level public folder. Instead of individually assigning permissions to them after creation, you can use inheritance. In this scenario, you should create the top-level public folder and assign the desired permissions to it. Then, you can create the public folders under the HR public folder. The new public folders automatically inherit the permissions from the HR public folder, which was already set to the desired permissions. Even if slight adjustments are needed to one or more of the public folders, you have saved some time.

## Summary

- Send As permissions enable you to send email as another mailbox. The recipient does not know that another person sent the email.
- Send on Behalf permissions enable you to send email on another mailbox's behalf. The recipient sees the identity of the original sender along with the sending mailbox's information.
- You can grant granular access rights to mailbox folders using permissions such as ReadItems and CreateItems. You can also use built-in roles that combine multiple permissions to simulate real-world scenarios. For example, an Author role enables a person to create items, delete and edit their own items, and read items.
- You can grant mailbox access by using built-in permissions such as FullAccess, DeleteItem, ReadPermission, and ChangePermission.
- For mailboxes that you have full access to, auto-mapping automatically adds them to Outlook. You can disable it by using the AutoMapping parameter with a value

of \$false.

- You use the Add-PublicFolderClientPermission to configure public folder permissions.

## Skill 4.4: Plan, deploy, manage, and troubleshoot Role Based Access Control

This section discusses how role-based access control (RBAC) is used to assign only the permissions levels that are necessary to perform a function. The idea behind using RBAC is to prevent lower level administrators from being able to manage all aspects of an Exchange organization. Another method of restricting permissions is to determine whether to use RBAC-based split permissions or Active Directory-based split permissions. This section compares the two to determine which method works best in certain environments. It also discusses how to delegate the installation permissions for Exchange to allow a user account that is not in the Organization Management role group to complete an Exchange server installation. Next, this section goes into using unscoped roles, which provide methods of using scripts, cmdlets, and special permissions that are not part of Exchange by default. Finally, this section discusses some options for troubleshooting RBAC, and configuring user assignment policies.

---

### This section covers how to:

- [Determine appropriate RBAC roles and cmdlets](#)
  - [Limit administration using existing role groups](#)
  - [Evaluate differences between RBAC and Active Directory split permissions plan and configure a custom-scoped role group](#)
  - [Plan and configure delegated setup](#)
  - [Plan and create unscoped top-level roles](#)
  - [Troubleshoot RBAC](#)
  - [Plan and configure user assignment policies](#)
- 

### Determine appropriate RBAC roles and cmdlets

When you use the principle of least privilege, you only assign the permissions that are needed for someone to complete a task. For example, a help desk administrator that assists with managing recipients doesn't need access to manage Exchange servers or anti-spam settings.

You can assign administrators to one or more RBAC groups specifically for the role that they are performing. The built-in role groups are:

- **Organization Management** This role should be used sparingly, as users with this role can perform most tasks in your Exchange environment.
- **View-only organization management** This role enables an administrator to view but not modify existing objects in the organization.
- **Recipient Management** This role enables an administrator to create and manage the recipients and mailboxes in the organization.
- **UM Management** This role enables an administrator to manage features of Unified Messaging, including the service configuration and auto attendants.
- **Help Desk** This role enables members to modify Outlook on the web settings for user accounts in the organization. This includes the display name, phone number, and other user properties. By default, this role cannot modify the mailbox size of a user account.
- **Hygiene Management** This role enables administrators to configure the anti-spam and anti-virus settings on the Exchange server. Third-party products can also be given this permission role to integrate with Exchange Server 2016.
- **Records Management** Members of this role can configure compliance settings, including retention tags, message classifications, and transport rules.
- **Discovery Management** Members of this role can search mailboxes in the organization and configure legal holds on mailboxes.
- **Public Folder Management** This role enables members to manage public folders, such as creating and deleting public folders.
- **Server Management** This role enables administrators to manage server-specific configurations, including transport roles, UM, client access, and mailbox features.
- **Delegated Setup** Members of this role can complete an Exchange server deployment that has been previously provisioned by a member of the Organization Management role group.
- **Compliance Management** This role enables members to configure and manage compliance settings for an organization.

[Figure 4-12](#) shows the admin roles that can be configured from the EAC.

The screenshot shows the Exchange admin center interface. At the top, there are browser navigation buttons (back, forward, search, refresh) and a tab bar with 'admin roles - Microsoft Exchange'. Below the header, the 'Enterprise' and 'Office 365' logos are visible. The main title 'Exchange admin center' is displayed. On the left, a sidebar menu lists categories: recipients, permissions (which is currently selected), compliance management, organization, protection, mail flow, mobile, public folders, unified messaging, servers, hybrid, and tools. The 'permissions' section is expanded, showing a list of management tasks. At the top of this list is 'Compliance Management', which is highlighted with a dark gray background. Other items in the list include Delegated Setup, Discovery Management, Help Desk, Hygiene Management, Organization Management, Public Folder Management, Recipient Management, Records Management, Server Management, UM Management, and View-Only Organization Management. A status message at the bottom of the list says '1 selected of 12 total'. The bottom of the screen features a horizontal scrollbar.

FIGURE 4-12 Exchange admin roles

## **Limit administration using existing role groups**

Understanding which permission levels that a role group grants and doesn't grant is a key concept in preparing for this section of the exam. A key strategy in many permission-based exam questions is to require a solution to use the principle of least privilege. For example, imagine that a question is asking you to configure a role to enable administrators to modify addresses and phone numbers of user accounts and ensure that personnel cannot manage anything else. To meet the question's requirements, you can assign the administrators the Organization Management role. The administrators would have access to manage mailboxes and Exchange servers however. Therefore, you should use the Help Desk role which only assigns the minimum permissions required to perform the tasks.

## **Evaluate differences between RBAC and Active Directory split permissions plan and configure a custom-scoped role group**

By default, Exchange Server installs in an Active Directory environment with shared permissions. This enables Exchange and Active Directory management from both the EAC and the management shell.

Many large organizations have multiple teams that manage different infrastructure components. For example, an Exchange team manages the Exchange infrastructure. An Active Directory team manages the directory related components such as Active Directory. These teams might frequently work together, but they do not have or need the same permissions. The separation of permissions between these teams is referred to as split permissions.

These are two different methods that you can use to split permissions:

- **RBAC split permissions** RBAC split permissions modify Active Directory to only enable Exchange servers, services, and role group members to create Exchange-related objects within Active Directory. This moves the permission management from Active Directory to Exchange. This model simplifies object creation because the creation and configuration can often occur in a single task or step.
- **Active Directory split permissions** Using Active Directory split permissions moves the permissions from Exchange to Active Directory. Any object creation must be completed by using Active Directory tools, not Exchange tools. This often means that Active Directory administrators create objects while Exchange administrators configure the Exchange attributes. This model is best suited for a high security environment where complete separation of permissions is required.

When using a split permissions model, you should use RBAC split permissions because it provides additional flexibility and simplicity compared to creating objects

from Active Directory tools. If security is the most important factor for your organization however, the Active Directory split permissions model is best.

## RBAC split permissions

When using RBAC split permissions, Active Directory is modified to require Exchange role group membership to create objects in Active Directory. To create objects, an administrator must be a member of the Mail Recipient Creation or Security Group Creation role groups. By default, members of the Organization Management and Recipient Management role groups can also create objects.

RBAC split permissions are good for environments that meet the following conditions:

- You need to be able to create objects by using tools other than Active Directory tools.
- You want services, including Exchange servers, to have the ability to create Active Directory objects.
- You want to simplify object creation.
- You plan to manage distribution groups and role group membership by using Exchange Server tools.
- You have third-party applications that need to use Exchange-based tools to create Active Directory objects.

Configuring RBAC split permissions is fairly simple. Follow these general steps to enable RBAC split permissions:

1. If necessary, disable Active Directory split permissions.
2. Create a new role group for the Active Directory administrators.
3. Create regular and delegated assignments between the Mail Recipient Creation and Security Group Creation roles and the role group that you created.
4. Remove the regular and delegated management role assignment between the Mail Recipient Creation and Security Group Creation roles from the Organization Management and Recipient Management role groups.

After you complete these steps, only the members of the role group that you created have the ability to create objects. Additionally, Active Directory administrators still need an Exchange administrator to modify additional attributes of an object after it has been created.

## Active Directory split permissions

With Active Directory split permissions, the permissions to create objects are restricted for Exchange Server. The Exchange Trusted Subsystem is modified to limit what Exchange administrators and servers can create in Active Directory.

After you enable Active Directory split permissions, a user account must first be created by using Active Directory tools. After you create an Active Directory user account, an Exchange administrator must enable a mailbox for that user account. Additional Exchange-related attributes can only be modified by Exchange administrators.

Active Directory split permissions are good for environments that meet the following conditions:

- You want to ensure that Active Directory objects are created outside of Exchange
- Exchange administrators must not have the ability to create Active Directory objects
- Distribution group management must be performed by Active Directory administrators
- Third-party Exchange-integrated applications must not be able to create objects from Exchange tools
- You want to maximize the security of your environment, even if it introduces additional complexity and administrative overhead

Active Directory split permissions can be enabled during installation by specifying the ActiveDirectorySplitPermissions and PrepareAD switches with setup.exe. You should restart the Exchange servers after enabling split permissions to ensure that they receive the latest Active Directory security token.

Enabling Active Directory split permissions prevents Exchange servers and administrators from creating and removing mailboxes, mail contacts, users, and remote mailboxes. Additionally, Exchange administrators and servers cannot add, modify, or remove distribution groups or modify group memberships.



### Exam Tip

If Exchange Server is installed on a domain controller, you cannot use split permissions.

---

## Plan and configure delegated setup

In many scenarios, Exchange Server is installed by the same administrators who manage it. However, in some environments there is one team for the deployment and a separate team for management and administration. For this scenario, you can delegate the permissions needed to install Exchange without making the user accounts members of the Organization Management role group.

When Exchange Server is installed, several configuration changes take place that require Organization Management permissions.

A server object is created in Active Directory:

[Click here to view code image](#)

```
CN=Servers,CN=Exchange Administrative Group  
(FYDIBOHF23SPDLT),CN=Administrative  
Groups,CN=<Organization Name>,CN=Microsoft  
Exchange,CN=Services,CN=Configuration,DC=<Ro  
ot Domain>,DC=<Your domain suffix>
```

The following permissions are added to the server object for the Delegated Setup role group:

- Full Control on the server object and its child objects
- Deny access for the Send As extended right
- Deny access for the Receive As extended right
- Deny CreateChild and DeleteChild permissions for Exchange Public Folder Store objects
- The computer object is also added to the Exchange Servers security group
- The server is added as a provisioned server in the EAC

With delegated setup, the deployment of a new Exchange server is split into two tasks. One task is referred to as the provisioning of the server. That part is handled by an Exchange administrator that is a member of the Organization Management role group. The other task is the installation of Exchange Server. That part is handled by the delegated administrator and must take place after the server provisioning.

Note that the environment must already contain at least one Exchange server to perform Delegated Setup.

To provision a new Exchange server named EX02, run the following command from location of the Exchange installation media:

[Click here to view code image](#)

```
setup.exe /NewProvisionedServer:EX02 /IAcceptExchangeServerLicenseTerms
```

If you do not use the /NewProvisionedServer parameter then EMS assumes the local

computer is being used. After you provision the Exchange server in Active Directory, you need to add the user account that will finalize the installation to the Delegated Setup role group. The user account is then able to perform the Exchange installation for the server that was provisioned, without needing to be a member of the Organization Management role group. From an exam scenario perspective, think about delegated setup when you are presented with scenarios where a remote administrator needs to perform an Exchange installation or when an environment has high security requirements.

## Plan and create unscoped top-level roles

While Exchange Server comes with built-in roles, you can create additional management roles based on an existing role group or as an empty, unscoped role. An unscoped role can contain scripts or cmdlets that aren't part of Exchange. The scripts or cmdlets can modify any object within the organization as long as the user account has the necessary permissions.

To create an unscoped role, you must be a member of the Unscoped Role Management role. To create an unscoped role named Scripts, run the following command:

[Click here to view code image](#)

```
New-ManagementRole -Name "Scripts" -UnScopedTopLevel
```

After the management role is created, add the role entries to define how the role is used. For example, you can add a script or a non-Exchange PowerShell cmdlet to the role group. Script files must be located in the RemoteScripts directory of the Exchange installation path. By default, this directory is located at %ExchangeInstallPath%\RemoteScripts.

To add a script named ProtocolCheck.ps1 to the role group, run the following command:

[Click here to view code image](#)

```
Add-ManagementRoleEntry Role\ProtocolCheck.ps1 -Type Script -  
UnScopedTopLevel
```

To add a PowerShell cmdlet named Get-ComplianceCheck to the existing Security role, run the following command:

[Click here to view code image](#)

```
Add-ManagementRoleEntry SecurityRole\Get-Compliancecheck -PSSnapinName  
Adatum.Security.  
Cmdlets -UnScopedTopLevel
```

In most scenarios, you should gather a list of responsibilities for a role and figure out which scripts and cmdlets enable a person to perform the role duties. Then, add all of

the scripts and cmdlets to the role. After you configure the role, you can assign it like you assign the built-in roles.

## Troubleshoot RBAC

When you are troubleshooting RBAC, your goal is to gather enough information to find out where the problem is. Is a role assigned to a role group? Is the role group assigned to another role group? Is something else wrong? You can use PowerShell to troubleshoot. There are many built-in PowerShell cmdlets that can be used to assist in troubleshooting or determining RBAC permissions with Exchange. You can use the following cmdlets to troubleshoot RBAC:

- **Get-ManagementScope** This cmdlet lists all of the management scopes. By default, there aren't any.
- **Get-ManagementRole** This cmdlet lists all of the management roles.
- **Get-ManagementRoleEntry** This cmdlet lists the role entries, mostly cmdlets, that are added to a management role. For example, you can run the `Get-ManagementRoleEntry "Legal Hold\*"` to find out exactly which actions an administrator can take based on the Legal Hold management role.
- **Get-RoleGroup** This cmdlet finds all of the role groups such as Organization Management, Recipient Management, and Records Management.
- **Get-RoleGroupMember** This cmdlet finds members of a role group. You just specify the role group as part of the command.
- **Get-RoleAssignmentPolicy** This cmdlet shows you role assignment policies. By default, there is only one that enables users to perform some self-service administrative tasks.
- **Get-ManagementRoleAssignment** This cmdlet outputs a plethora of information about the roles and assignments.

Each of these cmdlets retrieve a different aspect of RBAC permissions and displays information that assists in troubleshooting a permissions-based problem.

### Need More Review? Understanding RBAC

For more information about permissions and RBAC, see  
[https://technet.microsoft.com/en-us/library/dd351175\(v=exchg.160\).aspx#RoleBased](https://technet.microsoft.com/en-us/library/dd351175(v=exchg.160).aspx#RoleBased).

## Plan and configure user assignment policies

This skill, titled “[Plan and configure user assignment policies](#)” would make more sense as “Plan and configure role assignment policies.” Role assignment policies are used to manage which tasks a user can perform on their own mailbox. An existing default role assignment policy, named Default Role Assignment Policy, enables users to perform the following actions on their own mailbox:

- Update their contact information including address, mobile, and personal information.
- View and modify their distribution group membership, so long as the distribution group is configured to allow a user to join or leave the group.
- Work with custom apps, marketplace apps, and apps to access their mailbox.
- Manage their basic mailbox and account settings configuration.
- Manage their text messaging settings.
- Manage their voice mail settings.

But there are other permissions available that you can opt to grant to users, enabling them to:

- Update their name and display name. Many organizations avoid granting this permission to users to adhere to a naming convention or due to legal ramifications.
- Create, modify, and manage distribution groups. A user can modify or manage only distribution groups that they create and thus are the owner of.
- Manage retention tags.
- Perform diagnostics on their mailbox.

The following key points are important for you to know for the exam:

- **You can create multiple role assignment policies** If you want one set of users to be able to manage their contact information but others to be restricted, you can create two policies and assign them accordingly.
- **Mailboxes can only have one role assignment policy** While you can have multiple role assignment policies, you have to associate just one to each mailbox.
- **Administrative roles are not used with role assignment policies** Instead, only end user roles are valid for role assignment policies.

## Summary

- Built-in role groups enable you to grant permissions to administrators.
- To adhere to the principle of least privilege, limit permissions by assigning only

the minimum roles necessary.

- Use RBAC split permissions to control Exchange-related objects and their associated Active Directory objects from Exchange-based tools.
- Use Active Directory split permissions to control Active Directory objects for Exchange Server from Active Directory tools.
- Provision a server object in Active Directory to allow a different administrator to install Exchange by using delegated setup.
- Role assignment policies can be mapped to individual mailboxes to provide granular permissions for users.

## Skill 4.5: Plan an appropriate security strategy

One key skill growing in importance for Exchange administrators is security. Security is a key skill because corporate networks are becoming more open, and even borderless. Users are also routinely working with their own personal devices which often aren't as secure as corporate devices. If you factor in the growing sophistication of hackers and malware, you can imagine how important security is for the Exchange administrator today. The next two sections cover security-based topics. This section looks at securing Exchange data and Exchange server operating system data, as well as securing email communication.

### This section covers how to:

- [Plan and configure BitLocker](#)
- [Plan and configure S/MIME](#)

## Plan and configure BitLocker

BitLocker is the built-in volume encryption feature of the Windows operating system. You can use it to encrypt operating system volumes, data volumes, and even portable volumes. BitLocker can work with a Trusted Platform Module (TPM) with a minimum version of 1.2. A TPM is a special hardware component that provides cryptographic operations. BitLocker works best with a TPM 2.0 or newer chip, but can also work without a TPM by using software. The most secure BitLocker implementations use a TPM because they are very difficult to tamper with. Additionally, advanced BitLocker features, such as protection of the startup process and multi-factor authentication, require a TPM. The following key points outline BitLocker use on an Exchange server:

- **Virtualization means a lack of TPM** Today, many Exchange environments are virtualized. In a virtual environment, you do not have access to a TPM, so you must rely on software for a BitLocker implementation. That means that an

administrator has to enter a BitLocker password or insert a USB key every time you reboot an Exchange server. You can avoid this by not encrypting the boot volume.

- **You must account for data drives when you do not have a TPM** If you do not have a TPM in your Exchange server and you opt to only encrypt your data drives, you still need a way to unlock your data drives after a server restart. You can opt to do that manually, but that requires extra administrative overhead. You can also choose to have a script run as an automated task to automatically unlock the data drives. In such a scenario, you need to carefully monitor Exchange services. If your script takes too long to unlock the volumes, some Exchange services might not start up after a restart.
- **BitLocker impacts performance slightly** The generally accepted range for performance overhead is 1 percent to 9 percent. You should often go in the middle of that range at a minimum, somewhere about 5 percent. When you size an Exchange environment, you need to account for BitLocker if you plan to use it.
- **If you thin provision, you must use the option to encrypt used space only** BitLocker offers an option to encrypt an entire volume or just encrypt the used space. For most implementations with Exchange Server, you should encrypt the entire volume to maximize performance. If you use thin-provisioned storage, which is usually avoided due to performance degradation, you must use the used space only encryption option.

BitLocker is supported with Exchange Server 2016, but you need to weigh the pros and cons to see if it makes sense for your environment or for an environment that is presented to you on the exam. When you have physical Exchange servers, BitLocker is very compelling. When you have virtual servers, proceed with caution.

There are several methods that you can use for protecting volumes with BitLocker:

- **Password protector** A password can be used as the protecting mechanism. You should use a very strong password when using password protection. Upon restart, you need to enter the password to unlock the protected volume. This option is useful in environments that don't require high security and are protecting volumes without a TPM.
- **Startup key protector** A startup key can be stored on a USB drive. Then, you can insert the USB drive into the computer and unlock the protected volume. This option provides good security but has high administrative overhead. It is best used in environments without a TPM but in those that still want to maximize security.
- **TPM protector** If you have a TPM in a computer, you can use it for your BitLocker protection. This protection method requires less administrative overhead because BitLocker-protected volumes are automatically unlocked

without administrative intervention.

- **TPM and personal identification number (PIN) protectors** This protection method combines the TPM and a PIN to provide multi-factor authentication. This provides higher security than just TPM protection. Optionally, you can use the Network Unlock feature to unlock a BitLocker-protected volume automatically at startup. Without Network Unlock, administrative intervention is required for all server boots when volumes use TPM and PIN protectors. Imagine the impact during a monthly patching cycle or for remote servers.
- **TPM and startup key protectors** This protection method combines the TPM and a startup key stored on a USB drive to provide multi-factor authentication. This provides higher security than just TPM protection.
- **TPM and PIN and startup key protectors** This protection method combines a TPM, a PIN, and a startup key to provide multi-factor authentication. This is the most secure protection method for a BitLocker-protected volume.

What happens if you have a problem and lose the password or the protector stops functioning due to a hardware issue? In such a case, you can use a recovery method. There are two available recovery methods:

- **Recovery key protector** This is a recovery key file that you store on a USB drive. In a time of need, you can use the USB drive to unlock a BitLocker-protected volume.
- **Recovery password protector** This 48 character password can be stored in a file or in Active Directory. For non-domain joined machines, the password can also be stored as part of your Microsoft account, although this option isn't very applicable for an Exchange environment. Storing the password in Active Directory provides the best user and administrative experience. Wherever you store it, the recovery password can be used to unlock a BitLocker-protected volume.

To implement BitLocker, you need to perform the following steps. Note that this example uses the password protector. To use other protectors, you can follow the same steps but update the protector and the protector option parameters.

1. Install the BitLocker Drive Encryption feature on each server where you use BitLocker.
2. Restart the server.
3. Use Control Panel or PowerShell to enable BitLocker on desired volumes. For example, to use PowerShell to enable BitLocker on the G:\ volume, use a password key protector, and use a password of “Pleasedonttrytobuy1,000shares”, and then run the following commands:

[Click here to view code image](#)

```
$Password = ConvertTo-SecureString "Pleasdontrytobuy1,000shares" -  
AsPlainText  
-Force  
  
Get-BitLockerVolume -MountPoint G: | Enable-BitLocker -  
PasswordProtector -Password  
$Password
```

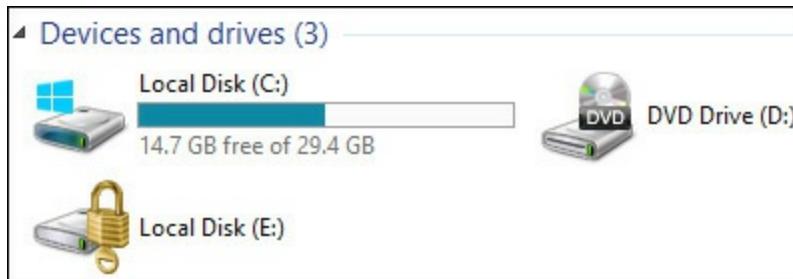
After the command, Windows begins the process of encrypting the volume. Optionally, you can use the EncryptUsedSpaceOnly parameter to decrease the initial encryption time.



### Exam Tip

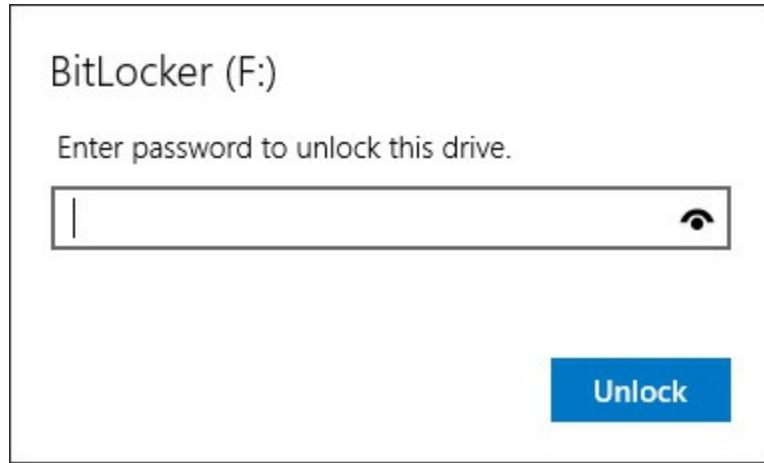
The option to encrypt an entire volume is not available for thin-provisioned volumes.

After you encrypt a volume, it is locked. When a volume is locked, you can't access it. [Figure 4-13](#) shows a locked E:\ volume. Notice the lock icon and the lack of details about the size and free space of the volume.



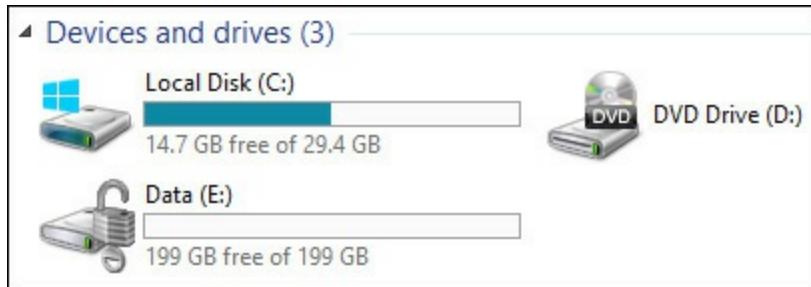
**FIGURE 4-13** A BitLocker-protected volume that is locked

If you use password protection for a BitLocker-protected volume, you are prompted for the password the first time you try to open the volume, as shown in [Figure 4-14](#).



**FIGURE 4-14** You must enter a password to unlock a BitLocker-protected volume that uses a password key protector

After you unlock a protected volume, the drive icon changes to an unlocked lock icon, as shown in [Figure 4-15](#).



**FIGURE 4-15** A BitLocker-protected volume has an unlocked lock icon to indicate that the drive is unlocked

While you can individually configure computers for BitLocker, it isn't efficient if you have a large number of computers. Instead, you should use Group Policy. Group Policy has dedicated BitLocker settings that enable you to granularly control BitLocker settings for your entire organization, or if desired, just for your servers or a subset of servers. You can specify encryption levels, protector requirements, and recovery requirements. You can also control settings based on the type of drive. For example, you can specify specific settings for fixed data drives, as shown in [Figure 4-16](#).

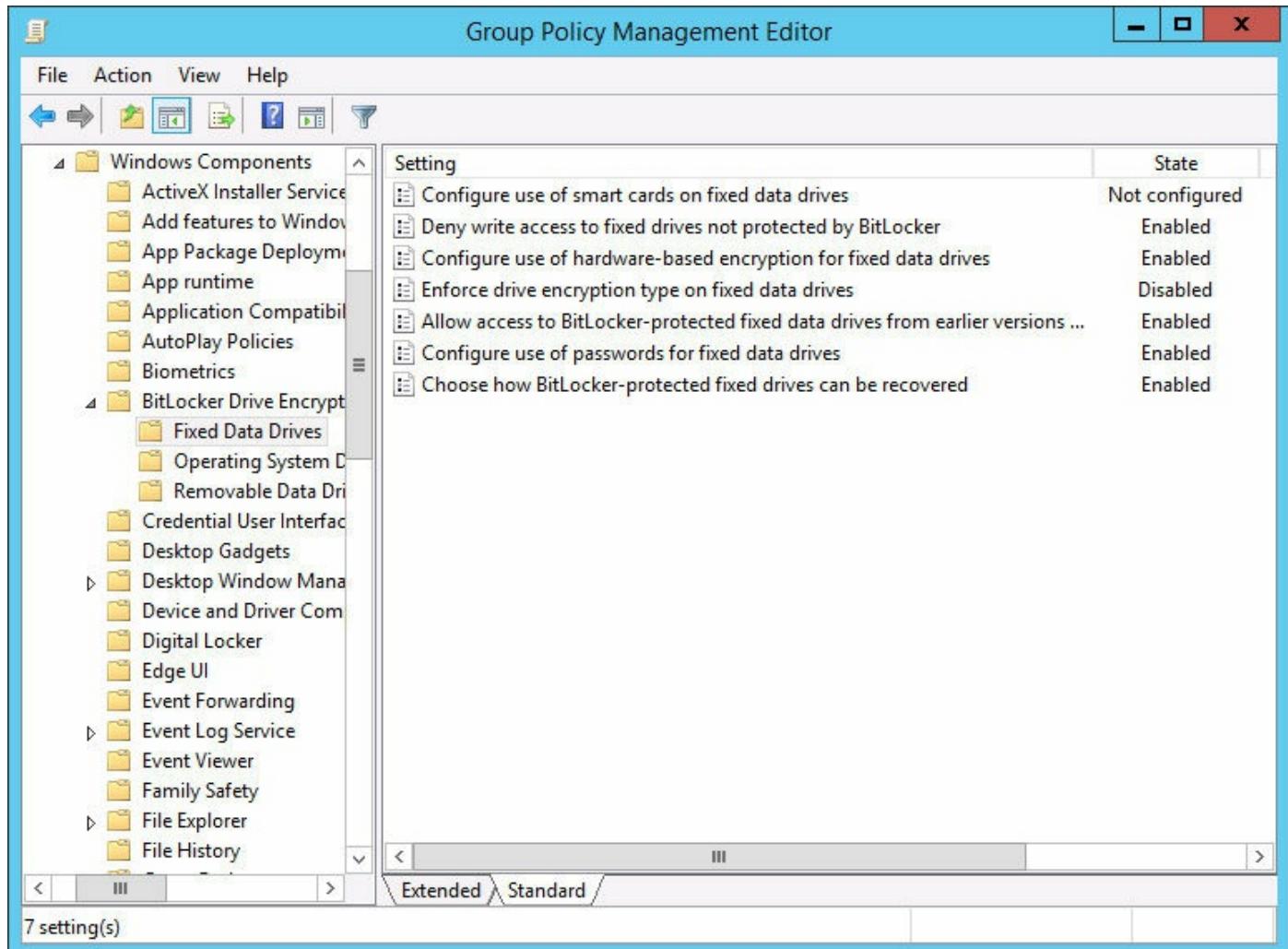


FIGURE 4-16 BitLocker GPO settings for fixed data drives

### Need More Review? BitLocker Frequently Asked Questions

For more information on BitLocker, take a look at the BitLocker Frequently Asked Questions page at [https://technet.microsoft.com/en-us/library/hh831507\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831507(v=ws.11).aspx).

## Plan and configure S/MIME

Secure/Multipurpose Internet Mail Extensions (S/MIME) enable you to communicate securely through email. There are two actions that you can take when you use S/MIME to secure email communication:

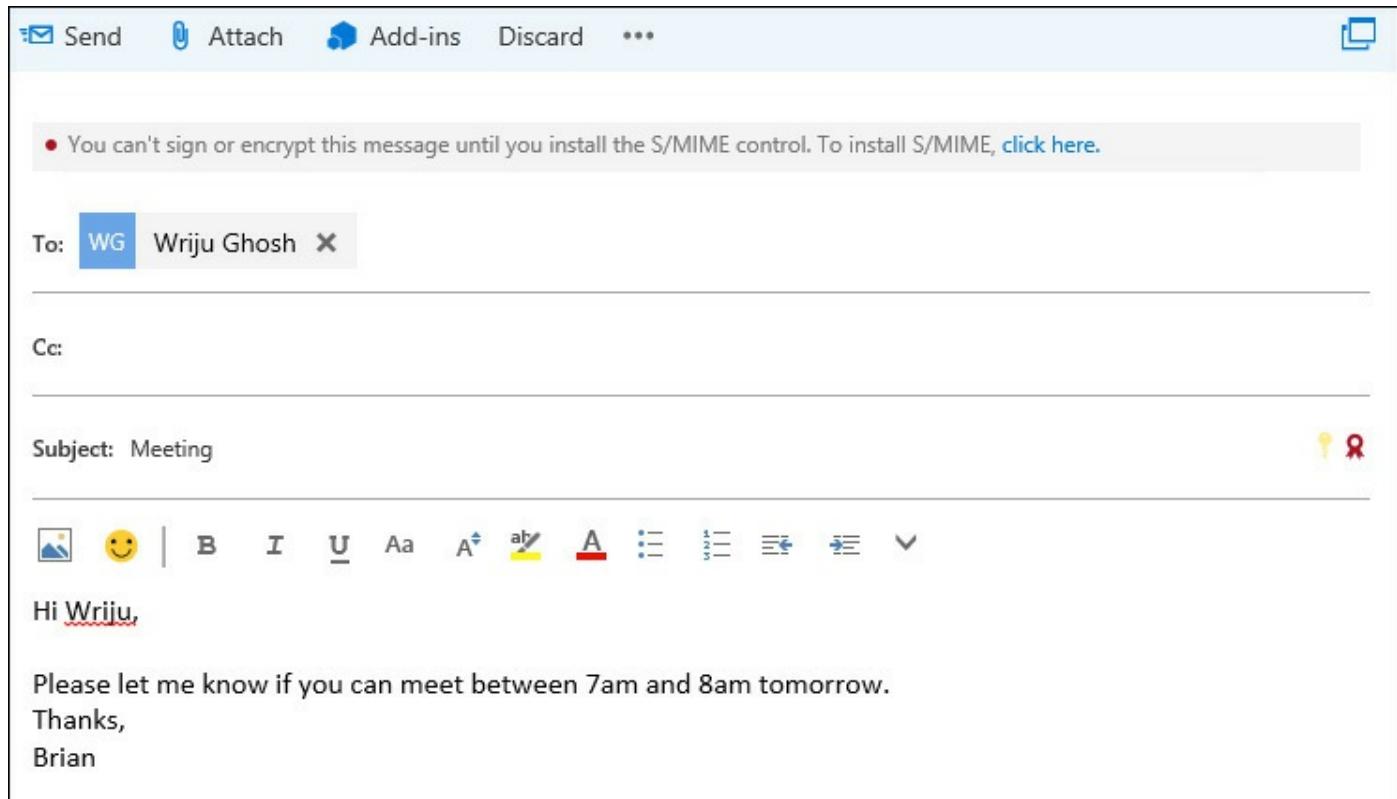
- **You can digitally sign an email message** By digitally signing an email message, you provide the following benefits to the recipient:
  - **The recipients can authenticate you as being the sender** This is referred to as message authentication.

- **The recipient knows that only you sent the email message** This is referred to as nonrepudiation.
- **The recipient knows that the original content of the email message hasn't changed since you sent it** In other words, somebody didn't intercept the email message, alter the contents, and then send it on to the recipient because that would invalidate the digital signature. This is referred to as data integrity and sometimes message integrity.
- **You can encrypt the contents of an email message** By doing so, you provide the following benefits to you and to the recipient:
  - **The email message content can only be viewed by the sender and recipient** If others attempt to access the contents of the email message, they are not able to. This is known as confidentiality.
  - **The email message has not been altered** This might seem obvious since a message cannot be viewed. This is known as data integrity, which is also provided by a digital signature.

In most situations, you digitally sign and encrypt an email. By doing so, you take advantage of the benefits of both. For the exam however, be prepared to choose one or the other based on specific requirements.

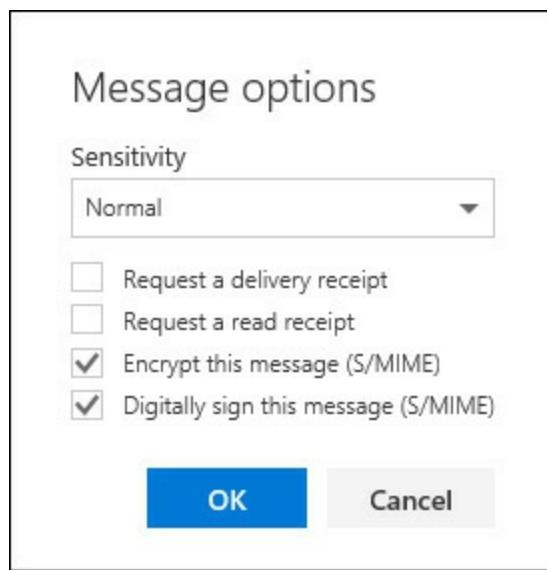
There are three primary ways to use S/MIME to secure your email communication. You should be familiar with each of these methods for the exam.

- **You can use Outlook on the web** You need to install the S/MIME control before you can use S/MIME with Outlook on the web. By default, Outlook on the web prompts you to install the control when you try to protect an email message with S/MIME or when you try to view a protected email message that you receive. In [Figure 4-17](#), Outlook on the web shows a prompt about the S/MIME control.



**FIGURE 4-17** Outlook on the web with the notification that the S/MIME control is required

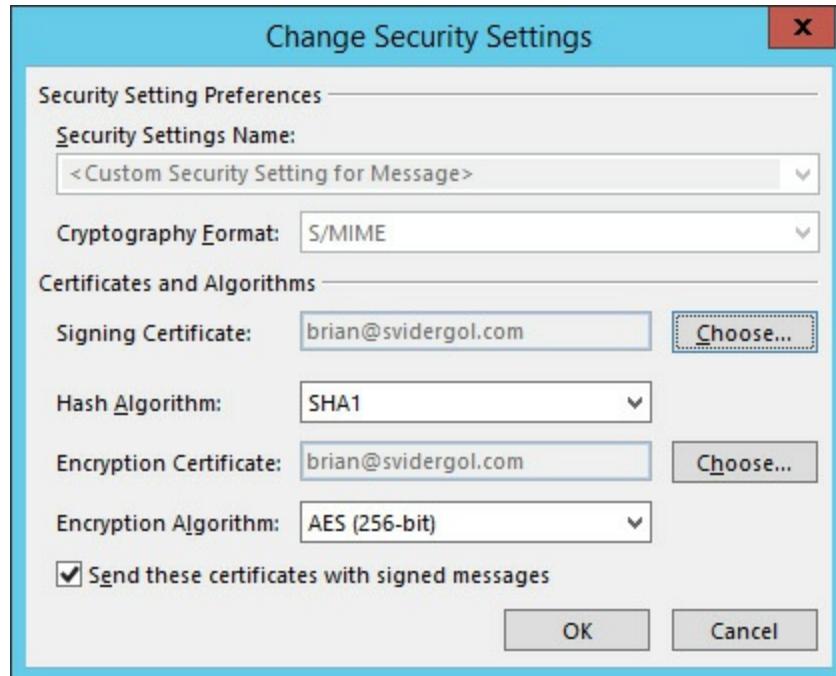
- In [Figure 4-18](#), the message options are shown for Outlook on the web.



**FIGURE 4-18** Outlook on the web with the message options including encrypting and signing

- **You can use Outlook** You need to perform the following high-level steps to enable Outlook to use S/MIME: add your certificate to your computer, digitally sign an email message in Outlook, and send it to the desired person. Have the desired person add a certificate to their computer and send you a digitally signed

message. After you receive the message, add the person as a contact in Outlook. The person also adds you as a contact when they receive your signed email. After the initial setup process, you can now sign and/or encrypt email messages to that person. [Figure 4-19](#) shows the Outlook settings which you modify to choose your certificate and certificate settings.



**FIGURE 4-19** Outlook security settings to change your certificate and certificate settings

- In [Figure 4-20](#), the properties of an email message in Outlook are shown. This is the area where you choose to sign and/or encrypt an email message.

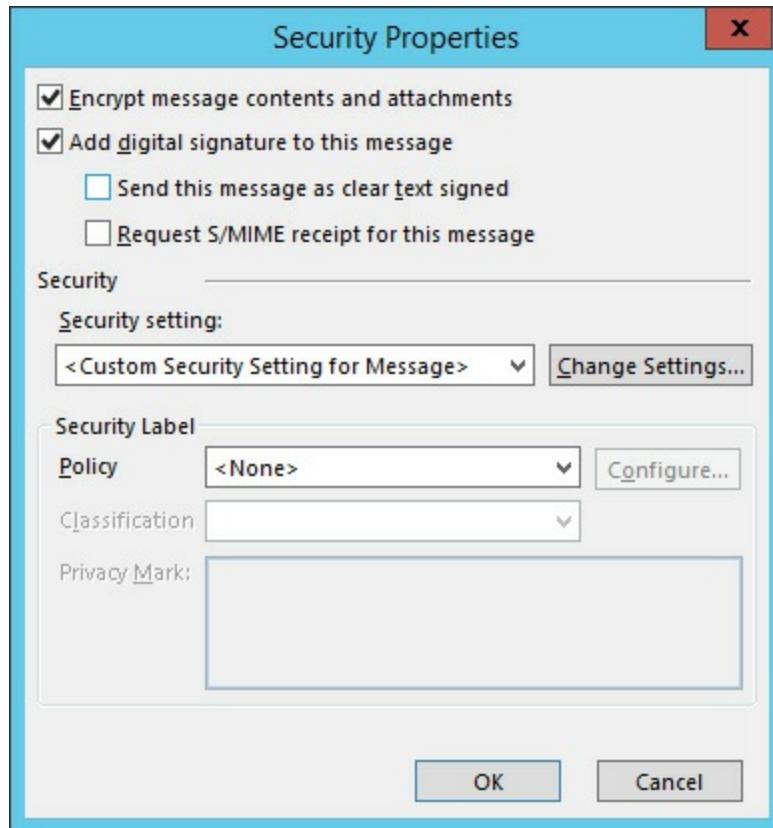


FIGURE 4-20 Outlook message security settings for signing and encrypting

- **You can use some mobile devices** Some phones and some email applications support the use of S/MIME. The setup process can vary from mobile device to mobile device and from email application to email application, but be aware that it is a feature available to many mobile devices.

Besides just knowing where and how, there are some miscellaneous points that are important to know for the exam:

- **Some mail flow rules might not work for email messages protected by S/MIME** That's because Exchange servers do not have a way to inspect the contents. If a rule requires inspecting the contents but the email message is protected by S/MIME, the rule won't work.
- **If you have Office 365, you have to perform some configuration to use S/MIME in Outlook on the Web** This isn't expected to be covered on the exam, but take a look at <https://blogs.technet.microsoft.com/exchange/2014/12/15/how-to-configure-smime-in-office-365/> for more information.

To prepare for S/MIME on the exam, you should acquire a free certificate, add it to your computer, set up Outlook for S/MIME, and then send and receive secure email messages. If you already have hands-on experience with S/MIME, reviewing the material here should be enough to prepare you for the exam.

## Summary

- When you digitally sign an email message, you ensure message authentication, nonrepudiation, and data integrity.
- When you encrypt the contents of an email message, you ensure confidentiality and data integrity.
- You can use Outlook on the web with S/MIME but you must install the S/MIME control.
- You use mail flow rules. However, if you inspect the contents of email messages with mail flow rules, you won't be able to inspect email message contents when they are protected by S/MIME.

## Skill 4.6: Plan, deploy, manage, and troubleshoot IRM

Previously you looked at S/MIME for securing email messages. In this section, you look at a different solution to secure email messages. This section reviews information for Active Directory Rights Management Services (AD RMS) and Azure Rights Management Services (Azure RMS). Both perform the same core functions and provide similar benefits, although Azure RMS has some additional capabilities on top of what AD RMS has. For the exam, you should be able to differentiate when you should use one over the other as well as know how to plan, deploy, manage, and troubleshoot both solutions.

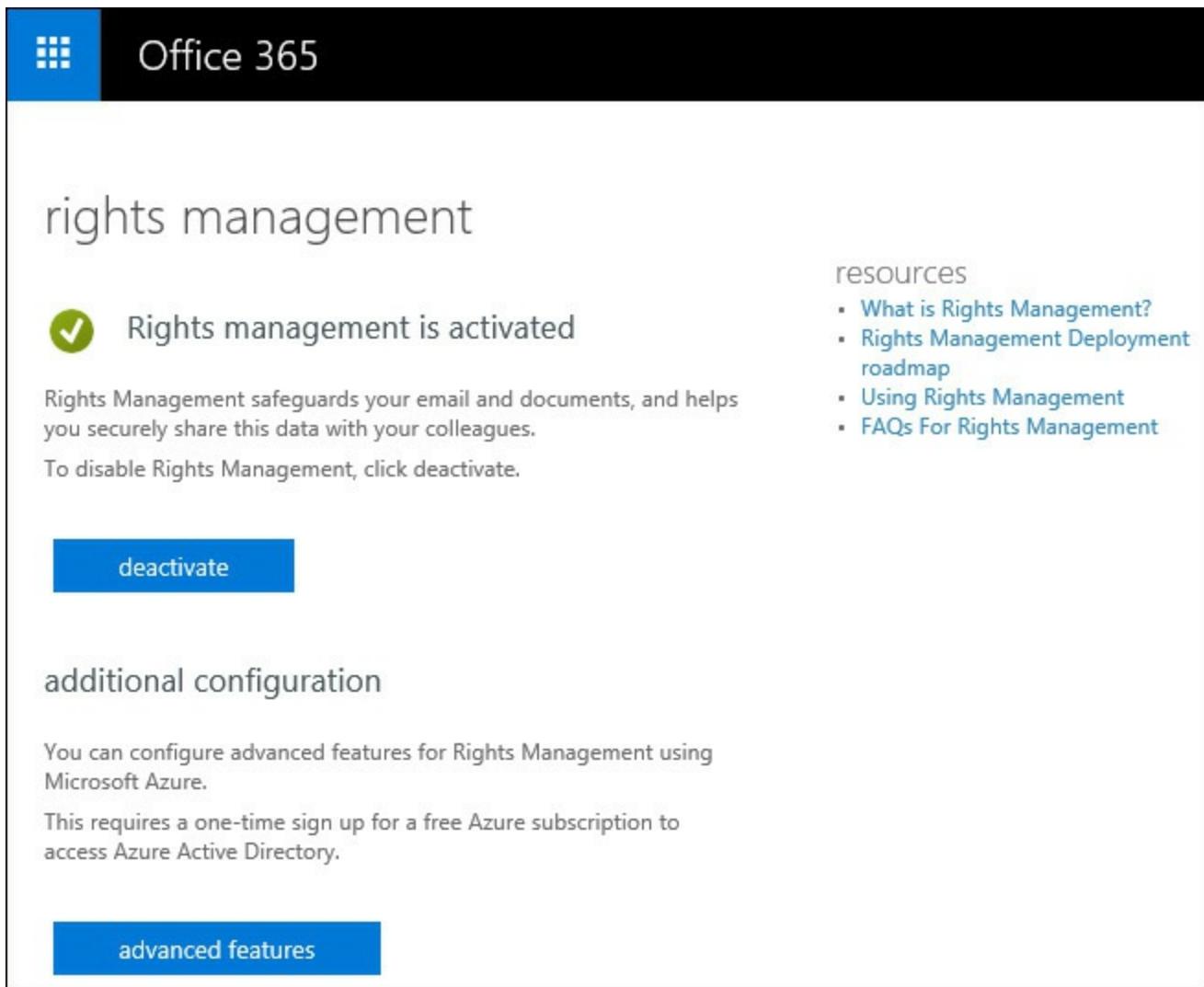
---

### This section covers how to:

- [Plan and configure Information Rights Management \(IRM\) in Exchange](#)
  - [Create an RMS template](#)
  - [Plan and create transport protection rules](#)
  - [Plan and create Outlook protection rule](#)
  - [Plan and configure journal report decryption](#)
  - [Plan and configure IRM for eDiscovery](#)
  - [Plan and configure pre-licensing for client access](#)
  - [Troubleshoot failed IRM protection](#)
-

## Plan and configure Information Rights Management (IRM) in Exchange

At the early stage of planning for IRM in Exchange, you need to consider the prerequisites for your infrastructure. For AD RMS, that means you need to have a working on-premises implementation of AD RMS and you need to integrate Exchange with it. For Azure RMS, it means that you need to have a subscription that includes Azure RMS and it needs to be activated. [Figure 4-21](#) shows Azure RMS after activation.



**FIGURE 4-21** Activated instance of Azure RMS

To integrate Exchange Server with AD RMS, perform the following high-level steps:

1. Modify the NTFS permissions for the ServerCertification.asmx file on the AD RMS server. You need to ensure that the Exchange Servers group has the Read and Execute permission and the Read permission.
2. Create an AD RMS Super Users group and enable Super Users functionality. Then, add the Federated Email mailbox to the AD RMS Super Users group. This

enables the Exchange environment to work with protected email messages and attachments.

To integrate Exchange Server with Azure RMS, perform the following high-level steps:

1. Install the Microsoft Rights Management connector. This is the service that communicates with Azure RMS for your on-premises Exchange environment.
2. Install the Microsoft Rights Management connector administration tool. This tool enables you to grant your Exchange environment access to Azure RMS.
3. Run the server configuration tool script (GenConnectorConfig.ps1) on your Exchange servers. This tool prepares Exchange Server for integration with Azure RMS. During this step, you specify the Exchange servers that are allowed to utilize the connector. This is a key step in the process. Note that the script modifies the registry on Exchange servers to point to Azure RMS.

## Create an RMS template

To improve the user experience with AD RMS and Azure RMS, you need to create templates. Templates simplify the task of protecting an email because they are pre-configured with groups or users and permissions. This means you don't have to manually select users or groups and you don't have to manually choose permissions each time you protect a document or an email message.

Use the following steps to create a new template in Azure RMS.

1. From the Azure portal, navigate to Active Directory.
2. On the Active Directory page, click the left arrow icon.
3. In the right pane, click Rights Management at the top of the page.
4. Click the name of your Rights Management instance.
5. Click Create a new rights policy template.
6. In the dialog box, select English—United States in the Language list. Type a name and description for the template and then click the check mark to complete the creation process.
7. Click Templates at the top of the page.
8. Click the name of the new template.
9. Click Get started under the Configure rights for users and groups.
10. On the Rights tab, click Get Started Now.
11. Select the users or groups that you want to configure for the template along with the desired rights, such as Viewer, Reviewer, Co-Author, Co-Owner, or Custom.

Note that groups must be mail-enabled.

**12.** Click the Configure tab in the right pane.

**13.** Click the Publish button and then click Save.

Use the following steps to create a new template in AD RMS.

**1.** Run the Active Directory Rights Management Services console.

**2.** In the left pane, expand the server's hostname and then click Rights Policy Templates.

**3.** In the right pane, click Create Distributed Rights Policy Template.

**4.** In the Create Distributed Rights Policy Template window, on the Add Template Identification Information page, click the Add button.

**5.** In the Add New Template Identification Information window, in the Name textbox, type Payroll as the name, type Payroll department template for the description and then click Add.

**6.** On the Add Template Identification Information page, click Next.

**7.** On the Add User Rights page, click the Add button. Normally you would specify the email address of a group here, but for this example, click the Anyone radio button and then click OK.

**8.** In the Rights for Anyone section, click the View checkbox and then click Next.

**9.** On the Specify Expiration Policy page, maintain the default setting so that documents do not expire. In some cases, such as when dealing with temporary data, for example a new user password that must be reset upon next sign-in, you might want to expire data. This is where you can do that. Alternatively, you can set expiration at the file level too. Click Next.

**10.** On the Specify Extended Policy page, maintain the default values so that the options are not enabled. Click Next.

**11.** On the Specify Revocation Policy page, maintain the default setting so that protected content cannot be revoked. In some situations, such as when you are distributing protected content to a large number of people, you might want to enable revocation so that you can take away a person's ability to view protected content after the content is sent to them. Click Finish.

## Plan and create transport protection rules

Transport protection rules enable you to protect email messages based on specified criteria. The protection is based off of existing templates. By default in AD RMS, there is a Do Not Forward template. In Azure RMS, by default, there is a Do Not Forward template, a confidential view only template, and a confidential template. For most environments, you need to create additional templates, especially if you plan to use transport protection rules.

To use a protection rule, perform the following high-level steps, which are valid whether you are using AD RMS or Azure RMS:

1. Create a new transport protection rule.
2. Specify a name for the rule and a condition for the rule, such as if the subject of the email message includes “\*\*\*Secure\*\*\*”.
3. Use the Apply Rights Protection To The Message With rule and select the template that you want to use.
4. Specify any exceptions.
5. Save the rule and then test it.

## Plan and create Outlook protection rule

Outlook protection rules perform a similar function as transport protection rules, they both apply protection to email messages. Outlook protection rules, which are configured on the Exchange server, apply protection to email messages before they leave the sender’s mailbox. With Transport protection rules, protection is applied in transport after email messages have left the sender’s mailbox. This is a key distinction and you should be very familiar with it for the exam. You should know how to choose between a transport protection rule and an Outlook protection rule based on a given scenario.

You can create Outlook protection rules by using the New-OutlookProtectionRule cmdlet. You can configure the protection to enable users to bypass it or not. Optionally, you can also enable users to choose a different template than specified by the Outlook protection rule.

In the following command, you create a new Outlook protection rule named Mergers which automatically protects email messages sent to [mergers@adatum.com](mailto:mergers@adatum.com) and uses the template named “Mergers and Acquisitions”:

[Click here to view code image](#)

```
New-OutlookProtectionRule -Name "Mergers" -SentTo mergers@adatum.com  
-ApplyRightsProtectionTemplate "Mergers and Acquisitions"
```

For Outlook protection rules, you can automatically protect email messages based on

the following conditions:

- **Messages sent by somebody in a specified department** For example, if anybody in the legal department sends an email, you can protect it.
- **Messages sent to specific recipients** For example, if email messages are sent to [compliance@adatum.com](mailto:compliance@adatum.com), they are automatically protected.
- **Messages sent to internal recipients or external recipients** For example, if messages are sent to internal recipients, they are automatically protected.

You can combine these conditions for more power and flexibility too.

## Plan and configure journal report decryption

If you journal email with Exchange, there is a challenge associated with dealing with encrypted email messages. In the case of S/MIME, it often means that you can't journal the email messages. In the case of AD RMS and Azure RMS, you can configure IRM-protected email messages to save an unprotected copy of IRM-protected email messages in journal reports along with the original IRM-protected email messages. You can also configure Exchange to reject email messages that it can't decrypt for journaling.

This functionality has a key prerequisite. That prerequisite is to have your federation mailboxes added to the AD RMS Super Users group. After you do that, you can use the Set-IRMConfiguration cmdlet to configure Exchange. For example, to enable transport decrypt and to enforce it so that Exchange rejects email messages that it can't decrypt, run the following command:

[Click here to view code image](#)

```
Set-IRMConfiguration -TransportDecryptionSetting Mandatory
```

If you don't want to enforce mandatory decryption, you can run the following command to just enable journal report decryption:

[Click here to view code image](#)

```
Set-IRMConfiguration -JournalReportDecryptionEnabled $true
```

Notice the different methods used for each.

## Plan and configure IRM for eDiscovery

When you have IRM in your environment, you also need to configure settings for search and eDiscovery. Otherwise, you might not be able to find protected email messages in a search. You can use the Get-IRMConfiguration cmdlet to view the current configuration for several Exchange IRM settings. [Figure 4-22](#) shows the settings.

InternalLicensingEnabled	:	False
ExternalLicensingEnabled	:	False
JournalReportDecryptionEnabled	:	True
ClientAccessServerEnabled	:	True
SearchEnabled	:	True
TransportDecryptionSetting	:	Mandatory
eDiscoverySuperUserEnabled	:	True
RMSOnlineKeySharingLocation	:	
RMSOnlineVersion	:	
ServiceLocation	:	
PublishingLocation	:	
LicensingLocation	:	<>

FIGURE 4-22 Exchange IRM settings

In [Figure 4-22](#), you can see that search and eDiscovery are both enabled. If search was disabled, you could enable it by running the following command:

[Click here to view code image](#)

```
Set-IRMConfiguration -SearchEnabled $true
```

If eDiscovery was disabled, you could enable it by running the following command:

[Click here to view code image](#)

```
Set-IRMConfiguration -EdiscoverySuperUserEnabled $true
```

One key thing about [Figure 4-22](#) is that the licensing components are not enabled. This means that IRM has not been integrated with Exchange Server yet. In such a case, you cannot protect email messages.

## Plan and configure pre-licensing for client access

Prelicensing is enabled by default. It improves performance by reducing the amount of communication between clients and AD RMS and/or Azure RMS. It also enables offline viewing of protected email messages and viewing of protected email messages in Outlook on the web. Because it is enabled by default after you configure the environment for IRM, you should be focused on troubleshooting scenarios for the exam. For example, IRM might not be enabled any longer.

## Troubleshoot failed IRM protection

While you've covered some troubleshooting-related information throughout the IRM sections, there are some key points that you need to be familiar with so you are prepared for exam scenarios around troubleshooting.

1. Is all IRM functionality broken? If so, it probably means that IRM is not enabled for internal messages. In such a scenario, you can run the `Set-IRMConfiguration -InternalLicensingEnabled $true` command to fix the problem. If internal licensing is already enabled, look at the AD RMS server to ensure that it is healthy, although this is much less likely on an Exchange exam.

2. Are some users having trouble using some templates? This is likely due to permissions issues. Check the template configuration to see which group is authorized to use the template. Compare that with the group membership of the user.
3. Are you unable to find an existing security group to use for a template? If so, it is likely because the group is not mail-enabled. Configure the group to be mail-enabled and then try again.
4. Are there sporadic issues with Azure RMS and Exchange? Check the connector configuration and ensure that all of your Exchange servers are allowed to utilize the connector.
5. Are your Exchange servers failing to locate Azure RMS? Check the registry. Look at the  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer\V15\IRM\key and ensure that a URL for [aadrm.com](#) is listed. If you don't see the IRM key, you need to configure IRM.
6. Are some mail flow rules that protect email messages with IRM failing? Check to see if the associated templates have been deleted. Be careful when deleting templates because they might be in use by mail flow rules.

## Summary

- To use Azure RMS with Exchange, you need to download and install the Microsoft Rights Management connector. For AD RMS, you don't.
- To provide an enhanced user experience, you should create templates for your organization. To specify groups that can use the templates, you must use mail-enabled groups.
- You can use transport protection rules to automatically secure email messages while they go through the transport process.
- You can use Outlook protection rules to automatically secure email messages before they leave a sender's mailbox.
- If you use IRM with Exchange, you need to plan for journal report decryption, search functionality, and eDiscovery.

## Thought experiment

You are the email administrator for your company, Alpine Ski House. Alpine Ski House is an outdoor recreational company focused on providing year-round recreational activities to mountainous areas around the world. The company is embarking on a major expansion which involves acquiring other companies and expanding into new markets. As part of the expansion, the management team has asked the IT department to begin focusing on enhancing environment security. This is in part to prevent leaks of acquisitions, but also to enhance security with expanded company visibility. Your manager asks you to focus on bringing security to the Exchange environment. He asks you to come up with solutions for the following business requirements:

- The executive management team needs to be able to communicate securely with each other via email. They want to be able to protect email so that some messages cannot be forwarded. They also want to ensure that unintended recipients of protected email messages cannot view the email contents. The solution must provide a good user experience however.
- Each member of the legal team needs to be able to communicate with some people outside of the company to confidentially discuss potential mergers and buyouts. It is imperative that the email messages cannot be read, by unauthorized people, even by members of the IT department.
- The company wants to choose a message security solution that remains on the cutting edge so that they have access to the latest enhancements. So far, the company has evaluated AD RMS and Azure RMS.

