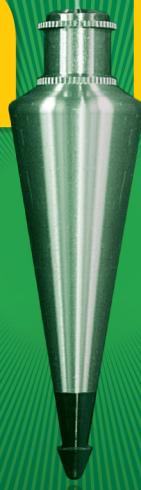
Microsoft

Designing and Deploying Messaging Solutions with Microsoft® Exchange Server 2010

Orin Thomas

MCITP

Exam Ref



EXAM

70-663

Exam Ref 70-663

Designing and Deploying Messaging Solutions with Microsoft® Exchange Server 2010

Professional-level prep for the professional-level exam.

Prepare for MCITP Exam 70-663—and help demonstrate your real-world mastery of enterprise messaging administration with Microsoft Exchange Server. Designed for experienced, MCTS-certified professionals ready to advance their status—*Exam Ref* focuses on the critical-thinking and decision-making acumen needed for success at the MCITP level.

Focus on the expertise measured by these objectives:

- Planning the Exchange Server 2010 Infrastructure
- Deploying the Exchange Server 2010 Infrastructure
- Designing and Deploying Security for the Exchange Organization
- Designing and Deploying Exchange Server 2010 Availability and Recovery
- Designing and Deploying Messaging Compliance, System Monitoring, and Reporting

Exam Ref features:

- Focus on job-role expertise
- Organized by exam objectives
- Strategic, what-if scenarios
- 15% exam discount from Microsoft. Offer expires 12/31/2016. Details inside.

CERTIFICATION

The Microsoft Certified IT Professional (MCITP) certification helps validate comprehensive skills in deploying, building, designing, optimizing, and operating technologies to ensure successful implementation projects.

JOB ROLE

The *Enterprise Messaging Administrator 2010* is responsible for Exchange Server messaging in an enterprise environment and acts as a technical lead over a team of administrators.

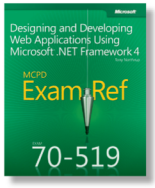
REQUIRED EXPERIENCE

Successful candidates generally have three or more years of real-world experience.

See full details at:
microsoft.com/learning/certification

MEET THE FAMILY

- Train
- Prep
- Practice



- Prep
- Optional Practice*

** Select titles coming soon*

- Review

About the Author

Orin Thomas, MCITP, MCTS, MCSE, Microsoft MVP for Consumer Security, is a consultant and author of Microsoft Press® *Training Kits* for Exams 70-662, 70-680, 70-646, and 70-647. He is also a contributing editor to *Windows® IT Pro* magazine.

ISBN: 978-0-7356-5808-0

U.S.A. $49.99
Canada $52.99
[*Recommended*]

Certification/
Microsoft Exchange Server

Microsoft® Exchange Server 2010

Microsoft®

Microsoft®

MCITP 70-663 Exam Ref:

Designing and Deploying Messaging Solutions with Microsoft® Exchange Server 2010

Orin Thomas

ISBN: 978-0-7356-5808-0

1 2 3 4 5 6 7 8 9 QG 6 5 4 3 2 1

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at *mspinput@microsoft.com*. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

Acquisitions and Developmental Editor: Ken Jones

Production Editor: Adam Zaremba

Editorial Production: S4Carlisle Publishing Services

Technical Reviewer: Ian McLean

Copyeditor: Becka McKay

Indexer: Potomac Indexing, LLC

Cover Composition: Karen Montgomery

Illustrator: S4Carlisle Publishing Services

Contents at a Glance

Contents

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/

Introduction

This Exam Ref is designed to assist you with studying for the MCITP exam 70-663, "Designing and Deploying Messaging Solutions with Microsoft Exchange Server 2010." This Exchange Server 2010 exam focuses on which technology to use to meet a particular design objective; the MCTS exam 70-662, "Microsoft Exchange Server 2010, Configuring" (*http://www.microsoft.com/learning/en/us/exam.aspx?id=70-662#tab2*) involves knowing how to configure that technology to meet a specific operational objective.

The 70-663 exam is aimed at messaging administrators in medium to large organizations. By passing the exam, you will demonstrate that you have the knowledge and experience to design complex, multi-site and multi-forest Exchange Server 2010 deployments. If you've also passed the 70-662 exam, passing this exam will earn you the MCITP: Enterprise Messaging Administrator 2010 certification.

This book will review every concept described in the following exam objective domains:

- Planning the Exchange Server 2010 Infrastructure
- Deploying the Exchange Server 2010 Infrastructure
- Designing and Deploying Security for the Exchange Organization
- Designing and Deploying Exchange Server 2010 Availability and Recovery
- Designing and Deploying Messaging Compliance, System Monitoring, and Reporting

This book covers every exam objective, but it does not necessarily cover every exam question. Microsoft regularly adds new questions to the exam, making it impossible for this (or any) book to provide every answer. Instead, this book is designed to supplement your relevant independent study and real-world experience with the product. If you encounter a topic in this book that you do not feel completely comfortable with, you should visit any links described in the text and spend several hours researching the topic further using TechNet, Exchange Server team blogs, and support forums. Ideally, you should also deploy your own complex Exchange environment. This involves deploying multiple servers across multiple sites and domains. The simplest way of doing this is to build your own virtualized lab.

Microsoft Certified Professional Program

Microsoft certifications provide the best method for proving your command of 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. Computer professionals who become Microsoft certified are recognized as experts and are sought after industry-wide. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **OTHER MICROSOFT CERTIFICATIONS**

For a full list of Microsoft certifications, go to *www.microsoft.com/learning/mcp/default.asp*.

Acknowledgments

I'd like to thank my good mate Ken Jones at O'Reilly for his support in getting the Exam Ref series off the ground. It's always a pleasure to work with Ken and I'm forever thankful for the opportunities that he presents me with as an author. Readers have Ken to thank for ensuring that Pro-level exams like 70-663 are now getting Microsoft Press coverage.

I'd also like to thank technical reviewer Ian McLean, production editor Jean Smith, production manager Dan Fauxsmith, and copy editor Rebecca McKay. Without your assistance and professionalism, the book wouldn't have come together as well as it has!

As always I'd like to thank my wife, Oksana, and son, Rooslan, for their patience with me during the writing process. I'd also like to thank Scott Schnoll for his excellent technical presentations, which really bring features such as how Exchange handles datacenter failover to life. I'd also like to thank Chris Brown for his feedback and Paul Cunningham for his great website *http://exchangeserverpro.com*.

I'd also like to thank you, the reader, for picking up this book. If you have any questions about anything and you want to get in touch with me, you can find me on twitter *http://twitter.com/OrinThomas*.

Support and Feedback

The following sections provide information on errata, book support, feedback, and contact information.

Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

http://www.microsoftpressstore.com/title/ 9780735658080

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at *mspinput@microsoft.com*.

Please note that product support for Microsoft software is not offered through the addresses above.

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://www.microsoft.com/learning/booksurvey

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in Touch

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

Preparing for the Exam

Microsoft certification exams are a great way to build your resume and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam Ref and another study guide for your "at home" preparation, and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you.

CHAPTER 1

Planning the Exchange Server 2010 Infrastructure

You have probably heard the expression "Measure twice, cut once." When it comes to the deployment of Exchange Server 2010, taking time with your organization's deployment can save you a lot of trouble later. In this chapter you'll learn about the different models for on-premises and cloud-based deployments, DNS requirements, how to translate Service Level Agreement (SLA) requirements into design decisions, and whether you need to plan Exchange federation. You'll learn how to design an appropriate topology to meet your organization's message routing requirements, design a Mailbox server deployment that is appropriate given your organization's topology, design a Client Access Server deployment to support your proposed Exchange deployment, and plan a deployment to meet any transition and coexistence requirements. This chapter is primarily about design considerations prior to deploying Exchange Server 2010. Chapter 2, "Deploying the Exchange Server 2010 Infrastructure," deals more with the specifics of configuring these technologies on the organizational network.

IMPORTANT

Have you read page xxi?

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

Objectives in this chapter:

- Objective 1.1: Design the Exchange Server 2010 installation
- Objective 1.2: Design Message routing
- Objective 1.3: Design the mailbox server role
- Objective 1.4: Design client access
- Objective 1.5: Plan for transition and coexistence

Real World

Most organizations don't get to deploy a brand new Exchange infrastructure from scratch, but instead have to perform a deployment based on the constraints imposed by an existing infrastructure. That makes the objectives in this chapter a little tricky because they involve testing your knowledge of a theoretical Exchange Server 2010 deployment rather than what you may encounter when actually deploying Exchange Server 2010. A good example of this is when I discuss preparing the schema and domains for the Active Directory deployment. As a friend of mine in the Exchange product team pointed out, it isn't actually necessary to run these commands separately because the Exchange Server 2010 installation wizard makes these preparations automatically the first time you install Exchange. If it all happens automatically, why mention it and why put it on an exam? Microsoft's aim in testing this knowledge on the exam is to ensure that you have an understanding of what is going on in the background—so you understand how the schema and domains are prepared even if you do just decide to run the installation wizard instead of carefully going through the Active Directory preparation first.

EXAM TIP

In reality crafting an Exchange design involves dealing with nuance and complexity, but actual exam questions are in a multiple-choice format where answers are either right or wrong. In reality some answers are better than others. If, in the exam, you have an option where it seems as though two answers could be right, but you can only choose one answer as correct, you've likely missed a clue in the question text that would allow you to discard one of these answers. This is because when exams are authored, not only does the question writer have to provide good reasons why one answer is correct, but he also has to provide good reasons as to why the other answers are incorrect. Although there is a small chance that you've come across a bad question that got through proofreading and peer review, it's more likely that in a stressful exam situation you've overlooked a vital bit of evidence that discounts an answer you suspect is correct.

Objective 1.1: Design the Exchange Server 2010 Installation

Microsoft provides guidance for IT professionals on the factors they should consider when planning to deploy Exchange Server 2010. In this objective you'll learn about the factors you need to consider when planning your Exchange deployment. In Chapter 2, "Deploying the Exchange Server 2010 Infrastructure," you'll learn about the practical steps you need to take to perform an Exchange Server 2010 deployment.

This objective covers:

- Define Exchange server locations.
- Determine Exchange DNS requirements.
- Consider SLA requirements.
- Consider Network and Active Directory site topologies.
- Plan for Exchange federation.
- Consider complex Active Directory requirements.
- Understand the Exchange Deployment Assistant.

Choosing Exchange Server Locations

You can choose between three general Exchange design options when deploying Exchange Server 2010: an on-premises deployment, a cloud deployment, or a coexistence deployment. In the real world, decisions about whether to go with an on-premises or cloud-based deployment are rarely technical in nature. These decisions are usually driven by business needs and cost and you are unlikely to encounter a question on the 70-663 exam that directly asks you whether a cloud-based or on-premises deployment is appropriate. You are more likely to be asked about what design considerations are involved if it becomes necessary to configure your organization to support an on-premises and cloud-based coexistence scenario. You'll need to know what steps you'd need to take to get such a deployment working, not whether an organization would be better off shunting everything to the cloud or keeping everything in-house.

On-Premises Deployments

The 70-663 exam primarily deals with the design of on-premises Exchange Server 2010 deployments and infrastructure. In part this is because a lot less design work is required if you go with an entirely cloud-based Exchange deployment than there is in deciding where to place hub transport, client access, and mailbox servers on a per-site basis. The focus is on local deployments because the vast majority of organizations who use Exchange still choose to go with on-premises rather than coexistence or entirely cloud-based deployments.

When choosing where to place Exchange servers, you need to take into account issues such as number of mailboxes, server capacity, and available bandwidth. While it might be possible to place an Exchange server that hosts the mailbox, client access, and hub transport server roles at each location, even in the biggest organizations such an approach isn't always necessary. For example, one multinational company I know of has approximately 2,000 employees spread across the capital cities of Australia and another 500 or so in New Zealand. All of these employees use Exchange servers hosted in Singapore and there is no local Exchange deployment. Each office has local domain controllers and global catalog servers to handle authentication, but the client access, hub transport, and mailbox servers are thousands of miles away in another country.

Cloud-Only Deployments

A completely cloud-based deployment involves your organization's Exchange server being hosted online, most likely through Exchange Online, which is a part of Microsoft Office 365. Cloud-only deployments have the following characteristics:

- The cloud-based Exchange deployment is completely separate from any local on-premises messaging system.
- Users need separate credentials to authenticate and access their cloud-hosted mailboxes.
- The local Active Directory infrastructure does not synchronize with the cloud-based deployments. User mailboxes and distribution groups are administered independently of any local on-premises mailbox and distribution groups.

Cloud-only deployments are often used for new organizations or organizations that want to move from a third-party mail system to a cloud-based Exchange mail system.

> ***MORE INFO*** **UNDERSTANDING CLOUD-ONLY DEPLOYMENTS**
>
> **For more information on cloud-only deployments, consult the following TechNet webpage: *http://technet.microsoft.com/en-us/library/gg583832.aspx*.**

Coexistence

Coexistence deployments involve both an on-premises Exchange deployment and a cloud-hosted Exchange deployment. Coexistence is generally used when an organization wants to transition from an existing Exchange Server 2003 or Exchange Server 2007 deployment to an entirely cloud-hosted Exchange 2010 deployment, though it is possible to configure coexistence between a local Exchange 2010 deployment and a cloud-hosted Exchange 2010 deployment as well.

When you deploy Exchange in a coexistence configuration, you need to deploy an on-premises coexistence server. A coexistence server is a computer running Exchange Server 2010 that you configure with the necessary Exchange Server 2010 roles that allow it to manage communication between the on-premises Exchange deployment and the cloud-based deployment. You also need to configure a directory synchronization server. This server synchronizes account information between the local and hosted Exchange deployments.

Hosted Exchange 2010 supports two types of coexistence. The difference between these is as follows:

- **Simple coexistence** Provides a unified Global Address List (GAL) and mail routing between the local and hosted Exchange organization.
- **Rich coexistence** Provides a unified GAL, mail routing, sharing availability information, and the ability to move mailboxes between the local and hosted Exchange organization. Rich coexistence requires that you configure a federation trust with the Microsoft Federation Gateway.

MORE INFO **COEXISTENCE**

To learn more about coexistence, consult the following page on TechNet: *http://technet.microsoft.com/en-us/library/gg476106.aspx*.

Planning Exchange DNS Support

Although it is possible to use Active Directory and Exchange with a third-party DNS solution such as BIND, doing so requires substantial administrative overhead. Microsoft recommends that you use Active Directory–integrated DNS zones to support your internal Active Directory and Exchange name resolution requirements. You should configure Active Directory–integrated zones to accept secure dynamic updates only, you should enable scavenging, and you should configure DNS zones to replicate to all domain controllers in the forest. Configuring DNS in this way ensures that internal DNS is updated appropriately when you introduce new servers hosting Exchange Server 2010 roles into your Active Directory environment.

Many organizations split the hosting of their externally resolvable DNS hosts from their internal DNS. For example, an organization might use the contoso.com Active Directory Integrated DNS zone to support the contoso.com forest. The problem is that while it will be fine for external clients to resolve hostnames like www.contoso.com and smtp.contoso.com, most organizations would not want internal host names such as SYD-FS1.contoso.com and SYD-EX1.contoso.com to be resolvable by hosts on the Internet.

You can deal with the problem by configuring DNS delegation to point to an externally hosted DNS zone that only holds records that you want available to hosts on the Internet, such as the host and MX records that point to your organization's SMTP server. A separate internal DNS infrastructure holds all records that should be accessible to internal hosts.

Rather than having the same zone hosted in two different locations, another option is to configure a split DNS namespace, where your organization's internal DNS domain name is a delegated sub-domain of the external DNS namespace. For example, the external DNS namespace might be adatum.com and the internal DNS namespace be configured as corp.adatum.com. When taking this approach it is necessary to ensure that you configure the root

domain as an accepted domain, so that recipients can receive email using the root domain as their mail domain. For example, being able to accept email @adatum.com rather than only at @corp.adatum.com.

> ***MORE INFO*** **SECURE DNS DEPLOYMENT**
>
> **For more information on securing DNS deployment, consult the following TechNet webpage: *http://technet.microsoft.com/en-us/library/cc770636(WS.10).aspx*.**

Common Shared Namespace

Some organizations use multiple mail systems, but only have a single address space. For example, an email message sent to kim.akers@contoso.com might need to be routed to an Exchange Server 2010 mailbox, whereas an email message to sam.abolrous@contoso.com might need to be routed to a mailbox hosted on a third-party messaging system. You can solve this design challenge within Exchange by configuring what is known as an *internal relay domain* and then creating a send connector to route email to the shared domain.

> ***MORE INFO*** **SHARED ADDRESS SPACE**
>
> **To learn more about configuring Exchange to route messages for a shared address space, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb676395.aspx*.**

Disjointed Namespace

A disjointed namespace exists when the primary DNS suffix of a computer does not match the DNS domain name of the domain of which the computer is a member. Microsoft supports three different scenarios for deploying Exchange in an environment where there is a disjointed namespace:

- The primary DNS suffix of all domain controllers differs from the DNS domain name. Computers that are members of this domain may or may not be disjointed. In this situation, you can have Exchange servers that use either the primary DNS suffix or the DNS domain name.
- One or more member computers in the domain have primary DNS suffixes that differ from the DNS domain name even though all domain controllers are not disjointed. In this situation, you can have Exchange servers that use either the primary DNS suffix or the DNS domain name.
- The NetBIOS name of domain controllers differs from the subdomain of the DNS domain name of those domain controllers. For example, the NetBIOS name might be SOUTHPACIFIC, but the primary DNS suffix and the DNS domain name might be contoso.com.

For servers running Exchange Server 2010 to have access to domain controllers in environments that have a disjointed namespace, it is necessary to modify the *msDS-AllowedDNSSuffixes* Active Directory attribute on the domain object container so that it includes both the DNS domain name and the primary DNS suffix, as shown in Figure 1-1.

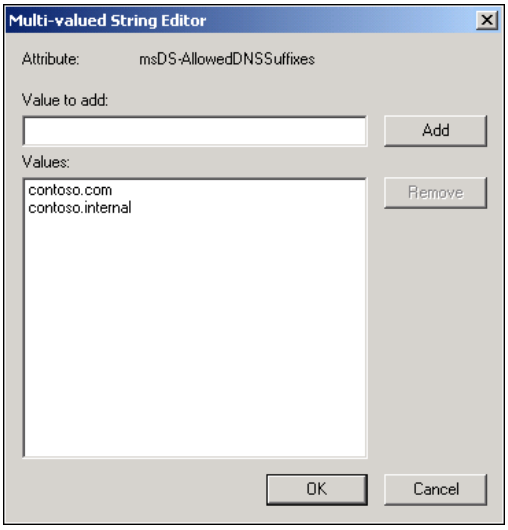


FIGURE 1-1 msDS-AllowedDNSSuffixes

You also need to ensure that the DNS suffix search list for computers includes all DNS namespaces used within your organization. This can be done by configuring the DNS Suffix Search List group policy item, located in the Computer Configuration\Policies\Administrative Templates\Network\DNS Client node.

To view the primary DNS suffix and DNS domain name of a computer running Windows Server 2008 or Windows Server 2008 R2, click the Computer Name tab of the System Properties dialog box, as shown in Figure 1-2. In the figure the namespace is disjointed as the primary DNS suffix is adatum.internal where the domain name is adatum.com.

MORE INFO **DISJOINTED NAMESPACE SCENARIOS**

To learn more about disjointed namespace scenarios, consult the following TechNet document: *http://technet.microsoft.com/en-us/library/bb676377.aspx*.

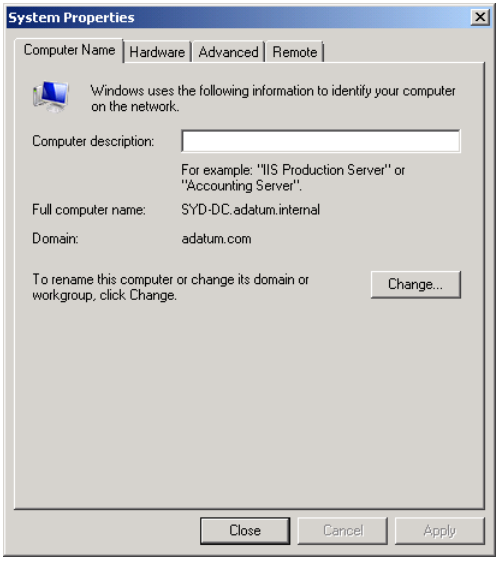


FIGURE 1-2 Disjointed namespace

Service Level Agreement Considerations

A Service Level Agreement (SLA) is an arrangement between the IT service provider and an organization that specifies measurable infrastructure performance levels. Although SLAs vary from organization to organization, they most commonly include goals related to the following service characteristics:

- **Availability** A way of defining how reliable the service is in terms of the amount of time the service may be unavailable in a given period. For example, an SLA might specify that Exchange has an allowable downtime for planned maintenance and unplanned faults for a total of five hours a month.
- **Performance** A way of defining minimum performance characteristics of the infrastructure. For example, an SLA might specify a maximum number of concurrent connections to a mailbox server. Performance may influence your design with relation to the hardware specifications of servers hosting Exchange.
- **Recovery** This is a way of defining how quickly data or services can be recovered in the event of an outage. For example, an SLA might specify a maximum recovery time for deleted mailbox items. Recovery objectives influence the data protection technologies that you include in your Exchange design.

You must explicitly define each performance characteristic in the SLA. For example, you might be designing an Exchange deployment for an organization that has a head office and two branch offices. The branch offices are so small that you decide not to deploy Exchange at

those sites, but instead have users connect to Exchange servers located at the head office site. If the site link between the head office and one of the branch office sites fails, blocking access to Exchange for the users at that branch office site, but all other users in the organization are able to access the centrally located Exchange servers, how will that outage be measured by the terms of the SLA?

Internal SLAs are arrangements between an organization's IT department and business units within the organization. In most organizations, internal SLAs tend to be less formal and the performance metrics less explicitly defined. External SLAs are contracts created between the organization and a third-party provider, such as a cloud service provider. External SLAs tend to be a lot more complicated and are generally legally binding contracts including cost, bonus, and penalty clauses. External SLAs are increasingly important for organizations that use a hybrid approach to their Exchange deployment, with some services hosted internally and other services hosted in the public cloud.

When you have an SLA in place, you will need to regularly attend to certain ongoing tasks, including:

- **Service catalog maintenance** A service catalog defines the services provided to the organization. It provides detailed descriptions of the service components and the IT functionality utilized by the business. You need to ensure that this is both comprehensive and up to date.
- **Service level monitoring** It is important to have a monitoring solution in place that verifies that the IT service provider is complying with the conditions of the SLA. Products such as System Center Operations Manager 2012 are designed to monitor Exchange Server 2010 deployments.
- **Service level reporting** You should regularly generate and distribute reports. These reports should describe metrics related to the performance levels specified in the SLA. SLA objectives must be specific and measurable. If you cannot measure an SLA objective, it is impossible to impartially determine whether that objective has been met. Having an SLA objective that is open to interpretation can lead to disagreements between the IT department and the organization as to whether the objective has been met.
- **SLA review** Plan to review the SLA periodically with all involved stakeholders. Use these reviews to determine whether you should modify the SLA to better meet the needs of the organization.

You should have an SLA in place before you complete the Exchange design process. Knowing what goals you need to meet allows you to ensure that your Exchange design suits the needs of your organization. For example, you might meet availability requirements by deploying multiple hub transport servers at each site, using Database Availability Groups and Client Access Server arrays. The terms of the SLA also impact the cost of the deployment. It is important to ensure that the terms of the SLA are realistic given the budgets involved. You can't realistically provide highly available redundant Exchange servers if your budget only allows you to deploy a single computer running Exchange at one central site.

MORE INFO **SYSTEM CENTER SERVICE MANAGER**

System Center Service Manger is Microsoft's service desk solution. You can configure the product to provide reports that detail how well an IT department is meeting the objectives laid out in the SLA. You can find out more about System Center Service Manager at *http://www.microsoft.com/systemcenter/en/us/service-manager.aspx*.

Active Directory and Network Topology

Exchange Server 2010 generates its network topology information by querying Active Directory for site information. Each Active Directory site is defined as a collection of IPv4 or IPv6 networks. Usually that collection is a single local high-speed network. Most organizations have configured Active Directory so that each physical location is its own distinct Active Directory site. For example, you might have one site that represents a branch office at Sydney and another site that represents a branch office in Melbourne. As Active Directory does not automatically create additional sites, you may occasionally encounter organizations where Active Directory hasn't been properly maintained and there is only one site even though the organization itself is spread across multiple branch offices.

By using the Active Directory site topology, Exchange can determine how to transport messages and which global catalog servers and domain controllers should be used for processing Active Directory queries. When deploying Exchange, you don't need to worry about configuring routing topologies—this is all handled by using the Active Directory site topology. The only exception to this is if you are introducing Exchange 2010 into an environment that has Exchange 2003.

When considering your Exchange design, you should ensure that your organization's Active Directory site configuration is appropriate and reflects the realities of your organization's network infrastructure. At a minimum this means ensuring that IP networks at each branch office site are associated with and appropriate site within Active Directory. You associate IP networks with Active Directory sites by using the Active Directory Sites and Services console.

MORE INFO **ACTIVE DIRECTORY SITES**

For more information on planning to use Active Directory sites for routing Exchange Server 2010 messages, consult the following TechNet document: *http://technet.microsoft.com/en-us/library/aa996299.aspx*.

Multiple Domains

Exchange is designed to be deployed and used in multiple domains across a single forest. A single Exchange organization can span a forest that has a single or multiple domain trees. That means that you can have one Exchange organization supporting domains with different names, such as wingtiptoys.com and tailspintoys.com, as long as those domains are a part of the same Active Directory forest.

If you do have multiple domain trees in your forest, you might want to configure Exchange to accept email for more than one authoritative domain. That means that you can design a single Exchange organization so that it will be able to receive and process email for separate mail domains representing different trees in the same forest, such as wingtiptoys.com and tailspintoys.com, as long as Exchange has been properly configured. You configure accepted domains on transport servers. You will learn more about configuring accepted domains in Chapter 2.

MORE INFO **GAL SEGMENTATION**

Exchange Server 2010 service pack 2 will support GAL segmentation. GAL segmentation allows you to create smaller address lists on a per-domain or per-domain tree basis rather than including all addresses in an Exchange organization. To find out more about GAL segmentation, consult the following Exchange product team blog article at: *http://blogs.technet.com/b/exchange/archive/2011/01/27/3411882.aspx*.

Multiple Forests

Some organizations have more than one Active Directory forest, with trust relationships configured between forests to allow users who have accounts in one forest to access resources in another forest. As you are aware, a single Exchange Server 2010 organization can only span a single forest. If your organization has more than one forest, you will need to use one of the supported multiple forest topologies when you create your deployment design. Exchange Server 2010 supports the following multiple forest topologies:

- **Cross-forest** The cross-forest topology involves multiple Active Directory forests with an Exchange Server 2010 organization in each forest. When designing an Exchange deployment to support a cross-forest topology you need to configure recipient synchronization so that the GAL in each forest holds information for recipients in all forests. You also need to configure the Availability service so that users in each forest are able to view availability information for users in all of your organization's other forests.

- **Resource-forest** The resource-forest topology involves one Active Directory forest that has Exchange deployed and other Active Directory forests that host user accounts. In the resource-forest model, the forest that hosts Exchange often does not host user accounts and the accounts which have Exchange mailboxes are disabled. At least one forest that does not have an Exchange organization must host user accounts. Disabled user accounts in the forest that hosts Exchange are associated with user accounts in the account forest.

MORE INFO **MULTIPLE-FOREST TOPOLOGIES**

To learn more about supporting multiple-forest topologies with Exchange Server 2010, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb124734.aspx*.

Microsoft recommends that you use a product such as Forefront Identity Lifecycle Manager (ILM) 2010 to ensure that the GAL in each forest in a cross-forest Exchange topology contains all the mail recipients from other forests. Enabling GAL synchronization requires that you create management agents that import mail-enabled groups, contacts, and users into a centralized metadirectory where they are represented as mail users. The management agents then synchronize these mail users to a specially configured OU in each target forest.

MORE INFO **PLANNING ACTIVE DIRECTORY**

To learn more about preparing Active Directory for the deployment of Exchange, consult the following webpage: *http://technet.microsoft.com/en-us/library/bb123715.aspx*.

Directory Synchronization with the Cloud

Active Directory synchronization allows you to configure an ongoing relationship between your organization's Active Directory infrastructure and a cloud service provider such as Office 365. Microsoft recommends that you configure single sign-on prior to setting up directory synchronization. Single sign-on allows a user to log on to cloud service providers, such as Office 365, using their organizational credentials. If single sign-on is not configured, it will be necessary to add and verify your organization's domains, and local password changes will not be synchronized with the hosted Exchange organization.

To configure your organization to support single sign-on, you need to take the following general steps:

1. Ensure that your organization's forest functional level is set to Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2.
2. Ensure that the domain that you will be federating can be resolved by hosts on the Internet.

3. Configure User Principle Names (UPNs) for all users. UPNs used for single sign-on can only contain letters, numbers, periods, dashes, and underscore characters. The UPN domain suffix must be a publicly registered domain. Microsoft recommends using a user's email domain as her account's UPN suffix.

4. Deploy Active Directory Federation Services (AD FS) 2.0. AD FS is required to support single sign-on to cloud service providers such as Office 365. Microsoft recommends deploying two federation services in a load balanced configuration. Federation server proxies will be required if you want to support roaming clients or smartphone access to hosted Exchange.

> ***MORE INFO*** **DEPLOY AD FS TO SUPPORT HOSTED EXCHANGE**
>
> **To learn more about deploying AD FS to support Hosted Exchange, consult the following article: *http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff652539.aspx*.**

5. Install and configure the Microsoft Online Services Module for Windows PowerShell for Single Sign On. This module requires a host running Windows 7 or Windows Server 2008 R2 with the Microsoft .NET Framework 3.51 feature enabled.

6. Each domain that you want to synchronize with the cloud service provider must be added as a single sign-on domain or converted to become a single sign-on domain. To perform this conversion you use the *Connect-MsolService*, *Set-MsolAdfscontext*, and *Convert-MsolDomainToFederated* cmdlets.

> ***MORE INFO*** **MICROSOFT ONLINE SERVICES MODULE FOR WINDOWS POWERSHELL**
>
> **To learn more about the Microsoft Online Services Module for Windows PowerShell, consult the following webpage: *http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff652560.aspx*.**

Once you have configured single sign-on, you will need to designate a computer as your organization's directory synchronization computer. This computer can be a virtual machine, but it must meet the following criteria:

- The synchronization computer must be a member of the Active Directory forest that will host the Exchange organization.
- The synchronization computer cannot be a domain controller.
- The synchronization computer must have the .NET Framework 3.5 or later installed.
- The computer must run a 32-bit version of the Windows Server 2003, Windows Server 2003 R2, or Windows Server 2008 operating systems. At present the directory synchronization tool cannot be installed on a computer running Windows Server 2008 R2 because 64-bit environments are not supported.

You will also need to configure an Exchange Server 2010 coexistence server to support the coexistence scenario.

MORE INFO **DIRECTORY SYNCHRONIZATION**

To learn more about Active Directory synchronization with the cloud, consult the following document on Microsoft's website: *http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff652543.aspx*.

Exchange Federation

Exchange federation allows people in your organization to configure your Exchange infrastructure so that contact information and calendar availability can be shared with external recipients, vendors, and partners. If you want to configure Exchange federation, you need to set up a one-time federation trust between your organization and the Microsoft Federation Gateway. The Microsoft Federation Gateway is a cloud-based service that functions as a trust broker between a locally hosted Exchange 2010 organization and other organizations that have configured Exchange federation.

When creating a federation trust between your organization and the Microsoft Federation gateway, you need to either create a self-signed certificate or install an X.509 certificate signed by a trusted CA on the Exchange 2010 server that you will use to create the trust. Microsoft recommends using a self-signed certificate, which the New Federation Trust Wizard will automatically create and install, vastly simplifying this process.

After you have configured this trust relationship, the Microsoft Federation Gateway will issue Active Directory authenticated users in the local forest special Security Assertion Markup Language (SAML) delegation tokens. SAML delegation tokens allow organizations that have configured Exchange federation to trust users from other organizations that have configured Exchange federation. Instead of having to create each inter-organizational trust relationship separately, each organization configures a single trust with the Microsoft Federation Gateway, enabling them to share availability information with other organizations that have a trust with the Microsoft Federation Gateway.

When you establish a federation trust between your organization and the Microsoft Federation Gateway, an application identifier (AppID) is generated that will be used by the Federation Gateway to uniquely identify your Exchange organization. You use the AppID in conjunction with a text (TXT) record in DNS to prove that your organization is associated with the domain that is used with the Microsoft Federation Gateway. It is necessary to create a TXT record in the DNS zone for each federated domain in your organization.

MORE INFO **INFRASTRUCTURE PLANNING AND DESIGN GUIDE FOR EXCHANGE SERVER 2010**

You can download a solution accelerator related to infrastructure planning and design for the deployment of Exchange Server 2010 with Service Pack 1 from the following address: *http://go.microsoft.com/FWLink/?Linkid=199004*.

You define which authoritative accepted domains in your organization are enabled for federation through the federated organization identifier (OrgID). Only those recipients that have email addresses associated with the OrgID will be able to use federated delegation features by the Microsoft Federation Gateway. Federation delegation uses a domain namespace for the OrgID that differs from the primary SMTP domain. This domain namespace should not be used for mailboxes, and Microsoft recommends that the namespace be called exchangedelegation. This subdomain works as the federated namespace for the Microsoft Federation Gateway, allowing it to manage unique identifiers for those recipients that need SAML delegation tokens. If you want to enable or disable all federation features for your Exchange organization, you can either enable or disable the OrgID.

MORE INFO **EXCHANGE FEDERATION**

For more information on Exchange Server 2010's federation features, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/dd351109.aspx*.

Exchange Pre-Deployment Analyzer

The Exchange Pre-Deployment Analyzer is a tool that allows you to perform a readiness scan of your organization's environment to determine what modifications need to be made prior to the deployment of Exchange Server 2010. This tool will also perform a deep analysis of an existing Exchange 2003 and Exchange 2007 organization to determine whether the configuration will support an in-place upgrade to Exchange 2010. The end report includes critical and warning notifications. A critical notification is one that will block Exchange Server 2010 from being deployed and includes items such as the forest not running in Windows Server 2003 functional mode or higher. A warning notification indicates that some Exchange Server 2010 functionality may not be present if a deployment is performed given the current conditions.

MORE INFO **PRE-DEPLOYMENT ANALYZER**

To learn more about the Exchange Pre-Deployment Analyzer, download the tool from the following Microsoft website: *http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11636*.

Exchange Deployment Assistant

The Exchange Deployment Assistant, also known as ExDeploy and shown in Figure 1-3, is a web-based tool that you can use in the early stages of planning an Exchange Server 2010 deployment. ExDeploy works by asking a series of questions about your organization's current environment. Based on these questions, ExDeploy generates advice and a custom checklist to assist you with that deployment. Links are provided to relevant TechNet documentation and the output of ExDeploy can be saved for later review.

ExDeploy can provide you with a checklist and advice in the following scenarios:

- Locally hosted on-premise deployments:
  - Upgrade from Exchange Server 2003
  - Upgrade from Exchange Server 2007
  - Upgrade from mixed Exchange 2003 and Exchange 2007 environment
  - New Exchange Server 2010 deployment
- Coexistence of locally hosted on-premise and cloud:
  - Exchange 2003
  - Exchange 2007
  - Exchange 2010
  - Cloud-only deployments

FIGURE 1-3 Exchange Deployment Assistant

MORE INFO **EXCHANGE DEPLOYMENT ASSISTANT**

You can run the Exchange Deployment Assistant by navigating to the following address: *http://technet.microsoft.com/en-us/library/ee681665.aspx*.

EXAM TIP

You should load the Exchange Server Deployment Assistant webpage and run through a few scenarios to understand how it functions and the advice it gives under changing conditions.

Objective Summary

- Exchange Server 2010 can be installed in an on-premise, cloud, or a coexistence configuration.
- The Active Directory Sites and Services console allows you to associate specific IP networks with specific Active Directory sites.
- SLA requirements determine parts of your Exchange design, primarily around high-availability features such as Database Availability Groups and Client Access Server Arrays.
- In multiple-forest environments, the resource-forest topology has Exchange deployed in one forest and accessed by users in other forests. The cross-forest topology has Exchange deployed in all forest and uses Forefront Identity Life Cycle Manager for GAL synchronization.
- Exchange Federation allows people in your organization to share contact and calendar availability information. Federation requires setting up a one-time federation trust between your organization and the Microsoft Federation Gateway.
- The Exchange Deployment Assistant (ExDeploy) is an online tool that provides advice and checklists to assist with planning an Exchange deployment based on answers to a set of questions about the current and intended environments.

Objective Review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You are in the process of planning an Exchange Server 2010 installation. Which console should you use on a Windows Server 2008 R2 domain controller to verify that branch office network subnets are associated correctly with branch office sites in Active Directory?

   A. Active Directory Administrative Center

   B. Active Directory Users and Computers

   C. Active Directory Domains and Trusts

   D. Active Directory Sites and Services

2. Your organization has a single domain forest. The DNS domain name of the domain is contoso.com. The primary DNS suffix of all domain controllers is contoso.com, but the primary DNS suffix of all member servers—including the servers on which you intend to deploy Exchange Server 2010—is contoso.internal. Which of the following steps must you take to ensure that Exchange Server 2010 will function properly when deployed in this environment? (Choose all that apply.)

   A. Set the *msDS-AllowedDNSSuffixes* Active Directory attribute so that it only includes contoso.internal.

   B. Modify the *msDS-AllowedDNSSuffixes* Active Directory attribute on the domain object container so that it includes both contoso.com and contoso.internal.

   C. Configure the DNS suffix search list group policy item so that it includes both contoso.com and contoso.internal.

   D. Configure the DNS suffix search list group policy item so that it only includes contoso.internal.

3. You are in the process of consulting on an Exchange design for two companies. The first, Tailspin Toys, has a three-forest Active Directory infrastructure. The second company, Wingtip Toys, has a two-forest Active Directory infrastructure. You are in the process of determining which multiple-forest topology would suit each company. Tailspin Toys would be best suited by deploying Exchange in each forest. Wingtip Toys would be best suited by deploying Exchange in one forest and keeping user accounts in the other forest. Which of the following Exchange multiple-forest topology models best suits each organization? (Choose all that apply.)

   A. Tailspin Toys should use the cross-forest topology.

   B. Tailspin Toys should use the resource-forest topology.

   C. Wingtip Toys should use the cross-forest topology.

   D. Wingtip Toys should use the resource-forest topology.

4. You are interested in measuring service availability as a part of monitoring compliance with a Service Level Agreement (SLA). Which of the following products could you use to monitor service availability, configuring alerts to be sent in the event that any component in the Exchange infrastructure fails?

   A. System Center Configuration Manager 2012

   B. System Center Data Protection Manager 2012

   C. System Center Virtual Machine Manager 2012

   D. System Center Operations Manager 2012

5. Which of the following products can you use to assist with global address list (GAL) synchronization if your organization is intending to deploy Exchange Server 2010 in a cross-forest topology?

   A. Forefront Threat Management Gateway 2010

   B. Forefront Endpoint Protection 2012

   C. Forefront Identity Life Cycle Manager 2010

   D. Forefront Unified Access Gateway 2010

THOUGHT EXPERIMENT
Preparing Contoso for Directory Synchronization with the Cloud

In the following thought experiment, apply what you've learned about the "Design the Exchange Server 2010 installation" objective to predict what steps you need to take to prepare Contoso for directory synchronization with the cloud. You can find answers to these questions in the "Answers" section at the end of this chapter.

Contoso has a four-domain Active Directory forest that currently has a small Exchange Server 2007 deployment. You want to configure a coexistence scenario where Exchange Server 2007 will coexist with a cloud hosted Exchange deployment through Office 365.

With this in mind, answer the following questions:

1. **What should you do prior to configuring directory synchronization to ensure that password changes are replicated to the cloud-hosted Exchange deployment?**
2. **What general steps must you take to configure single sign-on at Contoso?**
3. **Which two servers need to be deployed in the local organization to support the coexistence scenario?**

Objective 1.2: Design Message Routing

Designing a message routing infrastructure involves determining where you need to put transport servers to effectively route messages inside and outside your organization. Not only do you need to decide where to put the transport servers, but you also need to ensure that these servers are sufficiently capable of handling the message traffic generated by your organization. Your design needs to include the mail domains that your organization will accept mail for, how to handle the routing of email to third-party messaging systems that might be used within your environment, and how messages will be forwarded from your organizations to destinations on the Internet. In this objective, you'll learn about message routing design. In Chapter 2 you'll learn about how to implement message routing with Edge Transport and Hub Transport servers.

This objective covers:

- Design message transport.
- Plan reverse lookup zones.
- Scale transport server performance.
- Plan accepted and remote domains.
- Design send and Receive connector configuration.

Design Message Transport

At the most basic level, when designing Exchange transport server deployment you need to ensure that you place at least one Hub Transport server in each Active Directory site that has an Exchange Mailbox server. When designing a traditional Exchange 2010 deployment, you will also place at least once Edge Transport server on a perimeter network that is adjacent to an Active Directory site with a Hub Transport server.

Messages are routed through an Exchange 2010 organization in the following general way:

- **Internal Message Routing** When a message arrives at a Hub Transport server, processes within the Hub Transport server determine the Active Directory site location of the mailbox server that hosts the recipient's mailbox. If the destination Mailbox server is in another Active Directory site, the message is forwarded to the Hub Transport server in that site. If the destination Mailbox server is in the local Active Directory site, the message is queued for local delivery and delivered to the destination mailbox store using an Exchange remote procedure call (RPC).
- **External Message Routing** When a message arrives at a Hub Transport server and the Hub Transport server determines that the recipient does not have a mailbox within the Exchange organization, the Hub Transport server attempts to select a Send connector through which to send the message. If the source server for that Send connector is in another Active Directory site, the Hub Transport server forwards the

message to the Hub Transport server in that site. Through the configuration of Send connectors, you can also allow messages to be routed to other messaging systems within your organization. For example, if you have a cross-forest Exchange topology, you can configure a Send connector to route messages to the other internally hosted Exchange organization.

MORE INFO **MESSAGE ROUTING**

To learn more about message routing, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/aa998825.aspx*.

Modifying Default Message Routing Topology

If you don't modify the initial configuration, when a Hub Transport server needs to deliver a message to a recipient whose mailbox is hosted on a mailbox server in another Active Directory site, that Hub Transport server will initiate a direct connection to a Hub Transport server in that site. For example, if a Hub Transport server in the Melbourne site needs to deliver a message to a mailbox server in the Darwin site, it will initiate a connection to a Hub Transport server in the Darwin site. Although the default routing topology, based on Active Directory site topology, is suitable for most organizations, you can modify it in the following ways:

- Configure hub sites.
- Configure Exchange-specific routing costs.
- Configure expansion servers for distribution groups.

Configure Hub Sites

You can configure one or more Active Directory sites as hub sites. For example, you might configure the Sydney site as a hub site for all of the other Active Directory sites in your organization's Australian Exchange deployment. You should configure hub sites when your organization's network topology does not support direct connections between Hub Transport servers in different sites. When a hub site lies on a least-cost routing path between a source and destination Hub Transport server, the Hub Transport server at the hub site processes the messages before relaying them to the destination server.

You configure an Active Directory site as an Exchange hub site by using the *Set-AdSite* cmdlet. For example, to set the Sydney site as a hub site, use the following command:

```
Set-ADSite Sydney -HubSiteEnabled $true
```

Configure Exchange-Specific Routing Costs

You can alter the default routing topology by setting an Exchange cost on an Active Directory IP site link. Any set Exchange costs override the existing Active Directory assigned site cost. Use site-link costs to ensure that the least cost routing path between two sites goes through

a hub site. You use the *Set-ADSiteLink* cmdlet to configure an Exchange-specific cost for an Active Directory IP site link. For example, to set the Exchange-specific cost of 20 to the IP site link IPSiteLinkMELSYD, use this command:

```
Set-ADSiteLink -Identity IPSiteLinkMELSYD -ExchangeCost 20
```

To remove the Exchange specific site cost from the IP site link IPSiteLinkMELSYD, use the following command:

```
Set-ADSiteLink -Identity IPSiteLinkMELSYD -ExchangeCost $null
```

MORE INFO **MODIFYING EXCHANGE COSTS ON IP SITE LINKS**

To learn more about configuring Exchange costs on an Active Directory site link, consult the following TechNet document: *http://technet.microsoft.com/en-us/library/bb266946.aspx*.

Configure Expansion Servers for Distribution Groups

When a message is sent to a distribution group, the first Hub Transport server that intercepts the message performs the distribution group expansion, working out how to route messages to each member of the distribution group. With large distribution groups, this can cause a substantial performance hit on the Hub Transport server, slowing down all message routing operations. An alternative to allowing any Hub Transport server to perform distribution group expansion is to configure distribution groups to use specific Hub Transport servers to perform this task. You configure a specific Hub Transport server as a distribution group expansion server by modifying the properties of individual distribution groups. You'll learn more about configuring distribution groups in Chapter 2.

Transport Server Scalability

The simplest way to scale transport server performance is to add additional Hub transport servers at each Active Directory site. When you add additional Hub transport servers, messages route through each Hub transport server in a site in a load-balanced way. In theory, each Hub Transport server can queue a maximum of 500,000 messages. If your design calls for more than 500,000 messages to be queued in a single Active Directory site, you will need to add additional Hub Transport servers. Although the 500,000 figure represents the maximum number of messages that can be queued, most organizations will require a minimum inter-organizational delivery time frame for messages as a part of an SLA. You are more likely to have to add Hub Transport servers to ensure quick delivery than you are because you've reached the 500,000 message queue capacity.