You need to recommend solutions to meet the requirements. Which solutions do you recommend?

## Thought experiment answer

When an internal team, such as the executive management team, needs to be able to communicate securely with each other via email, you can use S/MIME, AD RMS, or Azure RMS. Each meets the requirement. When you also look at the requirement to provide a good user experience and the other requirement to use a security solution that remains on the cutting edge, the answer clearly becomes Azure RMS. S/MIME does not provide a good user experience and AD RMS is an on-premises technology that is already beginning to lag behind Azure RMS in functionality.

When a team such as the legal team needs to be able to securely communicate with people outside the company and that communication must remain confidential, your best option is S/MIME. With AD RMS and Azure RMS, IT administrators can gain access to email message contents even if they are protected. They can do this by using the AD RMS Super Users group, the Azure RMS Super Users group, or by looking at

eDiscovery data. With S/MIME, however, only the sender and recipient can view protected email contents. While an administrator could reset an executive management team member's password, sign in directly to their computer to assume their identity, and read email contents, this would normally attract IT security's attention as well as the executive's attention who would no longer be able to sign in. Remember, a single security solution by itself is rarely impenetrable.

When a company wants to choose a cutting edge solution that provides the latest enhancements, the answer is usually the cloud solution. For Microsoft products, the company has announced that the latest functionality is to be put into the cloud-based products first. In some cases, the same functionality is added to the on-premises versions of the products later. In other cases, the functionality is not added to the on-premises versions of the products. In this scenario, Azure RMS is the correct choice.

# **Chapter 5. Plan, deploy, and manage compliance, archiving, eDiscovery, and auditing**

For an Exchange 2016 organization, the concept of compliance can refer to many different things. Some organizations are bound by legislation in the country/region in which they operate, while others are bound by regulations that are specific to their industry. For some organizations, the concept of compliance only relates to their own internal policies. With email being one of the primary modes of communication in businesses today, meeting your compliance requirements is an important goal. Administrators need to provide the business with a technology solution to manage the lifecycle of email, retain messages for the required period of time, search and locate mailbox contents, provide email data for investigations and legal matters, and also prevent some emails from being sent or received.

While Exchange 2016 is capable of supporting the compliance objectives of most organizations, there is no single compliance switch that can be turned on and off. Instead, compliance involves the application of multiple solutions to meet the rules, regulations, and policies that apply to email communication for the organization.

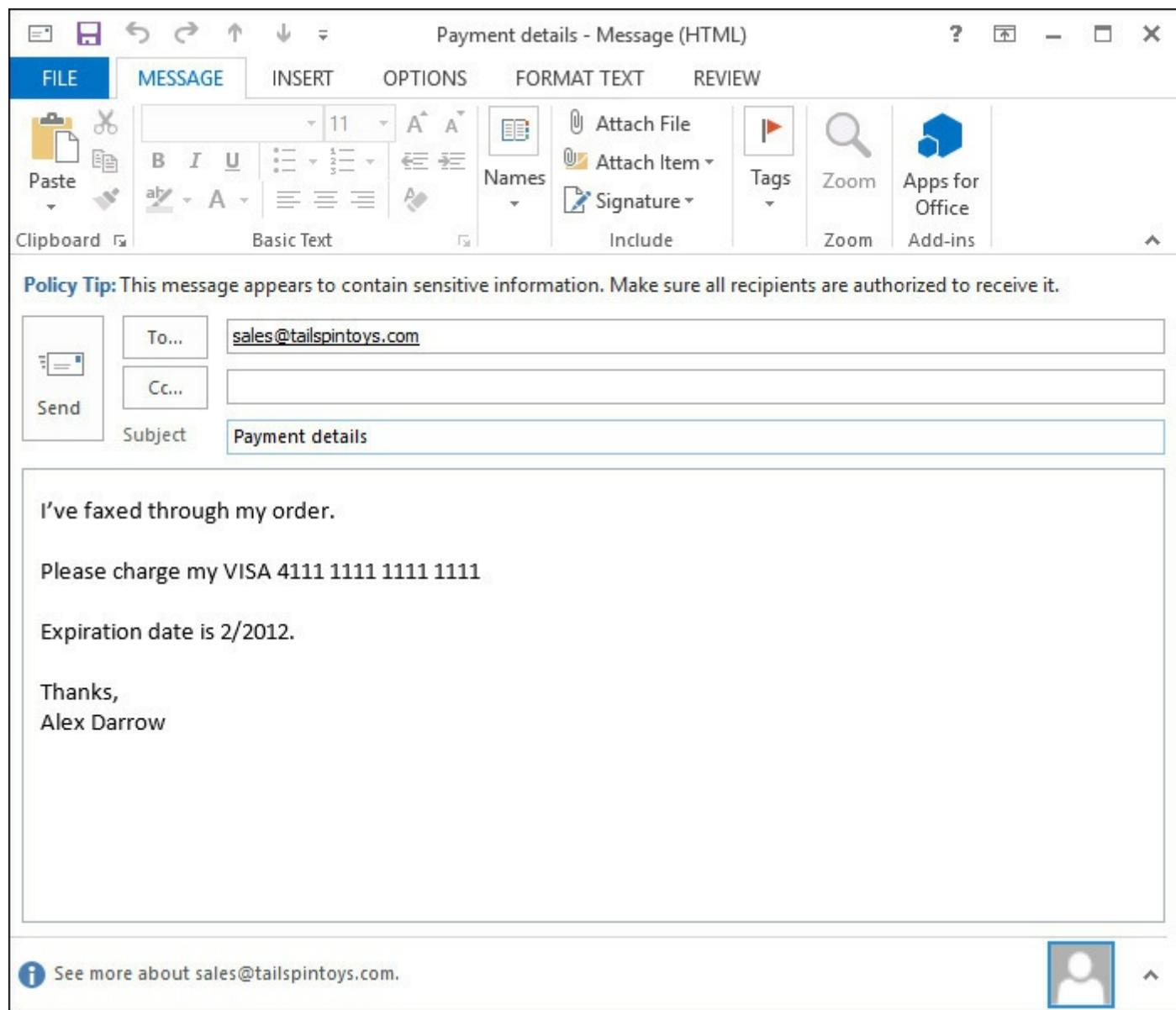
## **Skills in this chapter:**

- [Plan and configure Data Loss Prevention \(DLP\) solutions](#)
- [Plan, configure, and manage Archiving and Message Records Management \(MRM\)](#)
- [Plan, configure, and perform eDiscovery](#)
- [Plan, configure, and manage a compliance solution](#)
- [Plan, manage, and use mailbox and administrative auditing](#)

### **Skill 5.1: Plan and configure Data Loss Prevention (DLP) solutions**

Data Loss Prevention (DLP) is a compliance feature of Exchange 2016 that is designed to help your organization prevent the intentional or accidental exposure of sensitive information in emails to unwanted parties. DLP uses a content analysis engine to examine the contents of email messages and their attachments, looking for information such as social security numbers or credit card details. Such information should typically not be sent via email. If it must be transmitted by email, it might be more appropriate to protect the information with encryption to prevent accidental exposure. DLP policies can be used to either audit emails for sensitive information, present warnings to users before they send an email that might contain sensitive information, or actively block emails that are found to contain sensitive information.

Sensitive information is identified by regular expression pattern matching in combination with other evidence, such as keywords in proximity to the matching patterns. For example, credit card numbers are identified as a pattern of 16 digits. It is not simply a case of matching any string of 16 digits however. After all, the digits representing a credit card number might be a single string or separated in groups of four using spaces or hyphens. They might even be a harmless string of 16 digits that is not a credit card number at all. Therefore, to accurately detect credit card numbers, a calculation is performed to confirm that the numbers match a pattern known to come from a major credit card brand. Furthermore, the proximity of a date value that would indicate a credit card expiration date, as well as keywords such as “Visa” or “AMEX” is also considered. If the detected evidence adds up to a sufficient degree of confidence, the DLP policy takes action, such as notifying the user as shown in [Figure 5-1](#).



**FIGURE 5-1** A Policy Tip in Outlook

## Need More Review? Sensitive Information Types Inventory in Exchange 2016

DLP in Exchange 2016 includes 80 sensitive information types that can be used in DLP policies. The full list is available on TechNet at [https://technet.microsoft.com/library/jj150541\(v=exchg.160\).aspx](https://technet.microsoft.com/library/jj150541(v=exchg.160).aspx).

DLP policies are basically a package of transport rules that analyze email messages as they flow through the transport pipeline. All email messages sent and received in an organization, including between two mailboxes hosted on the same server or database, pass through the transport pipeline. By implementing DLP policies as transport rules, this ensures that every message is analyzed and handled appropriately.

### This section covers how to:

- [Plan a DLP solution to meet business requirements](#)
- [Plan and configure pre-built rules](#)
- [Plan and create custom rules](#)
- [Plan and configure custom DLP policies](#)
- [Plan and configure DLP finger printing](#)

## Plan a DLP solution to meet business requirements

Before you can implement a DLP solution, you must first understand what the business would consider a data loss incident. This involves understanding what information the business sends and receives under normal circumstances, and what information would be considered sensitive. Although it might seem obvious that data such as employee social security numbers should not be sent using email, there might be circumstances where that is considered normal. An example would be a manager emailing the human resources department with the personal details of a new hire.

Furthermore, the severity of data loss incidents changes depending on the amount of data being transmitted. A single credit card number sent from an executive to their assistant would be an inconvenience if exposed to unwanted audiences, but a Microsoft Excel spreadsheet containing the credit card numbers of thousands of customers is a serious breach that has legal and financial consequences for the business.

It is useful to determine how widespread the risk of data loss is within an organization. To that end, DLP policies can first be implemented in a testing mode, referred to as Test DLP policy without Policy Tips. This testing mode analyzes the email contents, but does not notify the user of any policy breaches or prevent the email

message from being sent. As you gain an understanding of the types of information that require protection using DLP policies, you can change the policy to testing with Policy Tips, or turn on enforcement of the policy.

Policy Tips are notification messages shown to Outlook and Outlook on the Web users while they are composing an email message to send. DLP analyzes the message while it is being composed to warn the user or prevent the message from being sent. When a DLP policy rule is configured to use Policy Tips, one of five actions can be taken:

- **Notify the sender, but allow them to send** The sender sees a notification message in Outlook or Outlook on the Web, unless they have turned off the option in their Outlook settings. This setting is called NotifyOnly when using the PowerShell cmdlets for transport rules.
- **Block the message** A message is displayed to the sender that they are not able to send the email message until they have resolved the condition that caused the DLP policy to be triggered. This setting is called RejectMessage in PowerShell.
- **Block the message, unless it's a false positive** Similar to blocking the message, however the user is able to override the block by flagging it as a false positive. The user sends the message without making any changes to its content and the Exchange server delivers it. This setting is called RejectUnlessFalsePositiveOverride in PowerShell.
- **Block the message, but allow the sender to override and send** Similar to blocking the message, however the user is able to indicate that they want to override the policy and send the message anyway. This setting is called RejectUnlessSilentOverride in PowerShell, because the user is not required to provide any reason for the override.
- **Block the Message, but allow the sender to override with a business justification and send** Similar to the previous action, but the user is required to provide a reason justifying why they are overriding the policy. The business justification is included in logs, as well as incident reports if the rule is configured to send one. This setting is called RejectUnlessExplicitOverride in PowerShell.

By combining the content analysis capabilities of DLP policies with Policy Tips to alert users to the possible consequences of their actions, you can strike the balance between user education and policy enforcement so that the risks of data loss can be reduced without applying excessive restrictions to your users' ability to communicate via email.

## Plan and configure pre-built rules

Exchange 2016 includes 40 pre-built DLP policies, suitable for detecting sensitive information types such as financial data, health information, and personal identification numbers. You can view the full list of DLP policy templates by running the Get-DlpPolicyTemplate cmdlet, as shown in [Listing 5-1](#).

### LISTING 5-1 DLP Policy Templates

[Click here to view code image](#)

---

```
#Viewing the list of DLP policy templates using PowerShell

[PS] C:\>Get-DlpPolicyTemplate | Select Name

Name
-----
Australia Financial Data
Australia Health Records Act (HRIP Act)
Australia Personally Identifiable Information (PII) Data
Australia Privacy Act
Canada Financial Data
Canada Health Information Act (HIA)
Canada Personal Health Act (PHIPA) - Ontario
Canada Personal Health Information Act (PHIA) - Manitoba
Canada Personal Information Protection Act (PIPA)
Canada Personal Information Protection Act (PIPEDA)
Canada Personally Identifiable Information (PII) Data
France Data Protection Act
France Financial Data
France Personally Identifiable Information (PII) Data
Germany Financial Data
Germany Personally Identifiable Information (PII) Data
Israel Financial Data
Israel Personally Identifiable Information (PII) Data
Israel Protection of Privacy
Japan Financial Data
Japan Personally Identifiable Information (PII) Data
Japan Protection of Personal Information
PCI Data Security Standard (PCI DSS)
Saudi Arabia - Anti-Cyber Crime Law
Saudi Arabia Financial Data
Saudi Arabia Personally Identifiable Information (PII) Data
U.K. Access to Medical Reports Act
U.K. Data Protection Act
U.K. Financial Data
U.K. Personal Information Online Code of Practice (PIOCP)
U.K. Personally Identifiable Information (PII) Data
U.K. Privacy and Electronic Communications Regulations
U.S. Federal Trade Commission (FTC) Consumer Rules
U.S. Financial Data
```

U.S. Gramm-Leach-Bliley Act (GLBA)  
U.S. Health Insurance Act (HIPAA)  
U.S. Patriot Act  
U.S. Personally Identifiable Information (PII) Data  
U.S. State Breach Notification Laws  
U.S. State Social Security Number Confidentiality Laws

---

Managing DLP policies can be complex and is best performed using the Exchange admin center. Navigate to the compliance management section, and select data loss prevention. Click the icon to create a new DLP policy and choose New DLP policy from template. Give the new policy a name and choose the template that you want to implement, such as U.S. Financial Data. The new DLP policy is created and defaults to a mode of Testing without Policy Tips. The same outcome is achieved by running the New-DlpPolicy cmdlet in PowerShell. When using PowerShell, the policy mode can be specified by using the Mode parameter with one of three values:

- **Audit** This is the same as Testing without Policy Tips in the Exchange admin center.
- **AuditAndNotify** This is the same as Testing with Policy Tips in the Exchange admin center.
- **Enforce** This is the same as Enforce in the Exchange admin center.

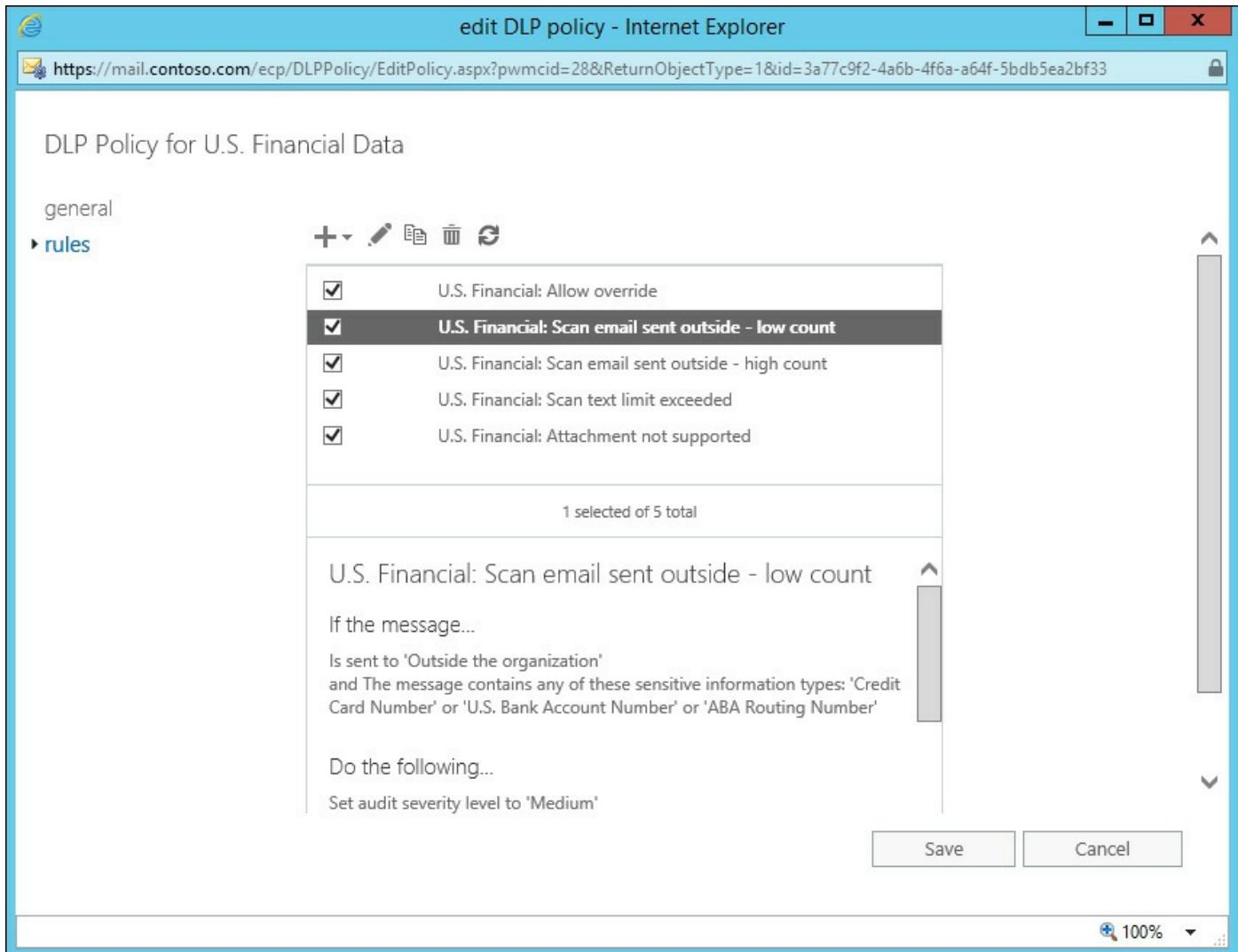
[Click here to view code image](#)

#Creating a new DLP policy from a template in PowerShell

```
[PS] C:\>New-DlpPolicy -Name "My DLP Policy" -Template "U.S. Financial Data" -Mode Audit
```

The new DLP policy automatically creates the associated transport rules. In the example of U.S Financial Data, there are five rules created. The rules can be viewed in the properties of the DLP policy or by navigating to mail flow in the Exchange admin center and selecting rules, as shown in [Figure 5-2](#). Each rule that is created by a DLP policy template applies to one or more sensitive information types. For example, the U.S. Financial Data policy template includes the following sensitive information types:

- Credit card number
- U.S. bank account number
- ABA routing number



**FIGURE 5-2** DLP policy rules

Two rules in the DLP policy for U.S. Financial Data are triggered depending on the number of instances of sensitive information found. The low count rule is triggered for between one and nine instances of matching data, and notifies the sender with a Policy Tip but allows the email message to be sent. The high count rule is triggered if 10 or more instances of matching data are found and notifies the sender with a Policy Tip and blocks the message, but allows the sender to override by providing a business justification.

Each of the transport rules are also set to a mode that matches the DLP policy. You can change the mode for each rule individually, or change the mode for the entire DLP policy to update all associated transport rules. In the data loss prevention section, highlight the policy and click the link to change the policy mode to Enforce. When a user now tries to send an email containing a high count of sensitive data, such as a CSV file containing a list of 10 or more credit card numbers, the Policy Tip warns the user that the email is blocked unless they override the policy, as shown in [Figure 5-3](#).

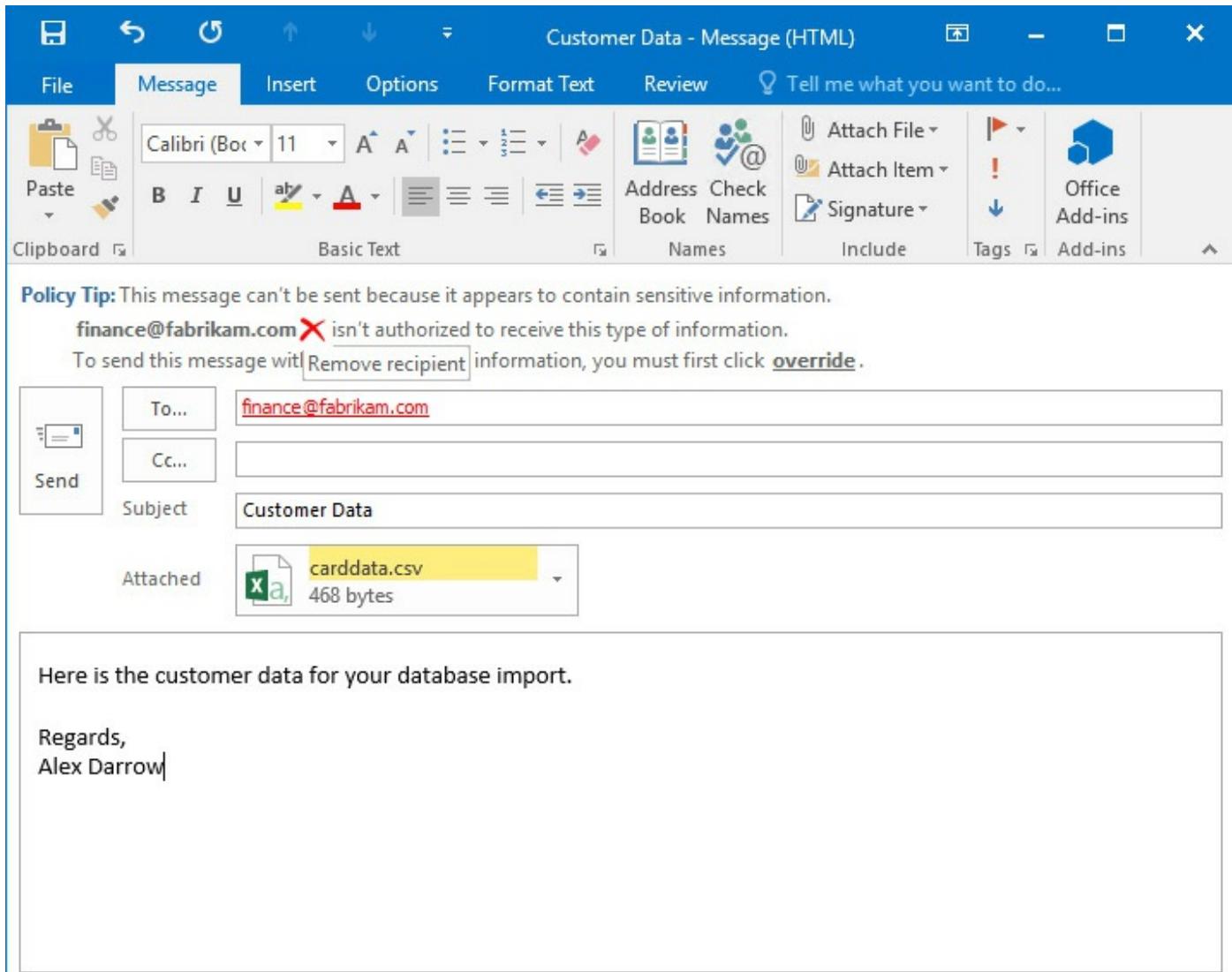


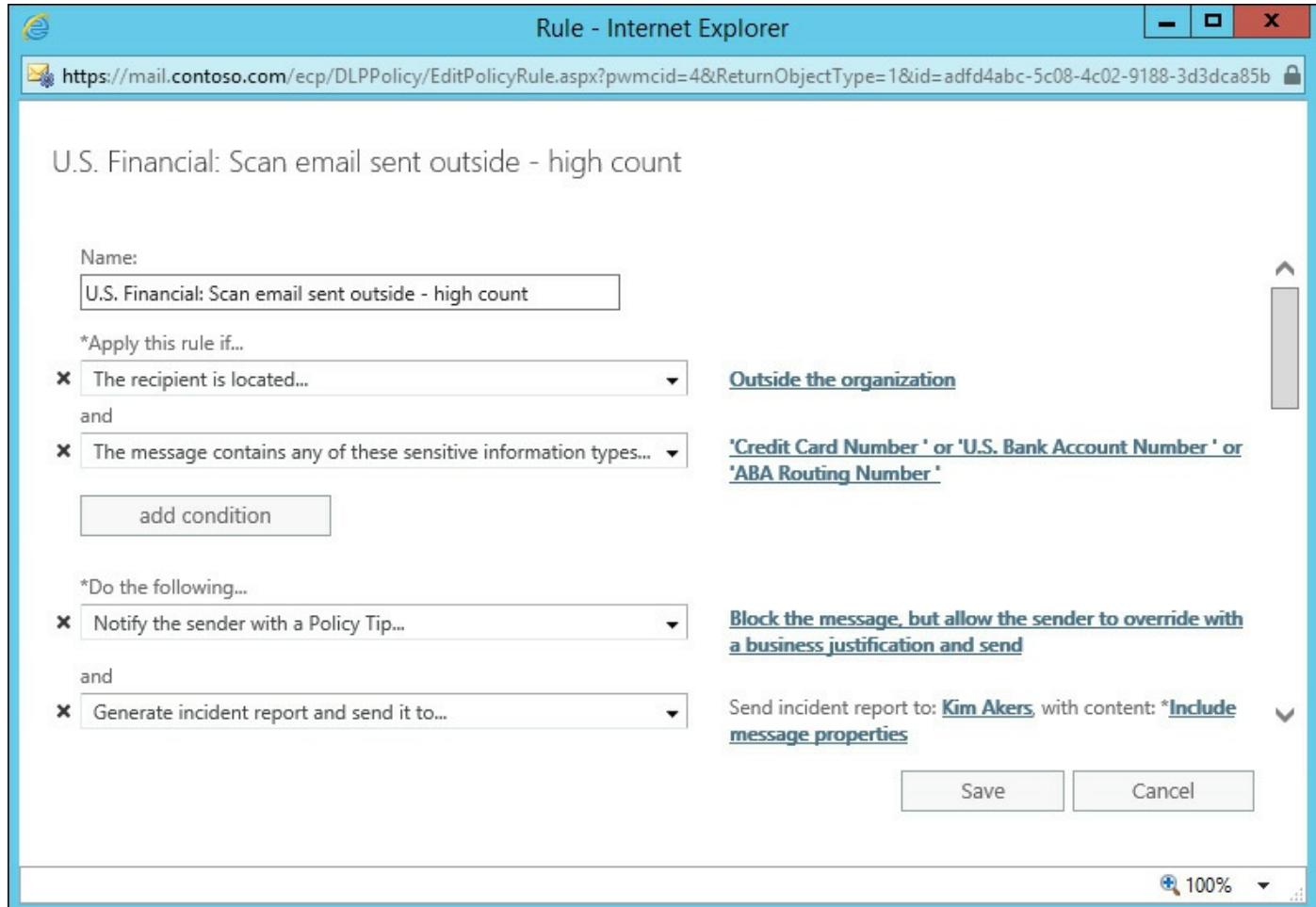
FIGURE 5-3 Overriding a DLP policy

## Plan and create custom rules

A DLP policy is a set of rules. In many cases, the rules that are created by a DLP policy template are suitable for an organization's compliance requirements. In some cases, however, an organization might have slightly different requirements than what the DLP policy template implements. In such cases, it is often more efficient to modify the rules that are created by the DLP policy template, than build your own custom rules or policies from scratch.

The transport rules for a DLP policy can be modified from either the properties of the policy itself, or from the rules area of the Exchange admin center that is found in the mail flow section. The customizations depend on your business requirements. For example, the DLP policy for U.S. Financial Data blocks emails containing 10 or more credit card numbers, but allows the sender to override. The Internal Audit department might want to be notified each time someone overrides the DLP policy and sends a high

amount of credit card numbers outside the organization. In that case, the high count rule in the DLP policy can be modified with an additional action to generate an incident report to a nominated recipient, as shown in [Figure 5-4](#).



**FIGURE 5-4** Customizing a DLP policy rule

In this example, the sender sees a Policy Tip and can override the DLP policy, providing a business justification for their decision. The incident report is sent to the nominated recipient and includes a copy of the email that was sent, as well as metadata about the DLP policy and the business justification that was provided by the sender.

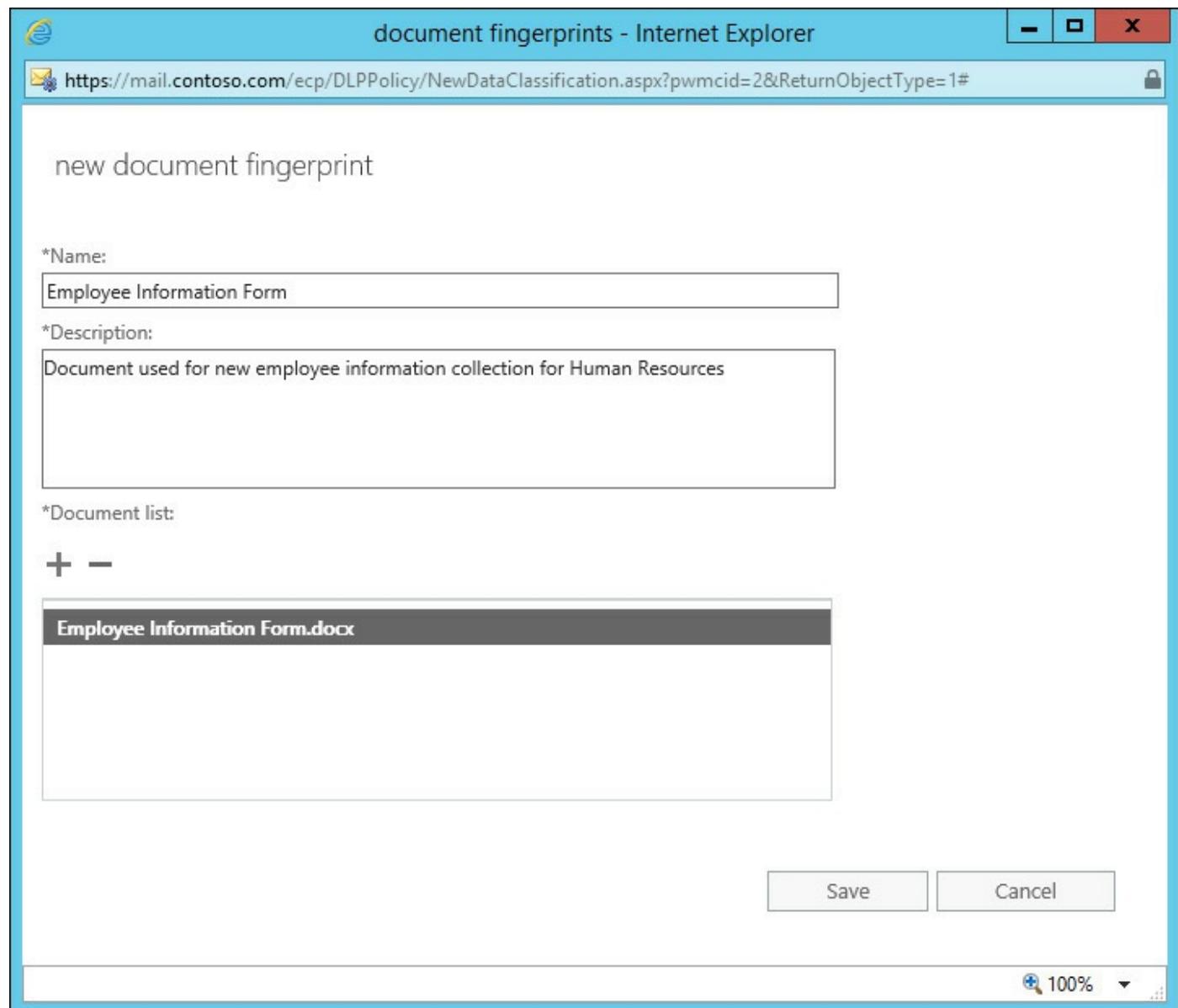
## Plan and configure DLP fingerprinting

Despite the broad range of sensitive information types that Exchange 2016 is capable of detecting, there are often situations within a company where sensitive data unique to that organization also needs protecting with DLP. An example that would be found in many environments is an employee information form sent by a manager to the Human Resources department when a new hire is made. Typically, such a form contains sensitive personal information about the new employee that should not be exposed to unauthorized people inside or outside of the organization for privacy reasons.

The solution that DLP provides is called fingerprinting. Forms or document, such as

the employee information form used in this example, are uploaded to the Exchange server for analysis. The document itself is not stored in Exchange, only the hash value, or fingerprint, that was calculated that represents the document. The fingerprint is then used as the sensitive information type for one or more DLP policy rules.

To create a new document fingerprint, navigate to the compliance management section of the Exchange admin center, and in the data loss prevention area select Manage Document Fingerprints. Add a new fingerprint, providing a name and description for the document type, and upload a file that represent the document that is to be fingerprinted, as shown in [Figure 5-5](#).



**FIGURE 5-5** Creating a new document fingerprint for DLP

## Need More Review? Supported File Types for DLP Fingerprinting

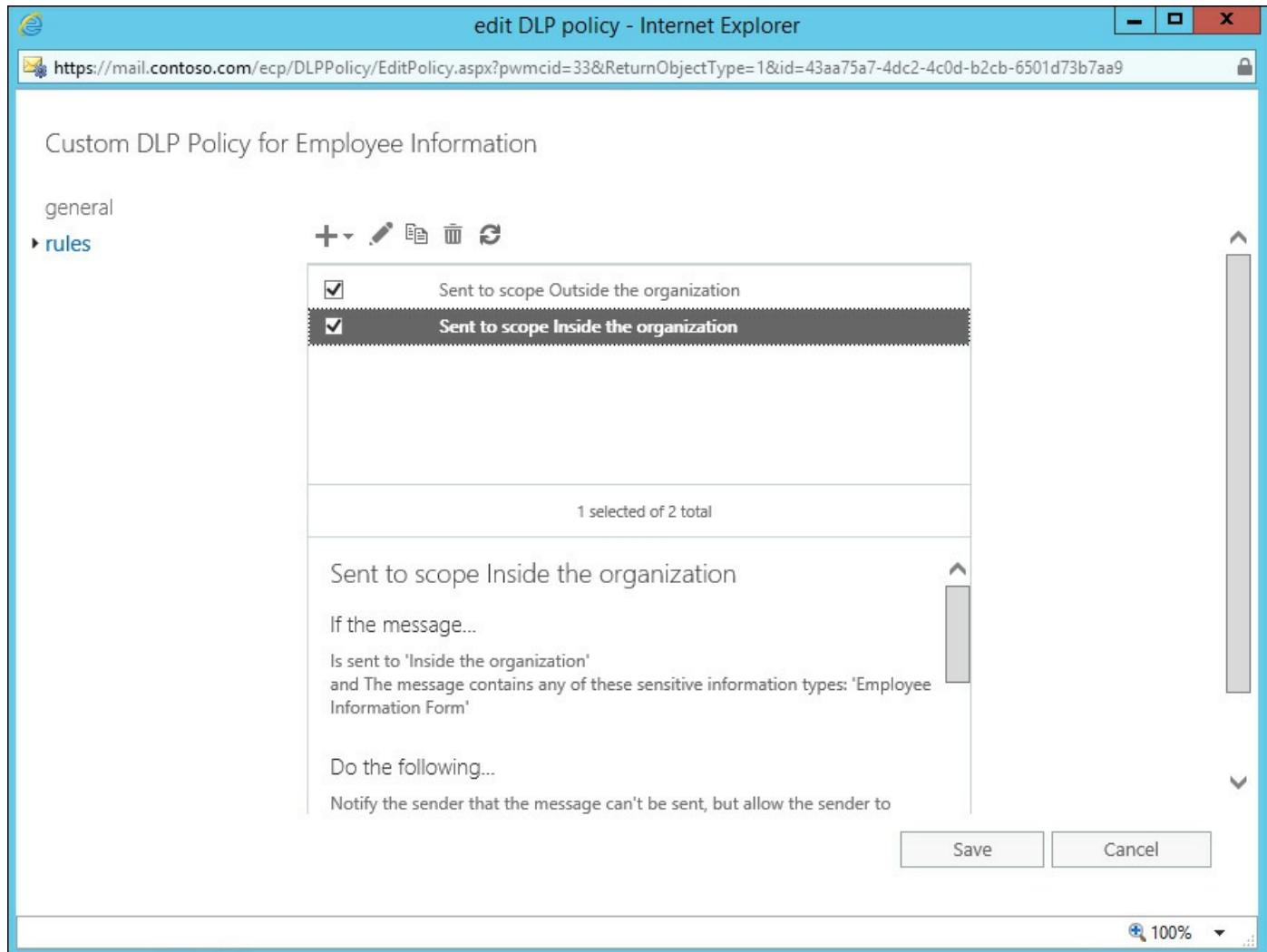
DLP fingerprinting supports the same file types supported for transport rules that inspect the contents of email attachments. The full list of supported file types is available on TechNet at [https://technet.microsoft.com/library/jj919236\(v=exchg.160\).aspx](https://technet.microsoft.com/library/jj919236(v=exchg.160).aspx).

## Plan and configure custom DLP policies

Since a DLP policy is essentially a set of transport rules, you can bundle your own rules into a single policy. An advantage of combining multiple rules into a single policy, instead of managing them individually as transport rules, is that you can change the mode for all of the rules in the policy together.

Navigate to the compliance management section, and select data loss prevention. Click the icon to create a new DLP policy, and choose New Custom DLP Policy. At this stage you can give the custom DLP policy a name, description, choose whether to enable or disable it, and also set the initial policy mode such as Test DLP policy with Policy Tips. After creating the custom DLP policy, open the properties of the policy and select the rules section. You can construct your set of DLP policy rules here. Keeping with the example of employee personal information used in the previous section, a set of rules such as those shown in [Figure 5-6](#) can be created to:

- Block emails to external recipients that contain the employee information form that was fingerprinted, and display a Policy Tip with no option to override.
- Block emails to internal recipients that contain the employee information form, unless the sender overrides the Policy Tip and provides a business justification, or the recipient is the Human Resources mailbox.



**FIGURE 5-6 Adding rules to a custom DLP policy**

### Note: Outlook Awareness of DLP Policies

In your own testing of DLP policies, if you want to see immediate results it is necessary to force Outlook to update its cache of DLP policy information, which is otherwise updated once every 24 hours. To force an update, delete the `LastDownloadTimesPerAccount` registry entry for the version of Outlook that you're running, such as 15.0 (2013) or 16.0 (2016). The steps for Outlook 2013 are provided on the Microsoft Support site at, <https://support.microsoft.com/en-us/kb/2823261>.

## Summary

- DLP policies are packages of transport rules that, when combined with the ability to perform deep content inspection of email messages and attachments, allows you to control the dissemination of sensitive information via email.

- DLP policies can be tested, with or without Policy Tips that are visible to the user, before they are enforced. Incident reports can be used to alert administrators to DLP policy events such as a sender overriding a policy.
- Custom DLP policies can be built to suit almost any data loss prevention requirement that an organization has, including detection of sensitive information that is unique to the organization through the use of document fingerprinting.

## **Skill 5.2: Plan, configure, and manage Archiving and Message Records Management (MRM)**

Message Records Management (MRM) is the term that encompasses all of the features of Exchange 2016 that can be used in combination with each other to manage the retention of mailbox data. Retention of mailbox data is important for many organizations to meet their compliance requirements, with the goal of ensuring that any data required for an investigation or legal matter is available without needing to recover data from backups. Retention can also mean the removal of data that is no longer required, or that is considered a risk to the organization, whether that risk is legal, financial, or simply a capacity management issue. In short, the goal of MRM is to keep the data you need, for as long as you need it, and no longer than necessary.

The archiving and retention features of Exchange 2016 provide part of the overall MRM solution for an organization. Retention policies in Exchange 2016 are not actually capable of guaranteeing that users do not delete data. That is a common misconception, most likely due to the slightly misleading term “retention”. In fact, preserving mailbox data is the role of In-Place Hold or Litigation Hold, not the role of retention policies.

---

### **This section covers how to:**

- [Plan and configure archive and retention policies](#)
  - [Plan, create, and configure custom tags](#)
  - [Assign policies to users](#)
  - [Plan and configure the Managed Folder Assistant](#)
  - [Remove and delete tags](#)
  - [Plan and configure in-place archiving](#)
  - [Plan and configure online archiving \(Office 365\)](#)
-

## Plan and configure archive and retention policies

Retention policies are assigned to mailboxes to manage the archiving or removal of mailbox data in accordance with your organization's retention goals. Although the terms "archive policy" and "retention policy" might sound like two separate things, both actions are managed using retention policies. A retention policy is a collection of retention tags. Retention tags are used to apply retention settings to individual folders and items within the mailbox. There are three types of retention tags that can be created in Exchange 2016:

- **Default policy tags** Applies to any folders or items in a mailbox that don't have a retention policy tag or a personal tag applied to them. A retention policy can have a maximum of one default policy tag of each action type. Users can't change the default policy tag for their mailbox, but they can choose a different personal tag for items or folders.
- **Retention policy tags** Applies to default mailbox folders such as the Inbox, Sent Items, or Deleted Items folder. Users can't change a retention policy tag on a mailbox folder to a different personal tag. Because the only retention actions for retention policy tags are to delete and allow recovery, or permanently delete, you should apply them with caution.
- **Personal tags** Manually applied to items and folders by the mailbox user. There is no limit to the number of personal tags that can be included in a retention policy, however, too many tags to choose from becomes confusing for your users.

Each tag defines the action that should be taken for that folder or item, and how much time should pass before the action should be triggered, which is referred to as the retention period. The available actions for retention tags are:

- **Move to archive** The item is moved to the user's archive mailbox, if they have one, after the retention period has lapsed. If the mailbox is not archive-enabled, no action is taken. Move to archive is possible for default policy tags and personal tags, but not for retention policy tags.
- **Delete and allow recovery** The item is moved to the user's recoverable deleted items folder after the retention period has lapsed. When the item is in the recoverable deleted items, it is subject to the deleted item retention period configured for the database or mailbox, before it is permanently purged from the database.
- **Permanently delete** The item is deleted when the retention period has lapsed, and can't be recovered from the recoverable deleted items folder. If the mailbox or items are subject to an In-Place Hold or Litigation Hold, they are preserved in the recoverable items folder for the mailbox for the duration of that hold.

Each retention tag is also configured with a retention period as a number of days. The retention period is the time after which the retention action is applied to any mailbox items that are stamped with that retention tag. The retention period can be set to “Never,” which means that the retention action is never applied to items with that retention tag.

With such a potentially confusing array of terminology, it’s worthwhile taking a look at the default retention policy that exists in an Exchange 2016 organization, which is named Default MRM Policy. The Default MRM Policy contains the retention tags shown in [Table 5-1](#). A variety of personal tags are present, as well as one default policy tag. Furthermore, there is a retention policy tag for the Recoverable Items folder.

Name	Type	Retention Period	Retention Action
1 Month Delete	Personal	30 days	Delete
1 Week Delete	Personal	7 days	Delete
1 Year Delete	Personal	365 days	Delete
5 Year Delete	Personal	1825 days	Delete
Default 2 year move to archive	Default	730 days	Archive
Never Delete	Personal	Unlimited	Delete
Personal 1 year move to archive	Personal	365 days	Archive
Personal 5 year move to archive	Personal	1825 days	Archive
Personal never move to archive	Personal	Unlimited	Archive
Recoverable Items 14 days	Recoverable Items Folder	14 days	Archive

TABLE 5-1 The retention tags for the default retention policy

The Default MRM Policy, when assigned to a mailbox user, provides a lot of flexibility to the user through the use of multiple personal tags. If the user does not assign any of the available personal tags to items or folders however, the net effect of the Default MRM Policy is that items are moved to the archive mailbox after two years.

The Default MRM Policy is assigned automatically to a mailbox when it is archive-enabled, unless another policy is specified instead or another policy is applied to the mailbox at a later time. Organizations can create multiple retention policies to suit different business requirements. For example, an education institute can use a retention policy for students that removes mailbox items after 4 years, and a separate retention policy for staff that removes mailbox items after 7 years. Retention policies can be created and modified in the Exchange admin center by navigating to the compliance management section, and choosing retention policies. Retention policies can also be

created using the New-RetentionPolicy cmdlet.

[Click here to view code image](#)

```
#Creating a new retention policy in PowerShell
```

```
[PS] C:\>New-RetentionPolicy -Name "Custom MRM Policy"
```

When you create a new policy, it is not mandatory to add any retention tags to the policy. If a retention policy containing no tags is assigned to a mailbox, the effect is that no items are stamped with new retention tags when the policy is processed, and therefore no changes occur on the mailbox items.

## Plan, create, and configure custom tags

In addition to the retention tags that are pre-configured in Exchange 2016 and included in the Default MRM Policy, you can create your own custom tags and assign them to retention policies. Although the same retention tag can be included in multiple retention policies, you should try to avoid creating a large number of policies containing the same tags, for the simple reason that more policies increases the complexity of managing your overall environment.

New retention tags can be created in the compliance management section of the Exchange admin center, or by running the New-RetentionPolicyTag cmdlet. The name of the cmdlet provides an example of one of the many confusing elements of Exchange 2016 retention policies. Even though the cmdlet is named New-RetentionPolicyTag, it is used to create all types of retention tags, including default policy tags, personal tags, and retention policy tags, not just “retention policy tags”. When you create a new retention tag using New-RetentionPolicyTag, you use the Type parameter to specify which type of tag you’re creating. Default policy tags have a type of “All”, and personal tags have a type of “Personal.” For retention policy tags, the Type parameter is used to specify which default mailbox folder the tag applies to, with one of the following values:

- Calendar
- Contacts
- DeletedItems
- Drafts
- Inbox
- JunkEmail
- Journal
- Notes
- Outbox

- SentItems
- Tasks
- RecoverableItems
- RssSubscriptions
- SyncIssues
- ConversationHistory

For example, to create a default policy tag that moves items to the archive mailbox after 1 year, use the following command.

[Click here to view code image](#)

```
#Creating a 1-year archive retention tag in PowerShell
```

```
[PS] C:\>New-RetentionPolicyTag -Name DPT-Archive-1Year -Type All -  
AgeLimitForRetention  
365 -RetentionAction MoveToArchive
```

As a similar example, to create a default policy tag that deletes items after 7 years, use the following command.

[Click here to view code image](#)

```
#Creating a 7-year deletion retention tag in PowerShell
```

```
[PS] C:\>New-RetentionPolicyTag -Name DPT-Delete-7Years -Type All -  
AgeLimitForRetention  
2557 -RetentionAction DeleteAndAllowRecovery
```

There is one special case for default policy tags, and that is to create a tag that applies to voicemail messages that are created by the Unified Messaging service in Exchange 2016. If your organization has a need to apply a different retention period to voicemail messages, create a default policy tag that applies to the Voicemail message class.

[Click here to view code image](#)

```
#Creating a voicemail message retention tag in PowerShell
```

```
[PS] C:\>New-RetentionPolicyTag -Name DPT-VoicemailDelete-30Days -Type All  
-MessageClass  
Voicemail -AgeLimitForRetention 30 -RetentionAction DeleteAndAllowRecovery
```

## Note: Naming Retention Tags

The name of retention tags has no bearing on the retention period or retention action that the tag uses. Retention tag names are visible to users however, so it is helpful if they accurately describe what the tag does. In the aforementioned example, the name of the retention tags uses the prefix DPT for default policy tag, and then keywords to describe the retention action and retention period.

The retention tags can then be added to an existing retention policy by editing the properties of the policy in the Exchange admin center, or by running the Set-RetentionPolicy cmdlet with the RetentionPolicyTagLinks parameter.

[Click here to view code image](#)

```
#Configuring the retention tags for a retention policy
```

```
[PS] C:\>Set-RetentionPolicy -Identity "Custom MRM Policy" -  
RetentionPolicyTagLinks  
"DPT-Archive-1Year", "DPT-Delete-7Years"
```

The RetentionPolicyTagLinks parameter of Set-RetentionPolicy sets the retention tags for the policy, however it overwrites the existing setting instead of adding to it. This means that when you want to make an addition to the retention tags for a retention policy, you must include all of the tags in your command. To avoid retyping every tag name in your command, you can use the following PowerShell technique to first capture the names of the existing tags in the policy to a collection, add the new tag names to the collection, and then apply the new list of tags to the policy, as demonstrated in [Listing 5-2](#). Often it is simpler to manage the tags for a retention policy in the Exchange admin center.

**LISTING 5-2** Adding retention tags to an existing retention policy without overwriting existing tags

[Click here to view code image](#)

```
[PS] C:\>$tags = @(Get-RetentionPolicy -Identity "Custom MRM Policy").  
RetentionPolicyTagLinks.Name  
  
[PS] C:\>$tags += "DPT-VoiceMailDelete-30Days"  
[PS] C:\>$tags += "1 Month Delete"  
[PS] C:\>$tags += "Never Delete"  
  
[PS] C:\>Set-RetentionPolicy -Identity "Custom MRM Policy" -  
RetentionPolicyTagLinks $tags
```

In this example, the Custom MRM Policy containing two default policy tags had an additional default policy tag and two personal tags added. Multiple default policy tags are supported because a retention policy can have one default policy tag per action taken. In the case of the Custom MRM Policy used as an example here, there is one default policy tag for archiving, one for deleting, and one for deleting voicemail messages, as well as the personal tags, as shown in [Figure 5-7](#).

NAME	TYPE	RETENTI...	RETENTION ACT...
<b>1 Month Delete</b>	<b>Personal</b>	<b>30 days</b>	<b>Delete</b>
DPT-Archive-1Year	Default	365 days	Archive
DPT-Delete-7Years	Default	2557 days	Delete
DPT-VoicemailDelete-30Days	Default	30 days	Delete

**FIGURE 5-7** The retention tags assigned to a retention policy

### Important: Combining Archive and Delete Actions in the Same Retention Policy

The use of two default policy tags for archiving and deleting mailbox items must be planned carefully. The delete action should have a longer retention age than the archive action. If the tag applying the delete action was configured for 6 months, and the tag applying the archive action was configured to 2 years, there would never be any mailbox items moved to the archive mailbox when the 2-year retention period lapses, because they were already deleted after 6 months.

## Assign policies to users

When a new mailbox is created, there is no retention policy assigned. You can assign the retention policy at the time the mailbox is created in the Exchange admin center, or when using the New-Mailbox or Enable-Mailbox cmdlets with the RetentionPolicy parameter. For existing mailboxes, the Set-Mailbox cmdlet is used to assign a retention policy.

[Click here to view code image](#)

```
#Assigning a retention policy using PowerShell
```

```
[PS] C:\>Set-Mailbox Alex.Darrow@contoso.com -RetentionPolicy "Custom MRM Policy"
```

Retention policies take effect on mailboxes even when the mailbox has not been archive-enabled, but only the tags that perform a delete action are processed. Tags that apply an archive action to mailbox items have no effect until an archive mailbox has been enabled for the user.

In addition to the personal tags that are assigned to a mailbox as part of a retention policy, users can choose to use any of the other personal tags configured in your organization. They do not have this right by default however. To grant users the right to choose from any of the available retention tags, the role assignment policy assigned to the users must be updated to include the MyRetentionPolicies management role. The Default Role Assignment Policy, which is applied to all mailbox users by default, can be updated with the MyRetentionPolicies management role.

[Click here to view code image](#)

```
#Adding a role to an assignment policy with PowerShell
```

```
[PS] C:\>New-ManagementRoleAssignment -Name "MyRetentionPolicies-Default Role Assignment Policy" -Role MyRetentionPolicies -Policy "Default Role Assignment Policy"
```

### Note: Modifying the Default Role Assignment Policy

It is not necessary to add the MyRetentionPolicies management role to the role assignment policy for users to be able to use personal tags. They are still able to use the personal tags that you assign to the retention policy.

They just aren't able to select additional personal tags that exist in the organization but are not included in their assigned retention policy.

## Plan and configure the Managed Folder Assistant

Retention policies are not effective on mailboxes until they have been applied by the Managed Folder Assistant. The Managed Folder Assistant (MFA) runs on Exchange 2016 mailbox servers, and processes any mailboxes with a retention policy assigned to stamp mailbox folders and items with retention tags. The MFA also performs the retention action on the items when the retention period has lapsed.

The MFA is a background process that is constantly running, but is throttled so that it doesn't consume excessive system resources. You can manually initiate the MFA to start processing a mailbox by running the Start-ManagedFolderAssistant cmdlet in PowerShell.

[Click here to view code image](#)

```
#Processing a mailbox with the Managed Folder Assistant
```

```
[PS] C:\>Start-ManagedFolderAssistant -Identity Alex.Darrow@contoso.com
```

As the MFA processes the mailbox contents, whether it is for the first time or any subsequent processing that is performed, it stamps any retention tags on the following basis:

- **Retention policy tags assigned to default folders, such as the Deleted Items folder, are applied to the folder** All sub-folders and items inherit the policy from the parent folder, except for items that the user has overridden with a personal tag. Note that users can't override retention policy tags on folders, only on individual items.
- **Default policy tags are assigned to any mailbox folders that do not have a retention policy tag specifically assigned to them** Again, all sub-folders and items inherit the policy from the parent folder. Users can override the default policy tag by assigning a personal tag to sub-folders or items. If the user assigns a personal tag to a folder, the sub-folders and items inherit that change, again unless the user has overridden any sub-folder or items with personal tags.
- **Personal tags that have been assigned to folders or items in the mailbox remain assigned, unless the personal tag has been deleted entirely from the Exchange organization** If a personal tag has been deleted, the folder or item inherits the tag from the parent folder.

As you can see, there is a combination of inheritance and direct assignment of tags at play. Mailbox items that are inheriting a tag from a parent folder and that are moved to a new location, inherit the tag of the new location. Mailbox items that are directly assigned a personal tag retain that personal tag no matter where they are moved.

If a retention tag is changed, such as changing the retention period, after it has already

been stamped on a mailbox folder or item, the MFA updates the mailbox contents that are already stamped with that tag with the new settings for the retention tag.

As the MFA processes the mailbox contents, it assesses the retention tag that is assigned to the item. If the retention period has lapsed, the recovery action is performed to archive or delete the item. Calculating whether the retention period has lapsed or not differs depending on the type of item, where it is located, and whether a personal tag has been assigned to the item.

- Most regular mailbox items, such as email messages, contacts, and non-recurring meetings or tasks, have a retention age based on the delivery date or date of creation.
- Recurring calendar items and tasks have a retention age based on their end date. If they have no end date, the items never expire.
- Deleted items of any kind have a retention age based on the date they were received or created. The items inherit the retention tag assigned to the Deleted Items folder, unless they were previously assigned a personal tag, in which case they retain their personal tag.

Based on the aforementioned conditions, consider an email message that is located in a folder that is assigned a retention tag to delete after 7 years. The email message has no personal tag assigned to it, therefore it is inheriting the tag of the parent folder. After one year has passed, if the item is moved to the Deleted Items folder that has a 30-day delete tag, the item is processed by the MFA based on its creation date and is found to be past the 30-day retention period for Deleted Items. Therefore, the email message is expired immediately and the retention action is performed by the MFA. In this example, the item is immediately deleted.

When a retention policy is assigned to existing mailboxes that hold a lot of historical data, there's a risk that a large amount of mailbox data is impacted when the MFA processes the mailbox. In situations where you want to roll out a retention policy without causing a large impact immediately, there are two approaches you can take. The first is to set the retention action on the tags in the policy to Never, so that the action is never undertaken. When this technique is used, the MFA still stamps retention tags on mailbox folders and items so that you can assess how the policy has been applied to mailboxes, however it does not archive or delete any items. While this does prevent items from being removed by the MFA, it might be misleading to users because they see that the tag is set to never expire, and then are surprised later when you configure a retention age for the tag.

The second approach is to configure mailboxes for retention hold. Retention hold prevents the MFA from processing retention actions on mailbox folders and items. The MFA still assigns tags to mailbox items in accordance with the retention policy, but

nothing is archived or deleted while the retention hold is in place. Retention hold is also useful when a mailbox user is absent for a long period of time. Using retention hold avoids situations where a user returns to work and the MFA has already expired items that the user never got a chance to review. To configure a mailbox for a retention hold, use the Set-Mailbox cmdlet with the RetentionHoldEnabled parameter. If you know the desired start and end dates for the retention hold, for example if the user is going to be absent for a specific planned period of time, you can configure an automatic start and end date for the retention hold as well.

[Click here to view code image](#)

```
#Configuring a retention hold on a mailbox using PowerShell
```

```
[PS] C:\>Set-Mailbox kim.akers@contoso.com -RetentionHoldEnabled $true  
-StartDateForRetentionHold 6/1/2016 -EndDateForRetentionHold 2/1/2017
```

## Remove and delete tags

When the time comes that you no longer want to use a retention tag for a retention policy, the tag can either be removed or deleted. The effect this has depends on whether the tag is only removed from the retention policy or whether it is deleted entirely from the Exchange organization.

Removing a tag from a retention policy causes the MFA to stop automatically stamping that retention tag to folders and items in the mailbox. The MFA, however, still processes the tags even after they are removed from the policy because the tag definition is still stored in Active Directory. If the mailbox folder or item is inheriting the tag from a parent, another default policy tag in the retention policy might be applied instead. If there are no other default policy tags in the retention policy, the previous tag continues to be applied as long as it still exists in the Exchange organization. The same is true for personal tags, which continue to be assigned to the items the user assigned them to, even if the tag has been removed from the retention policy.

To completely remove a tag and stop the MFA from processing it on existing items, the tag must be deleted from the organization. When the tag has been deleted, its definition is no longer stored in Active Directory, therefore the MFA can't process items with the tag's settings. When a tag has been deleted from the Exchange organization, all of the items that were previously assigned with that tag need to be reprocessed by the MFA to stamp a new tag on them.

## Plan and configure in-place archiving

So far, you've looked at how retention policies work and how the retention of mailbox contents can be managed using retention tags and retention policies. For retention tags that use a move to archive action, an archive mailbox is required before the Managed Folder Assistant (MFA) can perform that action.