Also remember that scalability is different from high availability. High availability involves adding additional servers to ensure that message routing continues in the event that a Hub Transport or Edge Transport server fails. You'll learn more about High Availability for transport servers in Chapter 4, "Designing and Deploying Exchange Server 2010 Availability and Recovery."

You can use several other technologies in your Exchange design to ensure that your transport server infrastructure isn't overwhelmed by excessive traffic. These include message throttling and back pressure.

Message Throttling

Message throttling allows you to limit the number of messages and connections that an Exchange 2010 Hub or Edge Transport server will accept. These limits ensure that the system resources of the transport server are not overwhelmed, either accidentally or intentionally. You can configure message throttling options on the transport server itself, on individual Send connectors, and on individual Receive connectors.

You can configure the following message throttling options:

- **Maximum concurrent mailbox deliveries** This option determines the maximum number of delivery threads that a Hub Transport server can concurrently use to deliver messages to mailboxes. The default value is 20. This setting can be configured with the *MaxConcurrentMailboxDeliveries* parameter of the *Set-TransportServer* cmdlet.
- **Maximum concurrent mailbox submissions** This option determines the maximum number of delivery threads that a Hub Transport server can concurrently use to accept messages from mailboxes. The default value is 20. This setting can be configured with the *MaxConcurrentMailboxSubmissions* parameter of the *Set-TransportServer* cmdlet.
- **Maximum connection rate per minute** This option determines the maximum rate at which the Hub Transport or Edge Transport server will accept new inbound connections. The default value is 1200 connections per minute. This setting can be configured with the *MaxConnectionRatePerMinute* parameter of the *Set-TransportServer* cmdlet.
- **Maximum outbound connections** This option determines the maximum number of outbound connections that a Hub or Edge Transport server can have open concurrently. The default value is 1000. You can configure this setting with the *MaxOutboundConnections* parameter of the *Set-TransportServer* cmdlet.
- **Maximum per domain outbound connections** This option limits the number of connections that a transport server connected to the Internet—which will usually be an Edge Transport server but might in some cases be a Hub Transport server—can open to any individual remote domain. The default value is 20. You can configure this setting with the *MaxPerDomainOutboundConnections* parameter of the *Set-TransportServer* cmdlet.
- **Pick up directory maximum messages per minute** This option limits the message processing rate for the Replay and Pickup directories. These directories are polled every five seconds and the default settings allows for eight messages to be processed every five-second interval. You can configure this setting with the *PickupDirectoryMaxMessagesPerMinute* parameter of the *Set-TransportServer* cmdlet. This figure you enter when using this parameter is for a 60-second duration, so you need to divide it by 12 to determine the number of messages processed during the polling interval.

- **Connection inactivity time out** This option limits the maximum amount of time that an SMTP connection to a remote server will remain open while idle before closing. The default value is 10 minutes. You configure this option on Send connectors by using the *ConnectionInactivityTimeOut* parameter with the *Set-SendConnector* cmdlet.
- **Connection time out** This option limits the maximum amount of time that an SMTP connection from a remote server will remain open, even if it is in the process of transmitting data. The default value on Hub Transport servers is 10 minutes and the default value on Edge Transport servers is 5 minutes. You configure this option on Receive connectors by using the *ConnectionTimeOut* parameter with the *Set-ReceiveConnector* cmdlet.
- **Maximum inbound connection** This option limits the maximum number of concurrent inbound connections that the Receive connector will accept. The default is 5000. You configure this option on Receive connectors by using the *MaxInboundConnection* parameter with the *Set-ReceiveConnector* cmdlet.
- **Maximum inbound connection percentage per source** This option limits the maximum number of SMTP connections that a Receive connector will accept from a single source as a percentage of available remaining connections. The default value is 2 percent. You configure this option on Receive connectors by using the *MaxInbound-ConnectionPErcentagePerSource* parameter with the *Set-ReceiveConnector* cmdlet.
- **Maximum inbound connection per source** This option limits the maximum number of SMTP connections that a Receive connector will accept from a single source as a fixed value. The default value is 100. You configure this option on Receive connectors by using the *MaxInboundConnectionPerSource* parameter with the *Set-ReceiveConnector* cmdlet.
- **Maximum Protocol errors** This option limits the maximum number of SMTP protocol errors that can occur over an established connection before that connection is terminated. The default value is 5. You configure this option on Receive connectors by using the *MaxProtocolErrors* parameter with the *Set-ReceiveConnector* cmdlet.
- **Tarpit Interval** This option determines the delay that is used when SMTP communications patterns suggest a directory harvest attack or other unwelcome messages. Directory harvest attacks are attempts to determine valid email addresses for use with spam. You configure this option on Receive connectors by using the *TarpitInterval* parameter with the *Set-ReceiveConnector* cmdlet.

MORE INFO **MESSAGE THROTTLING**

For more information on message throttling, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb232205.aspx*.

Back Pressure

Back pressure monitors the Microsoft Exchange Transport service on Hub and Edge Transport servers, taking action when resource pressures build up as a method of ensuring availability. Back pressure works by preventing system resources from being overwhelmed by rejecting or limiting incoming connections until the pressure on system resources eases. Back pressure works in conjunction with message throttling. The difference is that back pressure only applies when the transport server's system resources are under pressure, whereas message throttling limits apply all the time.

MORE INFO **BACK PRESSURE**

To learn more about back pressure, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb201658.aspx*.

Message Queues and Shadow Redundancy

Shadow redundancy is a transport server feature that ensures that email messages are not lost in transit if a transport server fails. Shadow redundancy works by waiting until the transport server can verify that delivery has occurred to the next hop in a message's path before deleting the local copy. If the next hop delivery fails, the transport server resubmits the message to the next hop. Shadow redundancy is handled by the Shadow Redundancy Manager, which is responsible for keeping track of the shadow server for each primary message that the server is currently processing and the discard status to be sent to shadow servers. Including shadow redundancy in an Exchange design accomplishes the following goals:

- Ensures that as long as a redundant message path exists in a routing topology, message routing will occur in the event of transport server failure.
- Allows you to bring a Hub or Edge Transport server down for maintenance without having to worry about emptying queues or losing messages.
- Minimizes additional network traffic because it doesn't require duplicate messages to be transmitted to multiple servers. The only additional traffic is a discard status message.
- Reduces the necessity for storage hardware redundancy on transport system. Even if you don't have a redundant path, you can get a replacement transport server in place and the mail flow will resume without losing any messages. Whether this is an appropriate strategy depends on your SLA.

Shadow redundancy requires an extension of the SMTP service that is currently supported only by Exchange Server 2010 transport servers. During SMTP communication, a check is performed to determine whether the next hop server supports the shadow redundancy feature. In the event that the next hop server does not support shadow redundancy, the Shadow Redundancy Manager marks the message as delivered after it has been handed off

to the next server and deletes it rather than waiting for confirmation from the next hop server that it has been successfully delivered to the next hop plus one server.

Shadow redundancy can be enabled or disabled on a per-organization level basis using the *Set-TransportConfig* cmdlet with the *ShadowRedundancyEnabled* parameter. For example, to enable shadow redundancy for all servers in the organization, use the following command:

```
Set-TransportConfig -ShadowRedundancyEnabled $true
```

MORE INFO **SHADOW REDUNDANCY**

To learn more about shadow redundancy, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/dd351027.aspx*.

Transport Storage Requirements

The amount of disk space required by a transport server depends on the number of messages sent and received each day, how long you keep transaction logs, and whether protocol logging has been set up. When including Hub Transport storage requirements in an Exchange design, you need to make an estimate of the number of messages that will queue on the server. Although a single server can queue up to 500,000 messages, unless a Hub Transport server routes messages directly to the Internet or a failure occurs, the average number of messages sitting in the queue is unlikely to be high. Your design should take into account failure scenarios, but you probably don't need to configure storage for a transport server so that it can cope with 500,000 queued messages, unless the server is likely to process that number of messages over a 24-hour period.

Your design needs to take into account how Hub Transport servers will respond in the event of some failure that prevents them from offloading messages to other transport servers.

When planning transport server storage requirements, take into account the following:

- If the average message size at an organization is 200 KB and 10,000 messages pass across the organization's main site every day, the queue database could grow to almost 2 GB if a failure occurs that stops messages being transmitted off the server for a 24-hour period.
- Message tracking logs consume roughly .5 KB per message sent or received. At a site that has 10,000 messages passing through each day, keeping message tracking logs for the default 7 days will consume another 35 MB or so of space.
- Agent, Protocol, and Connectivity logs record information about SMTP traffic. These logs vary in size depending on the size, amount, and kind of messages delivered by the transport server. Agent, Protocol, and Connectivity logs consume approximately 2 KB per message. At the theoretical site that processes 10,000 messages, that's another 20 MB a day.

- If you are using Database Availability Groups (DAGs), the transport dumpster can grow up to a default 18 MB for every mailbox database in a single Active Directory site. The Transport Dumpster holds a copy of messages sent to mailboxes that are part of a DAG and only deletes those messages when the message has successfully replicated to all members of the DAG. If a site hosts 200 Exchange mailboxes, it is theoretically possible that the combined transport dumpsters for those mailboxes will require approximately 3.6 GB of storage space.

You can modify the size of the Transport Dumpster and configure how long it retains messages on the General tab of the Transport Settings Properties dialog box, shown in Figure 1-4. You can access this dialog box by clicking the Global Settings tab when you have selected the Hub Transport node under Organization Configuration in Exchange Management Console. You can also configure the maximum dumpster size and retention time using the *Set-TransportConfig* cmdlet with the *MaxDumpsterSizePerDatabase* and *MaxDumpsterTime* parameters.

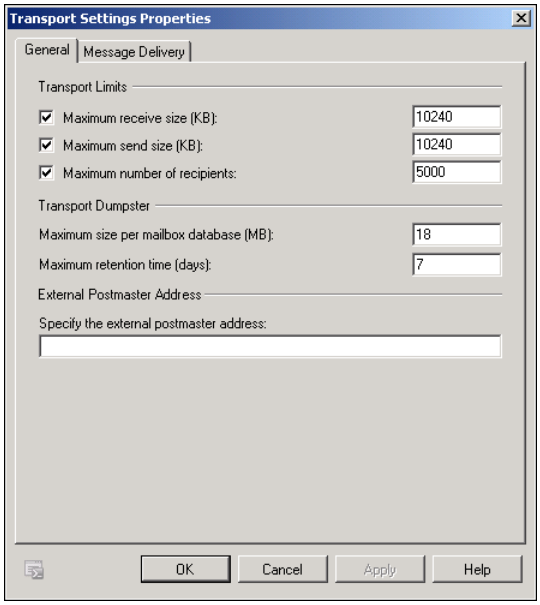


FIGURE 1-4 Transport Dumpster size

MORE INFO **CONFIGURE TRANSPORT DUMPSTER**

To learn about configuring transport dumpster settings and other transport settings, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb676532.aspx*.

Planning Accepted and Remote Domains

Your Exchange organization can only accept messages for email domains that are configured as accepted domains. An accepted domain is also an email domain for which your organization is able to send email. For example, if your organization needs to accept email for addresses within the @tailspintoys.com and @wingtiptoys.com domains, you will need to include these domains as accepted domains within your Exchange design. If your recipients want to use the @adatum.com email domain when sending messages from Exchange, @adatum.com will need to be configured as an accepted domain.

Exchange Server 2010 supports three types of accepted domain:

- **Authoritative Domains** This is the most obvious type of mail domain to include in your Exchange design because this is the domain you use for recipients who have mailboxes that are a part of your Exchange organization. The default authoritative domain for an Exchange organization is the fully qualified domain name (FQDN) of the forest root domain. This means that if the FQDN of your organization's forest root domain is contoso.internal, contoso.internal will be automatically configured as the default authoritative domain.
- **Internal Relay Domain** You include this type of email domain in your design when Exchange will need to forward messages to another email system on the internal network. You use internal relay domains in your design if you need to route messages to a third-party email system or to another Exchange organization if your organization has multiple forests and is using the cross-forest topology model. Your design should include an internal relay domain if you've split your address space and some accounts in an email domain are hosted by Exchange and others by a third-party mail system.
- **External Relay Domain** You include an external relay domain in your design if you need to configure your Exchange organization to accept email messages from external organizations so that they can be forwarded to another external organization. To have external relay domains function properly, Send connectors to the external domain must be configured on Edge Transport servers.

Remote domains allow you to control message formatting options for specific email address domains. They also allow you to configure whether external out-of-office messages will be sent to users in those domains. You include remote domains in your Exchange design when you want to control the types of messages and message formats that are sent to a specific external domain.

MORE INFO **ACCEPTED DOMAINS**

To learn more about accepted domains, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb124423.aspx*.

Planning Send and Receive Connectors

Send and Receive connectors control how messages flow in, out, and through your Exchange organization. You include them in your Exchange design when you want to route messages between Hub Transport and Edge Transport servers when you don't have an edge subscription, or between transport servers and other messaging systems on the internal network or the Internet.

The difference between these connector types is as follows:

- A Receive connector allows a transport server to receive SMTP traffic from specific sources. This can include SMTP servers on the Internet, Edge Transport servers that aren't configured to use edge synchronization, third-party SMTP servers on the internal network, and SMTP mail clients.
- A Send connector transmits a message to a destination location using the SMTP protocol. Send connectors can be configured to send email directly to a destination SMTP server, or you can configure a Send connector to route outgoing messages through a smart host.

MORE INFO **SMART HOST**

A smart host is a server, usually hosted by an organization's ISP, that functions as a mail-relay between SMTP servers on the Internet and an organization's Edge Transport or Hub Transport server. You can find out more about smart hosts by reading the following TechNet article: *http://technet.microsoft.com/en-us/library/cc626187(WS.10).aspx*.

You don't need to plan Send connectors or Receive connectors for message transmission between Hub Transport servers that are in the same Exchange organization because Hub Transport servers that are members of the same Exchange organization are automatically configured to communicate with each other when you deploy Exchange. You also don't need to plan Send connectors or Receive connectors between Hub Transport and Edge Transport servers when you configure an edge subscription because the edge subscription process creates the necessary connectors between these servers.

You do need to plan Send and Receive connectors in the following circumstances:

- You need to configure communication with another messaging system hosted on your organization's internal network.
- You need to send messages through a smart host.
- You need to configure a secure connection with a partner organization that uses a technology such as mutually authenticated TLS.
- You want to route messages through Exchange Hosted Services as a method of using features such as hosted filtering, hosted archive, hosted encryption, and hosted continuity.

MORE INFO **MAIL FLOW AND EXCHANGE HOSTED SERVICES**

To learn more about configuring Internet mail flow through Exchange hosted services, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb738161.aspx*.

Planning Outbound Message Flow

For your Exchange organization to send messages out to hosts on the Internet, you need to have at least one SMTP Send connector that includes within its address space Internet SMTP domains. Depending on the size and structure of your organization, you may choose to deploy multiple Edge Transport servers with multiple SMTP Send connectors. You can also configure one SMTP Send connector to use multiple Edge Transport servers as a source server depending on your organizational needs.

Organizations that have multiple sites can choose to deploy an Edge Transport server at each site so that outbound messages from that site are routed directly to the Internet, rather than being routed across the internal network to be forwarded to the Internet from a single perimeter network. The Edge Transport servers at each site can either be configured with an edge subscription to their local parent site, or you can manually configure Send connectors on that local site's Hub and Edge Transport servers. You'll learn about setting up Edge Transport servers with and without subscriptions in Chapter 2.

Planning Inbound Message Flow

For your Exchange organization to accept incoming messages from the Internet, it is necessary for you to configure at least one SMTP Receive connector that will accept anonymous SMTP connections from SMTP servers on the Internet. You also need to configure a DNS Mail Exchange (MX) record to point to the server that hosts the SMTP Receive connector in your organization's externally resolvable DNS zone. This record allows SMTP servers on the Internet to determine the IP address of your organization's SMTP gateway.

If your organization has more than one location, you may choose to have multiple Edge Transport servers that process incoming email. For example, if your organization has offices in the Australian state capital cities of Brisbane, Sydney, and Melbourne, you might choose to deploy an Edge Transport server on each site's perimeter network. Whether this would lead to any efficiencies when you are using a single email domain namespace is questionable. If you create MX records with equal priorities that point to each of these Edge Transport servers, incoming messages will distributed across each Edge Transport server with no guarantee that email messages to users in the Sydney site will enter through the Sydney Edge Transport server. Messages will still need to be routed internally in most cases unless they are lucky enough to arrive at the correct site. If you configure the MX records with different priorities, only the MX record with the lowest priority will be used and inbound messages will

only route to other servers in the event that the Edge Transport server associated with the lowest priority record is unavailable. Having Edge Transport servers at multiple sites is more beneficial for outbound traffic because these messages can be sent directly to Internet hosts without having to be routed internally.

You may also want to plan additional message connectors to meet specific business requirements. For example, your organization's external SMTP server needs to be able to accept messages from any SMTP server on the Internet. Historically the SMTP protocol does not require TLS, which means most organizations haven't configured it on their SMTP servers. If you required TLS on all incoming SMTP connections, you'd end up blocking messages from most organizations on the Internet. You do have the option, however, in conjunction with a partner organization, of configuring a special Receive connector that requires TLS encryption or authentication. This ensures that SMTP traffic that passes between your organization and the partner will be protected from interception as it passes across the public Internet. The majority of your incoming message traffic will not be protected, but message traffic to and from that particular partner will be.

Internal SMTP Relay

You include internal SMTP relay in your design when you need to configure your Exchange organization to route messages to recipients that are not hosted within the local Exchange organization, but may have mailboxes on a third-party messaging system or in another Active Directory forest located on your organization's internal network. This can either be in a shared address space scenario, in which multiple messaging systems host mailboxes in the same email address space, or the separate address space scenario, where Exchange accepts messages for an address space for which it doesn't host mailboxes and then routes those messages internally to another messaging system.

In both scenarios it is necessary to configure an Accepted domain as an internal relay domain and then configure a Send connector to route messages to SMTP servers of that separate—but internal—messaging system. For example, if you had two separate Active Directory forests, both of which were configured with Exchange and both of which used the contoso.com mail domain, you would configure one of those organizations to accept and route incoming messages to the other forest. The Send connector to the second forest's Exchange organization would only be utilized if the recipient mailbox wasn't hosted in the first forest that accepted the message from an SMTP server on the Internet.

MORE INFO **ROUTING MESSAGES FOR SHARED ADDRESS SPACE**

To learn more about routing messages to an internal shared address space, consult the following TechNet documentation: *http://technet.microsoft.com/en-us/library/bb676395.aspx*.

Planning DNS

Planning DNS for transport servers includes two main elements. The first is ensuring that your organization's Hub Transport and Edge Transport servers are able to resolve each other's names. The second is to ensure that your organization's external DNS servers respond if a mail server on the Internet performs a reverse lookup on the public IP address of your organization's Edge Transport servers.

Edge Transport DNS Resolution

Edge Transport servers need to be able to perform DNS resolution on Internet hosts, but also need to be able to resolve the addresses of Hub Transport servers to which they will route messages. When you are planning Edge Transport server deployment, you may need to configure different DNS server settings for the server's public and private network adapters, configuring the public adapter to use your ISP's DNS servers, and configuring the private network adapter to use your internal DNS servers. After you have done this, you can configure the Edge Transport server's properties by right-clicking the Edge Transport server in EMC and clicking Properties. Here you can specify external DNS lookup settings on the External DNS Lookups tab, as shown in Figure 1-5, or internal DNS lookup settings on the Internal DNS Lookups tab. You can configure Send and Receive connectors to use these internal and external DNS settings when performing name resolution during message transport.

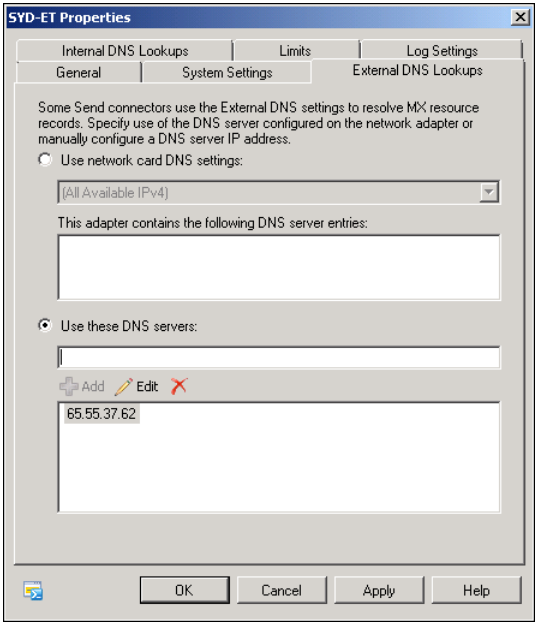


FIGURE 1-5 Configure external DNS lookup

Reverse Lookup Zones

Reverse lookup zones translate IP addresses to fully qualified domain names. You need to consider reverse lookup zones in your Exchange design because many organizations use reverse lookups as a method of filtering unsolicited commercial email, better known as spam. This process works by having an email gateway verify that the DNS domain name associated with the IP address of a remote SMTP server matches the mail domain of the email sent from that server. For example, if you did a DNS lookup on IP address 131.107.125.5 using the nslookup command-line utility, the DNS server would return the result mail.microsoft.com. If your email gateway received an incoming message from 131.107.125.5, it would match the sender's address against the DNS zone associated with that IP address.

Setting up local reverse lookup zones is straightforward and can be accomplished by performing the following general steps:

1. Open the DNS Manager console on a computer that hosts the DNS role service.
2. Right-click the Reverse Lookup Zones node and then click New Zone.
3. In the New Zone Wizard you specify what type of zone you want to create. In most cases this will be a primary zone.
4. Specify the DNS zone replication scope.
5. Specify whether you want to create an IPv4 or IPv6 reverse lookup zone:
   - If you want to create an IPv6 reverse lookup zone, you need to provide the IPv6 Address Prefix.
   - If you want to create an IPv4 reverse lookup zone, you can either provide the Network ID or the Reverse Lookup Zone Name, as shown in Figure 1-6. If you use the option to use the zone name, it needs to be in the format *z.y.x*.in-addr.apra where the IPv4 network that you are creating the zone for is in the format *x.y.z*.0. For example, network 131.107.125.0 would have the reverse lookup zone name 125.107.131.in-addr.apra.

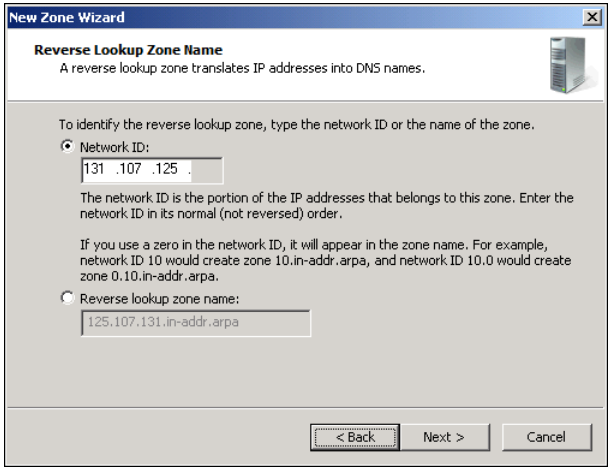


FIGURE 1-6 Create reverse lookup zone

6. Choose whether to allow secure dynamic updates only, no dynamic updates, or a mix of secure and nonsecure dynamic updates and then finish the wizard.

In most cases though, the public IP address that your organization's external mail gateway uses, which in a pure Exchange 2010 environment is an Edge Transport server, has been provided to your organization by an ISP. Reverse lookup zones are often managed by ISPs because reverse lookup zones are configured in such a way that the smallest reverse lookup zone is a class C address block. This means that you can't create a reverse lookup zone for the two or three public IP addresses that have been assigned to your organization. Instead you have to find which organization hosts the reverse lookup zone for the class C address block to which your organizations two or three public IP addresses belong. You'll then need to get the hosts of those zones to insert the appropriate reverse lookup record.

> ***MORE INFO*** **CREATING REVERSE LOOKUP ZONES**
>
> **To learn more about creating a reverse lookup zone on a computer running Windows Server 2008 R2, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/dd894426(WS.10).aspx*.**

Planning Transport Server Ports

Because you place Edge Transport servers on a perimeter network, there will be at least one firewall between any Edge Transport servers and the Hub Transport servers hosted in the adjacent Active Directory site. To support mail flow and edge synchronization between Edge Transport and Hub Transport servers, it is necessary to allow communication through specific network ports. Table 1-1 provides a list of the ports that need to be open between different components in an Exchange organization in the event that a firewall exists between them.

TABLE 1-1 Exchange Transport Roles and Required Ports

Exchange roles	Required ports
Hub Transport server to Hub Transport server	TCP port 25 (SMTP)
Hub Transport server to Edge Transport server	TCP port 25 (SMTP)
Edge Transport server to Hub Transport server	TCP port 25 (SMTP)
Edge Transport server to Edge Transport server	TCP port 25 (SMTP)
Mailbox server to Hub Transport server	TCP port 135 (RPC)
Hub Transport server to Mailbox server	TCP port 135 (RPC)
Edge subscription (EdgeSync) service from Hub Transport server to Edge Transport server	TCP port 50636
Active Directory Domain Controller from Hub Transport server	TCP and UDP port 389 (LDAP) TCP and UDP port 88 (Kerberos) TCP and UDP port 53 (DNS) TCP port 135 (RPC) TCP port 3268 (LDAP GC)
Hub Transport server to Active Directory Rights Management Services	TCP port 443 (HTTPS)
SMTP clients to Hub Transport server	TCP port 587 (SMTP) TCP port 25 (SMTP)

MORE INFO **TRANSPORT SERVER PORTS**

To learn more information about which ports need to be open when firewalls exist between two servers, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb331973.aspx*.

EXAM TIP

Be clear on the difference between a remote domain and a Send connector.

Objective Summary

- Ensure that at least one Hub Transport server is in each site that hosts a Mailbox server.
- Accepted domains determine the email domains for which the Exchange organization will process incoming messages. Authoritative domains are used when the Exchange organization hosts the mailbox. Internal relay domains are used in shared address space scenarios as well as when there is another messaging system on the internal network. External relay domains are used when accepted mail is to be processed and then relayed to an external organization.

- Remote domains allow you to control message formatting and distribution of out-of-office messages.
- Send connectors are used to forward outgoing SMTP traffic to a specific destination.
- Receive connectors are used to accept incoming SMTP traffic from a specific source.
- You can scale Hub Transport server performance by adding additional Hub Transport servers to sites.

Objective Review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. What type of accepted domain would you plan to use if you wanted your Exchange organization to route email messages accepted from hosts to a third-party messaging system hosted on your internal network? This email domain is not used by Exchange recipients.

   A. Authoritative domain

   B. Internal relay domain

   C. External relay domain

   D. Reverse lookup zone

2. You are in the process of designing an Exchange Server 2010 deployment. You will be using Edge Transport servers located on a perimeter network that will have edge subscriptions to Hub Transport servers located at your organization's main site. Which of the following ports need to be opened between the perimeter network and the main site internal network to support message transport and edge synchronization? (Choose all that apply.)

   A. TCP port 25

   B. TCP port 135

   C. TCP port 389

   D. TCP port 50636

3. Your organization has two separate Active Directory forests. You are planning to deploy an Exchange organization in each forest and want to use a shared address space so that recipients in both forests can use the @contoso.com email domain. Which of the following components will you need to configure in the Exchange organization that will be able to send and receive email from hosts on the Internet to ensure that recipients in the second Exchange organization receive messages? (Choose all that apply.)

   A. Internal relay domain

   B. Remote domain

   C. External relay domain

   D. Send connector

4. You want your Exchange design to use a different routing topology than the default Active Directory routing topology. Which of the following Exchange Management Shell (EMS) cmdlets would you use to set an Exchange-specific cost for an Active Directory IP site link?

   A. *Set-ADSite*

   B. *Set-ADSiteLink*

   C. *Get-ADSite*

   D. *Get-ADSiteLink*

5. Your organization does not use database availability groups. Which of the following features should you enable to ensure that email messages are not lost in transit in the event that a transport server fails?

   A. Remote domains

   B. Send connectors

   C. Transport dumpster

   D. Shadow redundancy

THOUGHT EXPERIMENT
Transport Server Design

In the following thought experiment, apply what you've learned about the "Designing message routing" objective to design a transport server infrastructure. You can find answers to these questions in the "Answers" section at the end of this chapter.

You are planning the transport server design for A. Datum Corporation. A. Datum has offices in the Australian state capital cities of Melbourne, Brisbane, Sydney, Adelaide, and Perth. A. Datum owns a subsidiary company Fabrikam, Inc. Fabrikam, Inc., has a separate Exchange organization located on their own network in the Northern Territory capital Darwin. While there is no direct connection between the Fabrikam network and the A. Datum network, you want to configure your Exchange organization to accept email for Fabrikam in the event that their Internet connection fails.

You are also concerned about the routing topology. You intend to deploy multiple Hub Transport servers in the Sydney branch office, but want to ensure that these servers are not overwhelmed by excessive traffic. The perimeter network at the Sydney office will also host the organization's Edge Transport server.

With these facts in mind, answer the following questions:

1. What kind of accepted domain should you configure for the fabrikam.com email domain?
2. Which transport server feature would you implement to ensure that a transport server is not overwhelmed by excessive message traffic?
3. Which Exchange Management Shell cmdlet can you use to configure the maximum connection rate per minute property to limit the number of inbound connections accepted per minute on the Edge Transport server hosted on the Sydney office's perimeter network?
4. Which Exchange Management Shell cmdlet should you use to configure the Sydney site as a hub site?
5. Which Exchange Management Shell cmdlet should you use to assign an Exchange cost to the Active Directory IP site links that connect the Melbourne and Brisbane sites to the Sydney site?

Objective 1.3: Design the Mailbox Server Role

Exchange Mailbox servers are big message storage servers. Out of all of the Exchange roles that you can deploy, the Exchange Mailbox server will utilize the most disk space. Most IT Professionals have heard of Moore's Law, which suggests that the number of transistors that can be placed on an integrated circuit doubles every two years. Although the growth isn't nearly as rapid, the amount of information transmitted by email across the world also doubles approximately every four years. This increase in information is reflected in most people's inboxes, and it is not unheard of in 2011 for some Exchange deployments to allow 50 GB mailbox quotas. This has become necessary because not only do people use Outlook to store email messages, but Outlook and Exchange mailboxes are also often used as informal document archives. In this objective you'll learn about planning database sizes, how to determine what sort of performance mailbox server storage will require, how to implement a multi-forest mailbox deployment, how to design a public folder infrastructure, and how to develop recipient and distribution group policies. In Chapter 2 you'll learn how to put these design decisions into operation.

This objective covers:

- Plan database sizing.
- Storage performance requirements.
- Multi-forest mailbox deployment.
- Design public folders.
- Develop recipient and distribution group policies.
- Mailbox provisioning policies.

Plan Database Sizing

Exchange Server 2010 mailboxes and public folders are stored in databases hosted on Exchange mailbox servers. Databases are stored in Extensible Storage Engine format. Each database has an associated set of transaction logs that record changes made to the database. Transaction logs are primarily useful during database recovery and you will learn more about using them in this manner in Chapter 4.

By default, each database and its associated transaction logs are stored in the same folder. These folders are unique to each database, with each database's folder typically stored under the C:\Program Files\Microsoft\Exchange\Server\v14\Mailbox folder as shown in Figure 1-7. If you are deploying Exchange on standard disks that do not use RAID striping, you should consider placing the mailbox database and the transaction logs on separate disks. This has the benefit of improving performance and simplifying recovery. You have less reason to do this when you are using RAID striping because disk read and write operations are already optimized through the use of multiple drives and controllers.

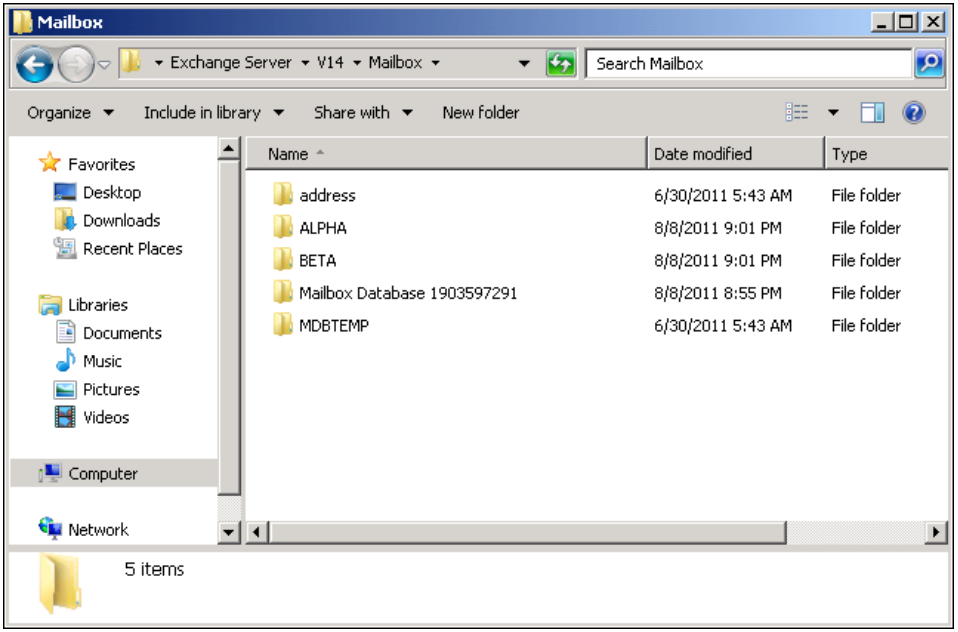


FIGURE 1-7 Database folders

The Standard edition of Exchange 2010 allows five databases per Mailbox server. One of these databases can be a public folder database. The Enterprise edition of Exchange 2010 allows 100 databases per Mailbox server. Only one of these databases can be a public folder database.

The following factors influence your plans when determining the size of mailbox databases:

- How many users will the mailbox database need to support?
- How large can mailbox databases grow? Even though most people won't reach their mailbox quota, you will need to plan the mailbox database size on the assumption that every mailbox will reach quota.
- What deleted item retention settings will you use? Deleted items consume database space in the same way that undeleted items do.
- Service Level Agreement (SLAs). Mailbox database size impacts recovery time, with larger mailbox databases meaning longer backup windows and longer recovery times. Backup and recovery can be more important to limiting mailbox database size than storage capacity.

The default database size limit for Exchange 2010 Service Pack 1 Standard edition is 1024 GB. If a mailbox database grows beyond this limit, the database automatically dismounts. You can modify the size limit of a database on the standard edition of Exchange 2010 by editing the registry. You can increase the database size limit to approximately 16 terabytes.

MORE INFO **MODIFYING DATABASE SIZE LIMIT**

For more information on modifying the database size limit on the Exchange Server 2010 Standard edition, consult the following TechNet webpage: *http://technet.microsoft.com/en-us/library/bb232092.aspx*.

Although it is possible for mailbox databases on the Enterprise edition of Exchange 2010 to grow to 16 terabytes in size, Microsoft recommends that you keep mailbox databases to approximately 2 terabytes in size—where that size is 120 percent of calculated maximum database size—if you are using a high-availability configuration. For example, if every user has a 5-GB mailbox quota and you use the 120 percent of calculated maximum database size rule, you'd be able to provision just over 340 mailboxes per mailbox database using the 2-terabyte limit. If you aren't using a high-availability configuration, the recommended maximum database size is approximately 200 GB. This figure was arrived at based on backup and recovery times and the requirements of normal SLAs. Using Database Availability Groups gives you more flexibility in terms of recovery, allowing a substantially higher database size limit.

MORE INFO **SIZE LIMITS**

To learn more about recommended mailbox database size limits, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ee832792.aspx*.

Determining mailbox database size is made more complicated by issues such as white space and database recoverable items. While an item deleted from a mailbox doesn't count towards a user's quota, the mailbox database still stores these items until the deleted item retention period expires. The amount of data consumed in this manner depends on the deleted item retention window. Microsoft provides the following formula for estimating how much storage is consumed in this manner:

Dumpster Size = (Daily Incoming/Outgoing Mail x Average Message Size x Deleted Item Retention Window) + (Mailbox Quota Size x 0.012) + (Mailbox Quota Size x 0.03)

MORE INFO **MAILBOX SERVER DESIGN EXAMPLE**

Microsoft has published an Exchange 2010 mailbox server role design example in a TechNet article. To review this example, go to: *http://technet.microsoft.com/en-us/library/ee832789.aspx*.

When planning mailbox database storage requirements, you must also consider the content index. Each mailbox database has a content index that allows users to be able to quickly search through mail items. This index usually consumes approximately 10 percent of a mailbox database's size.

MORE INFO **UNDERSTANDING MAILBOX DATABASE AND LOG CAPACITY FACTORS**

To learn more about mailbox database and log capacity factors, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ee832796.aspx*.

Plan Log Sizing

Transaction logs record every transaction performed by the Exchange database engine. Exchange writes each transaction to the log first and then those transactions are applied to the mailbox database later. Exchange Server 2010 transaction log files are 1 MB in size. Microsoft provides guidance that allows you to estimate the number of transaction logs that will be generated per mailbox per day assuming an average message that is 75 KB in size. A ballpark estimate is that for every five messages, Exchange generates one 1 MB transaction log file. Although you can enable circular logging, which overwrites transaction logs, Microsoft recommends you instead truncate transaction logs through regular backup. Products such as System Center Data Protection Manager 2012 allow you to perform backups every 15 minutes, truncating transaction logs regularly and minimizing the amount of transaction log data stored on the Exchange mailbox server.

Storage Performance Requirements

When planning storage for a mailbox server, you not only need to ensure that you dedicate enough space for the mailbox server, but you also need to ensure that the storage that you do use performs well enough to avoid being a bottleneck in the Exchange server's performance.

The basic principles of storage performance for mailbox servers are as follows:

- A larger number of users increases disk utilization.
- Users who send and receive more messages increase disk utilization.

Mailbox database performance is enhanced substantially through the use of server RAM for database caching. A user who sends and receives fifty 75-KB messages per day will utilize approximately 3 MB of RAM in the database cache. This user will also generate approximately 0.06 mailbox database I/O operations per second. A user who sends two hundred 75-KB messages per day will utilize approximately 12 MB of RAM in the database cache. This user will generate approximately 0.24 database I/O operations per second. When considering your mailbox server storage performance requirements, do not underestimate the impact of RAM. If the mailbox server has less RAM than is required to service each user's database cache needs, the number of database I/O operations per second will increase, reducing mailbox database performance.

The design of Exchange Server 2010 optimizes mailbox database I/O for standard hard disk drives. This means that you don't need specialized storage equipment to run an Exchange Mailbox server and that you'll have good performance even if you use "Just a Bunch of Disks" (JBOD), a technical way of describing standard, consumer-grade, hard-disk drives. Depending on your organization's requirements, you might choose to forego RAID 10 disk arrays in your storage design, relying less on redundant local storage and more on redundancy technologies such as Database Availability Groups. Of course it is always better to have a greater level of redundancy in any design. As any systems administrator knows, if something can go wrong, it will go wrong—usually at 4:50 P.M. on a Friday afternoon, right before you are about to go home for the weekend.

You can use the Exchange 2010 Mailbox Server Role Requirements Calculator, which you can download from Microsoft's website, to determine the precise storage and performance profile that will be necessary given your organization's needs. The tool is a spreadsheet that allows you to input information about your intended design. In general, though, Exchange 2010 is designed so that a 7200-RPM SATA disk will be easily able to handle the read and write traffic generated by a 2-terabyte mailbox database that hosts mailboxes that send and receive several hundred messages per day.

MORE INFO **EXCHANGE 2010 MAILBOX SERVER ROLE REQUIREMENTS CALCULATOR**

For more information about the Exchange 2010 Mailbox Server Role Requirements Calculator, consult this post on the Exchange team blog: *http://blogs.technet.com/b/exchange/archive/2009/11/09/3408737.aspx*.

When you are considering how to configure the disks used to host mailbox database and transaction logs, Microsoft recommends the following volume configurations:

- Use GUID partition table (GPT) rather than MBR in volume configuration. MBR is supported, but GPT is recommended.
- Only the NTFS file system is supported.
- Use an NTFS allocation unit of 64 KB for the volumes that host database files and log files.
- NTFS compression is not supported for database or log files.
- NTFS Encrypting File System is not supported for database or log files.
- BitLocker volume encryption is supported for volumes that host database files and log files.

Exchange supports the following storage architectures:

- **Direct-attached storage (DAS)** Directly attached to the server, without a storage network. Includes SCSI and SATA drives.
- **Storage Area Network (SAN)** Exchange supports the storage of mailbox databases on both iSCSI and Fibre Channel SANs.
- **Solid-state drive (SSD) flash disk** Exchange can be deployed on a solid-state (SSD) flash disk.

Windows Server 2008 and Windows Server 2008 R2 support 512-byte sector disks. Only Windows Server 2008 R2 with Service Pack 1 and Exchange Server 2010 with Service Pack 1 support 512e disks. All copies of the database must reside on the same disk type, you can't have some copies of a database stored on a 512-byte sector disk and other copies stored on 512e. If your organization is not using a UPS, you should disable physical disk-write caching.

MORE INFO **STORAGE CONFIGURATION**

To learn more about Mailbox server storage options, consult the following TechNet links: *http://technet.microsoft.com/en-us/library/ee832792.aspx*.

Best practice for hosting mailbox database or log data is RAID 1 or RAID 10. Microsoft recommends that when you use RAID 5, you have a maximum of seven disks in the array. If you are using RAID 6, you should enable high-priority scrubbing and surface scanning.

MORE INFO **MAILBOX STORAGE DESIGN**

For more information about the influence of performance on mailbox storage design, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ee832791.aspx*.

Mailboxes in Multiple-Forest Topologies

As you learned earlier, if your organization uses more than one forest, you can deploy Exchange in either the cross-forest topology or the resource-forest topology. When you deploy Exchange in a cross-forest topology, each Active Directory forest has its own Exchange organization and hosts its own Exchange mailboxes. When you use a resource-forest topology, one forest hosts the Exchange organization and the other forest hosts the user accounts used by recipients. You can give these users in a resource-forest topology mailbox access by using linked mailboxes.

Linked mailboxes are mailboxes in the resource forest that are associated with an account hosted in a trusted Active Directory forest. The accounts in the Exchange forest are disabled for logon. The disabled user account in the Exchange forest is then associated with an enabled user account in the accounts forest. You can create the disabled account separately, or have it created automatically as a part of the linked mailbox creation process.

To create a linked mailbox using EMC, perform the following general steps:

1. Navigate to Recipient Configuration console tree and click New Mailbox in the Action pane.
2. On the Introduction page, select Linked Mailbox and click Next.
3. On the User Type page, click New User and then click Next. This will allow you to create the dummy user account in the resource forest.

4. On the User Information page, enter the details of the dummy user account. You can choose a special Organizational Unit for the account. The password that you specify on this page will be used to access the mailbox even though the user account cannot be used for computer logon in the resource forest. This password does not have to match the password of the user account in the account forest.

5. On the Mailbox Settings pace, specify the mailbox database, retention policy, and Exchange ActiveSync mailbox policy that will be associated with the account.

6. On the Master Account page, shown in Figure 1-8, click Browse to specify the trusted domain, specify an account to access the linked domain controller, specify a domain controller in the trusted domain, and specify the account in the account domain that will be the master account for the linked mailbox. Click Next, New, and then Finish to complete the creation of the linked mailbox.

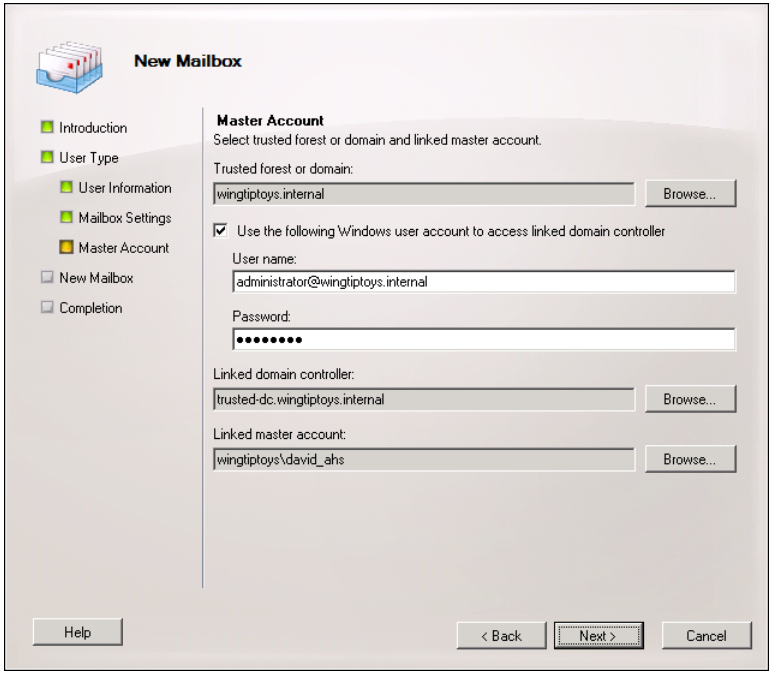


FIGURE 1-8 Linked mailbox master account

You can also create a linked mailbox from EMS by using the *New-Mailbox* cmdlet with the *LinkedMasterAccount* parameter. For example, to create a linked account for David Ahs in the local adatum.com forest when a trust has been established with the WingTipToys forest, use the following command:

```
New-Mailbox -Database "MBX-DB1" -Name "David Ahs" -LinkedDomainController
"DC01wingtiptoys" -LinkedMasterAccount wingtiptoys\david -OrganizationalUnit Users
-UserPrincipalName david@adatum.com -LinkedCredential:(Get-Credential wingtiptoys\Admin01)
```

A mail forest contact is a mail contact that is associated with a recipient object in another forest. Mail forests are present in cross-forest topology deployments and are usually created through Microsoft Identity Integration Server (MIIS) synchronization. Mail forest contacts can only be created through synchronization with other forests in a cross-forest deployment—you cannot modify or remove mail forest contacts using EMC or EMS.