Archive mailboxes are a secondary mailbox associated with a user that provides an alternate location to store older mailbox data. Each mailbox user is able to have one archive mailbox created for them. The archive mailbox can be stored on the same database as the primary mailbox, or on a different mailbox. Additionally, the archive mailbox can be hosted in Exchange Online (Office 365), as you discover in the next section. The benefits of using an archive location, that is for all intents and purposes just another mailbox, are that the archive mailbox can be made highly available using the same Database Availability Group architecture that protects regular mailboxes. Archive mailboxes can also be backed up using the same mechanisms as the primary mailboxes because they are just another mailbox hosted in a mailbox database.

Archive mailboxes are also subject to a separate storage quota than the primary mailbox. By default, mailboxes inherit the storage quotas from the mailbox database they are hosted on. The default storage quotas on a database are:

- Issue warning at 1.9 GB
- Prohibit send at 2 GB
- Prohibit send and receive at 2.3 GB

In comparison, the archive storage quotas for a mailbox user are much larger, with a warning at 90 GB and a hard limit at 100 GB, at which point no more contents can be added to the archive mailbox. The archive quotas allow in-place archiving to be used to manage primary mailbox sizes for users to avoid breaching their storage quotas, while still storing a large amount of historical data in the archive mailbox for compliance purposes.

Although some organizations try to store all of their archive mailboxes on specific databases, there is no particular advantage in doing so. In fact, it is simpler to host the archive mailbox on the same database as the primary mailbox, so that as mailbox data is moved from the primary mailbox to the archive mailbox and then later expired by the MFA, the overall storage footprint of the user remains roughly the same. For retention policies where mailbox data is never expired, co-locating primary and archive mailboxes provides consistency in the rate of growth and the user load across all of the databases in the organization.

Archive mailboxes can be created at the same time as the primary mailbox or can be added later for existing mailbox users. When you are creating new mailbox users with the New-Mailbox or Enable-Mailbox cmdlets, use the Archive parameter so the archive

mailbox is created at the same time. If no archive database is specified by using the ArchiveDatabase parameter, Exchange chooses one automatically for you. Archive mailboxes can be created for existing mailboxes by running the Enable-Mailbox cmdlet. For example, to create an archive mailbox for an existing user that is to be hosted on the same database as the primary mailbox, use the following command.

[Click here to view code image](#)

**#Creating an archive mailbox for an existing mailbox user**

```
[PS] C:\>Enable-Mailbox Kim.Akers@contoso.com -Archive -ArchiveDatabase  
(Get-Mailbox  
Kim.Akers@contoso.com).Database
```

The Default MRM Policy is automatically applied to the mailbox if no retention policy is already applied. For existing mailbox users, you can't use the RetentionPolicy to specify a non-default retention policy at the same time as you archive-enable the mailbox. If you need to change the retention policy after creating the archive mailbox, use the Set-Mailbox cmdlet with RetentionPolicy parameter.

When an archive mailbox has been created for a user, it can be accessed using Outlook and Outlook on the Web clients. The archive mailbox appears as a secondary mailbox visible to the user. Users can manually move items to the archive mailbox, perform searches, and even delete items if they want. Archive mailboxes are not available from most mobile devices and clients however, which could be a disadvantage for users who require frequent access to historical mailbox data when they are on mobile devices. Archive mailboxes are also not cached by Outlook clients for offline access, so any users who are roaming away from a network connection are unable to access their archived mailbox data.

## Plan and configure online archiving (Office 365)

When an Exchange 2016 organization has a Hybrid configuration with Exchange Online (Office 365), the archive mailboxes for on-premises users can optionally be hosted in the cloud. The full rich coexistence functionality of a Hybrid configuration, such as Hybrid mail flow and free/busy calendar information sharing, is not required for the archive functionality to work. The organization relationship and directory synchronization however, are critical components of a Hybrid configuration that allow online archives to be used.

A benefit of using Exchange Online archives is that it offloads the storage burden of what can potentially be very large archive mailboxes. This way your on-premises servers do not need to host all of that data and your organization does not need to carry the associated risks and costs. Online archive mailboxes also have an unlimited storage quota for some Office 365 subscriptions.

## Note: Which Office 365 Plans Have Unlimited Archives?

The Exchange Online limits change over time, so if you need to know exactly which plans offer unlimited archive mailbox quotas, you can check the service descriptions published on TechNet at <https://technet.microsoft.com/en-au/library/exchange-online-limits.aspx#StorageLimits>.

The behavior of Exchange Online archives is almost identical to on-premises archiving. Mailbox items are moved to the archive mailbox by applying retention policies to mailboxes. You must also consider the network connectivity between your on-premises users and Office 365. Poor connectivity results in a poor user experience when users are accessing their archive mailboxes.

The archive mailbox can be created in Exchange Online as a remote archive mailbox, or an existing on-premises archive mailbox can be moved to Exchange Online while leaving the primary mailbox hosted on-premises. Aside from establishing the Hybrid configuration, there are some preparation steps that are necessary before beginning to use Exchange Online archive mailboxes if on-premises retention policies have already been used. The Hybrid configuration does not synchronize existing retention tags and retention policies to Exchange Online. This means that when mailbox items that have already been tagged by the MFA on-premises are moved to the cloud, the MFA running in Exchange Online might not be able to find the same tag definitions and reprocesses the items with default policy tags. To avoid this problem, use the Export-RetentionTags.ps1 and Import-RetentionTags.ps1 scripts to export the on-premises retention tags to XML and import them into Exchange Online. You can then configure the same retention policies in Exchange Online in preparation for the move of archive mailboxes to the cloud.

To create a new archive mailbox in Exchange Online, the following process is used:

1. Use directory synchronization to synchronize the on-premises mailbox user to Office 365 and assign them a license that enables the use of Exchange Online archives.
2. Enable the mailbox for remote archive by running the Enable-Mailbox cmdlet. The ArchiveDomain is the email routing domain for the Office 365 tenant, for example contoso.mail.onmicrosoft.com.

[Click here to view code image](#)

```
#Enabling a remote archive for an on-premises mailbox user
```

```
[PS] C:\>Enable-Mailbox -Identity Ben.Smith -RemoteArchive -ArchiveDomain contoso.
```

3. Wait for the remote archive settings to synchronize from the on-premises Active Directory to Office 365. The wait time depends on the synchronization schedule configured on your directory sync server.
4. After synchronization of the changes to Office 365 has occurred, the archive mailbox is provisioned in Exchange Online, and the attributes of the mail-enabled user object in Azure Active Directory are updated with the changes. These changes then need to synchronize back to the on-premises Active Directory during a subsequent directory sync schedule.

Overall, the process of enabling an online archive mailbox for an on-premises user can take several hours to complete before the user sees the online archive mailbox appear in their Outlook or Outlook on the Web clients.

## Summary

- Retention policies manage the moving of mailbox items to an archive mailbox or removal of items from mailboxes. Retention policies do not enforce the retention of data or prevent the removal of data by users.
- A retention policy is a collection of retention tags that is assigned to a mailbox. The retention tags are then processed by the Managed Folder Assistant (MFA). The MFA stamps the tags on mailbox items and handles the moving or deletion of the items when the retention period has expired.
- Retention policies do not require the use of archive mailboxes. When mailboxes are archive-enabled however, the Managed Folder Assistant is able to perform the move to archive action of retention tags, and move the mailbox items to an on-premises or online archive mailbox.

## Skill 5.3: Plan, configure, and perform eDiscovery

Exchange 2016 eDiscovery allows an organization to perform searches of mailbox contents for internal investigations or legal matters. Discovery managers can log in to the Exchange admin center and use the familiar, user-friendly web interface to perform searches based on keywords, date ranges, sender and recipient email addresses, and message types. The results of eDiscovery searches can then be reviewed, preserved in-place, copied to an alternate location, exported, or removed from mailboxes entirely.

## This section covers how to:

- [Plan and delegate RBAC roles for eDiscovery](#)
- [Perform multi-mailbox searches in Exchange admin center \(EAC\) and Exchange Management Shell](#)
- [Enable a legal/litigation hold](#)
- [Perform a query-based in-place hold](#)
- [Integrate in-place federated search with Microsoft SharePoint Discovery center](#)

## Plan and delegate RBAC roles for eDiscovery

The ability to search every mailbox in the organization and gain access to their contents using eDiscovery is clearly very powerful, and therefore must be granted to only those people in the organization who are trusted to perform the task. In many organizations, eDiscovery permissions are given to non-technical users. No users are granted the permissions to perform eDiscovery searches by default, including members of the Organization Management group. The Organization Management group members can however, grant eDiscovery permissions to others or to themselves.

The role-based access control (RBAC) group named Discovery Management exists to provide a user with eDiscovery permissions. The Discover Management group is assigned the Mailbox Search role to perform searches, as well as the Legal Hold role to apply in-place holds or litigation holds. To grant a user both permissions, add them to the Discovery Management role group by running the Add-RoleGroupMember cmdlet.

[Click here to view code image](#)

```
#Adding a member to the Discovery Management role group
```

```
[PS] C:\>Add-RoleGroupMember -Identity "Discovery Management" -Member Jim.Daly@contoso.com
```

The individual Mailbox Search and Legal Hold roles can also be separately granted to a user if necessary, such as when you only want to allow a user to perform searches but not to apply holds. To create a management role assignment for the Mailbox Search role, the following steps shown in [Listing 5-3](#) are performed.

### LISTING 5-3 Granting permissions to perform mailbox searches

[Click here to view code image](#)

```
[PS] C:\>New-RoleGroup -Name "Mailbox Search Admins" -Description "Users
```

```
who can perform  
Mailbox Searches"  
[PS] C:\>New-ManagementRoleAssignment -Name "Mailbox Search Admins" -  
SecurityGroup  
"Mailbox Search Admins" -Role "Mailbox Search"  
[PS] C:\>Add-RoleGroupMember -Identity "Mailbox Search Admins" -Member  
jim.daly@contoso.  
com
```

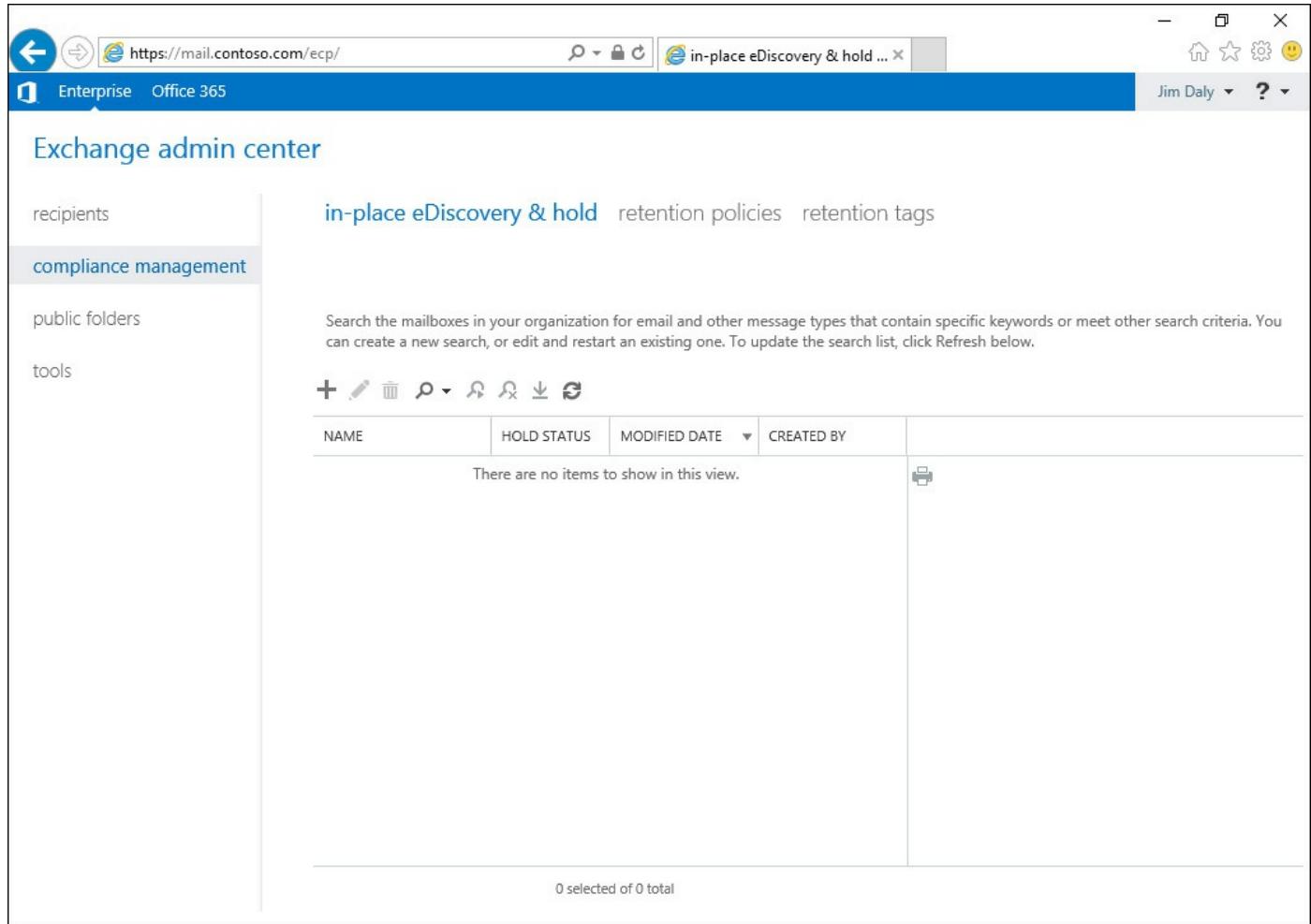
---

### Note: Organization Management and Legal Hold

The Organization Management group is already granted the permissions to apply in-place holds or litigation holds by default, which in itself is not particularly risky. Therefore, Organization Management role group members don't need to be added to the Discovery Management group to configure holds. It is the powerful Mailbox Search role, which provides the capability to search mailbox contents, that is not granted to anyone by default.

## Perform multi-mailbox searches in Exchange admin center (EAC) and Exchange Management Shell

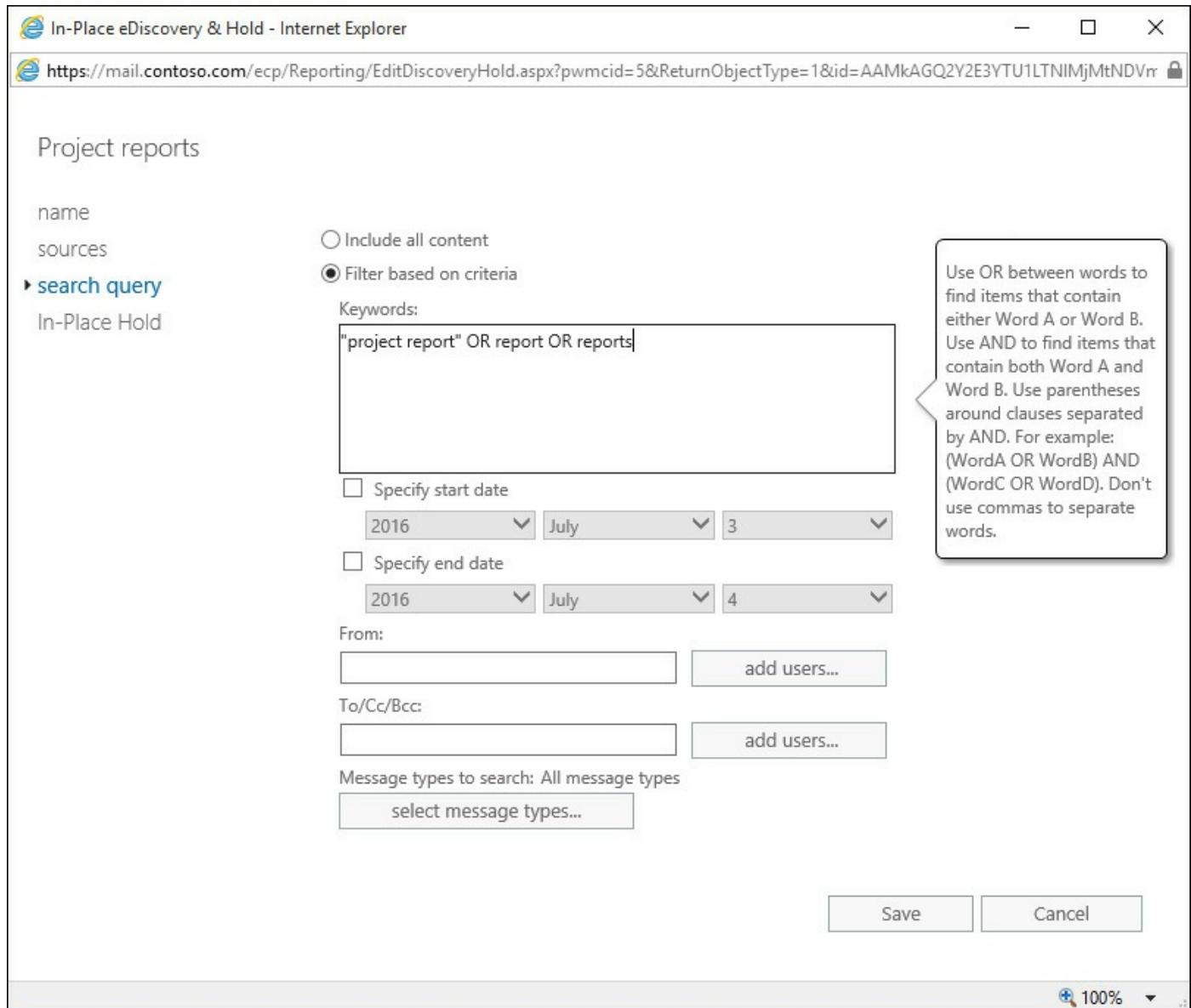
All eDiscovery searches are performed using the Exchange admin center. An administrator or a user who has been granted the permissions to perform mailbox searches can navigate to the compliance management section to find the in-place eDiscovery and hold interface, as shown in [Figure 5-8](#). Non-administrative users who are granted Discovery Management permissions are also able to see a limited number of other Exchange admin sections with read-only access, such as the recipients list, public folders, and retention policies.



**FIGURE 5-8** The eDiscovery console in Exchange admin center

When a new eDiscovery search is created to locate mailbox contents, you provide a name and description for the search so that you can identify it among other searches at a later time. Using case numbers or other unique identifiers is one approach you could take. The search name is also used as the folder name when copying search results to a discovery mailbox. Searches can be performed across all mailboxes or a selection of mailboxes. If you specify a group instead of one or more mailboxes, the mailboxes for all of the members of the group are searched. Searches that are performed across all mailboxes can't have a hold applied. In-place hold is explained in more detail later in this chapter.

Next, construct the search query to locate the contents that you're interested in, as shown in [Figure 5-9](#). A specific query is not required, and you can choose to include all content from the source mailboxes in the search instead. The larger the results that are returned by the search however, the more difficult it is to analyze them and extract the required information. That said, performing a search of all contents for a few specific mailboxes is a reasonable approach to start a discovery search. You can refine the search criteria to return fewer results on a second or third attempt.



**FIGURE 5-9** Constructing an eDiscovery search query

### Need More Review? eDiscovery Search Syntax

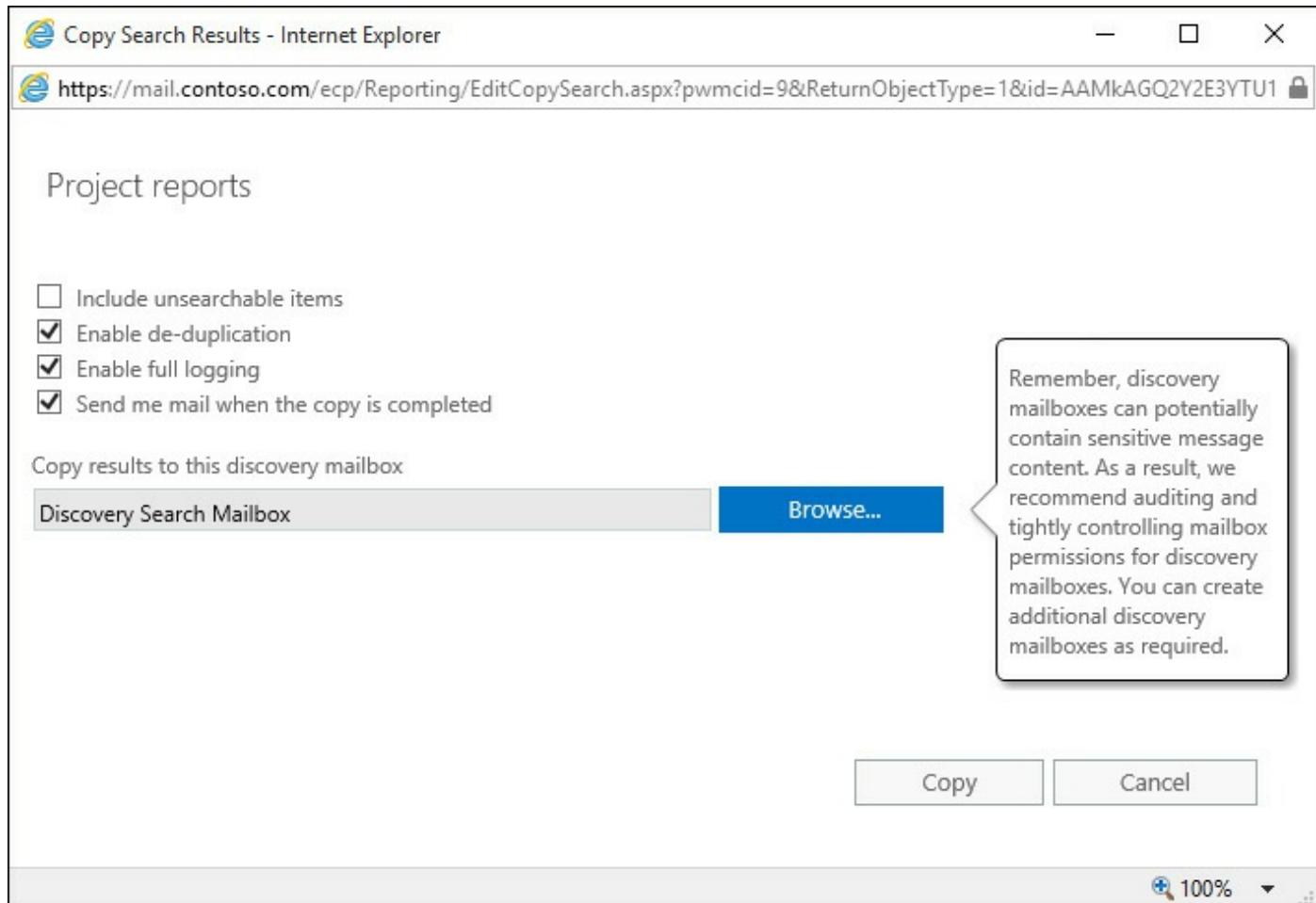
Exchange 2016 eDiscovery search queries use the Keyword Query Language (KQL), which is the same query language used in Outlook searches. You can find a detailed syntax reference for KQL on MSDN at [https://msdn.microsoft.com/library/ee558911\(v=office.15\).aspx](https://msdn.microsoft.com/library/ee558911(v=office.15).aspx).

After you've created the eDiscovery search, an estimate of the search results is produced. You can refresh the list of searches in the Exchange admin center to monitor the progress of the estimate. The estimate provides the number of items that match the query. You can also review a keyword statistics report to display the number of hits for each of the keywords that were included in your search query. The keyword estimate

helps you to identify parts of your search query that returned an unexpected number of hits, which could indicate that your search is not refined enough to discover the information needed in your investigation.

All eDiscovery in Exchange 2016 relies on the content indexes created by Exchange Search for each mailbox database, therefore if the content indexes are disabled or unhealthy, you might not see accurate search results or estimates. Similarly, search results might be impacted by users deleting email or by large amounts of email being imported to a mailbox and not yet being fully indexed.

After you're satisfied with the search results estimates, you can start the search and copy the results to a discovery mailbox for inspection. The copy process can also include de-duplication of messages, which is useful when the same message is found in multiple mailboxes. For large searches, you can also choose to receive an email when the copy is complete. Finally, select a discovery mailbox to copy the contents to, as shown in [Figure 5-10](#). There is one discovery mailbox in the Exchange organization that is created automatically when Exchange 2016 is installed or you can create additional discovery mailboxes by running the New-Mailbox cmdlet with the Discovery parameter. The default discovery mailbox is pre-configured with mailbox permissions that allow Discovery Management role group members to access the mailbox and review results. Any additional discovery mailboxes that you create are not automatically configured with mailbox permissions and require you to manually grant permissions to the user who needs to review the mailbox items that were copied.



**FIGURE 5-10** Copy eDiscovery search results to a discovery mailbox

When the search has completed you can open the results, which opens a new browser window or tab with Outlook on the Web to view the discovery mailbox that the search results were copied to.

For eDiscovery search results that need to be provided to a reviewer that can't access the Exchange admin center or the discovery mailbox, you can choose to export the results to PST file. When you start this process the eDiscovery export tool is downloaded to your computer, and the results are exported from the discovery mailbox. Select a folder to store the exported files, and choose whether you want the export to perform de-duplication and include unsearchable items. When the export is complete, the folder contains:

- The PST file with the exported mailbox items.
- A CSV file containing the details of the exported items. The CSV file is useful for performing searches or indexing in a separate application, which tends to be faster than opening a PST file for searching.
- A config file detailing the configuration of the eDiscovery search that was performed, including details such as the mailboxes that were searched and the search query that was used.

eDiscovery searches can also be created and managed in PowerShell. The New-MailboxSearch cmdlet performs the same role as the dialog used to create a new eDiscovery search in the Exchange admin center. For example, to search all mailboxes for members of the Human Resources group for messages relating to project reports, the following command can be used.

[Click here to view code image](#)

```
#Creating an eDiscovery search using PowerShell
```

```
[PS] C:\> New-MailboxSearch "Case ID 7001" -SourceMailboxes "Human  
Resources"  
-TargetMailbox "Discovery Search Mailbox" -SearchQuery '"project report"  
OR  
reports OR report' -MessageTypes Email
```

The eDiscovery search can be started by running the Start-MailboxSearch cmdlet. If you only want to retrieve an estimate of the results of the query, and not actually copy the items to the discovery mailbox, you can set the mailbox search to return estimates only.

[Click here to view code image](#)

```
#Configuring a mailbox search to retrieve estimated results
```

```
[PS] C:\> Set-MailboxSearch "Case ID 7001" -EstimateOnly $true -  
ExcludeDuplicateMessages  
$false
```

### Note: Duplicate Messages for eDiscovery Search Estimates

When you are configuring a mailbox search to return estimates only, you must configure the ExcludeDuplicateMessages option to \$false. When you're ready to run the search and copy items to a discovery mailbox, you can change the ExcludeDuplicateMessages option back to \$true if you require it.

After configuring the mailbox search, you can start it by running the Start-MailboxSearch and monitor the progress and results with the Get-MailboxSearch cmdlet. To view the estimates results of a search, run the following command.

[Click here to view code image](#)

```
#Retrieving the estimated results for an eDiscovery search
```

```
[PS] C:\>Get-MailboxSearch "Case ID 7001" | Select Result*
```

```
ResultNumber : 0  
ResultNumberEstimate : 3
```

```
ResultSize          : 0 B (0 bytes)
ResultSizeEstimate : 472.6 KB (483,960 bytes)
ResultSizeCopied   : 0 B (0 bytes)
ResultsLink        :
```

The searches that are created and managed in the Exchange admin center or by running New-MailboxSearch are useful for eDiscovery purposes. There are also situations in which multi-mailbox searches need to be performed in response to an incident, such as a virus outbreak. An eDiscovery search can find the virus messages, but can't remove them from the mailboxes where they are found. To remove such items, a compliance search is performed instead. In previous versions of Exchange, the Search-Mailbox cmdlet was used to perform searches with the goal of removing contents. Search-Mailbox however, is limited to searching 10,000 mailboxes at a time, making it unsuitable for large environments.

Compliance search requires the same Discovery Management role group membership as eDiscovery. A user with Discovery Management permissions can create a new compliance search by running the New-ComplianceSearch cmdlet.

[Click here to view code image](#)

```
#Creating a new compliance search in PowerShell
```

```
[PS] C:\>New-ComplianceSearch -Name "Remove fake invoice malware" -
ExchangeLocation all
-ContentMatchQuery 'subject:"Your invoice is attached"'
```

After creating the compliance search, use the Start-ComplianceSearch cmdlet to start it. You can then run the Get-ComplianceSearch cmdlet to monitor the progress of the search. When the search has reached a completed status, use the Get-ComplianceSearch cmdlet to retrieve the Items and SuccessResults properties, which displays the results for each of the searched mailboxes.

[Click here to view code image](#)

```
#Reviewing the results of a compliance search
```

```
[PS] C:\>Get-ComplianceSearch -Identity "Remove fake invoice malware" |
Format-List Items,SuccessResults

Items          : 3
SuccessResults : {Location: Alex.Darrow@contoso.com, Item count: 1, Total
size: 8107,
                  Location: Kim.Akers@contoso.com, Item count: 1, Total
size: 8101,
                  Location: Dan.Jump@contoso.com, Item count: 1, Total
size: 3858,
                  Location: Shannon.Dascher@contoso.com, Item count: 0,
Total size: 0,
                  Location: HRInbox@contoso.com, Item count: 0, Total size:
0,
```

```
size: 0, Location: Michael.Jurek@contoso.com, Item count: 0, Total  
Total size: 0, Location: Dave.Natsuhara@contoso.com, Item count: 0,  
size: 0, Location: Apurva.Dalia@contoso.com, Item count: 0, Total  
size: 0} Location: Jaka.Stele@contoso.com, Item count: 0, Total
```

After you've determined that the search results are accurate, the next step is to delete the items from the mailboxes where they are found. When the mailbox items are deleted, they are moved to the recoverable items folder of the mailbox. This makes the deleted items recoverable by users using Outlook or Outlook on the Web. The items can also be found by using eDiscovery searches. If a mistake is made however, and the wrong items are deleted, there is no automated way to restore them to their original location in the mailbox. Each user needs to recover their own items from the recoverable items folder. For this reason, it is recommended to proceed with caution when using compliance searches to remove mailbox items. When you're ready, run the New-ComplianceSearchAction cmdlet to delete the mailbox items that were found by the compliance search.

[Click here to view code image](#)

```
#Deleting mailbox items that were found by a compliance search
```

```
[PS] C:\>New-ComplianceSearchAction -SearchName "Remove fake invoice  
malware" -Purge  
-PurgeType SoftDelete
```

## Perform a query-based in-place hold

The same eDiscovery search capabilities that are used to find and copy mailbox contents for inspection can also be used to preserve data in-place. Consider a scenario in which an investigation has been started, and the results of an eDiscovery have been reviewed. There are items of interest included in the results, and before any further action is taken, you need to ensure that the mailbox items are not deleted by the user while the investigation proceeds. This capability is referred to as an in-place hold and is a configuration option when creating or modifying an eDiscovery search.

Mailbox searches that are targeted at all mailboxes can't be used to apply in-place holds. Any mailbox search targeted at one or more mailboxes or at the moments of one or more distribution groups however, can be used to apply an in-place hold. The hold can be configured when the search is first created, or later if the need arises. An in-place hold can be indefinite or it can be configured to apply to items for a specified period of time after the item was created or received.

Continuing from the previous example search, an in-place hold can be applied to an

existing search by editing it in the Exchange admin center, or by running the Set-MailboxSearch cmdlet with the InPlaceHoldEnabled parameter.

[Click here to view code image](#)

```
#Configuring an eDiscovery search to apply in-place hold
```

```
[PS] C:\>Set-MailboxSearch "Case ID 7001" -InPlaceHoldEnabled $true
```

The in-place hold settings might take up to an hour to take effect. After the in-place hold is applied, if the user deletes or modifies any mailbox contents, the item is compared to the in-place hold and if a match is found then the item is preserved. Deleted items are removed from the user's view of the mailbox and the user is unaware that an in-place hold is in effect for any of their mailbox contents. The deleted items are preserved in the recoverable items folder of the mailbox where it is still accessible by eDiscovery searches.

---

### Important: In-Place Holds Configured for Distribution Groups

When an in-place hold is configured for a group, all of the mailboxes for members of that group are included as source mailboxes for the hold.

However, at the time the hold is created, the mailboxes that are members of the group are added to the search as individual mailboxes. If the membership of the group changes at a later time, the search is not updated automatically with the changes and must be manually adjusted. You can read more about this at Microsoft MVP Jeff Guillet's blog at

<http://www.expta.com/2016/03/important-information-about-group.html>.

---

## Enable a legal/litigation hold

In-place holds use eDiscovery searches to preserve mailbox contents matching specific search criteria. Sometimes this is not a feasible approach, such as when the characteristics of the mailbox items you want to preserve are not well known, or when you need to preserve all mailbox contents for a user regardless of their characteristics. In such cases, a hold can be applied to the entire mailbox. This is referred to in Exchange 2016 as a Litigation Hold and was previously referred to as a Legal Hold in other versions of Exchange.

When a Litigation Hold is applied, users can delete items from their mailbox and are no longer able to see them. The deleted items, however, are preserved in the recoverable items folder of the mailbox, and are able to be searched and retrieved using eDiscovery searches.

As with in-place holds, a litigation hold can be permanently applied or it can be applied for a specific duration. The duration is not an end date for the Litigation Hold,

rather it is the period of time for which an individual item is subject to the Litigation Hold. This works in a similar way to retention policies, with the expiration of the Litigation Hold for non-recurring, regular mailbox item types being calculated based on the date the item was created or received. To place a mailbox on Litigation Hold, use the Set-Mailbox cmdlet.

[Click here to view code image](#)

#### #Applying a Litigation Hold to a mailbox

```
[PS] C:\>Set-Mailbox Kim.Akers@contoso.com -LitigationHoldEnabled $true  
-LitigationHoldDuration 3650
```

---



#### Exam Tip

The Set-Mailbox cmdlet also includes a LitigationHoldDate parameter. This parameter is used to specify the date that the Litigation Hold started, but is for reporting and informational purposes only. It has no bearing on when the LitigationHold actually starts or when it stops. In fact, you can enter any date you like in that field. If you do not use the LitigationHoldDate parameter, the field is automatically populated with the time and date when you applied the Litigation Hold.

---

## Integrate in-place federated search with Microsoft SharePoint Discovery center

The eDiscovery Center is a feature of SharePoint 2013 that provides a similar search experience as Exchange eDiscovery. In fact, SharePoint eDiscovery uses the same search query syntax and has similar features for exporting search results. SharePoint is also able to search Exchange mailboxes by leveraging the Federated search API. By integrating the two products, users who are performing discovery searches across both Exchange and SharePoint can do so from a single interface. For this integration to work, you need to configure server to server authentication between the two partner applications.

As prerequisites to integrating the two servers, the SharePoint site must be configured to use Secure Sockets Layer (SSL) and the Exchange Web Services Managed API must be installed on each SharePoint server. After the prerequisites have been met, use the following steps to configure server to server authentication. First on the SharePoint server, run the following command.

[Click here to view code image](#)

#### #Configure server to server authentication on the SharePoint 2013 server

```
[PS] C:\> New-SPTokenIssuer -Name Exchange -  
MetadataEndPoint  
https://mail.contoso.com/autodiscover/metadata/json/1
```

Next, on the Exchange server, run the following script located in the C:\Program Files\Microsoft\Exchange Server\V15\Scripts folder.

[Click here to view code image](#)

```
#Configure server to server authentication on the Exchange 2016 server
```

```
[PS] C:\...\> .\Configure-EnterprisePartnerApplication.ps1 -  
AuthMetadataUrl  
https://mysite.sharepoint.contoso.com/_layouts/15/metadata/json/1 -  
ApplicationType  
SharePoint
```

Finally, add the users performing searches in the SharePoint eDiscovery center to the Discovery Management role group for Exchange 2016.

## Summary

- Exchange 2016 eDiscovery is a powerful feature set that allows administrators and users to be assigned permissions to search and access the contents of mailboxes within the organization.
- eDiscovery searches can be used to locate mailbox items matching search criteria, and then copy the items to a discovery mailbox for analysis or apply in-place holds to the items that match the search criteria. For mailboxes that need their entire contents preserved, a Litigation Hold can be applied to the entire mailbox instead.
- Compliance searches differ from eDiscovery searches in that they can be used to remove items from mailboxes.

## Skill 5.4: Plan, configure, and manage a compliance solution

So far in this chapter you've looked at some of the features of Exchange 2016 that can be applied to meet your compliance requirements. In this section, you look at some of the other features that can be used to fill in the overall compliance solution.

## This section covers how to:

- [Plan and configure MailTips](#)
- [Plan, create, configure, and deploy message classifications](#)
- [Plan and configure transport rules to meet specified compliance requirements](#)
- [Plan and configure journaling](#)

## Plan and configure MailTips

MailTips are messages that are displayed to users while they are composing an email message in Outlook or Outlook on the Web. The goal of MailTips is to alert the sender to potential issues with the email they are composing, allowing them to make adjustments before they send it and avoid mistakes, non-delivery of email, or simply to avoid embarrassing situations. An Exchange 2016 server is pre-configured with several MailTips for common scenarios, such as internal recipients with full mailboxes, composing messages to a very large audience, or a recipient who has an out of office message. The complete list of default MailTips can be found on TechNet at [https://technet.microsoft.com/en-us/library/jj649091\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj649091(v=exchg.150).aspx).

The default configuration for Exchange 2016 is that all MailTips are enabled, except for the MailTip that warns about sending to external recipients. The large audience threshold is set to 25 and group metrics are enabled. Group metrics are used for MailTips that are displayed for large audiences and are regularly updated by the Mailbox servers in the organization. You can see the MailTips configuration for your organization by running the Get-OrganizationConfig cmdlet. Changes to the MailTips configuration are made by running the Set-OrganizationConfig cmdlet.

[Click here to view code image](#)

```
#View the MailTips configuration for the Exchange organization
```

```
[PS] C:\>Get-OrganizationConfig | Select MailTips*
```

```
MailTipsAllTipsEnabled          : True
MailTipsExternalRecipientsTipsEnabled : False
MailTipsGroupMetricsEnabled      : True
MailTipsLargeAudienceThreshold   : 25
MailTipsMailboxSourcedTipsEnabled : True
```

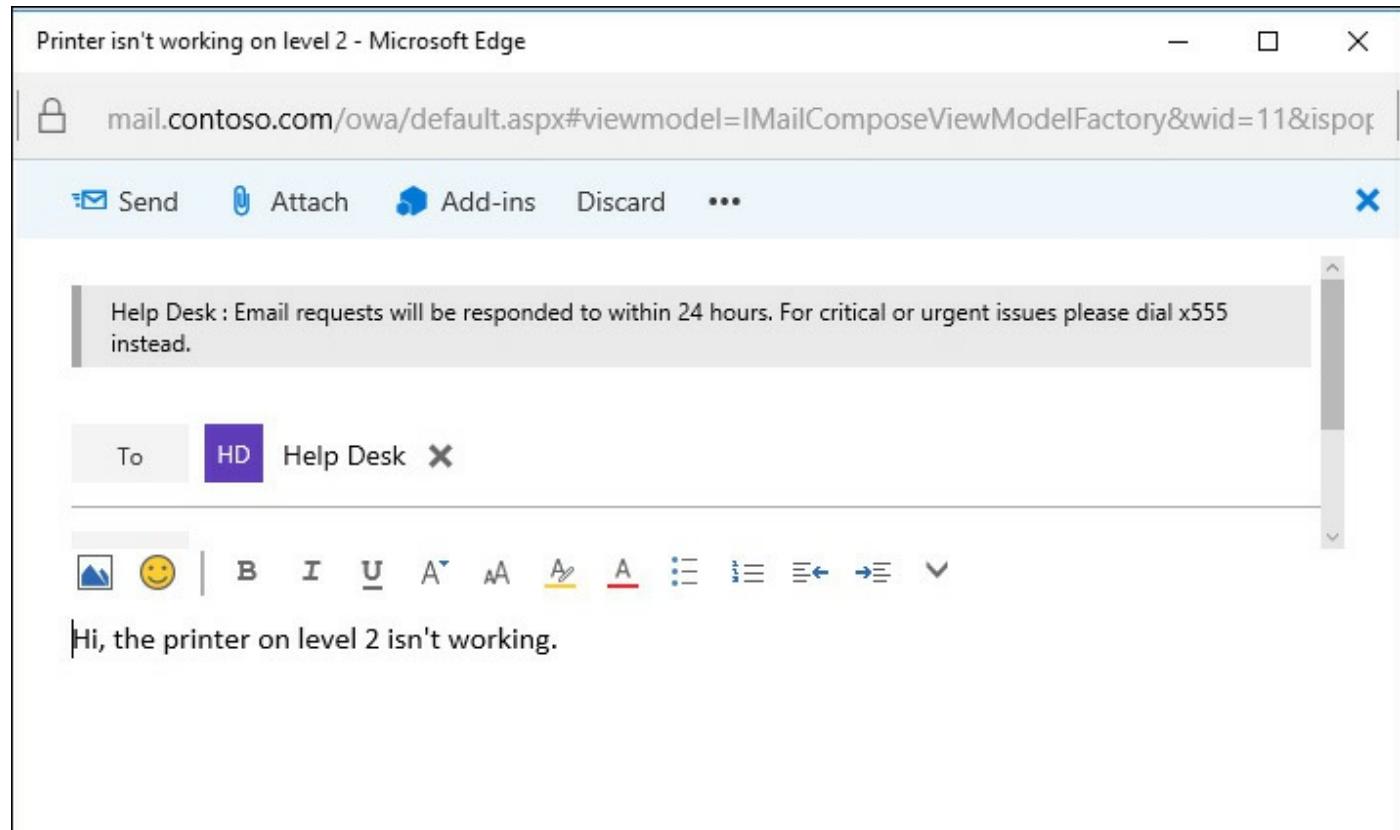
In addition to the default MailTips, you can configure custom MailTips on individual recipients. Custom MailTips can be up to 175 characters long and can be configured on user mailboxes, groups, room and equipment mailboxes, contacts, and shared mailboxes. To configure a custom MailTip, use the PowerShell cmdlet that applies to the recipient type. For example, to configure a custom MailTip on a Help Desk mailbox

to display a message for senders as shown in [Figure 5-11](#), the Set-Mailbox cmdlet is used.

[Click here to view code image](#)

#### #Configuring a custom MailTip on a mailbox

```
[PS] C:\>Set-Mailbox "Help Desk" -MailTip "Email requests will be  
responded to within 24  
hours. For critical or urgent issues please dial x555 instead."
```



**FIGURE 5-11** MailTips in action

## Plan, create, configure, and deploy message classifications

Message classifications in Exchange 2016 help an organization manage their compliance needs by allowing users to apply a classification to a message that describes the intended audience or use of the message. Classifications are applied using Outlook or Outlook on the Web and are stored in the headers of the email message, where the classification information can be read by transport rules. You can therefore configure transport rules to enforce compliance requirements based on classifications. For example, if a message has been classified as Company Confidential and a recipient inadvertently forwards the message to an external email address, a transport rule can detect and block the message. Messages that have a classification applied to them also display a message to users that describes the classification, which helps guide user behavior.

By default, there are three message classifications that exist in an Exchange 2016 organization. These classifications are described on TechNet at

[https://technet.microsoft.com/en-au/library/bb123498\(v=exchg.150\).aspx](https://technet.microsoft.com/en-au/library/bb123498(v=exchg.150).aspx).

- **Attachment removed** Notifies the recipient when attachments have been removed from the email message by Exchange.
- **Originator requested alternate recipient mail** Notifies the recipient that the message has been redirected from the originally addressed recipient.
- **Partner mail** Notifies the recipient that the message was encrypted and delivered through a secure connector.

Users can't add these default classifications to email messages, rather they are applied automatically by Exchange when appropriate.

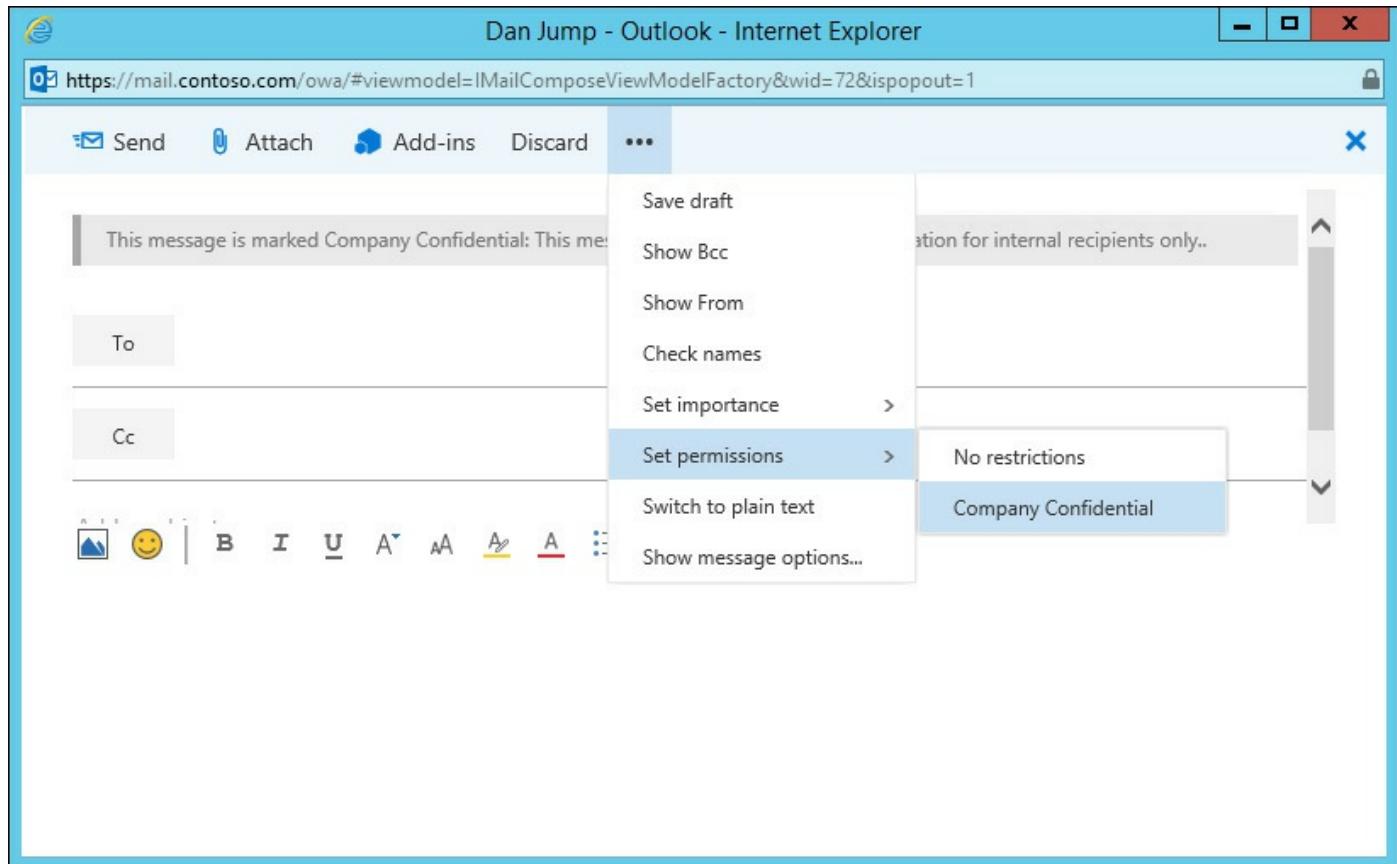
Message classifications are created by running the New-MessageClassification cmdlet. Each message classification is given a name that is visible to administrators and a display name that is visible to users. Each classification also requires a sender description, which is displayed to the user composing the message after they've applied the classification. An optional recipient message can also be configured, which is displayed to the recipients who receive the email message.

[Click here to view code image](#)

```
#Creating a new message classification using PowerShell
```

```
[PS] C:\>New-MessageClassification -Name CompanyConfidential -DisplayName  
"Company  
Confidential" -SenderDescription "This message contains confidential  
information for  
internal recipients only." -RecipientDescription "This message contains  
confidential  
information for internal recipients only."
```

Outlook on the Web users are able to see and use message classifications with no further action required by administrators, as shown in [Figure 5-12](#).



**FIGURE 5-12** Applying a message classification using Outlook on the Web

For organizations that have a user population that uses multiple languages, message classifications can be configured with localized display names, sender messages, and recipient messages. In the example shown earlier, no locale was specified for the message classification, therefore the classification defines the default display name and sender/recipient messages that are displayed. To add a new locale for the same message classification, the New-MessageClassification cmdlet is used again. This time the same name is used, but the new locale is specified. When a user whose system or mailbox is configured for the specific locale uses Outlook or Outlook on the Web, they see the localized version of the classification.

[Click here to view code image](#)

```
#Creating a locale-specific message classification using PowerShell
```

```
[PS] C:\>New-MessageClassification -Name CompanyConfidential -DisplayName  
"Compañía  
Confidencial" -Locale es-ES -SenderDescription "Este mensaje contiene  
información  
confidencial para destinatarios internos solamente." -RecipientDescription  
"Este  
mensaje contiene información confidencial para destinatarios internos"
```

sóamente."

Although Outlook on the Web users can make use of message classifications without additional administrative effort, Outlook users need the classification definitions distributed to their computers by an administrator as an XML file. The XML file is created by running the Export-OutlookClassification.ps1 script located in C:\Program Files\Microsoft\Exchange Server\V15\Scripts. When you run the script, the default classifications are exported. If you need to export the classifications for a specific locale, use the Locale switch when running the script.

The XML file can be distributed to computers using Group Policy preferences, a script, or a software deployment tool. The specific location of the file is not important as long as the file is located where Outlook can access it. You can then use Group Policy preferences, or run a script to import a registry file, to set the following registry settings on client computers, shown in [Listing 5-4](#).