MORE INFO **RESOURCE FOREST TOPOLOGY**

For more information about deploying Exchange Server 2010 in a Resource forest topology, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/aa998031.aspx*.

EXAM TIP

Understand the process of linked mailbox creation and the role of the disabled account.

MORE INFO **CREATE A LINKED MAILBOX**

For more information about creating a linked mailbox, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb123524.aspx*.

Recipient Policies

Recipient policies, also known as email address policies, allow you to configure email address formats for your organization. A single email address policy can define multiple address format variations. Email address policies allow you to generate addresses based on a person's first name, last name, middle initial, and accepted domains. You can only use accepted domains as the email domain suffix in an email address policy. You learned about accepted domains earlier in this chapter. The default email address policy for an organization involves the user's alias, the *at* symbol (@), and the default accepted domain.

You can use an email address policy to turn user name data into a variety of email addresses. By applying a policy, you could configure Exchange so that Kim Akers is given the following email addresses:

- k.akers@contoso.com
- kim.akers@contoso.com
- akers.kim@contoso.com
- akers.k@fabrikam.com

Although an email address policy can provision users with email addresses from multiple email domains, it's probably better to use separate policies when dealing with different email domains, which keeps things less complicated and more manageable. To create an email address policy using EMC, perform the following general steps:

1. Click the Organization Configuration\Hub Transport node and then click New E-mail Address Policy in the Actions pane.
2. On the Introduction page of the New E-mail Address Policy Wizard, enter a name for the policy, choose whether you want it to apply only to objects stored within a particular Active Directory container, and select the recipient types (mailbox users, mail-enabled users, and so on). Click Next.
3. On the Conditions page select which conditions will be used to limit the scope of the address policy. It is not necessary to limit the scope of the address policy—for example, if you want to apply the policy to all addresses in the organization. You can select from the following conditions:
   - **Recipient is in a State or Province** Checks for a match against the State/Province attribute of the Active Directory account. This property is set on the Address tab of an account's properties in Active Directory Users and Computers.
   - **Recipient is in a Department** Checks for a match against the Department attribute of the Active Directory account. This property is set on the Organization tab of an account's properties in Active Directory Users and Computers.
   - **Recipient is in a Company** Checks for a match against the Company attribute of the Active Directory account. This property is set on the Organization tab of an account's properties in Active Directory Users and Computers.
   - **Custom Attribute equals Value** It is also possible to configure up to 15 custom attributes for each account. The values of these attributes need to be set through Exchange management shell and aren't something that you can use Active Directory Users and Computers to configure.

MORE INFO **CONFIGURING CUSTOM ATTRIBUTES**

To learn more about configuring custom attributes, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ee423541.aspx*.

4. On the E-Mail Addresses page, click Add. On the SMTP E-Mail Address page, shown in Figure 1-9, select the format that you want to use for the email address and then click OK. If you want to add more address formats, you can click Add again. If you have multiple addresses listed in the policy, you need to specify one format as the default reply-to address. Click Next.

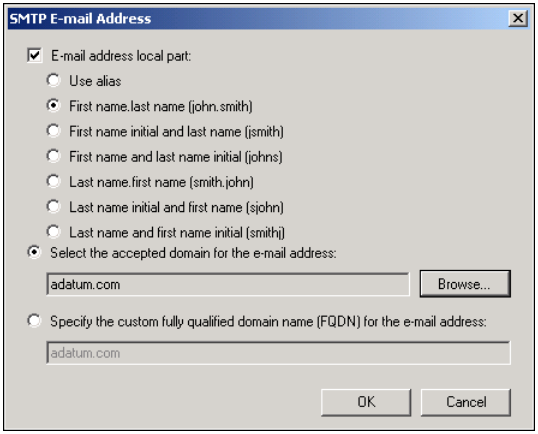


FIGURE 1-9 Email address format

5. On the Schedule page, select whether the policy is applied immediately, at a time in the future, or not applied at all.

You can apply multiple email address policies to a user. When you have multiple policies, you need to choose the order in which they apply. The reply-to address that is set in the policy with the highest priority is used as the default reply-to address. You can also manually configure a user's default reply-to address by editing the user's account properties directly. The default reply-to address set at this level overrides any set by policy.

You can use the following EMS cmdlets to manage email address policies:

- *New-EmailAddressPolicy* allows you to configure new address policies.
- *Get-EmailAddressPolicy* allows you to view the properties of existing policies.
- *Set-EmailAddressPolicy* allows you to modify the properties of existing policies.
- *Update-EmailAddressPolicy* allows you to apply policy changes to recipients within the scope of the policy. You must run this cmdlet after you create or modify an email address policy.
- *Remove-EmailAddressPolicy* allows you to remove existing policies, but will not remove email addresses from users that were created by those policies.

MORE INFO **RECIPIENT POLICIES**

For more information about email address policies, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb232171.aspx*.

Distribution Group Policies

A distribution group is a collection of recipients, sometimes known as mailing lists. When a user sends a message to a distribution group, Exchange will forward that message to all members of the distribution group. Exchange Server 2010 supports three types of distribution groups:

- **Distribution groups** A static group whose membership is managed manually.
- **Mail-enabled security groups** Similar to a distribution group, except that security permissions can be assigned to a mail-enabled security group. This static group type also requires that membership be managed manually.
- **Dynamic distribution groups** This group type has its membership generated automatically based on a query. For example, you might create a dynamic distribution group for everyone that works at a particular branch office according to their user account properties. When a person's account properties are updated to indicate that she works at that branch office, she will receive messages sent to that group. Group membership is calculated by a Hub Transport server when it receives a message addressed to the group.

MORE INFO **DISTRIBUTION GROUPS**

For more information about distribution groups, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb125256.aspx*.

Static Distribution Groups

Static distribution groups have several advantages over dynamic distribution groups. Static distribution groups allow you to define a membership where the objects in the group don't need to share a specific property. You can delegate management privileges of the distribution group to an ordinary user who can choose whom to add to the group. You can also configure group permissions so that users can add and remove themselves from the group as they choose. This functionality is very useful for things like project-based distribution groups. Mail-enabled security groups are also a type of static distribution group. If you are using the mail-enabled security group as a security group, remember that if you allow a non-administrative user to manage the group, you're also allowing that user to grant access to any resources to which the group has been assigned permissions.

To create a static distribution group using EMC, perform the following general steps:

1. Select the Recipient Configuration\Distribution Group node and then click New Distribution Group. This will launch the New Distribution Group Wizard.

2. Select whether you want to create a new distribution group or mail-enable an existing universal security group. If you want to mail-enable an existing universal security group, choose Existing Group, click Browse, and select the group. You can't mail-enable a security group with a domain local or global scope.

3. On the Group Information page, shown in Figure 1-10, choose between Distribution and Security. You can select an OU in which to place the group. You also need to provide a name, a pre-Windows 2000 name, and an alias name for the group. These can all be the same name. Then click Next, New, and then Finish.

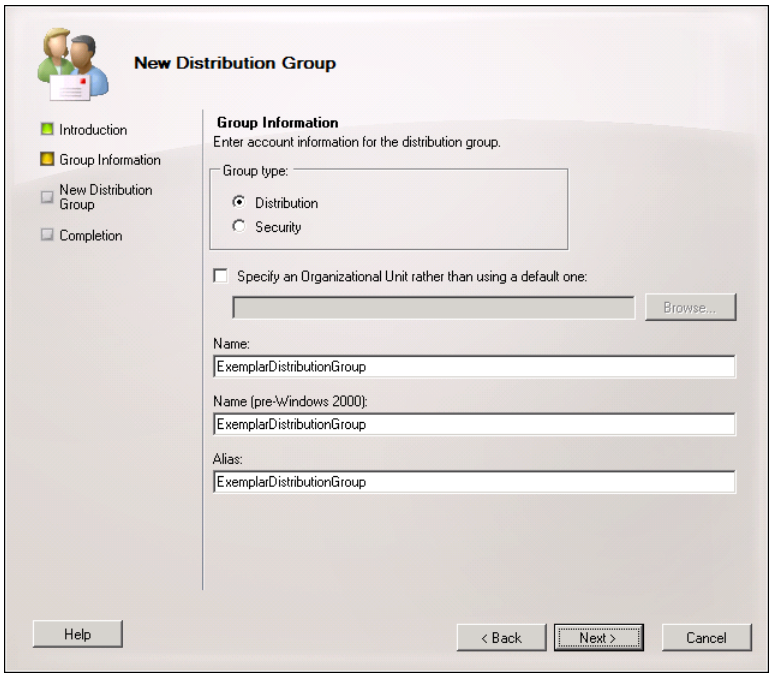


FIGURE 1-10 New distribution group

To create a new distribution group using EMS, use the *New-DistributionGroup* cmdlet. For example, to create a new mail-enabled security group named Alpha-Sec which will be stored in the Users container of the contoso.com domain, use the following cmdlet:

```
New-DistributionGroup -Name Alpha-Sec -OrganizationalUnit "Contoso.com/Users"
-SAMAccountName Alpha-Sec -Alias 'Alpha-Sec' -Type Security
```

The default manager of a distribution group is the user account that used to create the group. To delegate the ability to manage the group to another user, either use the *Set-DistributionGroup* cmdlet with the *ManagedBy* parameter, or navigate to the Group Information tab on the group's properties, shown in Figure 1-11, and click Add to specify a new group manager.

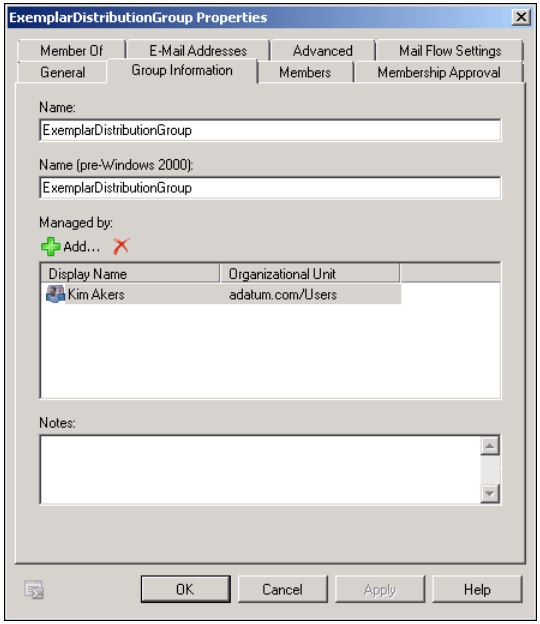


FIGURE 1-11 Configure distribution group manager

You can configure whether users are able to join the group themselves, whether they can join subject to approval, or if group members can only be added by the group managers on the Membership Approval tab, shown in Figure 1-12. You can also configure these settings using the *Set-DistributionGroup cmdlet* with the *MemberJoinRestriction* parameter using the options *Open, Closed*, or *ApprovalRequired*.

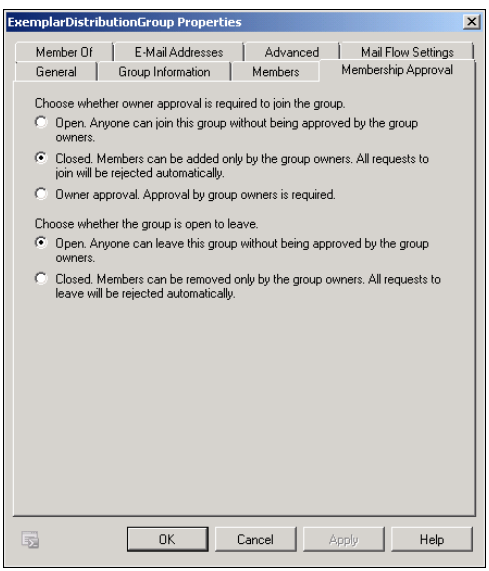


FIGURE 1-12 Membership approval

MORE INFO **CREATING STATIC DISTRIBUTION GROUPS**

For more information about creating static distribution groups, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb124513.aspx*.

Dynamic Distribution Groups

Creating a dynamic distribution group involves creating a query that defines the membership of the group. This query runs each time a message is sent to the group. This means that the membership of the group is calculated each time the group receives a new message. For example, a dynamic distribution group might be defined by a query that locates all accountants in the Traralgon office. Each time a message is sent to the group, Exchange calculates which recipients are accountants located in the Traralgon office and forwards the message appropriately. To create a dynamic distribution group in EMC, perform the following general steps:

1. Select the Recipient Configuration\Distribution Group node and then click New Dynamic Distribution Group in the Actions pane.
2. On the Introduction page, specify an Organizational Unit container to host the group if you do not want the group account stored in the default container. Specify a group name and alias. Click Next.
3. On the Filter Settings page, choose whether you want to only include objects from a specific Active Directory Domain or OU. Also, choose whether you want to include all recipient types or if you want to restrict the group to one or more of the following: mailbox users, mail-enabled users, resource mailboxes, contacts, and mail-enabled groups.
4. On the Conditions page select which conditions will be used to limit the scope of the address list. You can choose to limit the scope based on recipient Active Directory attributes including State or Province, Department, Company, or a custom attribute value. Click Next, New, and then Finish.

You can use EMS to create more complicated dynamic distribution groups—such as creating a distribution group that only includes users who have mailboxes on a specific mailbox server—through the use of recipient filters and the *New-DynamicDistributionGroup* cmdlet. For example, to create a dynamic distribution group called SYD-MBX-Users that contains only those users who have mailboxes on server SYD-EX1, use the following command:

```
New-DynamicDistributionGroup -Name "SYD-MBX-Users" -OrganizationalUnit Users
-RecipientFilter {((RecipientType -eq 'UserMailbox' -and ServerName -eq 'SYD-EX1') -and
-not(Name -like 'SystemMailbox{*'))}
```

MORE INFO **CREATING DYNAMIC DISTRIBUTION GROUPS**

For more information about creating dynamic distribution groups, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb123722.aspx*.

Public Folders

You need to include public folders in your design if you need to support clients that use Outlook 2003 or earlier. This is because these clients need to use public folders for performing free/busy searches and use them to obtain offline address books. A public folder database will be created on the first Exchange mailbox server that you deploy in your organization if you are deploying in a mixed environment, or indicate that you still need to support clients running Outlook 2003 or earlier.

Public folders almost always are inherited from a previous Exchange deployment. Organizations stick with them because of the effort involved in migrating to another solution. Microsoft recommends that organizations performing new deployments of Exchange use SharePoint rather than public folders. This is because the document management, authoring, and revisioning functionality of SharePoint better addresses how organizations interact with shared documents than Exchange public folder infrastructure does.

When designing public databases, consider the following:

- How large will your public folders be? As almost all organizations that use public folders with Exchange Server 2010 have used public folders with previous versions of Exchange. This means that you should be able to reasonably estimate the size of the necessary public folder databases. Unless you modify the registry, a public folder database cannot exceed 1024 GB in size on a computer running Exchange 2010 Standard edition.
- How often will public folders be accessed? The more often public folders are accessed, the greater the disk utilization.
- Do you need to support Outlook 2003? If your organization does not need to support Outlook 2003, you may wish to plan a migration of public folder content to SharePoint.
- If you want to support public folder replication as a way to make public folder content more failure tolerant, you will need to deploy a minimum of two public folder databases, each on a separate mailbox server.

You'll learn more about configuring public folders in Chapter 2.

MORE INFO **PUBLIC FOLDERS**

For more information about public folders, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb397221.aspx*.

Mailbox Provisioning Policies

Mailbox provisioning policies are a way of deciding where to place a specific Exchange mailbox. If you don't specify a mailbox database when provisioning a mailbox, the mailbox will be assigned automatically to an available mailbox database using a load-balanced approach. This can cause problems if you aren't careful—a new user's mailbox could be automatically deployed to a location that is geographically remote from where the user actually works.

Although placing a mailbox in the same Active Directory site as a user may be optimal from a performance standpoint because it allows high-speed access to a local Mailbox server, such a strategy might not be practical from an economic perspective. Mailbox servers cost money and you need to balance localized access performance with the economic realities of deploying multiple mailbox servers. If an organization has a large number of branch office sites with a relatively small number of employees, placing a Mailbox server at each site may not be viable from an administrative or economic standpoint. It may be cheaper to improve the connection to a central site than it is to provision that site with a local Mailbox server.

MORE INFO **MAILBOX SERVERS DON'T NEED TO BE IN THE SAME SITE**

All of the mailbox servers used by Microsoft's Australian and New Zealand offices are hosted in Singapore. From an end-user perspective, this works well without much in the way of appreciable lag. As long as you have a relatively high-bandwidth, low-latency connection to your mailbox server, it doesn't really matter if the mailbox server is in the same site or a different country.

When deciding where to place a mailbox, consider the following:

- Attempt to ensure that the mailbox is placed on a mailbox database that is either geographically close to the user or sufficiently provisioned with bandwidth that it does not cause the user performance problems.
- You can assign different quotas at the mailbox database and the individual mailbox level. Using a database-wide quota makes planning storage simpler than having a multitude of quotas applying to mailboxes hosted in the same database. If you need to use separate mailbox storage quotas in your organization, provision mailboxes to mailbox databases configured with appropriate quotas.
- If you use Exchange Online in conjunction with an on-premises deployment, it may make sense to place some mailboxes in the cloud rather than on a locally managed Exchange Mailbox server. This can be especially useful for remote sites with few users, though will require a cost benefit analysis to determine whether it is a more reasonable solution than hosting the mailbox at an on-premises location.
- Products such as Forefront Identity Manager (FIM) 2010 can be used to automate account and mailbox provisioning.

MORE INFO **EXCHANGE PROVISIONING WITH FIM 2010**

To learn more about automating mailbox provisioning with FIM 2010, consult the following TechNet magazine article: *http://technet.microsoft.com/en-us/magazine/ff472471.aspx*.

Your organization should also develop a mailbox deprovisioning policy. A mailbox deprovisioning policy details what steps should be taken in the event that a user leaves an organization. Although it might be tempting to simply delete the user mailbox after the user has left the building, compliance requirements often mean that the mailbox needs to be kept available in some manner for a certain period of time. How you design your deprovisioning policies will depend very much on your organizational needs and most organizations find a balance between deleting user mailboxes immediately and keeping zombie mailboxes on production servers for years after the employee has left the organization.

Objective Summary

- When determining how much storage space will be required by a mailbox database, take into account quotas as well as deleted item retention requirements.
- The amount of space required by transaction logs depends on average message size and how often the mailbox database is backed up.
- Although it is possible to have mailbox databases that are 16 terabytes in size, Microsoft recommends that mailbox databases do not exceed 2 terabytes in size on high-availability configurations and which do not exceed 200 GB in size for non-high-availability configurations.
- Use linked mailboxes to provide Exchange mailboxes to users with accounts in trusted forests.
- A maximum of five mailbox databases can be deployed on a mailbox server running the Standard edition of Exchange 2010. A maximum of 100 mailbox databases can be deployed on a mailbox server running the Enterprise edition of Exchange 2010. A maximum of one public folder database can be deployed per mailbox server.
- Recipient policies, also known as email address policies, determine the format of email addresses in the organization and the default reply-to address format.
- The membership of static distribution can be managed. Mail-enabled security groups must always use the universal scope. The membership of dynamic distribution groups is determined by a query.

Objective Review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. Your organization uses a resource-forest model, with two account forests and a single resource forest where you have deployed Exchange 2010. The account forests consist of multiple Active Directory domains. Which steps do you need to take to provision users in each account forests with mailboxes in the resource forest? (Choose two. Each answer forms part of a complete solution.)

   A. Ensure that there are forest trusts between the resource forest and the account forests.

   B. Install Exchange 2010 in the account forests.

   C. Create linked mailboxes in the resource forest.

   D. Create linked mailboxes in the account forests.

2. You have been asked by someone in management whether it is possible to configure a special address in Exchange so that people in the organization can send an email to that address and that email will be forwarded on to reach everyone who is currently a member of the Research department. The manager wants the mechanism by which this process works to be automatic. It should not require someone having to manually update the list of people who are in the Research department. The Human Resources department of your organization automatically populates the Department attribute for all Active Directory user accounts in your organization. Which of the following Exchange management shell commands would you use to meet management's goals?

   A. *New-Mailbox*

   B. *New-DistributionGroup*

   C. *Set-DistributionGroup*

   D. *New-DynamicDistributionGroup*

3. A mailbox database, hosted on a mailbox server running the standard edition of Exchange Server 2010 SP1, has dismounted because it has reached its maximum size. What steps can you take to increase the maximum size of the mailbox database beyond 1024 GB?

   A. Use the *New-MailboxDatabase* cmdlet.

   B. Use the *Get-MailboxDatabase* cmdlet.

   C. Edit the registry.

   D. Use the *Set-MailboxDatabase* cmdlet.

4. Your organization has three mailbox servers running Exchange Server 2010 SP1 Enterprise edition and two mailbox servers running Exchange Server 2010 SP1 Standard edition. What is the maximum number of Public Folder databases that you can deploy in this environment?

   A. 5

   B. 1

   C. 8

   D. 7

5. Your organization, currently known as Cohovineyard, is in the process of rebranding itself. An expensive consultant has decided that the name Cohowinery has more intrinsic synergy. You have obtained the appropriate rights to the cohowinery.com domain. You want to ensure that all users default reply-to address uses cohowinery.com rather than cohovineyard.com. Which of the following cmdlets should you use to accomplish this goal? (Choose three. Each answer forms part of a complete solution.)

   A. *New-AcceptedDomain*

   B. *Get-EmailAddressPolicy*

   C. *New-EmailAddressPolicy*

   D. *Update-EmailAddressPolicy*

THOUGHT EXPERIMENT
Recipient Policies, Distribution Groups

In the following thought experiment, apply what you've learned about the "Design the mailbox server role" objective to answer the following case study questions. You can find answers to these questions in the "Answers" section at the end of this chapter.

Your organization has two Active Directory forests, Contoso.com and Fabrikam.com. You have deployed Exchange Server 2010 in Contoso.com. A forest trust relationship exists between the Contoso.com and Fabrikam.com forests.

You want to help Simone from Accounts Receivable to set up a charity email list.

You have the following objectives:

- You need to be able to provide users who have accounts in the Fabrikam.com forest with email access in the Contoso.com Exchange organization.
- Users in the organization should use the *firstname.lastname*@contoso.com address format for their default reply-to address.
- Allow Simone from Accounts Receivable to manage the charity email list membership.
- Anyone in the organization should be able to join the charity email list subject to Simone's approval.

With this in mind, answer the following questions:

1. What kind of mailbox should you set up for users with accounts in the Fabrikam.com forest?
2. How can you ensure that all users in the organization will use the new default reply-to address format?
3. What steps should you take to create to support the charity email list?
4. What steps can you take to give Simone from Accounts Receivable the appropriate administrative privileges?
5. What approval setting should you configure for the group related to the charity email list?

Objective 1.4: Design Client Access

Client Access Servers (CAS) allow users to connect to their Exchange mailboxes, whether they are located on the same local area network or connecting remotely through Outlook Anywhere, VPN, Outlook Web App, or DirectAccess. When you are designing your organization's CAS deployment, you need to ensure that for every site with a mailbox server you have at least one CAS. In this objective, you'll learn about the factors you need to consider when creating a Client Access Server design for your organization. In Chapter 2 you'll learn about how to configure CAS to provide these services to users on your organization's network.

This objective covers:

- Plan Client Access Server location.
- Design to support remote and local access.
- Plan for supported Client Access Server services.
- Plan for Autodiscover.
- CAS support in multiple forest environments.

Planning Client Access Servers Location

The key fact that you need to remember when considering CAS placement is that you must place at least one CAS in every Active Directory site where there is a mailbox server. The greater the round-trip latency between the closest CAS and the mailbox server, the more degraded the experience is for clients accessing their mailboxes. You should also consider in your design the ability for CAS to function as proxies. This means that when a user who is in one site—for example, the Auckland site—is attempting to access his mailbox which is hosted on a mailbox server in a remote site such as the Wellington site, he will be able to use the CAS in the Auckland site to function as a proxy for the CAS in the Wellington site.

In earlier versions of Exchange, Outlook clients made a direct RPC connection to the mailbox server that hosted the appropriate mailbox. Exchange 2010 works differently in that the CAS functions as an intermediary, processing all client RPC requests. In an Exchange 2010 environment, the CAS interacts with the Mailbox server on behalf of the Outlook client. One of the most substantial benefits to this is that in the event of Mailbox server failure when Database Availability Groups are in use, the CAS automatically redirects clients to an available mailbox database.

NOTE **PUBLIC FOLDERS AN EXCEPTION**

Public folder connections are authenticated by the CAS, but still use RPC to interact directly with the public folder databases on the mailbox server.

CAS Proxying and Remote Access

The ability for one Exchange Server 2010 CAS to function as a proxy for another CAS will substantially influence your plans for an Exchange Server 2010 infrastructure. This is particularly useful when you have CAS and mailbox servers paired in sites that are not directly exposed to the Internet. For example, an organization may have CAS and Mailbox servers in the cities of Sydney and Melbourne, but only the Sydney CAS is exposed to the Internet. A user whose mailbox resides in the Melbourne site and who accesses OWA from the Internet would connect to the Sydney CAS. The Sydney CAS would then proxy that connection through to the CAS in the Melbourne site, rather than directly interacting with the mailbox server in the Melbourne site.

CAS Proxying not only works with traditional mailbox access through Outlook, but also works for access through Outlook Web App and Exchange ActiveSync. This technology allows you to provide access to Exchange for clients on the Internet by placing CAS on the perimeter network at a single site, knowing that CAS Proxying will ensure that those remote clients will be able to get access to the appropriate mailbox server.

MORE INFO **UNDERSTANDING CAS PROXYING AND REDIRECTION**

To learn more about CAS proxying and redirection, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb310763.aspx*.

Planning Client Access Server Services

When planning CAS deployment within your organization, you need to consider which services you want to offer. CAS provide the following services to an Exchange 2010 deployment:

- **Outlook Web App** Allows clients to access mailboxes through their browser. Many organizations provide this service to allow clients a quick way of remotely accessing their mailboxes without having to use a dedicated client.
- **RPC Client Access** Allows MAPI clients, such as Outlook 2010, to access mailboxes. This is the default way that Exchange mailboxes are accessed in most organizations through the CAS, primarily because organizations that are likely to use Exchange are also likely to use Outlook as their primary mail client.

- **POP3/IMAP4** Allows clients that don't support MAPI, such as Windows Live Mail, to access mailboxes. As more and more clients support either MAPI or (in the case of mobile clients) ActiveSync, the use of POP3 and IMAP4 is decreasing on most organizational networks.
- **Outlook Anywhere** Allows Outlook 2003 and later clients to access mailboxes through HTTPS. Outlook Anywhere can be used to allow remote mailbox access without granting DirectAccess or VPN access.
- **ActiveSync** Allows mobile devices that use Exchange ActiveSync to synchronize mailbox information. This protocol is often used by consumer devices such as the iPad to access Exchange mailboxes.
- **Availability Service** Provides clients with calendar free/busy information.
- **Exchange Web Services** Allows programmatic access to Exchange functionality through XML/SOAP interface. Rarely used by most organizations for Client Access scenarios.
- **MailTips** Provides users of Outlook 2010 and OWA with reminder information, such as whether the message recipient is out of office, or that they are sending to a distribution list.
- **Exchange Control Panel (ECP)** A web-based interface that allows Exchange administrators to perform certain tasks such as performing searches of all organizational mailboxes for messages that meet a specific set of criteria.
- **Address Book Service** Interface that allows address book queries.
- **Autodiscover** Service that allows clients running Outlook 2007 and later and Windows Mobile 6.1 and later to be automatically configured based on user profile settings.

Most of these services are enabled by default. It is possible to disable them specifically on a per-CAS or per-user basis. Figure 1-13 shows these services disabled on a per-mailbox basis.

MORE INFO **UNDERSTANDING CLIENT ACCESS SERVERS**

For more information about the functionality of Client Access Servers, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/bb124915.aspx*.

Exchange Control Panel

Exchange Control Panel (ECP) is a web-based control panel that, when accessed by a user, allows the user to configure items such as vacation settings, inbox rules, group management, password change, email signature, and spelling options. Users with administrative privileges can also use ECP to configured users, groups, roles, and auditing settings as shown in Figure 1-14. Users that have been delegated the Discovery Management role can use ECP to perform multi-mailbox searches.

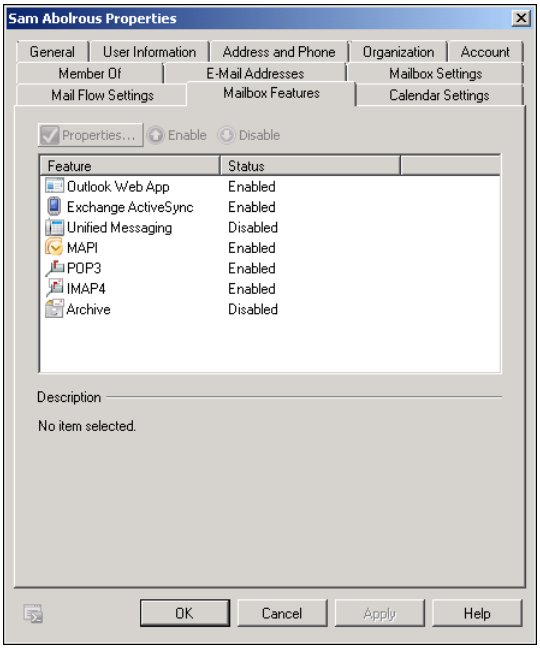


FIGURE 1-13 Client Access Server services

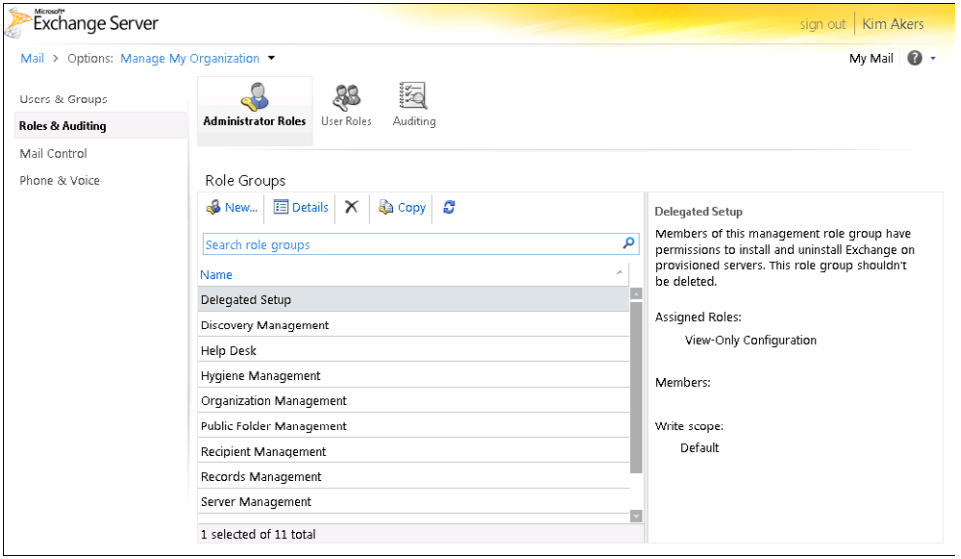


FIGURE 1-14 Exchange Control Panel

MORE INFO **EXCHANGE CONTROL PANEL**

For more information about the Exchange Control Panel, consult the following TechNet magazine article: *http://technet.microsoft.com/en-us/magazine/gg534653.aspx*.

Exchange ActiveSync

Exchange ActiveSync allows the syncing of Exchange mailbox information—including messages, calendar, and contact data—to mobile devices such as phones and tablets. ActiveSync supports a technology known as DirectPush. DirectPush allows the mobile device to maintain a persistent connection to Exchange, meaning that new messages are received in real time rather than according to a scheduled polling interval.

Exchange ActiveSync Policies, applied through the ActiveSync process on compatible devices, allow you to control the security of mobile devices. For example, you can use an ActiveSync policy to control password policies, whether to allow the use of hardware such as cameras, Bluetooth, or removable storage usage; whether to support remote-device wipe; and which applications can be executed on the device.

You would plan the use of ActiveSync policies in your Exchange Server 2010 infrastructure if you had specific concerns around mobile device security. You will learn more about ActiveSync policies and how they can be used to improve information security in Chapter 3, "Designing and Deploying Security For the Exchange Organization."

MORE INFO **UNDERSTANDING EXCHANGE ACTIVESYNC**

To learn more about Exchange ActiveSync, consult the following webpage: *http://technet.microsoft.com/en-us/library/aa998357.aspx*.

Testing Client Access Server Performance

Administrators can use the Load Generator (LoadGen) tool to plan an Exchange Server 2010 deployment to determine how well a CAS infrastructure performs under a simulated client load. By using this tool you can assess whether you need more CAS, whether your planned deployment meets expectations, or whether you have overprovisioned the CAS role.

LoadGen is able to simulate the following types of client activity:

- Microsoft Office Outlook 2003 (online and cached)
- Outlook 2007 (online and cached)
- POP3
- IMAP4
- SMTP

- ActiveSync
- Outlook Web App

You can choose whether to simulate a single-protocol workload or combine client protocols to determine how well the CAS infrastructure deals with a multi-protocol workload. Using LoadGen you can also calculate client computer response time when CAS are under a specific load, estimate the number of users that each CAS will be able to provide services to concurrently, and identify hardware and design bottlenecks.

> ***MORE INFO*** **EXCHANGE PERFORMANCE AND SCALABILITY TOOLS**
>
> **For more information on tools that you can use to test the performance and scalability of Exchange Server 2010, consult the following TechNet link: *http://technet.microsoft.com/en-us/library/dd335108.aspx*.**

Client Access Server Hardware Requirements

Microsoft has done a substantial amount of research on Client Access Server capacity. You can reference this research in detail if you are interested in determining the relative weighting that you should give Client Access Server processor capacity in terms of the capacity of your organization's Mailbox server. A rough summary of Microsoft's finding is that you should deploy three Client Access Server processor cores in an Active Directory site for every four mailbox server cores, assuming cores of equal processing capacity. Exchange Client Access Servers will still function if you use a ratio that differs from this theoretically optimal one. The idea of this ratio is to give you an idea of what the optimal ratio is, so that you can figure out if the Client Access Server at a site might be a bottleneck in Exchange performance because it is under-resourced with processor capacity, or if you have overprovisioned the Client Access Server role with CPU capacity that will never be utilized.

> ***MORE INFO*** **RELATIVE COSTS OF EXCHANGE 2010 CLIENT ACCESS SERVER WORKLOADS**
>
> **For more information about the relative performance costs of Client Access Server workloads, consult the following white paper on Microsoft's website: *http://technet.microsoft.com/en-us/library/ff803560.aspx*.**

Planning Autodiscover

The Autodiscover service simplifies the process of configuring Outlook 2007, Outlook 2010, and mobile devices. Autodiscover allows the automatic provisioning of a user's profile given the user's email address and password. Rather than having to configure all necessary settings, the user simply enters her email address and password into the email client and all relevant mail server settings are automatically provided to the client through the Autodiscover service.

MORE INFO **AUTODISCOVER**

To learn more about the Autodiscover service, consult the following TechNet document: *http://technet.microsoft.com/en-us/library/bb124251.aspx*.

Planning Site Affinity for Autodiscover

If your organization has a number of clients that move between sites, you may wish to configure the Autodiscover service to use site affinity. When you configure the Autodiscover service to use site affinity on the Client Access Server, clients using Outlook 2007 or Outlook 2010 will be provisioned with Autodiscover information from the closest Active Directory site. In some organizations with geographically dispersed branch offices, this can substantially improve the performance of Autodiscover.

MORE INFO **AUTODISCOVER SITE AFFINITY**

To learn more about configuring the Autodiscover service to use site affinity, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/aa998575.aspx*.

Planning Autodiscover for Internet Clients

You can configure Autodiscover so that remote clients on the Internet can automatically provision profile settings by entering their email address and password. For example, by using Autodiscover and using Outlook Anywhere, a user who is connected to the Internet can fully configure Outlook by entering his email address and password. The main requirement for Autodiscover for Internet clients is that you have an SSL certificate that is trusted by the client computer's operating system. If the majority of the clients that will use this service are using their own consumer devices, the simplest approach to ensuring that the SSL certificate is trusted by clients is to obtain the SSL certificate from a trusted third-party Certificate Authority.

MORE INFO **CONFIGURE AUTODISCOVER FOR INTERNET ACCESS**

To learn more about configuring the Autodiscover service for Internet clients, consult the following TechNet webpage: *http://technet.microsoft.com/en-us/library/aa995928.aspx*.

Autodiscover in Multiple-Forest Environments

Autodiscover, when appropriately configured, supports cross-forest topologies. When Autodiscover is appropriately configured, a client that supports Autodiscover on a computer in another forest can be provisioned automatically by the local forest's Client Access Servers. For example, Contoso might have a cross-forest topology in which one Exchange organization

is in Australia and another Exchange organization is in New Zealand. When Autodiscover is configured to support the multiple-forest environment, a user that logs on in the New Zealand forest—but who has been configured with a mailbox in the Australian Exchange organization—will be able to have those Australia-based profile settings automatically provided to her client by providing her email address and password.

MORE INFO **AUTODISCOVER IN MULTIPLE FORESTS**

For more information about configuring the Autodiscover service to support multiple-forest topologies, consult the following TechNet link: *http://technet.microsoft.com/en-us/library/aa996849.aspx*.

Planning Client Access Server Certificates

Server certificates, also commonly known as Secure Sockets Layer certificates, allow clients to establish a secure connection to a host that has a verified identity. This is very useful in CAS scenarios where a multitude of clients need to be able to use a CAS to securely access mailbox data through a variety of protocols.

Something that you must consider in your design is that unless you take specific steps to remedy the situation, Exchange defaults to using self-signed certificates created during the installation process. This is fine for communication between Exchange servers in the same organization because these servers trust these self-signed certificates. This is problematic for clients who are unlikely to trust these self-signed certificates without you performing remedial action. If a significant number of Exchange clients are going to be running computers that are not a part of your organization's domain, you should consider obtaining an SSL certificate from a trusted third-party Certificate Authority (CA). Although these trusted third-party CA certificates do have a fee associated with them, the cost of supporting the deployment of a certificate issued from an internal CA to clients that aren't members of a domain often exceeds the cost of obtaining the third-party certificate.

The key to planning the names assigned to certificates used by Client Access Servers is knowing the name that client will be using to access each required client protocol on the server. For example, you might be planning to have users connect to Outlook Web App using the address *https://owa.wingtiptoys.com,* to the POP3 server using POP.wingtiptoys.com, to Autodiscover using Autodiscover.wingtiptoys.com, and to IMAP4 using IMAP4.wingtiptoys.com. In this situation you need to ensure that the certificate you install supports all of these names. In this situation you can plan to take one of the following options:

- Obtain four separate certificates, one for each separate name. This is the traditional option, although it can be more cumbersome to implement.
- Obtain a single certificate that supports multiple subject alternative names (SANs). Getting a certificate that supports multiple SANs is usually the best option and almost all trusted third-party CAs will issue them more cheaply than they'll issue multiple

separate certificates. You have to perform a minor modification to a Windows Server 2008 R2 CA to configure them to support the issuance of certificates with multiple SANs.

- Obtain a certificate with a wildcard name. These certificates are also supported by most public CAs. In the example situation you would configure the certificate with the wildcard name *.wingtiptoys.com.
- Configure all services to use the same name, such as mail.wingtiptoys.com. This allows you to solve this problem by only needing to acquire a single certificate.

MORE INFO **SSL FOR CLIENT ACCESS SERVERS**

For more information about preparing to use SSL certificates with Client Access Servers, consult the following TechNet document: *http://technet.microsoft.com/en-us/library/bb310795.aspx*.

EXAM TIP

Remember to place a CAS in the same site as your organization's Mailbox servers.

Objective Summary

- Include Outlook Anywhere in your design if you want to allow users remote access to Exchange without having to provision a VPN solution or DirectAccess. Outlook Anywhere is supported on clients running Outlook 2007 and Outlook 2010.
- ActiveSync allows supported mobile devices to access mailbox data.
- You can configure Autodiscover to automatically provision Outlook 2007 and Outlook 2010 clients. When properly set up and used in conjunction with Outlook Anywhere, Autodiscover can provision clients on the Internet.
- You can configure Autodiscover with ActiveSync to automatically provision ActiveSync clients based on email address and password.
- POP3 and IMAP4 can be enabled on CAS to support non-Outlook messaging clients that do not support ActiveSync or MAPI.
- Subject Alternative Name (SAN) certificates allow multiple FQDNs to be associated with a single certificate.
- The Load Generator (LoadGen) tool can be used to test a CAS against a simulated client workload.
- Exchange Control Panel allows administrators to perform discovery and RBAC tasks. It allows normal recipients to perform tasks such as password change, group creation, and rules management.

Objective Review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You are in the process of evaluating a CAS deployment to determine whether it will be able to cope with a projected client load. Which of the following tools could you use to assist you in performing that evaluation?
   - **A.** LoadGen
   - **B.** Jetstress
   - **C.** Exchange Best Practices Analyzer
   - **D.** Exchange Remote Connectivity Analyzer
2. You are planning your organization's Exchange Server 2010 deployment. Your current plans involve placing two mailbox servers at the Sydney and Melbourne sites and one mailbox server at the Adelaide, Brisbane, and Darwin sites. What is the minimum number of Client Access Servers that you need to deploy to support this configuration?
   - **A.** 1
   - **B.** 4
   - **C.** 5
   - **D.** 7
3. Tailspin Toys has its main office in Auckland and branch offices in Christchurch, Wellington, and Dunedin. The Auckland site has two mailbox servers. What is the minimum number of Client Access Servers that need to be deployed to support this configuration?
   - **A.** 1
   - **B.** 2
   - **C.** 4
   - **D.** 8
4. What is the theoretical optimum ratio of Client Access Server processor cores to Mailbox server processor cores in a single Active Directory site?
   - **A.** Three Client Access Server processor cores for every four Mailbox server processor cores
   - **B.** Four Client Access Server processor cores for every three Mailbox server processor cores
   - **C.** Two Client Access Server processor cores for every three Mailbox server processor cores
   - **D.** Three Client Access Server processor cores for every four Mailbox server processor cores

5. You want to ensure that Outlook 2010 clients get Autodiscover information from the closest Active Directory site. Which of the following steps should you include in your Client Access Server deployment plan to accomplish this goal?

   A. Configure the Autodiscover Service for Internet Access.

   B. Configure the Autodiscover Service for Multiple Forests.

   C. Configure the Autodiscover Service to use Site Affinity.

   D. Configure Exchange ActiveSync Autodiscover Settings.

THOUGHT EXPERIMENT
Moving a Site from an Intranet to the Internet

In the following thought experiment, apply what you've learned about the "Design client access" objective to design a CAS implementation for Wingtip toys. You can find answers to these questions in the "Answers" section at the end of this chapter.

Wingtip Toys has its head office site in Auckland, New Zealand. There are branch office sites in the cities of Wellington, Dunedin, and Christchurch. You intend to deploy mailbox servers at each of these locations.

You want to support Outlook Web App, Outlook Anywhere, Autodiscover, IMAP4, ActiveSync, and MAPI.

You want to ensure that people working from home on their personal computers are able to securely access Outlook Web App.

You want to allow access to Exchange mailboxes for external clients running Outlook 2010 without having those clients use VPN or DirectAccess technologies.

With these factors in mind, answer the following questions:

1. **In which sites must you deploy Client Access Servers?**
2. **How can you ensure that clients using Autodiscover are provisioned with profile information from the closest Active Directory site?**
3. **You want to minimize the number of certificates that you install on each CAS. What steps could you take to accomplish this goal?**
4. **What technology should you deploy to allow remote access to Exchange mailboxes for clients running Outlook 2010?**
5. **What type of Certificate Authority should you use to obtain the SSL certificate for the Client Access Server hosting Outlook Web App at the Auckland site?**

Objective 1.5: Plan for Transition and Coexistence

One thing to keep in mind when planning for transition from Exchange 2003 or Exchange 2007 to Exchange 2010 or coexistence is that the term *upgrade* isn't entirely accurate. You can't perform an in-place upgrade from either Exchange 2003 or Exchange 2007 to Exchange 2010 in so far as it is not possible to directly upgrade a server running either of these products to Exchange 2010. An upgrade involves installing Exchange 2010 into your existing Exchange organization and then moving data and functionality across to the new Exchange 2010 servers. A migration involves moving from one messaging system to another. If you are performing a migration from Exchange 2003 or Exchange 2007, you install Exchange 2010 in a new Active Directory forest and then migrate data across.

This objective covers:

- Plan and investigate consolidation of Exchange servers.
- Plan transition from Exchange 2003 to Exchange 2010.
- Plan transition from Exchange 2007 to Exchange 2010.
- Plan transition from mixed Exchange 2003 and Exchange 2007 environment to Exchange 2010.
- Plan coexistence with third-party messaging systems.