## LISTING 5-4 Registry settings for message classifications for Outlook 2016

[Click here to view code image](#)

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Policy]
"AdminClassificationPath"="C:\\LocalData\\OutlookClassifications.xml"
"EnableClassifications"=dword:00000001
"TrustClassifications"=dword:00000001
```



### Exam Tip

You might be presented with scenarios that ask whether a message classification should be used, or whether Information Rights Management (IRM) should be used. When considering the distinction between the two, remember that message classifications are simply labels or suggestions that are added as metadata to a message. Although message classifications can be used by transport rules to enforce compliance requirements, they do not provide any enforcement on their own. Message classifications are also removed from message headers if the email message leaves the organization. In comparison, IRM applies protection directly to email messages and documents, and the protection travels with the email or document wherever it goes.

## Plan and configure transport rules to meet specified compliance requirements

Earlier in this chapter you looked at Data Loss Prevention, which is implemented using DLP policies that configure transport rules. DLP policies are useful for meeting compliance requirements that are common across organizations in the same industries, such as preventing disclosure of financial information. Many organizations, however, have compliance requirements that are unique to the organization or that are common in their industry, but are unable to be pre-packaged in the same way that DLP policies are. For example, the concept of an ethical wall between two departments within the same organization, such as editorial and advertising departments at a newspaper, is not unusual, but the specific implementation, such as the names of users or groups, is going to be unique even between very similar organizations.

Transport rules, also referred to as mail flow rules, provide a broad range of configuration elements that can be applied to email messages as they travel through the transport pipeline, so that the organization's compliance needs can be met. Some uses of transport rules, such as moderating messages sent to a social club distribution group, are not necessarily compliance-driven, but are implemented for convenience. Transport rules are created in the mail flow section of the Exchange admin center, or by running the New-TransportRule cmdlet.

Listing all of the available configuration options for transport rules would take up too much room here, but they can be summarized as follows:

- **Conditions (or predicates)** Used to define when a rule is applied. An example of a condition is when the address of a message's recipient is at a specific domain name. The full list of conditions is available on TechNet at [https://technet.microsoft.com/en-us/library/dd638183\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd638183(v=exchg.160).aspx).
- **Exceptions** A type of condition that further refines when a rule is applied. An example of an exception is when the sender of a message is a member of a group. Exceptions are drawn from the same list of options as conditions.
- **Actions** Used to define what should be done to messages that match the rule's conditions. An example of an action is rejecting a message. Some actions require additional details, for example you can reject messages and configure specific text to be included in the non-delivery report to the sender. The full list of actions is available on TechNet at [https://technet.microsoft.com/en-us/library/aa998315\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/aa998315(v=exchg.160).aspx).

A simple example of a transport rule is one that rejects email messages sent to a specific external domain name, unless the sender is a member of a group of people who are authorized to send to that domain. More complex rules can be created that have multiple conditions that must be met, and that perform multiple actions. For example, if

the message is sent from an address used to send contact form submissions from a website, and the message has been sent from the IP address of the web server, the action of modifying the spam confidence level (SCL) can be applied to ensure the message does not go to Outlook's junk email folder, as well as adding another recipient to the Bcc field.

When multiple transport rules exist in the organization, they are processed in order of priority. The highest priority rule has a priority of zero. Because an Exchange organization can have thousands of transport rules, managing the order of rules can become a very complex task. The priority order of your transport rules is important because it's possible that a rule you configure to take action on specific messages is never applied, because either:

- A higher priority rule rejected or deleted the message.
- A higher priority rule was configured to stop processing any further rules.

Finally, transport rules can be configured to run in test mode only, so you can verify they are working correctly before you enforce them. Transport rules can also be configured with an automatic start and end date when rules only need to be in effect for a specific period of time.

## Plan and configure journaling

All of the compliance features so far, such as retention policies, in-place archiving, Litigation Holds, and in-place holds, operate in a manner in which a single copy of mailbox items are retained in their original locations. In the case of items under hold that are deleted, a single copy is retained in the recoverable items folder of the mailbox. While these features satisfy the compliance needs of some organizations, others have additional requirements to make copies of email messages and other mailbox contents to a separate location.

In Exchange 2016, journaling is the feature that provides the capability to copy email messages to another location. There are two types of journaling that can be implemented:

- **Standard journaling** Configured on mailbox databases, standard journaling makes copies of all messages sent to or from the mailboxes on that database. Standard journaling is configured in the properties of the mailbox database or by running the Set-MailboxDatabase cmdlet.
- **Premium journaling** Configured using journal rules, premium journaling can make copies of all messages sent within an organization. Journal rules can be applied in a more targeted manner than standard journaling. You can configure journal rules to only journal external email or to only journal email for specific recipients in the organization. Journal rules are configured in the compliance

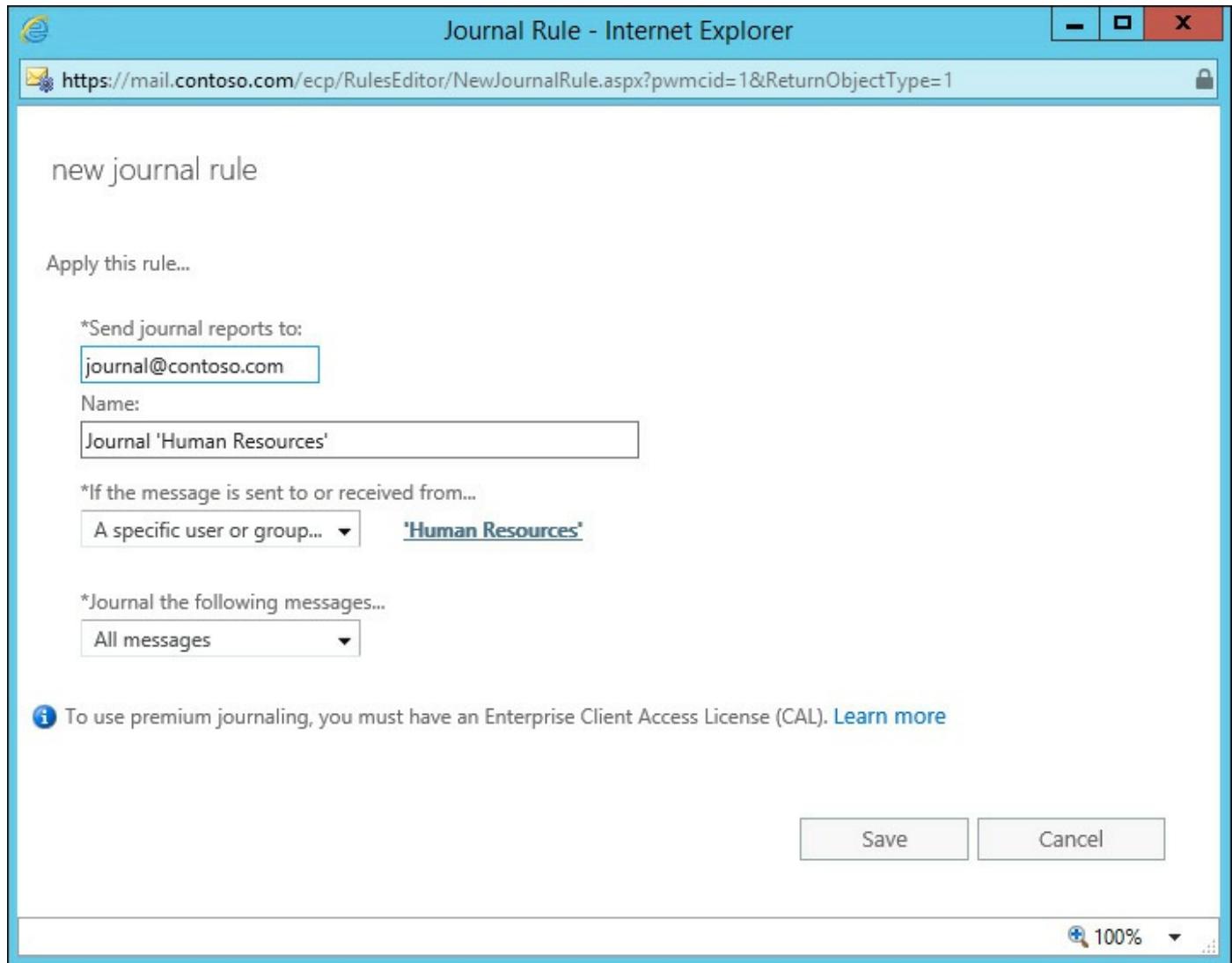
management section of the Exchange admin center or by running the New-JournalRule cmdlet.

Journaling produces journal reports, which are the messages sent to the journaling mailbox. The original message is included with the journal rule as an attachment. The journal mailbox can be a mailbox within the organization or it can be an external SMTP address. Because the journal mailbox contains potentially sensitive messages, you should take care to secure the mailbox from unauthorized access through the use of mailbox permissions. The more people who have access to the journal mailbox, the more concerns there can be when the time comes to use journal reports as evidence for legal proceedings.

You can use a single journal mailbox for all journaling in the organization or you can nominate separate journal mailboxes for different journaling scenarios, such as departments or geographic regions. Journal mailboxes can receive a very high rate of email on a day to day basis, especially when you are journaling every message sent internally and externally for the organization. As such, it is often required to place journal mailboxes on a separate, dedicated mailbox database due to the IOPS requirements of the mailbox, as well as the size of the journal mailbox as it grows over time. When you place journal mailboxes on dedicated databases, you can also disable content indexing for that database to reduce the load on the Exchange server. In doing so, however, you remove the ability to perform searches of the journaling mailbox. This is an issue if you're planning to retain the journal reports in the journal mailbox, but not if you plan to archive the journal reports to a separate, third party archiving system that has its own indexing and search functionality.

Although you can provide high availability for journal mailboxes by using a Database Availability Group, it's possible for the journal mailbox to be unavailable at times. This causes the journal reports to queue on Exchange servers, which might not be desirable. An alternate journaling mailbox for the organization can be configured, which receives any journal reports when the journal mailbox is unavailable. To configure the alternate journal mailbox, use the Set-TransportConfig cmdlet and specify the SMTP address to use for the JournalingReportNdrTo property. You must also consider that if the alternate journal mailbox is unavailable at the same time as the journal mailbox, the journal reports are lost completely. There is a trade-off between the desire to keep transport queues from growing too large, and the risk of both journal mailboxes being unavailable at the same time and therefore causing journal reports to be permanently lost.

When you are configuring a journal rule, as shown in [Figure 5-13](#), you define the scope of the rule by choosing all messages, internal messages only, or external messages only. An internal message is one sent between two recipients that have email addresses that are accepted domains for the organization. An external message is one sent to or from a person who is outside of the Exchange organization.



**FIGURE 5-13** Configuring a journal rule

In addition to the journal rule scope, the journal recipient is also configured. The journal recipient is not the address that receives the journal reports; that is the role of the journal mailbox. Rather, the journal recipient is configured either to include all messages or to only include messages sent or received by a specific user or group. If you configure a journal recipient that is a group, messages sent to or from all members of that group are journaled, not just the messages sent to the distribution group itself. In other words, the distribution group does not need to be a recipient of the message for the message to be journaled, only one or more of the group's members.

### **Note: Journaling IRM-Protected Email Messages**

When you are using journaling as well as Information Rights Management (IRM) in an Exchange 2016 organization, you must plan for the ability to index and search IRM-protected messages when they are archived from the journal mailbox to third party archiving systems. To include a plain text copy of IRM-protected messages in journal reports, use the Set-IRMConfiguration cmdlet to set the JournalReportDecryptionEnabled property to \$true. For more details about the additional IRM permissions configuration that is required, refer to the following TechNet article: [https://technet.microsoft.com/en-us/library/dd876936\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd876936(v=exchg.160).aspx).

## **Summary**

- User education is an important piece of an overall compliance solution. MailTips can be configured by administrators to display messages to users, letting them know about potential issues with email messages that they are composing before they actually send them. Message classifications provide users with the ability to mark email messages in a way that provides guidance to recipients about the intended audience and use of email messages.
- Transport rules provide administrators with very flexible capabilities to enforce compliance rules by taking action on emails that meet specific criteria as they pass through the transport pipeline.
- Journaling is designed to meet the requirement to make a copy of email messages to a secondary location, where they can be retrieved if necessary for investigations or legal matters.

## **Skill 5.5: Plan, manage, and use mailbox and administrative auditing**

Within an Exchange 2016 organization it's important to be able to audit and report on who has made changes to mailboxes and other objects. This type of auditing is provided in Exchange 2016 through the use of mailbox audit logging. Mailbox audit logging is used to track actions performed against mailbox folders and items, and administrator audit logging. Administrator audit logging is used to track actions performed against objects in the environment by administrators, who are running the Exchange management tools.

---

## This section covers how to:

- [Plan and configure mailbox audit logging](#)
  - [Plan and configure administrative audit logging](#)
  - Search and interpret audit logs
- 

## Plan and configure mailbox audit logging

When you need to know who took action on an item in a mailbox, you can turn to mailbox audit logging to get the answer. Mailbox audit logging is capable of tracking the actions taken by mailbox owners and delegates on mailbox folders and items. Consider scenarios such as a team that uses a shared mailbox to communicate with their customers. You might be asked to determine who deleted a customer's email or who sent an email from the shared mailbox's email address to a customer.

Mailbox audit logging is not enabled by default on new mailboxes, nor is it configured to track all user behaviors. Mailbox audit logging is configured on a per-mailbox basis. You can view the existing configuration of a mailbox by running the Get-Mailbox cmdlet, as shown in [Listing 5-5](#). The default configuration of mailbox audit logging on a new mailbox is:

- Mailbox audit logging is disabled.
- Audit log entries are retained for 90 days.
- Mailbox owner actions are not logged.
- Some delegate and administrator actions are logged.

### LISTING 5-5 The default mailbox audit logging configuration for a user mailbox

[Click here to view code image](#)

---

```
#Viewing the mailbox audit logging configuration for a mailbox using
PowerShell

[PS] C:\>Get-Mailbox Kim.Akers@contoso.com | fl *audit*

AuditEnabled      : False
AuditLogAgeLimit : 90.00:00:00
AuditAdmin        : {Update, Move, MoveToDeletedItems, SoftDelete,
HardDelete,
FolderBind, SendAs, SendOnBehalf, Create}
AuditDelegate     : {Update, SoftDelete, HardDelete, SendAs, Create}
AuditOwner        : {}
```

---

The AuditDelegate actions log any actions performed by mailbox delegates, mailbox

users who have shared access to a mailbox, and any service or administrator accounts that access mailbox contents. This means that if you grant access to a mailbox for your administrator account, actions that you take are logged according to the AuditDelegate settings. The AuditAdmin settings apply to mailbox access via eDiscovery searches, mailbox import/export operations, and external tools such as MFCMAPI.

## Mailbox audit log storage

Mailbox audit log data is stored in a sub-folder of the Recoverable Items folder named Audits. These mailbox folders are hidden from the mailbox owner and can't be accessed using clients like Outlook or Outlook on the web. Given that the mailbox audit logging data is stored for 90 days by default, you must plan for the impact that has on the size of the mailbox databases in your organization.

The amount of log data generated for a mailbox depends on which actions you're logging, whether you're logging for mailbox owners as well as delegates, and how busy that audited activity is. For example, if you enable mailbox audit logging of delegate actions for a mailbox user that has one delegate who occasionally helps manage calendar items, you can expect to see an increase in mailbox size of 1-2 percent. In contrast, if you enable every delegate logging option for a shared mailbox that is used by a large team, you can expect a much higher percentage increase in the size of the mailbox.

This means that you should carefully plan your mailbox audit logging configuration, so that you achieve the outcome you want in terms of auditing of mailbox activity, without having an adverse impact on your Exchange server's storage capacity.

## Configuring mailbox audit logging

Because mailbox audit logging is not enabled by default, you need to enable it on any mailboxes you need it for. Mailbox audit logging can be enabled and disabled by members of the Organization Management and Records Management role groups. To enable mailbox audit logging on a mailbox, use the Set-Mailbox cmdlet.

[Click here to view code image](#)

```
#Enabling mailbox audit logging using PowerShell
```

```
[PS] C:\>Set-Mailbox Kim.Akers@contoso.com -AuditEnabled $true
```

The Set-Mailbox cmdlet is also used to add further actions for mailbox audit logging to include in its logging. For example, the following command is used to add logging of soft deletes and hard deletes by the mailbox owner.

[Click here to view code image](#)

```
#Enabling additional mailbox audit logging actions
```

```
[PS] C:\>Set-Mailbox -Identity Kim.Akers@contoso.com -AuditOwner @  
{add='SoftDelete,HardDelete'}
```

In some organizations, a service account is used for frequent mailbox access by external systems, such as email archiving solutions. When mailbox audit logging is enabled, this access by service account triggers a high volume of logging that increases the amount of mailbox storage used. In this situation, a mailbox audit logging bypass can be configured for the service account by using the Set-MailboxAuditBypassAssociation cmdlet.

[Click here to view code image](#)

```
#Configuring a mailbox audit logging bypass
```

```
[PS] C:\>Set-MailboxAuditBypassAssociation -Identity  
serviceaccount@contoso.com  
-AuditBypassEnabled $true
```

## Searching mailbox audit logs

Searches of the mailbox audit logs are performed using the Search-MailboxAuditLog cmdlet. Each of the auditing types, Admin, Delegate, and Owner, can be searched individually or in a single search by using the LogonTypes parameter. Mailbox audit log searches can also be limited to a specific date range to speed up the search. To perform a mailbox audit log search, the user who is running the search must be a member of either the Organization Management, Records Management, or Compliance Management role group. The Compliance Management role group provides view-only access to mailbox audit logs.

Consider a scenario in which the user Dan Jump has sent a report via email to Kim Akers. After a few days, Dan follows up to see why he has not received a response. Kim advises Dan that she never saw the email. A help desk call is raised to investigate further. After reviewing the case, it is noticed that Kim's mailbox is also accessible by the user Alex Darrow. You decide to conduct a mailbox audit log search to determine whether any delegates of Kim's mailbox have deleted the missing email. For this scenario, the following command is used to display the mailbox audit logs.

[Click here to view code image](#)

```
#Performing a mailbox audit log search
```

```
[PS] C:\>Search-MailboxAuditLog -Identity "Kim Akers" -LogonTypes Delegate  
-ShowDetails
```

Mailbox audit logs can also be searched by performing a non-owner search, found under auditing in the compliance management section of the Exchange admin center, as shown in [Figure 5-14](#). Non-owner access reports can be generated for a date range and

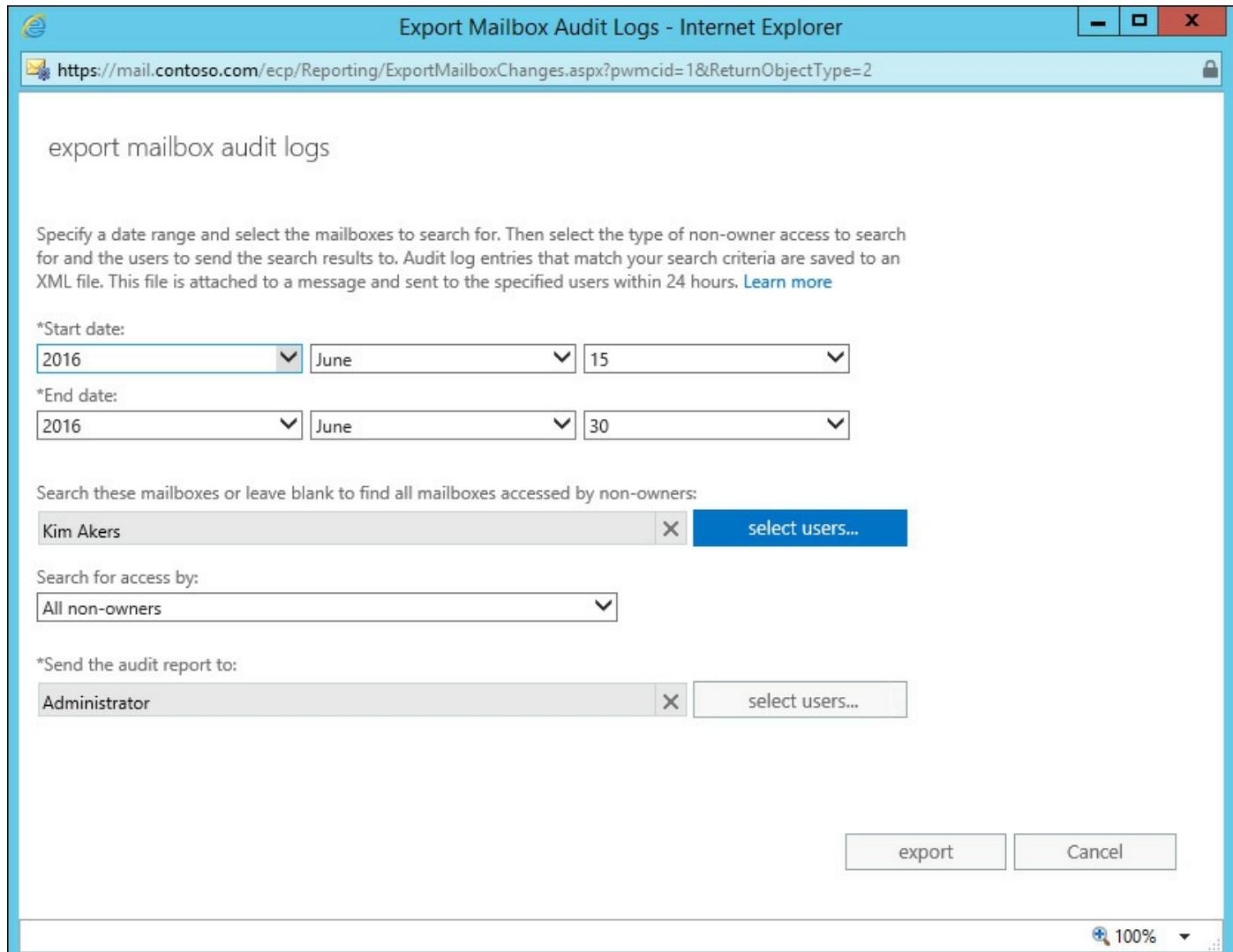
for a specific mailbox or across all mailboxes.

The screenshot shows a Microsoft Internet Explorer window titled "Search for Mailboxes Accessed by Non-Owners - Internet Explorer". The URL in the address bar is <https://mail.contoso.com/ecp/Reporting/NonOwnerAccessReport.aspx?pwmcid=1&ReturnObjectType=2>. The page contains the following fields and information:

- Search for mailboxes accessed by non-owners**
- Specify a date range and select the mailboxes to search for. Then select to search for non-owner access by anyone or by users inside or outside your organization. [Learn more](#)**
- \*Start date:** 2016 June 13
- \*End date:** 2016 June 28
- Search these mailboxes or leave blank to find all mailboxes accessed by non-owners:** (A text input field followed by a "select mailboxes..." button)
- Search for access by:** (A dropdown menu set to "All non-owners")
- Buttons:** "search" (blue) and "clear"
- Search results table:** Headers: Mailbox, LAST ACCESSED: (sorted by ascending). Subtext: "There are no items to show in this view." (with a printer icon)
- Buttons:** "Close" (bottom right)

**FIGURE 5-14** Running a non-owner access report in the Exchange admin center

Mailbox audit logs can also be exported to an XML file which is sent to an email address. There are two methods for exporting the XML file. The first is to choose Export mailbox audit logs, found under auditing in the compliance management section of the Exchange admin center, as shown in [Figure 5-15](#). You can choose a date range for the log data you want to search and you can also choose which types of access you're interested in seeing. The report is generated and sent to the specified recipient within 24 hours.



**FIGURE 5-15** Exporting mailbox audit logs to an XML file

The same XML report can be exported by running the `New-MailboxAuditLogSearch` cmdlet. At a minimum, the cmdlet requires at least one mailbox to be searched and a start and end date for the search. You can also specify the recipient who receives the report email and the logon types that you are searching for.

[Click here to view code image](#)

```
#Exporting mailbox audit logs to XML using PowerShell
```

```
[PS] C:\>New-MailboxAuditLogSearch -Name "Non-owners" -Mailboxes  
"Kim.Akers","Alex.  
Darrow" -LogonTypes Admin,Delegate -StatusMailRecipients  
administrator@contoso.com  
-StartDate 6/1/2016 -EndDate 6/30/2016
```

### **Note: Mailbox Audit Logging Delays**

Searching for mailbox audit log results less than 24 hours old can give you unreliable results. Under some conditions, you can expect accurate mailbox audit log results after 1 hour of an activity being performed on a mailbox.

For the most accurate results, however, you should consider 24 hours to be the delay.

## **Plan and configure administrative audit logging**

Administrator audit logging captures changes made by administrators when they use the Exchange management tools to administer objects in the organization. Changes made using other tools, such as Active Directory Users and Computers, are not logged. By default, administrator audit logging includes any administrative action that makes a change, for example using Remove-Mailbox. Administrative actions that do not make a change, for example using Get-Mailbox, are not logged.

The default configuration of administrator audit logging in an Exchange organization is:

- Administrator audit logging is enabled
- Audit log retention is set to 90 days
- All cmdlets that can make changes and all parameters of those cmdlets are logged
- Test cmdlets, such as Test-MapiConnectivity, are not logged
- The Log Level is set to None

### **Important: What Does the Log Level Mean?**

The Log Level setting of None doesn't mean that nothing is logged. Instead, it means that only the details of the command that was run, who ran it, and which object they modified are logged. The other option for Log Level is Verbose, which also logs the old and new values of the properties that were modified by the command.

Administrator audit logs are stored in a special mailbox type called an arbitration mailbox, which is named SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}. In a coexistence environment with older versions of Exchange, the arbitration mailbox used for administrator audit logging must be hosted on an Exchange 2016 mailbox database, otherwise it does not log actions performed using the Exchange 2016 management tools.

## Configuring Administrator Audit Logging

Changes to the administrator audit log configuration can be made by any member of the Organization Management or Records Management groups. Those are powerful administrative groups, and administrators who are members of those groups can even disable administrator audit logging. Although disabling administrator audit logging is also logged to the administrator audit logs, it can still be used to hide malicious administrative actions. Therefore, it is recommended to limit the membership of those groups to trusted individuals only.

The administrator audit log settings are configured by running the Set-AdminAuditLogConfig cmdlet. For example, to configure the log retention to 180 days and enable verbose logging, use the following command.

[Click here to view code image](#)

```
#Configuring administrator audit logging settings
```

```
[PS] C:\>Set-AdminAuditLogConfig -AdminAuditLogAgeLimit 180.00:00:00 -  
LogLevel Verbose
```

## Searching administrator audit logs

Administrator audit logs can be searched by users who are members of the Organization Management, Records Management, or Compliance Management role groups. To search administrator audit logs, use the Search-AdminAuditLog cmdlet. There are several approaches that can be used to search admin audit logs:

- Use the Cmdlets parameter to search for uses of specific cmdlets, such as Add-MailboxPermission.
- Use the ObjectIds parameter to search for modifications to specific objects, such as mailbox users.
- Use the UserIds parameter to search for modifications performed by a specific user account.

### Need More Review? Search-AdminAuditLog parameters

A full list of parameters that can be used to refine Search-AdminAuditLog searches can be found on TechNet at [https://technet.microsoft.com/en-us/library/ff459250\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/ff459250(v=exchg.160).aspx).

The parameters mentioned previously can be combined into a single command. For example, to search for all uses of the Add-MailboxPermission cmdlet by the user Administrator, the command shown in [Listing 5-6](#) can be used.

## LISTING 5-6 Searching administrator audit logs

[Click here to view code image](#)

---

```
#Searching administrator audit logs

[PS] C:\>Search-AdminAuditLog -Cmdlets Add-MailboxPermission -UserIds
Administrator@contoso.com

RunspaceId      : e90ba2ae-92a3-4fc1-a800-49a83c8a07c7
ObjectModified   : contoso.com/Company/Users/Kim Akers
CmdletName       : Add-MailboxPermission
CmdletParameters : {Identity, AccessRights, User}
ModifiedProperties: {}
Caller           : Administrator@contoso.com
ExternalAccess    : False
Succeeded         : True
Error             :
RunDate          : 6/28/2016 9:26:00 PM
OriginatingServer : NY-EXCH01 (15.01.0396.030)
Identity          :
AAMkAGQ2Y2E3YTU1LTNlMjMtNDVmMC04NWUxLWEwNWQxYmE2YTc5MwBGAAAAAAA

v+bnz9KpATIKSyMS8Xoy/BwDQxTkFL6NQSrCV7K3dnPiAAAAAAEZAADQxTkFL6NQ
SrCV7K3dnPiAAAbtM6DAAA=
IsValid          : True
ObjectState       : New
```

---

In the output shown in [Listing 5-6](#), the action performed by the user Administrator has been logged, however the precise details of the change the administrator made are not visible. This is because the information is stored in a hash table in the CmdletParameters property of the results. To view the details of the cmdlet parameters, use the PowerShell technique demonstrated in [Listing 5-7](#).

## LISTING 5-7 Searching administrator audit logs

[Click here to view code image](#)

---

```
#Searching administrator audit logs

[PS] C:\>$results = Search-AdminAuditLog -Cmdlets Add-MailboxPermission -
UserIds administrator@contoso.com

[PS] C:\>$results[0].CmdletParameters

Name          Value
----          -----
Identity      kim.akers
AccessRights  FullAccess
```

For complex or long-running searches, or when automatic scheduled searches need to be performed, the administrator audit log search results can be automatically emailed to a recipient by running the New-AdminAuditLogSearch cmdlet. The report typically arrives within 15 minutes and the results are provided as an XML file. For example, to email a report of all uses of the Add-MailboxPermission cmdlet during a certain date range, use the following command.

[Click here to view code image](#)

```
#Creating a new administrator audit log search
```

```
[PS] C:\>New-AdminAuditLogSearch -Name "Add mailbox permissions" -Cmdlets
Add-
MailboxPermission -StatusMailRecipients administrator@contoso.com -
StartDate 6/1/2016
-EndDate 6/28/2016
```

A similar report can be generated from the Exchange admin center by selecting “Export the admin audit log” under auditing in the compliance management section. This option includes all of the administrator audit log entries for the specified time period and can take up to 24 hours to be produced.

## Summary

- Mailbox audit logging is used to track actions taken by mailbox owners, delegates, and admins on mailbox contents. Mailbox audit logging must be enabled and configured on a per-mailbox basis.
- Administrator audit logging is used to track actions taken by administrators on Exchange objects using the Exchange management tools. Administrator audit logging is enabled by default for the organization.
- Audit logs can be searched from PowerShell and the Exchange admin center. Audit log search results can be exported to XML files and sent to an email recipient.

## Thought experiment

In this thought experiment, demonstrate your skills and knowledge of the topics covered in this chapter. You can find answer to this thought experiment in the next section.

Contoso, Ltd. is deploying Exchange 2016 for their organization. As a business that operates in the financial industry, they need to ensure that personal and financial details of their customers are not exposed to unauthorized personal. Due to the sensitive nature of the correspondence in board member mailboxes, it is necessary to prevent the

permanent deletion of items from their mailboxes. Furthermore, they need to ensure that customer email correspondence is retained for 10 years, in case of the need to refer to it for a legal case in the future.

1. What type of compliance solution should Contoso, Ltd. implement to protect customer financial details from exposure?
2. How can the board members' mailboxes be configured to prevent the permanent deletion of items?
3. What should you configure to preserve customer correspondence for 10 years?

## Thought experiment answer

This section contains the answers to the thought experiment.

1. A Data Loss Prevention (DLP) policy should be implemented that detects customer personal and financial details, using the DLP templates provided by Exchange. The DLP policy should be customized to prevent sensitive data from being sent to external recipients. Furthermore, incident reports should be configured on the DLP policy rules to alert internal compliance officers when users override the policies internally.
2. Each of the board members' mailboxes should be enabled for Litigation Hold.
3. Multiple solutions can be combined to meet the objective of preserving customer correspondence for 10 years. First, any shared mailboxes that are used for customer correspondence can be placed on Litigation Hold, with a hold duration of 3660 days, which is 10 years plus a few extra days to account for leap years. Second, a journal rule for external emails should be configured so that any emails between individual staff members and customers are preserved. The journal mailbox should have a retention policy that removes messages after 3660 days and a Litigation Hold for the same duration.

# **Chapter 6. Implement and manage coexistence, hybrid scenarios, migration, and federation**

Very few Exchange 2016 deployments occur where servers are deployed into a brand new environment with no pre-existing data to be concerned about. The majority of deployments are migrations from previous versions of Exchange on-premises or migrations to Exchange Online (Office 365). In addition to migration scenarios, some Exchange organizations need to integrate with other organizations for the purposes of collaborating, often in situations where companies are merging or divesting.

Exchange 2016 supports a variety of techniques for establishing coexistence with other Exchange versions, organizations, or with Exchange Online. An organization can establish minimal integration with other organizations, such as visibility of calendar free/busy information, or can establish a tightly integrated solution whereby two organizations work together seamlessly as one, such as a Hybrid configuration with Exchange Online.

## **Skills in this chapter:**

- [Plan, deploy, and troubleshoot coexistence with Office 365 \(Exchange Online\)](#)
- [Plan, deploy, manage, and troubleshoot Exchange federation](#)
- [Plan, deploy, and troubleshoot on-premises coexistence with earlier supported versions of Exchange](#)
- [Migrate from earlier supported versions of Exchange](#)

## **Skill 6.1: Plan, deploy and troubleshoot coexistence with Office 365 (Exchange Online)**

Exchange Online is the hosted version of Exchange that is run by Microsoft as part of the Office 365 cloud service. Exchange Online runs the same codebase as on-premises Exchange, which means that today Exchange Online is running Exchange 2016 code. There are undoubtedly some differences between the code provided to on-premises customers, as compared to the code running in the cloud. On-premises customers receive updates on a quarterly basis containing features and improvements that have been thoroughly tested in Exchange Online first. It's natural to expect that the cloud service is running code that is several versions ahead of the latest update provided to on-premises customers. Also, Exchange Online is wrapped in layers of automation and orchestration that most customers simply don't have the need to deploy on-premises. Exchange Online is tightly integrated with other services in Office 365, such as SharePoint Online, Skype for Business Online, OneDrive for Business, Delve Analytics, and many more.

When migrating from an on-premises Exchange server to Exchange Online there are several migration options for you to consider. Exchange 2016 supports cutover migrations, Hybrid configuration, IMAP migration, PST import, and third party migration tools. The Hybrid configuration approach provides a period of coexistence between the on-premises organization and Exchange Online, making it ideal for scenarios where all of the users and mailbox data can't be migrated in a single, short period of time. Hybrid configuration is also the solution for scenarios where there is a permanent coexistence in place, with some mailboxes located on-premises and some located in the cloud.

The staged migration approach, which is available for Exchange 2007 and earlier, is not supported for Exchange 2016. Hybrid configuration is recommended instead. All of the other migration methods that are available, such as cutover, IMAP, PST, and third party tools, do not provide for a coexistence period. While that is suitable for many customers who just need a quick migration to Exchange Online and those who are willing to bear some disruption while the migration occurs, the migration experience a Hybrid configuration provides is better overall for administrators and end users, particularly in large environments.

## This section covers how to:

- [Plan, deploy, and manage hybrid configuration](#)
- [Evaluate limitations of the Hybrid Configuration Wizard](#)
- [Troubleshoot transport with Exchange Online](#)
- [Troubleshoot client access with Exchange Online](#)
- [Troubleshoot directory synchronization](#)

## Plan, deploy, and manage hybrid configuration

A Hybrid Exchange configuration establishes a coexistence relationship between an on-premises Exchange organization and Exchange Online. The two organizations, while remaining separate, coexist in a way that appears to the user as one whole organization. Hybrid configurations can be used as a migration path between Exchange on-premises and Exchange Online, or as a permanent state of coexistence. Hybrid configuration provides:

- Improved sign-on experience for users, using either “same sign-on” or “single sign-on”. Both of these options can be abbreviated as SSO, but have different implementations that are covered later in this section.
- Protection from spam, phishing, and malware emails by using Exchange Online Protection (EOP), Microsoft’s cloud-hosted email security service to process inbound emails. EOP also scans email sent between on-premises and online mailboxes to ensure that a virus outbreak on-premises doesn’t spread into the cloud as well.
- Rich coexistence between on-premises Exchange and Exchange Online mailboxes, by providing a common Global Address List, calendar free/busy sharing, and treating email between on-premises and online mailboxes as internal email. To the user this makes it appear that everyone is part of the one organization, for the most part. There are some caveats with cross-premises access though. An Exchange Online mailbox user can’t access a shared mailbox, or another user’s mailbox for which they are a delegate, if the other mailbox is hosted on-premises. The same is true in the reverse scenario as well. This cross-premises limitation means that you must carefully plan where your mailboxes are hosted, so that teams who use a shared mailbox, and any users who have delegates, are hosted together either on-premises or online.
- The capability to migrate some or all of your organization’s mailboxes to Exchange Online, at your own pace. A Hybrid configuration is the only scenario that supports off-boarding of mailboxes from Exchange Online back to an on-

premises server. This is important if you need to move people back and forth due to their job roles. You can also provision archive mailboxes in Exchange Online to offload the burden of storing archive data on your on-premises Exchange servers.

A Hybrid configuration can be established between Exchange Online and any of the following versions of Exchange:

- Exchange Server 2010 updated to at least Service Pack 3.
- Exchange Server 2013 running a supported cumulative update. Hybrid configurations are supported for the latest and the previous cumulative update. At the time of this writing, cumulative update 13 (CU13) is the latest, which means that CU13 and CU12 are both supported for a Hybrid configuration. Since cumulative updates are released every three months by Microsoft, by the time you read this you can expect to find that neither CU13 nor CU12 are supported any more.
- Exchange Server 2016 running a supported cumulative update. Exchange 2016 has the same cumulative update release cadence and conditions as Exchange 2013. At the time of this writing, cumulative update 2 (CU2) is the latest.

If your organization is running an earlier version of Exchange, you need to add a server running one of the Hybrid-capable versions of Exchange previously listed. Microsoft provides a free Hybrid license for customers who need the Hybrid functionality, but who don't plan to host any mailboxes on the server. If you do plan to host mailboxes on the server, you're not eligible for the free Hybrid license and need to purchase the appropriate Exchange server and client access licenses.

#### **Note: There is no “Hybrid Server” Role**

There is often confusion about the term “Hybrid server” and how it relates to the Exchange 2016 server roles architecture. A “Hybrid server” is not a special server role, rather it is a term used to describe an Exchange 2016 mailbox server that is assigned to the task of handling Hybrid connectivity for the organization.

In addition to the requirement to run one of the previously mentioned versions of Exchange, you should also ensure that your Exchange servers continue to be updated to the latest service pack, update rollup, or cumulative update for the version of Exchange you're running. Maintaining updates to your on-premises server is important for ongoing compatibility as the code in Exchange Online continues to change over time. It is also important to remain in a supported Microsoft configuration should you ever need to call them for assistance with a technical issue.

## Hybrid Configuration and Identity Management

A Hybrid configuration requires that a synchronized identity model be implemented. An Office 365 tenant is not enabled for directory synchronization by default. You must enable it using the Office 365 admin portal first before you start synchronizing objects from the on-premises Active Directory. Synchronized identity involves the deployment of a directory synchronization tool, such as Microsoft's DirSync, Azure Active Directory Sync (AAD Sync), or Azure Active Directory Connection (AAD Connect). Although all of those directory synchronization tools are currently supported by Microsoft, both DirSync and AAD Sync have been deprecated and are no longer receiving updates from Microsoft. It's recommended for new Hybrid configurations that you use AAD Connect for the directory synchronization requirements. The directory synchronization tool can be installed on a dedicated server or on an existing server, including domain controllers, making it a low-cost solution to implement.

When directory synchronization is deployed, the on-premises Active Directory becomes the source of identity for the organization. Objects and their attributes, such as a user and their mail attributes, are synchronized from the on-premises Active Directory to Azure Active Directory. Azure Active Directory is hosted by Microsoft as part of their cloud services, as shown in [Figure 6-1](#). When a user logs on to Office 365 services, they are using the credentials of the Azure Active Directory user account to do so. This raises the matter of passwords for the Azure Active Directory user accounts. Having to manage two sets of user credentials for on-premises and Office 365 services is burdensome to the user. Even if you initially configure both accounts with the same password, eventually one of the passwords expires and needs to be updated by the user, making them different from each other and difficult to remember for a typical user. To solve this problem, the directory synchronization tool can also synchronize user account passwords so that the same password exists for the user account in Azure Active Directory. When the user updates their on-premises password, it is automatically synchronized to Azure Active Directory, usually within a few minutes. By automatically maintaining synchronized passwords on-premises and in Office 365, you are able to provide a "same sign-on" experience for the user.

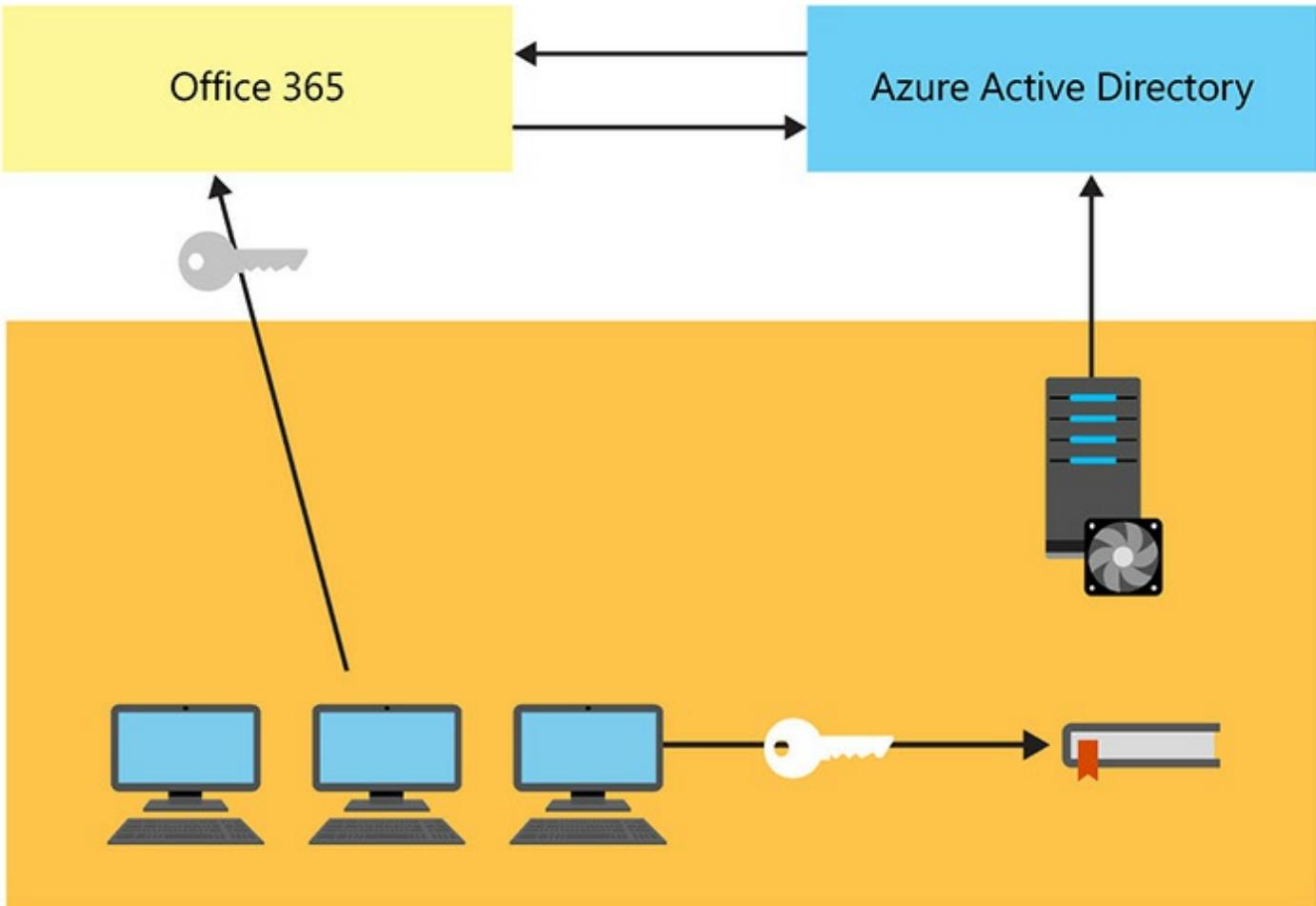


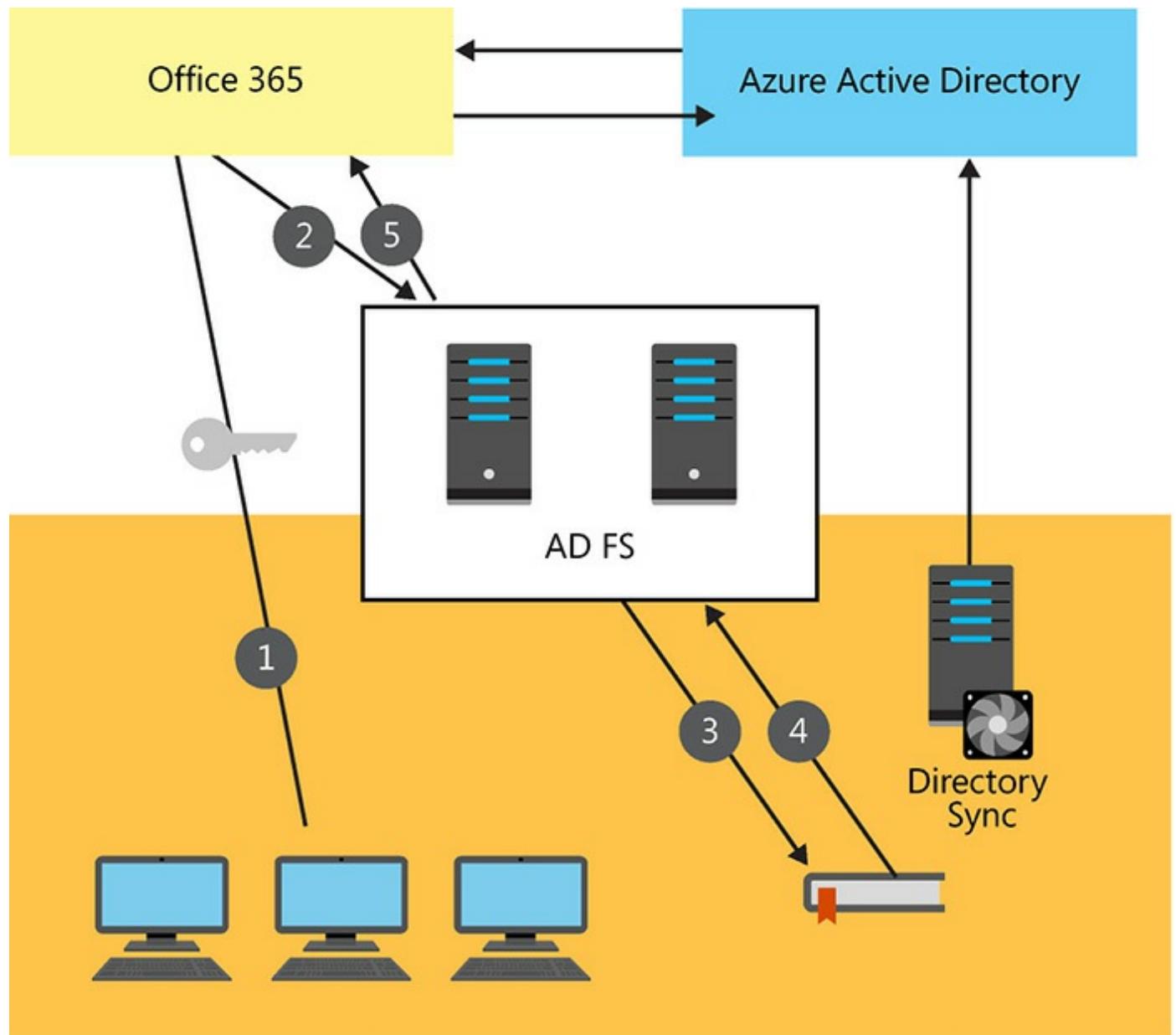
FIGURE 6-1 Synchronization of Active Directory objects to Azure Active Directory

### Need More Review? Synchronization of Passwords to Azure Active Directory

When you first begin studying password synchronization, it's quite normal to have some security concerns. After all, password security is important, so anything that is transmitting or storing passwords outside of your organization deserves scrutiny. You can read more about the security of the password hash synchronization process in Microsoft's Azure documentation at <https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnectsync-implement-password-synchronization/>.

Although directory synchronization is required, password synchronization is not a mandatory configuration. You might prefer to deploy a federated identity model to meet your organization's requirements instead. Federated identity uses directory synchronization to synchronize users and other objects to Azure Active Directory. Instead of using the password of the Azure Active Directory user object, however, any

authentication requests are passed back to the on-premises Active Directory to validate. This is achieved by deploying an on-premises Active Directory Federation Services (AD FS) infrastructure, which can be made up of one or more AD FS servers and optionally one or more Web Application Proxy (WAP) servers. AD FS is then responsible for authenticating the user and providing an authentication token for the user to access the cloud services in Office 365, as shown in [Figure 6-2](#).



**FIGURE 6-2** The AD FS authentication flow

Using AD FS provides for a nearly seamless single sign-on experience for users when they are connecting to many of the Office 365 services, particularly when using a web browser. In addition, AD FS allows your organization to enforce security policies such as logon hours, immediate disabling of accounts, third party multi-factor authentication, and restricting the IP address ranges that your users can access Office

365 services from.

The federated identity model removes the need to synchronize password hashes to Azure Active Directory for a single sign-on experience. In reality, you can still synchronize the password hashes, they just aren't used during authentication. Having them synchronized and available in Azure Active Directory, however, opens up the capability to switch from a federated identity model to a synchronized identity model. You could use this configuration in the event that the on-premises Active Directory or AD FS infrastructure becomes unreachable by the Office 365 services, such as in the event of a datacenter or Internet connectivity failure. This is not a trivial undertaking though, and shouldn't be relied on for day-to-day operational issues. Instead, it can be considered as a disaster recovery option when a serious failure occurs.

The nature of the federated identity model highlights the importance of ensuring the availability of your on-premises infrastructure when you are deploying the federated identity model. This configuration is not well suited to on-premises environments that have single points of failure that can make the entire infrastructure unavailable. Ideally, your on-premises environment spans multiple datacenters with redundant Internet connections and you are able to deploy multiple AD FS and WAP servers with load balancing. Such an investment in infrastructure might be uneconomical for your organization. You need to balance the technical and security requirements of your organization with the cost of deploying the required infrastructure to support it.

## **Preparing an Office 365 tenant for hybrid configuration**

Before you can create a Hybrid configuration, you must have an Office 365 tenant and be licensed to use Exchange Online. Exchange Online can be licensed independently of other services in Office 365 with plans such as Exchange Online Plan 1 and Exchange Online Plan 2, or it can be licensed by purchasing one of the bundled subscription options such as Enterprise E1 or Enterprise E3. All of the Office 365 subscriptions with Exchange Online support directory synchronization and Hybrid configurations.

After provisioning your Office 365 tenant, you need to add your organization's domain names to the tenant. By default, the tenant has one domain called the service domain and uses a naming convention of tenantname.onmicrosoft.com, for example contoso.onmicrosoft.com. Adding a domain name, sometimes referred to as a custom domain, to Office 365 requires you to complete a validation process to prove that you own and control the domain name. The validation process involves adding DNS records to the public DNS zone for the domain name. Microsoft offers two different DNS records that you can choose from, a TXT record or an MX record. The MX record points to Microsoft servers. Adding an MX record to your public DNS zone immediately after provisioning the tenant might be detrimental to your existing inbound mail flow, so it's usually better to use the TXT record to validate your domain names.

The domain validation process means that any domain name you can't prove ownership of can't be used in Office 365. This means that if your on-premises Active Directory uses a .local domain name, such as contoso.local, and the user principle name (UPN) of your Active Directory user accounts also uses that domain name, for example Kim.Akers@contoso.local, you are not able to validate that domain name for Office 365. When directory synchronization is enabled the user accounts provisioned in Azure Active Directory default to using the service domain for your tenant as the username, for example Kim.Akers@contoso.onmicrosoft.com. This is not ideal and the UPNs for on-premises Active Directory user accounts should be changed before you begin synchronizing to the cloud. The UPNs can be changed to any domain name that you can validate in Office 365, but the recommended approach is to match the UPN to the primary SMTP address for the user. This makes the user's life a little easier because they only need to remember to log on to Office 365 services with their email address and password.

### Note: Cleaning Up Active Directory

Trying to synchronize an unhealthy Active Directory to Azure AD is problematic. Directory synchronization has trouble synchronizing invalid data in the attributes of users and other objects, which tends to accumulate over time for any on-premises Active Directory. You can run the IDFix tool, provided by Microsoft, to scan your Active Directory and detect issues that cause directory synchronization problems, giving you a chance to proactively resolve the problems.

## Preparing the on-premises environment

The Hybrid configuration requires some firewall ports to be open. TCP port 25 is needed so that mail flow between Exchange on-premises and Exchange Online Protection (EOP) can occur. The EOP servers either connect to Exchange 2016 mailbox servers or to Exchange 2016 Edge Transport servers. The use of Edge Transport servers for Hybrid mail flow is optional, and suits organizations that don't like having external SMTP connections entering their core network. By placing one or more Edge Transport servers in a perimeter network, Hybrid mail flow can still occur while aligning with the customer's security policies. The other firewall port that is required is TCP 443 for HTTPS access, so that Exchange Online can connect to the on-premises Exchange server for calendar free/busy information.

## Need More Review? Office 365 URLs and IP Address Ranges

Microsoft maintains an up to date list of the URLs and IP address ranges that are needed for accessing each of the Office 365 services, including for Hybrid configurations. You can read the list, as well as Microsoft's guidance for using domain name-based filtering instead of IP address-based filtering, on the Office Support website at <https://support.office.com/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2?ui=en-US&rs=en-US&ad=US&fromAR=1>.

Because there are communications occurring over HTTPS, an SSL certificate is required on the on-premises Exchange server. The SSL certificate must be issued by a trusted, third party certificate authority (CA). The self-signed certificate Exchange installs by default can't be used for a Hybrid configuration because it can't be trusted by Exchange Online. SMTP communications are also encrypted using TLS, so the same certificate can be used for both HTTPS and SMTP. If you are planning to use Edge Transport servers for Hybrid mail flow, the same requirement applies to the Edge Transport server's SMTP certificate; it must be from a trusted, third party CA and not be a self-signed certificate.

## Running the Hybrid Configuration Wizard

Creating a new Hybrid configuration is performed by running the Hybrid Configuration Wizard, which is launched from the Exchange admin center. You can access the Exchange admin center using a web browser by navigating to <https://servername/ecp>, and logging on with your Exchange administrator credentials. The Exchange admin center has navigation tabs at the top left for Enterprise and Office 365. The first time you click Office 365, you are taken to the Office 365 login portal. Before logging in, make sure that the Exchange admin center URL, as well as \*.office365.com, are added to the trusted sites list in your web browser. After logging in to the Office 365 portal, you are able to manage both on-premises and Exchange Online using the same web interface, including launching the Hybrid Configuration Wizard.

The Hybrid Configuration Wizard is launched by selecting Hybrid from the left-hand menu of the Exchange admin center, and then by clicking Configure to start the wizard, as shown in [Figure 6-3](#). As you walk through the Hybrid Configuration Wizard it configures the following items for you:

- The client access services on the Exchange 2016 mailbox server are configured to enable the Mailbox Replication Service Proxy (MRS Proxy), which facilitates mailbox moves between Exchange on-premises and Exchange Online.

- The domain names used for the Hybrid configuration are enabled. If you have one accepted domain in the on-premises organization, that domain is enabled for Hybrid. If you have multiple accepted domains, you are prompted to choose which domain names are going to be used for Hybrid.
- The federation trust is enabled for the on-premises organization, so that calendar free/busy information can be shared with Exchange Online. The federation trust requires you to validate ownership of your domain names again. Even though you've already validated ownership for enabling the domains in Office 365, this step is required for validating ownership with the Azure Active Directory Authentication System, previously called the Microsoft Federation Gateway. A TXT record needs to be added to the public DNS zone for your domain name to complete the validation.
- Secure mail flow between the on-premises and online organizations is established by creating connectors. Inbound and outbound connectors are created in Exchange Online, and send and receive connectors are created on-premises. The on-premises connectors need to be configured with the SSL certificate that is used for TLS encryption of the SMTP connections. You also need to choose whether to use centralized transport. By default, centralized transport is not enabled, which allows the Exchange Online mailboxes to route outbound email directly to the Internet. Only email destined for on-premises mailboxes is sent via the Hybrid mail flow. If centralized transport is enabled, all email sent from Exchange Online mailboxes routes to the on-premises server first, where you can apply any necessary transport rules or compliance requirements for your organization before the messages are routed out to the Internet.

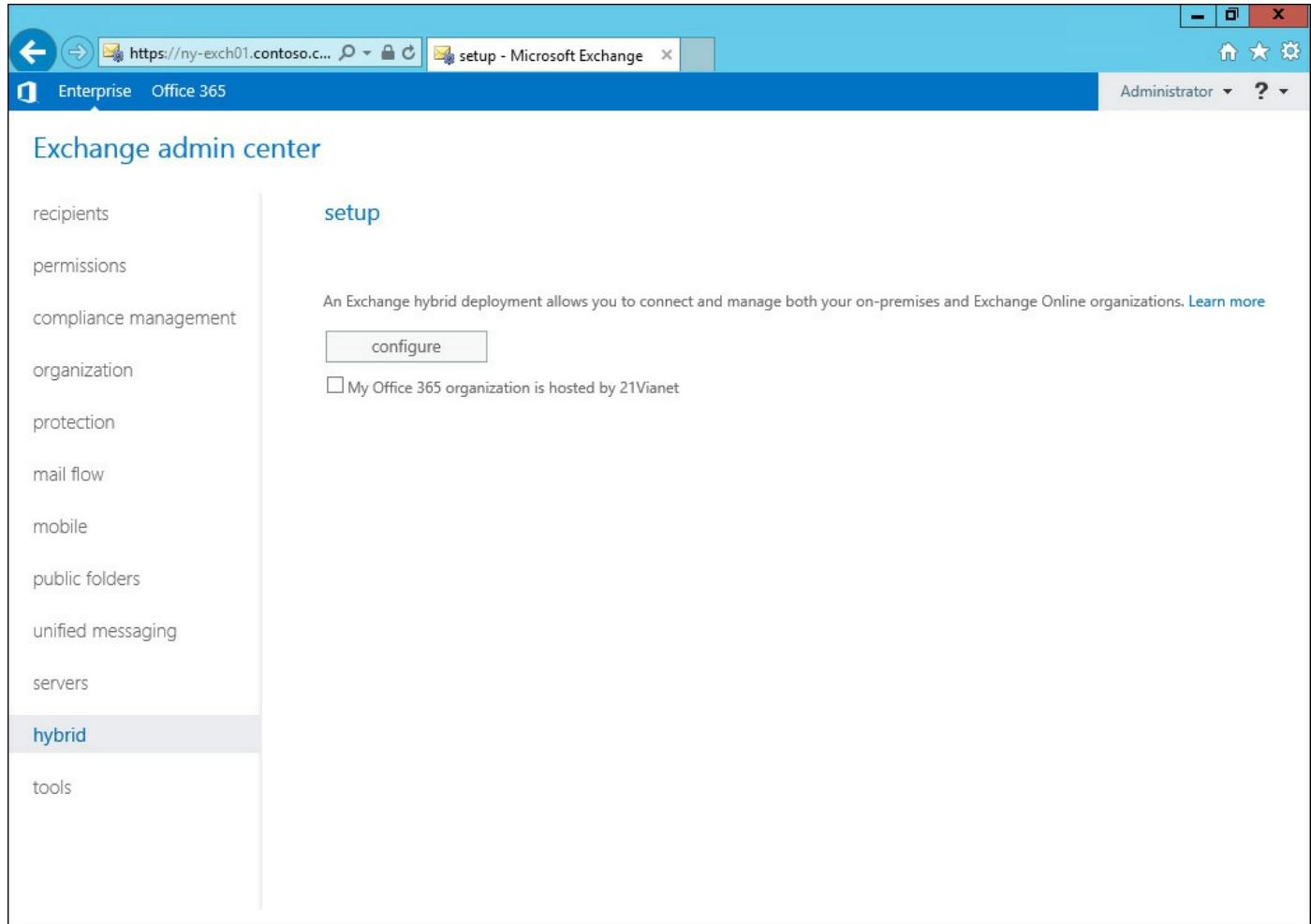


FIGURE 6-3 Starting the Hybrid Configuration Wizard from the Exchange admin center

### Important: Centralized Mail Flow Creates On-Premises Dependencies

When centralized mail flow is enabled, Exchange Online mailboxes depend on the on-premises Exchange server for routing outbound email. Because Exchange Online can't dynamically sense when the on-premises server is unavailable and "fail over" to sending directly out to the Internet, any issues with the on-premises server result in interruptions to external mail flow. This makes the availability of the on-premises server a critical element of the business.

When the Hybrid Configuration Wizard has successfully completed, you can view the properties of the Hybrid configuration by running the `Get-HybridConfiguration` cmdlet.

[Click here to view code image](#)

```
#Viewing the Hybrid configuration details
```

```
[PS] C:\>Get-HybridConfiguration
```

```

ClientAccessServers      : {}
EdgeTransportServers     : {NY-EDGE01}
ReceivingTransportServers: {}
SendingTransportServers  : {}
OnPremisesSmartHost     : mail.contoso.com
Domains                 : {contoso.com}
Features                : {FreeBusy, MoveMailbox, Mailtips,
                           MessageTracking,
                           Photos}
ExternalIPAddresses      : {}
TlsCertificateName       : <I>CN=DigiCert SHA2 Secure Server CA,
                           O=DigiCert Inc,
                           L=New York,
                           S=NY, C=US
Name                     : Hybrid Configuration
DistinguishedName        : CN=Hybrid Configuration,CN=Hybrid
Configuration,CN=Exchange: Server Pro,CN=Microsoft Exchange,CN=Services,
                           CN=Configuration,DC=contoso,DC=com
Identity                 : Hybrid Configuration
Guid                     : 680b1e2e-8d39-4c6d-a471-b55f2921c107
ObjectCategory           : contoso.com/Configuration/Schema/ms-Exch-
                           Coexistence-
                           Relationship
ObjectClass               : {top, msExchCoexistenceRelationship}
Id                       : Hybrid Configuration
OriginatingServer         : NY-DC01.contoso.com
IsValid                  : True
ObjectState               : Unchanged

```

If you need to make any changes to the Hybrid configuration at a later date, such as enabling or disabling centralized transport, or after installing a new Exchange server in the organization for Hybrid functionality, you can re-run the Hybrid Configuration Wizard to make the necessary changes.

## Evaluate limitations of the Hybrid Configuration Wizard

Although Hybrid configuration has several benefits, there are some limitations that you should be aware of. That said, the capabilities of Hybrid deployments are continually evolving over time, which means that something unsupported or limited today might be available in the near future.

- **Calendar free/busy** Two Exchange server organizations can manually configure federation trusts and organization relationships to enable calendar free/busy sharing to occur between them. The Hybrid Configuration Wizard automatically sets up the federation trust and organization relationship between an on-premises Exchange organization and Exchange Online to make calendar free/busy sharing possible for the Hybrid environment. In doing so, however, it breaks the

capability for a Hybrid environment to share calendar free/busy information for cloud-based mailboxes with other Hybrid or on-premises Exchange organizations. This means a company that wants to deploy a Hybrid configuration for itself, and also have organization relationships with other companies, needs to consider where they place the mailboxes for users who need to share that free/busy information.

- **Multi-forest scenarios** Although multiple Active Directory forests containing separate Exchange 2016 organizations can establish a Hybrid configuration with the same Office 365 tenant, the technical requirements are more complex. You can read more about multi-forest scenarios on TechNet at [https://technet.microsoft.com/library/jj873754\(v=exchg.150\).aspx](https://technet.microsoft.com/library/jj873754(v=exchg.150).aspx).
- **Validation of requirements** A Hybrid configuration depends on firewall and network access between the on-premises Exchange 2016 server and Exchange Online. Although the Hybrid Configuration Wizard might be able to successfully apply the various connectors and other configurations required for Hybrid functionality, it does not validate that all of the required connectivity is available. Therefore, you can't assume that a successful run of the Hybrid Configuration Wizard is a full validation of the technical requirements.
- **Exchange policies and configurations** The Hybrid Configuration Wizard doesn't automatically create or copy any of the policies and configurations from your on-premises Exchange 2016 environment into Exchange Online. This includes things such as transport rules, mobile device mailbox policies, retention tags and policies, and more. You need to manually configure the same policies and other items in Exchange Online and put manual procedures in place to maintain their consistency over time.
- **Rights Management** If Information Rights Management (IRM) is being used on-premises with Active Directory Rights Management Services (AD RMS), the cloud-based RMS services need to be manually configured before migrating any mailboxes to Exchange Online. This is achieved by enabling Azure Rights Management Services (Azure RMS), and then importing the Trusted Publishing Domain (TPD) from the on-premises organization. The Hybrid Configuration Wizard does not do any of these steps for you, nor does it bring the matter to your attention, so an understanding of whether IRM is used in your on-premises environment is necessary.
- **Unified Messaging** For Exchange Unified Messaging (UM) to work in a Hybrid configuration, the UM coexistence must be configured first before any UM-enabled mailboxes can be moved to Exchange Online. Again, the Hybrid Configuration Wizard does not perform any of the required configuration for you, nor does it bring it to your attention. You can identify UM-enabled mailboxes in

your on-premises Exchange organization by running the Get-UMMailbox cmdlet.

## Plan and manage hybrid deployment OAuth-based authentication

The use of a federation trust to enable sharing of calendar free/busy information between the on-premises Exchange environment and Exchange Online, relies on the Azure Active Directory Authentication System, previously known as the Microsoft Federation Gateway. The Azure Active Directory Authentication System acts as a broker for the secure communications between the two organizations, on-premises and online. The use of an external broker prevents a direct trust from being established between the two organizations. In particular, it means that the following features are not available:

- In-place archiving of items by automatically moving them from on-premises primary mailboxes to Exchange Online archive mailboxes.
- eDiscovery search and in-place hold across both the on-premises and online organizations.

For those features to be available, OAuth authentication needs to be configured. When the Hybrid Configuration Wizard is run in an organization that only contains Exchange 2013 CU5 or later servers, OAuth is automatically configured. For organizations that have any servers running Exchange 2013 CU4 or earlier, including Exchange 2010, OAuth must be configured manually. The on-premises Exchange organization is configured with an authorization server object, which is provided by Azure Active Directory Access Control Services (ACS) in your Office 365 tenant. The ACS is responsible for issuing tokens for OAuth authentication requests.

OAuth uses Intra-Organization Connectors (IOC) to define the trust between the two organizations. After configuring the authentication server object on-premises and uploading the on-premises authorization certificate to ACS, an IOC is configured in each organization by running the New-IntraOrganizationConnector cmdlet. Each IOC is configured with the Autodiscover endpoint that should be used for the other organization's recipients. For example, the IOC in the on-premises organization is configured with the Autodiscover endpoint for Exchange Online, which can be retrieved by running Get-IntraOrganizationConfiguration.

When OAuth has been configured between the two organizations, Exchange federation is no longer used for looking up calendar free/busy information. If the IOCs are misconfigured, the on-premises Exchange servers and Exchange Online do not "fail over" to using Exchange federation and free/busy information stops working.

## **Need More Review? Configuring OAuth Authentication Between Exchange and Exchange Online Organizations**

You can find more information about the full, step by step process for configuring OAuth in a Hybrid configuration on TechNet at  
[https://technet.microsoft.com/library/dn594521\(v=exchg.150\).aspx](https://technet.microsoft.com/library/dn594521(v=exchg.150).aspx).

## **Troubleshoot transport with Exchange Online**

An Exchange Hybrid environment can have several different mail routing topologies. It also has many different features and configurations that can influence the delivery of email. The mail routing topologies are influenced by four main factors; DNS records, centralized transport, custom routing, and third party devices and services. In addition to those factors, mail routing can also be impacted by firewalls, message size restrictions, and the configuration of individual recipients. When you are troubleshooting mail flow in a Hybrid environment, you need to take into account all of those factors as you approach each situation. Try to build a picture of the end to end mail flow for the scenario that you're troubleshooting and identify the elements that come into play at each step of the email message's journey from sender to recipient.

### **DNS records**

To get mail flow working in and out of your organization, there are some records that need to be added to the public DNZ zone for your domain names. When you add domain names to an Office 365 tenant, Microsoft provides you with the DNS records that they want you to add to your zone. It's not always necessary to add the DNS records immediately after you add the domain name to Office 365 and in some cases you should not add the DNS records at all. There are two types of DNS records that Microsoft provides to you, an MX record and an SPF record.

The mail exchanger (MX) records in DNS determine where other email servers on the Internet send email destined for recipients in your domain. When you have a Hybrid configuration in place, your MX records can point to either the on-premises Exchange servers, Exchange Online, a third party email appliance or service, or some combination of all of those. The decision is driven by your mail routing requirements. For example, if you need all inbound email to be sent to the on-premises infrastructure first where it can be scanned by an email security appliance that you have deployed, that is where the MX record should be pointed in DNS and you should not use the MX record supplied by Microsoft. Conversely, if you plan to use Exchange Online Protection (EOP) for all of your email scanning requirements, you should use the MX record provided by Microsoft that points to EOP.

The MX records can be tested by using online tools, such as Microsoft's Remove

Connectivity Analyzer located at <https://testconnectivity.microsoft.com>, which performs a DNS lookup for the MX record and then sends test emails to each of the MX records that were found. You can also look up MX records by running the Resolve-DnsName cmdlet in PowerShell.

[Click here to view code image](#)

#### #Looking up MX records using PowerShell