Exchange Consolidation

As organizations are able to deploy more powerful hardware, they are able to consolidate their Exchange deployment onto fewer servers. For example, an organization that may have had 10 Exchange 2007 mailbox servers might, with the substantially better hardware that has become available in the intervening years, be able to service the same number of clients with fewer servers. Hardware improvements aside, Exchange Server 2010 has been engineered to provide better performance on the same hardware compared to previous versions of Exchange. When planning a transition from Exchange 2003 or Exchange 2007 to Exchange 2010, remember that you may not need to have as many Exchange 2010 servers as you had previously because of improvements in hardware an Exchange performance.

To determine the capacity of your new servers, Microsoft makes available two tools that you can use to perform a capacity analysis on your hardware. The drawback of these tools is that you have to actually have the hardware to test it against. The first tool, Exchange Server Jetstress 2010, allows you to perform I/O benchmarking against the storage on a mailbox server. The second tools, Exchange Server Load Generator 2010 (LoadGen) allows you to simulate a client workload against a test Exchange environment. You learned about LoadGen earlier in this chapter. Using these tools, you can make informed estimates about the capacity of the Exchange 2010 servers that you are going to deploy.

MORE INFO **TOOLS FOR SCALABILITY EVALUATION**

To learn more about the tools that are available for evaluating scalability, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/dd335108.aspx*.

Upgrade Approaches

When you are developing your upgrade plan, you have to decide whether you are going to perform a single-phase upgrade or whether you are going to prepare a multiphase upgrade with coexistence. The differences between these two approaches are as follows:

- Single-phase upgrades involve replacing an existing messaging system with Exchange Server 2010. Single-phase upgrades minimize the coexistence period between the two systems and all required data and services are moved to Exchange 2010 as expeditiously as possible. These upgrades allow the transition to occur quickly, but the chance of problems arising is higher than when the transition occurs at a more measured pace.
- Multiphase upgrade with coexistence is a more measured approach to transitioning to Exchange Server 2010. This might involve upgrading one server at a time or one site at a time. This is often a more pragmatic approach for large sites where a quick transition of the existing infrastructure is infeasible because of the size of the migration. This involves planning for a period of interoperability. Although supporting interoperability is more complicated, the more measured approach allows each phase in the migration to be completed separately before moving on to the next phase.

When using a multiphase upgrade with coexistence strategy, you need to ensure that users that have mailboxes hosted on both the existing and the Exchange 2010 messaging system have access to the following:

- **Public folders** If your Exchange 2003 or Exchange 2007 organization uses public folders, you will need to come up with a way of replicating public folder data between systems. As an alternative, you could migrate public folder data to SharePoint if you don't need to support Outlook 2003 clients.
- **E-mail message flow** You need to keep this working transparently so that users of the old and new systems are able to send email to each other without having to know whether the destination mailbox is on the old or new system.
- **Global Address List (GAL)** You need to ensure that users of both systems are able to efficiently locate addresses and address lists on both the old and new systems.
- **Calendar information** Users in on both the old system and the new system need to be able to schedule meetings and view free/busy data of other people in the organization irrespective of which messaging system people's mailboxes reside on.
- **Administration tools** Exchange administrators need to be able to quickly and efficiently manage servers running both the original messaging system and Exchange Server 2010.

Multiple Sites

Transitioning an organization that has a single site from Exchange 2003 or Exchange 2007 to Exchange 2010 is far simpler than transitioning an organization that has sites spread across geographically dispersed locations. When planning a transition from a previous version of Exchange to Exchange 2010, keep the following in mind:

- You must upgrade Internet-facing sites prior to upgrading internal sites. This restriction is due to Client Access Server proxying functionality.
- When upgrading a site, upgrade Exchange roles by introducing servers in the following manner:
  1. Client Access
  2. Hub Transport
  3. Mailbox
  4. Edge Transport

The Edge Transport server is only necessary if you are choosing to use an Edge Transport server rather than a third-party email gateway. Edge Transport servers are also only deployed on perimeter networks at Internet-facing sites, so you don't need to plan on deploying them at every site during a transition to Exchange 2010.

Exchange 2003 Upgrade or Coexistence

When planning an upgrade or coexistence scenario for an Exchange 2003 organization that you wish to transition to Exchange 2010, first ensure the following:

- Your Exchange 2003 organization is running in Native rather than Mixed mode.
- All servers running Exchange 2003 are upgraded to Exchange 2003 Service Pack 2.
- At least one global catalog server in each site is running at Windows Server 2003 Service Pack 2 or later.
- The computer that hosts the schema master role is running at Windows Server 2003 Service Pack 2 or later.
- The domain and forest functional level are configured at the Windows Server 2003 or higher level.

As you'll learn in Chapter 2, the requirements for Exchange Server 2010 SP1 are slightly different than those published for Exchange Server 2010 RTM, and that the 70-663 exam targets RTM rather than SP1. It is also worth checking with the relevant TechNet documentation that is linked to this and the next chapter to determine whether any other prerequisites have changed when Exchange Server 2010 Service Pack 2 is released. Chapter 2 will cover the process in more detail, but in general your plan should involve the following steps:

1. Upgrade any Internet-facing sites first.

2. Install the Client Access Server first. Configure clients to use the new Exchange 2010 Client Access Server as their connection point to both Exchange 2010 and Exchange 2003.
3. Install the Hub Transport role after the Client Access Server has been deployed. The first Hub Transport server deployment will involve you specifying an Exchange 2003 bridgehead server.
4. Deploy the Mailbox servers in the site.
5. Deploy the Edge Transport server and configure EdgeSync.
6. After you have performed steps 2 through 4 on all Internet-facing sites, perform steps 2 through 4 on all non-Internet-facing sites.
7. Begin migrating public folders and mailboxes from the Exchange 2003 servers to the Exchange 2010 servers. In multiple-site upgrades, you can begin moving mailboxes and public folders prior to upgrading additional sites if you so choose.

When planning a transition from Exchange 2003 to Exchange 2010, remember that the following Exchange 2003 features are not supported in Exchange 2010:

- **Novell GroupWise connector** This connector allows coexistence between Novell GroupWise and an Exchange 2003 organization. If your organization requires the functionality this connector provides, it will be necessary to retain at least one server running Exchange 2003 in your environment until the functionality is no longer required or another solution becomes available.
- **NNTP** Network News Transfer Protocol (NNTP) allows the use of newsgroup content. If it is necessary to retain NNTP functionality in your organization, either retain a server running Exchange 2003 or look for a third-party NNTP server solution.
- **Office Outlook Mobile Access** The functionality that was provided by Office Outlook Mobile Access is now provided through ActiveSync.
- **Inter-Organization Replication Tool** This tool allowed the exchange of meeting, appointment, and contact data between two different Exchange 2003 organizations. Exchange Server 2010 uses Microsoft Federation Gateway to provide this functionality.

Once you have moved all public folder and mailbox server data from Exchange 2003 to Exchange 2010, you can begin to decommission the existing Exchange 2003 infrastructure. Microsoft recommends that you remove Exchange 2003 in the following manner:

- Remove Exchange 2003 back-end servers first. You can remove back-end servers as soon as all the relevant data on the server has been migrated across to Exchange 2010.
- Remove the Exchange Server 2003 bridgehead server after you've removed the last mailbox server in a routing group.
- Remove the Exchange 2003 front-end servers last.

MORE INFO **PLANNING EXCHANGE 2003 UPGRADE OR COEXISTENCE**

To learn more about the planning roadmap for Exchange 2003 upgrade or coexistence, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/aa998186.aspx*.

Exchange 2007 Upgrade or Coexistence

Exchange 2007 has a superficially similar structure to that of Exchange 2010 with both systems utilizing the Hub Transport, Edge Transport, Mailbox and Client Access Server roles. As is the case with an upgrade from Exchange 2003, you'll need to ensure that the global a catalog server in each site and the schema master is upgraded to the appropriate service pack level for the deployment of Exchange 2010 SP1. You also need to ensure that the forest functional level is set to Windows Server 2003. Finally, prior to attempting upgrade, ensure that all Exchange 2007 servers have Exchange 2007 Service Pack 2 installed. The specifics of upgrading Exchange 2007 to Exchange 2010 are covered in more detail by Chapter 2, but in general you need to perform the following steps:

1. In multi-site environments, upgrade any Internet-facing sites before upgrading any internal sites.
2. Deploy the Exchange 2010 Client Access Server first. After this is done, modify Autodiscover settings to point at the Exchange 2010 Client Access Server.
3. Install the Exchange Server 2010 Hub Transport server. During coexistence, you will have both Exchange Server 2010 and Exchange Server 2007 Hub Transport Servers in the same sites.
4. Install the Exchange Server 2010 Mailbox servers. You can begin migrating mailboxes and public folder data from Exchange Server 2007 Mailbox servers at this stage, or wait until several sites are upgraded fully before taking that step.
5. Install the Exchange Server 2010 Edge Transport Servers. Exchange Server 2010 Edge Transport servers can only synchronize with Exchange Server 2010 Hub Transport Servers.
6. Repeat steps 2 through 5 at all Internet-facing sites before performing steps 2 through 4 at all non-Internet-facing sites.

When planning an upgrade from Exchange 2007 to Exchange 2010, ensure that you account for the fact that the following Exchange 2007 features are not supported in Exchange 2010:

- **Single Copy Cluster** Exchange 2007 high-availability features have been replaced in Exchange 2010 by Database Availability Groups. You'll learn more about Database Availability Groups in Chapter 4.

- **Local Continuous Replication** Exchange 2007 high-availability features have been replaced in Exchange 2010 by Database Availability Groups. You'll learn more about Database Availability Groups in Chapter 4.
- **Cluster Continuous Replication** Exchange 2007 high-availability features have been replaced in Exchange 2010 by Database Availability Groups. You'll learn more about Database Availability Groups in Chapter 4.
- **Standby Continuous Replication** Exchange 2007 high-availability features have been replaced in Exchange 2010 by Database Availability Groups. You'll learn more about Database Availability Groups in Chapter 4.
- **Microsoft Transport Suite for Lotus Domino** This tool allowed for interoperability between Exchange 2007 environments and Lotus Domino. It also provided tools that could be used to migrate users from Lotus Domino to Exchange Server 2007. If you need to retain interoperability with your organization's Lotus Domino messaging system, you'll need to retain at least one server running Exchange 2007 in your Exchange organization.
- **Programmatic Access to Exchange through ExOLEDB, WebDAV, or CDOEX (CDO for Exchange 2000 Server)** This functionality has been replaced by the Exchange Web Services (EWS) or EWS-Managed API. If you have not migrated the applications that use this technology to utilize the EWS-Managed API, you'll need to retain at least one server running Exchange 2007 in your Exchange organization.

After you have moved all data from your organization's Exchange 2007 Mailbox servers to the new Exchange 2010 Mailbox servers, you'll be able to begin removing the Exchange 2007 infrastructure. Remove Exchange 2007 servers in the following order:

1. Remove Mailbox servers first. You can decommission a mailbox server as soon as you have removed all mailbox and public folder data from it.
2. When all Exchange 2007 Mailbox servers at a site have been removed, you can remove any Exchange 2007 Hub Transport servers at that site.
3. Remove the Exchange 2007 Client Access Servers and Edge Transport servers.

MORE INFO **PLANNING EXCHANGE 2007 UPGRADE OR COEXISTENCE**

To learn more about the planning roadmap for Exchange 2007 upgrade or coexistence, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/dd638158.aspx*.

Mixed Exchange 2003 and Exchange 2007 Environments

Planning to upgrade a mixed Exchange 2003 and Exchange 2007 environment is similar to upgrading from environments containing a single Exchange 2003 or Exchange 2007 organization. You'll need to upgrade Internet-facing sites first by introducing Client Access, Hub Transport, and then Mailbox servers. Introduce Edge Transport servers at this stage as

appropriate. Move data from Exchange 2003 back-end and Exchange 2007 Mailbox servers to Exchange 2010. Begin decommissioning, removing the Exchange 2003 back-end servers, bridgehead servers, and then front-end servers. Then remove the Exchange 2007 Mailbox servers, Hub Transport servers, Client Access Servers, and then Edge Transport servers.

Exchange Server Deployment Assistant

The Exchange Server Deployment Assistant, also known as ExDeploy, which you learned about earlier in this chapter, is an excellent tool for generating checklists to assist you with transitioning your organization from Exchange 2003, Exchange 2007, or a mixed Exchange 2003 and Exchange 2007 environment to Exchange Server 2010. The tool is Silverlight-based and generates a transition checklist based on the answers you provide to a series of questions about your environment. The checklist for an Exchange 2003 to Exchange 2010 environment is shown in Figure 1-15.

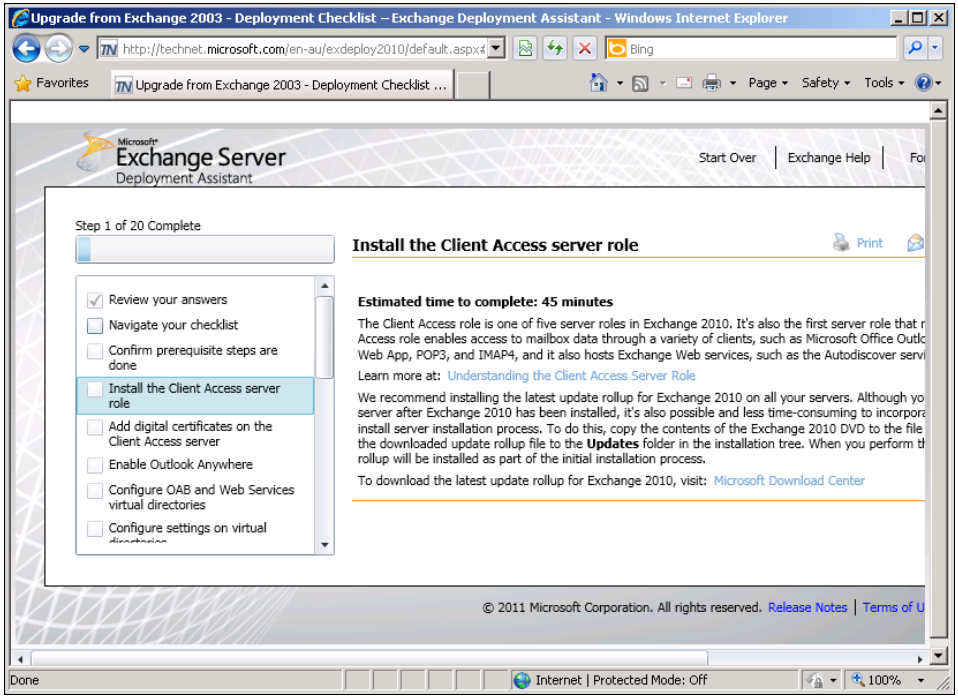


FIGURE 1-15 Exchange Server deployment checklist

You can use this automatically generated checklist as a guide in developing your plans to transition your organization from previous versions of Exchange. You can also use the checklist to verify each step of the transition process.

MORE INFO **EXCHANGE SERVER DEPLOYMENT ASSISTANT**

To learn more about the Exchange Server Deployment Assistant, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/ee681665.aspx*.

Coexistence with SMTP-Based Messaging Systems

Many organizations use messaging systems from multiple vendors. This is often the case in environments that have substantial UNIX-based deployments where each team of administrators is wary of using systems hosted on different platforms, though you may have other technical and political reasons to maintain a multi-vendor messaging infrastructure.

In most cases the third-party messaging system will support SMTP traffic and it is possible to get the both Exchange and the third-party messaging system to communicate by configuring appropriate internal Send and Receive connectors.

MORE INFO **UNDERSTANDING SEND CONNECTORS**

For more information about Send connectors, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/aa998662.aspx*.

Coexistence with non-SMTP Messaging Systems

Although almost all modern previous versions of Exchange did offer connector and migration tools for third-party products such as Lotus Notes and Novell GroupWise, but these connectors are not present in Exchange Server 2010. Exchange 2010 does support foreign connectors for third-party messaging systems, but you need to obtain those connectors from the vendor of the third-party messaging system or another third-party vendor who might provide their own set of tools.

You can also use delivery agents and Foreign connectors to deliver messages to third-party non-SMTP messaging systems. Although Foreign connectors are supported in Exchange Server 2010, Microsoft recommends that you use Delivery Agents for coexistence functionality. Delivery agents have the following benefits:

- Allows queue management for messages routed to foreign systems using standard queue management tasks
- Improved performance
- Can use the message representation and management features of Exchange
- Provides confirmation that messages have been delivered to the third-party system
- Allows administrators to track latency of message delivery to the foreign system

MORE INFO **DELIVERY AGENTS**

For more information about delivery agents, consult the following TechNet article: *http://technet.microsoft.com/en-us/library/dd638118.aspx*.

Global Address List Synchronization

In coexistence scenarios, it is often useful to include some sort of Global Address List scenario so that users of the Exchange messaging system are able to view and search addresses in the third-party messaging system. Similarly, users of the organization's third-party messaging system are likely to want to be able to search and view addresses of users with Exchange mailboxes. How effectively this can be done depends very much on the functionality available in the third-party messaging system. You have the following options when it comes to planning synchronization of Global Address lists between Exchange 2010 and third-party messaging systems:

- You may be able to use the GAL synchronization functionality available in Forefront Identity Manager 2010, though this is mostly used to support Exchange cross-forest topologies.
- The third-party vendor might provide a GAL synchronization tool that automatically synchronizes the third-party global address list with Exchange.
- You can create Lightweight Directory Access Protocol (LDAP) replication scripts. You can only do this if the third-party messaging system supports using LDAP queries to extract mailbox and contact information. These scripts will have to be run manually or be automated in some fashion.

MORE INFO **GAL SYNCHRONIZATION**

To learn more about GAL synchronization using the Forefront Identity Manager product, consult the following TechNet presentation: *http://technet.microsoft.com/en-us/edge/Video/hh150143*.

EXAM TIP

Remember the order in which you need to introduce servers when planning an upgrade from Exchange 2003 or Exchange 2007 to Exchange 2010.

Objective Summary

- JetStress allows you to test how well a mailbox server handles simulated load. LoadGen allows you to simulate CAS load. Both tools can be used when determining whether it is feasible to consolidate existing servers.
- Single-phase upgrades minimize the coexistence periods. These are suitable for smaller organizations. Cutover to Exchange 2010 occurs rapidly organization-wide.

- Multiphase upgrades with coexistence have longer coexistence periods. This upgrade type is suitable for larger organizations. Parts of the organization are moved across to Exchange 2010 in stages, rather than all at once.
- If an organization needs to support Outlook 2003 clients, it will be necessary to retain a public folder infrastructure after the upgrade to Exchange 2010 is complete.
- When performing an upgrade, Internet-facing sites must be upgraded before sites that do not have a direct Internet connection.
- When upgrading from Exchange 2003, Exchange 2007, or a mixture of Exchange 2003 and Exchange 2007, introduce CAS to a site first, then Hub Transport, and then Mailbox servers. Add Edge Transport servers at Internet-facing sites as appropriate.
- Remove Exchange 2003 back-end servers first, but only after you have migrated all mailbox and public folder data from these servers.
- The Exchange Server Deployment Assistant can analyze a current environment to determine whether it meets the necessary infrastructure.

Objective Review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of this chapter.

1. You are in the process of planning a migration from Exchange Server 2003 to Exchange Server 2010. As part of your migration you want to consolidate your Exchange deployment onto fewer servers. You have purchased new hardware for an Exchange Server 2010 test deployment that reflects the hardware profile of the servers you will eventually deploy. In your new deployment, the Hub Transport, Mailbox, and Client Access Server roles will all be located on the same server. You need to determine how many client computers can use this server as part of your consolidation planning. Which of the following tools can you use to accomplish this goal?

   A. Exchange Server Load Generator 2010

   B. Exchange Server Jetstress 2010

   C. Exchange Remote Connectivity Analyzer

   D. Exchange Server Best Practices Analyzer

2. You are planning a transition from an environment running Exchange Server 2003 to Exchange Server 2010. You are planning on a coexistence period of approximately four months where both messaging systems must run side by side. Which of the following Exchange Server 2010 roles must you plan to install first?

   A. Hub Transport server

   B. Mailbox server

C. Client Access Server

D. Edge Transport server

3. You are planning the transition from Exchange Server 2003 to Exchange Server 2010. You will be deploying each Exchange Server 2010 role on a separate computer. You are working on the deployment order plan for each role. Which of the following Exchange Server 2010 roles would you deploy after all the others have been deployed?

   A. Mailbox server

   B. Client Access Server

   C. Hub Transport server

   D. Edge Transport server

4. You are planning a transition from an environment running Exchange Server 2007 to one running Exchange Server 2010. You expect the transition to take approximately three months. Your organization intends to keep using public folders, but you intend to use a third-party appliance as a mail gateway rather than an Edge Transport server. Which of the following Exchange Server 2010 roles must you deploy prior to starting to move mailboxes hosted on Exchange 2007 mailbox servers to Exchange 2010? (Choose all that apply.)

   A. Client Access Server

   B. Hub Transport server

   C. Mailbox server

   D. Edge Transport server

5. You are in the process of planning an upgrade of a mixed Exchange 2003 and Exchange 2007 environment to Exchange 2010. Which of the following tools can you use to analyze your organization's environment to determine whether the existing infrastructure is prepared for the deployment of Exchange Server 2010?

   A. Exchange Remote Connectivity Analyzer

   B. Exchange Best Practices Analyzer

   C. Exchange Pre-Deployment Analyzer

   D. Exchange Server Jetstress 2010

THOUGHT EXPERIMENT
Planning the Introduction of Exchange Server 2010 Where There Is an Existing Exchange Deployment

In the following thought experiment, apply what you've learned about the "Plan for transition and coexistence" objective to develop a design to meet an organization's needs. You can find answers to these questions in the "Answers" section at the end of this chapter.

Wingtip Toys and Tailspin Toys are in the process of merging. Each organization has its own Active Directory forest running at the Windows Server 2003 forest functional level. Wingtip Toys has an existing Exchange 2007 deployment. Tailspin Toys has an existing Exchange 2003 deployment. Wingtip Toys has only one Internet-facing site, which is located in Auckland, New Zealand. The other Wingtip Toys sites in Wellington, Dunedin, and Christchurch are all connected to the Auckland site via WAN links. Tailspin Toys has two Internet-facing sites in the cities of Melbourne and Sydney, Australia. The cities of Adelaide and Perth also have branch offices, and these are connected to the Internet-facing site through WAN links. You want to use Edge Transport servers for routing inbound and outbound messages. Each organization should retain its own Active Directory forest.

With this in mind, answer the following questions:

1. Which site or sites at Wingtip Toys should you plan to upgrade first?
2. Which site or sites at Tailspin Toys should you plan to upgrade first?
3. In which sites should you deploy Edge Transport servers?
4. Which multiple-forest topology should you use?
5. Which Microsoft product should you use to perform GAL synchronization between the Wingtip Toys and Tailspin Toys organizations?
6. Which server role will you introduce first at each organization and in which sites?
7. Which server role will you decommission first in the Wingtip Toys organization?