```
PS C:\> Resolve-DnsName -Name contoso.com -Type MX
```

```
Name      : contoso.com
Type     : MX
TTL      : 3600
NameExchange : mail.global.frontbridge.com
Preference   : 10
```

In addition to the MX records for inbound email, you should also configure Sender Policy Framework (SPF) records for outbound email. SPF records define which hosts should be permitted to send email from your domain names. When a receiving server checks emails from your domain, they can look up the SPF record to see whether the message has been received from an IP address that should be allowed to send for that domain. If the SPF lookup determines that the IP address is not one of the permitted senders for the domain, the receiving server can either reject the email entirely or can factor it into the spam scoring that is applied to the message.

---

#### Need More Review? Sender Policy Framework (SPF)

The SPF record is a TXT record in DNS that uses a special syntax to define which hosts can send email for a domain and what a receiver should do if email is received from an unauthorized sender. SPF records are only a suggestion and it's up to the receiving server to decide what action it should take based on information in the SPF record. You can find more information about SPF records at <http://exchangeserverpro.com/a-sender-policy-framework-spf-primer-for-exchange-administrators/>.

---

## Centralized transport

For Hybrid configurations where centralized transport is enabled, any email received by EOP from the Internet is routed to the on-premises Exchange server before it is delivered to an Exchange Online mailbox. This creates a dependency on the on-premises infrastructure for successful email delivery to cloud mailboxes, which must be taken into account. For outbound mail, centralized transport also means that messages are routed to the on-premises Exchange server before they are sent from an Exchange Online mailbox to any recipients on the Internet.

The most common reason for enabling centralized transport is to send email through the on-premises server so that any processing that is required for compliance purposes can be applied. For example, all outbound email might be inspected by a transport rule to determine if it contains sensitive information, and held for moderation if any such information is found. If a transport rule was configured in both the on-premises and online organizations to achieve that goal, any applicable emails would trigger the rule in both organizations, effectively holding the email for moderation twice.

### **Important: Centralized Transport Can't Use Non-Exchange Servers**

When the centralized mail transport option for a Hybrid configuration is enabled, the mail flow between Exchange Online and the on-premises environment can't use a third party email server or appliance as an intermediate hop. Hybrid mail flow can only occur between on-premises Exchange servers and Exchange Online.

## **Custom routing**

For some companies, it's necessary to customize the routing of emails so that they are not sent directly out to the Internet. To achieve this, a custom outbound connector can be configured in Exchange Online by running the New-OutboundConnector cmdlet. You can view existing outbound connectors by running the Get-OutboundConnector. Every Hybrid configuration has at least one outbound connector for Hybrid mail flow that is created automatically by the Hybrid Configuration Wizard.

Custom routing can be used to achieve a variety of outcomes:

- Route all outbound mail through a third party service or appliance for compliance purposes.
- Secure messaging with partners by configuring an outbound connector for the partner's domain and enforcing TLS encryption on the connector.
- Route email to domains that do not have public MX records by configuring an outbound connector that delivers emails for that domain to a smart host.
- Route inbound emails to mailbox users in different geographic regions directly to on-premises Exchange servers in those regions.

Custom email routing can also be based on transport rules, which is referred to as conditional routing. Outbound connectors make routing decisions based on the domain name of the recipient of an email message. Transport rules provide a far greater number of conditions for matching individual messages, such as the content in the subject or body of the message, and can also be based on specific senders and recipients instead of entire domains. For conditional routing, an outbound connector is configured and the

option to use the connector for criteria-based routing is enabled during creation using the wizard or by running New-OutboundConnector with the -IsTransportRuleScoped parameter set to \$true.

## Firewalls and networks

As previously discussed in this chapter, there are only two network ports required for a Hybrid configuration; TCP port 25 (SMTP) for mail flow, and TCP port 443 (HTTPS) for calendar free/busy information and mailbox migrations. Those are the ports required for server to server access. Client network requirements are similar, but are used for different purposes.

Despite the minimal port requirements for a Hybrid configuration, there is a wide range of IP addresses that Microsoft's cloud services operate from. As you can imagine, running a service at the scale of Office 365 across the entire globe requires a lot of public IP addresses. From time to time those IP address ranges change as Microsoft adds new capacity or opens up new regions. Configuring and maintaining your firewall rules for all of those IP addresses can be a time consuming and error prone task. That's why Microsoft recommends that the firewall rules you configure, particularly for outbound access by your clients and servers, should be based on hostnames rather than IP addresses.

Even when the correct ports are open for the appropriate IP address ranges, the capabilities of modern firewalls can interfere with the communications between the two environments. Firewalls that perform application-level inspection of traffic can cause connections to fail. Similarly, misconfigured load balancers can have a detrimental effect on the stability of connections between the two environments.

### Note: Office 365 URLs and IP Address Ranges

Microsoft publishes the full list of URLs and IP address ranges required for Office 365 services on the Office Support website at  
<https://support.office.com/en-gb/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2>.

## **Message sizes and recipient restrictions**

Exchange Online applies size restrictions to email messages sent within the service and between internal and external recipients. The default message size limit for Exchange Online is advertised as 25 MB, but in reality it is configured to 35 MB to allow for various overheads and metadata in a typical email message. In effect this means that a 25 MB attachment is delivered successfully, but anything larger is likely to be rejected. In April of 2015 Microsoft increased the size limit to 150 MB, however the default limit configured in a new Office 365 tenant is still 35 MB. Administrators can configure a larger message size limit for their mailbox users if required, up to the maximum of 150 MB. If an email message is rejected due to exceeding the maximum size limit, a non-delivery report (NDR) is generated to the sender, explaining the reason for the message being rejected.

As well as the size limits, individual recipients can have restrictions applied so that they can only receive email messages from permitted recipients. The most common restriction is the default restriction applied to distribution groups, requiring that any messages can only be received from authenticated senders. In effect this means internal senders can send email to the distribution group, but an external sender can't. This default option exists to prevent abuse of distribution groups by spammers, and can be turned off by running the Set-Mailbox or Set-DistributionGroup cmdlets with the `-RequireSenderAuthenticationEnabled` parameter set to \$false. Recipients can also be configured to only accept emails from specific senders. As with the message size limits, if any emails are rejected due to a recipient configuration, an NDR is generated to the sender, including the reason for the message being rejected.

## **Message Tracing**

When a mail flow issue occurs on-premises, you have access to the server event logs, message tracking logs, and protocol logs to help you diagnose the problem. With Exchange Online, you do not have direct access to any of the server logs. By using the Exchange admin center, you can perform message traces to gather information to help with your troubleshooting. Message traces are found in the mail flow section of the Exchange admin center, as shown in [Figure 6-4](#).

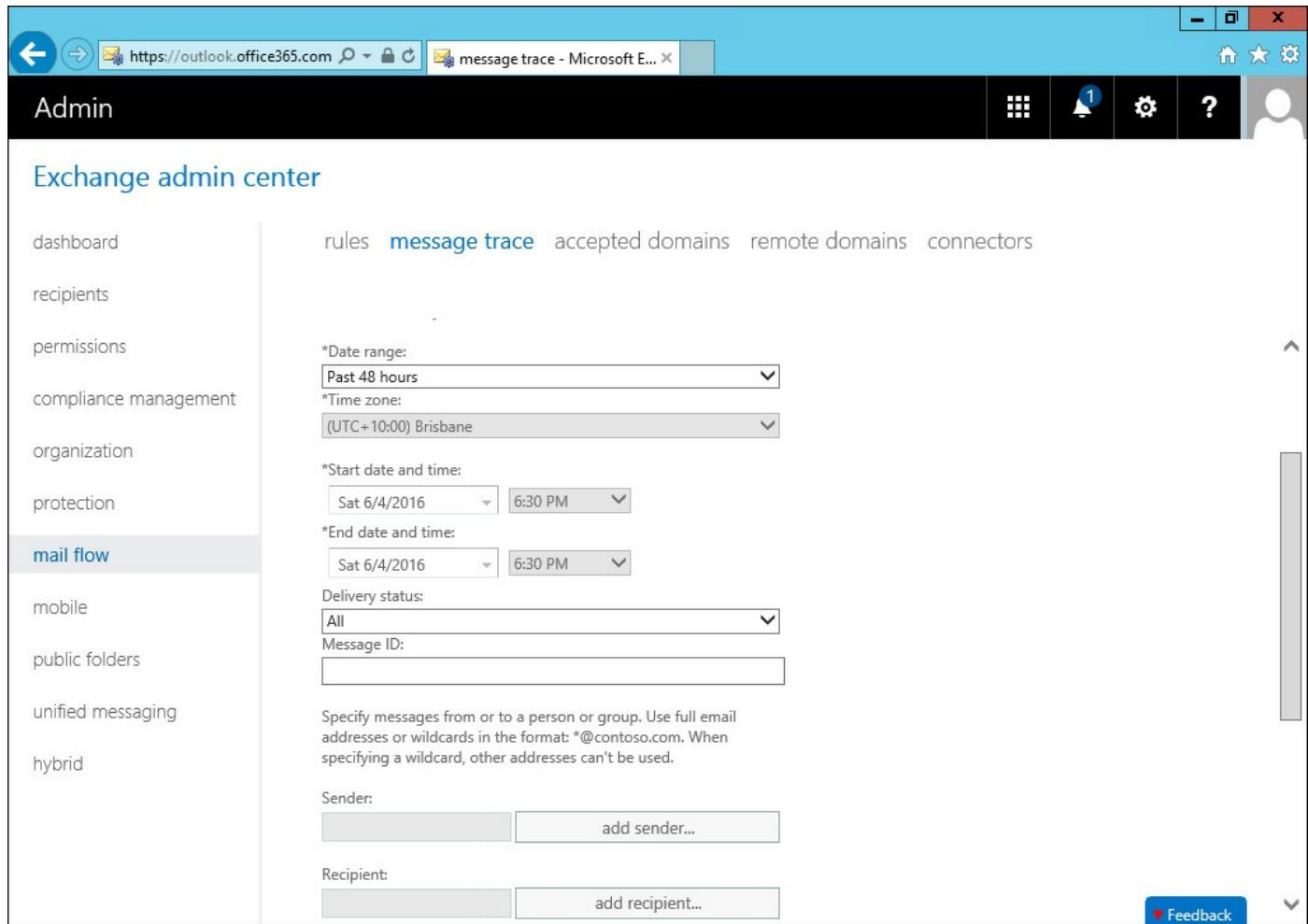


FIGURE 6-4 Performing a message trace in Exchange Online

## Troubleshoot client access with Exchange Online

In a Hybrid environment, troubleshooting client access issues takes a similar approach to troubleshooting on-premises client access issues. Mailboxes can be located both on-premises and in Exchange Online. Although on-premises mailbox access is largely influenced by on-premises conditions, access to Exchange Online mailboxes can be influenced by factors both within your network environment, as well as those within the Office 365 infrastructure. This means that you need to use an approach to troubleshooting that takes into account elements inside and outside of your control.

The main cause of client access issues with Exchange Online is the version of Outlook being used. Because of the constant development within Office 365, client software needs to be updated to keep pace with the latest changes. The further out of date Outlook becomes, the more likely it is to experience performance or connectivity problems. Even with up to date Outlook software, problems can still occur with access to Exchange Online mailboxes. Using the process of elimination, try connecting to the mailbox using a different protocol, such as Outlook on the web or a mobile device.

When Outlook on the web is working fine, a good area to focus your troubleshooting

on is Autodiscover. Outlook and mobile clients rely on Autodiscover for the initial setup of the Outlook profile and on an ongoing basis for discovering the Exchange Web Services endpoint to connect to for free/busy lookups and to access shared mailboxes. Mobile clients also rely on Autodiscover for initial configuration. In a Hybrid environment that has some mailboxes located on-premises, the Autodiscover namespace needs to point to the on-premises server so that it can respond to both on-premises and Exchange Online mailbox user requests. If Autodiscover is pointed at Exchange Online, any on-premises mailbox users are not able to query Autodiscover for information, because Exchange Online Autodiscover can only answer for online mailboxes.

Client access can also be impacted by changes to the protocol configuration on mailboxes. By default, each mailbox is enabled for all client access protocols, which includes Outlook (MAPI), Exchange Web Services, Outlook on the web, ActiveSync (mobile), POP, and IMAP. You can view the protocol access for a mailbox by running the Get-CASMailbox cmdlet. If any of the protocols need to be enabled, you can do so by using the Set-CASMailbox cmdlet.

[Click here to view code image](#)

#### #Viewing client protocol configuration for a mailbox

```
[PS] C:\> Get-CASMailbox alan.reid | Select *enabled  
ActiveSyncEnabled : True  
OWAEnabled : True  
OWAforDevicesEnabled : True  
ECPEnabled : True  
PopEnabled : True  
ImapEnabled : True  
MAPIEnabled : True  
UniversalOutlookEnabled : True  
EwsEnabled : True
```

## Troubleshoot directory synchronization

The directory synchronization tools provided by Microsoft are, generally speaking, quite reliable. You can install an instance of Azure Active Directory Connect (AAD Connect) in your on-premises environment, and when it is configured, it operates with very little intervention on your part, importing information from Active Directory and exporting it to Azure Active Directory where it is used for your Office 365 tenant.

AAD Connect is only as reliable as the data it is pulling from the on-premises Active Directory. Among the most frequently seen issues with directory synchronization is badly configured objects in Active Directory. The configuration issues are usually invalid attributes, such as the use of a .local domain in the user principle name (UPN), invalid characters in attributes such as phone numbers or addresses, or duplicate objects. The most obvious sign of bad data is that an object isn't syncing to Azure Active Directory at all, so that users are not able to login to Exchange Online and others

aren't seeing them in the Global Address List. Mismatched and duplicate objects showing up in Office 365 are also a sign of problems with the attributes of an on-premises object. You can use the IDFix tool from Microsoft to detect and repair issues with object attributes.

When you install AAD Connect you provide the login details for an on-premises Enterprise Admin and a Global Admin account in Office 365. Those credentials are only used for the initial setup. AAD Connect configures its own service accounts to use for ongoing access to both directories. The service accounts are subject to the same password policies as any other user in your environment. Synchronized user accounts use the same password policy as the on-premises Active Directory. The service account created by AAD Connect is not a synchronized account, rather it is a cloud-only account. As such, it is subject to the default 90 day password expiration policy in Office 365. If the password expires, synchronization of changes to Active Directory objects stop working, including the synchronization of password changes for users. The first time you notice the issue is likely after someone changes their on-premises password and is no longer able to login to Office 365 services. To avoid this issue, you should connect to Office 365 with PowerShell and set the synchronization account in Office 365 to have a non-expiring password.

[Click here to view code image](#)

```
#Configure the synchronization service account password to never expire  
  
PS C:\> Set-MsolUser -UserPrincipalName `'  
    (Get-MsolCompanyInformation).DirSyncServiceAccount `'  
    -PasswordNeverExpires $true
```

## Summary

- There are several migration paths that can be used to migrate to Exchange Online. Hybrid configuration offers the best migration experience for users and administrators and also provides a rich coexistence between the on-premises and online organizations.
- Identity management for Hybrid configurations involves synchronizing Active Directory objects into Azure Active Directory. The success of the directory synchronization service depends on the quality of the data that is imported from the on-premises Active Directory environment.
- The Hybrid Configuration Wizard automatically configures the on-premises and online Exchange environments for coexistence. The wizard is successful, provided you have met all of the technical requirements for a Hybrid configuration. The wizard's success, however, does not validate that all of the Hybrid functionality works.

- Troubleshooting Hybrid environments involves establishing a clear understanding of the scope of the problem, and then taking into consideration a broad array of factors in the environment that can influence mail flow, collaboration, and client connectivity.

## Skill 6.2: Plan, deploy, manage, and troubleshoot Exchange federation

Federation is a key component of the integration between an on-premises Exchange environment and Exchange Online in a Hybrid configuration. Exchange federation can also be used to share calendar free/busy information between separate on-premises Exchange organizations.

This section covers how to:

- [Plan, create, and manage federation trusts with Microsoft federation gateways](#)
- [Manage sharing policies](#)
- [Manage organization relationships](#)
- [Plan and create certificate and firewall requirements for federation](#)
- [Troubleshoot Exchange federation trust and organization relationships](#)
- [Troubleshoot cross-forest availability](#)

### Plan, create, and manage federation trusts with Microsoft federation gateways

Exchange federation involves setting up a federation trust with the Microsoft Federation Gateway, which is now referred to as Azure Active Directory Authentication System. During your exam however, you are likely to still see this referred to as the Microsoft Federation Gateway, so that is how it is referred to in this chapter.

The Microsoft Federation Gateway acts as a trust broker between two federated organizations. Both parties must agree to the sharing of information by each of them registering a federation trust and configuring organization relationships. As such, there is no risk that the federation trust exposes your organization to leakage of users' calendar free/busy information to unauthorized parties.

When a mailbox user requests calendar free/busy information for a mailbox that is external to the organization, the Exchange 2016 server checks to see whether an organization relationship exists for the other organization. The lookup of the organization relationship is based on the domain name of the external recipient's SMTP address. If an organization relationship exists for that domain, the Exchange server

sends a request to the Microsoft Federation Gateway for a delegation token. The delegation token is then sent to the other Exchange organization along with the request for free/busy information. The other organization has its own federation trust established, which permits its servers to validate the delegation token to ensure that it is not a forged or malicious request. The server that receives the request then responds with the details that are permitted by the organization relationship for the requesting organization.

For Exchange federation scenarios, the requirements are similar to a Hybrid configuration, except that there is no equivalent of the Hybrid Configuration Wizard to perform the configuration of the different components for you. To create the federation trust, open the Exchange admin center and navigate to the Organization section. Click Enable to create the federation trust. After the federation trust has been enabled, click Modify, and then browse the list of accepted domains in your organization to choose which domain name to use to establish the federation trust. If you have additional domains that you want to include in the federation trust you can add those as well.

When you've selected the domain name to use for the federation trust, the dialog window displays a cryptographic key value used to validate your ownership of that domain name. A TXT record needs to be created in the public DNS zone for the domain to prove that you are the domain owner before the federation trust works. A key is also provided in the dialog box for any additional domain names you enable for sharing. You can also get the key value by running the Get-FederatedDomainProof cmdlet with the DomainName parameter.

[Click here to view code image](#)

```
#Get the federated domain proof key value
```

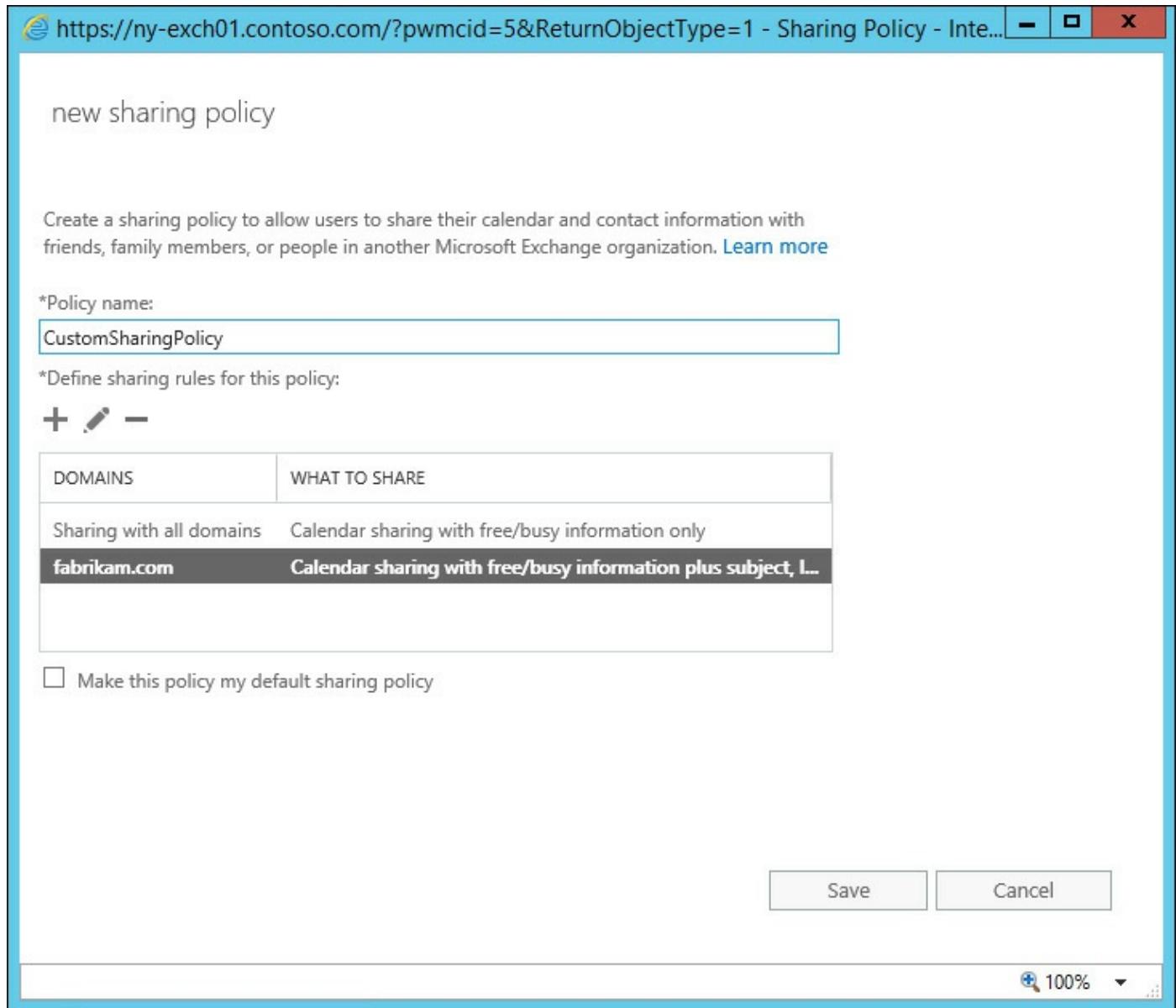
```
[PS] C:\>Get-FederatedDomainProof -DomainName contoso.com
```

After adding the TXT records to your public DNS zone you are able to complete the modification to the federation trust by clicking the Update button.

## Manage sharing policies

When the federation trust has been enabled in the Exchange admin center, the default sharing policy becomes visible in the Exchange admin center. The sharing policy already exists before the federation trust is enabled, and you can view it by running the Get-SharingPolicy cmdlet. Sharing policies are what makes it possible for mailbox users in your organization to make calendar sharing requests with users in other federated organizations. For non-federated organizations, the sharing policy enables the mailbox users to publish their calendar for external users to access it. The default sharing policy is enabled to share calendar free/busy information with the time data only. In other words, it does not share any details of the meetings in your users' calendars other than the start and finish times so that external users can see when someone is available.

The default sharing policy is scoped to all domains, including anonymous users. If you have specific requirements for another organization that differ from the default sharing policy, you can create an additional sharing policy for their domain name that shares more than the default policy, as shown in [Figure 6-5](#).



**FIGURE 6-5** Creating a new sharing policy

Additionally, sharing policies are assigned to mailbox users, and only one sharing policy can be applied to a mailbox at a time. Therefore, if you require a customized sharing policy for a given user, it must be configured for all of the domains that the user needs to share information with.

[Click here to view code image](#)

#### #Assigning a sharing policy to a mailbox

```
[PS] C:\>Set-Mailbox Kim.Akers@contoso.com -SharingPolicy  
CustomSharingPolicy
```

## Manage organization relationships

When the federation trust for your Exchange 2016 organization has been enabled and the domain names have been validated using the TXT records in your public DNS zones, you can proceed with the creation of organization relationships. There are no organization relationships created automatically or by default.

When you create an organization relationship in the Exchange admin center as shown in [Figure 6-6](#), or by running the New-OrganizationRelationship cmdlet, you define the domain name of the federated organization that you want to share information with and the amount of calendar free/busy information want to share. In addition, you can limit the sharing of data to a specific security group within your own organization. This is useful for situations such as when you want a smaller project team to be able to share calendar free/busy information with an external partner, but you do not want to expose your entire organization's calendar information to that external partner.

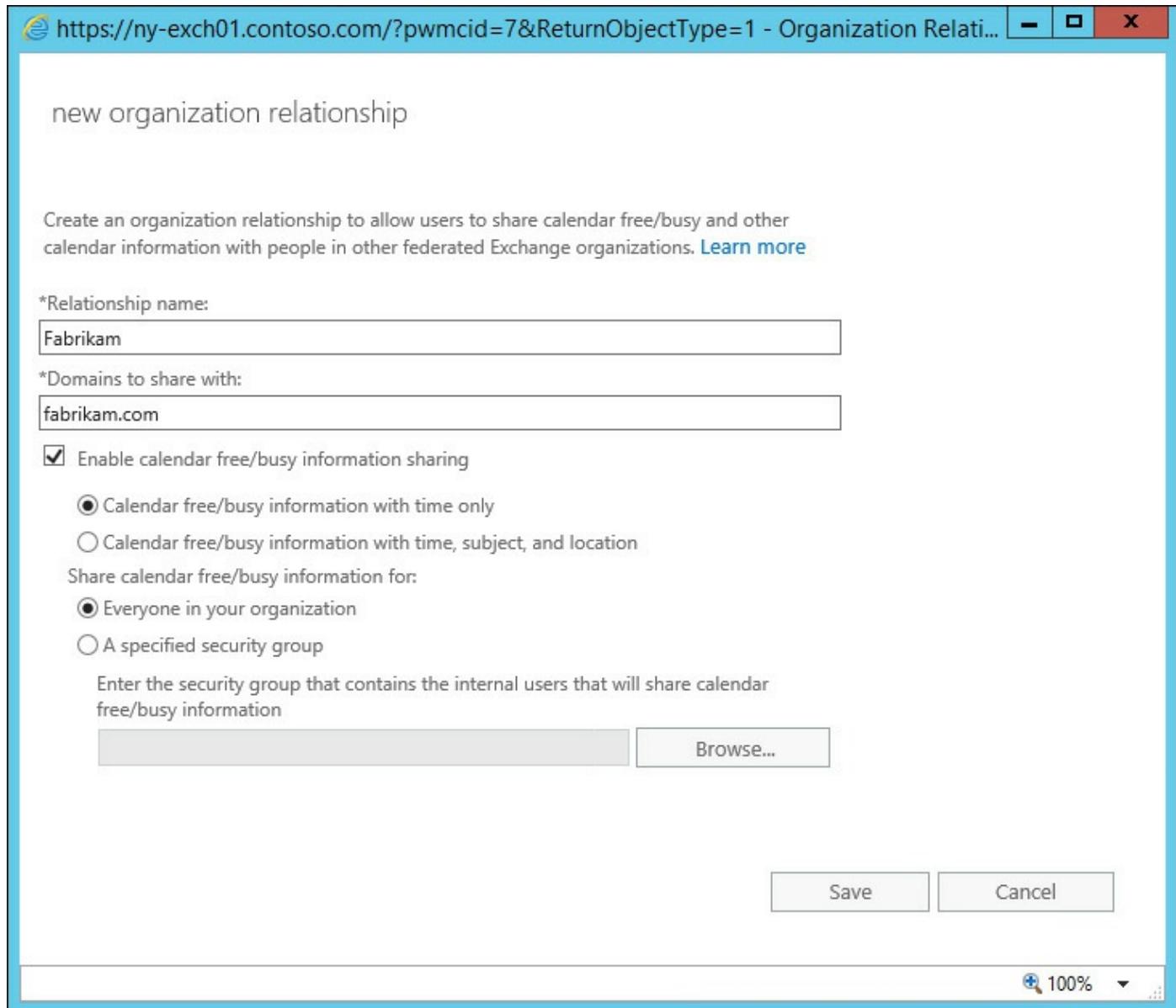


FIGURE 6-6 Creating a new organization relationship

## Plan and create certificate and firewall requirements for federation

The communications for federated sharing all occur over TCP port 443 (HTTPS). The Exchange 2016 mailbox servers in your organization need outbound HTTPS access through your firewall to the Internet so they can contact the Microsoft Federation Gateway and contact the Exchange servers of the other organization when making a request for calendar free/busy information. Similarly, inbound HTTPS access through the firewall to your Exchange 2016 mailbox servers is required so that the Exchange servers in other organizations can make free/busy requests to your server.

Because all of the communication is occurring over HTTPS, your Exchange 2016 mailbox servers need to be configured with a valid SSL certificate. A valid certificate is one that matches the hostnames that the other server is trying to connect to, which are

the Autodiscover and Exchange Web Services namespaces for your server. The certificate must also be issued by a certificate authority (CA) that the connecting server trusts. This means the self-signed certificate configured by Exchange setup is not suitable for the HTTPS traffic over which federated sharing occurs.

An additional self-signed certificate is automatically generated on the Exchange 2016 mailbox server used to enable the federation trust. The certificate is published to the Microsoft Federation Gateway and is used to sign and encrypt delegation tokens exchanged between the Microsoft Federation Gateway and your servers. Because each server in your organization that requests delegation tokens needs a copy of the certificate, it is distributed automatically to the other Exchange servers in the organization. You can verify that each server in the organization has a copy of the certificate by running the `Test-FederationTrustCertificate` cmdlet.

The self-signed certificate has a validity period of five years, which makes the need to renew it unlikely. If you do need to renew the certificate, however, you can generate a new Exchange certificate and then assign the new certificate to the federation trust, as shown in [Listing 6-1](#).

## LISTING 6-1 Updating the federation trust certificate

[Click here to view code image](#)

---

```
#PowerShell commands to update the federation trust certificate
```

```
[PS] C:\>New-ExchangeCertificate -SubjectName CN=Federation -  
SubjectKeyIdentifier Federation -PrivateKeyExportable $true  
  
Thumbprint Services Subject  
----- ---- -----  
101FED04D972957ED7C5F545FFCF9D0C0667725F ....S... CN=Federation  
  
[PS] C:\>Set-FederationTrust -Identity "Microsoft Federation Gateway" -  
Thumbprint  
101FED04D972957ED7C5F545FFCF9D0C0667725F
```

---

After setting the new federation certificate, new domain proof records need to be added to DNS. You can retrieve the values for the new domain proof records by running the `Get-FederatedDomainProof` cmdlet with the `-DomainName` parameter, and looking at the `OrgNextCertificate` proof value. The `OrgNextCertificate` value should be added to your public DNS zone as a `TXT` record before you publish the new certificate to the federation gateway. Use the `Test-FederationTrustCertificate` cmdlet to verify that the new certificate has copied to each Exchange server in the organization and then enable the new certificate by publishing it to the Microsoft Federation Gateway.

[Click here to view code image](#)

```
#PowerShell commands to publish the new federation certificate
```

```
[PS] C:\>Set-FederationTrust -Identity "Microsoft Federation Gateway"  
-PublishFederationCertificate
```

## Troubleshoot Exchange federation trust and organization relationships

Troubleshooting federation trust is a task that requires cooperation between you and an administrator in the other federated organization. You have visibility into elements of your own organization, such as:

- Confirming that the federation trust is enabled for your organization.
- Confirming that the federation trust certificate has not expired and has copied to all of the Exchange servers in your organization.
- Confirming that firewall access inbound and outbound from your Exchange servers is open on TCP port 443 (HTTPS).
- Confirming that an organization relationship exists for the other federated organization and that it is configured with the level of sharing that you require.

You can also query the Microsoft Federation Gateway to determine whether the domain name for the other organization has been enabled for federation, by running the Get-FederationInformation cmdlet.

[Click here to view code image](#)

```
#Querying the federation information for a remote domain
```

```
[PS] C:\>Get-FederationInformation -DomainName fabrikam.com
```

```
RunspaceId          : 48d6028c-8cde-4648-9bc7-f16901232518  
TargetApplicationUri : FYDIBOHF25SPDLT.fabrikam.com  
DomainNames        : {fabrikam.com}  
TargetAutodiscoverEpr :  
https://autodiscover.fabrikam.com/autodiscover/autodiscover.svc/  
WSSecurity  
TokenIssuerUris    : {urn:federation:MicrosoftOnline}  
Identity           :  
IsValid            : True  
ObjectState        : Unchanged
```

In this example, the Fabrikam organization has enabled the domain fabrikam.com for federation. You can't tell, however, whether an organization relationship has also been configured for the organization. Without the organization relationship, no free/busy requests to the Fabrikam servers are successful.

## Troubleshoot cross-forest availability

The Exchange 2016 Availability service runs on the mailbox server role, and is used to make free/busy information available to Outlook and Outlook on the web clients.

Clients can query the Availability service for free/busy information, working hours, and meeting time suggestions for mailboxes in the same organization, or from other Exchange organizations. This feature allows users to send meeting requests that suit the attendee's availability. As such, it is important that the Availability service works, is available when needed, and returns the correct information.

For your users to be able to look up free/busy information for users in other forests, those users need to appear in the Global Address List (GAL) in your forest. To achieve this, an identity synchronization tool needs to be installed. Microsoft supports the use of their own identity management tools for this purpose, tools which have gone by many names over the years such as Forefront Identity Manager (FIM), Identity Lifecycle Manager (ILM), and Microsoft Identity Manager (MIM). Tools from third party vendors also exist, often as part of a migration toolset for cross-forest scenarios. Typically, the solution involves importing the mailbox users and groups from one forest, and exporting them as mail users and contacts to the other forest. In doing so, they are visible in the GAL and have appropriate routing addresses stamped on them so that mail flow and free/busy lookups work between the two forests.

The Availability service is made available through Exchange Web Services. The Exchange Web Services URL is discovered by clients through an Autodiscover query, therefore the Availability service relies on both Autodiscover and Exchange Web Services to be available. This means that the Autodiscover and Exchange Web Services URLs must be configured and have the appropriate DNS records in place. In a forest trust scenario, if the Autodiscover service is not accessible via the well-known CNAME of [autodiscover.domain.com](#), the Autodiscover service connection point can be exported from each forest to the other trusted forest by running the Export-AutodiscoverConfig cmdlet. Autodiscover and Exchange Web Services also need to be reachable on TCP port 443 (HTTPS) through the firewall. As both services use HTTPS, it is also necessary for a valid SSL certificate to be installed.

## Summary

- An Exchange federation trust is used to broker authenticated connections between two separate Exchange organizations, so that calendar free/busy information can be retrieved by users in each organization. The federation trust needs to be enabled in both of the organizations that are sharing information.
- Organization relationships control the sharing of calendar free/busy information between two Exchange organizations that have enabled federation trusts. Without an organization relationship, your Exchange servers do not respond to free/busy

queries from other federated organizations.

- Sharing policies control how users in your organization are able to publish their calendar information to users outside of your organization. A default sharing policy exists that permits limited publishing of calendar information to other users on the Internet.
- The Availability service can be made available for cross-forest queries of calendar free/busy information. Cross-forest access to the Availability service can be configured for both trusted and untrusted forests, with the key difference being the amount of information that is available.

### **Skill 6.3: Plan, deploy, and troubleshoot on-premises coexistence with earlier supported versions of Exchange**

When you install Exchange 2016 into an existing organization, there is a period of time in which both the old and new versions of Exchange are running together, while the migration of data and services to Exchange 2016 is performed. This period is referred to as coexistence, and could be as short as a few days for smaller organizations, or up to several years for very large, complex organizations.

During the coexistence period it's important that full functionality within the environment is maintained. The coexistence configuration must take into account each of the different methods that clients use to access their mailboxes, as well as internal and external mail flow to the organization.

---

#### **This section covers how to:**

- [Plan, create, and configure namespaces for coexistence](#)
  - [Plan and configure proxy redirect](#)
  - [Plan firewall configuration for coexistence](#)
  - [Plan and configure for mail flow requirements](#)
  - [Plan for mailbox migrations](#)
  - [Troubleshoot transport in coexistence](#)
  - [Troubleshoot client access in coexistence](#)
- 

### **Plan, create, and configure namespaces for coexistence**

Client access namespaces are the hostnames or URLs that a user's client applications and devices connect to for accessing mailboxes. Over the history of Exchange Server, the coexistence between different Exchange versions has followed the same pattern:

- Users who have mailboxes hosted on the older version of Exchange in the

organization can connect to either the old version or the newer version of Exchange to access their mailboxes.

- Users who have mailboxes hosted on the newer version of Exchange in the organization must connect to the new version to access their mailboxes. If a user with a mailbox on the newer version of Exchange connects to an old version of Exchange, they are not able to access their mailbox.

Exchange 2016 changes slightly from that pattern. Because Exchange 2016 is so closely related to Exchange 2013 in terms of architecture and codebase, these two versions of Exchange are able to both “up proxy” and “down proxy” client connections for each other. This creates more flexibility for the organization deploying Exchange 2016 into an existing Exchange 2013 environment. In this configuration, the client access namespaces do not need to be switched over to the newer server for Exchange 2016 users to be able to access their mailboxes after they have been migrated. For Exchange 2010 environments, however, the deployment of an Exchange 2016 does require that namespaces be switched over to Exchange 2016 so that users can access their mailboxes after they have been migrated.

An Exchange server has multiple services with namespaces that must be considered when planning coexistence. The namespaces are:

- Autodiscover
- Outlook Anywhere
- MAPI over HTTP
- Exchange Web Services
- Offline Address Book
- Outlook on the web
- Exchange Control Panel
- Exchange ActiveSync
- POP
- IMAP

Different Exchange environments can use different namespace strategies depending on their technical requirements. The simplest strategy is to use the same namespace for all services, such as “mail.contoso.com.” In doing so, there are fewer DNS records to manage, and fewer names required on the SSL certificate installed on the Exchange server.

In contrast, some organizations might choose to use a different namespace for each service, such as “webmail.contoso.com” for Outlook on the web, “eas.contoso.com” for ActiveSync, and so on. There is nothing technically wrong with this approach, but it

means that more DNS records need to be created and managed, and more names are required on the SSL certificate. As far as user impact goes, only the Outlook on the web URL is typically known by the users because they need to type it in their web browser to access their mailbox. The other namespaces do not need to be known by users because they are discovered by the connecting applications and devices when they query the Autodiscover service.

Even when a simple namespace strategy is used, more than one namespace is sometimes configured. It's common to run the Autodiscover service on a different namespace than the other HTTPS servers. The main advantage of doing so is that during a migration project, you can switch over the Autodiscover service, which is always the first service to be migrated, to the newer version of Exchange independently of the other services. If a separate namespace is not used for Autodiscover, however, it doesn't prevent you from performing the migration. You just need to ensure that all of the HTTPS services are configured before you make the DNS change that switches over the namespace to point to the Exchange 2016 server. This approach works fine assuming all of your preparation and configuration is correct. Even so, it is recommended to have a test plan ready so that you can test the changes, and have a rollback plan ready if you identify any issues that require you to back out and reassess your configuration.

For organizations spanning multiple geographic regions, a regional namespace approach might be used for the different datacenters that host Exchange servers. For example, a company with servers in North America and Europe might use [mail-us.contoso.com](mailto:us.contoso.com) for North America, and [mail-eu.contoso.com](mailto:eu.contoso.com) for Europe.

#### Note: Not All Services Use Autodiscover

POP and IMAP services are not discoverable by connecting clients and devices because they are not included in the Autodiscover XML response.

By running the services using familiar names, however, such as [pop.contoso.com](mailto:pop.contoso.com) and [imap.contoso.com](mailto:imap.contoso.com), many of the modern POP/IMAP clients are able to automatically locate and connect to them.

Some organizations take advantage of an Exchange migration to switch to a different namespace for client access. For example, if an organization has recently rebranded, or has merged with another company, it might prefer to change from its previous namespace to a new one. In such a scenario, it is advisable to install the new Exchange 2016 servers using the new namespace into a different Active Directory site, so that Autodiscover is able to return the correct namespaces to clients as the mailboxes are moved to the new server.

## **Important: Namespaces, DAGs, and Active Directory Sites**

Although namespaces are configured on a per-server basis, you should consider them in the context of the entire Active Directory site. When multiple Exchange 2016 mailbox servers are installed into the same site, they should be configured with the same namespaces for each service.

Client access namespaces are directly related to Database Availability Groups (DAGs). Because DAGs can span multiple Active Directory sites, so too can client access namespaces. When a namespace resolves to Exchange servers in multiple sites, it is referred to as an Unbound Namespace. DAG members in each site can handle client traffic for mailboxes that are active in either site. This follows the Active-Active DAG model.

When you want to control which site clients connect to, for mailboxes hosted by a DAG that uses the Active-Passive model, you would use a Bound Namespace model. In the Bound model a namespace resolves to Exchange servers in a single site only. In the event of a datacenter switchover, the namespace is manually updated in DNS to point to the Exchange servers in the secondary site.

## **Split DNS**

The recommended practice for Exchange 2016 is to use the same namespace for internal and external access to each service. For example, configure Outlook on the web to use an internal and external URL of <https://mail.contoso.com/owa>. An advantage of this approach is that it simplifies the experience for users, so they have a single Outlook on the web URL to remember. For other services that users do not need to remember the URL for, there is still an advantage in that there are fewer hostnames to include on the SSL certificate for the server.

When the same namespace is used for internal and external access, split DNS is used to ensure that internal users connect to the internal IP address of the Exchange server and external users connect to the public IP address. Split DNS involves hosting two copies of the DNS zone; one public zone that is accessible to the world and has the DNS records associated with external IP addresses, and one internal zone that has the same DNS records associated with internal IP addresses.

## Autodiscover

The first service to consider is Autodiscover because it is also the most important service during a coexistence period. Without a working Autodiscover service, clients are not able to discover the namespace to connect to for any other service. Within an Active Directory site there should be only one Autodiscover namespace used, no matter which versions of Exchange are in coexistence. This prevents clients from querying the wrong version of Exchange for Autodiscover information.

Before installing a new Exchange 2016 server into an existing environment, you should review the Autodiscover namespace that is already being used. You can retrieve the current Autodiscover namespace information by running the Get-ClientAccessServer cmdlet.

[Click here to view code image](#)

```
#Retrieve Autodiscover information

[PS] C:\>Get-ClientAccessService -Identity NY-EX2010 | Select
Autodiscover*

AutoDiscoverServiceCN      : NY-EX2010
AutoDiscoverServiceClassName : ms-Exchange-AutoDiscover-Service
AutoDiscoverServiceInternalUri :
https://mail.contoso.com/Autodiscover/Autodiscover.xml
AutoDiscoverServiceGuid    : 77378f46-2c66-4aa9-a6a6-3e7a48b19596
AutoDiscoverSiteScope       : {NewYork,Chicago,Boston}
```

---



### Exam Tip

The Get-ClientAccessService cmdlet was introduced in Exchange 2013, and the Get-ClientAccessServer cmdlet is being deprecated. Exchange 2010 only has the Get-ClientAccessServer cmdlet available. Although both cmdlets are available in Exchange 2016 and work the same way, you should always consider which version of Exchange you're running the command on to determine which cmdlet to use.

---

When the Exchange 2016 mailbox server is installed and Autodiscover service connection point is registered for the server, the service connection point is registered using the server's full-qualified domain name, for example https://ny-exch01.contoso.com/Autodiscover/Autodiscover.xml. Immediately after installing the server you should update the Autodiscover service connection point to the same value as existing servers in the same Active Directory site by running the Set-ClientAccessService cmdlet.

[Click here to view code image](#)

```
#Configuring the Autodiscover service connection point
```

```
[PS] C:\>Set-ClientAccessService -Identity NY-EXCH01 -  
AutoDiscoverServiceInternalUri  
https://autodiscover.contoso.com/Autodiscover/Autodiscover.xml
```

The Autodiscover service has an additional configuration called the Autodiscover Site Scope, which defines the Active Directory sites that the service is responsible for. This is also sometimes referred to as site affinity. By default, the Site Scope value is configured with the name of the Active Directory site that the Exchange server is installed in. If clients in an Active Directory site can't locate an Autodiscover service connection point with a site scope matching their site name, they query any Exchange 2016 mailbox server in the environment for Autodiscover information. In a simple environment, this is not a concern. For more complex environments however, it could mean sub-optimal Autodiscover performance. Therefore, when you install an Exchange 2016 mailbox server into an Active Directory site, you should also configure the Site Scope to match the existing Exchange 2013 or 2010 client access servers, as shown in [Listing 6-2](#).

## LISTING 6-2 Adding site names to the Autodiscover Site Scope

[Click here to view code image](#)

```
#Configuring the Autodiscover Site Scope
```

```
[PS] C:\>$SiteScope = (Get-ClientAccessService -Identity NY-EXCH01).  
AutoDiscoverSiteScope
```

```
[PS] C:\>$SiteScope  
NewYork
```

```
[PS] C:\>$SiteScope.Add("Chicago")  
[PS] C:\>$SiteScope.Add("Boston")
```

```
[PS] C:\>Set-ClientAccessService -Identity NY-EXCH01 -  
AutoDiscoverSiteScope $SiteScope
```

```
[PS] C:\>Get-ClientAccessService -Identity NY-EXCH01 | Select Auto*
```

```
AutoDiscoverServiceCN : NY-EXCH01  
AutoDiscoverServiceClassName : ms-Exchange-AutoDiscover-Service  
AutoDiscoverServiceInternalUri :  
https://autodiscover.contoso.com/Autodiscover/Autodiscover.xml  
AutoDiscoverServiceGuid : 77378f46-2c66-4aa9-a6a6-3e7a48b19596  
AutoDiscoverSiteScope : {NewYork, Chicago, Boston}
```



## Exam Tip

Although there is an Autodiscover virtual directory on the server, and corresponding Get-AutodiscoverVirtualDirectory and Set-AutodiscoverVirtualDirectory cmdlets, they are not used for configuring the Autodiscover service. Any values that you set for the internal or external URLs on the Autodiscover virtual directory are ignored.

## Outlook Anywhere

Outlook clients use Outlook Anywhere to connect to mailboxes using RPC over HTTP. Connections to Exchange servers over Outlook Anywhere are encrypted with an SSL certificate. In Exchange 2010, Outlook Anywhere is an optional service that is not enabled by default, and is only enabled if external access is required. For internal access, Exchange 2010 mailbox users connect to the RPC Client Access Server, also known as the CAS Array. In Exchange 2013, Outlook Anywhere became the primary protocol for Outlook client access both internally and externally, and is therefore enabled by default. The same is true for Exchange 2016.

The Outlook Anywhere hostnames depend on the existing versions of Exchange in the environment:

- For Exchange 2010 only environments, Outlook Anywhere has an external hostname.
- For Exchange 2013 environments, Outlook Anywhere has both an internal and external hostname.

The Outlook Anywhere hostnames and authentication settings can be viewed by running the Get-OutlookAnywhere cmdlet. The ExternalHostname value is blank for an Exchange 2010 server.

[Click here to view code image](#)

```
#Retrieve the Outlook Anywhere settings using PowerShell

[PS] C:\>Get-OutlookAnywhere -Server NY-EX2013 | Select
Internalhostname,ExternalHostName,*auth*,*ssl*

InternalHostname : mail.contoso.com
ExternalHostname : mail.contoso.com
ExternalClientAuthenticationMethod : Ntlm
InternalClientAuthenticationMethod : Ntlm
IISAuthenticationMethods          : {Ntlm}
SSLOffloading                  : True
ExternalClientsRequireSsl       : True
InternalClientsRequireSsl      : True
```

To apply the same configuration to the Exchange 2016 server, use the Set-OutlookAnywhere cmdlet. When you run Set-OutlookAnywhere you must also specify the internal and external authentication methods, as well as the SSL requirements.

[Click here to view code image](#)

#### #Configuring Outlook Anywhere settings using PowerShell

```
[PS] C:\>Get-OutlookAnywhere -Server NY-EXCH01 | Set-OutlookAnywhere `  
-InternalHostname mail.contoso.com -ExternalHostname mail.contoso.com `  
-InternalClientAuthenticationMethod NTLM -InternalClientsRequireSsl $true  
`  
-ExternalClientAuthenticationMethod NTLM -ExternalClientsRequireSsl $true
```

### Important: Internal and External Authentication Methods for Outlook Anywhere

When the Outlook Anywhere internal and external hostnames are the same, only the external authentication method is used by clients. This is because the clients can't distinguish between the two hostnames and default to using the external authentication method. If you have a requirement for different internal and external authentication, for example if you want Kerberos for internal clients and NTLM for external clients, you must configure separate hostnames for Outlook Anywhere, such as an internal hostname of mail-internal.contoso.com, and an external hostname of mail-external.contoso.com. The external name should only be externally resolvable in DNS, and vice versa. There's no impact to users with this configuration because the Outlook Anywhere hostnames are automatically discovered using Autodiscover.

## MAPI over HTTP

The MAPI internal and external URLs are used by Outlook clients for Exchange 2013 and 2016 users in organizations with MAPI over HTTP enabled. The MAPI over HTTP protocol was introduced in Exchange 2013 Service Pack 1 and replaces Outlook Anywhere in future versions of Exchange. MAPI over HTTP is enabled by default at the organization level for new Exchange 2016 installations, but for existing organizations it is not enabled by default. Administrators can choose to enable it in existing organizations, which is recommended due to the performance and stability improvements that MAPI over HTTP provides for client connections when compared to Outlook Anywhere.

Exchange 2010 does not have a MAPI virtual directory, but Exchange 2013 does. By default, the MAPI virtual directory is configured with URLs containing the server's fully-qualified domain name. For organizations that have not enabled MAPI over HTTP,

the URLs might never have been changed from those original values. Whether you plan to enable MAPI over HTTP for an existing Exchange organization or not, it's still recommended to configure the MAPI over HTTP URLs with appropriate values by running the Set-MapiVirtualDirectory cmdlet.

[Click here to view code image](#)

```
#Configuring the MAPI virtual directory using PowerShell
```

```
[PS] C:\>Get-MapiVirtualDirectory -Server NY-EXCH01 | Set-MapiVirtualDirectory  
-InternalUrl https://mail.contoso.com/mapi  
-ExternalUrl https://mail.contoso.com/mapi
```

## Exchange Web Services

The Exchange Web Services internal and external URLs are used by Outlook and Outlook on the web clients to perform calendar free/busy queries, and manage Out of Office settings. To configure the Exchange Web Services URLs, run the Set-WebServicesVirtualDirectory cmdlet.

[Click here to view code image](#)

```
#Configuring the EWS virtual directory using PowerShell
```

```
[PS] C:\>Get-WebServicesVirtualDirectory -Server NY-EXCH01 | Set-WebServicesVirtualDirectory  
-InternalUrl https://mail.contoso.com/EWS/Exchange.asmx  
-ExternalUrl https://mail.contoso.com/EWS/Exchange.asmx
```

## Offline address book

The offline address book (OAB) is used by cached-mode Outlook clients to store a copy of the Global Address List (GAL) in the Exchange organization. This allows the client to access the GAL without relying on connectivity to the server. In Exchange 2016, the OAB is stored in an arbitration mailbox. Outlook clients discover the OAB URL in Autodiscover, and then make a connection to the OAB virtual directory. The Exchange 2016 mailbox server then proxies the client connection to the mailbox server hosting the database where the OAB mailbox exists so the OAB files can be downloaded. To configure the OAB namespace, run the Set-OabVirtualDirectory cmdlet.

[Click here to view code image](#)

```
#Configuring the OAB virtual directory using PowerShell
```

```
[PS] C:\>Get-OabVirtualDirectory -Server NY-EXCH01 | Set-OabVirtualDirectory  
-InternalUrl https://mail.contoso.com/OAB  
-ExternalUrl https://mail.contoso.com/OAB
```

## **Outlook on the Web and Exchange Control Panel**

The Outlook on the web internal and external URLs are used to access mailboxes using a web browser. When a user is connected to Outlook on the web, they can access configuration options for their mailbox by opening the Exchange Control Panel, which resides on a separate virtual directory from Outlook on the web. The Exchange Control Panel virtual directory is also used by administrators when they connect to the Exchange admin center.

The Outlook on the web and Exchange Control Panel virtual directories must be configured with the same URLs, as well as the same authentication methods. The authentication methods for Outlook on the web include forms-based, NTLM, and Basic. Forms-based is a popular choice because it presents an intuitive web form for logging in. Forms-based authentication is also the default on a new Exchange 2016 server for the Outlook on the web and Exchange Control Panel virtual directories. To configure the Outlook on the web and Exchange Control Panel URLs, run the Set-OwaVirtualDirectory and Set-EcpVirtualDirectory cmdlets.

[Click here to view code image](#)

```
#Configuring the OWA and ECP virtual directories using PowerShell
```

```
[PS] C:\>$hostname = "mail.contoso.com"
[PS] C:\>Get-OwaVirtualDirectory -Server NY-EXCH01 | Set-
OwaVirtualDirectory ` 
-InternalUrl https://$hostname/owa ` 
-ExternalUrl https://$hostname/owa
WARNING: You've changed the InternalURL or ExternalURL for the OWA virtual
directory. Please make the same change for the ECP virtual directory in
the same website.
[PS] C:\>Get-EcpVirtualDirectory -Server NY-EXCH01 | Set-
EcpVirtualDirectory ` 
-InternalUrl https://$hostname/owa ` 
-ExternalUrl https://$hostname/owa
```

## **Exchange ActiveSync**

The Exchange ActiveSync (EAS) internal and external URLs are used by mobile devices and applications to connect to mailboxes and synchronize email, calendar, and contact information. Although the ActiveSync URL is automatically discovered by mobile devices and apps via Autodiscover, when it is configured in the application, the Autodiscover service doesn't come into play again. This is in contrast to other services such as Exchange Web Services and OAB, where Outlook periodically redisCOVERS the URL at regular intervals or any time it is unable to connect to the URL that is already cached by the client, by making another Autodiscover query.

While other namespaces can be changed during a migration, changing the ActiveSync URL is more difficult because each mobile device or app needs to be reconfigured for

the new URL. If your organization is going through a change of brand that necessitates changing the URL, you can alias the old URL to the new one in DNS. As long as the SSL certificate on the Exchange server has both the old and new names on it, the mobile client connection should continue working.

To configure the ActiveSync URLs, run the Set-ActiveSyncVirtualDirectory cmdlet.

[Click here to view code image](#)

```
#Configuring the ActiveSync virtual directory using PowerShell
```

```
[PS] C:\>Get-ActiveSyncVirtualDirectory -Server NY-EXCH01 |  
Set-ActiveSyncVirtualDirectory  
-InternalUrl https://mail.contoso.com/Microsoft-Server-ActiveSync  
-ExternalUrl https://mail.contoso.com/Microsoft-Server-ActiveSync
```

## Managing the Namespace Switchover to Exchange 2016

When each of the namespaces have been configured on the newly installed Exchange 2016 mailbox servers, clients are still connecting to the old servers because that is where the namespaces resolve to in DNS. When you're ready to switchover to the Exchange 2016 servers, the DNS records for the namespace are updated.

Before making the change in DNS, it is recommended to lower the time-to-live (TTL) value for the DNS records. The TTL controls how long a DNS server or client caches the DNS record. Servers and clients with cached records do not see the changes you make in DNS until the TTL expires and they make a new DNS query. Therefore, by lowering the TTL to a value such as 5 minutes, you decrease the amount of time for the DNS change to take effect for the servers and clients on your network. The low TTL value also makes it faster to roll back the change in the event of a problem.

## Plan and configure proxy redirect

In previous Exchange coexistence scenarios, there were specific proxy and redirect considerations that needed to be planned for when Exchange 2007 or earlier versions of Exchange existed in the organization; specifically, the legacy namespace that Outlook on the web users would be redirected to after they logged in if their mailbox was not yet migrated. For Exchange 2016, the oldest version of Exchange that it can coexist with is Exchange 2010. In any Exchange 2016 coexistence with Exchange 2010 or 2013, there is no longer a legacy namespace that needs to be configured.

There are still proxy and redirect considerations for the different Exchange client access protocols, depending on whether a site is an Internet-facing site, a regional Internet-facing site, or a non-Internet-facing site. Fortunately with Exchange 2016, the proxy and redirect scenarios during coexistence are reasonably simple because Exchange handles most of it for you automatically.

You can control the behavior for some Exchange services by whether or not you configure an external URL. Sites with Exchange servers that have virtual directories configured with an external URL are considered Internet-facing, or regional Internet-facing. Sites with Exchange virtual directories that have an external URL value of \$null are considered non-Internet-facing.

## Autodiscover

The Autodiscover service does not have internal and external URLs configured on the virtual directory. Instead, internal clients look up the Autodiscover service connection point in Active Directory, and external clients look up the Autodiscover CNAME or SRV record in the public DNS zone. When the Autodiscover request is made to the Exchange 2016 mailbox server, the server locates the user's mailbox and proxies the connection to the mailbox server that hosts the user's mailbox. There is no redirection to consider for Autodiscover.

## Outlook on the web

Users enter the Outlook on the web URL into their web browsers to access their mailboxes, which might mean they are connecting to a URL that does not resolve to a server in the same site as their mailbox. The server that the user connects and logs on to locates the user's mailbox, and then:

- If the mailbox is hosted on a server in the same site, it proxies the request to that server.
- If the mailbox is hosted on a server in a site with no external URL, it proxies the request to a server in that site, which then performs a local proxy to the server hosting the mailbox.
- If the mailbox is hosted on a server in a site with a different external URL for example, a regional Internet-facing site, the server performs a cross-site silent redirection to the external URL of the site where the mailbox is hosted. Assuming that forms-based authentication is enabled on both servers, the user is automatically logged in to the server at the regional URL, which performs a local proxy to the server in the site that hosts the user's mailbox.

## **Other HTTPS Protocols**

For all other HTTPS protocols, the client discovers the namespace to connect to using Autodiscover. The client looks up the namespace in DNS, and connects to the IP address that it resolves to. The server that receives the request, if it is not the server that hosts the user's mailbox, proxies the request to the mailbox server that does host the user's mailbox at that time. Because Autodiscover always returns a URL for the site where the mailbox is hosted, there are no redirection scenarios to consider for other HTTPS protocols in on-premises coexistence.

## **POP and IMAP**

The POP and IMAP protocols behave in much the same way as the other HTTPS protocols. No matter where a POP or IMAP client connects to, the Exchange 2016 server always proxies the connection to the server that hosts the mailbox for that user. The main difference is that POP and IMAP do not use Autodiscover to determine where they should connect to. There are no redirection scenarios to consider for POP or IMAP.

## **Plan firewall configurations for coexistence**

When you switch over the client access namespaces to point to Exchange 2016, the clients must be able to connect to the server through the firewall. Most of the client access connectivity uses TCP port 443 (HTTPS), while POP uses TCP ports 110 and 995 and IMAP uses TCP ports 143 and 993. Because POP and IMAP are optional services that are not as commonly used, you might only need to open up the HTTPS port on your firewall and NAT the inbound connections to the Exchange 2016 server or to a load balancer that is being used to distribute client traffic to multiple Exchange servers.

Updating the firewall configuration to NAT the ports to Exchange 2016 is usually all that is required for switching over the external namespaces during a migration. This is because, for most organizations, the public IP addresses used for external access to Exchange are not being changed. Therefore, the public DNS entries for the client access namespaces can remain the same and the firewall is used to switchover instead.

## **Important: Exchange Servers and Firewalls**

While it is recommended to use a firewall to protect your Exchange servers from the Internet, it is not in any way supported to use firewalls to restrict traffic between two Exchange servers, or between Exchange servers and domain controllers. If any such firewalls exist inside your network, it is necessary to configure an “any any” rule for connectivity between Exchange servers, and between Exchange servers and domain controllers. The exception to this rule is the Edge Transport server, which is designed to be placed in a perimeter network and has documented firewall ports that it requires to be open.

## **Plan and configure for mail flow requirements**

During the coexistence period as you are migrating to Exchange 2016, there are three mail flow scenarios that you need to consider:

- Inbound mail flow to your organization from the Internet
- Outbound mail flow from your organization to the Internet
- SMTP relay for devices and applications on your network

Inbound mail flow from the Internet is controlled by the mail exchanger (MX) records published in your public DNS zone. If the public IP address you use for inbound SMTP connections is not changing, the MX record also does not need to change. The switchover of inbound email can therefore be managed by updating the firewall to NAT TCP port 25 (SMTP) to the Exchange 2016 server. If the public IP address for SMTP is changing, you can update the MX record in DNS, or the corresponding A record that the MX record points to. For the Exchange 2016 server itself, it is already configured with a receive connector that is ready to accept inbound SMTP connections from the Internet.

Outbound mail flow from your organization is controlled by using send connectors. Your organization should already have at least one send connector. You can either update the source transport servers on the existing send connector to include the new Exchange 2016 server and remove any old servers at the same time if you want to, or you can configure a new send connector that uses the Exchange 2016 server as the source transport server. When you are switching your outbound mail flow to go via the Exchange 2016 server, you should ensure that the firewall allows the server to make outbound connections on TCP port 25 (SMTP).

### **Note: Inbound/Outbound Mail Flow and Smart Hosts**

For many organizations, the Exchange servers do not send or receive email to and from the Internet directly. Instead, a smart host is used to perform email security functions such as antivirus and antispam. When a smart host is used for inbound mail flow, the switchover of mail flow to the Exchange 2016 server is performed on the smart host instead of via MX records or at the firewall. Similarly, when outbound mail flow goes via a smart host, the send connector is configured to use the smart host as the destination instead of looking up the recipient's MX records in DNS.

That just leaves SMTP relay to consider. It's common for network environments to have non-Exchange servers, applications, or devices that need to use the Exchange server as an SMTP service. By default, Exchange 2016 already has suitable receive connectors for receiving email from those systems, if the email is addressed to internal recipients. For external recipients, an SMTP relay connector is required on the Exchange server. The receive connector that you create for SMTP relay purposes can and should be restricted to the specific IP addresses that require SMTP relay access to prevent the connector from being abused by any rogue applications or users in your environment. Ideally, the devices and applications on your network that require SMTP relay are connecting to a DNS alias that points to an existing Exchange server. If so, after you've created the new receive connector for SMTP relay, you can update the DNS record to direct the traffic at the Exchange 2016 server. If the devices are not using a DNS alias, you need to reconfigure them all individually. A migration to a new server is a good opportunity to establish a DNS alias for SMTP relay purposes, so that future migrations are easier.

### **Need More Review? Allow Anonymous Relay on Exchange Servers**

The receive connector used for SMTP relay can be configured by running the New-ReceiveConnector cmdlet. The connector is configured with the remote IP addresses that are permitted to relay email through the connector, and configured with Active Directory permissions to permit anonymous connections to relay to external addresses. You can see the full configuration procedure on TechNet at

[https://technet.microsoft.com/library/mt668454\(v=exchg.160\).aspx](https://technet.microsoft.com/library/mt668454(v=exchg.160).aspx).

## Plan for mailbox migrations

When coexistence has been successfully configured and when you've switched over your client access namespaces and mail flow to Exchange 2016, you can begin migrating mailboxes. Migrations to Exchange 2016 are initiated from the Exchange admin center or the Exchange Management Shell on the Exchange 2016 server. You can think of the migration process as the newer Exchange server pulling the data from the source mailbox database to the destination database.

Mailboxes are moved from an Exchange 2010 or Exchange 2013 mailbox server by creating mailbox move requests. A move request moves an individual mailbox from one database to another. Move requests can be created individually, or they can be created as a batch of one or more move requests. The underlying migration process is the same. The migration of data is handled by the Mailbox Replication Service (MRS), which processes the move request as a background task. The MRS starts and stops the move request depending on the workload of the server at the time. If the server is under a heavy load, you can expect your move requests to take longer to complete. In some ways, this makes it more difficult to predict how long a mailbox migration takes because it's not a case of data copying from one place to another at maximum speed.

Being able to anticipate the duration of a move request, however, is not as important these days because the migration is processed as an online move. Users can continue to access their mailboxes on the source database while the move request processes the first 95 percent of the mailbox data. When it reaches 95 percent completion, the move request is automatically suspended if the administrator has configured it to do so. This allows you to control when the final cutover of the mailbox occurs. Alternatively, you can allow the MRS to complete the move automatically when it reaches 95 percent completion. The completion stage of the move request locks the user out of their mailbox. The MRS is then able to synchronize the remaining mailbox data, including any changes that the user made since the move request started. When all of the data is synchronized to the target database, the user's mail attributes are updated in Active Directory with the new database details and the mailbox is unlocked in the destination database. The final cutover process can take just a few minutes or longer, depending on how much data changed in the mailbox while the move request was running.

## **Important: Mailbox Moves and Autodiscover**

When a user restarts Outlook after a mailbox move, it is Autodiscover that updates the user's profile with the new location of their mailbox. Autodiscover queries Active Directory for the mail attributes of the user, therefore any delay in Active Directory replication might cause Autodiscover to return the wrong information. Furthermore, the Autodiscover service caches information for a period of time. Users who try to connect to their mailbox immediately after a move request completes might not be able to if the Autodiscover cache is causing the wrong information to be provided. In such cases, restarting the Autodiscover app pool in IIS clears the cache. In many real world migrations, restarting the app pool after completing a migration batch is a formal part of the migration process.

Moving mailboxes between databases generates a lot of changes within the target database, which in turn means that transaction logs are generated on the server hosting the target database. The amount of transaction logging generated depends on the amount of mailbox data being moved. As a general rule, you can plan for 1 GB of transaction log data to be generated for every 1 GB of mailbox data that is migrated. As such, you should plan your migration batches so that you do not exceed the amount of available transaction log disk space on the destination mailbox server. You can review the sizes of your mailboxes to plan migration batches by exporting the mailbox statistics to a comma-separated value (CSV) file.

[Click here to view code image](#)

```
#Export mailbox statistics to CSV file
```

```
[PS] C:\>Get-Mailbox | Get-MailboxStatistics | Export-Csv  
C:\Temp\MailboxStatistics.csv
```

When move requests or migration batches are created, the target database can be manually specified, or you can allow the MRS to automatically choose a target database for the move. If you do not want a database to be automatically selected as a target for a move, you can exclude it by running the Set-MailboxDatabase cmdlet to exclude the database from auto-provisioning.

[Click here to view code image](#)

```
#Exclude a mailbox database from automatic provisioning
```

```
[PS] C:\>Set-MailboxDatabase -Identity DB01 -IsExcludedFromProvisioning  
$true
```

Excluding a mailbox from automatic provisioning doesn't prevent you from manually choosing the database as the target for a move, it only prevents the Exchange server from automatically selecting it.

Exchange automatically balances the distribution of mailboxes across the available databases in terms of numbers, but not by taking into account the size of the mailbox. As such, you should still choose the target database for mailbox moves if you have concerns about balancing the size of your mailbox databases, or if you are moving a batch of very large mailboxes that you want to place on specific target databases. When you choose a target database you can also choose whether to move the user's archive mailbox to the same database or a different database, if they are archive enabled.

### **Important: Back Up Your Mailbox Databases**

Before you perform any mailbox migrations, you should ensure that the target mailbox databases are being successfully backed up. Database backups are important during a migration for two reasons. First, you do not want to risk your mailbox data by migrating it to a database that is not being protected by backups. Second, the backups truncate the transaction logs for the database, which recovers the disk space they were utilizing and prevents the migration activity from filling up all of the available capacity on a transaction log volume.

## **Troubleshoot transport in coexistence**

Internal mail flow between the Exchange servers within your organization does not require any special configuration. Exchange is capable of routing mail within the organization, including between different versions of Exchange. You do not need to configure send connectors or receive connectors to facilitate internal mail flow. In fact, doing so might break internal mail flow, particularly if you modify any of the receive connectors on the Exchange servers that are automatically created by Exchange setup.

Each Exchange server in your coexistence environment should ideally be able to connect to any other Exchange server on TCP port 25 (SMTP). You can test SMTP connectivity between servers by running the Telnet application. The Telnet client is not installed by default on Windows Server, so first you should install it by running Install-WindowsFeature. When Telnet is available you can connect to another Exchange server to verify connectivity.

[Click here to view code image](#)

```
#Using Telnet to connect to another Exchange server
```

```
C:\>telnet ny-exch02.contoso.com 25
```

```
220 NY-EXCH02.contoso.com Microsoft ESMTP MAIL Service ready at Sun, 5 Jun  
2016
```

```
20:48:17 +1000
```

Even though Telnet is able to connect, it does not indicate which receive connector on the server is accepting the SMTP connection. If the wrong receive connector handles a connection, it can cause the connection to fail. For example, if an Exchange server connects to another server to pass along a message for internal mail flow, but the SMTP relay connector on the target server accepts the connection, the configuration of the SMTP relay connector prevents the required authentication from successfully occurring between the two Exchange servers and the connection fails. This is commonly caused by adding the wrong IP addresses or IP address ranges to SMTP relay connectors. To help identify such issues with receive connectors, you can configure the SMTP banner on connectors to announce the name of the connector, rather than only announcing the name of the server.

[Click here to view code image](#)

```
#Configure the SMTP banner on a receive connector
```

```
[PS] C:\>Set-ReceiveConnector -Identity "NY-EXCH02\Relay" -Banner "220 NY-  
EXCH02\Relay"
```

To help you troubleshoot SMTP connectivity issues, you can also turn on protocol logging for receive connectors on your Exchange servers. Protocol logs are text files in CSV format, and contain information about the SMTP communications that are occurring on the receive connectors for a server. All of the details are logged to a single file that rolls over each day and includes useful data such as the source IP address of the connection, the receive connector that handled the request, and the SMTP commands and responses that occurred during the session. Some of the receive connectors that Exchange setup creates already have protocol logging enabled by default. If you need to enable protocol logging for additional connectors, use the Set-ReceiveConnector cmdlet.

[Click here to view code image](#)

```
#Reviewing the protocol logging configuration for a server
```

```
[PS] C:\>Get-ReceiveConnector -Server NY-EXCH02 | Select  
Name,ProtocolLoggingLevel
```

Name	ProtocolLoggingLevel
Default NY-EXCH02	None
Client Proxy NY-EXCH02	None
Default Frontend NY-EXCH02	Verbose
Outbound Proxy Frontend NY-EXCH02	Verbose
Client Frontend NY-EXCH02	None

Relay

None

```
[PS] C:\>Set-ReceiveConnector NY-EXCH02\Relay -ProtocolLoggingLevel  
Verbose
```

If the SMTP communications between two servers is occurring without issue, you can continue your troubleshooting with the message tracking logs. Message tracking is enabled by default on mailbox and transport servers. The message tracking logs files are also text files in CSV format, so they are human-readable. You can get more value out of them by performing message tracking log searches with the Get-MessageTrackingLog cmdlet. For example, to search for emails sent by Kim Akers in the last 24 hours, you can run the following command.

[Click here to view code image](#)

```
#Searching message tracking log files
```

```
[PS] C:\>Get-MessageTrackingLog -Sender Kim.Akers@contoso.com -Start (Get-  
Date).  
AddHours (-24)
```

### Need More Review? Searching Message Tracking Logs

The Get-MessageTrackingLog cmdlet is quite powerful, with a variety of parameters that are used to search for messages based on sender, recipients, message subject, date ranges, servers, and more. In addition, the message tracking log search results can be filtered to specific events, error codes, and a variety of other metadata that is useful for determining the cause of a mail flow issue. You can find more information about message tracking log searches on TechNet at

[https://technet.microsoft.com/library/bb124926\(v=exchg.160\).aspx](https://technet.microsoft.com/library/bb124926(v=exchg.160).aspx).

## Troubleshoot client access in coexistence

When you switch over the client access namespaces during the coexistence period, you can immediately run into problems if there is a misconfiguration in your environment. If the issues are affecting all of your users, a DNS or server-side problem is the most likely issue. Rolling back your DNS change while you re-evaluate the configuration restores service, but you still need to be able to investigate the problem. Using a host file entry on a test computer is a good way to force one client to start connecting to the Exchange 2016 server, without making a DNS change that would impact all of your users.

Client connectivity issues can be protocol-specific. For example, Outlook might not work, but Outlook on the web does. That type of analysis of the situation helps you

narrow down the possible causes of the issue. Any client that relies on Autodiscover and is having problems means you might have an issue with the Autodiscover namespace or service. You can test Autodiscover internally from Outlook clients by running the Test E-Mail AutoConfiguration utility in Outlook. External Autodiscover testing can be performed using the Microsoft Remove Connectivity Analyzer (<https://testconnectivity.microsoft.com>).

Because client connectivity occurs over HTTPS, you can use the IIS logs to help troubleshoot the problem. Particularly when connections are being proxied between Exchange servers, the IIS logs can help you to identify such issues as authentication errors, SSL negotiation errors, and misconfigured URLs.

In high availability deployments, the configuration of the load balancer is also a factor in client connectivity. A misconfigured load balancer can send client traffic to unhealthy Exchange servers, causing some of your clients to have issues while others are working fine. Testing a load balancer involves either bypassing it completely, by pointing the DNS records for your namespaces directly at an Exchange 2016 server, or by using the load balancer to disable the passing of client traffic to specific servers in a process of elimination.

## Summary

- Few Exchange 2016 deployments are made into brand new environments, so it is common to install Exchange 2016 into an existing organization and configure the environment for a period of coexistence.
- The namespaces in a coexistence environment should be pointed at the highest version of Exchange in the organization. For Exchange 2013 coexistence, the namespaces can be pointed at either Exchange 2013 or 2016 because the two products proxy connections to each other seamlessly.
- The coexistence configuration is made up of several pieces working together. Client connectivity is determined by the namespace configuration. Mail flow is determined by MX records in DNS, send connectors for outbound connectivity, and custom relay connectors for internal SMTP requirements.
- Plan your mailbox migrations based on the sizes of the mailboxes and how you want them distributed across the available target mailboxes. Be mindful of the transaction logging generated by the migration activity and plan your migration batches and database backups accordingly.

## **Skill 6.4: Migrate from earlier supported versions of Exchange**

Exchange 2016 can coexist with Exchange 2010 Service Pack 3 with Rollup Update 11 or later and with Exchange 2013 cumulative update 10 or later. Although those are the minimum coexistence requirements for Exchange 2016, you should be mindful of the support status of the updates for the earlier versions of Exchange. At the time of this writing, cumulative update 10 for Exchange 2013 is already out of support. Therefore, you should not assume that being supported for coexistence means the same as being supported for deployment in a production environment. If you encounter issues with unsupported update levels, Microsoft support requests that you update to a supported version before they provide support for your problems. To lower the likelihood of encountering coexistence issues, and to ensure that you can receive support from Microsoft, you should deploy the latest available updates for your servers.

---

### **This section covers how to:**

- [Determine transition paths to Exchange](#)
  - [Migrate mailboxes](#)
  - [Migrate to modern public folders](#)
  - [Troubleshoot Mailbox Replication Services](#)
  - [Plan for discontinued features](#)
  - [Transition and decommission servers](#)
- 

### **Determine transition paths to Exchange**

An Exchange organization exists within a single Active Directory forest. You can install Exchange 2016 into an existing Exchange 2013 or Exchange 2010 organization and migrate the data and services to the new server. If any versions earlier than Exchange 2010 exist in the organization, the installation of Exchange 2016 is blocked. For organizations running Exchange 2007 or earlier, you need to develop a strategy to achieve the migration:

- You can perform an intermediate migration to a supported version of Exchange. For example, an Exchange 2003 or 2007 organization can be migrated to Exchange 2010. When the Exchange 2003 or 2007 servers have been fully decommissioned, you can introduce the Exchange 2016 server, perform another migration, and then remove the Exchange 2010 server. This approach preserves the existing Active Directory forest and Exchange organization, and might be the best approach for companies that have many other systems tightly integrated into the environment.
- You can deploy Exchange 2016 into a new Active Directory forest. A forest trust

is then created, and cross-forest mail flow and Availability are configured to provide users with a good collaborative experience during the coexistence period. If you only migrate Exchange resources into the new forest, you have multiple Active Directory forests to provide hardware infrastructure and software licenses for, and you need to manage and maintain both forests going forward.

Although this section describes migration approaches that use the native capabilities of Exchange and Active Directory, you should also be aware that a number of third party migration products exist that can facilitate a migration between two versions of Exchange that are unsupported for coexistence. Although the third party tools can't overcome the inability to run Exchange 2016 in an organization with Exchange 2007 or earlier services, they can make the complexity of cross-forest migrations easier to manage.

## Migrate mailboxes

Before you migrate any user mailboxes to Exchange 2016, you must first migrate the arbitration mailboxes. The arbitration mailboxes perform functions such as storing administrator audit logs for the organization and storing messages that are being held by moderated transport. In a coexistence environment, the arbitration mailboxes need to be moved first so that they are hosted on the highest version of Exchange in the organization, which allows those functions to continue working. To create move requests for the arbitration mailboxes, run the New-MoveRequest cmdlet.

[Click here to view code image](#)

```
#Moving arbitration mailboxes
```

```
[PS] C:\>Get-Mailbox -Arbitration | New-MoveRequest -TargetDatabase DB08
```

You can then monitor the progress of the move requests by running the Get-MoveRequestStatistics cmdlet. When the arbitration mailboxes are finished migrating, you can move on to migrating other mailboxes. You can create individual move requests by using the New-MoveRequest cmdlet mentioned previously, or you can manage the migrations by using the Exchange admin center. Log in to the EAC and click Recipients, and then Migration. Start a new migration batch from the menu by choosing to “Move to a different database.”

Mailboxes can be added to the batch by selecting them from the picker, as shown in [Figure 6-7](#), or you can use a CSV file. The CSV file has just one required field named EmailAddress, which contains the primary SMTP address of the users to migrate. There are four optional fields that you can also include in the CSV file:

- **TargetDatabase** Allows you to specify different target databases for each mailbox in the migration batch. Without this field, you can only specify one target

database for the entire batch, or alternatively you can allow Exchange to automatically choose a target database for you.

- **TargetArchiveDatabase** Works the same way as the TargetDatabase field, but for archive mailboxes.
- **BadItemLimit** Controls how many corrupt items you're willing to discard from each mailbox to complete the migration successfully. The default value is 10, and it's common for every mailbox to have at least a few corrupt items. If the threshold is reached, that particular mailbox in the batch fails to migrate, but the remaining mailboxes in the batch can continue to be migrated.
- **MailboxType** Specifies whether to move the primary mailbox, the archive mailbox, or both. If this field is excluded, the default behavior is to move both the primary and archive mailboxes.

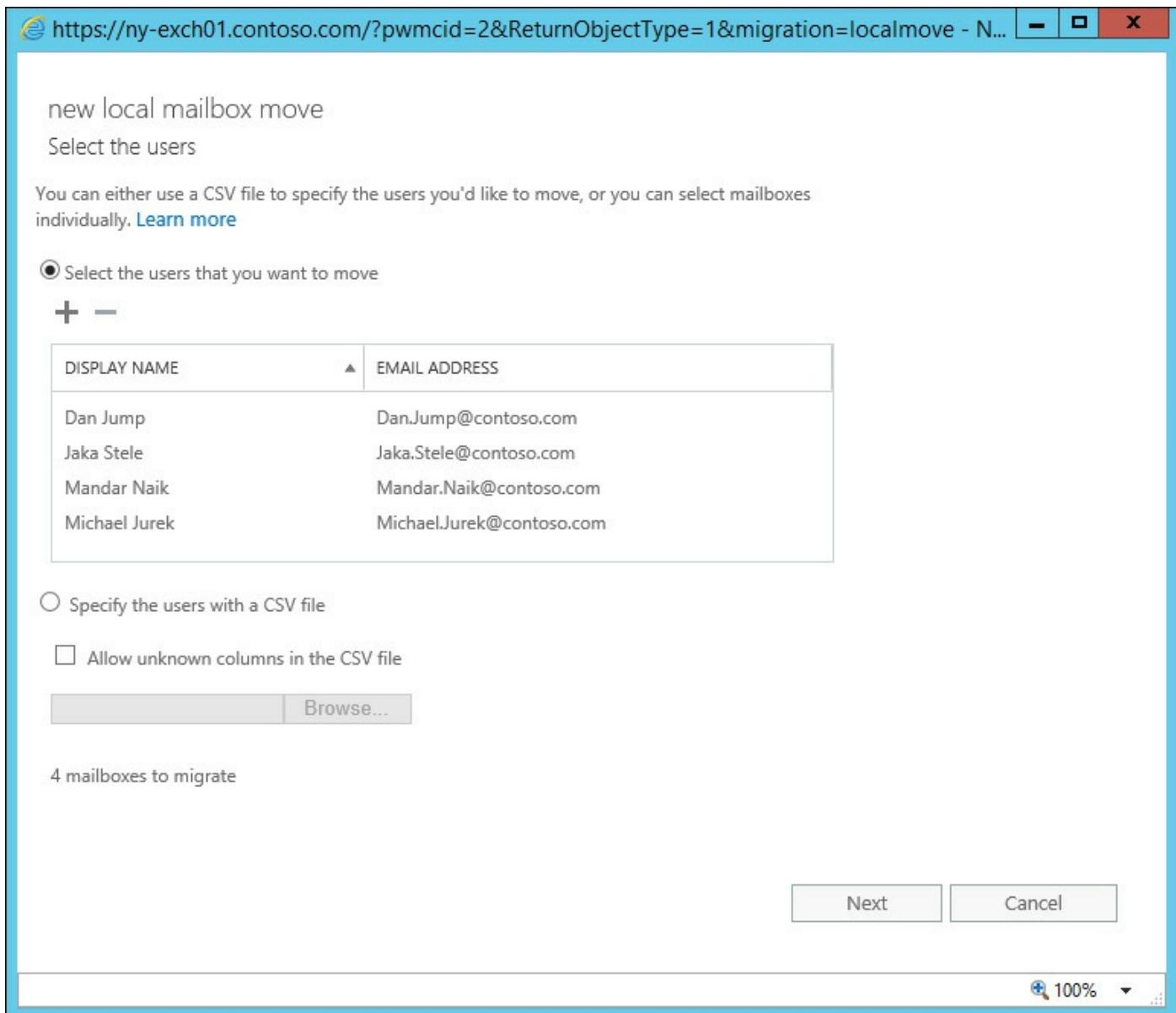


FIGURE 6-7 Creating a new migration batch

After selecting the mailboxes to move, you must give the migration batch a name and then choose how to handle primary and archive mailboxes. This is the stage where you can also manually select a target database for the mailboxes in this batch if you need to. The bad item limit can also be adjusted at this stage. Finally, you can choose a recipient for the email notifications sent for the migration batch and choose whether to automatically start and complete the batch.

A migration batch can also be created by running the New-MigrationBatch cmdlet. When you use the PowerShell cmdlet to create a migration batch, you can provide the CSV file containing the email addresses of the mailboxes to move or provide a comma-separated list of users to migrate. Using a CSV file is easier than typing out a long list of users for large migration batches.

[Click here to view code image](#)

#### #Creating a migration batch using PowerShell

```
[PS] C:\>New-MigrationBatch -Local -Name MigrationBatch1  
-CSVData ([System.IO.File]::ReadAllBytes("C:\Migrations\batch1.csv"))  
-AutoComplete:$false -NotificationEmails administrator@contoso.com
```

You can create migration batches ahead of time, and then start them when you're ready by running the Start-MigrationBatch cmdlet. You can then observe the status of the migration batch by running the Get-MigrationUser cmdlet. When the batch is ready to complete, if you did not configure it to autocomplete, you can then run the Complete-MigrationBatch cmdlet.

[Click here to view code image](#)

#### #Viewing the status of a migration batch

```
[PS] C:\>Get-MigrationUser -BatchId MigrationBatch1 | ft -auto
```

Identity	Batch	Status	LastSyncTime
Ryan.Danner@contoso.com	MigrationBatch1	Syncing	
Mike.Danseglio@contoso.com	MigrationBatch1	Syncing	
Alex.Darrow@contoso.com	MigrationBatch1	Syncing	
Shannon.Dascher@contoso.com	MigrationBatch1	Syncing	
WillsonRaj.David@contoso.com	MigrationBatch1	Syncing	
Dan.Jump@contoso.com	MigrationBatch1	Syncing	

## Migrate to modern public folders

After completing the migration of mailboxes to Exchange 2016, you can perform the migration of legacy public folders from Exchange 2010. In reality, you can start the migration process at any time during your mailbox migration. For larger public folder environments this might be necessary to get a head start on the public folder data migration, rather than leave it all to the very end of the mailbox migrations. You do need to consider the load on the Exchange 2016 servers generated by the public folder migration, which might slow down or delay the mailbox migration if the two workloads are competing for resources on the same server.

You should not complete the public migration from Exchange 2010 until all of the mailboxes are completed. The reason is that Exchange 2010 mailbox users can't access the modern public folders that Exchange 2016 provides. Modern public folders in Exchange 2016 are hosted in public folder mailboxes, not in public folder databases as they were for Exchange 2010 and earlier.

A public folder migration is a good time to clear out unwanted public folder data. The less unnecessary data and the fewer folders you migrate to Exchange 2016, the easier it is to migrate and manage going forward. Unfortunately, for many organizations it's too challenging to determine what is and isn't required in the public folder data, so you are forced to migrate all of it. In this case you need to take care to size the modern public folder mailboxes appropriately. At the time of this writing, the size limit for an individual public folder is 100 GB, and any single public folder must not exceed 10 GB in size. There is also an upper limit of 1,000,000 total public folders and a series of limits as to the number and depth of sub-folders that can exist in the hierarchy. Those are support limits, not hard technical limits, but they exist for performance and stability reasons.

### Need More Review? Public Folder Limits

The public folder limits have changed over time as Microsoft has been able to squeeze more efficiency out of the modern public folder architecture. They haven't changed recently however, so it's possible they are not going to increase from their current limits during the lifecycle of Exchange 2016. You can read the full list of public folder limits on TechNet at

[https://technet.microsoft.com/library/dn594582\(v=exchg.160\).aspx](https://technet.microsoft.com/library/dn594582(v=exchg.160).aspx).

The migration from legacy public folders to modern public folders uses a batch migration process. A series of PowerShell scripts, provided by Microsoft, are used to collect information about the size and makeup of the existing public folder hierarchy and

export it to XML and CSV files. When you review the CSV file containing the folder names and sizes of the legacy public folders, use that information to decide how many modern public folder mailboxes you are going to create by choosing a maximum size for the public folder mailboxes. For example, if the CSV file shows that you have 50 GB of public folder data, and you elect to have a maximum public folder mailbox size of 10 GB, a map that distributes the data across five public folder mailboxes is generated by Microsoft's script.

At least one public folder mailbox is necessary to store the primary copy of the hierarchy. As a best practice, it is not recommended to store public folder data in the same mailbox, except for very small environments. When you've created the public folder mailboxes with names that align to the mailbox names in the script-generated map, you're ready to begin the batch migration process. The new public folder migration batch is started and allowed to run until it has completed the initial synchronization of data, at which time it sends you an email notification.

You can then schedule downtime for the public folders to complete the migration. During the completion stage, the legacy public folders are locked and are inaccessible to users. The time required for the final synchronization phase depends on how much public folder data has changed since the initial synchronization process was completed. When the final synchronization is successful, you can unlock the modern public folders and mark the public folder migration complete.

### Need More Review? Public Folder Migration

The full process for performing a batch migration of legacy public folders to Exchange 2013 is available on TechNet at  
[https://technet.microsoft.com/library/mt463355\(v=exchg.150\).aspx](https://technet.microsoft.com/library/mt463355(v=exchg.150).aspx).

For Exchange 2013 environments where public folders have already been migrated to modern public folders, the migration to Exchange 2016 is made much simpler. All that is required is to perform mailbox migrations for the public folder mailboxes to a target database on the Exchange 2016 mailbox server.

## Troubleshoot Mailbox Replication Services

The Mailbox Replication Service (MRS) processes the data migration for mailboxes and public folders to Exchange 2016. If a migration batch or a move request did not complete successfully, you can review the statistics for the move to determine why it failed. For individual move requests, use the Get-MoveRequestStatistics cmdlet, and review the Status, StatusDetail, Message, FailureCode, and FailureType attributes. If the move request failed due to the bad item limit being exceeded, you can review the BadItemLimitEncountered attribute.

[Click here to view code image](#)

```
#Reviewing move requests statistics using PowerShell
```

```
[PS] C:\>Get-MoveRequest "Ryan Danner" | Get-MoveRequestStatistics | Format-List
```

For migration batches, you can also review the output of Get-MigrationUserStatistics, which includes Status, StatusSummary, and ErrorSummary attributes that provide some information about the reason for the failed move as well.

[Click here to view code image](#)

```
#Reviewing migration user statistics using PowerShell
```

```
[PS] C:\> Get-MigrationUser ryan.danner@contoso.com | Get-MigrationUserStatistics | Format-List
```

If the move request and migration user statistics do not reveal the cause of migration failures, you can also review the event logs on the Exchange 2016 mailbox servers that were involved in processing the migration. To determine which servers were involved, run the Get-MigrationBatch cmdlet and use the -IncludeReport parameter.

[Click here to view code image](#)