Chapter Summary

- Exchange Server 2010 can be installed in an on-premises, cloud, or coexistence configuration.
- SLA requirements determine parts of your Exchange design, primarily around high-availability features such as Database Availability Groups and Client Access Server Arrays.
- In multiple-forest environments, the resource-forest topology has Exchange deployed in one forest and accessed by users in other forests. The cross-forest topology has Exchange deployed in all forests and uses Forefront Identity Life Cycle Manager for GAL synchronization.
- Ensure that there is at least one Hub Transport server in every site where there is a Mailbox server on a per-forest basis.
- ActiveSync allows supported mobile devices to access mailbox data.
- You can configure Autodiscover to automatically provision Outlook 2007 and Outlook 2010 clients.
- The Load Generator (LoadGen) tool can be used to test a CAS against a simulated client workload.
- JetStress allows you to test how well a mailbox server handles simulated load. LoadGen allows you to simulate CAS load. Both tools can be used when determining whether it is feasible to consolidate existing servers.
- When performing an upgrade, Internet-facing sites must be upgraded before sites that do not have a direct Internet connection.
- When upgrading from previous versions of Exchange, introduce CAS to a site first, then Hub Transport, and then Mailbox servers. Add Edge Transport servers at Internet-facing sites as appropriate.
- The Exchange Server Deployment Assistant can analyze a current environment prior to the introduction of Exchange Server 2010.

Answers

This section contains the answers to the Object Reviews and the Thought Experiments.

Objective 1.1: Review

1. **Correct Answer:** D
   - **A. Incorrect:** Active Directory Administrative Center allows administrators to perform simple tasks such as password reset and can search Active Directory for information. Although you can extend the tool with custom components, by default it cannot be used to view information about Active Directory site configuration.
   - **B. Incorrect:** Active Directory Users and Computers can be used to view and manipulate user, computer, and group account information as well as manage organizational unit structure. You cannot use Active Directory Users and Computers to view or modify Active Directory site information.
   - **C. Incorrect:** Active Directory Domains and Trusts can be used to view forest information as well as to establish trust relationships with other forests or Kerberos realms. You cannot use Active Directory Domains and Trusts to view or modify Active Directory site information.
   - **D. Correct:** Active Directory Sites and Services can be used to verify current mappings between IP networks and specific Active Directory sites. You can also use this console to create mappings between IP networks and specific Active Directory sites.
2. **Correct Answers:** B and C
   - **A. Incorrect:** Both the primary DNS suffix and the DNS domain name must be included on the *msDS-AllowedDNSSuffixes* Active Directory attribute if Exchange is to function in an environment with a disjointed namespace.
   - **B. Correct:** To ensure that the Exchange servers can properly communicate with Active Directory, it is necessary to ensure that both the primary DNS suffix and the DNS domain name are included on the *msDS-AllowedDNSSuffixes* Active Directory attributed on the domain object container.
   - **C. Correct:** To ensure that the Exchange servers and clients can properly communicate in the disjointed namespace environment, you need to include both the primary DNS suffix and the DNS domain name in the DNS suffix search list group policy item.
   - **D. Incorrect:** You must include both the DNS domain name and the primary DNS suffix in the DNS suffix search list group policy item to ensure that the Exchange servers and clients can properly communicate in the disjointed namespace environment.

3. **Correct Answers:** A and D

   A. **Correct:** Tailspin Toys should use the cross-forest topology. This topology involves deploying Exchange in each forest and then using GAL synchronization to ensure that recipients from each forest are visible in every other forest.

   B. **Incorrect:** Tailspin Toys should not use the resource-forest topology because in this topology Exchange is only installed in one forest rather than all forests as suggested by the question text.

   C. **Incorrect:** Wingtip Toys should not use the cross-forest topology because Exchange should only be deployed in one forest at this organization.

   D. **Correct:** Wingtip Toys should use the resource-forest topology because in this topology Exchange is deployed in one forest and user accounts are stored in other forests.

4. **Correct Answer:** D

   A. **Incorrect:** System Center Configuration Manager 2012 can be used for application, software update, and operating system deployment. You cannot configure System Center Configuration Manager 2012 to measure service availability as part of monitoring compliance with an SLA.

   B. **Incorrect:** System Center Data Protection Manager 2012 can be used to back up and restore organizational data. You cannot configure System Center Data Protection Manager 2012 to measure service availability as part of monitoring compliance with an SLA.

   C. **Incorrect:** System Center Virtual Machine Manager 2012 allows you to manage large deployments of virtual machines. You cannot configure System Center Virtual Machine Manager 2012 to measure service availability as part of monitoring compliance with an SLA.

   D. **Correct:** System Center Operations Manager 2012 can be used to monitor service availability. System Center Operations Manager 2012 can raise alerts in the event that specific services or servers fail.

5. **Correct Answer:** C

   A. **Incorrect:** Forefront Threat Management Gateway 2010 is an advanced firewall product. You cannot use this product to support GAL synchronization in an Exchange cross-forest topology.

   B. **Incorrect:** Forefront Endpoint Protection 2012 is an anti-malware solution. You cannot use this product to support GAL synchronization in an Exchange cross-forest topology.

   C. **Correct:** Forefront Identity Life Cycle Manager 2010 can be used to implement GAL synchronization when Exchange Server 2010 is deployed in a cross-forest topology.

D. **Incorrect:** Forefront Unified Access Gateway 2010 allows you to provide access to internal resources for external clients. You cannot use this product to support GAL synchronization in an Exchange cross-forest topology.

Objective 1.1: Thought Experiment

1. You need to configure single sign-on prior to configuring directory synchronization.
2. You need to ensure that the domain that you are federating can be resolved by hosts on the Internet. You need to configure User Principle Names for all users. You need to deploy Active Directory Federation Services.
3. It will be necessary to deploy a computer to host the Directory Synchronization and an Exchange Server 2010 coexistence server.

Objective 1.2: Review

1. **Correct Answer:** B
   A. **Incorrect:** You use authoritative domains for email domains where the intended recipient has a mailbox hosted within the same Exchange organization, or where the email domain is split across Exchange and another messaging system.
   B. **Correct:** You would configure an Internal Relay domain to ensure that your Exchange organization would accept messages and then route them to a third-party messaging system hosted on your organization's internal network.
   C. **Incorrect:** You use an external relay domain when you want your Exchange organization to accept email messages and then route them to another messaging system.
   D. **Incorrect:** You use a reverse lookup zone to provide IP address to FQDN translation. This is created in DNS and is not something that you need to set up to ensure that your Exchange organization accepts messages and then routes them to a third-party messaging system hosted on the organization's internal network.
2. **Correct Answers:** A and D
   A. **Correct:** TCP port 25 is required for message transport between Edge Transport and Hub Transport servers.
   B. **Incorrect:** TCP port 135 is used for RPC communication between mailbox servers and Hub Transport servers. This port is not used for communication between Edge Transport servers and Hub Transport servers.
   C. **Incorrect:** TCP port 389 is used for LDAP communication between Hub Transport servers and Active Directory Domain Controllers. This port is not used for communication between Edge Transport servers and Hub Transport servers.

D. **Correct:** TCP port 50636 is used by the edge synchronization process to replicate configuration data from Hub Transport servers to Edge Transport servers.

3. **Correct Answers:** A and D

   A. **Correct:** You need to configure an internal relay domain and a Send connector when using a shared address space.

   B. **Incorrect:** You do not need to configure a remote domain when supporting a shared address space. Remote domains are used to configure message formatting options as well as whether out-of-office information is transmitted to remote recipients.

   C. **Incorrect:** You do not need to configure an external relay domain. External relay domains are used to route mail to organizations outside your internal network. In this case the organization is located on your internal network.

   D. **Correct:** You need to configure an internal relay domain and a Send connector when using a shared address space.

4. **Correct Answer:** B

   A. **Incorrect:** The *Set-ADSite* cmdlet is used to configure Active Directory site properties in Exchange. You cannot use this cmdlet to configure an Exchange specific cost for an Active Directory IP site link.

   B. **Correct:** You can use the *Set-ADSiteLink* cmdlet to configure an Exchange specific cost for an Active Directory IP site link.

   C. **Incorrect:** The *Get-ADSite* cmdlet provides information about Active Directory sites. You cannot use this cmdlet to configure an Exchange specific cost for an Active Directory IP site link.

   D. **Incorrect:** The *Get-ADSiteLink* cmdlet allows you to view the properties of Active Directory IP site links. You cannot use this cmdlet to configure an Exchange specific cost for an Active Directory IP site link.

5. **Correct Answer:** D

   A. **Incorrect:** Remote domains are used to control message formatting and out-of-office messages. You can't use remote domains as a redundancy technology.

   B. **Incorrect:** Send connectors are used to route messages to locations outside the Exchange organization. You can't use Send connectors as a redundancy technology.

   C. **Incorrect:** The transport dumpster is a redundancy feature that is used with database availability groups.

   D. **Correct:** Shadow redundancy is a transport server feature that ensures that email messages are not lost in transit if a transport server fails.

Objective 1.2: Thought Experiment

1. You should configure an external relay domain because the Fabrikam mail servers are not located on your organization's internal network.
2. You configure message throttling to ensure that a transport server is not overwhelmed by too much message traffic.
3. Use the *Set-Transport* cmdlet with the *MaxConnectionRatePerMinute* parameter to configure the maximum connection rate per minute for inbound connections.
4. Use the *Set-ADSite* cmdlet to configure the Sydney site as a hub site.
5. Use the *Set-ADSiteLink* cmdlet to configure Exchange costs for the Active Directory site links that connect the Melbourne and Brisbane sites to the Sydney site.

Objective 1.3: Review

1. **Correct Answers:** A and C
   - A. **Correct:** You need to ensure that a trust relationship is established between the resource forest and the domains that host accounts in the account forests. The easiest way to accomplish this is to set up forest trusts, although in environments with more complex security needs you may configure more selective trusts.
   - B. **Incorrect:** You do not need to install Exchange 2010 in the account forests to accomplish this goal. Exchange 2010 is installed in multiple forests.
   - C. **Correct:** Linked mailboxes are created in the resource forest and linked to accounts in the account forests.
   - D. **Incorrect:** You create linked mailboxes in the resource forest and not in the account forest.
2. **Correct Answer:** D
   - A. **Incorrect:** The *New-Mailbox* cmdlet is used to create mailboxes. In this case, you want to create a group which uses a query against an Active Directory attribute to populate its membership.
   - B. **Incorrect:** The *New-DistributionGroup* cmdlet allows you to create a new distribution group. Distribution groups have static memberships and require manual membership changes, which is not appropriate given management's requirements in this situation.
   - C. **Incorrect:** The *Set-DistributionGroup* cmdlet is used to modify the properties of an existing distribution group. You cannot use the *Set-DistributionGroup* cmdlet to create a dynamic distribution group.
   - D. **Correct:** Dynamic distribution groups can be configured using queries based on an Active Directory attribute, such as department membership. The membership of dynamic distribution groups is determined when the group is expanded on a Hub Transport server.

3. **Correct Answer:** C

   A. **Incorrect:** You cannot use the *New-MailboxDatabase* cmdlet to modify the default mailbox database maximum size limit on an Exchange Server 2010 SP1 mailbox server. You can only modify this limit by editing the registry.

   B. **Incorrect:** You cannot use the *Get-MailboxDatabase* cmdlet to modify the default mailbox database maximum size limit on an Exchange Server 2010 SP1 mailbox server. You can only modify this limit by editing the registry.

   C. **Correct:** The default maximum mailbox database size on an Exchange Server 2010 SP1 mailbox database server is 1024 GB. You can increase this size by editing the registry.

   D. **Incorrect:** You cannot use the *Set-MailboxDatabase* cmdlet to modify the default mailbox database maximum size limit on an Exchange Server 2010 SP1 mailbox server. You can only modify this limit by editing the registry.

4. **Correct Answer:** A

   A. **Correct:** Each Exchange Server 2010 SP1 mailbox server can only host one public folder database. This is irrespective of whether the server has an Enterprise or a Standard license. Five servers means a maximum of five public folder databases.

   B. **Incorrect:** Each Exchange mailbox server can only host one public folder database. Because there are only five mailbox servers, there is a maximum of five public folder databases.

   C. **Incorrect:** Each Exchange mailbox server can only host one public folder database. Because there are only five mailbox servers, there is a maximum of five public folder databases.

   D. **Incorrect:** Each Exchange mailbox server can only host one public folder database. Because there are only five mailbox servers, there is a maximum of five public folder databases.

5. **Correct Answers:** A, C, and D

   A. **Correct:** You use the *New-AcceptedDomain* cmdlet to create a new accepted domain. This will be necessary if you want to use the email domain cohowinery.com in an email address policy.

   B. **Incorrect:** *Get-EmailAddressPolicy* lists the properties of an email address policy. You can't use this cmdlet to create and apply a new email address policy.

   C. **Correct:** You use the *New-EmailAddressPolicy* to create a policy that will apply the cohowinery.com email domain in default reply-to addresses in the organization. It is also possible to modify the existing policy, but that option was not available.

   D. **Correct:** You use the *Update-EmailAddressPolicy* cmdlet to apply a new or modified email address policy.

Objective 1.3: Thought Experiment

1. You should set up linked mailboxes in the Contoso.com Exchange organization for users with accounts in the Fabrikam.com forest.
2. You can modify the existing email address policy or create a new email address policy.
3. You should create a static distribution group. This will allow you to delegate the appropriate administrative privileges to Simone from Accounts Receivable.
4. You should make Simone from Accounts Receivable the group owner, also known as the group manager.
5. Set the approval setting to Owner Approval. This will allow Simone from Accounts Receivable to approve membership.

Objective 1.4: Review

1. **Correct Answer:** A
   - A. **Correct:** The LoadGen tool, also known as the Exchange Server Load Generator, allows you to test the adequacy of a CAS deployment for a specific number of clients.
   - B. **Incorrect:** The Jetstress tool allows you to simulate mailbox database I/O and is suitable for testing mailbox server performance, but it does not allow you to simulate specific client load against a CAS deployment.
   - C. **Incorrect:** The Exchange Best Practices Analyzer allows you to compare an Exchange deployment against best practices, but it does not allow you to simulate specific client load against a CAS deployment.
   - D. **Incorrect:** The Remote Connectivity Analyzer allows you to verify that ActiveSync, Exchange Web Services, Outlook, and Internet Email work correctly, but it cannot be used to simulate specific client load against a CAS deployment.
2. **Correct Answer:** C
   - A. **Incorrect:** It is necessary to have a Client Access Server in each site where there is a mailbox server. Deploying one Client Access Server would be insufficient when the proposed design has five sites with mailbox servers.
   - B. **Incorrect:** It is necessary to have a Client Access Server in each site where there is a mailbox server. Deploying four Client Access Server would be insufficient when the proposed design has five sites with mailbox servers.
   - C. **Correct:** It is necessary to have a Client Access Server in each site where there is a mailbox server. Because there are five sites, a minimum of five Client Access Servers are necessary.

D. **Incorrect:** It is necessary to have a Client Access Server in each site where there is a mailbox server. Although having seven Client Access Servers would provide redundancy in the event that a Client Access Server failed, five Client Access Servers is the minimum amount necessary.

3. **Correct Answer:** A

A. **Correct:** The mailbox servers are only in a single site, so you only need to deploy a single Client Access Server to support this configuration.

B. **Incorrect:** You only need to deploy a single Client Access Server to support this configuration.

C. **Incorrect:** You only need to deploy a single Client Access Server to support this configuration.

D. **Incorrect:** You only need to deploy a single Client Access Server to support this configuration.

4. **Correct Answer:** A

A. **Correct:** Microsoft's theoretical optimum ratio is that there are three processor cores on a site's Client Access Servers for every four processor cores on a site's Mailbox servers.

B. **Incorrect:** Microsoft's theoretical optimum ratio is that there are three processor cores on a site's Client Access Servers for every four processor cores on a site's Mailbox servers.

C. **Incorrect:** Microsoft's theoretical optimum ratio is that there are three processor cores on a site's Client Access Servers for every four processor cores on a site's Mailbox servers.

D. **Incorrect:** Microsoft's theoretical optimum ratio is that there are three processor cores on a site's Client Access Servers for every four processor cores on a site's Mailbox servers.

5. **Correct Answer:** C

A. **Incorrect:** Configuring the Autodiscover service for Internet Access allows clients on external networks to be configured automatically through Autodiscover. Taking this step will not ensure that Outlook 2010 clients get Autodiscover information from the closest Active Directory site.

B. **Incorrect:** Configuring the Autodiscover for multiple forests allows users running Outlook 2007 or Outlook 2010 in one forest to access Client Access Servers in a remote forest. Taking this step will not ensure that Outlook 2010 clients get Autodiscover information from the closest Active Directory site.

C. **Correct:** Configuring the Autodiscover service for Site Affinity ensures that Outlook 2007 and Outlook 2010 clients get Autodiscover information from the closest Active Directory site.

D. **Incorrect:** Configuring the Exchange ActiveSync Autodiscover settings allows automatic configuration of ActiveSync clients. Taking this step will not ensure that Outlook 2010 clients get Autodiscover information from the closest Active Directory site.

Objective 1.4: Thought Experiment

1. You must deploy Client Access Serves in the Auckland, Wellington, Dunedin, and Christchurch sites.
2. You can ensure that clients using Autodiscover are provisioned with profile information from the closest Active Directory site by configuring site affinity.
3. You can configure CAS to use the same name for all services, you can use certificates that support SANs, or you could configure the CAS with wildcard certificates.
4. You should deploy Outlook Anywhere because you want to allow remote access to Exchange mailboxes for clients running Outlook 2010 without configuring VPN or DirectAccess.
5. Because you need to support users accessing Outlook Web App from personal computers, you should use a trusted third-party CA, which will minimize the problems involved in getting clients to trust the certificates.

Objective 1.5: Review

1. **Correct Answer:** A

   A. **Correct:** The Exchange Server Load Generator 2010 allows you to test a simulated client workload against all aspects of an Exchange Server 2010 deployment. You can use this tool to determine how many clients a simulated Exchange Server 2010 deployment can comfortably handle.

   B. **Incorrect:** The Exchange Server Jetstress 2010 tool allows you to benchmark mailbox server storage, but does not allow you to test other aspects of an Exchange Server deployment.

   C. **Incorrect:** The Exchange Server Remote Connectivity Analyzer allows you to test client connectivity configuration, but does not allow you to test an Exchange server deployment against a simulated number of clients.

   D. **Incorrect:** The Exchange Server Best Practices Analyzer allows you to diagnose an existing deployment against Exchange best practices. You cannot use this tool to determine the capacity of an Exchange deployment.

2. **Correct Answer:** C

   A. **Incorrect:** You must install the Client Access Server role first when transitioning from Exchange 2003 to Exchange 2010. You install the Hub Transport server role after installing the Client Access Server role.

   B. **Incorrect:** You must install the Client Access Server role first when transitioning from Exchange 2003 to Exchange 2010. You install the Mailbox server role after you have installed the Client Access and Hub Transport server roles.

   C. **Correct:** You must install the Client Access Server role first when transitioning from Exchange 2003 to Exchange 2010.

   D. **Incorrect:** You must install the Client Access Server role first when transitioning from Exchange 2003 to Exchange 2010. You install the Edge Transport server role after you have installed the Client Access, Mailbox, and Hub Transport server roles.

3. **Correct Answer:** D

   A. **Incorrect:** When transitioning from an Exchange 2003 environment to an Exchange 2010 environment, the Edge Transport server role is installed after the other roles have been deployed.

   B. **Incorrect:** When transitioning from an Exchange 2003 environment to an Exchange 2010 environment, the Edge Transport server role is installed after the other roles have been deployed.

   C. **Incorrect:** When transitioning from an Exchange 2003 environment to an Exchange 2010 environment, the Edge Transport server role is installed after the other roles have been deployed.

   D. **Correct:** When transitioning from an Exchange 2003 environment to an Exchange 2010 environment, the Edge Transport server role is installed after the other roles have been deployed.

4. **Correct Answers:** A, B, and C

   A. **Correct:** You must plan to deploy the Client Access, Hub Transport, and Mailbox server roles before it is possible to migrate mailboxes from Exchange 2007 to Exchange 2010 Mailbox servers.

   B. **Correct:** You must plan to deploy the Client Access, Hub Transport, and Mailbox server roles before it is possible to migrate mailboxes from Exchange 2007 to Exchange 2010 Mailbox servers.

   C. **Correct:** You must plan to deploy the Client Access, Hub Transport, and Mailbox server roles before it is possible to migrate mailboxes from Exchange 2007 to Exchange 2010 Mailbox servers.

   D. **Incorrect:** The design will not use an Edge Transport server, so it is not necessary to deploy this role prior to migrating mailboxes from Exchange 2007.

5. **Correct Answer:** C

   A. **Incorrect:** The Exchange Remote Connectivity Analyzer allows you to verify remote connectivity to a Client Access Server. You can't use this tool to determine whether Exchange 2003 and Exchange 2007 are ready for the deployment of Exchange 2010.

   B. **Incorrect:** The Exchange Best Practices Analyzer allows you to examine your organization's environment to determine whether your Exchange configuration complies with best practices. You can't use this tool to determine whether Exchange 2003 and Exchange 2007 are ready for the deployment of Exchange 2010.

   C. **Correct:** The Exchange Pre-Deployment Analyzer can examine your organization's environment to determine whether Exchange 2003 and Exchange 2007 are ready for the upgrade or transition to Exchange 2010.

   D. **Incorrect:** The Exchange Server Jetstress 2010 tool allows you to analyze mailbox server storage to assess performance characteristics under a specified load. You can't use this tool to determine whether Exchange 2003 and Exchange 2007 are ready for the deployment of Exchange 2010.

Objective 1.5: Thought Experiment

1. You should plan to upgrade the Auckland site at Wingtip Toys first because this site is Internet-facing.
2. You should plan to upgrade the Melbourne and Sydney Tailspin Toys sites first because these sites are Internet-facing.
3. You will need to deploy Edge Transport servers in the Melbourne, Sydney, and Auckland sites because these sites are Internet-facing.
4. You should use the cross-forest topology because both Wingtip Toys and Tailspin Toys will retain their own Exchange 2010 organizations.
5. You should use Forefront Identity Manger 2010 to perform GAL synchronization between the Wingtip Toys and Tailspin Toys Exchange organizations given that a trust exists between them.
6. You should deploy the Client Access Server role at the Melbourne, Sydney, and Auckland sites first.
7. You will decommission the Wingtip Toys back-end servers first.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

About the Author

ORIN THOMAS holds multiple MCITP certifications, including the Enterprise Messaging Administrator 2010 credential. His first job managing a production Exchange deployment was running Exchange 5.5 at one of Australia's biggest manufacturing companies more than a decade ago. He is an MCT, a Microsoft MVP, and is a contributing editor at *Windows IT Pro* magazine. He regularly speaks at events in Australia and around the world, including TechED and Microsoft Management Summit. Orin founded and runs the Melbourne System Center Users Group, and has authored more than 20 books for Microsoft Press, including books on Exchange 2003, Exchange 2007, and Exchange 2010. You can follow him on Twitter at *http://twitter.com/orinthomas*.