```
#Viewing the migration batch report using PowerShell
```

```
[PS] C:\>Get-MigrationBatch -Identity MigrationBatch1 -IncludeReport | Select Report | Format-List
```

### Note: Adjusting MRS Performance Values

The performance of the MRS depends on the workload on the server at any given time. When a server is under a heavy load, it de-prioritizes the migration tasks, or even stops them entirely, so that resources can be used for client requests. The MRS also processes a maximum amount of data at any one time. It's possible to adjust the behavior of the MRS to be more tolerant of high workloads, or to migrate data faster, but this is not recommended unless under the direction of Microsoft Support.

## Plan for discontinued features

With each release of Exchange Server, it is normal to find that some features of previous versions of Exchange have been discontinued. Exchange 2016 is no different, and a number of features have been deprecated or discontinued. For deprecated features, you can continue to use them, but you should expect them to be discontinued in a future release of Exchange. It is a good idea to begin making plans to replace those features with another solution if you still need the functionality.

For discontinued features, you have no choice but to seek alternatives. Some discontinued features have a clear way forward. For example, Exchange 2016 does not support Outlook 2003 as a client, but you can upgrade to a supported version of Outlook to solve that. Other discontinued features are of very low impact. Spell check, for example, has been removed from Outlook on the web, as most modern browsers provide their own spell check functionality.

### Need More Review? Discontinued Features from In Exchange 2016

A full list of discontinued features from Exchange 2010 and Exchange 2013 and suggestions for their replacements, is provided on TechNet at  
[https://technet.microsoft.com/library/jj619283\(v=exchg.160\).aspx](https://technet.microsoft.com/library/jj619283(v=exchg.160).aspx).

## Transition and decommission servers

When you've completed the migration of client access namespaces, mail flow, mailboxes, and public folders to Exchange 2016, you can begin planning to remove the unused Exchange 2013 or 2010 servers from the organization. When you remove an Exchange server it is vital that you uninstall the Exchange Server software from the computer properly. If you simply shut down a server, all of the objects and configurations relating to that server are left behind in Active Directory. This is more than just the computer account; there is a significant amount of data in Active Directory for Exchange server configurations. When all of that configuration data is not cleanly removed, it can cause issues with the ongoing operations of your Exchange 2016 environment and can also block the installation of future versions of Exchange.

Before you completely uninstall the legacy Exchange servers from the environment, there are some things that you should consider. First, the servers might still be responding to a small number of client requests. Most commonly, this is due to SMTP connections from devices or applications that were missed during the migration. You can use protocol logging and message tracking log searches to check for any such connectivity that might be occurring. Similarly, you can use IIS logging to check for client activity. Unfortunately, the IIS logs on legacy servers continue to show activity due to the health probes that are part of the Managed Availability system for Exchange.

2016. Here, you need to filter the IIS logs to exclude system-generated traffic.

There is also the matter of future database restores. Exchange mailbox databases can only be restored and mounted on the same version of Exchange that previously hosted them. This means that you can't restore an Exchange 2010 database from your backups and mount it on an Exchange 2016 server to recover data. Unfortunately, it's not a simple matter of reinstalling an earlier version of Exchange to handle that restore scenario. When the last legacy server has been removed from the environment, you can no longer install any servers of that version into the organization again. Furthermore, your Exchange organization might be migrated to a version that does not coexist with the legacy version that you need for data recovery purposes.

Some companies deal with this situation by retaining at least one Exchange server running the previous version of Exchange for a suitable period of time after the migration is complete. In such cases, it's better to leave the server running, configured in a way that clients and mail flow do not depend on it, rather than shut it down and only power it on when needed. For one thing, the computer account of the server might expire while it is shut down, complicating the process of bringing the server back online. Another risk is that the server is forgotten, or is not maintained with regular patching and updates.

Ultimately, the goal is to remove the legacy Exchange servers to complete the migration to Exchange 2016. If data restoration scenarios are a concern, there is a range of third party tools that can mount Exchange databases for the purposes of restoring data that do not require any version of Exchange be installed to work.

## Summary

- An Exchange organization can migrate to Exchange 2016 from supported versions of Exchange 2010 and 2013. For scenarios where there is a block preventing Exchange 2016 from being introduced to the same organization, cross-forest scenarios and third party tools can be used to achieve the migration to Exchange 2016.
- Mailbox migrations are processed using move requests and migration batches. Administrators are provided with flexible options to configure, manage, and monitor the migrations to completion.
- If public folder data is to continue being used by the organization, a migration from legacy public folder databases to modern public folder mailboxes must be performed. Modern public folders are subject to support limits that don't impact most organizations. Every organization can benefit from taking the opportunity to clean up and reduce their public folder data size and complexity.
- Legacy Exchange servers must be properly decommissioned from the

organization. If not, they cause lingering performance and stability problems in the future. You should always consider how to achieve data recovery in scenarios where the legacy versions have been removed.

## Thought experiment

Contoso, Ltd. is running an Exchange 2007 environment and wants to migrate some of its email workload to Office 365 to take advantage of the larger mailbox size limits, better webmail experience, and the security of Exchange Online Protection.

A portion of the email workload for specific departments is to be retained on-premises. The company also has a compliance regulation that is met by journaling all Internet emails to an on-premises archiving solution.

1. How should the migration to Exchange Online be performed?
2. What type of Exchange server should be deployed on-premises?
3. What is the email routing topology that should be configured in the environment?

## Thought experiment answer

This section contains the answers to the thought experiment.

1. To meet the requirement of maintaining some mailbox users on-premises and migrating the rest of the mailboxes to Exchange Online, a Hybrid configuration should be deployed. The Hybrid configuration provides the rich coexistence between on-premises and online users, and also facilitates the migration of mailboxes to Exchange Online.
2. To provide the best Hybrid experience, an Exchange 2016 server should be deployed on-premises. Because the server is hosting mailboxes, it is not eligible for the free Hybrid license from Microsoft. The server can't be installed while the Exchange 2007 server still exists in the organization. Therefore, a migration from Exchange 2007 to 2010 or 2013 must be performed first.
3. To make use of Exchange Online Protection to prevent spam and mail-borne malware, the MX records for the domain are pointed to Office 365. To meet the requirement of journaling all Internet email to the on-premises archiving system, centralized transport must be enabled when the Hybrid Configuration Wizard is run.

# Index

## A

ABQ [93–94](#)

access. See data access

access control

mobile devices [79–80](#)

role-based [218–226, 269](#)

ACEs. See [Access Control Entries \(ACEs\)](#)

ACLL. See [Attempt Copy Last Logs](#)

ACM. See [Application Compatibility Manager](#)

ACT. See [Application Compatibility Toolkit](#)

ActivationOnly switch [62](#)

Activation Preference (AP) number [35–36, 50](#)

Active-Active DAG [40](#)

active database copy [36](#)

Active Directory [56, 57](#)

Active Directory (AD)

split permissions [221–223](#)

user accounts [199](#)

Active Directory Domain Services (AD DS) [76, 132–135, 187–198](#)

dedicated, for Exchange [190](#)

DNS changes for Exchange [191](#)

domain controllers, number of [188–190](#)

preparing for Exchange [192–198](#)

schema extension [192](#)

site topology [194–197](#)

throttling policies [197](#)

Active Directory Federation Services (AD FS) [299–301](#)

Active Directory Federation Services (AD FS) Proxy role service. See [Web Application Proxy](#)

Active Directory forest [339](#)

Active Directory Lightweight Directory Services (AD LDS) [145](#)

Active Directory Rights Management Services | (AD RMS) [235–241, 306](#)

integration of Exchange Server with [236](#)

RMS template creation [237–238](#)  
Super Users group [236](#)  
transport protection rules [238](#)

Active Directory Site [38, 49](#)  
ActiveDirectorySite parameter [42](#)

Active Directory sites  
namespaces and [323](#)

Active Manager [48, 49, 50, 182, 183](#)  
Active-Passive DAG [39–40](#)

ActivSync devices  
security policies for [80–82](#)

Add-DatabaseAvailabilityGroup cmdlet [29](#)  
Add-MailboxDatabaseCopy cmdlet [35](#)  
Add-MailboxPermission cmdlet [214, 293](#)  
Address Book Policy Routing agent [86](#)

address lists  
hierarchical [84–85](#)

address rewriting [156](#)  
Address Rewriting Inbound Agent [156](#)  
Address Rewriting Outbound Agent [156](#)  
Add Roles and Features Wizard [98](#)  
Add-WindowsFeature cmdlet [98](#)  
administrative audit logging [290–293](#)  
configuration [291](#)  
searching audit logs [291–293](#)

administrative connectivity [75](#)  
AllowLegacyDNMismatch switch [59](#)  
alternate File Share Witness [41–42](#)  
Alternate Service Account (ASA) [115](#)  
AlternateWitnessServer parameter [42](#)  
anti-malware policy [164–166](#)  
apps. See also application management  
App-V. See Microsoft Application Virtualization  
arbitration mailboxes [291, 339](#)  
architecture  
Exchange Server 2016 [1, 24, 61](#)

archive mailboxes [265–266](#), [267–268](#)  
capacity and placement [5–6](#)  
archives [266–268](#)  
archive storage quotas [265](#), [267](#)  
archiving [256–268](#)  
    in-place [265–266](#)  
    online [266–268](#)  
    policies [257–258](#)  
attachment access [79](#)  
attachment filtering [167](#)  
Attempt Copy Last Logs (ACLL) [48](#)  
AuditDelegate actions log [287](#)  
auditing  
    administrative audit logging [290–293](#)  
    mailbox audit logging [286–290](#)  
audit log storage [287](#)  
authentication  
    Basic [75](#), [79](#), [82](#), [115](#)  
    configuration [74–75](#)  
    Digest [75](#), [79](#)  
    forms-based [74–75](#), [79](#), [115](#), [328](#)  
    integrated [74](#)  
    Integrated Windows [79](#), [82](#), [115](#)  
    Kerberos [74](#), [75](#), [115](#)  
    mutual [144–145](#)  
    NTLM [75](#)  
    OAuth [88–89](#)  
    OAuth-based [306–307](#)  
    Outlook Anywhere [327](#)  
    Outlook on the web [79](#)  
    planning [74–75](#)  
    pre-authentication [75](#)  
    troubleshooting [115](#)  
AutoDagDatabasesRootFolderPath property [12](#)  
AutoDagVolumesRootFolderPath property [12](#)  
AutoDatabaseMountDial settings [50–51](#)

Autodiscover [68](#), [72](#), [123](#), [312](#), [320](#), [322](#), [323](#), [324](#)–[325](#), [330](#), [331](#)

mailbox migration and [334](#)

plan, deploy, and configure [76](#)

testing [337](#)

troubleshooting [116](#)

Autodiscover Site Scope [325](#)

auto-mapping [216](#)

automatic activation [49](#)–[50](#)

lagged copies and [62](#)

automatic failovers [126](#), [127](#)

automatic provisioning [334](#)

automatic redirection [71](#)

automatic site failovers [34](#)

auto reseed [12](#)–[14](#)

Azure

DAG members in [36](#)–[37](#)

hosting witness server on [34](#)–[35](#)

Azure Access Panel. See [Access Panel](#)

Azure Active Directory [298](#)–[299](#)

Azure Active Directory Authentication System [304](#), [306](#), [314](#)–[315](#)

Azure Active Directory Connect (AAD Connect) [298](#), [313](#)

Azure Active Directory Sync (AAD Sync) [298](#)

Azure Cloud Witness [34](#)

Azure Premium Storage [36](#)

Azure Rights Management Services (Azure RMS) [235](#)–[241](#), [306](#)

activated instance of [236](#)

integration of Exchange Server with [236](#)

RMS template creation [237](#)–[238](#)

transport protection rules [238](#)

## B

backend services [67](#)–[68](#), [70](#)

backup solutions [54](#)–[56](#)

Recovery Point Objective (RPO) [54](#)

recovery process and [57](#)

Recovery Time Objective (RTO) [54](#)

snapshot-based [15–16](#)  
types [55–56](#)  
bandwidth [37](#)  
Basic authentication [75, 79, 82, 115](#)  
Best Copy and Server Selection (BCSS) process [48, 48–49](#)  
BitLocker [227–231](#)  
blocked senders [168](#)  
block mode  
    of continuous replication [44](#)  
bound deployment [69](#)  
built-in role groups [219](#)

## C

caching  
    credentials [75](#)  
calendar free/busy sharing [305, 306, 314, 315](#)  
calendar processing [215](#)  
CAPA command [151](#)  
CAS Array [326](#)  
centralized transport [304, 309](#)  
certificate authorities (CAs) [145, 160, 302, 317](#)  
certificate requests [73](#)  
certificates [69, 160](#). See digital certificates; See user certificates  
    configuration [72–74](#)  
    federation [317–318](#)  
    for site failovers [127](#)  
    planning and deploying [71–74](#)  
    self-signed [71–72, 318](#)  
    SSL [76, 79, 302, 317, 320](#)  
    Subject Alternative Name (SAN) [73](#)  
    third-party [72, 73](#)  
    wildcard [73](#)  
change management process [27](#)  
circular logging [21, 48](#)  
CircularLoggingEnabled attribute [21](#)  
Clean Shutdown state [52, 58](#)

## client access

namespaces for [323](#)

troubleshooting [312](#), [337](#)

### Client Access server role [68](#)

#### client access services [67–130](#)

authentication [74–75](#)

Autodiscover [76](#)

certificates [71–74](#)

client connectivity [106–118](#)

components of [67–68](#)

Exchange ActiveSync (EAS) [79–82](#)

Exchange Admin Center (EAC) [79](#)

Exchange Web Services (EWS) [78–79](#)

hierarchical address book (HAB) [84–85](#)

IMAP4 [83](#)

load balancing [95–106](#)

mobility solutions [86–94](#)

Office Online Server (OOS) [83](#)

Offline Address Book (OAB) [84](#)

Outlook Anywhere [76–77](#)

Outlook MAPI over HTTP [77–78](#)

Outlook on the web [79](#)

planning namespaces [68–69](#)

POP3 [82–83](#)

proxy and redirection requirements [69–71](#)

site-resilient [118–127](#)

#### client connectivity [75](#)

authentication [115](#)

Autodiscover [116](#)

Exchange ActiveSync [117](#)

Exchange Web Services (EWS) [110–111](#)

IMAP4 [113–114](#)

Outlook Anywhere connectivity [106–108](#)

Outlook MAPI over HTTP connectivity [108–110](#)

Outlook on the web [112–113](#)

planning namespaces for [68–69](#)

POP3 [113–114](#)  
proxy and redirection issues [118](#)  
troubleshooting [106–118](#)

Client connectors [147](#)  
cloud-based Exchange [1](#)  
cloud computing [36](#)  
cluster administrative access point (CAAP) IP address [28](#)  
Cluster IP Addresses page [99–100](#)  
Cluster Network Object (CNO) [28](#)  
Cluster Parameters page [100](#)  
cluster port rules [101](#)  
coexistence  
    Autodiscover and [324–325](#), [330](#), [331](#)  
    client access troubleshooting in [337](#)  
    Exchange ActiveSync (EAS) and [329](#)  
    Exchange Web Services and [327](#)  
    firewall configurations for [331](#)  
    mailbox migrations and [333–335](#)  
    mail flow and [332–333](#)  
    MAPI over HTTP and [327](#)  
    namespaces for [321–329](#)  
    offline address book (OAB) and [328](#)  
    Outlook Anywhere and [326–327](#)  
    Outlook on the web and [328](#), [330](#)  
    proxy redirect for [329–331](#)  
    split DNS and [323–324](#)  
    transport troubleshooting in [335–337](#)  
with earlier supported versions of Exchange [321–338](#)  
with Office [365](#) [295–314](#)  
    Hybrid configuration [296–308](#)  
collaboration. See also [sharing](#)  
Complete-MigrationBatch cmdlet [341](#)  
compliance [245](#)  
    archiving and [256–268](#)  
    Data Loss Prevention and [245–256](#)  
    eDiscovery and [268–277](#)

Message Records Management and [256–268](#)

solutions [278–286](#)

journaling [283–285](#)

MailTips [278–279](#)

message classification [279–281](#)

transport rules for [282–283](#)

Compliance Management role [219, 288](#)

compliance searches [274–275](#)

conditional routing [310](#)

configuration

ABQ [93–94](#)

Active Directory Domain Services [187–198](#)

administrative auto logging [291](#)

alternate File Share Witness [41–42](#)

archive policies [257–258](#)

authentication [74–75](#)

Autodiscover [76](#)

auto-mapping [216](#)

certificates [72–74](#)

connection filtering [169–171](#)

DAGs [28–29](#)

Azure DAG members [36–37](#)

cross-site [38–40](#)

networks [29–32](#)

Datacenter Activation Coordination (DAC) [40–41](#)

Data Loss Prevention (DLP) [248–252, 253–255](#)

delegated setup [223–224](#)

distribution lists [206–208](#)

DNS [191](#)

domain security [160](#)

Edge Transport [145–146](#)

Exchange ActiveSync (EAS) [79–82](#)

Exchange Admin Center (EAC) [79](#)

Exchange Web Services (EWS) [78–79](#)

File Share Witness (FSW) [32–35](#)

firewalls [331](#)

hierarchical address book (HAB) [84–85](#)  
Hybrid Exchange [296–308](#)  
IMAP4 [83](#)  
Information Rights Management (IRM) [235–236](#)  
in-place archiving [265–266](#)  
journaling [283–285](#)  
linked mailboxes [210](#)  
load balancer [337](#)  
load balancing [95–106](#)  
mailbox audit logging [286–290](#)  
mailbox database copies [35–36](#)  
mailbox databases [17–19](#)  
mailboxes [199–201](#)  
mailbox folder permissions [213–214](#)  
mailbox permissions [214–215](#)  
mailbox servers [49–50](#)  
mail-enabled users/contacts [206](#)  
mail exchange (MX) records [143–144, 176–177](#)  
mail flow [332–333](#)  
MailTips [278–279](#)  
malware filtering [164–166](#)  
Managed Folder Assistant (MFA) [262–264](#)  
moderation [208–209](#)  
namespaces [119–124](#)  
namespaces for coexistence [321–323](#)  
NTLM [74](#)  
Office apps [94](#)  
Office Online Server (OOS) [83](#)  
Offline Address Book (OAB) [84](#)  
online archiving [266–268](#)  
Outlook [76](#)  
Outlook Anywhere [76–77](#)  
Outlook MAPI over HTTP [77–78](#)  
Outlook on the web [79](#)  
Outlook on the web policies [88–91](#)  
OWA for Devices [87–88](#)

POP3 [82–83](#)  
proxy redirects [329–331](#)  
public folder permissions [217](#)  
public folders [210](#)  
recipient filtering [171–172](#)  
resource mailboxes [201–205](#)  
retention policies [257–258](#)  
Safety Net [140–141](#)  
Secure/Multipurpose Internet Mail Extensions (S/MIME) [231–235](#)  
Sender Policy Framework (SPF) [172–173](#)  
send/receive connectors [146–149](#)  
shared mailboxes [205–206](#)  
site-resilient [118–127](#)  
site-resilient namespace URLs [124–125](#)  
site topologies [194–197](#)  
Spam Confidence Level (SCL) thresholds [174–176](#)  
spam filtering [166–168](#)  
throttling policies [197](#)  
transaction log properties [20–21](#)  
transport rules [282–283](#)  
user assignment policies [225–226](#)  
Windows NLB [98–101](#)  
ConfigurationOnly switch [42, 57](#)  
connection filtering [169–171](#)  
connectivity [75](#). See also [client connectivity](#)  
    Exchange Web Services (EWS) [110–111](#)  
    internal vs. external [69](#)  
    Outlook Anywhere connectivity [106–108](#)  
    Outlook MAPI over HTTP connectivity [108–110](#)  
    Outlook on the web [112–113](#)  
connectivity issues [337](#)  
Connect-Mailbox cmdlet [58, 60](#)  
connectors [304, 310](#). See also [receive connectors](#); See also [send connectors](#)  
contacts  
    mail-enabled [206](#)  
content analysis engine [245–246](#)

content indexes [4](#), [46–47](#), [50](#), [271](#)  
contiguous domains [191](#)  
continuous replication [44–45](#)  
Continuous Replication Circular Logging (CRCL) [48](#)  
copy activation  
    troubleshooting [48–51](#)  
copy backup [55](#)  
copy queue length [45](#), [47](#), [48](#)  
corruption [58](#)  
credential caching [75](#)  
cross-forest availability  
    troubleshooting [319–320](#)  
cross-site DAG configuration [38–40](#)  
cumulative updates [297](#), [338](#)  
custom domains [301](#)  
Custom receive connectors [147](#)  
custom routing [309–310](#)  
cutover migrations [296](#)

## D

DAC. See [Datacenter Activation Coordination](#); See [Dynamic Access Control](#); See [Data Access Control \(DAC\)](#)

DAG networks

- configuration of [29–32](#)
- creating [29](#)
- management of [29–32](#)
- multiple [30](#), [31](#)
- site-resilient [121](#)

DAGs. See [Database Availability Groups](#)

DAS. See [Direct-Attached Storage](#)

data

- shared. See shared resources

DatabaseAutoActivationPolicy attribute [26](#)

Database Availability Groups (DAGs) [6](#), [8](#), [138](#)

- about [22–23](#)

- across multiple datacenters [38–43](#)

Active-Active DAG [40](#)  
Active-Passive DAG [39–40](#)  
adding members to [29](#)  
adding new database copy to [35–36](#)  
autoconfiguration of [31](#)  
auto reseed feature and [12–14](#)  
circular logging in [21](#)  
configuration of [28–29](#)  
    cross-site [38–40](#)  
creating [28–29](#)  
for high availability [22–37](#)  
    creating and configuring copies [35–36](#)  
    File Share Witness [32–35](#)  
    identifying failure domains [23–24](#)  
    SLA requirements and scheduled downtime [24](#)  
    software updates and server maintenance planning [25–28](#)  
in Microsoft Azure [36–37](#)  
IP subnets [40](#)  
management of [28–29](#)  
namespaces and [323](#)  
naming [32](#)  
network interfaces [31–32, 40](#)  
public folders and [1](#)  
quorum issues [53–54](#)  
quorum modes [22](#)  
recovery process [16, 57–58](#)  
resiliency of [31](#)  
risk management and [27](#)  
site-resilient [38–43](#)  
    alternater FSW [41–42](#)  
    Datacenter Activation Coordination (DAC) [40–41](#)  
    site recovery [42–43](#)  
DatabaseCopyActivationDisabledAndMoveNow attribute [26](#)  
DatabaseCopyAutoActivationPolicy [49](#)  
database files [4–5, 10, 12](#)  
    placement of [19](#)

Database parameter [200](#)  
databases. See [mailbox databases](#)  
Datacenter Activation Coordination (DAC) Mode [40–41](#)  
Datacenter Activation Coordination Protocol (DACP) [41–42](#)  
datacenters  
    IP subnets in [38](#)  
    secondary [40, 42, 42–43](#)  
    switchovers [42, 42–43](#)  
    using multiple [38–43](#)  
data deduplication [9](#)  
data drives  
    BitLocker and [227](#)  
data loss [54](#)  
    in hard recovery [52](#)  
    protecting against [4–5, 10](#)  
    risk of [247](#)  
Data Loss Prevention (DLP) [245–256, 282](#)  
    custom policies [254–255](#)  
    custom rules [252–253](#)  
    fingerprinting [253–254](#)  
    policy templates [248–250](#)  
    Policy Tips [247–248](#)  
    pre-built rules [248–252](#)  
    solution to meet business requirements [247–248](#)  
    testing [247](#)  
data retention [256–268](#)  
data storage. See also [storage architectures](#); See also [storage requirements](#)  
    capacity and placement [4–5](#)  
failure  
    auto reseed feature and [12–14](#)  
public folders [1](#)  
quotas [8](#)  
size requirements [2–3](#)  
storage architectures [9–10](#)  
testing [16–17](#)  
unsupported [9](#)

virtual machines [15](#)  
DCP. See [Data Collection Package](#)  
dedicated namespaces [69](#), [121](#), [122](#), [123](#)  
dedicated replication networks [30](#)  
Default MRM Policy [258](#), [266](#)  
default policy tags [257](#), [259–260](#), [260](#), [263](#)  
DefaultPublicFolderMailbox property [8](#)  
Default Role Assignment Policy [225–226](#), [262](#)  
DelayNotificationTimeOut parameter [177](#)  
Delegated Setup role [219](#), [223–224](#)  
delegates  
    room mailbox [215](#)  
delegation tokens [315](#)  
deleted mail items  
    recovery of [59–60](#)  
DeleteExistingFiles parameter [48](#)  
deployment  
    ABQ [93–94](#)  
    Autodiscover [76](#)  
    bound [69](#)  
    certificates [71–74](#)  
    Exchange ActiveSync (EAS) [79–82](#)  
    Exchange Admin Center (EAC) [79](#)  
    Exchange Web Services (EWS) [78–79](#)  
    hierarchical address book (HAB) [84–85](#)  
    IMAP4 [83](#)  
    incremental [22](#)  
    mailbox databases [2](#), [3](#)  
    Office apps [94](#)  
    Office Online Server (OOS) [83](#)  
    Offline Address Book (OAB) [84](#)  
    Outlook Anywhere [76–77](#)  
    Outlook MAPI over HTTP [77–78](#)  
    Outlook on the web [79](#)  
    OWA for Devices [87–88](#)  
    POP3 [82–83](#)

unbound [68](#)  
deprecated features [344](#)  
Details Template Editor [157](#)  
device access rules [93–94](#)  
DFS. See [Distributed File Share](#); See [Distributed File System \(DFS\)](#)  
dial tone restore [61–62](#)  
differential backup [55](#)  
Digest authentication [75, 79](#)  
digital signatures [231–232](#)  
Direct-Attached Storage (DAS) [9](#)  
directory synchronization [301–302](#)  
    troubleshooting [313](#)  
directory synchronization tools [298, 313](#)  
DirSync [298](#)  
Dirty Shutdown state [51–52, 58](#)  
disaster recovery  
    for virtual machines [15](#)  
discontinued features  
    planning for [344](#)  
discovery mailboxes [272](#)  
Discovery Management role [219, 269, 270, 272, 277](#)  
disjoint namespaces [191](#)  
disk failure [4–5](#)  
    auto reseed feature and [12–14](#)  
disk space [159](#)  
Distributed File Share (DFS) [32](#)  
distribution groups [311](#)  
distribution groups/lists [203](#)  
    creating and configuring [206–208](#)  
    in-place holds [276](#)  
    moderation of [208–209](#)  
DLP. See [Data Loss Prevention \(DLP\)](#)  
DNS records [307–308](#)  
document collaboration [123](#)  
documents. See also [files](#)  
domain controllers [188–190, 331](#)

as File Share Witness servers [33](#)  
read-only [188](#)  
read-write [188](#)  
same-site [188](#)

domain names  
federation trusts [315](#)  
for Hybrid configuration [303](#)  
for Office [365](#) tenant [301](#)  
validating ownership of [303–304](#)

domain name service (DNS)  
changes for Exchange [191](#)

Domain Name System (DNS)  
split [69, 125](#)

domain proof records [318](#)  
domains

preparing for Exchange [194](#)

Domain Secure [161](#)

DomainSecureEnabled parameter [161](#)

domain security  
configuration [160](#)

downtime [22](#)

scheduled [24](#)

DRA. See [Data Recovery Agent \(DRA\)](#)

drive letters [11](#)

dynamic disks [10](#)

dynamic memory [36](#)  
virtual machines and [15](#)

Dynamic Quorum [53](#)

## E

E:\DB01 folder [28](#)

EdgeSync [146](#)

Edge Transport [131, 145–146, 162](#)  
troubleshooting [162–163](#)

EdgeTransport.exe.config file [178](#)

Edge Transport servers [139, 302, 331](#)

## eDiscovery [240](#), [268–277](#)

duplicate messages and [273](#)

export tool [273](#)

in-place federated search [277](#)

legal/litigation holds [276](#)

multi-mailbox searches [270–276](#)

query-based in-place holds [275–276](#)

RBAC roles for [269](#)

search queries [270–271](#)

SharePoint [277](#)

using PowerShell [273–275](#)

## eDiscovery Center [277](#)

EFS. See [Encrypting File System](#); See [Encrypting File System \(EFS\)](#)

## email

Outlook app for accessing [87–88](#)

email attachments [79](#), [83](#)

### email delivery

attachment filtering [167](#)

centralized [304](#)

coexistence and [332–333](#)

connection filtering [169–171](#)

custom routing [309–310](#)

Edge Transport [145–146](#)

inter-org mail flow [135–138](#)

inter-site mail flow [132–135](#)

intra-site mail flow

redundancy for [138–140](#)

mail exchange (MX) records [143–144](#)

### message hygiene

connection filtering [169–171](#)

malware filtering [164–166](#)

recipient filtering [171–172](#)

spam filtering [166–168](#)

message sizes [310–311](#)

message tracing [311](#)

recipient filtering [171–172](#)

recipient restrictions [310–311](#)  
resubmission and reroute queues [177–179](#)  
Safety Net [140–141](#)  
Sender Policy Framework (SPF) [172–173](#)  
send/receive connectors [146–149](#)  
shadow redundancy [141–143](#)  
SLA requirements for [132](#)  
transport layer security (TLS) [144–145](#), [160–161](#)  
troubleshooting [161–163](#), [307–311](#)  
    failure scenarios [159–160](#)  
    SMTP mail flow [156–159](#)  
email delivery reports [154](#)  
email messages  
    de-duplication of [272](#)  
    digitally signed messages [231–232](#)  
    encrypted messages [232](#)  
    IRM-protected [235–241](#)  
    journaling [239](#), [283–285](#)  
    MailTips [278–279](#)  
    message classification [279–281](#)  
    Policy Tips in [246–248](#)  
    sensitive information in [246](#), [250](#)  
    S/MIME-protected [231–235](#)  
email routing [37](#)  
Enable-Mailbox cmdlet [262](#), [266](#)  
Encrypting File System (EFS) [10](#)  
encryption [232](#), [239](#)  
    reversible [75](#)  
EncryptUsedSpaceOnly parameter [229](#)  
Enterprise Admins group [193](#)  
enterprise edition license [18](#)  
equipment mailboxes [205](#)  
error pages  
    redirection [71](#)  
ESEUtil tool [52](#), [63](#)  
ESRA. See [EdgeSync replication account \(ESRA\)](#)

event logs [51](#)  
Exchange ActiveSync (EAS) [68](#), [79–82](#), [329](#)  
    device access control [79–80](#)  
    passwords [81–82](#)  
    troubleshooting [117–118](#)  
Exchange admin center [302–303](#)  
Exchange admin center (EAC)  
    configuring moderation in [209](#)  
    managing DLP policies in [250](#)  
    multi-mailbox searches in [270–276](#)  
    roles [220](#)  
Exchange Admin Center (EAC) [68](#), [79](#), [136](#)  
Exchange Administration Center [59](#)  
Exchange Control Panel [328](#)  
Exchange costs [161](#)  
Exchange eDiscovery [277](#)  
Exchange federation [314–320](#)  
    certificate requirements for [317–318](#)  
    cross-forest availability [319–320](#)  
    federation trusts [314–315](#)  
    firewall requirements for [317–318](#)  
    organization relationships [316–317](#), [318–319](#)  
    sharing policies [315–316](#)  
    troubleshooting [318–319](#)  
Exchange Management Shell [333](#)  
Exchange Management Shell (EMS) [199](#)  
    multi-mailbox searches in [270–276](#)  
Exchange Online [1](#), [61](#), [295–314](#)  
    about [295–296](#)  
    client access [312](#)  
    hybrid configuration [296–308](#)  
    licensing [301](#)  
    message sizes [310–311](#)  
    message tracing [311](#)  
    migration from on-premises Exchange [296](#)  
    recipient restrictions [310–311](#)

troubleshooting transport with [307–311](#)

Exchange Online Protection (EOP) [297](#), [302](#), [308](#)

Exchange Server

- Active Directory (AD) Domain Service for [187–198](#)
  - DNS changes [191](#)
  - Global Catalog placement [190](#)
  - number of domain controllers [188–190](#)
  - preparation [192–198](#)
  - site topology [194–197](#)
  - throttling policies [197](#)
- BitLocker on [227–231](#)
- delegated setup [223–224](#)
- preparing domains for [194](#)

Exchange Server 2007 [329](#)

Exchange Server 2010 [1](#), [119](#), [297](#), [322](#), [329](#), [342](#)

Exchange Server 2010 Service Pack [3](#) [338](#)

Exchange Server 2013 [1](#), [119](#), [297](#), [321](#), [338](#)

Exchange Server 2016

- AD DS schema for [192](#)
- architecture [1](#), [24](#), [61](#)
- clean removal of [57](#)
- coexistence
  - with earlier supported versions of Exchange [321–338](#)
- cumulative updates [297](#)
- discontinued features in [344](#)
- hosting in Azure [36–37](#)
- license editions [18–19](#)
- mailbox server role [1](#)
- migration from earlier versions to [338–346](#)
- namespaces [119–124](#)
- pre-defined scripts [114](#)
- proxying [70](#)
- recovery of [56–57](#)
- redirection in [70–71](#)
- retention policies [256](#)
- schema requirements for [192–193](#)

server size calculator [3–4](#), [14](#), [16](#), [36](#)  
setup wizard [192](#)  
site-aware decisions by [38](#)  
site-resilient configuration [118–127](#)  
transport services [131–186](#)  
virtualization [14–16](#)  
Exchange Server Role Requirements Calculator [3–4](#), [14](#), [16](#), [36](#), [51](#)  
Exchange Server services  
    namespaces for [68–69](#)  
Exchange Toolbox [157](#)  
Exchange Trusted Subsystem [222](#)  
Exchange Trusted Subsystem group [33](#)  
Exchange Web Services [320](#), [327](#)  
Exchange Web Services (EWS) [68](#), [78–79](#)  
    troubleshooting [110–111](#)  
Exchange Web Services Managed API [277](#)  
Export-AutodiscoverConfig cmdlet [320](#)  
Export-OutlookClassification.ps1 [281](#)  
Export-RetentionTags.ps1 [267](#)  
external clients  
    Autodiscover and [76](#)

## F

FailedAndSuspended status [13](#)  
failover clusters [22](#), [25](#), [98](#)  
failovers [23](#), [181–183](#)  
    automatic [34](#), [126](#), [127](#)  
    certificate requirements for [127](#)  
    client behavior during [127](#)  
failover scenarios  
    MX records for [176](#)  
failure domains [23–24](#)  
federated identity model [299–301](#)  
Federated search API. [277](#)  
federation trusts [303](#), [305](#), [314–320](#)  
    certificate requirements for [317–318](#)

cross-forest availability [319–320](#)  
domain names [315](#)  
firewall requirements for [317–318](#)  
Microsoft Federation Gateway [314–315](#)  
organization relationships [316–317](#)  
sharing policies [315–316](#)  
troubleshooting [318–319](#)

file mode  
of continuous replication [44](#)

files  
co-locating, on same volume [12](#)  
content index [4](#)  
database [4–5, 10, 12, 19](#)  
shared. See shared resources  
transaction log [4–5, 12, 19, 44, 50, 51, 61](#)  
    accumulation of [48](#)  
    configuration of [20–21](#)

File Share Witness (FSW) [29, 39](#)  
    configuration of [32–35](#)  
    creating [32–35](#)  
    location of [33–34](#)  
    management of [32–35](#)  
    placement of alternate [41–42](#)  
    quorum voting and [32](#)  
    using domain controllers as [33](#)

file systems  
    requirements for [10–11](#)  
fingerprinting, DLP [253–254](#)  
firewalls [162, 310](#)  
    Exchange servers and [331](#)  
    for federation [317–318](#)  
    IMAP4 settings and [83](#)  
    MAPI over HTTP and [78](#)  
    POP3 settings and [82](#)

Force switch [57](#)  
Forefront Identity Manager (FIM) [319](#)

forest trusts [339](#)  
forms-based authentication [328](#)  
forms-based authentication (FBA) [74–75](#), [79](#), [115](#)  
Frontend Transport role [147](#)  
Front End Transport service [162](#)  
FSW. See [File Share Witness](#)  
full backup [55](#)  
fully qualified domain names (FQDNs) [68](#), [69](#), [76](#)  
    certificates for [72–73](#)  
    Outlook Anywhere and [77](#)

## G

Get-AutodiscoverVirtualDirectory cmdlet [325](#)  
Get-CASMailbox cmdlet [312](#)  
Get-ClientAccessServer cmdlet [324](#)  
Get-ComplianceSearch cmdlet [274](#)  
Get-Credential cmdlet [114](#)  
Get-DatabaseAvailabilityGroup cmdlet [29](#)  
Get-DatabaseAvailabilityGroupNetwork cmdlet [31](#), [40](#)  
Get-Disk cmdlet [11](#)  
Get-DlpPolicyTemplate cmdlet [248](#)  
Get-EdgeSubscription command [162](#)  
Get-FederatedDomainProof cmdlet [315](#), [318](#)  
Get-FederationInformation cmdlet [319](#)  
Get-HybridConfiguration cmdlet [304](#)  
Get-Mailbox cmdlet [286](#)  
Get-MailboxDatabase cmdlet [52](#)  
Get-MailboxDatabaseCopyStatus cmdlet [45](#), [46](#), [47](#), [63](#)  
Get-MailboxSearch cmdlet [274](#)  
Get-MailboxServer cmdlet [26](#)  
Get-MailboxStatistic cmdlet [58](#)  
Get-ManagementRoleAssignment cmdlet [225](#)  
Get-ManagementRole cmdlet [225](#)  
Get-ManagementRoleEntry cmdlet [225](#)  
Get-ManagementScope cmdlet [225](#)  
Get-MessageTrackingLog cmdlet [152](#), [336](#)

Get-MigrationBatch cmdlet [343](#)  
Get-MigrationUser cmdlet [341](#)  
Get-MigrationUserStatistics cmdlet [343](#)  
Get-MobileDevice cmdlet [93](#)  
Get-MoveRequestStatistics cmdlet [339](#), [343](#)  
Get-OrganizationConfig cmdlet [7](#), [278](#)  
Get-OutboundConnector cmdlet [309](#)  
Get-OutlookAnywhere cmdlet [326](#)  
Get-Queue cmdlet [156](#)  
Get-QueueDigest cmdlet [156](#), [156–157](#)  
Get-ReceiveConnector cmdlet [147](#)  
Get-RoleAssignmentPolicy cmdlet [225](#)  
Get-RoleGroup cmdlet [225](#)  
Get-RoleGroupMember cmdlet [225](#)  
Get-ServerHealth cmdlet [112](#)  
Get-TransportConfig cmdlet [160](#)  
Global Address List [84](#)  
Global Address List (GAL) [297](#), [313](#), [319](#), [328](#)  
Global Catalog processor cores [188](#), [190](#)  
Global Catalog servers [188](#)  
Global Catalog services [190](#)  
GlobalThrottlingPolicy [197](#)  
group membership [193](#)  
Group Policy [230](#), [281](#)  
groups  
    distribution [206–208](#)  
GUID partition table (GPT) [10](#)

## H

hard recovery [52](#)  
hardware resources  
    sharing, by virtual machines [14](#)  
hashed passwords [75](#)  
healthcheck.htm page [97](#)  
health monitoring  
    load balancing with [97](#)

HELO/EHLO analysis [168](#)  
Help Desk role [219](#), [220](#)  
hierarchical address book (HAB) [84](#)–[85](#)  
high availability [1](#)  
    for mailbox databases [22](#)–[37](#)  
        creating and configuring copies [35](#)–[36](#)  
        File Share Witness [32](#)–[35](#)  
        identify failure domains [23](#)–[24](#)  
        SLA requirements and scheduled downtime [24](#)  
        software updates and server maintenance planning [25](#)–[28](#)  
    SLAs for [24](#)  
    virtualization and [15](#)  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ExchangeServer\V15\IRM\CertificationServer-Redirection key [241](#)  
hostnames [310](#), [321](#)  
    Outlook Anywhere [326](#)  
HTTP  
    redirection [71](#)  
HTTPS [317](#), [320](#), [331](#)  
    redirection [71](#)  
hub and spoke topology [195](#)–[196](#)  
hub sites [161](#), [194](#)  
Hub Transport role [147](#)  
HubTransport server component [25](#)  
Hybrid configuration [266](#), [267](#)  
Hybrid Configuration Wizard  
    limitations of [305](#)–[306](#)  
    running [302](#)–[305](#)  
Hybrid Exchange configuration [296](#)–[308](#)  
    client access in [312](#)  
    Hybrid Configuration Wizard [302](#)–[306](#)  
    identity management and [298](#)–[301](#)  
    limitations of [305](#)–[306](#)  
    network ports for [310](#)  
    OAuth-based authentication [306](#)–[307](#)  
    on-premises environment for [302](#)

plan, deploy, and manage [296–298](#)  
preparation of Office [365](#) tenant for [301–302](#)  
sign-on experience [296](#)  
troubleshooting [307–311](#)  
Hybrid licenses [297](#)  
hybrid servers [298](#)  
hygiene. See [message hygiene](#)  
Hygiene Management role [166](#), [219](#)  
hypervisors [15](#)  
Hyper-V Live Migration [15](#)

## I

Identity Lifecycle Manager (ILM) [319](#)  
identity management [319](#)  
    Hybrid configuration and [298–301](#)  
IDFix tool [313](#)  
IIS custom error page [71](#)  
IIS logs [345](#)  
IIS Manager [112](#)  
image templates. See [template images](#)  
IMAP4 [68](#)  
    configuration [83](#)  
    troubleshooting [113–114](#)  
IMAP4 protocol logs [150–152](#)  
IMAP migration [296](#)  
IMAP protocol [331](#)  
Import-RetentionTags.ps1 [267](#)  
inbound connectors [304](#)  
IncludeFolders parameter [59](#)  
incremental backup [55](#)  
incremental deployment [22](#)  
Information Rights Management (IRM) [235–241](#), [306](#)  
    for eDiscovery [240](#)  
    journal report decryption [239](#)  
    message classifications and [281](#)  
    Outlook protection rules [238–239](#)

planning and configuring [235–236](#)  
prelicensing for client access [240](#)  
RMS template creation [237–238](#)  
transport protection rules [238](#)  
troubleshooting [240–241](#)

Information Store [19](#)  
    restarting, for new databases [18](#)

infrastructure-as-a-service (IaaS) approach [36](#)

inheritance [217](#)  
    of retention tags [263](#)

InheritanceType parameter [205](#)

in-place archiving [265–266](#)

In-Place eDiscovery & Hold console [59](#)

In-Place Hold [256](#)

in-place holds [275–276](#)

input/output per second (IOPS) [1](#)

Install-AntiSpamAgents.ps1 [166](#)

Install-WindowsFeature [335](#)

integrated authentication [74](#)

Integrated Windows authentication [79, 82, 115](#)

Internal connectors [147](#)

internal distribution groups [171](#)

Internet connectors [147](#)

Internet for Domain Secure [160–161](#)

Internet Group Management Protocols (IGMPs) [100](#)

Internet Information Services (IIS) [74](#)  
    resetting [113](#)

inter-org mail flow [135–138](#)  
    troubleshooting [161–162](#)

inter-site mail flow [132–135](#)

Intra-Organization Connectors (IOC) [307](#)

intra-site mail flow  
    redundancy for [138–140](#)

Intune. See [Microsoft Intune](#)

Invoke-MonitoringProbe cmdlet [88–89](#)

IP address

associated with FQDN [69](#)  
blocking [169–171](#)  
Exchange Online [310](#)  
for cluster communications [99–100](#)  
for DAG [28](#)  
IP Allow list [169–171](#)  
IP Block list [160, 169–171](#)  
IP-less clusters [28](#)  
IP subnets [40](#)  
iSCSI connected storage [9](#)  
IsExcludedFromServingHierarchy parameter [7](#)  
IsHierarchyReady attribute [7](#)

## J

Jetstress [16–17](#)  
journaling [283–285](#)  
JournalingEnabled attribute [46](#)  
journaling mailboxes [46](#)  
JournalingReportNdrTo property [284](#)  
journal recipients [284](#)  
journal report decryption [239](#)  
journal reports [283](#)  
junk email folder [282](#)  
Junk Email folder threshold [175–176](#)  
“just a bunch of disks” (JBOD) [10, 12](#)

## K

Kerberos authentication [74, 75, 115](#)

## L

lagged mailbox database copies [49, 61–64](#)  
latency [37, 38, 121](#)  
layer 4 load balancing [101–102](#)  
layer 7 load balancing [102–105](#)  
least-connection load balancing [96](#)  
legacy servers

IIS logs on [345](#)  
uninstalling [344–345](#)

legal hold. See [litigation hold](#)

Legal Hold [276](#)

Legal Hold role [269](#)

legal/litigation holds [276](#)

licensed editions [18–19](#)

licenses

- Hybrid [297](#)
- linked mailboxes [210](#)

Litigation Hold [256, 276](#)

LitigationHoldDate parameter [276](#)

load balancer

- configuration of [337](#)
- load balancing [27, 36, 95–106, 177, 301](#)
  - configuring namespace [95–101](#)
  - layer 4 vs. layer 7 [101–105](#)
  - MAPI over HTTP and [78](#)
  - methods [96](#)
  - single namespace [121–122](#)
  - SIP [97–98](#)
  - Windows Network Load Balancing (Windows NLB) [98–101](#)
    - with health monitoring [97](#)

local area networks (LANs) [69](#)

location-based namespaces [125–126](#)

log buffer [44](#)

log files. See [transaction log files](#)

Log Level setting [291](#)

logon attempts

- failed [81](#)

LogonTypes parameter [288](#)

logs

- message tracking [150, 152–154](#)
- protocol [155](#)
- SMTP [155](#)

log stream [20–21](#)

log truncation [20–21](#)

Lync Online. See Skype for Business

## M

mailbox audit logging [286–290](#)

- audit log storage [287](#)

- configuration [287–288](#)

- searching audit logs [288–290](#)

mailbox data

- retention of [256–268](#)

mailbox database copies

- activating [23](#)

- prevention of [26](#)

- activation

- troubleshooting [48–51](#)

Activation Preference (AP) number [35–36](#)

active [23, 36](#)

- creating and configuring [35–36](#)

- lagged [49, 61–64](#)

- passive [23](#)

- reseeding [48–49](#)

- status of [46–47](#)

- suspended [48–49](#)

mailbox databases [1–66](#)

- activation policies [49–51](#)

- backup solutions [54–56](#)

- configuration [17–19](#)

- transaction log properties [20–21](#)

- continuous replication of [44–45](#)

- creating [17–19](#)

- deployment of [2, 3](#)

- dial tone [61–62](#)

- failovers [23](#)

- functions of [1](#)

- hard recovery of [52](#)

- high availability [22–37](#)

hosting public folders in [1](#)  
layout approach for [11](#)  
management of [19–20](#)  
maximum number of [18–19](#), [49](#)  
monitoring [44–47](#)  
mounting [19](#)  
mount points for volumes [11](#), [13](#)  
moving [20](#)  
naming [20](#)  
placement of multiple [5](#)  
planning for [2–17](#)  
    archive mailboxes [5–6](#)  
    auto reseed [12–14](#)  
    capacity and placement [4–5](#)  
    file system requirements [10–11](#)  
    public folder capacity and placement [6–9](#)  
    size [2–3](#)  
    storage architecture [9–10](#)  
    storage requirements [2–3](#)  
    virtualization [14–16](#)  
recovery solutions [56–65](#), [58–59](#)  
renaming [20](#)  
restarting Information Store for [18](#)  
site-resilient DAGs [38–43](#)  
soft recovery of [52](#), [63](#)  
storage design  
    Jetstress [16–17](#)  
switchovers [22–23](#)  
troubleshooting  
    copy activation [48–51](#)  
    database failures [51–52](#)  
    performance [51](#)  
    quorum issues [53–54](#)  
    replication and replay [47–48](#)  
unmountable [52](#)  
use of multiple [12](#)

## mailboxes

arbitration [291, 339](#)  
archive [5–6, 265–266, 267–268](#)  
assigning policies to [89–90, 91](#)  
assigning retention policies to [262](#)  
auto-mapping [216](#)  
backing up [335](#)  
client access issues [312](#)  
configuration [199–201](#)  
creating [199–201](#)  
cross-premises access [297](#)  
discovery [272](#)  
distribution lists [203, 206–208](#)  
equipment [205](#)  
Exchange Online [312](#)  
excluding from autoprovisioning [334](#)  
internal [172](#)  
journal [283–285](#)  
journaling [46](#)  
linked [210](#)  
migration of [333–335, 339–341](#)  
mobile device access to [87–88](#)  
multi-mailbox searches [270–276](#)  
on-premises [312](#)  
Outlook on the web policies for [88–91](#)  
permissions [214–215](#)  
primary [5–6](#)  
protocol configuration [312](#)  
public folder [6–9, 60–61, 210–211](#)  
recovery of [58–59](#)  
resource [201–205](#)  
retention hold of [264](#)  
retention tags and [262–264](#)  
room [201–205, 215](#)  
shared [205–206](#)  
Mailbox Features page [90–91](#)

mailbox folder permissions [213–214](#)  
mailbox folder roles [213–214](#)  
Mailbox Replication Service (MRS) [333–334](#)  
    troubleshooting [343–344](#)  
Mailbox Replication Service Proxy (MRS Proxy) [303](#)  
Mailbox Search role [269](#)  
MailboxServer parameter [42](#)  
mailbox server role [1](#), [68](#), [70](#)  
Mailbox Server role [131](#)  
mailbox servers  
    configuration of [49–50](#)  
    multiple, for redundancy [138–140](#)  
Mailbox Transport Delivery service [137–138](#), [139](#)  
Mailbox Transport Submission service [136–138](#)  
mail-enabled contacts [206](#)  
mail-enabled objects [198–211](#)  
    permissions for [212–218](#)  
mail-enabled users [206](#)  
mail exchange (MX) records [148](#)  
    about [143](#)  
    for failover scenarios [176–177](#)  
    plan and configure [143–144](#)  
mail exchanger (MX) records [308](#), [332](#)  
mail flow. See also [email delivery](#); See also [message delivery](#)  
    coexistence and [332–333](#)  
    troubleshooting, in coexistence [335–337](#)  
mail items  
    recovery of [59–60](#)  
Mail Recipient Creation role [221](#), [222](#)  
MailTips [207](#), [278–279](#)  
maintenance  
    high availability and [25–28](#)  
maintenance mode [25–28](#)  
malware filtering [164–166](#)  
Managed Availability [1](#), [12](#), [44–47](#)  
Managed Availability feature [97](#), [103](#)

Managed Folder Assistant [6](#)  
Managed Folder Assistant (MFA) [262–264](#)  
MAPI network interface [31, 40](#)  
MAPI networks [121](#)  
MAPI over HTTP [77, 77–78, 327](#)  
master boot record (MBR) [10](#)  
MaxIdleTimeBeforeResubmit parameter [178](#)  
MaximumActiveDatabases parameter [49](#)  
memory  
    dynamic [15](#)  
mesh topology [196](#)  
message classification [279–281](#)  
message delivery. See also [email delivery](#)  
    coexistence and [332–333](#)  
    components [132](#)  
    inter-org mail flow [135–138](#)  
    intra-site mail flow [138–140](#)  
    mail exchange (MX) records [143–144](#)  
    resubmission and reroute queues [177–179](#)  
    Safety Net [140–141](#)  
    send/receive connectors [146–149](#)  
    shadow redundancy [141–143](#)  
    SLA requirements for [132](#)  
    transport layer security (TLS) [144–145, 160–161](#)  
    troubleshooting [161–163](#)  
        failure scenarios [159–160](#)  
        SMTP mail flow [156–159](#)  
MessageExpirationTimeOut parameter [178](#)  
message hygiene [163, 164–175](#)  
    connection filtering [169–171](#)  
    malware filtering [164–166](#)  
    recipient filtering [171–172](#)  
Sender Policy Framework (SPF) [172–173](#)  
Spam Confidence Level (SCL) thresholds [174–176](#)  
spam filtering [166–168](#)  
Message Records Management (MRM) [256–268](#)

custom retention tags [259–261](#)  
retention policies [257–258](#)  
    assigning to users [262](#)  
    Managed Folder Assistant (MFA) [262–264](#)  
    removal of tags from [264–265](#)  
message retries [177–178](#)  
message tracing [311](#)  
MessageTrackingLogMaxAge parameter [152](#)  
MessageTrackingLogPath parameter [152](#)  
message tracking logs [150, 152–154, 336](#)  
message transport. See [transport](#)  
mh switch [52](#)  
Microsoft Azure. See [Azure](#)  
Microsoft Azure Active Directory. See [Azure Active Directory \(Azure AD\)](#)  
Microsoft Exchange logs [112](#)  
Microsoft Federation Gateway [304, 314–315, 318, 319](#)  
Microsoft Identity Manager (MIM) [319](#)  
Microsoft Management Console (MMC) [157](#)  
Microsoft Remove Connectivity Analyzer [337](#)  
Microsoft Rights Management connector [236](#)  
Microsoft Support and Recovery Assistant [109–110, 116](#)  
migration  
    cutover [296](#)  
    decommissioned servers and [344–345](#)  
    discontinued features and [344](#)  
    from on-premises Exchange to Exchange Online [296](#)  
    mailboxes [333–335, 339–341](#)  
    to Exchange 2016 [338–346](#)  
    to modern public folders [341–343](#)  
    transition paths for [339](#)  
    troubleshooting [343–344](#)  
MIME filtering [167](#)  
mobile devices  
    access policies [79–80, 93–94](#)  
    mailbox policy [81–82](#)  
    passwords for [81–82](#)

quarantined [80](#), [93–94](#)  
remotely wiping [81](#)  
security policies for [80–82](#), [91–92](#)  
sign-in on idle [81](#)  
S/MIME and [234](#)  
use of [86–94](#)  
wiping, after failed logon attempts [81](#)

mobility solutions [86–94](#)  
mobile device policies [91–92](#)  
Office apps [94](#)  
Outlook on the web policies [88–91](#)  
OWA for Devices [87–88](#)

moderation [208–209](#)

modern public folders [1](#)

monitoring  
client connectivity [106–118](#)  
health [97](#)  
mailbox databases [44–47](#)  
transport services [150–155](#)

MountAtStartup attribute [19](#)

Mount-Database cmdlet [52](#), [58](#)

mounted databases  
defined [19–20](#)

mount points [11](#), [13](#)

Move-ActiveDatabaseCopy cmdlet [50](#)

Move-ActiveMailboxDatabase cmdlet [43](#), [63](#)

Move-DatabasePath cmdlet [19](#)

Move-PublicFolderBranch.ps1 script [8](#)

MRM. See [Messaging Records Management](#)

MSExchange Secure Mail Transport [161](#)

multi-forest scenarios [305](#)

multi-mailbox searches [270–276](#)

multi-master replication [6](#)

mutual authentication [144–145](#)

mxExchDelegateListLink attribute [216](#)

MyRetentionPolicies management role [262](#)

# N

## namespaces

- Autodiscover [324–325](#)
  - contiguous [191](#)
  - dedicated [69, 121, 122, 123](#)
  - disjoint [191](#)
  - Exchaneg Web Services [327](#)
  - Exchange ActiveSync [329](#)
  - Exchange Control Panel [328](#)
  - for coexistence [321–329](#)
  - internal and external [125](#)
  - load balancing configuration for [95–101](#)
  - location-based [125–126](#)
  - MAPI over HTTP [327](#)
  - multiple, without session affinity [104–105](#)
  - noncontiguous [191](#)
  - OAB [328](#)
  - Outlook Anywhere [326](#)
  - Outlook on the web [328](#)
  - planning, for client connectivity [68–69](#)
  - regional [323](#)
  - required [119](#)
  - shared
    - troubleshooting [155–156](#)
  - single [155](#)
  - single-label [191](#)
  - single site-resilient [121](#)
  - site-resilient [119–124](#)
  - split DNS [323–324](#)
  - switchover to Exchange 2016 [329](#)
  - unified [68](#)
  - using layer [4](#) load balancing [101–102](#)
  - using layer [7](#) load balancing [102–105](#)
- namespace URLs
- site-resilient [124–125](#)
- NAT. See [network address translation \(NAT\)](#)

Native Data Protection [61](#)

Network-Attached Storage (NAS) [9](#)

network connectivity [37](#)

network file system (NFS) storage [9](#)

network interfaces [31](#), [32](#), [40](#)

disabling [32](#)

network latency [37](#), [38](#)

networks

DAG [29–32](#)

dedicated replication [30](#)

local area [69](#)

MAPI [121](#)

replication [31](#)

wide area [30](#), [39–40](#)

New-ActiveSyncDeviceAccessRule cmdlet [93](#)

New-AdminAuditLogSearch cmdlet [293](#)

New-ComplianceSearchAction cmdlet [275](#)

New-ComplianceSearch cmdlet [274](#)

New-DatabaseAvailabilityGroup cmdlet [28](#), [33](#)

New-DlpPolicy cmdlet [250](#)

New-JournalRule cmdlet [283](#)

New-MailboxAuditLogSearch cmdlet [290](#)

New-Mailbox cmdlet [7](#), [201](#), [262](#), [266](#), [272](#)

New-MailboxDatabase cmdlet [18](#), [58](#)

New-MailboxRestoreRequest cmdlet [58](#)

New-MailboxSearch cmdlet [59](#), [273](#), [274](#)

New-MalwareFilterPolicy cmdlet [165](#)

New-MalwarePolicyRule cmdlet [166](#)

New-MessageClassification cmdlet [280](#)

New-MigrationBatch cmdlet [341](#)

New-MobileDeviceMailboxPolicy cmdlet [92](#)

New-MoveRequest cmdlet [339](#)

New-OrganizationRelationship cmdlet [316](#)

New-OutboundConnector cmdlet [309](#), [310](#)

New-OutlookProtectionRule cmdlet [239](#)

New-PublicFolderMoveRequest cmdlet [8](#)

New-ReceiveConnector cmdlet [147](#), [333](#)  
New-RetentionPolicy cmdlet [258](#)  
New-RetentionPolicyTag cmdlet [259](#)  
new-TestCasConnectivityUser.ps1 [114](#)  
New-TransportRule cmdlet [282](#)  
NICs. See [network interface cards \(NICs\)](#)  
Node and File Share Majority quorum mode [22](#)  
Node Majority quorum mode [22](#)  
noncontiguous domains [191](#)  
non-delivery report (NDR) [311](#)  
NTFS file system (NTFS) [10](#)  
NTLM [74](#), [75](#)

## O

OAuth-based authentication [306](#)–[307](#)  
object permissions  
    mail-enabled [212](#)–[217](#)  
Office 365 [1](#)  
    coexistence with [295](#)–[314](#)  
    Hybrid configuration [296](#)–[308](#)  
    IP addresses [310](#)  
    online archiving [266](#)–[268](#)  
Office apps [94](#)  
Office Customization Tool (OCT) [94](#)  
Office Online Server (OOS) [83](#), [123](#), [124](#), [125](#)  
Office Telemetry. See [telemetry](#)  
offline address book (OAB) [19](#), [328](#)  
Offline Address Book (OAB) [84](#)  
online archiving [266](#)–[268](#)  
Organization Management role [166](#), [219](#), [220](#), [221](#), [223](#), [224](#), [269](#)  
organization relationships [316](#)–[317](#)  
    troubleshooting [318](#)–[319](#)  
outbound connectors [304](#), [310](#)  
Outlook [312](#)  
    cached mode [46](#)  
    message classifications in [281](#)

online mode [46](#)  
protection rules [238–239](#)  
S/MIME and [233–234](#)

Outlook 2016  
    configuration [76](#)  
    planning and deployment [94](#)

Outlook Anywhere [68, 76–77, 326–327](#)

Outlook app [87–88](#)

Outlook Connection Status window [107](#)

Outlook MAPI over HTTP [68, 77–78](#)  
    troubleshooting connectivity [108–110](#)

Outlook on the web [68, 69, 79](#)  
    authentication [74–75](#)  
    coexistence and [328, 330](#)  
    message classifications [280–281](#)  
    policies [88–91](#)  
    S/MIME and [232–233](#)  
    troubleshooting [112–113](#)

Outlook Room Finder function [203–204](#)

Outlook Web App (OWA) [70](#)

OWA. See [Outlook Web App \(OWA\)](#)

OWA for Devices [87–88](#)

## P

Partner connectors [147](#)

passwords [80](#)  
    alphanumeric [81](#)  
    BitLocker and [228](#)  
    for mobile devices [81–82](#)  
    hashed [75](#)  
    history [81](#)  
    maximum age of [81](#)  
    minimum length for [81](#)  
    non-expiring [313](#)  
    recovery [229](#)  
    simple [80](#)

synchronization of [298–299](#)  
pattern matching [246](#)  
performance [132](#)  
    troubleshooting [51](#)  
performance counters [51](#)  
permissions  
    auto-mapping [216](#)  
    delegated setup [223–224](#)  
    eDiscovery [269](#)  
    for mail-enabled objects [212–218](#)  
    inheritance [217](#)  
    mailbox [214–215](#)  
    mailbox folder [213–214](#)  
    principal of least privilege [219, 220](#)  
    public folder [217](#)  
    role assignment policies [225–226](#)  
    role-based access control and [218–226](#)  
    Send As [212](#)  
    Send on Behalf [212–213](#)  
    split [221–223](#)  
    to shared mailboxes [205](#)  
personal identification number (PIN) [228](#)  
personal tags [257, 263](#)  
PFS. See [Perfect Forward Secrecy \(PFS\)](#)  
platform-as-a-service. See [PaaS](#)  
Policy Tips [247–248](#)  
POP3 [68](#)  
    configuration [82–83](#)  
    troubleshooting [113–114](#)  
POP3 protocol logs [150–152](#)  
POP protocol [331](#)  
port [25 310, 332, 335](#)  
port [110 82, 114](#)  
port [143 83, 114](#)  
port 443 [310, 317, 320, 331](#)  
port 993 [83, 114](#)

port 995 [82](#), [114](#)

port flooding [98](#)

power loss [51](#)

PowerShell

    creating mailboxes using [200](#)

    disk management cmdlets [11](#)

    eDiscovery searches in [273–275](#)

    looking up MX records in [308](#)

    malware filtering using [165–166](#)

    parameters [208](#)

    RBAC troubleshooting using [225](#)

pre-authentication [75](#)

Preferred Architectur [24](#)

Preferred Architecture [61](#)

prelicensing [240](#)

premium journaling [283](#)

primary hierarchy mailbox [6–8](#)

primary mailboxes [5–6](#)

principal of least privilege [219](#), [220](#)

protocol logging [336](#)

protocol logs [150–152](#), [155](#)

proxy

    open [168](#)

proxy redirect

    for coexistence [329–331](#)

proxy servers/proxying [69–70](#), [96](#)

    push notification [88–89](#)

    reverse [75](#)

    troubleshooting [118](#)

PST import [296](#)

Public Folder Management role [211](#), [219](#)

public folders [1](#)

    capacity and placement [6–9](#)

    creating and configuring [210–211](#)

    hierarchy, recovering [60](#)

    limits on [342](#)

migration to [341–343](#)  
moving between mailboxes [8](#)  
permissions for [217](#)  
recovery of [60–61](#)  
size of [8](#)  
user access [8](#)  
push notification proxy [88–89](#)

## Q

quarantined devices [80, 93–94](#)  
query-based in-place holds [275–276](#)  
queues [156–159, 159–160](#)  
Queue Viewer [156, 157–158, 179](#)  
quorums [22](#)  
    troubleshooting [53–54](#)  
quorum voting [32](#)

## R

RDS. See [Remote Desktop Services](#)  
read-only domain controllers (RODCs) [188](#)  
read-write domain controllers (RWDCs) [188](#)  
real-time block lists (RBLs) [169–171](#)  
real-time transport protocol (RTP) [98](#)  
receive connectors [136, 146–147, 161, 179–181, 332, 336](#)  
RECEIVED SMTP header [172](#)  
recipient filtering [171–172](#)  
Recipient Management role [219, 221](#)  
Records Management role [219](#)  
recoverability [132](#)  
recovery databases [19, 58–59](#)  
recovery keys [229](#)  
recovery password [229](#)  
Recovery Point Objective (RPO) [54](#)  
recovery solutions  
    dial tone restore [61–62](#)  
    Exchange Server 2016 [56–57](#)

lagged database copies [61–64](#)  
mailbox databases [56–65](#)  
mailboxes [58–59](#)  
mail items [59–60](#)  
public folder hierarchy [60](#)  
public folders [60–61](#)  
Recovery switch [58](#)  
Recovery Time Objective (RTO) [54](#)  
recovery workflow [13–14](#)  
redirection [70–71](#)  
    troubleshooting [118](#)  
redundancy  
    for intra-site mail delivery [138–140](#)  
    Safety Net for [140–141](#)  
    shadow [38, 141–143, 162](#)  
redundant array of independent disks (RAID) [1, 10, 17, 24](#)  
regional namespaces [323](#)  
regular expression pattern matching [246](#)  
RemoteApp  
    Azure. See [Azure RemoteApp](#)  
Remote Connectivity Analyzer [108–109, 110–111, 114, 116, 117, 157](#)  
Remove-ClusterNode cmdlet [57](#)  
Remove Connectivity Analyzer [308](#)  
Remove-DatabaseAvailabilityGroupServer cmdlet [57](#)  
Remove-Mailbox cmdlet [291](#)  
Remove-MailboxDatabaseCopy cmdlet [57](#)  
replay issues  
    troubleshooting [47–48](#)  
replay lag intervals [62](#)  
replay queue length [45, 50](#)  
replication [23](#)  
    continuous [44–45](#)  
    multi-master [6](#)  
        troubleshooting [47](#)  
replication networks [30, 31](#)  
reroute queues [177–179](#)

reseeding databases [48–49](#)  
resilience [31](#)  
Resilient File System (ReFS) [10–11](#)  
Resolve-DnsName cmdlet [308](#)  
resource contention [14](#)  
resource mailboxes [201–205](#)  
Restore-DatabaseAvailabilityGroup cmdlet [42](#)  
resubmission, of email messages [177–179](#)  
Resume-MailboxDatabaseCopy cmdlet [48](#)  
Resume-Message cmdlet [179](#)  
retention hold [264](#)  
retention period [263](#)  
retention policies [256](#), [257–258](#)  
    adding retention tags to [260–261](#)  
    archive mailboxes and [265–266](#)  
    assigning to users [262](#)  
    creating [258](#)  
    custom [259–261](#)  
    default [258](#)  
    Managed Folder Assistant (MFA) [262–264](#)  
    removal of tags from [264–265](#)  
RetentionPolicyTagLinks parameter [260](#)  
retention policy tags [257](#), [263](#)  
retention tags [257](#)  
    adding to retention policy [260–261](#)  
    changes to [263](#)  
    custom [259–261](#)  
    inheritance of [263](#)  
    naming [260](#)  
    removal and deletion of [264–265](#)  
Retry-Queue cmdlet [178](#), [179](#)  
reverse DNS lookup [168](#)  
reverse proxy  
    authentication and [75](#)  
    MAPI over HTTP and [78](#)  
reversible encryption [75](#)

Rights Management Services [168](#)

risk

    acceptable level of [23](#)

risk management [27](#)

role assignment policies [225–226](#)

role-based access control (RBA)

    eDiscovery and [269](#)

    role-based access control (RBAC) [218–226](#)

        creating unscoped top-level roles [224](#)

        delegated setup [223–224](#)

        roles and cmdlets [219–220](#)

        split permissions [221–222](#)

        troubleshooting [225](#)

        user assignment policies [225–226](#)

        using existing role groups [220](#)

roles

    creating top-level [224](#)

    mailbox folder [213–214](#)

    RBAC [219–220](#)

    unscoped [224](#)

rollbacks [16](#)

room mailboxes [201–205](#)

    booking requests [215](#)

    with delegates [215](#)

RootPublicFolderMailbox [7](#)

round robin load balancing [96, 125](#)

round trip network latency [38](#)

RPC Client Access Server [326](#)

RPC over HTTP/HTTPS [76, 77](#)

## S

Safety Net [38, 62, 63, 140–141, 162](#)

same-site domain controllers [188–190](#)

scheduled downtime [24](#)

Schema Admins group [193](#)

schema extension [192](#)

SCP. See [Service Connection Point](#)

Search-AdminAuditLog cmdlet [291–292](#)

Search-MailboxAuditLog cmdlet [288](#)

Search-Mailbox cmdlet [59](#), [274](#)

secondary hierarchy mailboxes [6–8](#)

Secure/Multipurpose Internet Mail Extensions (S/MIME) [231–235](#)

secure real-time transport protocol (SRTP) [98](#)

Secure Sockets Layer (SSL) [144](#), [277](#)

security. See also [passwords](#)

- BitLocker [227–231](#)
- Information Rights Management (IRM) [235–241](#)
- Secure/Multipurpose Internet Mail Extensions (S/MIME) [231–235](#)
- transport layer security (TLS) [144–145](#)
  - troubleshooting [160–161](#)

Security Group Creation role [221](#), [222](#)

security policies

- for ActiveSync devices [80–82](#)
- mobile devices [91–92](#)

seedling [35](#)

self-service deployment. See user-driven client deployments

self-signed certificates [71–72](#), [302](#), [318](#)

Send As permissions [212](#)

send connectors [136](#), [146](#), [147–149](#), [160](#), [179–181](#), [332](#)

Sender Policy Framework (SPF) [172–173](#)

Sender Policy Framework (SPF) records [308](#)

sender reputation level [168](#)

Send on Behalf permissions [212–213](#)

sensitive information [246](#), [250](#), [253](#)

ServerCertification.asmx [236](#)

server maintenance

- high availability and [25–28](#)

Server Management role [219](#)

server size calculator [3–4](#), [14](#), [16](#), [36](#)

Service Connection Point (SCP) [76](#)

service disruptions [27](#)

service level agreements (SLAs)

backup solutions and [54–56](#)

solutions to meet requirements in [24](#), [132](#)

session affinity

load balancing and [95](#), [96](#), [101–105](#)

`Set-ActiveSyncVirtualDirectory` cmdlet [329](#)

`Set-AdminAuditLogConfig` cmdlet [291](#)

`Set-AutodiscoverVirtualDirectory` cmdlet [325](#)

`Set-CalendarProcessing` cmdlet [215](#)

`Set-CASMailbox` cmdlet [88–89](#), [89–90](#), [312](#)

`Set-ClientAccessServer` cmdlet [76](#)

`Set-ClientAccessService` cmdlet [324](#)

`Set-ContentFilterConfig` cmdlet [174](#)

`Set-DatabaseAvailabilityGroup` cmdlet [31](#), [32](#), [41](#), [43](#)

`Set-DistributionGroup` cmdlet [311](#)

`Set-EcpVirtualDirectory` cmdlet [328](#)

`Set-IRMConfiguration` cmdlet [239](#)

`Set-Mailbox` cmdlet [8](#), [200](#), [262](#), [264](#), [287](#), [288](#), [311](#)

`Set-Mailbox` cmdlet a [276](#)

`Set-MailboxDatabase` cmdlet [8](#), [19](#), [20](#), [21](#), [46](#), [334](#)

`Set-MailboxDatabaseCopy` cmdlet [36](#)

`Set-MailboxSearch` cmdlet [275](#)

`Set-MailboxServer` cmdlet [49](#), [124](#)

`Set-MapiVirtualDirectory` cmdlet [327](#)

`Set-OabVirtualDirectory` cmdlet [328](#)

`Set-OrganizationConfig` cmdlet [278](#)

`Set-OutlookAnywhere` cmdlet [326](#)

`Set-OwaVirtualDirectory` cmdlet [328](#)

`Set-ReceiveConnector` cmdlet [147](#), [155](#), [161](#), [336](#)

`Set-RetentionPolicy` cmdlet [260](#)

`Set-SenderIDConfig` cmdlet [173](#)

`Set-TransportConfig` cmdlet [141](#), [160](#), [166](#), [178](#), [284](#)

`Set-TransportServer` cmdlet [177](#)

`Set-TransportService` cmdlet [177](#), [178](#)

setup process [56](#)

`Set-WebServicesVirtualDirectory` cmdlet [79](#), [327](#)

shadow redundancy [38](#), [141–143](#), [162](#)

Shadow Safety Net [38](#)  
shared mailboxes [205–206](#)  
shared namespaces  
    troubleshooting [155–156](#)  
Sharepoint. See [Microsoft Sharepoint](#)  
SharePoint 2013 [277](#)  
sharing. See also [collaboration](#)  
    external. See external users  
sharing policies [315–316](#)  
Simple Mail Transfer Protocol (SMTP) [332–333](#), [335–336](#)  
single-label domains [191](#)  
single namespaces [155](#)  
single sign-on (SSO) [300](#)  
SIP addresses. See [Session Initiation Protocol \(SIP\) addresses](#)  
SIP load balancing [97](#)  
site-aware decisions [38](#)  
site recovery  
    testing and performing [42–43](#)  
site resilience cmdlets [41](#)  
site-resilient client access services [118–127](#)  
    document collaboration [123](#)  
    namespaces [119–124](#)  
    namespace URLs [124–125](#)  
site-resilient Data Availability Groups [38–43](#)  
site-resilient Database Availability Groups  
    alternate FSW [41–42](#)  
    cross-site DAG configuration [38–40](#)  
    Datacenter Activation Coordination (DAC) [40–41](#)  
    site recovery [42–43](#)  
site resilient transport services [176–183](#)  
    MX records for failover scenarios [176–177](#)  
    resubmission and reroute queues [177–179](#)  
    send/receive connectors [179–181](#)  
    transport failover and switchover [181–183](#)  
site topologies [194–197](#)  
SkipLagChecks switch [63](#)

smart hosts [332](#)  
SMTP. See [Single Mail Transfer Protocol \(SMTP\)](#); See [Simple Mail Transfer Protocol \(SMTP\)](#)  
SMTP logs [155](#)  
SMTP mail flow  
    troubleshooting [156–159](#)  
SMTP relay [332–333](#), [335–336](#)  
snapshots [15–16](#)  
soft recovery [52](#), [63](#)  
software updates  
    high availability and [24–27](#), [25–28](#)  
solid state drives (SSDs) [36](#)  
spam confidence level [168](#)  
spam confidence level (SCL) [282](#)  
Spam Confidence Level (SCL) thresholds [174–176](#)  
spam filtering [166–168](#)  
SPF. See [send policy framework \(SPF\) records](#)  
split brain conditions [40–41](#)  
“split-brain” DNS [69](#), [125](#)  
split DNS [323–324](#)  
split permissions  
    Active Directory [221–223](#)  
    RBAC [221–222](#)  
spoofed email messages [172–173](#)  
SSL certificates [56](#), [76](#), [79](#), [302](#), [317](#), [320](#)  
staged migration [296](#)  
standard edition Exchange 2016 license [18](#)  
standard journaling [283](#)  
Start-ComplianceSearch cmdlet [274](#)  
Start-EdgeSyncrhonization command [146](#)  
Start-MailboxSearch cmdlet [273](#), [274](#)  
Start-MigrationBatch cmdlet [341](#)  
startup keys [228](#)  
Stop-DatabaseAvailabilityGroup cmdlet [42](#)  
storage architectures  
    Direct-Attached Storage (DAS) [9](#)

“just a bunch of disks” (JBOD) [10](#), [12](#)  
Network-Attached Storage (NAS) [9](#)  
planning [9–10](#)  
redundant array of independent disks (RAID) [10](#), [17](#)  
Storage Area Network (SAN) [9](#)  
Storage Area Network (SAN) [9](#)  
Storage Message Block (SMB) [9](#)  
storage quotas [8](#)  
storage requirements  
    Azure and [36–37](#)  
    for lagged copies [62](#)  
    for mailbox databases [2–3](#)  
store service [51](#)  
Subject Alternative Name (SAN) certificates [73](#)  
subnet broadcasts [98](#)  
Super Users group [236](#)  
Support and Recovery Assistant [109–110](#), [116](#)  
SuspendComment parameter [47](#)  
Suspend-MailboxDatabaseCopy cmdlet [47](#), [49](#), [62](#), [63](#)  
switchovers [22–23](#), [42](#), [126](#), [181](#), [183](#)  
    client behavior during [127](#)  
synchronized identity model [298–301](#)  
SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} [291](#)

## T

teamed network interfaces [24](#)  
Telnet application [335](#)  
Test-ActiveSyncConnectivity cmdlet [117](#)  
Test DLP policy without Policy Tips [247](#)  
Test DLP policy with Policy Tips [255](#)  
Test E-Mail AutoConfiguration tool [107–108](#), [116](#)  
Test E-Mail AutoConfiguration utility [337](#)  
test environment [27](#)  
Test-FederationTrustCertificate cmdlet [318](#)  
Test-ImapConnectivity cmdlet [113–114](#)  
Test-OutlookConnectivity cmdlet [77](#)

Test-PopConnectivity cmdlet [113–114](#)  
Test-ReplicationHealth cmdlet [45–46](#)  
thin-provisioned storage [228](#)  
third-party certificates [72, 73](#)  
throttling policies [197](#)  
TLS connections [82, 83](#)  
TLSReceiveDomainSecureList property [160](#)  
TLSSendDomainSecureList property [160](#)  
TPM. See [Trusted Platform Module](#); See [Trusted Platform Module \(TPM\)](#)  
transaction log files [4–5, 12, 44, 50, 51, 61](#)  
    accumulation of [48](#)  
    configuration of [20–21](#)  
    placement of [19](#)  
    rolling forward [63](#)  
TransientFailureRetryCount parameter [177](#)  
transport architecture  
    troubleshooting [161–163](#)  
transport dumpster [140, 162](#)  
transport layer security (TLS) [144–145](#)  
    troubleshooting [160–161](#)  
transport protection rules [238](#)  
transport rules [247, 250–251, 252–253, 279, 310](#)  
    for compliance requirements [282–283](#)  
Transport service  
    restarting [167](#)  
transport services [131–186](#)  
    connection filtering [169–171](#)  
    Edge Transport [131, 145–146](#)  
    inter-org mail flow [135–138](#)  
    inter-site mail flow [132–135](#)  
    intra-site mail delivery [138–140](#)  
    Mailbox Server role [131](#)  
    mail exchange (MX) records [143–144](#)  
    message hygiene [164–175](#)  
    message tracking logs [150, 152–154](#)  
    monitoring [150–155](#)

planning [132–149](#)  
protocol logs [150–152](#), [155](#)  
recipient filtering [171–172](#)  
Safety Net [140–141](#)  
Sender Policy Framework (SPF) [172–173](#)  
send/receive connectors [146–149](#), [160–161](#)  
shadow redundancy [141–143](#)  
site resilient [176–183](#)  
SLAs and [132](#)  
transport layer security (TLS) [144–145](#), [160–161](#)  
transport-related tasks [144–149](#)  
troubleshooting  
    failure scenarios [159–160](#)  
    shared namespaces [155–156](#)  
    SMTP mail flow [156–159](#)  
    transport architecture [161–163](#)  
troubleshooting  
    address rewriting [156](#)  
    authentication [115](#)  
    Autodiscover [116](#)  
    client access [312](#)  
    client access in coexistence  
        in coexistence [337](#)  
    client connectivity [106–118](#)  
    cross-forest availability [319–320](#)  
    directory synchronization [313](#)  
    Edge Transport [162–163](#)  
    email delivery [161–163](#), [307–311](#)  
    Exchange ActiveSync (EAS) [117–118](#)  
    Exchange Web Services (EWS) [110–111](#)  
    federation trusts [318–319](#)  
    Hybrid Exchange configuration [307–311](#)  
    IMAP4 [113–114](#)  
    Information Rights Management (IRM) [240–241](#)  
    mailbox databases  
        copy activation [48–51](#)

database failures [51–52](#)  
performance [51](#)  
quorum issues [53–54](#)  
replication and replay [47–48](#)  
Mailbox Replication Service (MRS) [343–344](#)  
message delivery [161–163](#)  
migration [343–344](#)  
Outlook Anywhere connectivity [106–108](#)  
Outlook MAPI over HTTP connectivity [108–110](#)  
Outlook on the web [112–113](#)  
POP3 [113–114](#)  
proxy [118](#)  
redirection [118](#)  
role-based access control [225](#)  
Safety Net [162](#)  
shadow redundancy [162](#)  
shared namespaces [155–156](#)  
SMTP mail flow [156–159](#)  
transport  
    in coexistence [335–337](#)  
    transport architecture [161–163](#)  
    transport layer security (TLS) [160–161](#)  
    transport services [159–163](#)  
Trusted Platform Module (TPM) [227, 228](#)  
Trusted Publishing Domain (TPD) [306](#)

## U

UCE. See [Update Compatibility Evaluator \(UCE\)](#)

UE-V. See [User Experience Virtualization](#)

UM Management role [219](#)

unbound deployment [68](#)

unified messaging [97–98](#)

Unified Messaging service [260](#)

Unified Messaging (UM) [306](#)

unified namespaces [68](#)

unscoped roles [224](#)

Update-MailboxDatabaseCopy cmdlet [48](#)

uptime [132](#)

URLs [68](#)

Autodiscover [76](#)

EAC [79](#)

EWS [78–79](#)

internal and external [78](#)

MAPI virtual directories [78](#)

OAB [84](#)

redirection [70–71](#)

site-resilient namespace [124–125](#)

UseDatabaseQuotaDefaults attribute [8](#)

user accounts. See also identities

user assignment policies [225–226](#)

user identities. See identities

user principle name (UPN) [301](#), [313](#)

users

mail-enabled [206](#)

U.S. Financial Data policy template [250](#)

## V

validation process

for custom domain [301](#)

View-only organization management role [219](#)

virtual directories

MAPI over HTTP [78](#)

Outlook on the web [79](#)

virtualization

lack of TPM and [227](#)

requirements and scenarios [14–16](#)

thin provisioning [15](#)

virtual machines (VMs)

disaster recovery planning [15](#)

dynamic memory and [15](#), [36](#)

hardware sharing by [14](#)

hosting witness server on [34–35](#)

memory allocation [14](#)  
migration of [15](#)  
network connectivity and [37](#)  
sizing requirements [36](#)  
snapshots [15–16](#)  
storage allocation [15](#)  
storage requirements [36–37](#)  
voicemail messages [260](#)

## W

WCE. See [Windows Compatibility Evaluator](#)  
WDS. See [Windows Deployment Services \(WDS\)](#)  
Web Application Proxy (WAP) servers [299](#)  
wide area networks (WANs) [30, 39–40](#)  
wide-area network (WAN) optimization controllers (WOCs) [144](#)  
wildcard certificates [73](#)  
WIM. See [Windows Imaging Format \(WIM\)](#)  
Windows Failover Clustering [98](#)  
Windows Network Load Balancing (Windows NLB) [98–101](#)  
WitnessDirectory [29](#)  
witness server [32–35, 41–42, 126](#)  
WitnessServer [29](#)

## About the authors

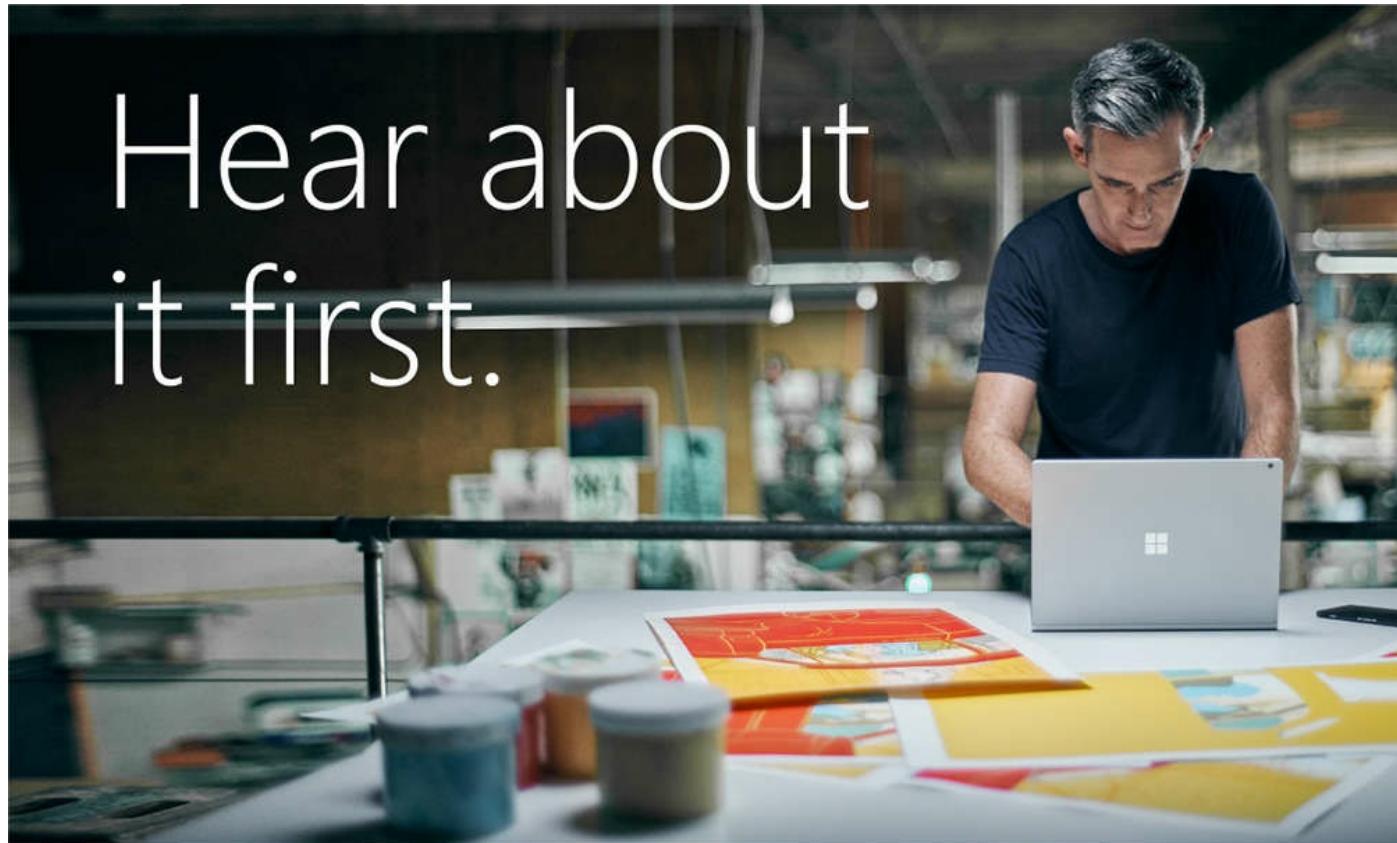


**PAUL CUNNINGHAM** is an independent consultant, writer, and trainer who specializes in Office 365 and Exchange Server. Paul runs the [ExchangeServerPro.com](http://ExchangeServerPro.com) and [Practical365.com](http://Practical365.com) websites. He is a co-author of Office 365 for IT Pros, and has been awarded as a Microsoft Most Valuable Professional (MVP) since 2012.



**BRIAN SVIDERGOL** builds Microsoft infrastructure and cloud solutions with Windows, Exchange Server, Active Directory, Microsoft Azure, Office 365, and related technologies. He holds many industry certifications, including the Microsoft Certified Trainer (MCT) and Microsoft Certified Solutions Expert (MCSE) - Server Infrastructure. Brian is the author of several books on Microsoft technologies. He served as an MCT Ambassador at TechEd North America 2013 and at Microsoft Ignite 2015. Brian works as a subject matter expert (SME) on many Microsoft Official Curriculum courses and Microsoft certification exams.

# Hear about it first.



Get the latest news from Microsoft Press sent to your inbox.

- New and upcoming books
- Special offers
- Free eBooks
- How-to articles

Sign up today at [MicrosoftPressStore.com/Newsletters](https://MicrosoftPressStore.com/Newsletters)



Visit us today at



[microsoftpressstore.com](http://microsoftpressstore.com)

- **Hundreds of titles available** – Books, eBooks, and online resources from industry experts
- **Free U.S. shipping**
- **eBooks in multiple formats** – Read on your computer, tablet, mobile device, or e-reader
- **Print & eBook Best Value Packs**
- **eBook Deal of the Week** – Save up to 60% on featured titles
- **Newsletter and special offers** – Be the first to hear about new releases, specials, and more
- **Register your book** – Get additional benefits





From technical overviews to drilldowns on special topics, get *free* ebooks from Microsoft Press at:

[www.microsoftvirtualacademy.com/ebooks](http://www.microsoftvirtualacademy.com/ebooks)

Download your free ebooks in PDF, EPUB, and/or Mobi for Kindle formats.

Look for other great resources at Microsoft Virtual Academy, where you can learn new skills and help advance your career with free Microsoft training delivered by experts.

Microsoft Press



Now that  
you've  
read the  
book...

Tell us what you think!

Was it useful?

Did it teach you what you wanted to learn?

Was there room for improvement?

**Let us know at <http://aka.ms/tellpress>**

Your feedback goes directly to the staff at Microsoft Press,  
and we read every one of your responses. Thanks in advance!





# Code Snippets

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the eBook in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a “Click here to view code image” link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

```
[PS] C:\>Get-OrganizationConfig | Select-Object RootPublicFolderMailbox  
  
RootPublicFolderMailbox  
-----  
612fd5f2-1e50-4280-bce4-dd4b0791744d  
[PS] C:\>Get-Mailbox -PublicFolder | Where {$_.ExchangeGuid -eq "612fd5f2-1e50-4280-bce4-dd4b0791744d"}
```

Name	Alias	ServerName	ProhibitSendQuota
-----	-----	-----	-----
PFMailbox01	PFMailbox01	ny-exch01	Unlimited

```
[PS] C:\>New-Mailbox -PublicFolder -Name PFMailbox02 -IsExcludedFromServingHierarchy  
$true
```

Name	Alias	ServerName	ProhibitSendQuota
----	-----	-----	-----
PFMailbox02	PFMailbox02	ny-exch01	Unlimited

```
[PS] C:\>Get-Mailbox -PublicFolder PFMailbox02 | Select IsHierarchyReady  
IsHierarchyReady : True
```

```
[PS] C:\>Set-Mailbox -PublicFolder PFMailbox02 -IsExcludedFromServingHierarchy $false
```

```
PS C:\> Get-Disk
Number Friendly Name      OperationalStatus Total Size Partition Style
---- -----
2    Microsoft Virtual Disk Online        100 GB   GPT
1    Microsoft Virtual Disk Online        100 GB   GPT
3    Microsoft Virtual Disk Online        100 GB   RAW
0    Virtual HD ATA Device  Online        95 GB    MBR
```

```
PS C:\> Get-Disk 3 | Initialize-Disk -PartitionStyle GPT -PassThru | New-Partition -UseMaximumSize | Format-Volume -FileSystem ReFS -NewFileSystemLabel Volume3 -SetIntegrityStreams $false
```

#### Confirm

Are you sure you want to perform this action?

Warning, all data on the volume will be lost!

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):  
y

DriveLetter	FileSystemLabel	FileSystem	DriveType	HealthStatus
	Volume3	ReFS	Fixed	Healthy

#Creating a mailbox database in the Exchange management shell

```
[PS] C:\>New-MailboxDatabase -Name DB01 -Server NY-EXCH01 -EdbFilePath C:\ExchangeDatabases\DB01\DB01.db\DB01.edb -LogFolderPath C:\ExchangeDatabases\DB01\DB01.log
```

Name	Server	Recovery	ReplicationType
----	-----	-----	-----
DB01	NY-EXCH01	False	None

```
[PS] C:\>Set-MailboxDatabase "Mailbox Database 0135571303" -Name DB05  
[PS] C:\>Move-DatabasePath -Identity DB05 -EdbFilePath C:\ExchangeDatabases\DB05\DB05.edb -LogFolderPath C:\ExchangeDatabases\DB05\DB05.log
```

Confirm

Are you sure you want to perform this action?

Moving database path "DB05".

[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): y

Confirm

To perform the move operation, database "DB05" must be temporarily dismounted, which will make it inaccessible to all users. Do you want to continue?

[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (default is "Y"): y

```
[PS] C:\>Set-ServerComponentState NY-EXCH01 -Component HubTransport -State Draining  
-Requester Maintenance  
[PS] C:\>Redirect-Message -Server NY-EXCH01 -Target EX2016SRV2.exchangeviewerpro.net
```

#Suspending a cluster node for maintenance

[PS] C:\>Suspend-ClusterNode -Name NY-EXCH01

```
#Setting the DatabaseCopyActivationDisabledAndMoveNow attribute  
[PS] C:\>Set-MailboxServer -Identity NY-EXCH01 -DatabaseCopyActivationDisabledAndMoveNow  
$true
```

```
#Setting the database auto activation policy
```

```
[PS] C:\>Set-MailboxServer -Identity NY-EXCH01 -DatabaseAutoActivationPolicy Blocked
```

```
#Checking for active database copies on the server
```

```
[PS] C:\> Get-MailboxDatabaseCopyStatus -Server NY-EXCH01 | Where {$_.Status -eq  
"Mounted"}
```

#Taking server components offline for maintenance

```
[PS] C:\> Set-ServerComponentState NY-EXCH01 -Component ServerWideOffline -State InActive -Requester Maintenance
```

```
[PS] C:\>Set-ServerComponentState NY-EXCH01 -Component ServerWideOffline -State Active  
-Requester Maintenance  
[PS] C:\>Resume-ClusterNode -Name NY-EXCH01  
[PS] C:\>Set-MailboxServer NY-EXCH01 -DatabaseCopyAutoActivationPolicy Unrestricted  
[PS] C:\>Set-MailboxServer NY-EXCH01 -DatabaseCopyActivationDisabledAndMoveNow $false  
[PS] C:\>Set-ServerComponentState NY-EXCH01 -Component HubTransport -State Active -  
Requester Maintenance
```

```
#Creating a new database availability group
```

```
[PS] C:\>New-DatabaseAvailabilityGroup -Name DAG01 -WitnessServer NY-DC01.contoso.com  
-FileSystem ReFS
```

#Adding an Exchange 2016 server as a DAG member

[PS] C:\>Add-DatabaseAvailabilityGroupServer -Identity DAG01 -MailboxServer NY-EXCH01

```
#Command to view all properties of a DAG
```

```
[PS] C:\>Get-DatabaseAvailabilityGroup -Identity DAG01 -Status | Format-List
```

```
#Command to enable manual DAG network configuration
```

```
[PS] C:\>Set-DatabaseAvailabilityGroup -Identity DAG01 -ManualDagNetworkConfiguration  
$true
```

```
#Command to enable automatic DAG network configuration  
[PS] C:\>Set-DatabaseAvailabilityGroup -Identity DAG01 -ManualDagNetworkConfiguration  
$false
```

```
#Command to ignore a DAG network
```

```
[PS] C:\>Set-DatabaseAvailabilityGroupNetwork "DAG01\ReplicationDagNetwork01"  
-IgnoreNetwork $true
```

```
#Adding a new database copy to another DAG member
```

```
[PS] C:\> [PS] C:\>Add-MailboxDatabaseCopy -Identity DB01 -MailboxServer NY-EXCH02
```

```
#Viewing the mailbox database copy status
```

```
[PS] C:\>Get-MailboxDatabaseCopyStatus DB01 | Select Name,Status,ActivationPreference,CopyQueueLength
```

Name	Status	ActivationPreference	CopyQueueLength
DB01\NY-EXCH01	Mounted	1	0
DB01\NY-EXCH02	Healthy	2	0

#Configuring the Activation Preference for a mailbox database copy

```
[PS] C:\>Set-MailboxDatabaseCopy -Identity DB02\NY-EXCH02 -ActivationPreference 1
```

#Enabling DAC Mode for a Database Availability Group

[PS] C:\>Set-DatabaseAvailabilityGroup -Identity DAG01 -DatacenterActivationMode DagOnly

```
#Terminating the DAG in a failed datacenter
```

```
[PS] C:\>Stop-DatabaseAvailabilityGroup -Identity DAG01 -ActiveDirectorySite NewYork  
-ConfigurationOnly
```

```
#Restoring the DAG in the secondary datacenter
```

```
[PS] C:\>Restore-DatabaseAvailabilityGroup -Identity DAG01 -ActiveDirectorySite  
SanFrancisco -AlternateWitnessServer SF-DC01
```

#Using Test-ReplicationHealth to monitor Exchange 2016 DAG members

[PS] C:\>Test-ReplicationHealth -Server NY-EXCH01

Server	Check	Result
-----	-----	-----
NY-EXCH01	ClusterService	Passed
NY-EXCH01	ReplayService	Passed
NY-EXCH01	ActiveManager	Passed
NY-EXCH01	TasksRpcListener	Passed
NY-EXCH01	TcpListener	Passed
NY-EXCH01	ServerLocatorService	Passed
NY-EXCH01	DagMembersUp	Passed
NY-EXCH01	MonitoringService	Passed
NY-EXCH01	ClusterNetwork	Passed
NY-EXCH01	QuorumGroup	Passed
NY-EXCH01	FileShareQuorum	Passed
NY-EXCH01	DatabaseRedundancy	Passed
NY-EXCH01	DatabaseAvailability	Passed
NY-EXCH01	DBCopySuspended	Passed
NY-EXCH01	DBCopyFailed	Passed
NY-EXCH01	DBInitializing	Passed
NY-EXCH01	DBDisconnected	Passed
NY-EXCH01	DBLogCopyKeepingUp	Passed
NY-EXCH01	DBLogReplayKeepingUp	Passed

```
#Using Get-MailboxDatabaseCopyStatus to monitor database replication
```

```
[PS] C:\>Get-MailboxDatabaseCopyStatus
```

Name	Status	CopyQueueLength	ReplayQueueLength	ContentIndexState
DB01\NY-EXCH01	Mounted	0	0	Healthy
DB02\NY-EXCH01	Healthy	0	0	Healthy
DB03\NY-EXCH01	Healthy	0	0	Healthy
DB04\NY-EXCH01	Healthy	0	0	Healthy

#Viewing the reason for a suspended database copy

```
[PS] C:\>Get-MailboxDatabaseCopyStatus | Select Name,Status,SuspendComment
```

Name	Status	SuspendComment
DB01\NY-EXCH01	Mounted	
DB02\NY-EXCH01	Healthy	
DB03\NY-EXCH01	Suspended	Performing disk maintenance
DB04\NY-EXCH01	Healthy	

```
#Reseeding a mailbox database copy
```

```
[PS] C:\>Update-MailboxDatabaseCopy DB03\NY-EXCH01 -DeleteExistingFiles
```

```
#Activating a database copy
```

```
[PS] C:\>Move-ActiveMailboxDatabase -Identity DB03 -ActivateOnServer SF-EXCH02
```

#Using ESEUtil to determine the database state

C:\>eseutil /mh C:\ExchangeDatabases\DB01\DB01.db\DB01.edb

#Soft repair of a mailbox database with ESEUtil

C:\>eseutil /r E01 /d E:\DB01 /l F:\DB01

```
#Reconnect a disconnected mailbox
```

```
[PS] C:\>Connect-Mailbox -Identity "Kim Akers" -Database DB01 -User "Kim Akers"
```

```
#Create a mailbox restore request
```

```
[PS] C:\>New-MailboxRestoreRequest -Name "Kim Akers restore" -SourceDatabase RecoveryDB  
-SourceStoreMailbox "Kim Akers" -TargetMailbox "Kim Akers"
```

```
#Enabling a mailbox for Single Item Recovery
```

```
[PS] C:\>Set-Mailbox -Identity "Kim Akers" -SingleItemRecoveryEnabled $true
```

#Restoring a specific mailbox folder

```
[PS] C:\>New-MailboxRestoreRequest -Name "Kim Akers sent items" -SourceDatabase RecoveryDB -SourceStoreMailbox "Kim Akers" -TargetMailbox "Kim Akers" -IncludeFolders "#SentItems#"
```

```
#Configuring a 7-day replay lag
```

```
[PS] C:\>Set-MailboxDatabaseCopy -Identity DB04\SF-EXCH02 -ReplayLagTime 7.0:0:0
```

#Configuring a 7-day replay lag

```
[PS] C:\>Suspend-MailboxDatabaseCopy -Identity DB04\SF-EXCH02 -ActivationOnly
```

```
Set-OrganizationConfig -MapiHttpEnabled $True
```

```
Set-WebServicesVirtualDirectory -Identity EX-01\EWS(Default Web Site) -ExternalUrl  
https://mail.contoso.com/EWS/exchange.asmx -InternalUrl https://mail.contoso.com/EWS/  
exchange.asmx
```

```
New-DistributionGroup -Name "Adatum, Inc" -DisplayName "Adatum" -Alias  
"AdatumRoot" -OrganizationalUnit "adatum.com/HAB" -SamAccountName "AdatumRoot"  
-Type "Distribution"
```

```
Set-OrganizationConfig -HierarchicalAddressBookRoot "Adatum" command
```

```
New-DistributionGroup -Name "Engineering" -DisplayName "Engineering" -Alias  
"Engineering" -OrganizationalUnit "adatum.com/HAB" -SamAccountName "Engineering"  
-Type "Distribution"
```

```
Set-Group -Identity "Engineering" -IsHierarchicalGroup $True
```

```
New-DistributionGroup -Name "Software" -DisplayName "Software" -Alias "Software"  
-SamAccountName "Software"
```

Add-DistributionGroupMember -Identity "Engineering" -Member "Software"

```
Set-CASMailbox -Identity Marc -OWAforDevicesEnabled $False
```

Enable-PushNotificationProxy -Organization adatum.com

```
Invoke-MonitoringProbe PushNotifications.Proxy\  
PushNotificationsEnterpriseConnectivityProbe -Server EX01.adatum.com
```

```
Set-OwaMailboxPolicy -Identity NoPasswordChange -ChangePasswordEnabled $False
```

```
Set-CASMailbox -Identity Marc -OwaMailboxPolicy:NoPasswordChange
```

```
New-MobileDeviceMailboxPolicy -Name Policy2 -AllowSimplePassword $True
```

```
Set-CASMailbox -Identity Marc -ActiveSyncMailboxPolicy Policy2
```

```
New-ActiveSyncDeviceAccessRule -Characteristic DeviceOS -QueryString "iOS 7.0.2 11A501"  
-AccessLevel Block
```

```
Get-MobileDevice | Format-List DeviceOS,DeviceModel,DeviceType
```

```
Set-ServerComponentState EX01 -Component OwaProxy -Requestor Maintenance -State Inactive
```

```
Add-WindowsFeature -Name NLB -IncludeManagementTools
```

```
Get-ServerHealth EX01 | where HealthSetName -eq "OWA" | FT Name,AlertValue -AutoSize
```

Test-PopConnectivity -ClientAccessServer EX01.contoso.com  
Test-ImapConnectivity -ClientAccessServer EX01.contoso.com

Test-ActiveSyncConnectivity -ClientAccessServer nyc-ex1.contoso.com

```
Set-MailboxServer EX01 -WACDiscoveryEndPoint https://oos.west.adatum.com/hosting/discovery
```

```
Set-AdSite "Site 1" -HubSiteEnabled $True
```

```
Set-AdSiteLink -Identity Site3-Site1 -ExchangeCost 25
```

```
Set-ReceiveConnector SERVER1\WAN1 -SuppressXAnonymousTLS $true
```

```
New-EdgeSubscription -FileName e:\temp\subscription.xml
```

```
New-EdgeSubscription -FileData ([byte[]]$([Get-Content -Path "d:\temp\subscription.xml" -Encoding Byte -ReadCount 0])) -Site "HQ".
```

```
Set-PopSettings -Server EX-03 -ProtocolLogEnabled $True
```

```
Set-ImapSettings -Server EX-03 -ProtocolLogEnabled $True
```

2016-06-14T04:11:07.250Z,00000000000000009,0,[2601:101:c000:1503:998:4be:fa4c:371c]:995,[2601:101:c000:1503:458b:9fa2:446f:b825]:57837,,1,0,51,OpenSession,,,

2016-06-14T04:11:07.265Z,00000000000000009,1,[2601:101:c000:1503:998:4be:fa4c:371c]:995,[2601:101:c000:1503:458b:9fa2:446f:b825]:57837,,1,4,37, capa,,R=ok,

2016-06-14T04:11:07.265Z,00000000000000009,2,[2601:101:c000:1503:998:4be:fa4c:371c]:995,[2601:101:c000:1503:458b:9fa2:446f:b825]:57837,user2,1,10,5,user,user2,R=ok,

2016-06-14T04:11:07.265Z,00000000000000009,3,[2601:101:c000:1503:998:4be:fa4c:371c]:995,[2601:101:c000:1503:458b:9fa2:446f:b825]:57837,user2,2,10,56,pass,\*\*\*\*\*,"R=""-ERR Logon failure: unknown user name or bad password."";Msg=LogonFailed:LogonDenied;ErrMsg=LogonFailed:LogonDenied",

2016-06-14T04:11:07.265Z,00000000000000009,4,[2601:101:c000:1503:998:4be:fa4c:371c]:995,[2601:101:c000:1503:458b:9fa2:446f:b825]:57837,user2,0,0,0,CloseSession,,,

```
Get-MessageTrackingLog -Server NYC-EX1 -Sender "user1@contoso.com" | FL Sender,Recipients,MessageSubject,MessageId
```

```
Sender      : User1@contoso.com
Recipients   : {managers@adatum.com}
MessageSubject : Tomorrow's meeting
MessageId    : 2a48b06dce944de793134062ce912cd7@contoso.com
```

```
Get-MessageTrackingLog -MessageID "2a48b06dce944de793134062ce912cd7@contoso.com"
| FL
```

RunspaceId	:	06d04667-4a4d-4d07-b193-88f961f140cd
Timestamp	:	6/13/2016 8:39:08 PM
ClientIp	:	2601:101:c000:1503:998:4be:fa4c:371c
ClientHostname	:	NYC-EX1.contoso.com
ServerIp	:	2601:101:c000:1503:998:4be:fa4c:371c
ServerHostname	:	NYC-EX1
SourceContext	:	08D393FF7B4C6721;2016-06-14T03:39:07.959Z;0
ConnectorId	:	NYC-EX1\Default NYC-EX1
Source	:	SMTP
EventId	:	RECEIVE
InternalMessageId	:	2847563317266
MessageId	:	2a48b06dce944de793134062ce912cd7@contoso.com
NetworkMessageId	:	0172c47b-949b-4388-76b2-08d3940570eb
Recipients	:	{managers@adatum.com}
RecipientStatus	:	{}
TotalBytes	:	7805
RecipientCount	:	1
RelatedRecipientAddress	:	
Reference	:	
MessageSubject	:	Tomorrow's meeting
Sender	:	User1@contoso.com
ReturnPath	:	User1@contoso.com
Directionality	:	Originating
TenantId	:	
OriginalClientIp	:	2601:101:c000:1503:458b:9fa2:446f:b825
MessageInfo	:	0cI:
MessageLatency	:	
MessageLatencyType	:	None
EventData	:	{[FirstForestHop, NYC-EX1.contoso.com], [FromEntity, [AccountForest, contoso.com]]}

```
Set-ReceiveConnector -Identity 'EX-01\Default Frontend EX-01' -ProtocolLoggingLevel  
Verbose
```

```
Get-ReceiveConnector -Server EX-01 | Set-ReceiveConnector -ProtocolLoggingLevel Verbose
```

```
New-MalwareFilterPolicy -Name Policy1 -Action  
DeleteAttachmentAndUseDefaultAlertText
```

```
New-MalwareFilterRule -Name Rule1 -MalwareFilterPolicy Policy1 -RecipientDomainIs  
contoso.com
```

```
Set-TransportConfig -InternalSMTPServers @{Add="192.168.1.112"}
```

`Get-TransportAgent "Connection Filtering Agent"`

**Enable-TransportAgent "Connection Filtering Agent"**

```
Add-IPBlockListEntry -IPRange 10.0.0.0/24
```

```
Set-RecipientFilterConfig -BlockListEnabled $true
```

```
Set-SenderIdConfig -SpoofedDomainAction Delete -BypassedRecipients user1@contoso.com
```

```
Set-ContentFilterConfig -SCLDeleteEnabled $True -SCLDeleteThreshold 7
```

```
Set-OrganizationConfig -SCLJunkThreshold 4
```

```
Set-TransportService -TransientFailureRetryCount 10
```

```
Get-Message -Filter {FromAddress -like "*@contoso.com"} -Server NYC-EX1 | ForEach-Object  
{$Temp="C:\ "+$_.InternetMessageID+".eml";$Temp=$Temp.Replace("<","_");$Temp=$Temp.  
Replace(">","_");Export-Message $_.Identity | AssembleMessage -Path $Temp}
```

```
Setup.exe /PrepareAllDomains /IacceptExchangeServerLicenseTerms
```

```
New-ThrottlingPolicy -Name OWAConcurrency -OwaMaxConcurrency 5 -ThrottlingPolicyScope Organization
```

```
Set-ThrottlingPolicy PowerShellCmdlets -PowerShellMaxCmdlets 10  
-PowerShellMaxCmdletsTimePeriod 60
```

```
Enable-Mailbox -Identity "Brian Svidergol"
```

```
Set-Mailbox -Identity "Wriju Ghosh" -EmailAddressPolicyEnabled $False
```

```
Set-Mailbox -Identity "Wriju Ghosh" -PrimarySmtpAddress wriju@adatum.com
```

```
Set-Mailbox -Identity "Wriju Ghosh" -LitigationHoldEnabled $True
```

```
$password = Read-Host "Password?" -AsSecureString

New-Mailbox -UserPrincipalName wghosh@adatum.com -Alias wghosh -Name wghosh
-OrganizationalUnit CorpUsers -Password $password -FirstName Wriju -LastName
Ghosh-DisplayName "Wriju Ghosh" -ResetPasswordOnNextLogon $true
```

```
New-Mailbox -Room -Name "GTNP" -ResourceCapacity 10 -Phone "307-555-1299"
```

```
Set-Mailbox -Name "Signal Mountain" -ResourceCapacity 12
```

```
$ResourceConfiguration = Get-ResourceConfig  
  
$ResourceConfiguration.ResourcePropertySchema+=("Room/Projector")  
  
$ResourceConfiguration.ResourcePropertySchema.Add("Room/Smartboard")  
  
$ResourceConfiguration.ResourcePropertySchema+=("Room/Whiteboard")  
  
Set-ResourceConfig -ResourcePropertySchema $ResourceConfiguration.ResourcePropertySchema
```

```
$ResourceMailbox = Get-Mailbox -Identity "Building 3 Tech Room"  
  
$ResourceMailbox.ResourceCustom.Add("Smartboard")  
  
$ResourceMailbox | Set-Mailbox -ResourceCustom $ResourceMailbox.ResourceCustom
```

```
New-DistributionGroup -Name "Building 1 rooms" -OrganizationalUnit "adatum.com/Exchange/  
DLs" -RoomList
```

```
Add-DistributionGroupMember -Identity "Building 1 rooms" -Member "Building 1 Sales Room"
```

New-Mailbox -Equipment -Name "Wireless projector"

```
Add-MailboxPermissions -Identity "Warranty" -User "Kari" -AccessRights "Full Access"  
-InheritanceType all
```

```
Enable-MailUser -Identity Wriju -ExternalEmailAddress wriju@contoso.com
```

```
New-MailContact -Name Marc -ExternalEmailAddress marc@contoso.com
```

```
Set-MailUser -Identity Wriju -DisplayName "Wriju Ghosh (Contoso Ltd.)"
```

```
New-MailUser -Name "Wriju Ghosh" -ExternalEmailAddress wriju@contoso.com -Password  
(ConvertTo-SecureString -String 'Dr. Pepper had 20 ounces.' -AsPlainText -Force)
```

```
New-DistributionGroup -Name "Azure Admins"
```

```
New-DistributionGroup -Name "Azure RMS Admins" -HiddenFromAddressListsEnabled $True
```

```
Set-DistributionGroup -Name "Canadian Sales" -MemberJoinRestriction Open
```

```
New-DistributionGroup -Name "Azure RMS Admins" -ModeratedBy "Kari" -ModerationEnabled $True -RequireSenderAuthenticationEnabled $False
```

```
New-Mailbox -Name Wriju -LinkedMasterAccount "Wriju Ghosh" -LinkedDomainController  
"DC-01.tailspintoys.com" -LinkedCredential :(Get-Credential TAILSPINTOYS\ITAdmin)
```

**New-Mailbox -PublicFolder -Name PFMB1**

New-PublicFolder -Name "Company Communications"

```
Add-RoleGroupMember -Identity "Public Folder Management" -Member Kari
```

```
Add-PublicFolderClientPermission -Identity "\Corporate\HR" -AccessRights PublishingEditor -User Kari
```

```
Add-ADPermission -Identity Warranty -User Kari -ExtendedRights "Send As"
```

```
Set-Mailbox -Identity Warranty@adatum.com -GrantSendOnBehalfTo Kari@adatum.com
```

```
Add-MailboxFolderPermission -Identity kari@adatum.com:\HR -User marc@adatum.com  
-AccessRights ReadItems
```

```
Add-MailboxFolderPermissions -Identity kari@adatum.com:\Inbox -User marc@adatum.com  
-AccessRights Author
```

```
Add-MailboxPermission -Identity "Brian" -User "Kari" -AccessRights ReadPermission
```

```
Set-CalendarProcessing -Identity "Building 1 Sales Room" -ResourceDelegates "Kari"
```

```
Set-CalendarProcessing -Identity "Building 2 Board Room" -MaximumDurationInMinutes 180
```

```
Set-CalendarProcessing -Identity "Building 3 Tech Room" -AutomateProcessing None
```

```
Add-MailboxPermission -Identity Warranty -User Kari -AccessRight FullAccess  
-InheritanceType All -Automapping $false
```

```
Add-PublicFolderClientPermission -Identity "\Corporate Communications" -User Kari  
-AccessRights CreateItems
```

```
Add-PublicFolderClientPermission -Identity "\Corporate Communications" -User Kari  
-AccessRights Author
```

CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Organization Name>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Root Domain>,DC=<Your domain suffix>

```
setup.exe /NewProvisionedServer:EX02 /IAcceptExchangeServerLicenseTerms
```

```
New-ManagementRole -Name "Scripts" -UnScopedTopLevel
```

```
Add-ManagementRoleEntry Role\ProtocolCheck.ps1 -Type Script -UnscopedTopLevel
```

```
Add-ManagementRoleEntry SecurityRole\Get-Compliancecheck -PSSnapinName Adatum.Security.  
Cmdlets -UnscopedTopLevel
```

```
$Password = ConvertTo-SecureString "Pleasenottrytobuy1,000shares" -AsPlainText  
-Force  
  
Get-BitLockerVolume -MountPoint G: | Enable-BitLocker -PasswordProtector -Password  
$Password
```

```
New-OutlookProtectionRule -Name "Mergers" -SentTo mergers@adatum.com  
-ApplyRightsProtectionTemplate "Mergers and Acquisitions"
```

```
Set-IRMConfiguration -TransportDecryptionSetting Mandatory
```

```
Set-IRMConfiguration -JournalReportDecryptionEnabled $true
```

```
Set-IRMConfiguration -SearchEnabled $true
```

```
Set-IRMConfiguration -EdiscoverySuperUserEnabled $true
```

```
#Viewing the list of DLP policy templates using PowerShell
```

```
[PS] C:\>Get-DlpPolicyTemplate | Select Name
```

Name

----

Australia Financial Data

Australia Health Records Act (HRIP Act)

Australia Personally Identifiable Information (PII) Data

Australia Privacy Act

Canada Financial Data

Canada Health Information Act (HIA)

Canada Personal Health Act (PHIPA) - Ontario

Canada Personal Health Information Act (PHIA) - Manitoba

Canada Personal Information Protection Act (PIPA)

Canada Personal Information Protection Act (PIPEDA)

Canada Personally Identifiable Information (PII) Data

France Data Protection Act

France Financial Data

France Personally Identifiable Information (PII) Data

Germany Financial Data

Germany Personally Identifiable Information (PII) Data

Israel Financial Data

Israel Personally Identifiable Information (PII) Data  
Israel Protection of Privacy  
Japan Financial Data  
Japan Personally Identifiable Information (PII) Data  
Japan Protection of Personal Information  
PCI Data Security Standard (PCI DSS)  
Saudi Arabia - Anti-Cyber Crime Law  
Saudi Arabia Financial Data  
Saudi Arabia Personally Identifiable Information (PII) Data  
U.K. Access to Medical Reports Act  
U.K. Data Protection Act  
U.K. Financial Data  
U.K. Personal Information Online Code of Practice (PIOCP)  
U.K. Personally Identifiable Information (PII) Data  
U.K. Privacy and Electronic Communications Regulations  
U.S. Federal Trade Commission (FTC) Consumer Rules  
U.S. Financial Data  
U.S. Gramm-Leach-Bliley Act (GLBA)  
U.S. Health Insurance Act (HIPAA)  
U.S. Patriot Act  
U.S. Personally Identifiable Information (PII) Data  
U.S. State Breach Notification Laws  
U.S. State Social Security Number Confidentiality Laws

#Creating a new DLP policy from a template in PowerShell

```
[PS] C:\>New-DlpPolicy -Name "My DLP Policy" -Template "U.S. Financial Data" -Mode Audit
```

#Creating a new retention policy in PowerShell

[PS] C:\>New-RetentionPolicy -Name "Custom MRM Policy"

```
#Creating a 1-year archive retention tag in PowerShell
```

```
[PS] C:\>New-RetentionPolicyTag -Name DPT-Archive-1Year -Type All -AgeLimitForRetention  
365 -RetentionAction MoveToArchive
```

#Creating a 7-year deletion retention tag in PowerShell

```
[PS] C:\>New-RetentionPolicyTag -Name DPT-Delete-7Years -Type All -AgeLimitForRetention  
2557 -RetentionAction DeleteAndAllowRecovery
```

```
#Creating a voicemail message retention tag in PowerShell
```

```
[PS] C:\>New-RetentionPolicyTag -Name DPT-VoicemailDelete-30Days -Type All -MessageClass Voicemail -AgeLimitForRetention 30 -RetentionAction DeleteAndAllowRecovery
```

```
#Configuring the retention tags for a retention policy
```

```
[PS] C:\>Set-RetentionPolicy -Identity "Custom MRM Policy" -RetentionPolicyTagLinks  
"DPT-Archive-1Year","DPT-Delete-7Years"
```

```
[PS] C:\>$tags = @(Get-RetentionPolicy -Identity "Custom MRM Policy").  
RetentionPolicyTagLinks.Name  
  
[PS] C:\>$tags += "DPT-VoiceMailDelete-30Days"  
[PS] C:\>$tags += "1 Month Delete"  
[PS] C:\>$tags += "Never Delete"  
  
[PS] C:\>Set-RetentionPolicy -Identity "Custom MRM Policy" -RetentionPolicyTagLinks  
$tags
```

#Assigning a retention policy using PowerShell

```
[PS] C:\>Set-Mailbox Alex.Darrow@contoso.com -RetentionPolicy "Custom MRM Policy"
```

```
#Adding a role to an assignment policy with PowerShell
```

```
[PS] C:\>New-ManagementRoleAssignment -Name "MyRetentionPolicies-Default Role Assignment Policy" -Role MyRetentionPolicies -Policy "Default Role Assignment Policy"
```

#Processing a mailbox with the Managed Folder Assistant

[PS] C:\>Start-ManagedFolderAssistant -Identity Alex.Darrow@contoso.com

```
#Configuring a retention hold on a mailbox using PowerShell  
[PS] C:\>Set-Mailbox kim.akers@contoso.com -RetentionHoldEnabled $true  
-StartDateForRetentionHold 6/1/2016 -EndDateForRetentionHold 2/1/2017
```

#Creating an archive mailbox for an existing mailbox user

```
[PS] C:\>Enable-Mailbox Kim.Akers@contoso.com -Archive -ArchiveDatabase (Get-Mailbox  
Kim.Akers@contoso.com).Database
```

```
#Enabling a remote archive for an on-premises mailbox user
```

```
[PS] C:\>Enable-Mailbox -Identity Ben.Smith -RemoteArchive -ArchiveDomain contoso.  
mail.onmicrosoft.com
```

#Adding a member to the Discovery Management role group

```
[PS] C:\>Add-RoleGroupMember -Identity "Discovery Management" -Member Jim.Daly@contoso.com
```

```
[PS] C:\>New-RoleGroup -Name "Mailbox Search Admins" -Description "Users who can perform  
Mailbox Searches"  
[PS] C:\>New-ManagementRoleAssignment -Name "Mailbox Search Admins" -SecurityGroup  
"Mailbox Search Admins" -Role "Mailbox Search"  
[PS] C:\>Add-RoleGroupMember -Identity "Mailbox Search Admins" -Member jim.daly@contoso.  
com
```

#Creating an eDiscovery search using PowerShell

```
[PS] C:\> New-MailboxSearch "Case ID 7001" -SourceMailboxes "Human Resources"  
-TargetMailbox "Discovery Search Mailbox" -SearchQuery '"project report" OR reports OR  
report' -MessageTypes Email
```

```
#Configuring a mailbox search to retrieve estimated results
```

```
[PS] C:\> Set-MailboxSearch "Case ID 7001" -EstimateOnly $true -ExcludeDuplicateMessages  
$false
```

```
#Retrieving the estimated results for an eDiscovery search  
[PS] C:\>Get-MailboxSearch "Case ID 7001" | Select Result*
```

```
ResultNumber          : 0  
ResultNumberEstimate : 3  
ResultSize           : 0 B (0 bytes)  
ResultSizeEstimate   : 472.6 KB (483,960 bytes)  
ResultSizeCopied     : 0 B (0 bytes)  
ResultsLink          :
```

```
#Creating a new compliance search in PowerShell
```

```
[PS] C:\>New-ComplianceSearch -Name "Remove fake invoice malware" -ExchangeLocation all  
-ContentMatchQuery 'subject:"Your invoice is attached"'
```

#Reviewing the results of a compliance search

```
[PS] C:\>Get-ComplianceSearch -Identity "Remove fake invoice malware" | Format-List  
Items,SuccessResults
```

```
Items : 3  
SuccessResults : {Location: Alex.Darrow@contoso.com, Item count: 1, Total size: 8107,  
                 Location: Kim.Akers@contoso.com, Item count: 1, Total size: 8101,  
                 Location: Dan.Jump@contoso.com, Item count: 1, Total size: 3858,  
                 Location: Shannon.Dascher@contoso.com, Item count: 0, Total size: 0,  
                 Location: HRInbox@contoso.com, Item count: 0, Total size: 0,  
                 Location: Michael.Jurek@contoso.com, Item count: 0, Total size: 0,  
                 Location: Dave.Natsuhara@contoso.com, Item count: 0, Total size: 0,  
                 Location: Apurva.Dalia@contoso.com, Item count: 0, Total size: 0,  
                 Location: Jaka.Stele@contoso.com, Item count: 0, Total size: 0}
```

#Deleting mailbox items that were found by a compliance search

```
[PS] C:\>New-ComplianceSearchAction -SearchName "Remove fake invoice malware" -Purge  
-PurgeType SoftDelete
```

#Configuring an eDiscovery search to apply in-place hold

```
[PS] C:\>Set-MailboxSearch "Case ID 7001" -InPlaceHoldEnabled $true
```

#Applying a Litigation Hold to a mailbox

```
[PS] C:\>Set-Mailbox Kim.Akers@contoso.com -LitigationHoldEnabled $true  
-LitigationHoldDuration 3650
```

```
#Configure server to server authentication on the SharePoint 2013 server  
[PS] C:\> New-SPTtrustedSecurityTokenIssuer -Name Exchange -MetadataEndPoint  
https://mail.contoso.com/autodiscover/metadata/json/1
```

```
#Configure server to server authentication on the Exchange 2016 server
```

```
[PS] C:\...\> .\Configure-EnterprisePartnerApplication.ps1 -AuthMetadataUrl  
https://mysite.sharepoint.contoso.com/_layouts/15/metadata/json/1 -ApplicationType  
SharePoint
```

```
#View the MailTips configuration for the Exchange organization  
[PS] C:\>Get-OrganizationConfig | Select MailTips*
```

```
MailTipsAllTipsEnabled : True  
MailTipsExternalRecipientsTipsEnabled : False  
MailTipsGroupMetricsEnabled : True  
MailTipsLargeAudienceThreshold : 25  
MailTipsMailboxSourcedTipsEnabled : True
```

#Configuring a custom MailTip on a mailbox

```
[PS] C:\>Set-Mailbox "Help Desk" -MailTip "Email requests will be responded to within 24  
hours. For critical or urgent issues please dial x555 instead."
```

#Creating a new message classification using PowerShell

```
[PS] C:\>New-MessageClassification -Name CompanyConfidential -DisplayName "Company Confidential" -SenderDescription "This message contains confidential information for internal recipients only." -RecipientDescription "This message contains confidential information for internal recipients only."
```

#Creating a locale-specific message classification using PowerShell

```
[PS] C:\>New-MessageClassification -Name CompanyConfidential -DisplayName "Compañía Confidencial" -Locale es-ES -SenderDescription "Este mensaje contiene información confidencial para destinatarios internos solamente." -RecipientDescription "Este mensaje contiene información confidencial para destinatarios internos solamente."
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Policy]
"AdminClassificationPath"="C:\\LocalData\\OutlookClassifications.xml"
"EnableClassifications"=dword:00000001
"TrustClassifications"=dword:00000001
```

```
#Viewing the mailbox audit logging configuration for a mailbox using PowerShell
[PS] C:\>Get-Mailbox Kim.Akers@contoso.com | fl *audit*

AuditEnabled      : False
AuditLogAgeLimit : 90.00:00:00
AuditAdmin        : {Update, Move, MoveToDeleteItems, SoftDelete, HardDelete,
FolderBind, SendAs, SendOnBehalf, Create}
AuditDelegate     : {Update, SoftDelete, HardDelete, SendAs, Create}
AuditOwner        : {}
```

#Enabling mailbox audit logging using PowerShell

[PS] C:\>Set-Mailbox Kim.Akers@contoso.com -AuditEnabled \$true

```
#Enabling additional mailbox audit logging actions
```

```
[PS] C:\>Set-Mailbox -Identity Kim.Akers@contoso.com -AuditOwner @  
{add='SoftDelete,HardDelete'}
```

```
#Configuring a mailbox audit logging bypass
```

```
[PS] C:\>Set-MailboxAuditBypassAssociation -Identity serviceaccount@contoso.com  
-AuditBypassEnabled $true
```

#Performing a mailbox audit log search

[PS] C:\>Search-MailboxAuditLog -Identity "Kim Akers" -LogonTypes Delegate -ShowDetails

```
#Exporting mailbox audit logs to XML using PowerShell
```

```
[PS] C:\>New-MailboxAuditLogSearch -Name "Non-owners" -Mailboxes "Kim.Akers","Alex.Darrow" -LogonTypes Admin,Delegate -StatusMailRecipients administrator@contoso.com -StartDate 6/1/2016 -EndDate 6/30/2016
```

```
#Configuring administrator audit logging settings
```

```
[PS] C:\>Set-AdminAuditLogConfig -AdminAuditLogAgeLimit 180.00:00:00 -LogLevel Verbose
```

```
#Searching administrator audit logs
```

```
[PS] C:\>Search-AdminAuditLog -Cmdlets Add-MailboxPermission -UserIds Administrator@contoso.com
```

```
RunspaceId      : e90ba2ae-92a3-4fc1-a800-49a83c8a07c7
ObjectModified   : contoso.com/Company/Users/Kim Akers
CmdletName       : Add-MailboxPermission
CmdletParameters : {Identity, AccessRights, User}
ModifiedProperties: {}
Caller           : Administrator@contoso.com
ExternalAccess    : False
Succeeded         : True
Error             :
RunDate          : 6/28/2016 9:26:00 PM
OriginatingServer: NY-EXCH01 (15.01.0396.030)
Identity          : AAMkAGQ2Y2E3YTU1LTNlMjMtNDVmMC04NWUxLWEwNWQxYmE2YTc5MwBGAAAAAAA
                    v+bnz9KpATIKSyMS8Xoy/BwDQxTkFL6NQSrCV7K3dnPiAAAAAEZAADQxTkFL6NQ
                    SrCV7K3dnPiAAAbtM6DAAA=
IsValid          : True
ObjectState       : New
```

```
#Searching administrator audit logs
```

```
[PS] C:\>$results = Search-AdminAuditLog -Cmdlets Add-MailboxPermission -UserIds  
administrator@contoso.com
```

```
[PS] C:\>$results[0].CmdletParameters
```

Name	Value
---	-----
Identity	kim.akers
AccessRights	FullAccess
User	alex.darrow

```
#Creating a new administrator audit log search
```

```
[PS] C:\>New-AdminAuditLogSearch -Name "Add mailbox permissions" -Cmdlets Add-MailboxPermission -StatusMailRecipients administrator@contoso.com -StartDate 6/1/2016 -EndDate 6/28/2016
```

```
#Viewing the Hybrid configuration details
```

```
[PS] C:\>Get-HybridConfiguration
```

```
ClientAccessServers      : {}
EdgeTransportServers     : {NY-EDGE01}
ReceivingTransportServers : {}
SendingTransportServers  : {}
OnPremisesSmartHost     : mail.contoso.com
Domains                 : {contoso.com}
Features                : {FreeBusy, MoveMailbox, Maitips, MessageTracking,
                           OwaRedirection, OnlineArchive, SecureMail, Photos}
ExternalIPAddresses      : {}
TlsCertificateName       : <I>CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc,
                           C=US<S>CN=*.contoso.com,OU=IT, O=Contoso, L>New York,
                           S=NY, C=US
Name                     : Hybrid Configuration
DistinguishedName        : CN=Hybrid Configuration,CN=Hybrid Configuration,CN=Exchange
                           Server Pro,CN=Microsoft Exchange,CN=Services,
                           CN=Configuration,DC=contoso,DC=com
Identity                 : Hybrid Configuration
Guid                     : 680b1e2e-8d39-4c6d-a471-b55f2921c107
ObjectCategory           : contoso.com/Configuration/Schema/ms-Exch-Coexistence-
                           Relationship
ObjectClass               : {top, msExchCoexistenceRelationship}
Id                       : Hybrid Configuration
OriginatingServer         : NY-DC01.contoso.com
IsValid                  : True
ObjectState               : Unchanged
```

```
#Looking up MX records using PowerShell
```

```
PS C:\> Resolve-DnsName -Name contoso.com -Type MX
```

```
Name      : contoso.com
Type      : MX
TTL       : 3600
NameExchange : mail.global.frontbridge.com
Preference   : 10
```

#Viewing client protocol configuration for a mailbox

```
[PS] C:\> Get-CASMailbox alan.reid | Select *enabled  
ActiveSyncEnabled : True  
OWAEnabled : True  
OWAforDevicesEnabled : True  
ECPEnabled : True  
PopEnabled : True  
ImapEnabled : True  
MAPIEnabled : True  
UniversalOutlookEnabled : True  
EwsEnabled : True
```

```
#Configure the synchronization service account password to never expire  
PS C:\> Set-MsolUser -UserPrincipalName  
(Get-MsolCompanyInformation).DirSyncServiceAccount  
-PasswordNeverExpires $true
```

```
#Get the federated domain proof key value
```

```
[PS] C:\>Get-FederatedDomainProof -DomainName contoso.com
```

#Assigning a sharing policy to a mailbox

[PS] C:\>Set-Mailbox Kim.Akers@contoso.com -SharingPolicy CustomSharingPolicy

```
#PowerShell commands to update the federation trust certificate
```

```
[PS] C:\>New-ExchangeCertificate -SubjectName CN=Federation -SubjectKeyIdentifier Federation -PrivateKeyExportable $true
```

Thumbprint	Services	Subject
----- 101FED04D972957ED7C5F545FFCF9D0C0667725F	....S..	CN=Federation

```
[PS] C:\>Set-FederationTrust -Identity "Microsoft Federation Gateway" -Thumbprint  
101FED04D972957ED7C5F545FFCF9D0C0667725F
```

```
#PowerShell commands to publish the new federation certificate
```

```
[PS] C:\>Set-FederationTrust -Identity "Microsoft Federation Gateway"  
-PublishFederationCertificate
```

```
#Querying the federation information for a remote domain
```

```
[PS] C:\>Get-FederationInformation -DomainName fabrikam.com
```

```
RunspaceId          : 48d6028c-8cde-4648-9bc7-f16901232518
TargetApplicationUri : FYDIBOHF25SPDLT.fabrikam.com
DomainNames         : {fabrikam.com}
TargetAutodiscoverEpr : https://autodiscover.fabrikam.com/autodiscover/autodiscover.svc/
WSSecurity
TokenIssuerUris     : {urn:federation:MicrosoftOnline}
Identity            :
IsValid             : True
ObjectState          : Unchanged
```

```
#Retrieve Autodiscover information
```

```
[PS] C:\>Get-ClientAccessService -Identity NY-EX2010 | Select Autodiscover*
```

```
AutoDiscoverServiceCN      : NY-EX2010
AutoDiscoverServiceClassName : ms-Exchange-AutoDiscover-Service
AutoDiscoverServiceInternalUri : https://mail.contoso.com/Autodiscover/Autodiscover.xml
AutoDiscoverServiceGuid     : 77378f46-2c66-4aa9-a6a6-3e7a48b19596
AutoDiscoverSiteScope       : {NewYork,Chicago,Boston}
```

#Configuring the Autodiscover service connection point

```
[PS] C:\>Set-ClientAccessService -Identity NY-EXCH01 -AutoDiscoverServiceInternalUri  
https://autodiscover.contoso.com/Autodiscover/Autodiscover.xml
```

```
#Configuring the Autodiscover Site Scope  
[PS] C:\>$SiteScope = (Get-ClientAccessService -Identity NY-EXCH01).  
AutodiscoverSiteScope  
  
[PS] C:\>$SiteScope  
NewYork  
  
[PS] C:\>$SiteScope.Add("Chicago")  
[PS] C:\>$SiteScope.Add("Boston")  
  
[PS] C:\>Set-ClientAccessService -Identity NY-EXCH01 -AutoDiscoverSiteScope $SiteScope  
  
[PS] C:\>Get-ClientAccessService -Identity NY-EXCH01 | Select Auto*  
  
AutoDiscoverServiceCN : NY-EXCH01  
AutoDiscoverServiceClassName : ms-Exchange-AutoDiscover-Service  
AutoDiscoverServiceInternalUri : https://autodiscover.contoso.com/Autodiscover/  
Autodiscover.xml  
AutoDiscoverServiceGuid : 77378f46-2c66-4aa9-a6a6-3e7a48b19596  
AutoDiscoverSiteScope : {NewYork, Chicago, Boston}
```

```
#Retrieve the Outlook Anywhere settings using PowerShell
```

```
[PS] C:\>Get-OutlookAnywhere -Server NY-EX2013 | Select InternalHostname,ExternalHostname,*auth*,*ssl*
```

```
InternalHostname : mail.contoso.com
ExternalHostname : mail.contoso.com
ExternalClientAuthenticationMethod : Ntlm
InternalClientAuthenticationMethod : Ntlm
IISAuthenticationMethods      : {Ntlm}
SSLOffloading                : True
ExternalClientsRequireSsl    : True
InternalClientsRequireSsl    : True
```

```
#Configuring Outlook Anywhere settings using PowerShell
```

```
[PS] C:\>Get-OutlookAnywhere -Server NY-EXCH01 | Set-OutlookAnywhere  
-InternalHostname mail.contoso.com -ExternalHostname mail.contoso.com  
-InternalClientAuthenticationMethod NTLM -InternalClientsRequireSsl $true  
-ExternalClientAuthenticationMethod NTLM -ExternalClientsRequireSsl $true
```

#Configuring the MAPI virtual directory using PowerShell

```
[PS] C:\>Get-MapiVirtualDirectory -Server NY-EXCH01 | Set-MapiVirtualDirectory `  
-InternalUrl https://mail.contoso.com/mapi  
-ExternalUrl https://mail.contoso.com/mapi
```

#Configuring the EWS virtual directory using PowerShell

```
[PS] C:\>Get-WebServicesVirtualDirectory -Server NY-EXCH01 |  
Set-WebServicesVirtualDirectory  
-InternalUrl https://mail.contoso.com/EWS/Exchange.asmx  
-ExternalUrl https://mail.contoso.com/EWS/Exchange.asmx
```

#Configuring the OAB virtual directory using PowerShell

```
[PS] C:\>Get-OabVirtualDirectory -Server NY-EXCH01 | Set-OabVirtualDirectory  
-InternalUrl https://mail.contoso.com/OAB  
-ExternalUrl https://mail.contoso.com/OAB
```

```
#Configuring the OWA and ECP virtual directories using PowerShell
```

```
[PS] C:\>$hostname = "mail.contoso.com"
```

```
[PS] C:\>Get-OwaVirtualDirectory -Server NY-EXCH01 | Set-OwaVirtualDirectory `  
-InternalUrl https://$hostname/owa `  
-ExternalUrl https://$hostname/owa
```

```
WARNING: You've changed the InternalURL or ExternalURL for the OWA virtual directory.
```

```
Please make the same change for the ECP virtual directory in the same website.
```

```
[PS] C:\>Get-EcpVirtualDirectory -Server NY-EXCH01 | Set-EcpVirtualDirectory `  
-InternalUrl https://$hostname/owa `  
-ExternalUrl https://$hostname/owa
```

#Configuring the ActiveSync virtual directory using PowerShell

```
[PS] C:\>Get-ActiveSyncVirtualDirectory -Server NY-EXCH01 |  
Set-ActiveSyncVirtualDirectory  
-InternalUrl https://mail.contoso.com/Microsoft-Server-ActiveSync  
-ExternalUrl https://mail.contoso.com/Microsoft-Server-ActiveSync
```

```
#Export mailbox statistics to CSV file
```

```
[PS] C:\>Get-Mailbox | Get-MailboxStatistics | Export-Csv C:\Temp\MailboxStatistics.csv
```

```
#Exclude a mailbox database from automatic provisioning
```

```
[PS] C:\>Set-MailboxDatabase -Identity DB01 -IsExcludedFromProvisioning $true
```

#Using Telnet to connect to another Exchange server

C:\>telnet ny-exch02.contoso.com 25

220 NY-EXCH02.contoso.com Microsoft ESMTP MAIL Service ready at Sun, 5 Jun 2016

20:48:17 +1000

#Configure the SMTP banner on a receive connector

[PS] C:\>Set-ReceiveConnector -Identity "NY-EXCH02\Relay" -Banner "220 NY-EXCH02\Relay"

#Reviewing the protocol logging configuration for a server

```
[PS] C:\>Get-ReceiveConnector -Server NY-EXCH02 | Select Name,ProtocolLoggingLevel
```

Name	ProtocolLoggingLevel
Default NY-EXCH02	None
Client Proxy NY-EXCH02	None
Default Frontend NY-EXCH02	Verbose
Outbound Proxy Frontend NY-EXCH02	Verbose
Client Frontend NY-EXCH02	None
Relay	None

```
[PS] C:\>Set-ReceiveConnector NY-EXCH02\Relay -ProtocolLoggingLevel Verbose
```

#Searching message tracking log files

```
[PS] C:\>Get-MessageTrackingLog -Sender Kim.Akers@contoso.com -Start (Get-Date).AddHours(-24)
```

#Moving arbitration mailboxes

[PS] C:\>Get-Mailbox -Arbitration | New-MoveRequest -TargetDatabase DB08

```
#Creating a migration batch using PowerShell
```

```
[PS] C:\>New-MigrationBatch -Local -Name MigrationBatch1 `  
-CSVData ([System.IO.File]::ReadAllBytes("C:\Migrations\batch1.csv")) `  
-AutoComplete:$false -NotificationEmails administrator@contoso.com
```

#Viewing the status of a migration batch

```
[PS] C:\>Get-MigrationUser -BatchId MigrationBatch1 | ft -auto
```

Identity	Batch	Status	LastSyncTime
Ryan.Danner@contoso.com	MigrationBatch1	Syncing	
Mike.Danseglio@contoso.com	MigrationBatch1	Syncing	
Alex.Darrow@contoso.com	MigrationBatch1	Syncing	
Shannon.Dascher@contoso.com	MigrationBatch1	Syncing	
WillsonRaj.David@contoso.com	MigrationBatch1	Syncing	
Dan.Jump@contoso.com	MigrationBatch1	Syncing	

#Reviewing move requests statistics using PowerShell

```
[PS] C:\>Get-MoveRequest "Ryan Danner" | Get-MoveRequestStatistics | Format-List
```

```
#Reviewing migration user statistics using PowerShell  
[PS] C:\> Get-MigrationUser ryan.danner@contoso.com | Get-MigrationUserStatistics |  
Format-List
```

```
#Viewing the migration batch report using PowerShell
```

```
[PS] C:\>Get-MigrationBatch -Identity MigrationBatch1 -IncludeReport | Select Report | Format-List
```